Ease of Information Warfare in the Corporate Environment

GIAC Security Essentials Certification (GSEC)
Practical Assignment Version 1.4b – Option 1
Jennifer Fritz
August 8, 2004

1. Abstract

The adoption of the Internet by the public signaled a paradigm shift in the way we live our lives. How many times have you turned to the Internet for directions, news, shopping or communication instead of the phone, newspaper or the mall? We are past the point of no return, but this interconnectivity has come with some harsh consequences. In today's corporate environment, information warfare has become a daily occurrence. Almost every day, there is mention of virus, a defaced website, or source code being stolen. This dramatic increase of information warfare has its foundation in two distinct reasons: technology issues and the human factor.

The objective of this paper is to discuss the definition of information warfare, how it applies to the corporate environment, and the alarming trend of increased attacks. More importantly, it is intended to discuss why this increase has occurred in reference to both technological issues and human factors. The ease of information warfare has increased due to the following technological issues: the consolidation of Internet services, the monopoly of a single operating system and an out-dated concept of patch management. It is not technology alone, but human factors as well, such as: the decreased need of know-how to hack, the rise of the unsophisticated user, and the lack of diligence of corporate upper management. Finally, some solutions will be proposed in hopes of decreasing the impact of information warfare on the corporate environment.

2. Introduction

In order to discuss the increasing ease of information warfare in the corporate environment, it will first have to be defined. In addition to the definition, the increasing number of attacks on corporate networks will be discussed.

2.1. Definition of Information Warfare

Information warfare is “the offensive and defensive use of information and information systems to deny, exploit, corrupt, or destroy, an adversary's information, information-based processes, information systems, and computer-based networks while protecting one's own.”[1]

Traditionally, information warfare is a term used when discussing a conflict between nations and their enemies, whether they are other nations or individual groups such as terrorists. This is no longer case; the definition has broadened to include that of conflicts between corporations and their adversaries, be they disgruntled former employees, market competitors or malicious attackers.

2.2. Increasing number of incidents

The number of vulnerabilities and incidents has dramatically increased in the past couple of years. In 2000, there were a total of 171 vulnerabilities reported. In contrast, in the first half of this year, the number of reported vulnerabilities is 1,740.[2] The number and sophistication of viruses and worms has also increased dramatically in the same time period. These worms have the added intelligence of allowing the attacker complete control of the infected system, erasing security software, as well as creating denial of service (DoS) attacks on security websites, such and Windows Update or McAfee.

Unfortunately, the days of putting up a firewall and calling your network safe are over. There is no such thing as perimeter protection; there are too many avenues to a corporation's data. These avenues include but are not limited to: virtual private networks (VPNs); mobile devices such as PDAs, laptops, or cell phones; third party access and email. These modern conveniences have systematically eroded the concept of a perimeter. There is no longer one or even several ways into the network, but hundreds. This fundamental change combined with the increased number of vulnerabilities, has dramatically increased the number of incidents in the past year alone. According to the CERT 2004 E-Crime Watch Survey, "forty-three percent (43%) of respondents report an increase in e-crimes and intrusions versus the previous year and 70% report at least one e-crime or intrusion was committed against their organization."[3]

3. Technology issues

In today's Internet, there are no physical single points of failure. This is not to say that the Internet is failure-proof, just that "a systemic failure at the packet-switching level is of very low probability."[4] Unfortunately, the consolidation of Internet services such as DNS and advertising and the monopoly of a single operating system have dramatically increased the ease of information warfare. In addition to these factors, the out-dated methods of patch management in the production environment and the lack of patching at home have also increased the impact of information warfare.

3.1. Consolidation of Internet services

The underlying network of the Internet may be distributed, however it is the services such as DNS, advertising, or search engines that are consolidated. "It is these services that create today's Internet."[5] Recently there have been several incidents that have demonstrated how consolidated these services have become. On June 15, 2004, "an outage of some sort at Akamai's distributed DNS service brought down access to some major site from various parts of the world, including Google, Yahoo and Microsoft."[6] Another recent attack happened on July 28, 2004 when malicious hackers used an army of previously infected systems to perform a DOS attack on DoubleClick Inc.'s, an advertising company for hundreds of online commercial sites, effectively disrupting access to some of the Internet's most heavily visited site.[7]

In the past year, there have been worms designed specifically to perform a distributed DOS attacks on targeted websites, including Microsoft's Windows Update and anti-virus websites. Targeting these websites creates a two-fold attack, one it prevents the user from cleansing their system from infection or protecting themselves from future vulnerabilities and two it prevents others from being able to access these websites, thus allowing for the potential of infecting additional systems. This consolidation of services has provided malicious attackers with single targets to disrupt the whole of the online community and thus increasing the ease of information warfare.

