Kevin Orrey

Cyber Attack: Exploiting the User - There are so many ways!

MSc Computer Security and Forensics
Masters Thesis Report
Faculty of Creative Arts, Technologies and Science (CATS)

Dr Ali Mansour

2010/11

Abstract

Cyber Attacks are reportedly being conducted world-wide on a daily basis targeting individuals, corporations and countries alike. Whilst corporations such as Google and countries such as America attempt to mitigate such attacks, for the most part, users do not even realise they have been targeted! Given the wide range of applications, protocols and operating systems currently in use, attack vectors are often wide and varied, ensuring users are vulnerable in a plethora of ways. The motive and reasoning behind these attacks are normally categorised as monetary gain, politically motivated or just for kudos and enhanced credibility amongst peer groups.

Attack vectors may include so called social engineering and phishing attacks with users being duped into clicking links or visiting nefarious websites leading to exploitation or theft of personal credentials. This was purportedly the method used by Chinese hackers in the Google Aurora attack according to the United States-China Economic and Security Review Commission.

Physical access attacks can also be successful via the use of removable media which may contain pre-loaded malware. Malware may be coded to grab copies of documents, system passwords, encrypt the hard drive or worse still destroy all data contained thereon. A recent attack in this field, the Stuxnet worm, has been developed which even enables the auto-exploitation of computers with extremely limited, if any, user and operating system interaction.

To mitigate against these attack vectors, defense in depth mechanisms should be employed as suggested by the SANS Technology Institute. Additional reading such as the NSA Lockdown guides goes some way to add a level of protection for users, furthermore they advise on mechanisms to protect IT networks.

This thesis will research and evaluate disparate attack vectors which are being utilised today to successfully to exploit users. It will explore why users are susceptible, the countermeasures that can be applied to protect them and will be followed by a critical analysis of the attack vectors discussed. In addition it will demonstrate that such attacks can and sometimes are combined to make them more dangerous based on certain set conditions.

Table of Contents

Table of Figures

CHAPTER 1: INTRODUCTION

1.1 Background

Cyber Attacks are described by (Tatum, 2010), as "*an attempt to undermine or compromise the function of a computer-based system, or attempt to track the online movements of individuals without their permission. Attacks of this type may be undetectable to the end user... or lead to such a total disruption of the network that none of the users can perform even the most rudimentary of tasks*". Computer Network Attacks (CNA) achieves the above but more specifically according to the Cyberspace and Information Study Centre is specifically geared towards attacking military type systems, with the intention to "*disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves*."

There is a clear and ever present threat from Cyber Attacks as reported by the BBC, (2010) but targets of such attacks are not just the preserve of countries, as was historically the case, today individual users can and are often targeted. Whilst targeting of users becomes more complex and common place, organisations and society in general struggle to maintain an adequate level of awareness through education and pragmatic steps need to be taken to increase awareness and training.

Organisations have the ability to instigate user education programs to aid user awareness which may complement existing mechanisms such as hardware and software security boundaries. This awareness training, however, can often take years to complete and with personnel turnover so high in some organisations, full adoption is unlikely to succeed. The UK Cabinet Office conducted its Data Handling Review in 2007 with The Register reporting that today "*more than 92 per cent of MoD staffs have now completed the appropriate level of awareness training*". This awareness training though is generally geared towards basic Physical and Personnel security, as opposed to education on aspects of software based Cyber-attacks, such as working from home, over the internet, browsing from within the corporate environs or general home use. This leaves the user unaware of wider threat vectors. The user thus has to rely on second and third hand information gleaned from the media and hearsay, which does nothing to aid, educate or mitigate potential attack vectors.

Any security boundary is only as strong as its weakest link and whilst it's true to say according to the latest report from Tipping Point's DVLabs, (2010) systems are becoming more secure with patches being released quicker by vendors to plug security holes, improving patching strategies and effective lockdown guides, coupled with improved application security support. Users though, are generally the weak link in the defense-in depth analogy by inadvertently carrying out actions which open up the entire network to attack, bypassing any security controls in force.

1.2 Problem Statement

Cyber Attacks are a problem that is ever increasing and some of this is due to the fact the world is becoming more and more interconnected electronically as the work force becomes more and more geographically remotely spread. Today we have moved to a non-traditional work arrangements, have a lack of qualified IT Security professionals, increased financial pressures on providing secure infrastructure, and ever increasing customer demands and expectations according to Jacknowitz (2010). These factors provide a larger attack space for attackers to access networks previously unavailable 5 – 10 years ago. Most work was then conducted within potentially more secure corporate environs which had limited external connectivity and thus were less exposed. In essence users have moved outside the perceived secure bastions that corporate networks provided thereby opening themselves up to different attack vectors with less support available to them and consequently limited protection afforded to them.

Communication Electronic Security Group (CESG, 2009) state threat sources and actors actively involved in attacks come from numerous sources each with their own motives, goals, capability and funding:

a. Insiders (Disaffected or dishonest employees),

b. Foreign Intelligence Services (FIS),

c. Hackers, virus and malware writers,

d. Terrorist and Extremist Groups,

e. Investigative Journalists,

f. Commercial Competitors and Service Providers,

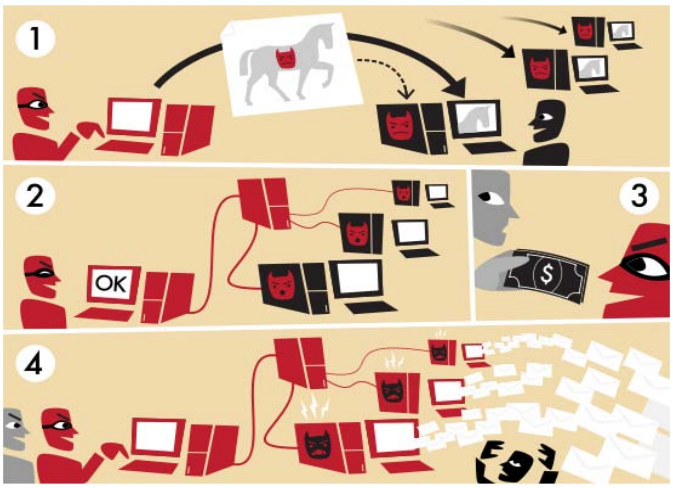
g. Organised Criminal groups,

h. Radio Enthusiasts,

i. Academic Researchers to name but a few.

Attacks have evolved to specifically target the user, they are diverse, simple to execute and for the most part highly successful. As an example, botnets[1], are created when computers become infected with viruses and Trojan horses. A user can be exploited and used in a botnet via clicking innocuous email links and attachments, once infected their machine can be used to carry out Distributed Denial of Service (DDoS) attacks or Spamming campaigns. To show how big they are the Mariposa botnet recently infected in excess of 13 million computers before it was taken down according to Techworld.com, (2010), in addition the Kroxxu botnet is currently active and has potentially infected over a million users to date according to SC Magazine, (2010). The Mariposa and Kroxxu botnets are just two of many hundreds of similar ones and the likely scale of computers infected will likely run to tens of millions of hosts.

[1] A botnet is a "*group of computer systems that have had malicious software installed by worms, Trojan horses or other malicious software that allows the "botnet herder" or botnet's originator to control the group remotely*". (Michigan.gov, 2010)



1 – Users are infected with malware

2 – Users join a botnet after being infected

3 – Botnet Herder receives a payment to provide a service

4 – Spam is sent from the botnet to millions of undisclosed users

Figure 1 - Botnets – Initial infection to Profitable use (Kath, 2010)

Users can be targeted in a number of ways but generally from the three main problem areas to be discussed further in this thesis:

a. Network based attacks – Encompasses all possible attacks designed to exploit software vulnerabilities locally, remotely or whilst data is routed along network paths from source to destination.

b. Physical Security Issues - This encompasses all attacks specifically designed to utilise hardware to exploit vulnerabilities and weaknesses in a system which in turn lead to the compromise of an unsuspecting user.

c. Personal Security Issues - This encompasses all attacks designed to exploit the weaknesses and naivety of user's i.e. social engineering.

Any attack could target one specific area or all of those specified. Today threats and the associated attacks exploiting them are being combined together into what is known as Blended Threats. These are when an attacker combines the characteristics of viruses, worms, malicious code etc. with server, client-side and Internet vulnerabilities to initiate, transmit, and spread an attack. In this way multiple methods and techniques are used, enabling the rapid spread and widespread damage caused by malware and the increased chances of successful exploitation of victim computers. Multiple and differing attack vectors which, if used in combination, would increase the chances of an attacker's success. According to Websense, (2010), Cybercriminals are using a wide range of attack vectors in combination making "*blended threats ... the chief online security risk to enterprises [requiring] a new approach ….to defend against these threats*".

Attackers are becoming skilled at creating duplicate websites, using sophisticated exploit frameworks to auto-exploit visitors to these or simply steal credentials or online banking details. Building an effective response to these attacks and making users aware of the threats may go some way to reducing these attacks, but this has to be a constant and iterative process. Given that the nature of these threats is ever evolving user awareness cannot keep up with this as there are still too many unsuspecting users who do not get the message nor for that matter understand the threats they are subjected to.

This research will highlight how poor user education and awareness, coupled with inappropriately applied, configured and poorly updated defence mechanisms can lead to exploitation by multiple means and attack vectors.

1.2.1 Research Aims

This thesis will discuss separate attacks from these three areas, but they can easily be combined together to form an excellent example of a blended threat. The scenario for this thesis is that a user has a hardware USB device. This device contains many standalone portable applications, a web browser, a privacy and anonymity tool and the user lacks an awareness to the many threats they could be exposed to, which as previously documented is a realistic possibility.

These three things combined or in isolation potentially allow the end-user to be exploited in many ways:

a. Running an older version of a browser may open them up to browser exploits that have been patched by the latest web browser version,

b. Become infected with malware as they plug in the USB into an infected computer,

c. Enticed to visit websites which an attacker controls,

d. Logging on to websites without encryption potentially allowing credentials to be intercepted.

e. Plugging the USB into another network allowing malware to jump the “air-gap” from the original network and exploit more users and devices.

1.3 Objectives of Research

1.3.1 General Objectives

Identify research and document possible ways a Cyber Attack can be carried out against a user based on the thesis scenario.

1.3.2 Specific Objectives

The following are the specific objectives for this thesis:

- The need to identify problem areas that an attacker could use to actively exploit users.

- De-construct problem areas into distinct sections and identify and research attack vectors that utilise these.

- Provide guidance and recommendations on how to mitigate against the threats identified.

- Critically analyse the areas identified, commenting using comparative work and from personal experience.

1.4 Research Strategy

The strategy adopted for this thesis was to research and examine potential problem areas and vulnerabilities within them that can be used to target and exploit users. Firstly there would be a need to identify the potential problem areas and also correlate the reasons why users have been exploited in the past. The following factors either alone or in combination have left networks and users open to exploitation in the past, all of which an attacker will use time and time again for their own gains:

a. Poor patching regime,

b. Poor Anti-virus update policy,

c. Inadequate Business Continuity Plans,

d. Inadequate Security Training (Administrators and Users),

e. Inadequate User Awareness Training,

f. Misconfiguration of software/ hardware,

g. Default accounts left enabled.

All such factors identified can be blamed directly on users (and administrators alike) and hence the user is the weak link in **ANY** computer network, without them IT networks would potentially be more secure. Users introduce human weaknesses into the equation and this is what an attacker will use to their benefit.

Having identified the problem areas and possible vulnerabilities that affect them, there potentially would be a multitude of ways to exploit users through them. With so many issues and disparate threat vectors, a lot of these attacks would have previously been covered in great depth elsewhere i.e. Cross Site Scripting (XSS), SQL Injection Attacks etc. and so the primary focus of this work would be fourfold;

a. The proviso would be to research the most current Cyber Attack threats and potentially those that are still being utilised in the wild.

b. Review such attacks noting how they have evolved from previous iterations i.e. Stuxnet.

c. Concentrate on well-known attacks but trying to carry out research from another angle that may not have previously been covered in great depth.

d. Finally research an area that is still a threat, but has not been generally seen in the media for some time and therefore highly dangerous as new users may not be aware of the threats involved in using it.

With these primary goals now focused, follow-up action would be to identify some suitable candidates for further research. The following based on this strategy were selected to research further:

a. Certain problem areas have come to focus in recent months and are still being heavily researched i.e. physical security issues with the use of removable media to automatically infect computers. Microsoft (2010) currently report heavily on "*The Stuxnet Sting*" which is an automatic exploit mechanism that has evolved from a long line of previous attacks using such devices.

b. Other attacks most users not from the security community may not be aware of include problems with The Onion Router (Tor) network which is designed to enable Internet anonymity yet has a darker side that is open to abuse and in which the user has limited control over.

c. Phishing attacks (albeit with a twist), looking at potential ways a user is exploited and the mechanisms used to achieve this rather than how phishing attacks are deployed to the user via spam etc.

Having identified these areas, more thorough research into each was conducted together with identifying any countermeasures, hardware, software, user education etc. that could be utilised to reduce the associated risks from these forms of Cyber Attacks. In addition critical analysis of these areas was carried out which could be used as a platform for further research in the future.

1.5 Research Scope

The aim and focus of this thesis is to research potential attacks from the three problem areas based on the previously identified goals. This would be achieved by the identification of new threats, how they evolved from previous iterations and how previously identified attacks are still being utilised in the wild. Suitable candidates from each problem area were identified to research further:

a. Network - The use of Tor has been selected and user attacks in relation to this will be discussed.

b. Physical - The use of USB devices have been selected and research into how users can be exploited via this medium.

c. Personal Security - The naivety of users and lack of awareness in relation to phishing type attacks and the exploit frameworks utilised to exploit users will be discussed.

These three problem areas and the examples will be discussed separately but use of blended attacks could mean they directly overlap one another. For example a user may use Tor and have their credentials stolen (Network), accessing Tor via a USB device which becomes infected by malware (Physical) and who whilst browsing is coerced into visiting a nefarious website consequently getting exploited (Personal).

Specifically, the following from the three problem areas will provide;

a. Why in its current implementation vulnerabilities exist, how they can be mitigated against and what countermeasures can be applied to remove or reduce the risk associated with them. Finally to critically analyse these examples and make recommendations for improvements, further research etc.

b. Information Assurance advice and recommendations to System Administrators, Accreditors etc. and enable the ability to provide effective Security Education advice to end users. In this way the focus of this thesis is as follows:

   i. Provide a thorough understanding of the technology used.

   ii. Provide details of possible avenues of exploitation.

   iii. Expand knowledge of current and discuss future attack vectors.

   iv. Provide mitigation strategies and countermeasures to protect corporate or end user infrastructure.

1.6 Research Limitations

As the avenues to possible attack are huge there must be severe limitations placed on the boundaries of this thesis. The limitations are:

a. Only one specific example from each problem area is to be researched.

b. Only those attacks directly exploiting a user are to be researched.

c. Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF), SQL Injection and other similar user attack vectors are out of scope.

d. Denial of Service (DoS) Attacks are out of scope.

e. Attacks specifically targeting the operating system unless directly related to the attack are out of scope i.e. Exploits targeting a user who has an un-patched vulnerability associated with an open port and vulnerable service running upon it.

f. Attacks involving exploiting and manipulation of standard network services i.e. DNS are out of scope unless it directly relates to a vulnerability within the problem area i.e. using standard software update services whilst using Tor the user is directed to an attackers website rather than the correct DNS address.

g. A limitation on the available hardware and software utilised in the research precludes any in-depth analysis and software reverse-engineering of malware i.e. Stuxnet. No suitable sandbox environment and associated hardware to mimic an attack was available coupled with the required skill set to reverse engineer this complex piece of software.

h. The budget for research is extremely limited due to personal and corporate financial constraints.

i. Ensure whatever research carried out does not endanger the hardware utilised by the author. This would be achieved via the use of virtual machines, effective antivirus and firewall systems coupled with previous user awareness knowledge and experience within this field.

j. Protocol analysis is out of scope including the review of the cryptographic makeup and all such algorithms in use within the Tor network.

k. Tor hidden services are out of scope; this thesis looks at the basic implementation of Tor for web browsing only.

l. Traffic Analysis of Tor is briefly overviewed from an information leakage angle only, the actual analysis of traffic in use via Tor and attacks reviewing latency and shaping patterns is out of scope.

m. No real credentials are to be utilised when conducting tests on the Tor network. All tests are to be conducted within a VMWare virtual appliance.

n. Varied UK Legislation, (available from legislation.gov.uk, (2010)), was to be strictly adhered to i.e. Computer Misuse Act (1990) , Communications Act (2003) and the Regulation of Investigatory Powers Act (2000) etc.

o. Phishing and its derivatives and the way users are exploited via this means will be covered; other examples of social engineering techniques are out of scope.

1.7 Thesis Organisation

This thesis has been organised as follows:

Chapter One provides the background to the thesis and introduces the subject matter, the problem statement and identifies the research strategy and objectives.

Chapter Two provides a literary review of selected books, texts, published papers and web resources in relation to research conducted as part of the thesis. It provides an overview of the availability of relevant subject matter and topics covered in previous research conducted by security professionals and academic researchers in the past. It also outlines a comparison against previous work conducted in the field of research.

Chapter Three describes in great detail the ways to abuse Network Traffic, specifically focusing on the Tor Network. It details research into the vulnerabilities and exploitation potential for Network Traffic Abuse, associated mitigation and countermeasure techniques are identified that may reduce the risks associated with these vulnerabilities. In addition it provides a critical analysis of the problem area discussed.

Chapter Four describes in great detail Physical Security issues specifically focusing on the history of USB Attacks with a case study on the Stuxnet worm. It details research into the vulnerabilities and exploitation potential using removable media and provides countermeasures which may be applied to protect users from these associated threats. In addition it provides a critical analysis of the problem within the area discussed.

Chapter Five describes in great detail Personal Security issues specifically focusing on Phishing and the use of Exploitation frameworks. It details the many ways phishing type attacks occurs and the Exploit packs in use today together with providing an analysis of the vulnerabilities they target. Countermeasures against the associated threats and a critical analysis of the use of Phishing and Exploit Packs are also discussed.

Chapter Six outlines any conclusions identified from research conducted for the thesis and provides a summary and recommendations based on the findings in the thesis. It outlines the potential for follow-up research that could be conducted to further enhance the knowledge into the selected subject areas.

CHAPTER 2: LITERATURE REVIEW AND COMPARISON AGAINST PREVIOUS WORK

2.1 Literature Review

Thorough research over the three problem areas revealed a plethora of resources, some of which were entirely relevant, some though, (Sky News, 2010), were highly speculative and unsubstantiated. A balanced and substantiated review was thus carried out on papers, web resources and books relevant to:

a. Network Traffic Abuse.

b. Physical Security Issues.

c. Personal Security.

2.1.2 Network Traffic Abuse

In reviewing what literary sources are available to aid in research for this thesis it was found that there are no books relating solely to Tor and its specific vulnerabilities.

The network has been around for many years, however anecdotal evidence suggests the limited financial gain of this project is potentially the reason why no texts have been written. The lack of work may also be down to the fact the Tor network is quite small and niche and there is far more scope and issues surrounding more prevalent, operating systems/ applications etc.

There also exist few papers published on the network. The majority of those published have been produced by Security Researchers or academics that have used certain topics about this network for their thesis or presentation at various Hacker conferences. Perry's (2007) paper on securing the Tor network provides a generalized overview of Tor and some generic attacks that can be made against it alongside possible countermeasures and mitigation strategies. This paper is, however, not very in depth and as such provides only a starting point to conduct further in depth research from. Perry's, (2008) work on traffic flow is, however, very much different and covers an in depth analysis of traffic flow through Tor, something his previous years talk would have benefited from being included. This looks into research into identifying malicious exit nodes but it provokes more research due to its lack of definitive results.

Bauer et al, (2007) provides a more in depth insight into Tor, including how node selection takes place and possible ways an attacker can manipulate this. *"Tor's tendency to favour routers that claim to be high-resource with high-uptime"* allows attackers to strip off anonymity protection usually provided in the network. Experimental results are also provided as evidence to add weight to their suppositions.

Huber et al (2010) provided sound experimental data on the protocols in use over Tor and thus provides a starting point for this thesis into the possible attacks on both privacy and anonymity. The amount of traffic over Tor that uses clear-text protocols is extremely high and the limited protection used by users according to their research intimates that an attacker with a malicious exit node would have an effective attack platform.

2.1.3 Physical Security Issues

Analysis of Stuxnet is still ongoing by varied antivirus vendors and security professionals as is the research into the particular malware and as such no books have been written, however, it is opined that this will change in the near future as its use and implications are profound and a turning point in malware infection and targeting of specific systems using multiple attack vectors.

Brian and Barbara Anderson (2010) recently released a text detailing the history of attacks utilising USB which forms part of the popular Syngress series detailing a number of attacks against a plethora of technologies. It is a shame that this book was released prior to the discovery of Stuxnet as it provides a great deal of information on attacks specifically using USB devices as well as providing good background to the history of such attacks and the technology that allows them to happen. The book is well written, easily understood, technically detailed, although appears to have an awful lot of information cut/ pasted from varied web resources which pads out the book somewhat.

Most resources relating to Stuxnet are web-based with few papers available to research from. By far the most comprehensive and informative paper from those available is that from the research conducted by the Symantec Corporation, (2010*)*. This is a very technically complex read, hugely comprehensive having resourced information not just in-house but from external security researchers and vendors alike. The amount of detail and length of the paper adds to the weight of how important a threat the Security industry thinks the Stuxnet malware is and the fact it is leap years ahead of any malware attacks and techniques previously seen. Kaspersky, (2010) presented its analysis of Stuxnet at the Virus Bulletin 2010 Conference alongside Symantec. This was very much just an overview of Stuxnet and obviously just a small subset of the information they have on the subject judging by the Stuxnet Mindmap they presented which detailed the huge amount of interactions between systems, services and resources. It is a pity the actual paper that the presentation came from is not released which would be complementary to the paper presented by Symantec. No doubt in 2011 when “Hacker” conference season starts again, there will be numerous lectures and papers about this topic.

A large amount of Stuxnet related material on the web also delves into conspiracy theories discussing possible attribution and its intended target. The majority of sources, (War in Context, (2010), BBC, (2010), ComputerWorld, (2010) indicate that the Bushehr Nuclear Reactor as the intended target and the US or Israel as potential perpetrators. Initial web reports were speculative at best but as more and more information became available on the inner workings of Stuxnet, the initial target could be a plausible possibility. From the research perspective of this thesis the actual target and its perpetrators are superfluous, it is the inner workings of Stuxnet that is important and the technology behind it, and hence a lot of resources were discounted.

2.1.4 Personal Security Issues

Limited literature exists relating exclusively to Phishing. Authors now seem to be putting more emphasis on the whole social engineering perspective with phishing purely referenced as part of this. Exploit packs do not seem to have been given much coverage within the published arena. Of the purely phishing texts released, Lininger et al, (2005) provides in this very dated text an overview of phishing, introducing a subject that at the time of writing was

still in its time of infancy and on the rise. The book itself is not very technical, possibly due to the target audience but also due to the way phishing was conducted at that time. Industrialisation of the process is not alluded to and it very much goes into manually carrying this attack out. James, (2005), goes one step further and although still provides a basic introduction is more technical in mind and introduces the use of exploit code within phishing sites as a dual attack mechanism. Other attack mechanisms and channels are also explored i.e. Session Initial Protocol, (SIP) and how social engineering techniques are starting to be utilised as a way of obtaining more information about users to enable them to be targeted better. As technology has progressed these books have become out-dated, other such white papers and web resources were thus of more use during research for this thesis.

Shema, (2010) provides an interesting chapter on the web of distrust specifically referencing malicious websites, the techniques used to exploit users and the avenues of such attacks. In addition he intimates the complexity of the resources used by an attacker whereby they can customise content delivered to a victim on-the-fly and black or whitelist those they wish to attack based on geolocation data. Although not specifically referencing exploit packs as such, the technology employed is essentially the same.

MessageLabs, (2010), in their recent Annual Security Report based on statistics obtained from spam filtering and blocking services recorded that one out of every 284.2 emails during 2010 contained malware. It also reported that attackers have increased the use of different types of malware by a factor of 100 over the 12 months to almost 340. This change potentially reflects the increased use of open source and commercial tools that attackers have been using to quickly and simply craft infected mail, providing the facility to automate inclusion of differing types of malware that potentially will not be blocked by anti-virus or spam filtering products consequently having a better chance of success. Phishing emails account for only 1 in every 444.5 and appears to be on the decline.

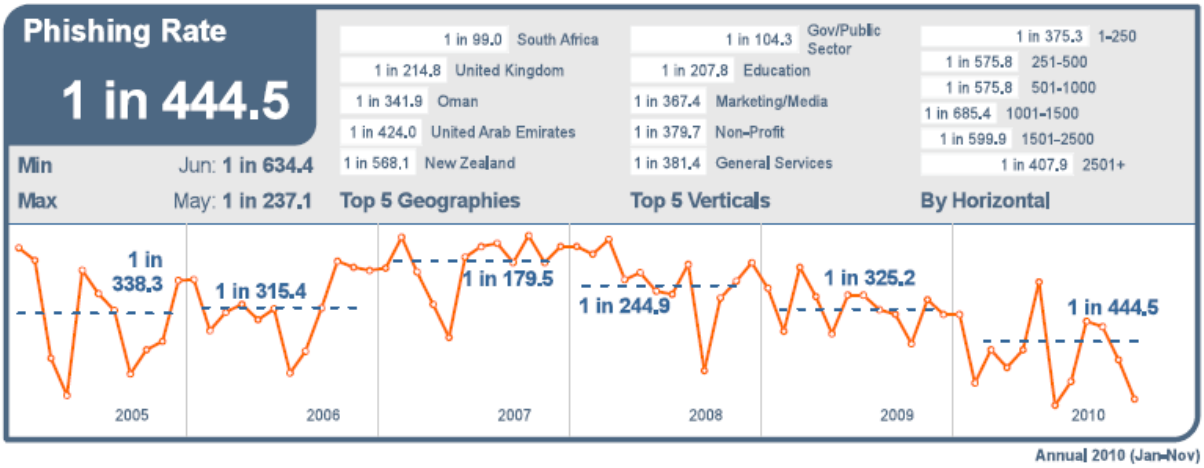


Figure 2 Phishing Rates (Secunia, 2010)

All other reference materials relating to exploit packs and their use within phishing were limited to web resources the majority of which relate to large Security vendors, Symantec, Avast and McAfee, etc. and a few niche sites that deal with malware and their use within exploit packs, (MalwareIntelligence, 2010; KrebsonSecurity, 2010) Due to the underground nature of the distribution and use of exploit packs, the majority of these resources just provide a snapshot of what is in use in the wild and what exploit they specifically target.

Most literary sources point to the fact that exploit packs are becoming more application than OS vulnerability centric. This may be due to the fact that OS vendors are making their

platforms more secure, or when a vulnerability has been identified their update mechanism is much more robust with automated Microsoft Update and Windows Service Update Services (WSUS) for the Enterprise to protect users. Certain 3rd party applications have manually configured update programs and are not as extensible as OS variants, the frequency and complexity of needing to manage many different update mechanisms will most probably mean that users are not fully covered. This all combined with inadequate user awareness to the threat posed by not patching 3rd party applications is a boon to attackers which they are actively exploiting. This is backed up by Secunia, (2010) in its half yearly report. A user who has 50 programs installed which will have 3.5 times more vulnerabilities in 3rd party programs than in the Microsoft programs installed. This ratio is expected to rise to 4.4 before the end of 2010.

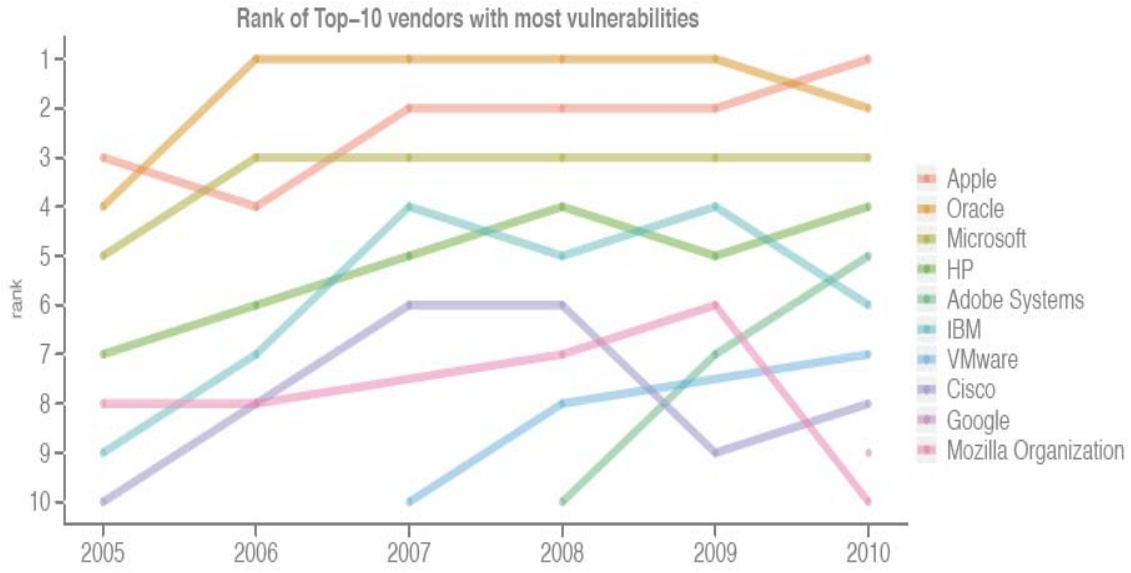


Figure 3 Ranking of the Top-10 vendors with most vulnerabilities per year (Secunia, 2010)

It has been agreed by numerous sources, Microsoft, and KrebsonSecurity (2010), to name but a few, that Java by far is the current exploit mechanism of choice at the moment.

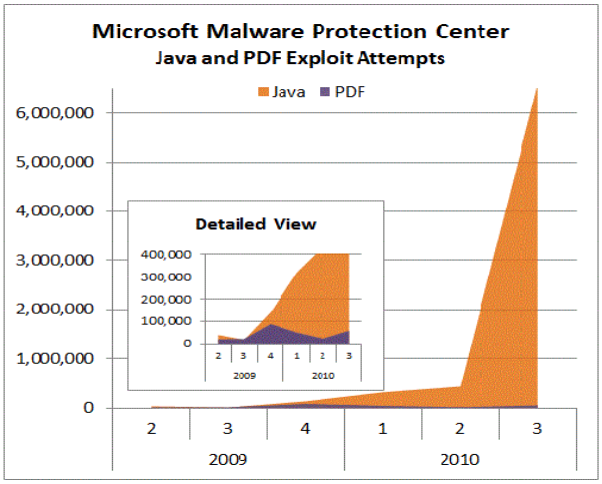


Figure 4 – Java and PDF Exploit Attempts (Microsoft, 2010)

2.2 Comparison Against Previous Work

During the research for this thesis, a number of resources were identified as authoritative within the chosen fields. These did not, however, fully cover all the attack vectors discussed for exploiting users and offer full and appropriate countermeasures and mitigation, together with critical analysis.

2.2.1 Network Traffic Abuse

The breadth of coverage on Network Traffic Abuse attacks encompassing the Tor network is piecemeal. Certain aspects have been looked at, notably for numerous Blackhat and other Security related conferences, with Perry, (2008) and Huber et al, (2010) but these seem to just cover certain aspects of the most obvious attacks that can be carried out, with some just providing a basic overview of Tor itself. Tor only seems to be flavor of the month when something big is discovered i.e. when Dan Egerstad set up a rogue exit router and harvested numerous user credentials as reported by Wired, (2007). It is then revisited occasionally. This may be due to several reasons:

a. The relatively small amount of servers in use over the Internet

b. The subject matter in question which may not seem as important as other potential security vulnerabilities that befall major products.

c. This may also be due to the low user awareness of the potential vulnerabilities that exist for user's utilising this service.

Huber et al for instance noted a high use of insecure protocols being used over the network. This issue has been known about since Tor's inception and more prominently due to Egerstad's demonstration but Huber just provided some current statistics to highlight the fact that issues still exist and provide a reminder that user's haven't learnt from previous issues or the threats haven't been highlighted enough. Perry's work in the field of Traffic Flow Analysis showed a lot of promise and goes a lot further than other work in the field but still leaves a number of areas that need to be researched further to get a fuller idea of how traffic actually flows through the network and is there any particular way to trace it based on latency and leakage. More devious attacks utilising exit routers, apart from credential harvesting, have not been discussed in much depth and this avenue looks like the next progression.

2.2.2 Physical Security Issues

By far the most authoritative piece of work relating to Stuxnet is that conducted by Symantec (2010). Other comparative work in the general field of physical security issues is by Anderson (2010). Combining both resources would offer a history of previous physical security attacks and a complementary look at the entire problem researched and does offer a number of associated mitigation measures identified but does not full cover the subject in question. Various countermeasures and critical analysis has not been carried out together with providing any recommendations and an idea of the direction that similar attacks we are likely to see will go in the future.

Other major research has been completed by other anti-virus vendors, Kaspersky et al (2010) but the detail from this has mostly been kept in-house with limited release of technical

information and so cannot be judged for its technical perspective nor any advice offered to safeguard networks against similar type attacks.

A plethora of open source research has been conducted by numerous security professionals but does not go to the depth produced by Symantec with a fair proportion tending to concentrate on the likely target and attribution of the creators of the Stuxnet worm.

Specific user education and awareness programs are not really touched upon by the majority of sources which would complete and form part of the overarching defence in depth mechanism employed to protect users in corporate environments.

2.2.3 Personal Security Issues

Brian Krebs keeps an extensive exploit related blog, (krebsonsecurity.com, 2010), which is complemented by the malware centric blog run by Jorge Mieres (malwareint.blogspot.com 2010). These provide the most extensive resources currently regarding so called crimeware and exploit packs, information posted on their respective blogs are often re-distributed by a number of other resources and also used as background by mainstream security vendors, McAfee, Microsoft etc. These websites offer up to date trends on the way crimeware and exploit packs are being developed and utilised in the wild together with what vulnerabilities they are currently exploiting.

They have noted the increased use of Traffic Redirection Scripts (TDS), which can be used to redirect and manipulate web traffic to different web instances and servers, which has just been incorporated into the BlackHole exploit pack. This is a new direction for exploit pack developers, with TDS potentially providing load balancing features together with redirecting victims to different exploit servers based on their country of origin which may bring benefits and a nice selling point for the developers.

The information provided by these sites more importantly details the success rates of such attacks, based on administrative panel access, detailing exploited hosts against number of page loads which can give an indication on the prevalent patch status of user's and potentially where enterprises need to tighten up security, user education etc. This information though, can only be opined, and requires analysis and extrapolation from the limited results supplied.

CHAPTER 3: EVALUATION AND RESEARCH – NETWORK TRAFFIC ABUSE

3.1 Background

Three problem areas have been identified whereby the majority of threats that target users emanate from. These will be discussed separately with specific examples from each area, notably Tor, Stuxnet and Phishing and Exploitation Frameworks. Each of these will be researched thoroughly and critically analysed reviewing the vulnerabilities, any countermeasures and mitigating action that can be done to reduce the effect if an attack occurs from one of these vectors. This said, rather than being three separate examples they sometimes can and could be combined into multiple attacks which the reader should be made aware of.

3.2 Network Traffic Abuse

3.2.1 Introduction

Network Traffic emanating from a user's PC traverses multiple routers and switches on its journey to its final destination. How can a basic user be sure that one/all of these points is secure and nothing malicious has occurred in transit? The simple answer is they can't. The use of Virtual Private Networks, (VPN's) and other secure networking architectures can provide a level of trust and assurance but they are not commonly used by home and corporate users accessing general Internet services. An assumed level of trust is made in this connection and this trust is reinforced based on the assumption that the Internet Service Provider (ISP) is securing the transited data. In addition, user data is not necessarily hosted by an ISP where one might think i.e. several "UK" ISPs, (Orange, Sky), host their mail servers overseas, a situation most users are not aware of and thus data traverses outside the boundaries of the U.K. leaving it potentially open to abuse and monitoring by other providers etc. Data is chunked or multiplexed together and can travel over a multitude of different paths before it reaches its final destination, a user has no assurance that nothing malicious has occurred whilst this takes place.

Cloud services are being offered by many providers, Microsoft, Google, Salesforce.com, Rackspace and Amazon to name but a few. These offer a way to cheaply outsource a number of services, software or provisioning of full enterprise infrastructure. These services are assumed by users to be, by inference safe with their data housed in secure environs. This assumption can sometimes lead to a false sense of security as the user is not aware of the security applied in the Cloud provider's network or in fact the data channels used to upload and interact with the data held there.

There have been many high profile incidents where network traffic has been abused; the most notable of these has been achieved by carrying out:

a. Domain Name Server (DNS) Redirection Attacks as illustrated by WindowsITPro, (2008) and TechCrunch, (2009).[2]

[2] These types of attacks usually involve altering DNS records for a legitimate website by an attacker to now point to a server they control. A request for the legitimate website would thus then resolve to a different Internet Protocol (IP) address and traffic would be directed not to the intended site but to the attackers. The attacker's server would either host look-alike sites designed to steal logon credentials, deliver malware and attempt to exploit unwary users or being used for other malicious purposes.

b. Address Resolution Protocol (ARP) spoofing attacks[3]

c. Sniffing Attacks[4]

d. Man in the Middle Attacks (MiTM)[5]

e. Router Redirection[6]

The former has been subject to intense research, numerous high profile security researchers have continuously found holes in key Internet services and have been able to practically subvert network traffic either locally or remotely via a variety of means. This was highlighted recently by The Register, (2010) whereby a Chinese ISP purportedly hijacked UK Military and Government traffic. Network redirection attacks in this case were carried out utilising vulnerabilities in the Border Gateway Protocol and huge portions of network traffic were sent along different paths before reaching their intended destination. Security vulnerabilities have been discovered, patched, mitigated against but due to advances in technology, new services have emerged which build on existing infrastructure and protocols which with them open up other avenues for attack.

Apart from the above, network traffic can be attacked when users utilise the Tor Network via a number of disparate attack vectors. Vulnerabilities' against the Tor network have been documented and exposed in numerous white papers and talks which will be highlighted and security improvements have been utilised to plug them by the Tor project. Compare this to other networks and technologies though; Tor has almost become a forgotten mode of attack which requires further research into its current status and usefulness in conducting a Cyber Attack.

3.2.2 Case Study - Exploiting vulnerabilities in Tor Network

3.2.2.1 Tor Introduction

The Tor network was established predominantly as a method to enable anonymous use of the Internet and is used extensively in areas of the world whether suppression of free speech and filtering of internet services are enforced, i.e. China and Iran.

The network comprises a number of Tor routers (a.k.a nodes) that can be coupled together and used by Tor proxies (normal users using installed Tor client-side software) to build an encrypted path or virtual circuit through the network. A virtual circuit usually comprises, unless specified, three servers, an entry server, sometimes called an entry guard, a middle router, sometimes called a relay, and an exit router. Like the Domain Name Service (DNS),

[3] These occur on the same physical network (broadcast domain) as the user requiring the attacker to be more localised to carry this out. This attack usually involves poisoning the ARP cache of a client to resolve to the attackers machine rather than the default gateway or router they wish to traverse through. This enables a Man in the Middle (MiTM) attack to be performed whereby a user requests a website, this request now goes through the attacker due to the ARP Spoofing and is then relayed to the actual website requested. In this way the attacker gets access to all data including potential logons of the legitimate user.

[4] Usually involves localised capture of data packets transmitted. The content is then reviewed to identify sensitive information that may benefit an attacker i.e. passwords, session tokens etc.

[5] An attack whereby data can be intercepted and potentially modified whilst in transit between two users by an attacker. The attacker usually impersonates a resource or another user which enables them to route all traffic through themselves from the victim and then eventually pass on to the actual "real" destination. In these way passwords, sensitive data etc. can be stolen.

[6] Users are redirected to a site they did not request, this can be by design/configuration, i.e. a router redirecting to an ad portal if a 404 error page is displayed. It can also be done maliciously with a rogue/hacked router seeing traffic emanate from a certain IP range and redirecting to a pre-defined IP address/Uniform Resource Indicator (URI) based on an inputted Access Control List. Alternatively a router may have a rootkit installed and seamlessly redirect a user to a malicious IP.

there are also so called Directory Servers which manage router information for the network and provide and assign details to new Tor proxies of the available entry guards. In addition Directory Servers provide availability information to entry guards who wish to establish the next hop in the virtual circuit.

Entry guards are usually selected based on them offering higher than average bandwidth, long uptime and low latency rates when compared to other available routers within the Tor network. Relays are selected based on similar parameters to entry guards; but to add some protection from attackers trying to shape traffic via the most likely available and predictable paths they are randomly selected from the available router pool based on a unique algorithm. The algorithm, (below), explained by Bauer et al (2007) gathers a list of advertised bandwidth (router_adv_bw) combining this with a random integer from all "*Tor routers … and outputs a pseudo-randomly chosen router, weighted toward the routers advertising the highest bandwidth*". This is then assigned as the next hop for the Tor Proxy requesting access to the network.

Algorithm	**Explanation**
foreach router r Є router_list do	**# for every router from the router list get**
router_bw = get router_adv_bw(r)	**# router bandwidth (bw) = get advertised bw from each router**
B = B + router_bw	**# B = 0 + router bw**
bw_list = bw_list Ụ router_bw	**# bw list = bw list from router bw**
end	
C = random_int (1,B)	**# c = random integer x (between 1 and router bw)**
while T < C do	**# if T (time) is less than C**
T = T + bw_list¡	**# T = T and bw list(as an integer)**
¡ = ¡ + 1	**# integer = integer +1**
end	
return router_list¡	**# Output router list**

According to Torproject.org, (2010), each router initially reports a number of parameters to the Directory Servers which will create a database from which entry guards and circuits can be assigned and setup from:

- "bandwidth" bandwidth-avg bandwidth-burst bandwidth-observed
- "uptime" number
- "router" nickname address ORPort SOCKSPort DirPort

ORport = port that listens for routers/proxies
SocksPort = port that listens for applications (speaking SOCKS[7])
DirPort = port that listens for directory download requests

Packets that travel on the network are called cells and data is encrypted within 3 separate layers using 256 bit Advanced Encryption Standard (AES) symmetric keys. The Tor proxy when initially building the virtual circuit negotiates and obtains a public encryption keys for each router along the prospective route and builds and encrypts a cell such that only the routers private key can decrypt the layer of the cell that passes through them before they in turn pass the message on, as shown in Figure 5. In this way as a cell travels though the network, a layer of encryption is peeled off (rather like an onion) by each router until finally on the exit router, the packet is left exposed and totally decrypted. The packet is then sent further along its path to its final destination or terminates at this node if this is its final

[7] A protocol utilising a proxy server to route packets between client/ server applications.

destination. A circuit once setup can be utilised again for a period of ten minutes then it is torn down and a new one rebuilt as an extra security precaution to prevent network profiling attacks.

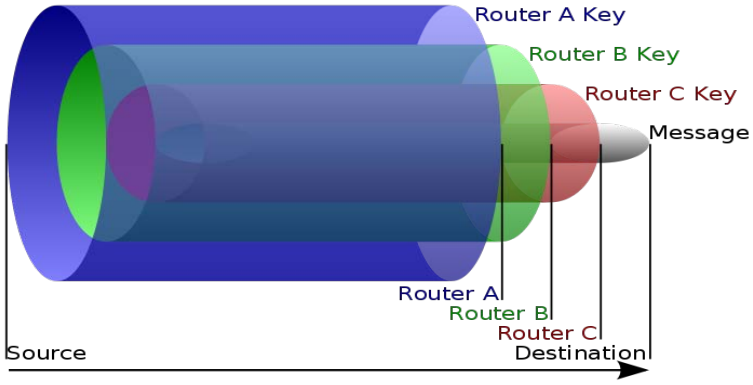


Figure 5 – Onion Routing (Cassandra Security, 2009)

As an added layer of security in the network the nodes themselves use Transport Layer Security (TLS) when communicating with each other, with the AES encrypted cells contained within, as displayed in figure 6 below.

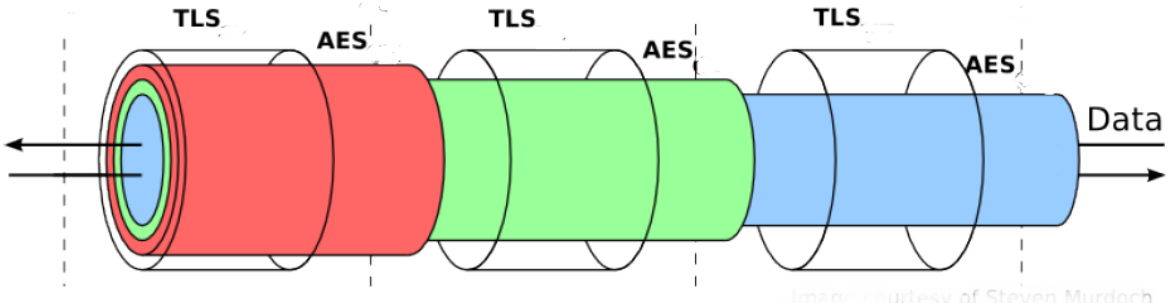


Figure 6 – Tor Encryption (Blackhat, 2007)

To add to the anonymity in the network, the nodes along the circuit only know details of the source of the cell and obviously the next hop parameters to route it too. In essence the relay only knows of the entry guard and exit node, the exit node only knows the relay and final destination, (if this is not itself). In this way the full route is (in theory) not disclosed to all parties and thus anonymity is afforded between the user and recipient of the conversation.

3.2.3 Attacks against Tor, Mitigation and Countermeasures

There are a number of ways to attack Tor users and various mitigation mechanisms and countermeasures can be applied to provide some level of protection against these threats. The following vulnerabilities and issues affect Tor, numerous countermeasures can be employed to mitigate these risks and reduce where possible, although there still exists some residual risk from using any system or application.

3.2.3.4 Rogue Routers

The main way to attack users via Tor is to set up Rogue routers. The most obvious and beneficial node to be used by an attacker would be an exit node as all layers of encryption are stripped from the data and it is at this point that the data is viewable in clear-text to the operator of the server. Dependent on what node is being utilised by an attacker the following attacks can be carried out, each particular node in the circuit will have different levels of success utilising one of these methods:

a. Sniffing Attacks

b. Sybil Attacks

c. Privacy Attacks

d. Session Hijacking

e. MiTM Attacks

Sniffing Attacks

Operators of rogue exit nodes can use various sniffing and harvesting programs, i.e. Wireshark, to make it possible to gather hundreds/ thousands of plain-text Hypertext Transport Protocol (HTTP), Post Office Protocol 3 (POP3) etc. logins, as reported by Wired.com, (2007). Recent research by Macoy et al, (2008) noted from traffic observed transiting their Tor servers that 90% of all traffic observed was for unencrypted HTTP requests.

Exit nodes can also stipulate, via the torrc configuration file, what available traffic they allow to exit from them thus reducing the amount of uninteresting traffic that would normally route increasing their potential for harvesting usernames and passwords i.e.

```
ExitPolicy accept      *:80
ExitPolicy accept      *:110
ExitPolicy reject      *:*
```

If an attacker wanted to be a middle relay in the virtual circuit they would have to specify that no traffic may exit from them:

```
ExitPolicy reject      *:*
```

Apart from credential gathering it was also reported by Wired.com (2010) that it is also possible to extract and rebuild entire documents from captured traffic, this was purported to have been used when the now infamous Wikileaks website was first formed whereby Chinese hackers were exfiltrating hundreds of sensitive documents from exploited machines belonging to Foreign Governments'.

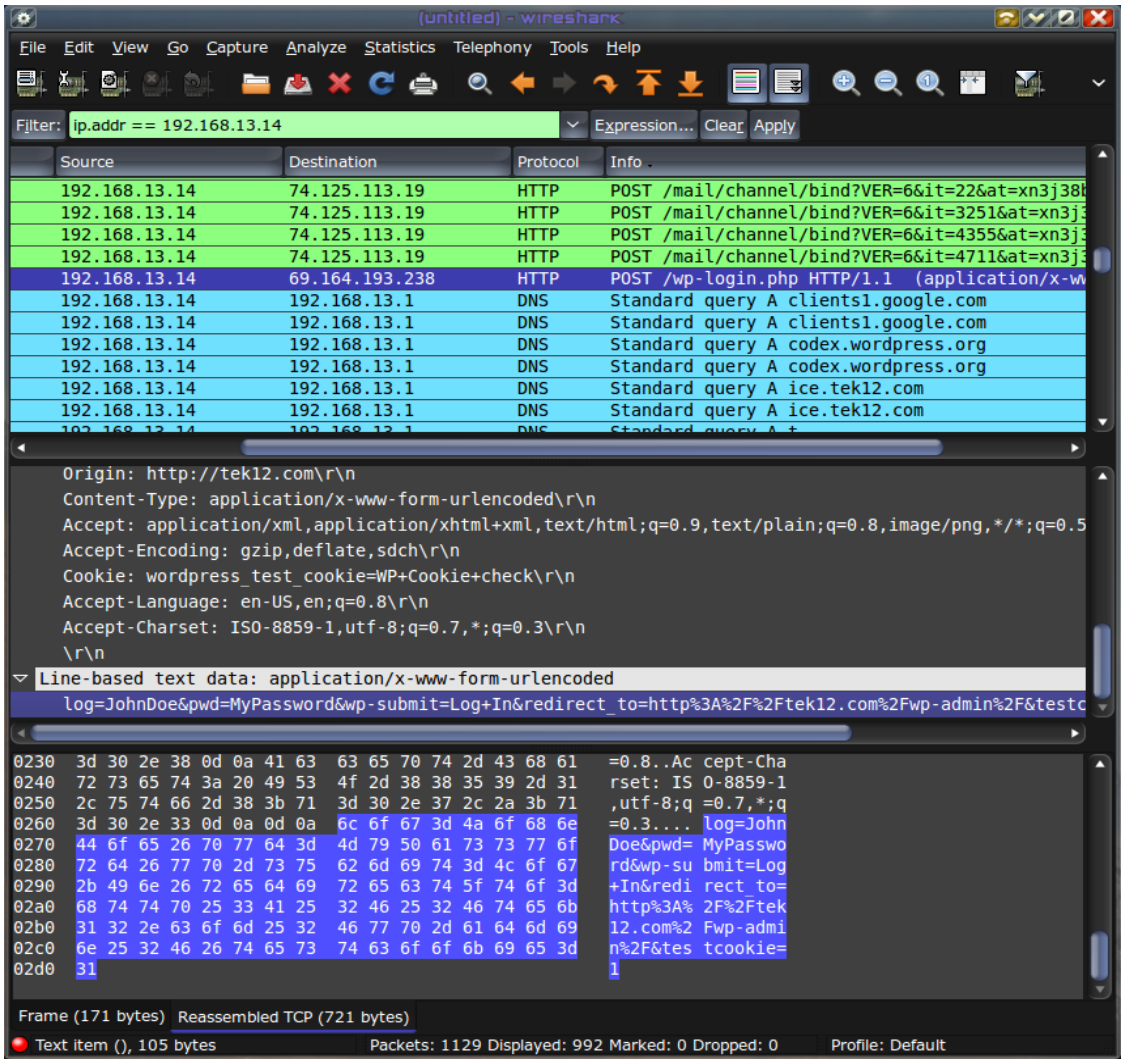


Figure 7 – Credential Gathering from Sniffing (Ubuntu North Carolina Local Community Team, 2008)

With these credentials, it is possible to carry out what CESG, (2010), defines as Masquerades, i.e. the use of someone else's credentials to gain access to their webmail, web or other remote services.