3.2. Monopoly of a single operating system

In today's business world there is a near complete monopoly in regards to the operating system on the end user's desktop, Microsoft Windows. "The presence of this single, dominant operating system in the hands of nearly all end users is inherently dangerous."[8] Since almost every network computer will be running a single operating system, once a vulnerability has been discovered it is almost certain that the majority of system will be vulnerable to it. Thus for minimal work, the attacker can affect a maximum number of systems. Cascading failures, those caused by self- propagating worms such as MyDoom, are made possible by this lack of diversification on the desktop.

The problem does not just lie in the fact that most users use Microsoft's operating system, but that "Microsoft's operating systems are notable for their incredible complexity and complexity is the first enemy of security."[9] Software products will have bugs, the more complex the software package the more bugs it will have. Microsoft, in order to protect its monopoly has created an extremely complex operating system as well as integrating many of its applications with the operating system including its browser and Office suite. This integration introduces even more complexity. In addition, fixing a discovered vulnerability becomes extremely difficult due to this integration.

It is not just this near monopoly that has increased the ease of information warfare, but the fact that it is the de facto operating system for the unsophisticated home user. It is these users that are less likely to keep their system's patches up-to-date, use anti-virus protection or spyware removal tools, thus further increasing the likelihood of infection or control of their system's by attackers.

3.3. Patching, not just for corporations any more

> "The exploitation of exposed vulnerabilities is becoming more frequent, widespread, and costly. The sheer number of patches released by vendors, and the costs associated with rolling out even a single patch enterprisewide, has long meant that patching was viewed as a time-consuming and expensive proposition"[10]

One of the greatest benefits of the Internet and the services it provides, such as shopping, news, and email, is that it's available every day of the week at every hour. This availability of services such as Amazon, eBay or CNN has become expected, rather than a luxury. It has become a requirement for today's corporations to provide this constant service if they are to retain a loyal user base and thus stay in business. It is this necessity that drives the current outdated model of patching one's production environment once, maybe twice annually. "As the costs and business interruptions related to security incidents have mounted however, enterprises have increasingly begun looking at patching as a business problem that needs to be solved."[11]

The problems with patching are three-fold. First there have been countless times where a patch promised to solve a problem has either introduced another problem or caused an application to no longer function. It is this fear that has caused many enterprises to delay patching until the patch has been fully tested. Unfortunately, the time between when a vulnerability has been publicly announced and the time that an exploit has been released in the wild has shortened considerably in the past several years. One such exploit, Blaster "arrived just weeks after Microsoft announced the RPC DCOM vulnerability."[12] As one can see this outdated method of patching leaves numerous systems vulnerable to attack.

The second is that many end-users are unaware of the need to patch their computers on a regular basis and therefore there are numerous computers drastically out-of-date that are easy prey for the would-be attacker. The advent of cheaper Internet access and always-on broadband connections has allowed the general populace unprecedented access to the Internet with unintended consequences. It is these systems of non-technical users that are most likely to remain patch free and thus vulnerable to attack. It is not that these users consciously chose not to patch, it is that they are unaware that there is a need to do so. Unfortunately this has left an army of systems that have most likely been compromised and at the disposal of the attacker.

Lastly, there are new devices that have entered the market, most notably mobile devices such as the cell phone, PDA and other handheld devices. "Mobile devices today still largely remain unmanaged and unchecked and thus represent the newest threat to IT within the enterprise."[13] These devices number in the hundreds of millions, all of which could potentially have access to corporate data. To date there has been no patch management solution for these devices, and thus the news on July 20, 2004 of the first virus designed to infect handheld devices powered by Microsoft Windows CE is truly disturbing.[14]

4. Human Factor

Technology issues, while important in increasing the ease of information warfare, are not as nearly as dangerous as the human factor. The first of these is the automation of the majority of hacking tools; special knowledge or ability is no longer needed to exploit the many vulnerabilities in existence. Second, the Internet has become an integral part of society, so much so that non-technical users have become the fastest growing population on it. These users are easy prey for the sophisticated techniques used by attackers. Thirdly, security has been seen as an afterthought in the corporate environment. It is rare to see upper management risk the delay of a product due to security concerns.