Rogue entry guards and relays in the network are essentially defeated by the layered effect of Encryption on the cells which is an extremely effective countermeasure to ensure the confidentiality of the data is protected. Exit routers do not employ this countermeasure as the last key is decrypted providing no confidentiality to the data. In mitigation of this security issue the exit router does not yet have details of the source of the data and although usernames and passwords etc. would be known, the "real" identity of the account holder is still not known and details of the person may only become known dependent on the information found in their personal mailboxes post-masquerade; thus the anonymity of the user may still remain. To alleviate this, a user collecting mail etc. via Tor should utilise where possible and feasible a 2 factor login system, for example:

a. User identifier, pseudo random request for certain characters from password and personal identification number (PIN) – Usually employed by a large number of finanacial organisations.

b. RSA SecurID or alternative two-factor authentication mechanisms include hardware token authenticators combined with user credentials.

c. Usernames, passwords supplemented with potentially a captcha mechanism included, although the latter may be defeated by such programs as xrumer7, reCaptchaOCR and other manual techniques.

d. Alternatively many webmail companies, (windows live etc.), now offer a single sign-on facility whereby a user's mobile phone is registered with the company and a user can request a one-time use password sent via SMS to them. Use of this to logon to the account can still be sniffed; however, an attacker would not be able to use the sign-on code as it would have expired giving the user some protection and protecting their main password. Users though would have to ensure they signed out of the account otherwise an attacker would be able to continue utilising their cookie.

The above provide an enhanced level of security and would potentially thwart automated access to email accounts and in some cases would require many logon sessions to be "sniffed" in order to obtain the necessary characters needed to identify the full password and PIN.

Tor is unencrypted at the exit router, numerous security measures can be employed to protect the data transiting the Tor network, and one such mechanism created by the Electronic Frontier Foundation (EFF) is to employ a Firefox plug-in called HTTPS Everywhere. This has been developed by the EFF in conjunction with Tor designers to force traffic on an ever increasing number of websites to use HTTPS instead of HTTP. Sites like Google, Facebook and Amazon etc. now offer the user the ability to use Secure Sockets Layer (SSL) sessions, this provides another level of protection and encryption for the user and protects their traffic in transit especially when exiting the Tor network.

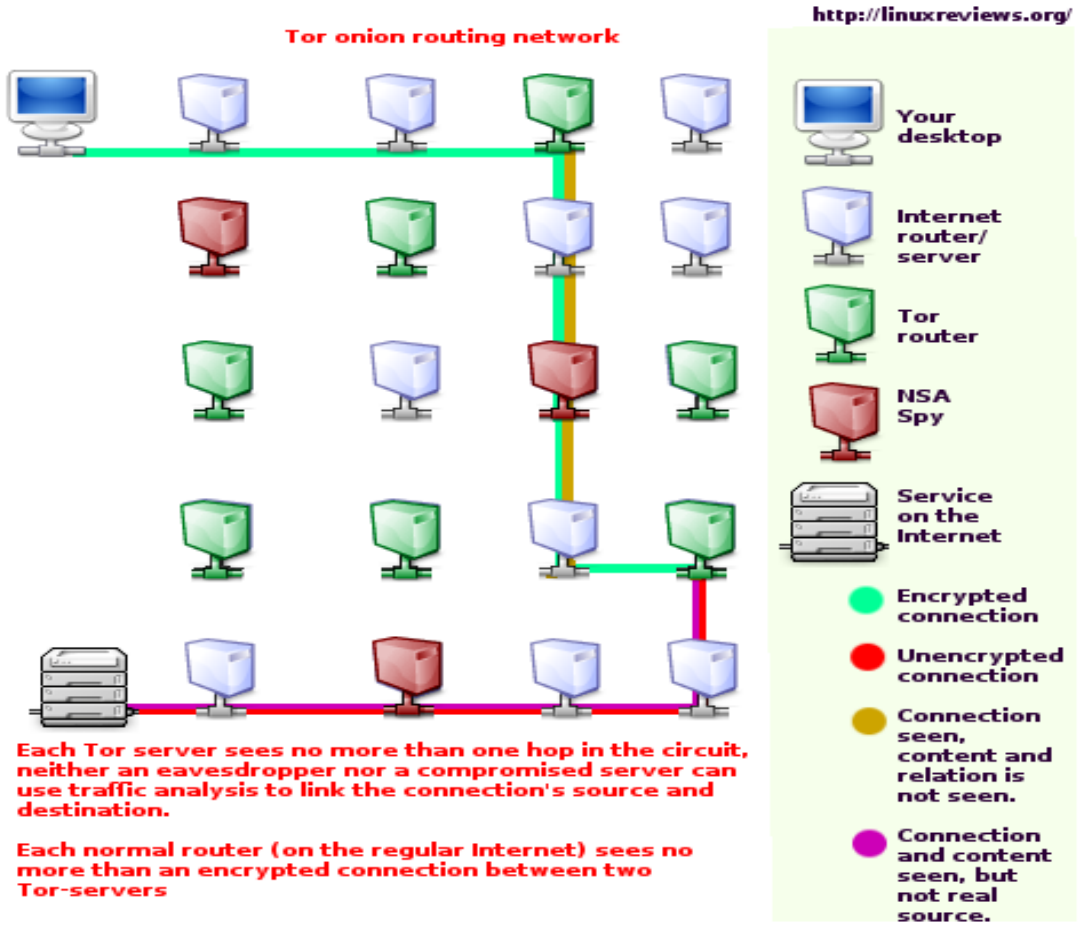


Figure 8 - How the Tor network works (Linuxreviews.org, 2010)

Sybil Type Attacks

Tor used to allow multiple instances of Tor to run on a single IP address which for an attacker would have allowed them to increase the throughput of traffic they could potentially sniff and strip credentials from.

To mitigate this type of attack, only 3 Tor instances are now allowed to reside on the same IP. In addition, each node in a virtual circuit may not share two class B network addresses. This goes some way to ensuring that with 3 servers all three will not make up two thirds or the entire virtual circuit for a given Tor Proxy. For a network though encompassing just 2000 available servers, a small amount of servers set up in this manner still increases the likelihood of an attacker being able to gather unencrypted traffic.

MiTM Attacks

MiTM attacks come in many forms and the two most common to Tor and the use of nodes would be Session Hijacking attacks and circumventing Software Update Services (SUS).

a. Session Hijacking

Session hijacking in its simplest terms is stealing an already authenticated connection to a web resource. This can be carried out in numerous ways and involves either stealing credentials or user/ machine cookies. Manual stealing of sessions via proxy tools such as Paros, Burp and Zap etc. is easily carried out

providing you can gather cookies or credentials but can be a little cumbersome so many automated tools exist which could be used on a rogue exit router for this purpose.

Countermeasures to thwart these attacks have been discussed above, although it should be noted, mitigation of a cookie hijack is difficult. To lessen the attack vector, a user should always sign out of sessions, delete cookies on browser close and also reduce cookie lifetimes if applicable. Some web application specify when you last logged in and from where from, this could alert a user, albeit after the fact, that there account has been hijacked, although this is not ideal it could allow them to change credentials/ settings etc. to prevent this re-occurring.

An example of a Session Hijacking tool is SSLStrip. The tool proxies a user's request on the fly for a secure connection to a legitimate server over HTTPS changing the requests from HTTPS to HTTP and back again and thus is able to capture unencrypted traffic to a local file for offline analysis. In essence it gives the ability to steal credentials and other sensitive user information, figure 9 refers.

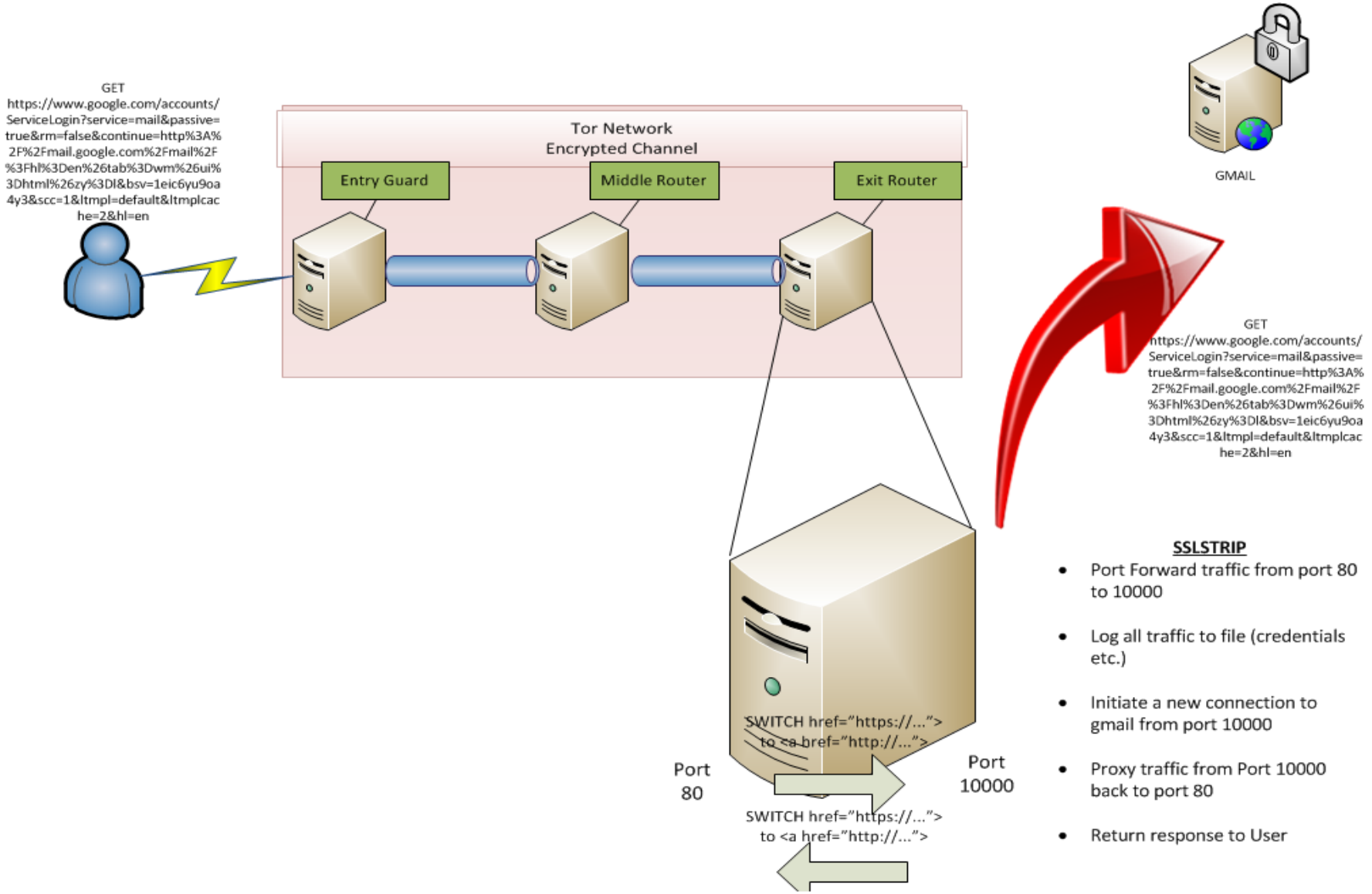


Figure 9 – SSLStrip Scenario (Thoughtcrime, 2010)

b. Software Update Services

Applications and operating systems have their own individual software update services to support them, some of which can be carried out automatically or require users to specify the frequency of checks for new hotfixes and patches and when to install them. Sometimes this is done on actual installation of the product and requires no user input whatsoever, leaving a new service i.e. java update (jusched.exe) running constantly in the background, checking at adhoc intervals for new releases. From a security perspective up to date programs are good as holes are regularly patched, however, this also introduces an opportunity for an attacker to snare a victim using SUS.

One such tool that could be utilised with a rogue exit server is Evilgrade which allows an attacker to try and exploit a user by injecting fake update requests to them. The tool comes with pre-made binaries (agents), default configuration for fast exploitation with its own Web Server and DNS Server bundled. As the attacker already owns the rogue exit server they basically control the traffic into and out and can quite easily hijack any update requests generated by applications on the user's computer.

Most update services provide pop-ups requesting the user to allow or deny install of the update, a large number of users by default just click yes, not reading any information that is displayed to them on screen making it easier for an attacker to exploit them. Security education of users should ideally get them to read and understand such occurrences, getting them to check currently installed version numbers against the version available at the "proper" vendor's website would also give an indication of the validity of updates that are requesting to be installed. Off-line manual updates should also be potentially configured, any update then downloaded from the vendors website should be virus checked before installation and if the vendor provides the facility ensure the MD5 hash of the file downloaded matches that reported by the vendor.

Privacy Attacks

Tor, if used correctly and as directed by the Tor Project can provide an effective layer of privacy to the user, however, Huber et al (2010) noted that users are not following the basic guidelines and are allowing information to be leaked from their browsers that could potentially identify them. It was noted that 78% of users did not utilise the Tor button and thus browser information in the form of user agent strings was leaked potentially providing geo-location and host PC configuration information to be identified by a determined attacker. In this way an attacker may potentially be able to tailor attacks to specific versions of browsers in use and language packs etc. In addition using HTTP requests via search engines will potentially provide a clue to user location i.e. country specific searches, or Google map information requests etc. The Tor button and other such user agent switching plug-ins to certain web browsers will attempt to prevent the divulgence of geo-location information and OS details by "spoofing" details of defined user agent strings. Mitigation and countermeasures to geo-locating via user search terms would ideally be user education and also using only specific HTTPS search engines for this task.

Browser	
Full User Agent String	Per cent (%)
'Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.0.7) Gecko/2009021910 Firefox/3.0.7'	18.86
'-'	4.48
'Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9) Gecko/2008052906 Firefox/3.0'	2.71
'Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.16) Gecko/20080702 Firefox/2.0.0.16'	1.81
'Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)'	1.66
'Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)'	1.64
'Mozilla/5.0 (Windows; U; Windows NT 6.0; en-US; rv:1.9) Gecko/2008052906 Firefox/3.0'	1.59
'Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)'	1.50
'Mozilla/5.0'	1.34
'Opera/9.63 (Windows NT 5.1; U; en) Presto/2.1.1'	1.31

Figure 10 Top Ten User Agent Strings Huber et al (2010)

A pictorial summary of an exploitation attack utilising Tor can be found at Appendix A.

Corporate Countermeasures

Tor is predominantly utilised by users whether in private residence or public accessible places i.e. Cyber Cafes etc. This said, users with enhanced rights on corporate networks may be able to install and run software or use removable media with “portable” editions of Tor installed and executable on them. From a corporate perspective the following countermeasures should be utilised to prevent access to the Tor network and consequently provide an added level of protection to the user and Enterprise:

a. Group Policy should be utilised in conjunction with software restrictions to disallow should programs to execute.

b. Users should be restricted from installing and executing new applications and only be allowed appropriate rights consummate to the role they need to fulfill.

c. Removable media, where possible, should be disallowed access to the host PC and varied lockdown measures enforced to prevent them being used.

d. Removable media, if allowed, should be virus checked prior to use.

e. Corporate Firewalls and Filtering Software should disallow Tor traffic traversing the corporate network. This would include implementing stateful packet inspection for layer 3 traffic complimented with application inspection for blocking peer-to-peer traffic Potentially blocking the following default Tor ports may go some way to achieve this:

Port	Service	Port	Service
8118	Privoxy Port	9051	Tor Control Port
8123	Polipo Proxy Port	9030	Directory Port (Relays)
9001	Tor Server Port	9090	OR Listen
9050	Tor SOCKS Proxy	9091	Dir Listen

f. Effective User Education programs should be enforced warning users of the dangers and threats that exist combined with enforcing an acceptable use policy.

g. Regular independent or in-house audits should be carried out to ensure illicit software is not installed and being utilised.

h. Varied lockdown guides exist to assist administrators to secure systems and application, most notably guides from the National Security Agency, (NSA) and the National Institute of Standards and Technology, (NIST) etc.

General Countermeasures

If a user is sure of the credibility of a node in the network i.e. it could be run by themselves, a trusted source or individual they know, the best countermeasure to safeguard against sniffing, MiTM and other such attacks is to specify which servers to use for entry and exit. The Tor Project, (2010) specify that this can be achieved although it is not recommended by placing associated entries in the torrc config file:

`EntryNodes $fingerprint,$fingerprint` A list of preferred entry nodes to use.

`ExitNodes $fingerprint,$fingerprint` A list of preferred exit nodes to use.

`ExcludeNodes $fingerprint,$fingerprint` A list of nodes never to use.

`ExcludeExitNodes $fingerprint,$fingerprint` A list of exit nodes never to use.

Tor may not always obey these rules, but to make them mandatory insert the following configuration settings; `StrictExitNodes 1` or `StrictEntryNodes 1`.

Note: - Tor connections will cease if all nodes specified are unreachable. Fingerprints are usually in the format `$9D4D995AA745A3CAA6276AFAD505D3E4097AA021`.

3.2.4 Critical analysis of Tor

Reviewing and analysing the vulnerabilities and countermeasures available to offset and mitigate them, a number of thoughts for future extensions of the project were identified that may benefit users. In addition an analysis of the way Tor was designed and is currently operating encompassing the pros and cons was carried out.

a. There are currently in excess of 2100 Tor routers being utilised on the Internet, almost half of which are currently designated as exit routers. Middle routers amount to only 25% of the total available which means all available traffic is currently being focussed in just a small percentage of the network but given more available exit routes so as to gain the required global reach as shown in figure 11.

Aggregate Network Statistic Summary | Graphs / Details		
Total Bandwidth of displayed Routers [KBytes/s]:	481443	
Total Number of Routers:	2109	100%
Routers in Current Query Result Set:	2108	99.95%
Total Number of 'Authority' Routers:	9	0.43%
Total Number of 'Bad Directory' Routers:	0	0%
Total Number of 'Bad Exit' Routers:	5	0.24%
Total Number of 'Exit' Routers:	930	44.1%
Total Number of 'Fast' Routers:	2022	95.87%
Total Number of 'Guard' Routers:	660	31.29%
Total Number of 'Hibernating' Routers:	13	0.62%
Total Number of 'Named' Routers:	1418	67.24%
Total Number of 'Stable' Routers:	1112	52.73%
Total Number of 'Running' Routers:	2109	100%
Total Number of 'Valid' Routers:	2108	99.95%
Total Number of 'V2Dir' Routers:	1055	50.02%
Total Number of 'Directory Mirror' Routers:	1055	50.02%

Figure 11 – Tor Router Status (Kowalski, 2006)

b. One could surmise in an ordinary routable network that the current scheme of limited middle routers is bad practice as the majority of your traffic is being funneled which could possibly create bottle-necks, however, one has to weigh up what the premise for Tor is, and that is to provide anonymity. From this perspective alone operational security is enhanced providing protection of the user's traffic. This is due to the way Tor works with the middle router only knowing the entry guard and exit routers address so far from being a weak link its strength is in the position the router is in and gives the user the anonymity that they require. Whether this though outweighs the other issue of bottle-necks is another matter, although it is opined that due to the low amount of servers in use around the world and to provide full global coverage this is a trade-off that has to be accepted based on the current model.

c. The use of Public Key Cryptography to encrypt data in layers is an example of applying defense in depth mechanisms to the network with all data being encrypted and unreadable from when it enters the network to when it exits. This said data exiting the network identified in the vulnerabilities section has been unencrypted using the exit routers private key and is now viewable by all and sundry. If the user did not add their own encryption to the message via secure protocols i.e. HTTPS would it be possible in the future for exit routers to setup, where possible, an encrypted onward session to final destinations? This would add another layer of security for the user. For Tor to implement this, though, it would require that on initial virtual circuit setup when the router keys are initially being obtained by the Tor proxy a further lookup by the potential exit router would need to establish an encrypted session with the final endpoint. This would provide huge security benefits to the user but would potentially be too difficult to integrate into the current system. This system in itself though could still potentially be defeated by a rogue exit node using such tools as SSLStrip which was demonstrated at BlackHat (2009) which essentially performs a MiTM attack superimposing HTTPS requests for HTTP between itself and a client remembering which links have been changed.

d. It has been suggested that Tor reduce the requirement to have a middle relay thus only an entry guard and exit router will be required, due to there being relatively so few nodes available world-wide. Whilst this would provide added bandwidth into

the network, reducing the hop count etc. it would also mean that privacy and security would also be reduced. Setting up a rogue node would either then mean that it would be designated as an entry guard or exit node, either way the user loses, entry guards know who is sending the traffic and can potentially conduct traffic flow analysis attacks to determine traffic endpoints and exit nodes can grab a copy of all unencrypted traffic. If rogue nodes are employed on both entry and exit nodes in a user's route, essentially it is pointless using Tor as all privacy and security has been totally compromised.

e. Regarding multiple instances of Tor server on the same IP, from an attacker's perspective, this is still advantageous and beneficial due to the limited amount of Tor nodes in use which would increase the possibility of being used as an exit node or entry guard. Combine this with the instances configured to offer high bandwidth and stability means the high probability of being selected as entry guards or exit routers.

f. One of the issues of setting defined entry and exit nodes to guard against rogue nodes via the torrc configuration file are that it may be possible with enough resources to carry out extensive traffic analysis. Analysis of Tor communications could potentially identify the actual source and destination addresses, thus removing all elements of anonymity and privacy that Tor is designed to provide. A user utilising this configuration as a countermeasure should in this case routinely swap the order of nodes they use to build their virtual circuits.

g. The developers of Tor know that rogue nodes are in use, would it not be possible and prudent to put some added protection into the software to try and identify this fact? The author suggests that Tor provide the ability for the application to check and verify the underlying operating system to see if any distinct processes are running that may indicate that the node is running:

    i A sniffer

    ii. Routing a copy of the user's traffic to a disparate connection other than that which was requested.

h. Being able to search for an executable or binaries running on the system that may be being used for nefarious purposes, i.e. Wireshark, Tcpdump, Dsniff, Httpcapture and if found:

    i Automatically disabling the node preventing communications via Tor.

    ii. Flagging the fact to the directory server which then removes the node from the network.

    This, however, may be very intrusive and may be easily circumvented by potentially changing binary names and hashes but may be worth potential further investigation.

3.2.5 Network Traffic Abuse Summary

This thesis has only listed one distinct attack vector from within a multitude of possible threats and may give an indication of the scale of the attack platform available to an attacker. Attacks against network traffic very much depend on what applications and services are being utilised by a user requiring the attacker to modify their methods to accommodate for this. Tor is predominantly an anonymity and privacy tool and utilised sensibly and safely may provide an effective tool for a user to carry out their business in an anonymous fashion.

It should, however, be used with other forms of security mechanisms by users to ensure the failings within it, especially with regards to rogue servers are mitigated where possible. Secure communications should always be setup by users in addition to those utilised by Tor together with one time passwords and reduction of information leakage from the web browser.

Attacks relating to Physical Security Issues will now be discussed predominately looking at USB devices. This area will be discussed as a standalone topic, however, as mentioned previously it could quite easily be combined into a blended threat whereby a user has accessed Tor and have been subject to all manner of associated attacks and be equally susceptible to attacks utilising this device at the same time.

CHAPTER 4: EVALUATION AND RESEARCH – PHYSICAL SECURITY ISSUES

4.1 Background

Gone are the days whereby there were limited if any portable devices that could be plugged into a computer network and work straight out of the box without any extra drivers installed. Today we have plug and play, meaning any number of devices, using a vast array of services such as Bluetooth, Firewire, Universe Serial Bus (USB) etc. can be utilised on our home and corporate network. This gives us choice in our ways of working, freedom and the flexibility to fulfill our IT and working needs in a changing work environment. With this increase in technology though, comes with it different threat vectors which must be identified and addressed to ensure adequate security can still be provided to protect our assets.

Early adopters of such technology lay themselves more open to such threats, security researchers and hackers alike find holes in new products only after they have been initially released, able to study the hardware itself, its standards and protocols and the software utilised for accessing it. Attacks are then discovered, exploited, patched and closed, further holes are discovered or previously closed ones reinvented through a different attack avenue and the cycle continues. Early adopters have to go through the pain, exposure and cleanup operations from such initial attacks until the technology employed reaches a predominantly more secure stage. It is only after this indeterminate period of time that adoption for main stream users is a safer option.

This thesis will look at removable USB devices and will draw upon the history of vulnerabilities associated with them and concentrate on a case study of Stuxnet, the latest, (and greatest (for now!)), attack to utilise this physical security issue.

4.2 Physical Security Attacks

4.2.1 History of USB Attacks

Attacks using USB removable devices have been around for many years, it is just the way they implemented that has changed over time. Throughout the history involving such attacks, the weak link in the chain that can be exploited is yet again the user utilising their naivety and other social engineering techniques to achieve the attackers aim.

The initial specification for USB 1.0 came out in 1996 and has moved along rapidly since this time with version 3.0 released in 2008, although USB 3.0 products were not seen on the market until 2010. Back in 1996, regular transfer speeds of 12Mb/s were supported but today this has potentially risen to in excess of 3 GB/s such is the increase in technology and the thirst for ever quicker data transfer mechanisms.

Automatically being able to run programs from removable devices started with CD/DVD drives, whereby placing the file autorun.inf in the root of the media. If the autorun.inf command contained what is known as an OPEN command pointing to a specified program this would execute once the disk had been inserted. This, with a few alterations in the normal configuration settings on windows, would also allow the same thing to happen on USB devices, against the normal behaviour of having the autoplay menu displayed.

Integrated technology that works in conjunction with USB such as U3 was co-developed by SanDisk and M-Systems in 2005. U3 technology, in essence, uses two partitions on a USB device, one which is read-only and which Windows interprets as a CD drive partition. This

contains the autorun.inf (autorun) file and associated LaunchPad software. The LaunchPad software then uses the second partition, which is file allocation table (FAT) formatted, which contains a hidden “system” folder from which installed applications can be run from. Thus when a U3 enabled USB device is plugged into a computer it will automatically launch associated applications installed.

Before discussing the latest Stuxnet attack utilising USB, it is best to go through the varied history of attacks using this medium. Before technologies such as U3 were created the way to execute anything from a drive be it USB or for that matter CD/ DVD was to use the autorun feature. This generally worked out of the box to try and aid the user and speed up access to data but unfortunately with the side effect of allowing things to execute with limited user interaction, in essence a boon to the potential attacker.

The evolution of attacks utilising USB as the physical delivery mechanism according to Anderson, (2010) can be broken down into the following attacks:

a. Autorun

Creating an autorun file in the root of the USB drive with the following parameters could potentially be used to exploit a user. Autorun will not execute the program by default and the autoplay windows dialog box will be displayed but getting the user to open folders to view files from this normal windows pop-up is a trivial manner as they expect such things to happen. In addition having suitable icons representing programs to make them look innocuous will add to the credibility of a program/ application.

```
[autorun]
action=Open Files On Folder
icon=icons\drive.ico
shellexecute=badthingshappen.exe
```

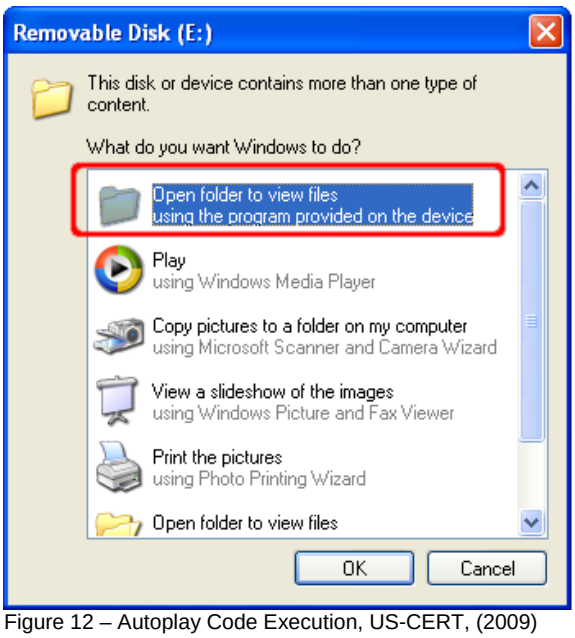


Figure 12 – Autoplay Code Execution, US-CERT, (2009)

Autorun can be disabled in many ways, Microsoft, (2010), provides a number of support guides:

i. Install the relevant security updates MS08-038 (kb953252) and then utilise the Group Policy Editor Tool selecting to “Turn off Autoplay” from within Computer Configuration.

ii. Utilise Microsoft’s Fix it for me facilities to auto-fix the issue.

iii. Alter the following Windows Registry key modifying the Value data box to 0xFF:

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\NoDriveTypeAutorun

b. USB Dumper

USB Dumper, developed by Secuobs and released in 2006, was the starting point from which attacks using USB got more and more sophisticated. USB Dumper created a background process on the system and once a USB was plugged into it, it started to copy the contents to a directory created based on the current date. An attacker could then read through the contents of the data at a later time. As you can see this is good but not very useful to a remote attacker who needs to logon to retrieve data.

Countermeasures to this program would include, keeping antivirus up to date in conjunction with process monitoring and blocking, using kiosk/ thin client type environments whereby a user gets a “vanilla” build of the operating system every time they log on so data cannot be retrieved by anyone else.

c. USB Hacksaw

USB Hacksaw from hak5 is an extended version of USB Dumper which addresses the need for a remote attacker to revisit the machine the USB is plugged into. The tool is installed on the system in a hidden folder. Dependent on a user’s rights the tool will survive a reboot and starts either from a registry run command or from being placed in the startup folder. Once a USB is plugged in, USB Dumper will copy the files to disk. A batch file is then run (send.bat) which compresses these files using WinRAR. The tool will then utilise stunnel, which allows a user to encrypt TCP connections even when non-SSL aware daemons and protocols are being utilised as the forwarding transport mechanism, to initiate a SSL connection. Blat is then used which allows mail delivery to be carried out using Simple Mail Transport Protocol (SMTP), to deliver the files to a specified mail address. All associated documents and compressed archives are then removed from disk.

d. USB Switchblade

USB Switchblade is an evolution of Hacksaw and although requiring administrative access to the machine to be attacked, it does offer an awful lot of functionality. Different variants and installation methods for this tool exist, notably Amish, Kapowdude etc. These do not rely on U3 technology to work. By far the most favoured version though is the U3 enabled GonZor Switchblade. This version combines all the functionality of USB Hacksaw, Dumper et al but offers an awful lot more including the ability to kill anti-virus software, dump system information, network and varied windows and application user passwords together with installing Virtual Network Computing (VNC). This which would allow a remote attacker to connect to the machine and remotely control it. Plugging in a Switchblade configured USB to a target computer allows pre-configured programs to be executed and their output saved to the USB, enabling a local attacker to quickly acquire

sensitive information. In addition hacksaw can also be installed which will then enable an attacker to dump and exfiltrate data from every USB device inserted afterwards.

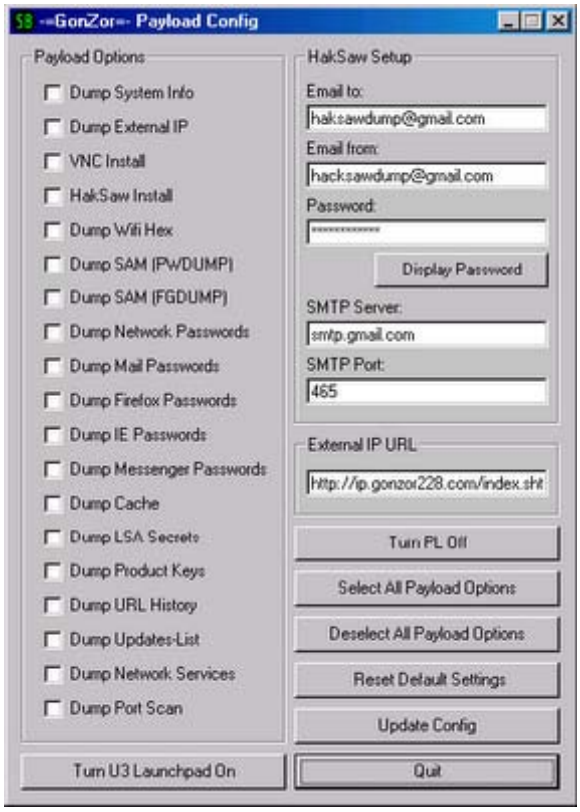


Figure 13 USB Switchblades Initial Configurations, Thinkgeek, (2008)

Countermeasures and mitigations against both USB Hacksaw and Switchblade include the following:

i. U3 technology Hacksaw and Switchblade attacks can be mitigated and the level of threat reduced by reducing the privileges of logged on users which may reduce the functionality and impact experienced from the tool.

ii. OS and application level patching may reduce attack vectors and the use of privilege escalation attacks in addition to Hacksaw and Switchblade.

iii. Disable autorun.

iv. Restrict USB devices on the network, either by group policy, user rights and hardware profiles or use of associated software i.e. Lumension Device Control, DeviceLock, GFI Endpoint Security etc.

v. Provide user awareness training; is USB activity continuing for longer than expected, does network traffic start unexpectedly, are any pop-ups experienced asking to initiate a connection or allow an application etc.

vi. Use of Data Leakage Protection (DLP) hardware appliances, Cisco IronPort etc.

vii. The authors of the tool have also released a tool entitled USB Antidote which automatically carries out a number of the above, however, this contains a number of scripts and registry key changes and it may be more prudent to rely on more "proven" software vendors advice due to the possibility that this may harm a users system or install "extra" functionality which may be used for nefarious means.

e. USB-Based Virus/Malicious Code Launch

USB based viruses and malicious code usually use the aforementioned autorun, autoplay or U3 technology to infect hosts. Examples of which include Worm:AutoIt/Renocide.gen!A and Worm:Win32/Nuj.A, etc. These once installed will infect any USB device utilised on the system, creating custom autorun files on the device which will then execute if plugged into other hosts.

Countermeasures to protect against this attack vector are:

i. Anti-virus installed and regularly updated.

ii. Disable autorun.

iii. Stop the OS parsing autorun.inf files on the system; this can be achieved by creating the following .reg file:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\
IniFileMapping\Autorun.inf]
@="@SYS:DoesNotExist"
```

Autorun.inf files will then be treated as if they were a pre-Windows 95 application configuration files. This is due to the "IniFileMapping" key instructing the OS to read its sub keys upon encountering autorun.inf files. The "DoesNotExist" value ensures that the autorun.inf file is treated as if it were empty so any command syntax within is not run.

iv. User education especially with regards to sharing files and ensuring software is obtained from reliable trusted sources.

f. USB Device Overflow

There have been a couple of occasions whereby the act of actually inserting the USB device into a computer has allowed an attacker to execute their own code. These attacks were presented at BlackHat, by SPI Dynamics, (2005) and MWR Labs, (2009) at Defcon respectively and although used different hardware solutions to initially create there attack both their end goals achieved the same aim, causing a buffer overflow in a driver allowing the ability to run their own code. Once a USB device is inserted, vendor identification (VID) and product identification (PID) take place and the associated driver is loaded into memory. Multiple PIDS can be designated so the attacker need only alter the PID to match that of a vulnerable driver to enable the exploit to occur. This may sound simplistic but an extensive knowledge of hardware and software is required for this to succeed.

Counter measures to these attacks include:

i. Use Group Policy to disable USB, CD-ROM and Floppy Disks.

ii. Prevent users connecting new USB devices.

iii. USB Port lockdown.

g. Social Engineering and USB Come Together for a Brutal Attack.

Social Engineering is essentially working on and exploiting the weaknesses in users. Users have many traits that can be exploited and one of the main ones is their naivety. Users welcome gifts or things that are free, or if asked like to assist/ help out if someone is in need. Each of these foibles can be exploited in conjunction with USB attacks to target users. For example a user finding a USB device on the floor or given one at a conference will plug it into their system to see what is on it. They should ideally virus check it first, preferably with a standalone sheep-dip machine. This, however, is usually not carried out, so they are susceptible to all previous attacks mentioned. In addition, a pre-compiled reverse shell created using Metasploit could be the payload which would create, if successful, an immediate remote connection back to an attacker.

Countermeasures to guard against these sorts of attacks include those previously mentioned; the most effective though would be Security awareness and user training.

4.2.2 Stuxnet

The Stuxnet worm's[8] end goal according to Symantec, (2010), was to sabotage and reprogram industrial control systems (ICS) utilised in gas pipelines and power plants. This was to be achieved by modifying code within specific types of programmable logic controllers (PLC) which controlled frequency converter drives that maintained the speed of varied motors. Stuxnet would ensure that these motors would speed up and slow down at varied intervals, thus causing damage to the system as a whole as the system was not designed to withstand such changes in motor speeds.

USB devices were to be utilised within the attack as a means of propagation, enabling the worm to spread quickly and effectively. These devices also enabled the possibility of jumping air-gaps between Internet connected and closed networks. Stuxnet was programmed to try and identify Field Programmable Gateway (PG) devices, which usually take the form of a Windows based laptop, used to program PLC's via proprietary Step 7 and WinCC software. The latter is used in Supervisory Control and Data Acquisition (SCADA) systems as a Human-Machine Interface (HMI) and allows interaction with Step 7 projects and files. The Dynamic Link Library (DLL) S7OTBXDX.DLL used by Siemens WinCC systems was replaced by Stuxnet which allowed it to read/ write and control the PLC's.

From initial release of the worm, four variants of the worm have been identified:

a. Variant 1 – Compiled on Mon Jun 22 16:31:47 2009.

b. Variant 2 - Compiled on Mon Mar 01 05:52:35 2010.

c. Variant 3 - Compiled on Wed Apr 14 10:56:22 2010.

d. Variant 4 - Is likely to exist but has yet to have been recovered.

These variants have undergone specific changes from one another to provide them with new capability and increase the effectiveness of their infection and propagation routines.

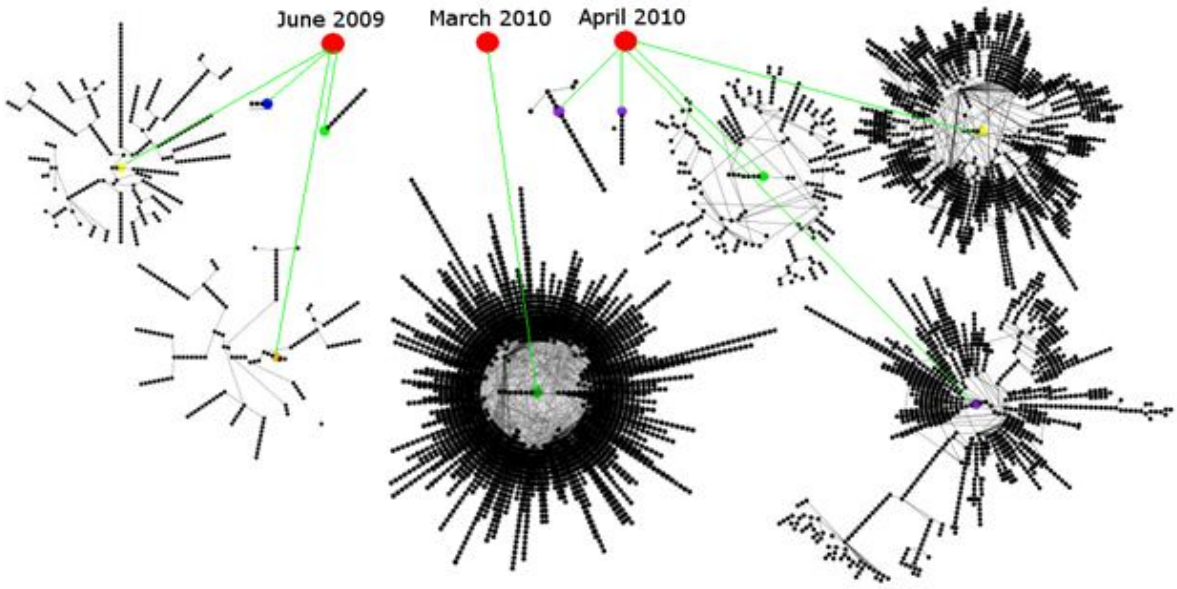
[8] A worm is a piece of malware that self-replicates

Three waves incorporating five attacks were carried out by the worm against 5 specific organisations in Jun, Jul 2009 and Mar, Apr and May 10. Based on retrieved information Symantec were able to partially provide a pictorial representation detailing the spread and success of each particular campaign. These attacks amounted to 12000 separate infections alone from the 100,000 total recorded, the remaining 88,000 infections could be apportioned to collateral damage caused by the initial targeting of and the many ways the worm was able to propagate.

The success of these attacks was potentially increased using lessons identified from previous attacks with two distinct change programs instigated between variants:

a. Physical - Better seeding[9] i.e. targeting of machines.

b. Software – Upgrade and extra capability added.



Stuxnet Cluster of Infections (Symantec, 2011)

Stuxnets' need to find the Field PG's made propagation via USB a key element in the whole process. In order to achieve this and ensure that user's were not aware of the attack, the worm needed to be built in such a way to:

a. Defeat Antivirus Products so that its actions would not be flagged as suspicious.

b. Propagate to other machines via user interaction; utilisation of network shares etc. ensuring a check is first conducted to ensure the machine is not already infected.

c. Hide within plain site, i.e. install visible files to disk but using rootkit technology to disguise itself from system and user defences by integrating itself within valid system processes. This would allow it to function unhindered both on the PLC and also the base OS.

d. Be controlled by the attacker via a Command and Control system to allow:

[9] Using clandestine operations to be able to plug infected USB devices into target machines, or deliver the Stuxnet malware as an email attachment, sent to a very specific group of individuals.

i. An encrypted auto update mechanism,

ii. Carry out a survey of infected machine identifying OS details, installed software (including Step7/ AV variants), IP addressing etc.

iii. Provide the ability to remotely execute commands sent from the attacker.

e. Have an inbuilt payload and the commands to execute it when the correct PLC's have been infected (for attacking those system not connected to the Internet).

f. Utilise driver files that were digitally signed to ensure its underlying code base was verified[10].

g. Reduce collateral damage and the spread of the worm by limiting its propagation to three machines only.

Stuxnet used a number of 0-Day vulnerabilities, (which will be discussed), to propagate and also used previously unseen privilege escalation techniques to gain the right amount of privileges to be able to initially install itself, remain resident in memory and survive a reboot.

Installation

Stuxnet carried out a number of checks before it installed itself on a target machine or removable drive, to ensure that:

a. It was not already installed[11] [12].

b. The operating system was of a specific type[13].

c. The date has to be before 24 Jun 12, the date that Stuxnet has been programmed to stop spreading, although no evidence has been found to date why this date is important.

d. A suitable Antivirus product was installed and could be utilised.

e. It had suitable installation privileges i.e. Admin or could acquire them via a Privilege Escalation Attack. Stuxnet utilised two such attacks dependant on the OS targeted:

i. Windows 2000/XP used the Win32k.sys (MS10-073) windows kernel-mode driver vulnerability which loaded a specially crafted keyboard layout allowing code to be run with SYSTEM privileges.

ii. Windows Vista+ used the Task Scheduler (MS10-092) vulnerability whereby scheduled tasks can be run without the OS properly validating the request, allowing commands to be run with SYSTEM privileges.

[10] This would be achieved by using digital certificates stolen from Realtek Semiconductor Corporation and JMicron Technology Corporation.
[11] Registry Key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\MS-DOS Emulation was not present and if present did not have the value 19790509 set.
[12] A certain amount of debate over this value continues, as potentially it denotes the date Habib Elghanian was executed by firing squad in Iran, this may be a ruse or give an indication of political motivation behind the attack.
[13] Must not be 64-bit and be Windows 2000 or higher.

f. It could communicate with Command and Control servers (although not required to execute its planned payload to attack PLC's).

The installation process is summarised in figure 14.

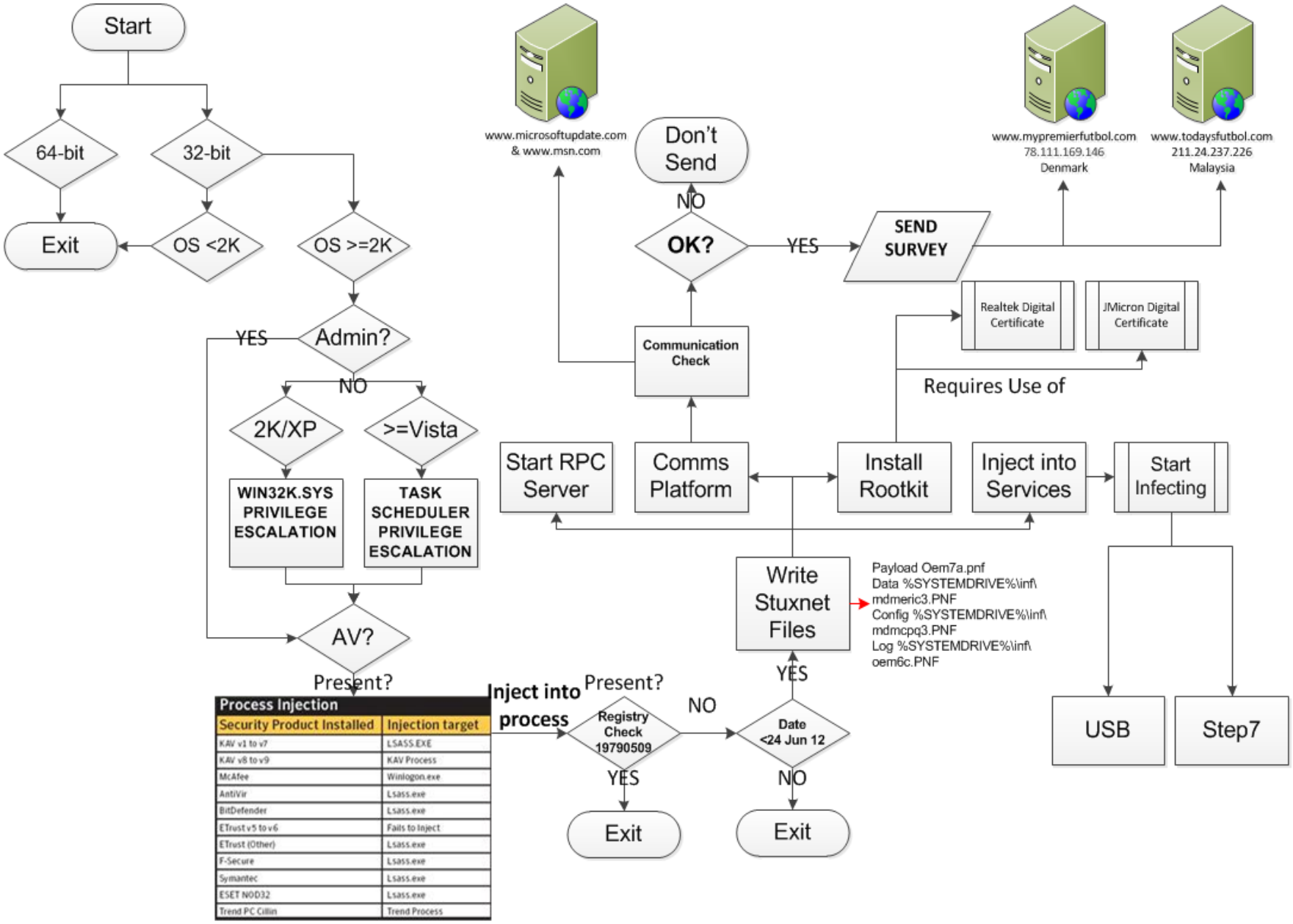


Figure 14 Stuxnet Installation Cycle, (Symantec, 2010)

Propagation

Stuxnet propagated in a number of ways, via removable media and also over the network. The following methods were utilised, a pictorial summary of which can be found at Appendix C:

a. Removable Media (USB) – The MRNet.sys file which forms part of the rootkit intercepts access to all I/O requests from USB devices to the base OS. As such Stuxnet is able to intercept read and write requests and copy itself to the device (figure 15). The .LNK files are the actual exploits that load and execute the .tmp files which then drop Stuxnet to disk when the USB device is re-inserted into a further machine. The vulnerability it exploited in the explorer process needs only to render the contents of the USB drive for it to propagate, (MS10-046 refers).

   Note: - There have been four detected variants of the Stuxnet worm, the oldest of which dates back to Jun 09 which used autorun as its means of propagation before the .LNK vulnerability was utilised.

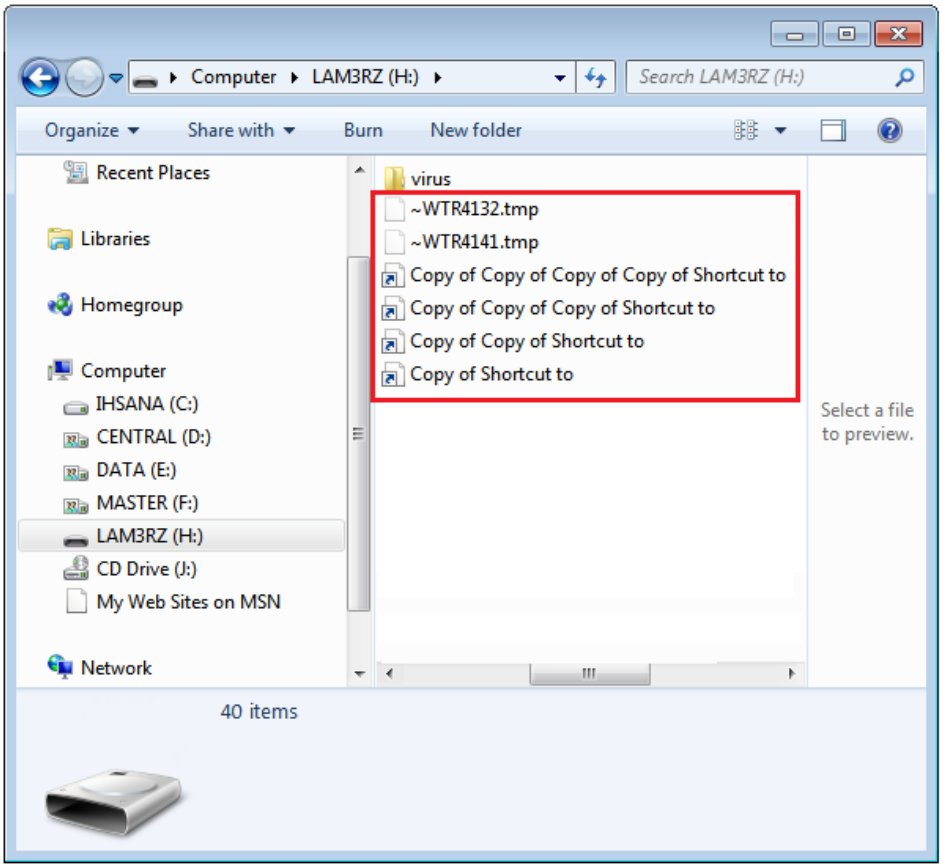


Figure 15 Stuxnet USB Presence (Ihsana IT Solution, 2010)

b. Peer to Peer – The Remote Procedure Call (RPC) Server started as part of the installation process listens for connections, a RPC Client will connect and determine if there version of Stuxnet is up to date, if not it will be updated by the RPC Server.

c. WinCC – Stuxnet will send malicious SQL queries to the WinCC SQL Server Database using a hard coded default password that cannot be changed by the vendor, (CVE-2010-2772 refers). This enables the copying and execution of Stuxnet to the remote host.

d. Network Shares – Using user credential tokens or the explorer.exe process users on the domain are enumerated and Stuxnet is installed to remote shares using Windows Management Instrumentation (WMI) and the scheduling service[14].

e. Print Spooler Vulnerability (MS10-61) – The Print Spooler process allows files to be written to the %SYSTEM% folder and executed if a user is sharing a printer on the network.

f. Windows Server Service Vulnerability (MS08-67) – Uses a previously identified vulnerability to connect via Server Message Block (SMB) to copy itself to a remote machine. Stuxnet would check that the patch is not installed and AV signatures were no newer than 1 Jan 09 to ensure it was not "caught" during this process.

Figure 16 – WORM_STUXNET.A infection diagram (Trend Micro Incorporated, 2010)

[14] This schedules a job to execute 2 minutes which starts the Stuxnet process ensuring it remains resident on disk and runs on startup.

4.2.3 Stuxnet Countermeasures and Risk Mitigation

There are a number of countermeasures that can be applied that may go some way to protect users from the current threat of the Stuxnet worm and may provide protection in the future from similar variants:

Anti-Virus

Ensure that it is kept up to date, this may have defeated one of the propagation mechanisms via the use of SMB which validated that signatures were not newer than 1 Jan 09 before it attempted to install. TrendMicro, (2010) reported that the ZBOT and SALITY family of malware utilised the .LNK vulnerability not long after Stuxnet was identified, up to date AV would therefore detect an attempt to install on the system via this attack vector.

Corporate Countermeasures

Numerous countermeasures have already been identified for defeating other forms of USB attacks, (see history of USB Attacks), which may provide some level of defence. According to isssource, (2010) the corporate focus should be on instigating a thorough Defence in Depth strategy to protect the network and its users. Other protective mechanisms could also be instigated include:

a. Host Intrusion Prevention Systems (HIPS) can utilise rule and behavioral monitoring that notes any changes to the file system on the installed machine. HIPS utilise a system whereby a cryptographic checksum is taken of files and any associated changes to them are flagged. This can then be alerted to a central reporting repository for further action when used in conjunction with a Network Intrusion Prevention System (NIPS).

b. Host Intrusion Detection Systems (HIDS) can identify changes to the file system and the creation of new services; Stuxnet used DLL injection, in conjunction with installing a rootkit and these actions may have been detected. Any alerts could then be sent to a central reporting repository for further action when used in conjunction with a Network Intrusion Detection System (NIDS).

c. DLP via egress filtering of outbound connections.

d. Maintain effective security policies and procedures.

e. Ensure appropriate Incident Response Procedures are in place and regularly practiced.

f. Potential employment of honeypots.

g. Regular vulnerability assessments to be carried out to ensure no obvious vulnerabilities exist within the network.

h. Use of alternate OS would have defeated this attack, although in saying this the PLC programmable devices required the use of Windows to function so is not possible.

For corporations that utilise ICS the following resources may help with extra security measures to be adopted, together with coding guidelines for developers:

a. NIST 800-82: Guide to Industrial Control Systems (ICS) Security.

b. Department of Homeland Security: Catalogue of Control Systems - Security Recommendations for Standards Developers.

Patching

Protection against 0-day attacks is difficult, bordering on impossible, but a common theme within the plethora attack vectors utilised is that they for, the most part, use tried and tested exploits for previously released vulnerabilities to propagate. Keeping systems up to date with the latest patches for the users' browser of choice in conjunction with flash player, java, adobe etc. could potentially stop an exploit attempt. Browser specific updates from Microsoft or any other OS vendor generally focus on the browser only; it is the users' responsibility to update the add-ons they have installed. Given the lack of user awareness and education, this is normally a weak point attackers can exploit. Previously Evilgrade was mentioned as a way to exploit users on a Tor exit node via software update services, the same care should be taken by users when upgrading these applications. Corporate organisations also generally have a slower patch release and update process due to the necessity to fully test and integrate changes into what can be a complex infrastructure. As such a user targeted in this fashion may leave the corporation more exposed. For Stuxnet, though, patching would only have partially helped as numerous vulnerabilities did not have an associated patch nor were they identified. The one vulnerability that was identified prior to the Stuxnet attack was in Apr 09 by Hakin9 magazine, (2009) which attacked the Print Spooler service and which was not patched by Microsoft until Sep 10. Installing MS08-67, the patch which fixes the Windows Server Service vulnerability would have stopped propagation via SMB so may have reduced the spread of the worm by this vector. Any application in use on the system should also be regularly updated, Siemens, like other vendors release regular SIMATIC security updates which should be applied after thorough testing.[15]

User Awareness

By far the soundest advice for users it to refrain from using such devices in untrusted machines.

4.2.4 Critical analysis of Stuxnet and its aftermath

One of the limitations in this thesis was that reverse-engineering was out of scope. Instead, critical analysis of Stuxnet will concentrate on how it could have been better designed together with an analysis of the incident response mechanisms employed and fallout from this attack.

The Washington Times, (2010) and other reputable news sources recently reported that the U.S National Board of Information Security Examiners recently recommended that utilities have separate business systems from control systems. This means that attacks cannot jump from Internet-connected business systems to sensitive and critical control systems. Further recommendations include the enactment of legislation to ensure these recommendations are mandated. This in itself would be advantageous and provide another barrier to malware and would-be-attackers but one of the key attack mechanisms employed by Stuxnet was "air-gap" jumping which even with physical separation would not prevent a similar attack succeeding. Therefore it is the author's suggestion that legislation should go one step further and enforce adequate security mechanisms on all systems with such things

[15] SIMATIC Security Update that will protect against the .lnk vulnerability together with providing a Stuxnet disinfection tool in conjunction with TrendMicro.

as default configurations changed, patching and updating etc. enforced to protect all systems to lessen the chances of infection should an air gap jump occur. Security must be taken seriously and critical national infrastructure, major utilities and the like should be afforded the level of security they NEED.

A certain amount of speculation has been made over the actual target for this attack and whether it was indeed directed at the Bushehr Nuclear Power Plant as many people believe. Stuxnet first came to the fore in July 10 and even now new things are being discovered about this piece of complex coding. Anti-virus signatures were quickly distributed and the domains redirected away from their original IP addresses but from an incident response perspective the attack is not over and the response to such until it is fully clear what components are being targeted. A specific Programmable Logic Controller (PLC) was identified quite early on in the process and thus certain post exploit action could take place to protect facilities that use this hardware but some five months later another important piece of the puzzle was uncovered. The ability of Stuxnet to change the speed of two very distinct frequency converter drives as reported by Symantec, (2010) narrows down the respective targets and also provides the ability to potentially introduce extra counter measures. Incident Response is by no means over in this case, just the square edges being rounded off so to speak to get the full finished product.

Malware developers, dependent on their ability and the actual purpose of the malware itself whether it is to survive and propagate long term, have been seen on many occasions to spend that extra time ensuring that when malware is installed on a machine a pseudo random filename is created each time, (Win32/Autorun.DM etc.). Alternatively developers ensure the MD5 hash of the malware file names change every time the malware executes, (Downloader-CJX etc.). In this way, if ever caught, it would make it that bit more difficult identifying the malware itself, reverse-engineering the creation and install process, thus allowing for the creation of a signature for anti-virus product engines to alert to if they detect it. With Stuxnet this was not the case. This could be attributed to any number of factors, a few of which are discussed;

a. Their coding skills did not reach to this. It is assessed that this is unlikely due to the complexity of the code and the many ways it propagated and many different methods.

b. They may have used mules/ intermediaries. Coders sometimes sell their wares onto third parties and potentially this third party could not be as technically astute as the malwares creator. From a command and control perspective it is easier to manage exploited machines if the location and names of files are known.

c. Upgrade path. It may be that definitive filenames and install path locations may help in future upgrades etc. so may be a reason to define these and keep a finite and definitive list.

The Stuxnet developers potentially missed a trick once they were discovered. This, however, could depend on their end goal; if it was to ensure that the malware survived one of the commands that should have been sent to previously infected machines would have been to change the command and control server URI's away from www.todaysfutbol.com and www.mypremierfutbol.com to provide extra redundancy. Rotating to a plethora of pre-bought domains owned by the attackers would at least provide a mechanism to prolong the life and retain control of infected machines. (Kroxxu mentioned previously, had thousands of domains to potentially report to). In addition the attackers could have potentially changed the signature of the Stuxnet binaries to defeat signature based antivirus products and Intrusion prevention Systems etc. One must also think, surely the attackers would have

thought of this and although there is no evidence yet from the security community could previous Stuxnet infected hosts potentially reporting elsewhere currently.

If, however, having been caught, the attackers may have realised the extra effort required to manage changing domains and obfuscating binaries may be nugatory work and so accepted the situation to be a lost cause and moved on to other attack vectors.

It is opined that the entire code-base and installation and exploit mechanism will be heavily re-worked and be reborn as a more complex and robust piece of malware as is the case with malware when new variants are released with slightly different signature and propagation mechanisms. This would, however, require the need to identify more "0" day vulnerabilities that allow the malware to propagate and spread not to mention potentially a different mechanism to allow privilege escalation to occur, both of which Stuxnet utilised heavily to exploit and propagate.

Only time will tell when a variant of Stuxnet will appear and one also must be mindful to the fact that Stuxnet itself had, according to reports, been active for over a year potentially before it was identified by the mainstream security community as a whole. In this way a new Stuxnet type "hack" may in fact be out there in the wild already but undiscovered and carrying out what it nefarious purposes it was intended to do.

The attackers may also have put in place a way of protecting their own assets and those of the country they belonged to, although evidence of this has not come to light. The Stuxnet worm was observed in 155 separate countries and detected on 100,000 machines; it may have been that the attack got out of control and may have caused collateral damage from its intended target. There were a few mechanisms put in place to limit the worms spread; based on the date of infection and the setting of a maximum propagation count to 3 from each USB device to prevent its spread, but even these preventative measures failed to stop it infecting all around the world.

4.2.5 Physical Security Issues Summary

Stuxnet is a major game changer with regards to attacks targeting and using physical infrastructure. What it did, how it did it and what it was designed to do was a radical evolution and far in advance of previous attacks using similar devices. Future iterations of Stuxnet or malware similar will no doubt use the lessons identified from this to specifically target other systems and propagate by multiple avenues. In addition the code base is now known and could potentially be adapted and modified with other proprietary code to form more dangerous and destructive variants.

In some ways it is lucky that Stuxnet was so targeted to attack specific program logic controllers and products, if it was for any other nefarious destructive reasons, there could well have been more serious repercussions.

Stuxnet has shown that in only half a decade how advanced attacks can develop using this medium and is a long way from those earliest attacks that simply dumped files to disk for later retrieval.

Attacks relating to Personal Security Issues will now be discussed predominately looking at Phishing, Exploitation Frameworks and Exploit Packs. This area will be discussed as a standalone topic, however, it could easily be utilised in a blended attack whereby a user has been browsing through Tor using a portable version of the application which launched from a

USB device but whilst accessing their webmail they clicked a nefarious link which caused them to get exploited.

CHAPTER 5: EVALUATION AND RESEARCH – PERSONAL SECURITY ISSUES

5.1 Background

Personal security issues encompass all such attacks that are designed to exploit the weaknesses, foibles and naivety of user's. Neuro Linguistic Programming (NLP), the so called science looking into how we think in conjunction with cognitive biases can be utilised, whereby users tend to differ in their normal patterns of behaviour given certain situations. An example of the latter may be a pop-up, the majority of users may read the message in the first one or two, checking them as they are wary of where they came from and what they want to do, but finding them legitimate, they accept them, but unbeknownst to them, this forms a pattern so given a similar situation whereby an attacker creates a pop-up, a user is predicated to selecting "yes" to dismiss it and accept its legitimacy and consequently gets exploited. Apart from certain extreme circumstances like blackmail, physical coercion etc. the majority of attacks would be carried out using social engineering[16] techniques.

Social engineering can be broken down into the following types of attacks:

a. Pretexting – Using a prepared scenario to try and get the target user to trust the attacker and thus increase their chances of obtaining sensitive information, i.e. pretending to be IT support and asking users to perform an action which ultimately could allow an attacker access to the computer/ network.

b. Phishing[17] (encompassing Spear phishing[18] and Whaling[19]).

c. Baiting – This is heavily linked to physical security issues discussed previously, relying on a user's greed to enable the attacker to exploit their machine i.e. leaving a malware infected USB device lying around which most users will pick up and explore, often plugging into corporate or home computers out of curiosity but ultimately providing the attacker with the access or effect they intended.

d. Quid pro quo - Essentially providing something a user needs in exchange for something an attacker wants. The BBC, (2004) reported that exhibitors at the Infosec conference successfully offered free chocolate in exchange for a user's password. A user may provide one that is incorrect but their naivety may lull them into a false sense of security not thinking that an attacker provided with a real

[16] The "*art of manipulating persons in order to bypass security measures and tools. The purpose is to obtain confidential information from users through phone, e-mail, [etc.] and … use this data to gain illegal access*"

[17] A malicious attempt usually made via email purportedly delivered from well-known organisations to entice users to visit a "spoofed" copy cat version of a legitimate website. This is carried out in the hope of stealing personal, credit cards or other sensitive information. Due to the generic nature of such requests emails may also appear from sites that the user does not even have an account for.

[18] This is similar to phishing with ultimately the same goals or to go in further actually exploiting the user; however, it targets groups of users or organisations. Spear phishing emails may relay on open source information gleaned about a group or organisation from which an attacker will craft an email tailoring it to suit the intended targets. Potential targets may have been identified from online profiles; facebook et al to like a particular football team may be provided crafted emails purportedly offering reduced/ free tickets in an email "spoofed" from the team's website.

[19] *"Whaling" is phishing that is targeted at corporate executives, affluent people and other "big phish." Like spear phishing, whaling emails often are customised with information directed to the recipient (name and other personal information) and sent to a relatively small group of people".*

password could research user naming conventions on the target network from open source circles and then potentially try to log on via open web resources.

General user awareness into the dangers of social engineering and the use of certain technologies, applications, resources and alike is very much dependent on their technical skill set, exposure to effective security education and awareness of the dangers that exist. Those within a corporate environment may be better protected with varied hardware and software protection mechanisms, restricted rights and privileges combined with in-house security training. Those general home users, however, are not afforded this luxury so potentially are more vulnerable to such attacks.

This chapter will cover a number of aspects of phishing coupled with the use of phishing frameworks and exploit packs:

a. Current Phishing Targets – This will detail the current targets of such attacks and the potential reasons for such, noting the use of new defence mechanisms that Phishers are using to prolong the life of their copycat sites.

b. Phishing Obfuscation Techniques – How Phishers try and trick users to click on links.

c. Phishing Attack Frameworks – The most prevalent in use today and what vulnerabilities they exploit to target users.

d. How Attack Frameworks Work – Discussing reconnaissance techniques, iframes and their use in attacks.

e. Exploit Packs – Discussing examples, business models, which exploits they utilise and the ways they obfuscate registrant details.

5.2 Phishing

Phishing attacks tend to utilise copycat websites to entice users to trust and interact with them. The success of this can depend on how high profile the website is the attacker is copying in combination with the size of its respective user base. Getting this right gives an attacker a better than average chance when the “spoofed” email lands in a user’s email box that the user will have a respective account at the copied website in question.

5.2.1 Current Phishing Targets

Phishers seem to be changing the particular users’ they target and the ways they use to carry them out. According to Phishtank, (2010), The Top Ten most popular targets for November 2010 were PayPal, Facebook, Zynga, Internal Revenue Service, Orkut, Sulake Corporation, HSBC Group, World of Warcraft, Steam, and Bradesco. When compared to 2009, where PayPal, Internal Revenue Service, Tibia, eBay, Inc, Facebook, Bank of America Corporation, JPMorgan Chase and Co, HSBC Group, Google, HSBC were the most popular so we can see a marked shift away from Banking and Revenue type websites to the more social networking, online community and gaming arenas.

This may be due to attackers changing the ways they target users to achieve other aims or potentially users may be becoming wiser to spoofed emails purportedly from banking and commerce sites. From an exploitation perspective targeting users from the social and gaming arena may make it a little easier for an attacker as users may not be as security aware than if they were targeted via a “bogus” banking site. Emails and websites requesting

passwords, PIN numbers and other personal information potentially should make users more wary of passing across their personal and sensitive details. This could mean the attacker wants to exploit users for other means, potentially to use them as bots or for other purposes rather than just too simply steal their online banking details. Banking and e-commerce sites have shifted to using secondary authentication schemes. This requires an attacker to potentially have a user visit a "bogus" web page multiple times to actually gather the full password and PIN details they need, something that is not guaranteed to occur and may raise the users' suspicions.

Targeting multiple users and exploiting them through phishing social networking and gaming sites may lead them to have key loggers, backdoors and alike installed on their machines which would eventually harvest banking credentials anyhow but also give an attacker the flexibility to use these machines as spam relays, install Pay-Per-Install (PPI) programs, whereby the attacker is paid by a third party for installing specific programs i.e. fake anti-virus programs etc. The actual attack frameworks used in this scenario will be discussed.

Phishers have evolved their own types of defence mechanisms, they realise that there sites will be potentially taken down and blocked so have started to use the following techniques:

a. Rock-Phish Attacks

So called large-scale phishing attacks attributed to criminals who have prior purchased a number of domains, usually with meaningless names i.e. wasu69.biz. A phishing attack would then be prepend the real domain name to be targeted onto these domains i.e. http://www.hsbc.com.id345.wasu.biz. The id345 is a unique identifier that is used to defeat potentially spam filtering technology. The attackers DNS is configured to process all similar URI's as a wildcard all of which resolve to a single IP address which is actually a proxy server. All web requests are then relayed to an obfuscated server hosted elsewhere. Attempts then to takedown the proxy requires the attacker to just change the DNS entries to a new one and so traffic will be automatically re-routed and attacks will continue.

b. Fast-flux Attacks

This is similar to rock-phish attacks, however, the domain name in question resolves to multiple IP addresses all of which change dynamically at adhoc intervals thus actually identifying and putting measures in to stop the attack server is difficult.

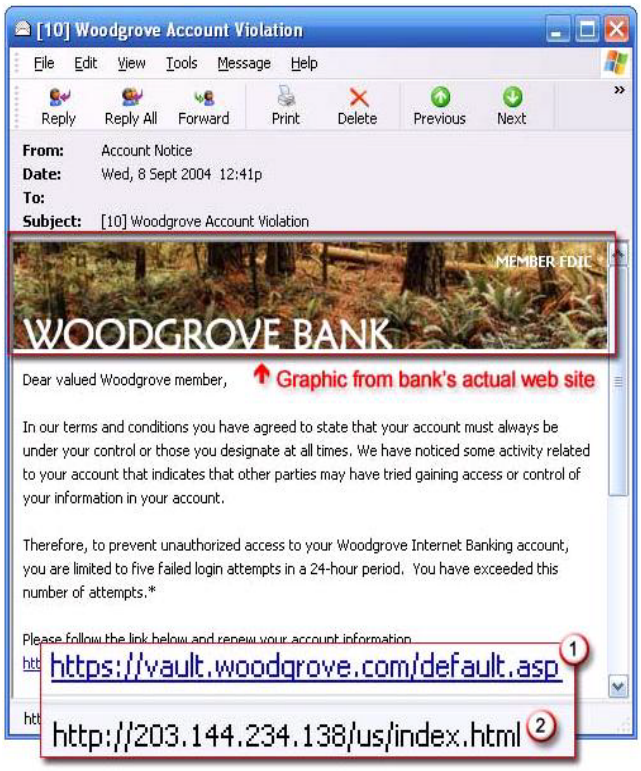
5.2.2 Phishing Obfuscation Techniques

Phishing emails appearing in user inboxes in many formats to try and lure users, common techniques for luring and exploiting users include:

Link manipulation – Users can be fooled by:

a. Similar or subtly misspelled URI's i.e. www.citi-bank.co.uk

b. Displayed URI's may not actually send users to this address with alternative URI's/ IP addresses being the actual underlying link,



(1) Correct URI

(2) Actual IP address user is sent to upon clicking the link

Figure 17 Phishing Link manipulations (Microsoft, 2010)

c. Using the @ symbol i.e. http://www.hsbc.com@phish.ru/

d. URI shortening services i.e. bit.ly

https://www.nwolb.com/default.aspx?refererident=5A34F58771C34308A23738550713BED9933484A6&cookieid=31458&noscr=false&CookieCheck=2010-12-10T08:37:06 shortens to http://bit.ly/gDjLTc

e. Using IP addressing as the link,

f. Pre-pending real URI's i.e. http://www.hsbc.com.id345.wasu.biz

g. Page attachments – When an attacker does not set up a full site but delivers a pre-compiled web page as an attachment to an unsuspecting user. Opening this up may request malicious code to be executed on the victim's machine and user consequently exploited.

h. Zip file attachments – Containing malware that if opened will exploit a user's machine.

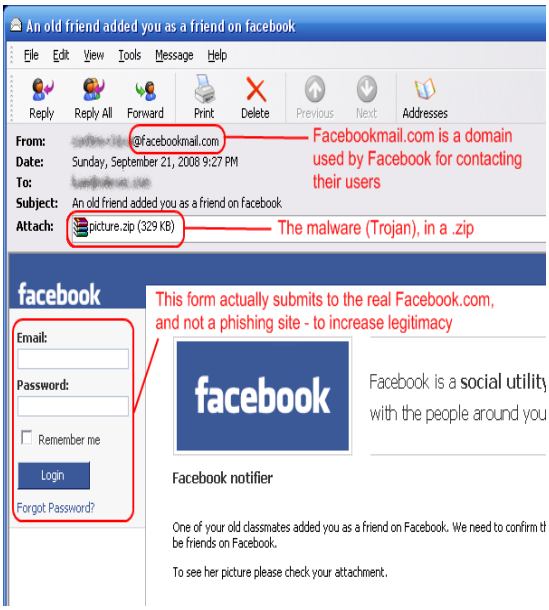


Figure 18 Phishing Malware Attachment – Facebook (NgepRESS.COM, 2009)

Spoofed Source Details

Spoofing the details of the sender can make the email look more legitimate, again this would only provide an initial level of obfuscation. The message source may give away the true identity of the sender or clues that the email has not come from a legitimate source and thus should not be trusted i.e.:

Received: from User ([173.200.167.50]) by murphysonmacdade.com with Microsoft SMTPSVC(6.0.3790.1830);
Wed, 24 Nov 2010 15:09:49 -0500
From: "NatWest Bank" onlineaccess@natwestbank.com

A recently received phishing email from Natwest was relayed via a U.S 24 Hour plumbing and electric contractor's mail server which most probably is either compromised or is acting as a spam relay.

Images

In conjunction with the above using realistic images from the domain the email purports to be from. The images in question would be ideally drawn directly from the site the attacker wishes to target i.e.

src="http://www.santander.co.uk/csgs/StaticBS?blobcol=urldata&blobheader=image%2Fgif&blobkey=id&blobtable=MungoBlobs&blobwhere=1223401013051&cachecontrol=immediate&ssbinary=true&maxage=3600">

Character Control Set

Use of the correct character control set dependent on the geolocation of the user targeted is another key way of legitimising the email i.e. Western European for targets in the U.K rather than Cyrillic!

5.3 Phishing Attack Frameworks

Frameworks that can be used in conjunction with Phishing and Social Engineering Attacks exist in many guises. There are the commercially available tools for the ethical Security tester, Core Impact, CANVAS, etc. and then from the Open source arena we have

Metasploit, Social Engineering Toolkit (SET) and the Social Engineering Ninja (SEN), Imposter etc.

SEN is an example of a basic Phishing Attack framework which can host a number of high profile copycat websites, Twitter, Yahoo etc. The specific code base for this and similar frameworks is based on the general purpose scripting language, Hypertext Pre-processor (PHP) and utilises a MySQL backend database, enabling the attacker to log and retrieve details of user interaction and exploitation results. Whilst pretty basic in nature, with limited end user exploits, it does provide the ability to insert iframes into web pages which can cause users to be exploited and provides the ability to harvest a great deal of user credentials:

Figure 19 SEN Phished Credentials (Social-engineer.org, 2010)

Phishing Attack frameworks, dependant on their complexity can be employed to carry out the following:

a. Steal or set cookies/ Flash Local Shared Objects – Cookies may be imported into varied proxy tools for replay i.e. Paros, Zap etc.

b. Steal passwords stored in the browsers cache i.e. Local network attack against Firefox's' saved password repository.

c. Poison browser cache (enabling potential exploit and redirection to malicious websites etc.)

d. Steal files from the victim's local file system via the use of flash and Internet Explorer – Demonstrated by Kuppan, (2010) in his "*Flash+IE = Prison Break*" this can only be carried out on a local network due to Flash security restrictions and also requires a fair number of pre-requisites i.e. anonymous access to a network share, file splitting above 244 bytes etc.

e. Harvest Credentials and personal information.

f. Attempt to carry out client side exploits via:

   i. Malicious Java Applets.
   ii. Malformed Adobe files.
   iii. Malicious ActiveX Controls.
   iv. Malicious Media Player Plug-ins.

v. Varied vendor specific browser vulnerabilities, IE6-8, Firefox etc.

vi. Assorted other web based exploit mechanisms, (QuickTime, Yahoo webcam etc.)

vii. Integration with other exploit frameworks i.e. Metasploit shell payloads.

g. Web jacking Attacks – Attacks that are initiated with a user clicking a link and appears to be from the real site they wish to visit, however, they are presented with a message stating the web resource has moved asking them to click on a link to the new address, which in turn redirects them to the attackers malicious website.

h. Assorted combinations of the above.

i. Infectious Media Generator – Similar to those attacks discussed in Physical Security Issues, whereby the SET toolkit is used to setup a listener on the attacker's machine waiting for connections. A malicious payload is distributed physically via USB or other removable media options and providing Autorun is enabled a remote connection is established immediately to the attacker's machine.

Note: - Some of these attacks require a user to be on the same network as the attacker as the attacker's machine may require controlling DNS settings and thus resolving user requests to their own machine.

5.3.1 How Attack Frameworks Work

Reconnaissance

Attack Frameworks are configured in such a way that whenever a user has been enticed to visit the site, their particular web browser is probed to first of all identify its version, language type and known installed plug-ins it supports. Figure 20 provides an abridged version of the authors Internet Browser Settings detailing the OS being used, the browser type, flash settings etc. which would provide similar results when the attackers probe is carried out.

Browser Information:

- Browser: Firefox
- Browser Version: 3.6.13
- User Agent String: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-GB; rv:1.9.2.13) Gecko/20101203 Firefox/3.6.13

Computer Environment:

- Operating System: Microsoft Windows 7
- IP Address: (Port : 52713, Host : cpc1-stav2-0-0-cust249.aztw.cable.virginmedia.com)
- Platform: Win32 - Windows 32-bit platform
- Screen Resolution: 1440 x 900 (Available: 1440 x 860) (Color depth: 24 Pixel depth: 24)
- .Net Framework: No or unable to detect...

Plugin Settings:

- Adobe Flash Player: Flash installed - (version : 10.1)
- Shockwave Plugin: Shockwave installed
- QuickTime Plugin: Quicktime installed - (version : 7.6.8)
- Windows Media Player Plugin: Media player installed - (version : 5.2 or higher)

Cookie Settings:

- Cookies enabled? Yes
- JavaScript Cookies: Yes

Figure 20 Detect Browser Settings (DigitalCoding.com, 2010)

Once this information has been obtained, a lookup of potential vulnerabilities that the user may be susceptible to based on the software versions of installed applications/ OS and Plug-ins detected is carried out. If a particular vulnerability is identified then an attempt may be made to use a tailored exploit to transparently install malicious software on the host. Exploit frameworks also provide the ability to geolocate victim's IP addresses via integrated databases from Maxmind, IP2Location etc. According to Syngress, (2010) dependent on where the user is browsing from an attacker may provide different content to match the potential language of the visitor and thus make the website more convincing. It is also possible to limit those exploited to those from certain regions only; such is the complexity of these exploit packs and the lucrative nature of their returns.

Malicious Iframes

Iframes are HTML tags that can be used to place an image into a normal HTML document, potentially sourced from a local or remote site. Iframes used for nefarious purposes have been around for a long time, an example of which is:

<iframe width="1" height="1" frameborder="0"src="http://www.liagand.cn/hlp/?id=9"></iframe>[20]

Attackers generally specify a zero size iframe or make them hidden so the remote/ local resource they reference is not visible on the page but does, however, cause the web browser to make an automatic request to retrieve the content referenced by them. The content from the attacker's nefarious web resource in turn exploits the user's browser or installs unwanted malicious software. Malicious iframes have been integrated into numerous attacks and come embedded within these attack frameworks. Websites are sometimes compromised by attackers and iframes inserted into certain pages allowing users to be redirected elsewhere. Administrators of such websites may not even be aware of this action as the content they display is unaffected and well known websites will attract many users making them an excellent resource for redirection attacks.

Iframes may also be obfuscated by attackers to hide their malicious intent from cursory user inspection but would still be automatically rendered by the browser:

```
[Script Language='Javascript']
[!--
document.write(unescape('%3C%69%66%72%61%6D%65%20%73%72%63%3D%1D%68%74%74%70%3A%2F%2F%67%6
F%6F%6F%6F%67%6C%65%61%64%73%65%6E%63%65%2E%62%69%7A%2F%3F%63%6C%69%63%6B%3D%38%46
%39%44%41%1D%20%77%69%64%74%68%3D%31%20%68%65%69%67%68%74%3D%31%20%73%74%79%6C%65%3
D%1D%76%69%73%69%62%69%6C%69%74%79%3A%68%69%64%64%65%6E%3B%70%6F%73%69%74%69%6F%6E
%3A%61%62%73%6F%6C%75%74%65%1D%3E%3C%2F%69%66%72%61%6D%65%3E'));
//-->
[/Script]
```

JavaScript de-obfuscation would be able to decode the above to its original meaning with varied online services exist that can perform this service:

<iframe src=http://goooogleadsence.biz/?click=8F9DA width=1 height=1 style= visibility:hidden;position:absolute></iframe>'

5.3.2 Exploit Packs

The frameworks of real interest though are the so-called Exploit Packs those used by the unethical, designed purely to exploit users to further the attackers own gain and which allow automated attacks against unprotected users. Not only do these packs provide a source of income for the attacker, they are also generally sold on by the actual developers themselves.

[20] According to http://support.clean-mx.de/clean-mx/viruses.php?domain=liagand.cn&sort=first%20desc this URI is still valid and Firefox reports this as still a current Attack Site.

These packs range upwards from $250 - $2000 and usually come from varied Russian developers. Each respective sale consists of a custom version build using tools such as PHP ion Encoder and tailored to work for the purchaser only so as to provide copy protection and to maximise the sales revenues. In addition by purchasing these packs direct support is provided and also access to exploit updates, thus providing a greater chance of success when targeting users. Installation and use of exploit packs with this type of protection will either restrict the purchaser to:

a. Run on particular IP addresses and/ or server names or

b. Auto expire files after a set time period

Numerous exploit packs exist but the most lucrative, prevalent and supported ones are currently:

a. Black Hole

b. Crimepack

c. Eleonore

d. Fragus

e. Phoenix

f. Siberia

g. SEO Sploit Pack

h. YES Exploit Pack

The majority of the above are sold on forums, requiring a potential purchaser to contact the seller via ICQ, MSN, Jabber etc. offline. Due to the underground nature of these exploit packs it proved difficult to gather exact details of where to obtain some of them from. The packs usually have a 4 tier pricing model:

a. The actual exploit pack.

b. Anti-virus obfuscator to reduce the risk of detection.

c. Add on extra exploit domains should the original tied to the exploit pack be blacklisted.

d. Support and updates.

A number of other packs are available and some are extremely well known within the security community i.e. Mpack, Icepack etc. but although still in use have been superseded by more extensible variants above.

When investigating the registrant details for the site purportedly selling the Yes Exploit pack, (which is currently unavailable), it was determined after completing an open source search that, the registrant, Vladimir Ivanov also potentially owns about 260 other domains and his listed contact details, user234@mail.ru is also a contact on the whois record of 29 domains

He also has alternative contact details of abc@abc.com. From the authors own experience this is common for phishing/ crimeware related sites whereby numerous domains are registered almost as throwaway entities, providing backup to those sites which are blacklisted, innocuous contact details do not identify the registrant and their name In this case is that of a high profile male model.

Varied older versions of Exploit packs can be obtained from numerous underground Russian language forums; however, these are not supported and may also be trojaned. In addition Software as a Service, (SaaS) add-ons are coming to the fore according to McAfee, (2010) and a new business model is being offered by Exploit Pack writers, providing pre-built exploit domains on Virtual Private Servers (VPS) that can be leased for certain periods of time making things much easier for the attacker.

A recent overview of Exploit packs by McAfee provided the following results, detailing what vulnerability, (mapped to the Common Vulnerabilities and Exposures (CVE) reference), and subsequent exploit was utilised in each respective pack:

CVE	TITLE	CRIMEPACK	PHOENIX	ELEONORE	FRAGUS	YES EXPLOIT	SIBERIA	EL FIESTA	ICEPACK	MPACK	WEB ATTACKER
CVE-2003-0111	MS03-011 - ByteCode Verifier component flaw in Microsoft VM										Yes
CVE-2004-1043	MS05-001 - HTML vulnerabilities										Yes
CVE-2005-2127	COM Object Instantiation Memory Corruption (Msdss.dll)							Yes			
CVE-2005-2265	MFSA2005-50 - Firefox InstallVersion.compareTo			Yes							Yes
CVE-2006-0003	MS06-014 for IE6/Microsoft Data Access Components (MDAC) Remote Code Execution	Yes				Yes		Yes	Yes	Yes	Yes
CVE-2006-0005	MS06-006 - Windows Media Player plug-in vulverability for Firefox & Opera			Yes					Yes	Yes	Yes
CVE-2006-1359	MS06-013 - CreateTextRange										Yes
CVE-2006-3643	Microsoft Management Console (MMC) Redirect Cross-Site Scripting (XSS) vulnerability (IE)								Yes	Yes	
CVE-2006-3677	Firefox -JS navigator Object Code			Yes					Yes		
CVE-2006-3730	WebViewFolderIcon (IE)							Yes	Yes	Yes	
CVE-2006-4868	MS06-055 - Windows Vector Markup Language Vulnerability										Yes
CVE-2006-4777	DirectAnimation ActiveX Controls Memory Corruption Vulnerability							Yes			
CVE-2006-5559	MS07-009 - IE6/Microsoft Data Access Components (MDAC) Remote Code Execution		Yes	Yes		Yes					
CVE-2006-5745	Microsoft XML Core Services Vulnerability							Yes			
CVE-2006-5820	AOL SuperBuddy ActiveX Control "LinkSBIcons()" Vulnerability							Yes			
CVE-2006-6884	WinZip FileView ActiveX (IE)									Yes	
CVE-2007-0015	Apple QuickTime RTSP URI (IE)							Yes		Yes	
CVE-2007-0018	NCTsoft NCTAudioFile2 ActiveX Control Remote Buffer Overflow Vulnerability							Yes			
CVE-2007-0024	Vector Markup Language Vulnerability (IE)								Yes		
CVE-2007-0071	Integer overflow in Adobe Flash Player 9		Yes		Yes						
CVE-2007-3147/3148	Yahoo! Messenger Webcam (IE)								Yes		
CVE-2007-4034	Yahoo! Widgets YDP (IE)								Yes		
CVE-2007-4336	DirectX - DirectTransform FlashPix ActiveX (IE)								Yes		
CVE-2007-5327	CA BrightStor ARCserve Backup Multiple Vulnerabilities							Yes			
CVE-2007-5659/2008-0655	PDF Exploit -collab. collectEmailInfo	Yes	Yes	Yes	Yes	Yes	Yes	Yes			
CVE-2007-5755	AOL Radio AmpX Buffer Overflow	Yes									
CVE-2007-6250	AOL Radio AmpX (AOLMediaPlaybackControl) ActiveX control vulnerability				Yes						
CVE-2008-0015	MS09-032 DirectX DirectShow (IE)		Yes	Yes	Yes						
CVE-2008-1309	RealPlayer ActiveX Control "Console" Property Memory Corruption							Yes			
CVE-2008-2463	MS08-041 - MS Access Snapshot Viewer	Yes			Yes	Yes		Yes			
CVE-2008-2992	PDF Exploit - util.printf	Yes	Yes	Yes	Yes	Yes	Yes				
CVE-2008-4844	Internet Explorer 7 XML Exploit	Yes									
CVE-2008-5353	Javad0 – JRE Calendar		Yes	Yes							
CVE-2009-0075/0076	MS09-002 - IE7 Memory Corruption			Yes	Yes	Yes					
CVE-2009-0355	Firefox - Components/sessionstore/src/nsSessionStore.js	Yes									
CVE-2009-0806	IEPeers Remote Code Execution	Yes									
CVE-2009-0927	PDF Exploit - collab.getIcon	Yes	Yes	Yes	Yes	Yes	Yes				
CVE-2009-1136	MS09-043 - IE OWC Spreadsheet ActiveX control Memory Corruption	Yes			Yes						
CVE-2009-1869	Integer overflow in the AVM2 abcFile parser in Adobe Flash Player		Yes								
CVE-2009-2477	Firefox - Font tags			Yes							
CVE-2009-3269	Telnet for Opera TN3270	Yes									
CVE-2009-3867	Java Runtime Env. getSoundBank Stack BOF	Yes	Yes								
CVE-2009-4324	PDF Exploit - doc.media.newPlayer		Yes	Yes							
CVE-2010-0188	PDF Exploit - LibTIFF Integer Overflow	Yes	Yes								
CVE-2010-0806	IE7 Uninitialized Memory Corruption	Yes									

Figure 21 McAfee Overview of Exploit Packs (McAfee, 2010)

The findings from Microsoft tallies with varied statistics obtained from multiple Exploit Packs Administrative Panels by varied security researchers. The majority of most successful exploits in the Crimepack, SEO Sploit and Blackhole packs are java based, with java exploits accounting for 90% of successful exploits in Blackhole alone, 70% on Crimepack and between 50 and 65 percent of malware installs on SEO Sploit. It may be possible to detect that an Exploit Pack is being utilised at a particular URL by such tools as wepawet.

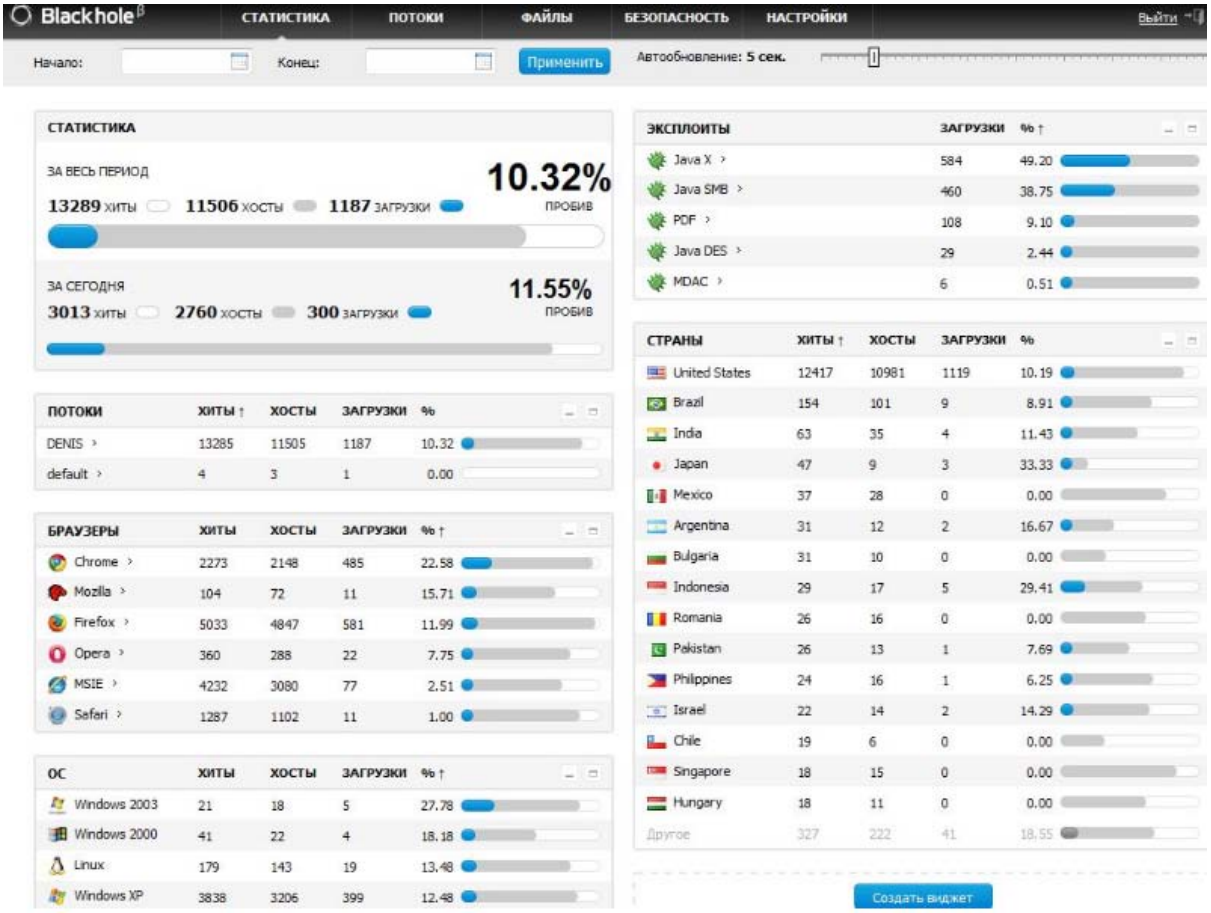


Figure 22 Blackhole Exploit Pack (KrebsonSecurity, 2010)

A pictorial summary of an exploitation attack utilising phishing and an exploit pack can be found at Appendix B.

5.4 Phishing and Exploit Pack Countermeasures and Risk Mitigation

There are a number of countermeasures that can be utilised to reduce the risks to users:

Browser Add-ons and Utilities

Certain web browsers provide the facility to install first and second party add-ons to provide extra functionality. Firefox in particular is very extensible in this respect and add-ons such as NoScript, QuickJava, etc. which can allow fine grained control over JavaScript, Flash content etc. User can select which websites to allow this type of content and by default this content does not run until allowed. In this way users are protected from attacks utilising this format. The majority of current web browsers provide the ability to disable this content permanently but this option, although very secure, may not provide a productive web

experience. Internet Explorer also has an add-on phishing filter which potentially alerts a user that they are browsing a phishing website.

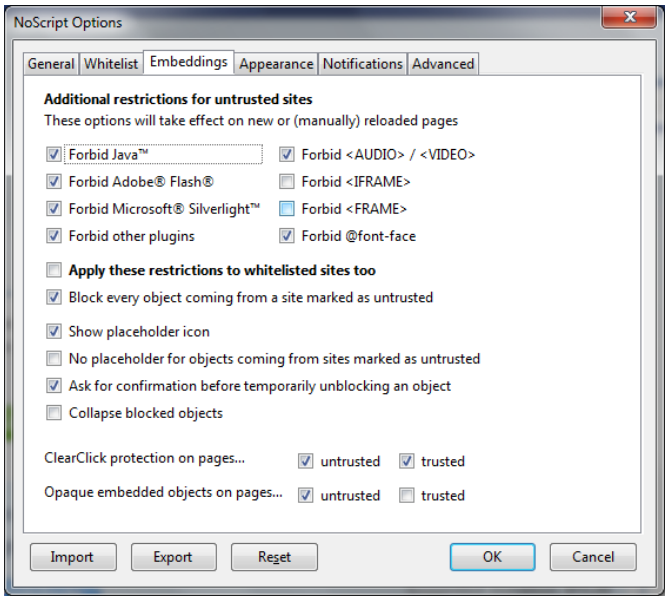


Figure 23 NoScript Options (noscript.net, 2010)

Utilities such as PDFid can also disable certain JavaScript options within Adobe documents which will add some form of protection to a user.

Sandboxing

Provide virtual machines to enable browsing or a sandboxed environment whereby potential malicious code, run time environment and propagation can be examined in a secure environment is another defence mechanism. Although this may not stop exploitation in the first place, it does, however allow organisations to view the malware in its native environment, thereby enhancing their knowledge of the payload and limiting the effect of the attack. Virtual machines can be powered-off between user sessions and a fresh "known good" copy utilised on every session to ensure no user information/ cookies or data is allowed to retain state.

Firewalling and Filtering

Should users be exploited and respective backdoors call back to command and control servers, it may be possible to limit and restrict egress of data as was recommended previously with regards to DLP when dealing with physical attacks.

Patching

Various tools also exist that assist with identifying missing patches, some are OS specific, i.e. Microsoft Baseline Security Analyser, (MBSA) others though will cover 3rd party application also making them much more extensible, i.e. Secunia Personal Software Inspector (PSI). Users can then ensure those missing patches are updated.

Website takedown

Dependant on the location of the servers and the Internet Service Providers hosting phishing websites it may be possible to get the website taken offline. If this is not possible it may be possible to alter DNS records, as was done for Stuxnet, to redirect users to a safe site. Moore et al, (2008), in his paper noted that with regards to phishing type websites that it is more likely, if brand owners are made aware and actively participate that the website will be taken down within 4 hours.

-	Sites	Lifetime (hours)	
		Mean	median
Free web-hosting			
all	395	47.6	0
brand owner aware	240	4.3	0
brand owner missed	155	114.7	29
Compromised machines			
all	193	49.2	0
brand owner aware	105	3.5	0
brand owner missed	155	103.8	10
Rock-phish domains	821	70.3	33
Fast-flux domains	314	96.1	25.5

Figure 24 Phishing Website Lifetimes by Attack Type (Moore et al, 2008)

The option of taking down proxy servers will not defeat Rock-Phish style attacks and the only realistic solution in this case would be to arrange for the domain registrar to remove the malicious domains in question from DNS. Alternatively identifying the obfuscated server that is actually carrying out the attack could make takedown feasible. Fast-flux attacks again cannot be defeated by taking down servers and require domain names to be suspended by the appropriate registrar.

User Security Awareness Training

This will go some way to reduce the risk of users clicking on links, alternatively if they do, may provide a means to spot potential copycat websites purporting to be legitimate. A number of resources are available that could protect users:

a. PayPal, Sonicwall, Phishtank and numerous other sources offer online tests to raise user awareness into this problem and hopefully may provide the knowledge required to alert those fooled into visiting these types of sites.

b. Reporting suspect emails to reputable vendors, banks etc. Antiphishing.org provides an online report form. This information gets amalgamated and is used by numerous sources to protect users, various browser vendors for example will attempt to stop a user visiting a potentially suspect site, as shown in Figure 25 below.

Figure 25 Firefox 3 Malware Protection (Google Operating System Blog, 2007)

5.5 Critical Analysis of Phishing and Exploitation Attacks

The amount of phishing emails blocked as opposed to malware is surprising. Anecdotal evidence suggests utilising multiple email accounts, generally 5 times more phishing type emails are received that those containing malware. MessageLabs noted that the amount and prevalence of botnets is not decreasing even with high profile take downs of some of the largest. This combined with the decline in phishing attacks could point to a shift in the focus and motive for attacks taking place. Bots can be seen as easily acquired, needing limited management and are easily replaced but acquiring them and in huge amounts gives an attacker the ability to utilise them for multiple means, some will obviously be for monetary gain, harvesting credentials which would normally have been achieved by phishing but the extensibility these bots give an attacker is worth far more.

Being able to send and relay spam messages has remained at roughly the same levels year on year potentially providing a steady income stream for bot herders, but the ability to wage DoS and DDoS attacks, renting out so-called botnets to the highest bidder could be seen as the major cash cow of the future,. This can also provide double income for an attacker, being able to hold corporations to ransom and also getting paid for someone to carry attacks out.

The costs for renting out portions of botnets are declining and definitely well within the budgets of everyday users. When will we see Cyber retaliation from individuals or companies slighted by rivals, partners or in fact have we seen this already but it has not been reported? As ever, attribution of any attack and the pay masters behind is difficult to achieve together with gathering the necessary proof, the financial cost of doing this may not even be cost effective especially if such attacks were small scale. This said less technical perpetrators as reported by The Register, (2010) sometimes trip themselves up with the use of open source tools like the Low Impact Ion Cannon, (LOIC). This is currently being used as a DoS tool against a number of high profile websites, (MasterCard, PayPal etc.) in retaliation against the charges laid against the creator of Wikileaks and the decision by certain vendors to cease processing payments which supports this website. LOIC unfortunately for those using the tool broadcasts their actual source IP, unless the user takes measures to obfuscate it, which is fortunate for law enforcement for attribution purposes but still not very common in other similar attacks.

Direct phishing with copycat website asking for user details do work but time and time again banks have re-iterated that they will never ask for this type of information or send those types of emails. User's may, over time, learn and adapt their surfing habits accordingly, thus reducing the success rates from this type of attack. Phishers should possibly try a more

softly softly approach; banks are continually offering advice to consumers to protect themselves, (consequently to try and reduce their losses), this may be a new tact that attackers may take in the future. Pro-active emails appearing in inboxes offering safety advice for users from "their" banks could be the way forward. This could work based on a user's fear of being exploited and their overarching need to protect themselves from online threats. So many services are outsourced these days that it may also be possible to use a totally separate company altogether but with references/ images to multiple banks who have requested they carry out this training on their behalf.

Attack frameworks that fail to harvest any credentials or to exploit users usually just wait for other potential victims to connect. There may be some potential for extending frameworks further to include other attack vectors. Ransomware and scareware are another source of revenue to malware writers and could be used as another attack vector within these frameworks if all else fails. This may provide a way to gain a foothold on a user's machine or as another form of monetary resource. There are numerous instances of fake antivirus products displayed to users who have visited certain websites. These often claim the user's computer is infected and offer a disinfection service followed by various pay support services afterwards. User's who unfortunately click on these links then download an infected program from the attacker's website. A recent survey carried out by Google and reported in the Telegraph, (2010) found this practice widespread.

5.6 Personal Security Issues Summary

Exploit Packs and their use within Phishing attacks are on the rise as attackers seek to find more industrialised mechanisms to acquire users and their machines. They are using more and more obfuscation techniques and employing more robust defence mechanisms to try and stay one step ahead of defenders. The users they are potentially targeting have changed and more things need to be done to protect them from these threats. There are a number of countermeasures that can be utilised to carry this out but by far the most effective is user education training.

All three problem areas have now been discussed and associated attacks from within them, from these a number of conclusions have been drawn and possible areas of future work that could be carried out to thwart of mitigate such attacks.

CHAPTER SIX: CONCLUSIONS AND FUTURE WORK

6.1 Conclusions

0 day exploits will always exist; these are not though just the premise of an underworld, used for the benefit of malicious attackers but in use daily by reputable security vendors wishing to add value to their service by providing the ability that others cannot match. Once these exploits become known a limited time exists whereby they can be utilised by a wide range of attackers before the respective patches, hotfixes or workaround close the vulnerability. In saying this, corporations can be very slow to rollout updates; they have robust configuration control and release processes which they use to manage the network, install and upgrade. With thousands upon thousands of users and disparate, hardware and software it can be a gigantic task keeping everyone and everything protected so potentially leaving them exposed in certain respects.

Effective user education would provide a means to better protect users from the many dangers discussed in this thesis. Corporate users are generally provided with this but the home user is often left to fend for themselves leaving them potentially vulnerable.

Tor we have seen is somewhat a niche service, but suffers from limited hardware resources coupled with poor user practices which opens up users to attacks from malicious exit nodes and other sources.

Software bundles such as Vidalia which offer Tor, Privoxy and the Tor Button combined do provide a mechanism which ensures a certain level of privacy and security is automatically obtained if they are utilised correctly; but these should potentially be extended further to provide added security benefits to the user. This could include other browser add-ons to add an extra level of security for the user with respect to protecting their anonymity and privacy which today, according to Huber et al they are not doing. Simple plug-ins like HTTPS Everywhere will enforce a secure connection to an otherwise insecure HTTP web request.

Stuxnet provided a wakeup call to the art of the possible; it was light years ahead of previous exploitation methods using this medium and combined multiple propagation methods using different attack methods to achieve its aim. Son of Stuxnet will appear, (if it hasn't already unbeknownst to us), and the industry need to be ready for this.

The impact of 0 day exploits needs to be addressed and the methods to protect against them analysed to see if they can be managed more effectively. In the case of Stuxnet, air gaps were able to be jumped to attack potentially less secure systems, unfortunately this is all too often the case as our lives, our technology, user requirements etc. require a more flexible more connected way of working. It is only by managing these networks more effectively and making them more secure will we provide the level of protection to safeguard them. It may be that we need to take a step back and rethink our current ways of working. Potentially the answer is yes and then we must make changes, sticking to them to provide the security our networks and users need, only experience, results and research will tell.

Attribution of attacks is something that is extremely difficult to carry out, never mind definitively prove in a court of law. ISP's are now required to keep records for long periods of time but the use of multiple paths, proxy servers, cyber-cafés etc. makes finding the actual initiation point difficult. Different countries have their own respective legislation and log retention rules, however, when dealing with a state sponsored criminal set, there will always be difficulty getting information for the "last leg" of the hack.

Vendors are being responsible by trying to provide better security to their user base, Google, (2010) for example have recently provided an add-on within its search results to protect users, informing them that the website may have been compromised, others are looking aggressively at vulnerabilities identified within their applications and OS and are actively and regularly patching them but the line in the sand keeps moving, technology improves and so do the ways that attackers use to target their victims.

6.2 Future Work

As mentioned when critically analysing the use and vulnerabilities within Tor, there must be some way to look further into and identify rogue nodes and add more protection to users. Perry's, (2008) went some way to trying to identify malicious nodes but was inconclusive, so it is recommended that more detailed analysis and research in this area is carried out.

Browser plug-ins or helper add-ons should be actively geared to providing a more secure browsing experience for users and it is recommended that ways to achieve this are researched, identified and implemented. Actually making users aware is also paramount, it may be prudent to try and identify ways to provide this, be they tutorials on application install or helpful guides and recommendations from the vendor itself. More work in these areas is recommended.

Thorough research needs to be made into ways to enhance the discovery of malware such as Stuxnet and other such variants. This could be achieved by potentially looking at enhanced ways to identify that data is actually being exfiltrated or researching the specific types and format of the traffic generated when such malware calls home to command and control servers. This is a mammoth task, small call-back and control commands do not take up much bandwidth and spotting this from within the gigabits of data potentially traversing backwards and forwards through networks would be extremely difficult. More research needs to be carried out to identify such occurrences and thus potentially provide enough knowledge to create a mechanism to defend against this threat.

With regards to the impact experienced from the combined 0 day exploits utilised to infect and propagate the Stuxnet worm, better detection mechanisms need to be researched combined with complementary Incident Response Mechanisms. Previously it was mentioned that legislation is being suggested to actively enforce protection in critical ICS systems but this should only be the starting point and more works should be done to provide extra security for these networks. This may be difficult due to financial constraints, the perceived threat model but Stuxnet should be the wakeup call to drive this forward.

The difficulty of identifying potential perpetrators of Cyber Attacks and providing adequate response mechanisms to them was identified. Future work looking into better ways to carry out attribution and the ability to carry this out in a timely fashion is critical and must be addressed, although may prove difficult die to geographical boundaries, legislation and the like. A common ground may have to be found first whereby there must be seen to be a potential gain to all parties concerned which is in itself a huge task.

Google was identified as providing new defense mechanisms to protect users who utilise its search facility, this is currently within its infancy and although a step forward in the right direction but it is recommended that more work should be done as the service currently provides false negatives according to multiple sources. There are vast tracts of the Internet that are not cached and that are not visited frequently (or at all) by the varied search engine bots. Potentially this is an area that could be researched into further to identify better ways to spider the Internet. Combined with this would there be the possibility of more frequent

visits which may provide a better idea of the many malicious websites that are created or compromised or give an indication that something nefarious has occurred.

Would it be possible for the bots to be more intrusive and look specifically for malicious iframes for example with potentially an automated backend support sandbox environment that actively follows iframe links and determines if the source is benign. This may be reaching in capability or in fact may have legal issues associated with it but this would aid users, owners and hosting companies alike and may provide a quicker response mechanism if malicious content is detected. It is recommended that the possibility of instigating such a mechanism is looked into further.

APPENDICES

Appendix A - Network Traffic Abuse using TOR

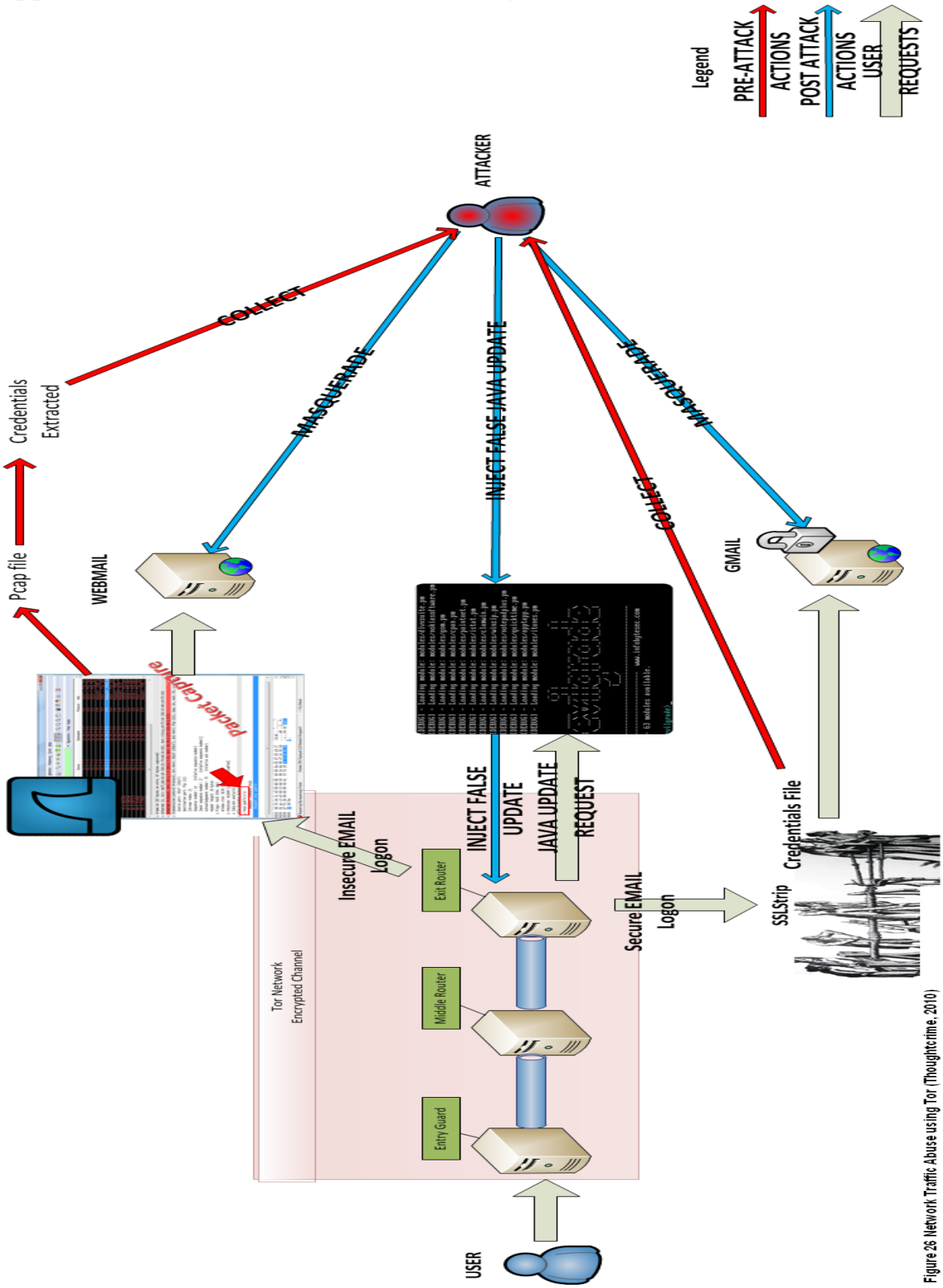


Figure 26 Network Traffic Abuse using Tor (Thoughtcrime, 2010)

Appendix B - Personal Security Issues – Phishing attack using Exploitation Framework

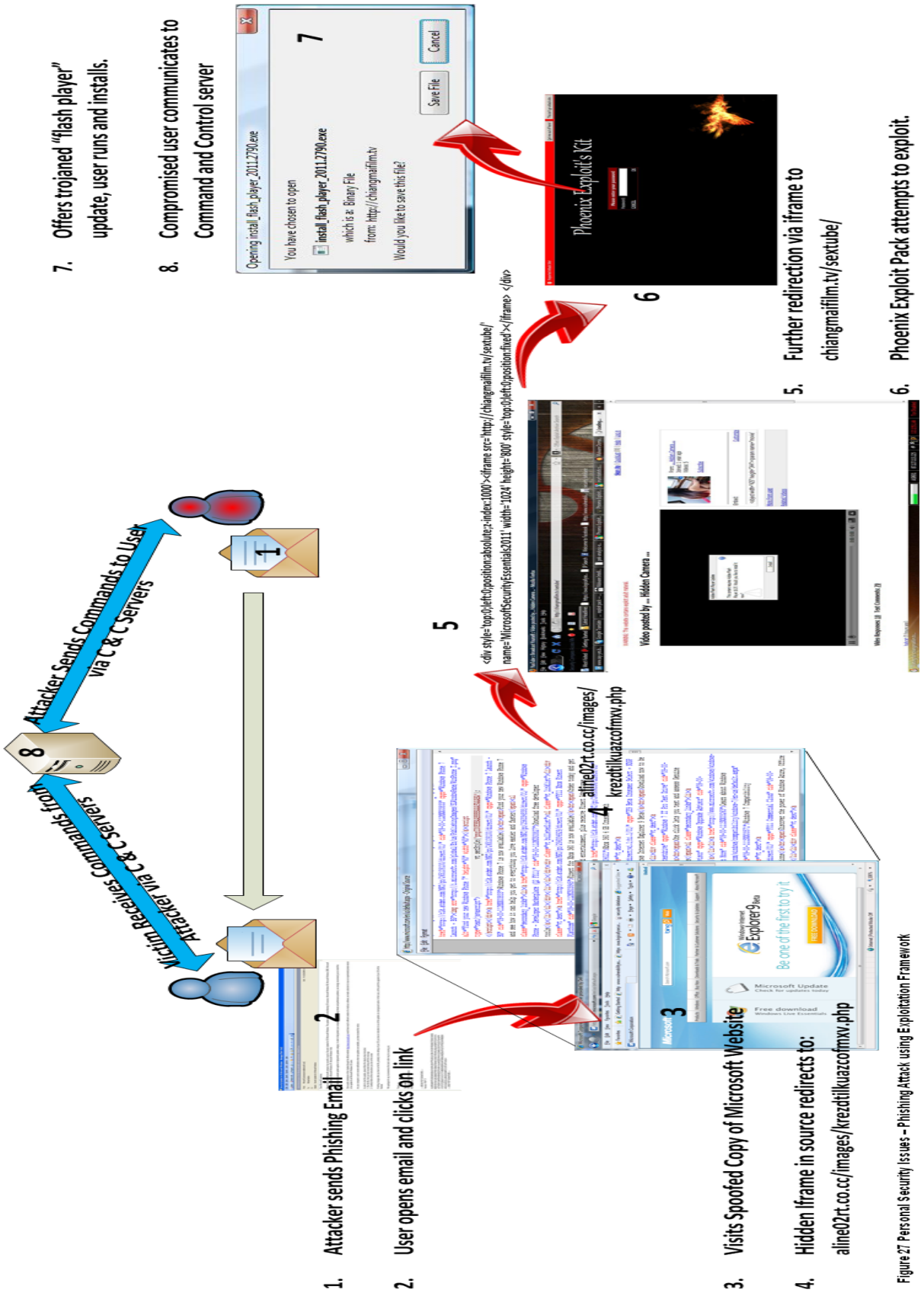


Figure 27 Personal Security Issues – Phishing Attack using Exploitation Framework

Appendix C - Physical Security Issues – How Stuxnet Propagated

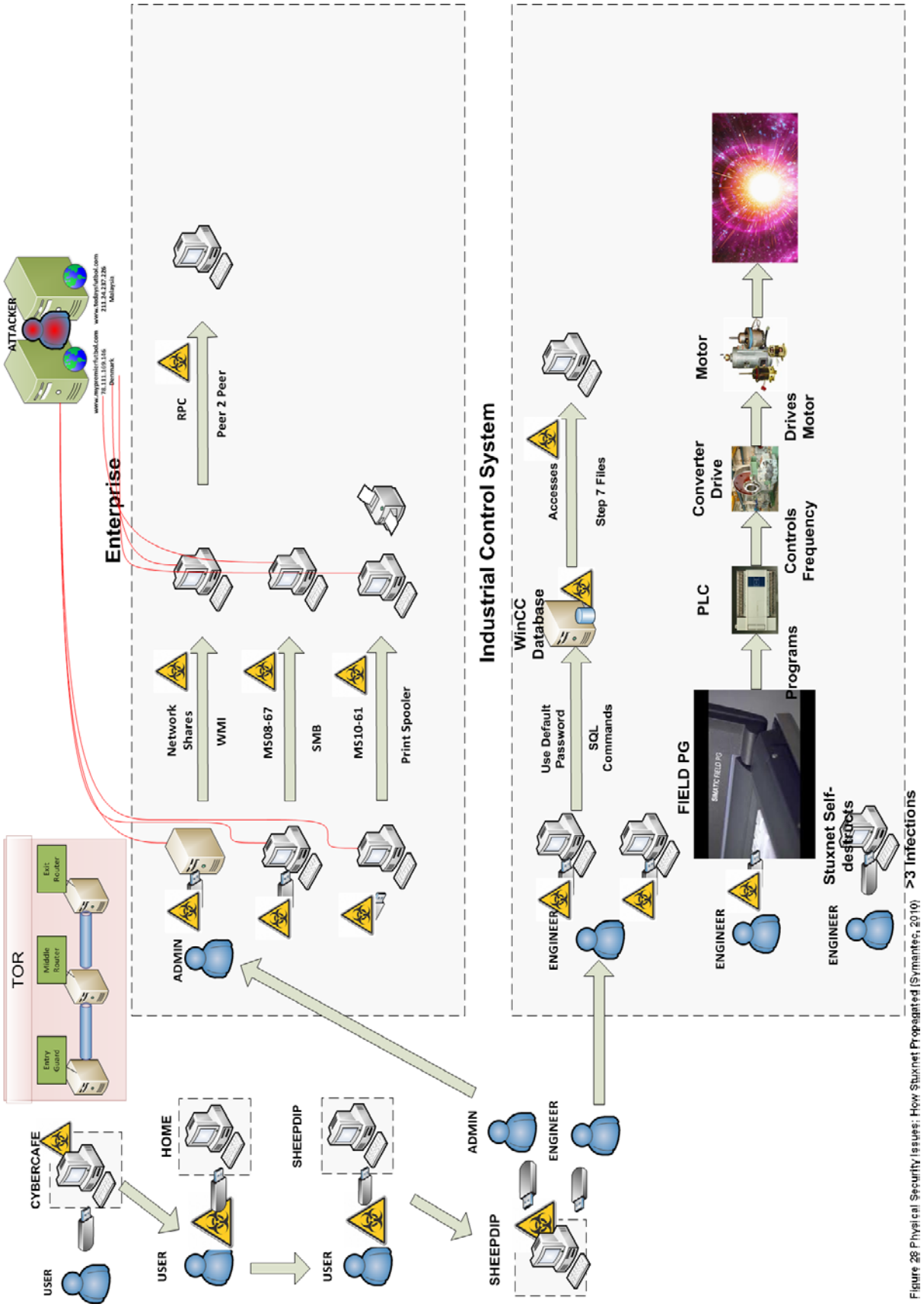


Figure 28 Physical Security Issues: How Stuxnet Propagated (Symantec, 2010)

Cyber Attack: Exploiting the User - There are so many ways!

Introduction

There is an ever present threat from Cyber Attacks
Organisations should use effective user education
Any security boundary is only as strong as its weakest link

Problem Statement

Users are targeted in 3 main problem areas:
a. Network based attacks
b. Personal Security Issues
c. Physical Security Issues

Aims and Objectives

Critically analyse the areas identified
Identify problem areas
De-construct problem areas
Identify and research attack vectors
Provide countermeasures to mitigate threats

Research Strategy

Research the most current Cyber Attack threats
Research the evolution of these attacks
Concentrate on well-known attacks
Carry out research from another angle

Network Traffic Abuse

Types of Attack
a. Domain Name Server (DNS) Redirection Attacks
b. Address Resolution Protocol (ARP) spoofing attacks
c. Sniffing Attacks
d. Man in the Middle Attacks (MiTM)
e. Router Redirection

Personal Security Issues

Social Engineering
a. Pretexting
b. Phishing, Spear phishing and Whaling
c. Baiting
d. Quid pro quo

Physical Security Issues

History of Attacks
a. Autorun
b. USB Switchblade et al
c. USB-Based Virus/Malicious Code Launch
d. USB Device Overflow
e. Social Engineering and USB

Conclusions

0 day exploits will always exist
Attribution of attacks is poor
Current Incident Response mechanisms are poor
Ineffective patching and updating is employed
User education is poor

TOR Case Study

Rogue Router Attacks
a. Sniffing Attacks
b. Sybil Attacks
c. Privacy Attacks
d. Session Hijacking
e. MiTM Attacks

Phishing Case Study

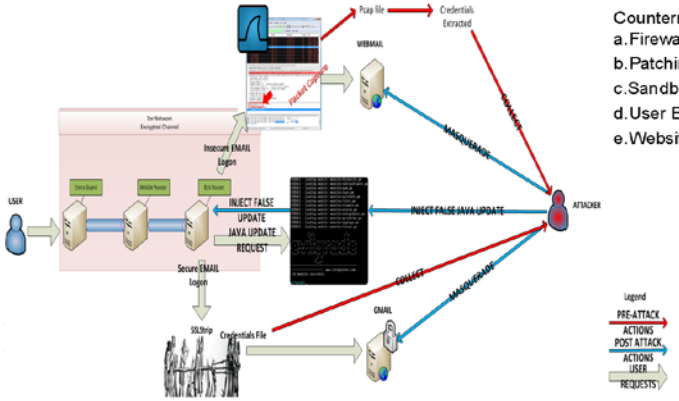
Background
a. Current Phishing Trends and Targets
b. Phishing Obfuscation Techniques
c. Phishing Attack Frameworks
d. How Attack Frameworks Work
e. Exploit Packs

Stuxnet Case Study

Countermeasures
a. Regularly updated Anti-Virus
b. Effective Patching
c. Host Intrusion Prevention Systems (HIPS)
d. Host Intrusion Detection Systems (HIDS)
e. Data Leakage Prevention
f. User Awareness

Future Work

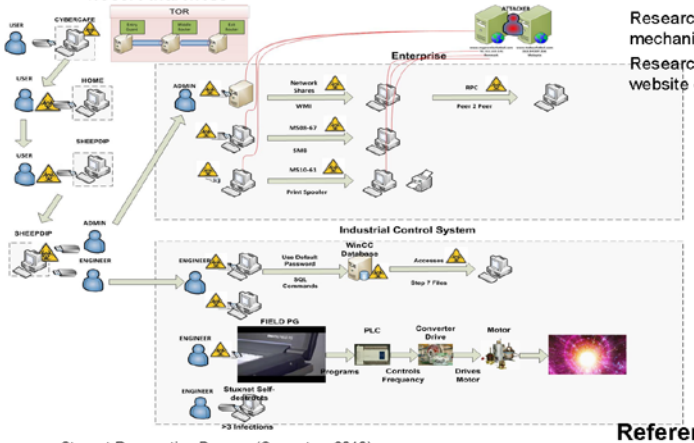
Enhance the discovery of malware
Identify more effective user education methods
Identify Rogue Nodes
Identify better attack detection mechanisms
Research more effective user security mechanisms
Research into automated malicious website detection



Tor Network Abuse (Thoughtcrime, 2010)

Countermeasures

a. Firewall and Filtering
b. Patching
c. Sandboxing
d. User Education
e. Website Takedown



Stuxnet Propagation Process (Symantec, 2010)

Countermeasures

Two-factor authentication mechanisms
Single sign-on facilities
Utilise secure protocols
Reduce user rights
Use trusted Entry and Exit nodes
Software Restrictions
Effective user education program

References

National Security Agency, (2009) "*Security Configuration Guides*" Available from: http://www.nsa.gov/ia/guidance/security_configuration_guides/index.shtml [Accessed 6 Jan 11]
Perry, Mike, (2008) "*TorFlow: Tor Network Analysis*" Available from: http://fscked.org/talks/TorFlow-HotPETS-final.pdf [Accessed 6 Dec 10]
Shema, Mike, (2010) in the "*Seven Deadliest Web Application Attacks*" Syngress
Symantec Corporation, (2010) "*W32.Stuxnet Dossier*" Available online from: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf [Accessed 16 Nov 10]

Kevin Orrey. 0818507, MSc Computer Security and Forensics, Dr Ali Mansour

REFERENCES

Aldeid.com, (2010) "*Social Engineering Ninja (aka S-E Ninja)*" Available from: http://www.aldeid.com/index.php/Social-Engineering-Ninja [Accessed 6 Jan 11]

Anderson Brian, Anderson, Barbara, (2010) "*Seven Deadliest USB Attacks*" Syngress

APWG, (2010) "*Report a Suspected Phishing Site*" Available from: http://www.antiphishing.org/report_phishing.html [Accessed 6 Jan 11]

Attack and Defense Labs, (2010) "*What is Imposter?*" Available from: http://www.andlabs.org/tools/imposter/Imposter.html [Accessed 6 Jan 11]

Bauer, Kevin, McCoy, Damon, Grunwald, Dirk, Kohno, Tadayoshi, Sicker, Douglas, (2007) "*Low-Resource Routing Attacks against Anonymous Systems*" Available from: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.140.9042&rep=rep1&type=pdf [Accessed 14 Oct 10]

BBC (2010) "*Security experts say Google cyber-attack was routine*" Available on-line from: http://news.bbc.co.uk/1/hi/technology/8458150.stm [Accessed 31 Aug 10]

BBC, (2004) "*Passwords revealed by sweet deal*" Available from: http://news.bbc.co.uk/1/hi/technology/3639679.stm [Accessed 22 Dec 10]

BBC, (2009) "*BBC team exposes cyber crime risk*" Available from: http://news.bbc.co.uk/1/hi/programmes/click_online/7932816.stm [Accessed 10 Dec 10]

BBC, (2010) "*Cyber attacks against Australia 'will continue'*" Available from: http://news.bbc.co.uk/1/hi/technology/8513073.stm [Accessed 20 Nov 10]

BBC, (2010) "*Cyber attacks and terrorism head threats facing UK*" Available from: http://www.bbc.co.uk/news/uk-11562969 [Accessed 20 Nov 10]

BBC, (2010) "*Stuxnet worm 'targeted high-value Iranian assets'*" Available from: http://www.bbc.co.uk/news/technology-11388018 [Accessed 6 Dec 10]

BBC, (2010) "*Yahoo targeted in China cyber-attacks*" Available from: http://news.bbc.co.uk/1/hi/8596410.stm [Accessed 20 Nov 10]

Binarysec, (2009) "*P-S*" Available online from: http://www.binarysec.com/cms/docs/resources/glossary/p-s.html [Accessed 7 Dec 10]

Blackhat, (2007) "*Securing the Tor Network*" Available from: https://www.blackhat.com/presentations/bh-usa-07/Perry/Whitepaper/bh-usa-07-perry-WP.pdf [Accessed 5 Oct 10]

Blackhat, (2009) "*New Tricks For Defeating SSL In Practice*" Available online from: http://www.blackhat.com/presentations/bh-dc-09/Marlinspike/BlackHat-DC-09-Marlinspike-Defeating-SSL.pdf [Accessed 4 Nov 10]

BlackhatMoneyMaker.com, (2010) "*YES Exploit system for sale! Excellent pack from Russian blackhats*" Available from**:** http://www.blackhatmoneymaker.com/forum/buy-sell-

trade/2166-yes-exploit-system-sale-excellent-pack-russian-blackhats.html [Accessed 6 Jan 11]

Blat, (2011" "*What is Blat?*" Available from: http://www.blat.net/ [Accessed 6 Jan 11]

Cassandra Security, (2009) "*Onion Routing and Darknets*" Available online from: http://cassandrasecurity.com/index.php?s=onion+routing [Accessed 4 Oct 10]

CESG, (2009) "*HMG IA Standard No.1 - Technical Risk Assessment - Issue 3.51, October 2009*" Available online from: http://www.cesg.gov.uk/publications/media/policy/is1_risk_assessment.pdf [Accessed 5 Oct 10]

CESG, (2010) "*Good Practice Guide 23- Assessing the Threat of Technical Attack Against ICT Systems*" Communications Electronics Security Group

Chinotec Technologies Company, (2004) "*Paros*" Available from: http://www.parosproxy.org/ [Accessed 6 Jan 11]

Cisco, (2011) "*Cisco IronPort Data Loss Prevention*" Available from: http://www.cisco.com/en/US/prod/vpndevc/ps10128/ps10154/dlp_overview.html [Accessed 6 Jan 11]

Computerweekly.com, (2010) "*Blended threats demand new security approach, says Websense*" http://www.computerweekly.com/Articles/2010/03/12/240595/Blended-threats-demand-new-security-approach-says-Websense.htm [Accessed 4 Nov 10]

Computerworld, (2010) "*Alleged China attacks could test U.S. cybersecurity policy*" Available from: http://www.computerworld.com/s/article/9144440/Alleged_China_attacks_could_test_U.S._cybersecurity_policy [Accessed 22 Dec 10]

ComputerWorld, (2010) "Was *Stuxnet built to attack Iran's nuclear program?*" Available from: http://www.computerworld.com/s/article/9186920/Was_Stuxnet_built_to_attack_Iran_s_nuclear_program_ [Accessed 6 Dec 10]

Core Security Technologies (2010) "*CORE IMPACT Pro Overview*" Available from: http://www.coresecurity.com/content/core-impact-overview [Accessed 6 Jan 11]

Cyberspace and Information Study Centre, (2010) "*Computer Network Operations and Network Warfare Operations*" Available on-line from: http://www.au.af.mil/info-ops/netops.htm [Accessed 31 Aug 10]

DamageLab, (2010) "*Eleonore Exp v1.6.2*" Available from: https://damagelab.org/index.php?showtopic=17952 [Accessed 6 Jan 11]

Damon McCoy, Kevin Bauer, Dirk Grunwald, Tadayoshi Kohno, and Douglas Sicker, (2008) "*Shining Light in Dark Places: Understanding the Tor Network*". In Proceedings of the 8th Privacy Enhancing Technologies Symposium (PETS 2008), Leuven, Belgium, July 2008.

Dennis Publishing, (2010) "Botnets *for hire: £6 an hour*"Available from: http://www.pcpro.co.uk/news/security/358207/botnets-for-hire-6-an-hour [Accessed 10 Dec

10]

DeviceLock, Inc. (2011) "*DeviceLock*" Available from: http://www.devicelock.com/ [Accessed 6 Jan 11]

Digicert Inc, (2009) "*Phishing - A Primer on What Phishing is and how it Works*" Available online from: http://www.antiphishing.org/sponsors_technical_papers/DigiCert_Phishing_White_Paper.pdf [Accessed 8 Dec 10]

DigitalCoding.com, (2010) "*Detect Internet Browser Settings*" Available from: http://www.digitalcoding.com/tools/detect-browser-settings.html [Accessed 15 Dec 10]

DomainTools, LLC, (2011) "*Whois Record For xn----8sbfnlobtdfef1cc1f.com*" Available from: http://whois.domaintools.com/xn----8sbfnlobtdfef1cc1f.com [Accessed 6 Jan 11]

Electronic Frontier Foundation (EFF), (2010) "*HTTPS Everywhere*" Available online from: https://www.eff.org/https-everywhere [Accessed 1 Oct 10]

ESET, (2010) "*Stuxnet the Inscrutable*" Available from: http://blog.eset.com/2010/10/13/stuxnet-the-inscrutable [Accessed 1 Nov 10]

GFI Software, (2011) "*GFI Endpoint Security*" Available from: http://www.gfi.com/endpointsecurity [Accessed 6 Jan 11]

Goggle, (2010) "*New Hacked Site Notifications in Search Results*" Available from http://googlewebmastercentral.blogspot.com/2010/12/new-hacked-site-notifications-in-search.html [Accessed 22 Dec 10]

Google, (2011) "*vladimir ivanov wega ltd*" Available from: http://www.google.co.uk/search?q=vladimir+ivanov+wega+ltd [Accessed 6 Jan 11]

Google Operating System Blog, (2007) "*Firefox 3 Will Include Malware Protection*" Available from: http://googlesystem.blogspot.com/2007/06/firefox-3-will-include-malware.html [Accessed 8 Dec 10]

GreyZer0, (2010) "*Social-Engineering Ninja v0.4 is out!*" Available from: https://grey0.wordpress.com/2010/12/04/social-engineering-ninja-v0-4-is-out/ [Accessed 15 Dec 10]

hak5.org, (2011) "*Amish*" Available from: http://www.hak5.org/releases/2x02/switchblade/AMISH1.0-payload.rar [Accessed 6 Jan 11]

hak5.org, (2011) "*USB Antidote*" Available from: http://www.hak5.org/w/index.php/USB_Antidote [Accessed 6 Jan 11]

hak5.org, (2011) "*USB Hacksaw*" Available from: http://www.hak5.org/wiki/USB_Hacksaw [Accessed 6 Jan 11]

hak5.org, (2011) "*USB Switchblade*" Available from: http://www.hak5.org/wiki/USB_Switchblade [Accessed 6 Jan 11]

Hakin9, (2009) "*Print Your Shell*" Available from: http://hakin9.org/magazine/885-my-erp-got-hacked [Accessed 29 Dec 10]

Hewlett-Packard Development Company, (2010) "2010 *Top Cyber Security Risks Report*" Available from: http://dvlabs.tippingpoint.com/toprisks2010 [Accessed 20 Nov 10]

Homeland Security, (2011) "*Catalog of Control Systems Security: Recommendations for Standards Developers*" Available from: http://www.us-cert.gov/control_systems/pdf/Catalog_of_Control_Systems_Security_Recommendations.pdf [Accessed 6 Jan 11]

Huber, Mark, Mulazzani, Martin and Weippl, Edgar, (2010) "*Tor HTTP usage and Information Leakage*" Available from: http://www.sba-research.org/wp-content/uploads/publications/2010%20-%20Huber%20-%20Tor%20HTTP%20Usage.pdf [Accessed 8 Nov 10]

Ihsana IT Solution, (2010) "*Analisa Virus Tmphider atau Stuxnet [07-2010]*" Available online from: http://www.ihsana.com/?page=vblog&id=16 [Accessed 1 Oct 10]

Immunity, Inc. (2011) "*CANVAS*" Available from: http://www.immunitysec.com/ [Accessed 6 Jan 11]

Infobyte Security Research, (2011) "*ISR-evilgrade* " Available from: http://www.infobytesec.com/down/isr-evilgrade-Readme.txt [Accessed 6 Jan 11]

InformIT, (2007) "*USB Hacks*" Available from: http://www.informit.com/guides/content.aspx?g=security&seqNum=263 [Accessed 22 Nov 10]

IonCube Ltd. (2011) "*The ionCube PHP Encoder*" Available from: http://www.ioncube.com/sa_encoder.php?page=features [Accessed 6 Jan 11]

IP2Location.com (2011) "*Web Query to Reverse Lookup Country, State, City, Latitude, Longitude and ISP by IP address*" Available from: http://www.ip2location.com/free.asp [Accessed 6 Jan 11]

IronGeek, (2011) "*Manual Reference Pages - httpcapture*" Available from: http://www.irongeek.com/i.php?page=backtrack-3-man/httpcapture# [Accessed 6 Jan 11]

Isssource.com, (2010) "*Stuxnet Mitigation: Defense in Depth Needed*" Available from: http://www.isssource.com/stuxnet-mitigation-defense-in-depth-needed/ [Accessed 31 Dec 10]

Jacknowitz, Alison (2010) "*CYBER-ATTACKS! Trends in US Corporations*" Available on-line from: http://www.bizforum.org/whitepapers/rand001.htm [Accessed 31 Aug 10]

James, Lance, (2005) "*Phishing Exposed*" Syngress

Joseph B. Kowalski, (2006) "*Tor Network Status*" Available online from: http://torstatus.blutmagie.de/ [Accessed 4 Oct 10]

Kaspersky, (2010) "*Unraveling Stuxnet*" Available from: http://www.kaspersky.com/downloads/press/aleks_gostev,_costin_g._raiu._unravelling_stux

net.zip [Accessed 10 Dec 10]

Kath, Ravi (2010) "*Botnet World and the 10 Most wanted Spam Botnet's…*" Available on-line from: http://ravikanthl.wordpress.com/2010/07/25/botnet-world-and-the-10-most-wanted-spam-botnets/ [Accessed 1 Sep 10]

Krebs on Security, (2010) "*Exploit Packs"* Available from: http://krebsonsecurity.com/tag/exploit-pack/ [Accessed 6 Jan 11]

Krebs on Security, (2010) "*Google Debuts "This Site May Be Compromised" Warning*" Available from: http://krebsonsecurity.com/2010/12/google-debuts-this-site-may-be-compromised-warning/#more-7153 [Accessed 22 Dec 10]

KrebsonSecurity, (2010) "*Java: A Gift to Exploit Pack Makers*" Available from: http://krebsonsecurity.com/2010/10/java-a-gift-to-exploit-pack-makers/ [Accessed 21 Dec 10]

Kuppan, Lavakumar (2010) "*Flash+IE = Prison Break - stealing Local Files through the Flash Plugin in IE*" Available from: http://andlabs.org/whitepapers/F_IE_PrisonBreak.pdf [Accessed 20 Dec 10]

legislation.gov.uk, (2010) "*Communications Act 2003*" Available from: http://www.legislation.gov.uk/ukpga/2003/21/contents [Accessed 5 Jan 11]

legislation.gov.uk, (2010) "*Computer Misuse Act 1990*" Available from: http://www.legislation.gov.uk/ukpga/1990/18/contents [Accessed 5 Jan 11]

legislation.gov.uk, (2010) "*Regulation of Investigatory Powers Act 2000*" Available from: http://www.legislation.gov.uk/ukpga/2000/23/contents [Accessed 5 Jan 11]

Linniger, Rachael, Vines, Russell, (2005) "*Phishing: Cutting the Identity Theft Line*" Wiley Publishing

Linuxreviews.org, (2010) "*Tor*" Available online from: http://en.linuxreviews.org/Tor [Accessed 1 Oct 10]

Lumension Security, (2010) "*Lumension Device Control (formerly sanctuary)*" Available from: http://www.lumension.com/device-control-software/usb-security-protection.aspx [Accessed 6 Jan 11]

MalwareIntelligence, (2010) "*Malware and Exploit Packs*" Available from: http://malwareint.blogspot.com/ [Accessed 6 Jan 11]

MaxMind, Inc. (2010) "*Maxmind*" Available from: http://www.maxmind.com/ [Accessed 6 Jan 11]

McAfee, (2011) "*W32/Renocide*" Available from: http://vil.nai.com/vil/content/v_153535.htm [Accessed 6 Jan 11]

McAfee, (2010) "*An Overview of Exploit Packs*" Available from: http://blogs.mcafee.com/mcafee-labs/an-overview-of-exploit-packs [Accessed 19 Dec 10]

Message Labs, (2010) "*Symantec Announces MessageLabs Intelligence 2010 Annual Security Report*" Available from: http://www.messagelabs.co.uk/resources/press/64370

[Accessed 7 Dec 10]

Metasploit, (2011) "*Metasploit Framework*" Available from: http://www.metasploit.com/ [Accessed 6 Jan 11]

Michigan.gov, (2010) "*Definitions*" Available on-line from: http://www.michigan.gov/cybersecurity/0,1607,7-217-34415---,00.html [Accessed 1 Sep 10]

Microsoft, (2010) "*Have you checked the Java?*" Available from http://blogs.technet.com/b/mmpc/archive/2010/10/18/have-you-checked-the-java.aspx [Accessed 21 Dec 10]

Microsoft, (2010) "*How to disable the Autorun functionality in Windows*" Available from: http://support.microsoft.com/kb/967715 [Accessed 30 Nov 10]

Microsoft, (2010) "*How to recognise a phishing scam email*" Available online from: https://www.microsoft.com/nz/digitallife/security/how_to_recognise_a_phishing_scam_e-mail.mspx [Accessed 10 Dec 10]

Microsoft, (2010) "*The Stuxnet Sting*" Available on-line from: http://blogs.technet.com/b/mmpc/archive/2010/07/16/the-stuxnet-sting.aspx [Accessed 31 Aug 10]

Microsoft, (2008) "*Frequently Asked Questions*" Available from: https://phishingfilter.microsoft.com/PhishingFilterFaq.aspx [Accessed 6 Jan 11]

Microsoft, (2011) "*Fix-it*" Available from: http://go.microsoft.com/?linkid=9741395 [Accessed 6 Jan 11]

Microsoft, (2011) "*How can I prevent users from connecting to a USB storage device?*" Available from: http://support.microsoft.com/default.aspx?scid=kb;EN-US;823732 [Accessed 6 Jan 11]

Microsoft, (2011) "*HOWTO: Use Group Policy to disable USB, CD-ROM, Floppy Disk and LS-120 drivers*" Available from: http://support.microsoft.com/kb/555324 [Accessed 6 Jan 11]

Microsoft, (2011) "*Microsoft Security Bulletin MS08-067 – Critical*" Available from: http://www.microsoft.com/technet/security/bulletin/ms08-067.mspx [Accessed 6 Jan 11]

Microsoft, (2011) "*Microsoft Security Bulletin MS10-046 - Critical*" Available from: http://www.microsoft.com/technet/security/bulletin/ms10-046.mspx [Accessed 6 Jan 11]

Microsoft, (2011) "*Microsoft Security Bulletin MS10-061 - Critical*" Available from: https://www.microsoft.com/technet/security/Bulletin/MS10-061.mspx [Accessed 6 Jan 11]

Microsoft, (2011) "*Microsoft Security Bulletin MS10-073 - Important*" Available from: http://www.microsoft.com/technet/security/bulletin/ms10-073.mspx [Accessed 6 Jan 11]

Microsoft, (2011) "*Microsoft Security Bulletin MS10-092 - Important*" Available from: http://www.microsoft.com/technet/security/bulletin/ms10-092.mspx [Accessed 6 Jan 11]

Microsoft, (2011) "*MS08-038: Vulnerability in Windows Explorer could allow remote code execution*" Available from: http://support.microsoft.com/kb/950582/en-us [Accessed 6 Jan 11]

Microsoft, (2011), "*Microsoft Baseline Security Analyzer*" Available from: http://technet.microsoft.com/en-us/security/cc184924 [Accessed 6 Jan 11]

Moore, Tyler, Clayton, Richard, (2008) "*The Impact of Incentives on Notice and Take-down*" Seventh Workshop on the Economics of Information Security (WEIS 2008), June 25–28 2008.

Mozilla.org, (2011) "*QuickJava 1.7.2*" Available from: https://addons.mozilla.org/en-us/firefox/addon/1237/ [Accessed 6 Jan 11]

MWR Labs, (2009) "*USB Attacks: Fun with Plug and 0wn*" Available from: http://labs.mwrinfosecurity.com/files/Publications/mwri_usb-attacks-defcon17_2009-08-02.pdf [Accessed 3 Dec 10]

National Security Agency, (2009) "*Security Configuration Guides*" Available from: http://www.nsa.gov/ia/guidance/security_configuration_guides/index.shtml [Accessed 6 Jan 11]

NgepRESS.COM, (2009) "*Mygener.im | Mygener.im Virus or Phishing Site Facebook???"* Available from: http://ngepress.com/news/mygenerim-mygenerim-virus-or-phishing-site-facebook/ [Accessed 10 Dec 10]

NIST, (2011) "*Guide to Industrial Control Systems (ICS) Security*" Available from: http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf [Accessed 6 Jan 11]

NIST, (2011) "*National Checklist Program Repository*" Available from: http://web.nvd.nist.gov/view/ncp/repository?cid=1 [Accessed 6 Jan 11]

NoScript.net, (2010) "*NoScript - JavaScript/Java/Flash blocker for a safer Firefox*" Available from: http://noscript.net/ [Accessed 6 Jan 11]

OWASP, (2011), "*OWASP Zed Attack Proxy Project*" Available from: http://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project [Accessed 6 Jan 11]

Patzcatz.com, (2011) "*Javascript DeObfuscator*" Available from: http://www.patzcatz.com/unescape.htm [Accessed 6 Jan 11]

Paypal, (2010), " *Can you spot phishing?*" Available from: https://www.paypal-marketing.co.uk/safetyadvice/TakeTheQuiz.htm [Accessed 6 Jan 11]

Perry, Mike, (2008) "*TorFlow: Tor Network Analysis*" Available from: http://fscked.org/talks/TorFlow-HotPETS-final.pdf [Accessed 6 Dec 10]

Phishtank, (2009) "*Stats › November 2010*" Available online from http://www.phishtank.com/stats/2009/11/ [Accessed 8 Dec 10]

Phishtank, (2010) "*Stats › November 2010*" Available online from http://www.phishtank.com/stats/2010/11/ [Accessed 8 Dec 10]

PortSwigger Ltd, (2010) "*Burp*" Available from: http://portswigger.net/burp/ [Accessed 6 Jan 11]

Rapidshare, (2011) "*Kapowdude*" Available from: http://rapidshare.de/files/34686392/MAD_1.0.rar.html [Accessed 6 Jan 11]

SANS, (2007) "*SANS Laboratory – Defense in Depth Series*" Available from: http://www.sans.edu/resources/securitylab/321.php [Accessed 20 Nov 10]

SecManiac.com, (2011) "*Home of the Social Enginerring Toolkit*" Available from: http://www.secmaniac.com/ [Accessed 6 Jan 11]

Secunia ApS, (2010) "*Secunia Personal Software Inspector (PSI)*" Available from: http://secunia.com/vulnerability_scanning/personal/ [Accessed 6 Jan 11]

Secunia, (2010) "*Secunia Half Year Report 2010*" Available from: http://secunia.com/gfx/pdf/Secunia_Half_Year_Report_2010.pdf [Accessed 21 Dec 10]

Secuobs, (2011) "*USBDumper*" Available from: http://www.secuobs.com/USBDumper.rar [Accessed 6 Jan 11]

SecureComputing.com, (2010) "*Kroxxu botnet targets one million users*" Available from: http://www.securecomputing.net.au/News/239314,kroxxu-botnet-targets-one-million-users.aspx [Accessed 29 Nov 10]

Shema, Mike, (2010) in the "*Seven Deadliest Web Application Attacks*" Syngress

Siemens AG, (2010) "*SIMATIC WinCC / SIMATIC PCS 7: Information concerning Malware / Virus / Trojan*" Available from: http://support.automation.siemens.com/WW/llisapi.dll?func=ll&objid=43876783 [Accessed 6 Jan 11]

Sky News, (2010) "*Super Virus A Target For Cyber Terrorists*" Available from: http://news.sky.com/skynews/Home/World-News/Stuxnet-Worm-Virus-Targeted-At-Irans-Nuclear-Plant-Is-In-Hands-Of-Bad-Guys-Sky-News-Sources-Say/Article/201011415827544?lpos=World_News_First_Home_Article_Teaser_Region_2&lid=ARTICLE_15827544_Stuxnet_Worm%3A_Virus_Targeted_At_Irans_Nuclear_Plant_Is_In_Hands_Of_Bad_Guys%2C_Sky_News_Sources_Say [Accessed 3 Dec 10]

Social-engineer.org, (2010) "*Computer Based Social Engineering Tools: Social Engineer Toolkit (SET)*" Available from: http://www.social-engineer.org/framework/Computer_Based_Social_Engineering_Tools:_Social_Engineer_Toolkit_%28SET%29#Infectious_Media_Generator [Accessed 20 Dec 10]

Song, Dug, (2011) "*Dsniff*" Available from: http://monkey.org/~dugsong/dsniff/ [Accessed 6 Jan 11]

Sonicwall, (2010) "*SonicWALL Phishing and Spam IQ Quiz*" Available from: http://www.sonicwall.com/phishing/index.html [Accessed 6 Jan 11]

Sophos Ltd.(2010) "*19790509: The mysterious number inside the Stuxnet worm*" Available from: http://nakedsecurity.sophos.com/2010/11/23/19790509-the-mysterious-number-inside-the-stuxnet-worm/ [Accessed 6 Jan 11]

SPI Dynamics, (2005) "*Plug and Root: The USB Key to the Kingdom*" Available from: http://www.blackhat.com/presentations/bh-usa-05/BH_US_05-Barrall-Dewey.pdf [Accessed 3 Dec 10]

Stevens, Didier, (2009) "*Quickpost: Disarming a PDF File*" Available from: http://blog.didierstevens.com/2009/04/29/quickpost-disarming-a-pdf-file/ [Accessed 6 Jan 11]

Stunnel.org, (2011) "*Stunnel -- Universal SSL Wrapper*" Available from: http://www.stunnel.org/ [Accessed 6 Jan 11]

Symantec Corporation, (2010) "*W32.Stuxnet Dossier*" Available online from: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf [Accessed 16 Nov 10]

Symantec, (2010) "*Stuxnet: A Breakthrough*" Available from: http://www.symantec.com/connect/blogs/stuxnet-breakthrough [Accessed 29 Nov 10]

Tatum, Malcolm (2010) "*What Is a Cyber-attack?*" Available on-line from: http://www.wisegeek.com/what-is-a-cyberattack.htm [Accessed 31 Aug 10]

Tcpdump/Libpcap, (2010) "*Welcome*" Available from: http://www.tcpdump.org/ [Accessed 6 Jan 11]

TechCrunch, (2009) "*The Anatomy of the Twitter Attack: Part II*" Available on-line from: http://techcrunch.com/2009/12/18/anatomy-twitter-attack-2-dns-iran/ [Accessed 2 Sep 10]

Techcrunch, (2010) "*Google Defends Against Large Scale Chinese Cyber Attack: May Cease Chinese Operations*" Available from: http://techcrunch.com/2010/01/12/google-china-attacks/ [Accessed 22 Dec 10]

Techworld.com, (2010) "*Spanish police shut down 'world's largest' botnet*" Available on-line from: http://news.techworld.com/security/3214049/spanish-police-shut-down-worlds-largest-botnet/?olo=rss [Accessed 1 Sep 10]

Telegraph, (2010) "*Fake antivirus software is 'growing threat' to computer users, warns Google*" Available from: http://www.telegraph.co.uk/technology/google/7647112/Fake-antivirus-software-is-growing-threat-to-computer-users-warns-Google.html [Accessed 21 Dec 10]

The Associated Press, (2010) "*Stuxnet virus could target many industries*" Available online from: http://www.washingtonpost.com/wp-dyn/content/article/2010/11/17/AR2010111702516.html [Accessed 20 Nov 10]

The MITRE Corporation, (2011) "*CVE*" Available from: http://cve.mitre.org/ [Accessed 6 Jan 11]

The MITRE Corporation, (2011) "*CVE-2010-2772 (under review)*" Available from: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2772 [Accessed 6 Jan 11]

ThinkGeek, (2008) "*Hack U3 USB Smart Drive to Become Ultimate Hack Tool*" Available from: http://shailendra88.blogspot.com/2007/11/hack-u3-usb-smart-drive-to-become.html

[Accessed 23 Nov 10]

thoughtcrime.org, (2011) "*SSLStrip*" Available from: http://www.thoughtcrime.org/software/sslstrip/ [Accessed 6 Jan 11]

The Register, (2008) "*Hijacking huge chunks of the internet - a new How To* "Available from: http://www.theregister.co.uk/2008/08/27/bgp_exploit_revealed/ [Accessed 20 Nov 10]

The Register, (2010) "*Chinese ISP hijacked US military, gov web traffic* "Available from: http://www.theregister.co.uk/2010/11/17/bgp_hijacking_report/ [Accessed 20 Nov 10]

The Register, (2010) "*Glitch diverts net traffic through Chinese ISP* "Available from: http://www.theregister.co.uk/2010/04/10/bgp_glitch/ [Accessed 20 Nov 10]

The Register, (2010) "*MoD bod warns of cyber-attack risk*" Available on-line from: http://www.theregister.co.uk/2010/08/12/mod_accounts/ [Accessed 31 Aug 10]

The Register, (2010) "*Texas man cops to botnet-for-hire charges - DDoS demo backfires*" Available from: http://www.theregister.co.uk/2010/04/28/botnet_for_hire_guilty/ [Accessed 10 Dec 10]

The Register, (2010) "*Greek police cuff Anonymous spokesman suspect*" Available from: http://www.theregister.co.uk/2010/12/16/anonymous_arrests/ Accessed 17 Dec 10]

Torproject.org (2010) "*Tor Directory Specification*" Available from: http://gitweb.torproject.org/tor.git?a=blob_plain;hb=HEAD;f=doc/spec/dir-spec-v2.txt [Accessed 4 Oct 10]

Trend Micro Incorporated, (2010), "*Stuxnet Malware Targeting SCADA Systems*" Available from: http://threatinfo.trendmicro.com/vinfo/web_attacks/Stuxnet%20Malware%20Targeting%20SCADA%20Systems.html [Accessed 30 Dec 10]

Trend Micro Incorporated, (2010), "*STUXNET: Old Tricks, New Exploit*" Available from: http://threatinfo.trendmicro.com/vinfo/articles/securityarticles.asp?xmlfile=091410-STUXNET.xml [Accessed 1 Nov 10]

Ubuntu North Carolina Local Community Team, (2008) "*There are no secrets… anymore*." Available from: http://ubuntunc.com/nosecrets/ [Accessed 10 Oct 10]

United States-China Economic and Security Review Commission, (2010) "*Operation Aurora*" In 2010 REPORT TO CONGRESS of the U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION, ONE HUNDRED ELEVENTH CONGRESS SECOND SESSION, Nov 2010.

Unmask Parasites, (2010) "*Hackers Turn Legitimate Websites into Underground Software Stores*" Available from: http://blog.unmaskparasites.com/2010/12/10/hackers-turn-legitimate-websites-into-undeground-software-stores/ [Accessed 22 Dec 10]

US-CERT, (2009) "*Microsoft Windows Does Not Disable Autorun Properly*" Available from: http://www.us-cert.gov/cas/techalerts/TA09-020A.html [Accessed 30 Nov 10]

UCSB Computer Security Lab, (2010) "*Wepawet (alpha)*" Available from: http://wepawet.iseclab.org/index.php [Accessed 6 Jan 11]

Verisign Inc. (2010) "*Phish or No Phish?*" Available from: https://www.phish-no-phish.com/default.aspx [Accessed 6 Jan 11]

Virus Bulletin, (2010), "*VB 2010"* Available online from: http://www.virusbtn.com/conference/vb2010/index [Accessed 6 Jan 11]

Vulnes, (2011) "*Phoenix Exploit Pack 1.x*" Available from: http://vulnes.com/showthread.php?t=713 [Accessed 6 Jan 11]

War In Context, (2010) "*Iran confirms Stuxnet found at Bushehr nuclear power plant*" Available from: http://warincontext.org/2010/09/26/iran-confirms-stuxnet-found-at-bushehr-nuclear-power-plant/ [Accessed 6 Dec 10]

Wikileaks, (2011) "*Wikileaks*" Available from: http://wikileaks.org/ [Accessed 6 Jan 11]

WindowsITPro, (2008) "*ICANN Falls Victim to DNS Redirection Attack*" Available on-line from: http://www.windowsitpro.com/article/dns/icann-falls-victim-to-dns-redirection-attack.aspx [Accessed 2 Sep 10]

Wired, (2007) "*Rogue Nodes Turn Tor Anonymizer Into Eavesdropper's Paradise*" Available from: http://www.wired.com/politics/security/news/2007/09/embassy_hacks?currentPage=1 [Accessed 28 Dec 10]

Wired.com, (2010) "*WikiLeaks Was Launched with Documents Intercepted from Tor*" Available online from: http://www.wired.com/threatlevel/2010/06/wikileaks-documents [Accessed 5 Oct 10]

Wireshark Foundation, (2011) "*Wireshark*" Available from: http://www.wireshark.org/ [Accessed 6 Jan 11]

xrumer, (2011) "*XRumer 7 Elite Is Out!*" Available from: http://www.xrumer7.info/ [Accessed 6 Jan 11]

Zscaler, (2010) *".LNK (CVE-2010-2568) / Stuxnet Incident*" Available online from: http://research.zscaler.com/2010/07/lnk-cve-2010-2568-stuxnet-incident.html [Accessed 1 Nov 10]