4.1. Automation of hacking tools

“Automatic hacking tools with easy point and click interfaces, ready made for script kiddies, cause a lot of damage to organizations and their network.”[15] In the past, attackers had specialized knowledge and most likely understood exactly what the exploit code they were releasing into the wild would accomplish. Unfortunately this is no longer the case, in fact it is more likely that someone besides the person that wrote the exploit code, whether a virus or malware, will release it into the wild. “Professional espionage and criminal elements are seeding the hacking tools to amateurs who create noise to hide the highly targeted attacks by professionals.”[16]

The lifespan of a vulnerability is identical to the lifespan of the product that it is related to due to the fact that it will never be patched on one hundred percent of the systems worldwide. This means that the total number of vulnerabilities increases as time progresses. Herein lies the problem, with the automation of scanning tools; an attacker can continuously scan for said vulnerability as well as others at the same time, thus increasing his or her chances of successfully compromising a networked computer.

“Our modern virus epidemic is thus born of a symbiotic relationship between the people smart enough to write a virus and the people dumb enough – or malicious enough – to spread it.”[17] Chances are one or both of these individuals are living outside of the country that their virus is spreading rapidly. The question becomes how do you prosecute someone who has started a virus in one country and lives in another. This question has yet to be answered, and has further implications when it comes to targeted attacks. This lack of a global legal response to information warfare further increases its ease in today’s society.

4.2. Unsophisticated users

How many times has a virus or worm spread within a corporation because some user has clicked on attachment they received? This is not something that happens occasionally but often within the corporation, no matter how many times an IT department sends out warnings about attachments; reminding users not to open them, even from those you know unless you are expecting it. An important factor in the non-technical user's psyche is that commonly available commercial anti-virus software has given them a false sense of security in that they expect it to catch the virus for them and so they open emails with utter abandon.[18]

Unfortunately, as attacker techniques become more and more sophisticated, the fastest growing population on the Internet is that of the non-technical user. It is these users that are most likely to use the Internet with no thought to security. They use the exact services that are used by attackers to spread their malicious code, such as peer-to-peer networks, instant messaging and email providing easy targets for these attackers. In addition, it is the non-technical users that are most likely to "chose weak passwords and resent having to change them regularly. They share Ids. They forget their smart cards."[19]

"The ability of attackers to rapidly gain control of vast numbers of Internet hosts poses an immense risk to the overall security of the Internet."[20] Unfortunately this is a reality due to the number of unsophisticated users currently connected to the Internet. It is because of these users that attackers control not thousands, but millions of systems that they can use to spread their malicious code. Unfortunately, because of their non-technical nature, it is less likely that they will detect that their system has been compromised thus the reduction in the number of attacker owned systems is unlikely. At present time, the time between a vulnerability announcement and exploit code being able is measured in days. As the number of compromised systems and sophistication of attacker techniques increase, this span will be reduced to hours if not minutes.

4.3. Upper management

Spending money on security is protecting the company against would be malicious acts. Unfortunately, in many cases upper management does not see it this way. They see it as throwing money away towards the off chance that their systems may be compromised. This approach both leads to a reactive approach to security, which is more costly in the long run and deemphasizes security down the chain of command.

Though this model of accepting the risk worked in the past, the increasing number of vulnerabilities due to the complexity of operating systems and applications combined with the increased sophistication of attacker techniques and a decrease of the overall sophistication of the worldwide user base makes this thought process a fallacy in today's Internet. It is not that upper management is against security, far from it, it is the fact that when push comes to shove, delaying a product to patch a vulnerability or harden a system very rarely happens. Information security departments around the world have announced serious vulnerability alerts to their company though whatever process they have and a suggested course of action, only to watch their warning fall on deaf ears.

The belief of upper management that by installing a firewall, email filters and anti-virus software, they will be protected from malicious attacks is another common mistake. "The conceit is that technologies can somehow 'solve' computer security, and the end result becomes an expense and a barrier to business."[21] It is people, more specifically the IT department that is responsible for these technologies; in many cases they lack the training to configure or maintain the products properly.

Lastly, when corporations build products for the world's consumption, such as operating systems or common applications, security is not the first concern of upper management. They are more interested in getting the product out the door with the promised functionality and on time. Security is thought of as an afterthought, and due to the complexity of many products the likelihood that there are vulnerabilities is a given, thus increasing the ease of information warfare.

5. Suggested solutions

The risks of being on the Internet are real and increasing dramatically. "As risky as the Internet is, companies have no choice but to be there….There is no alternative. This more than anything else, is why computer security is so important."[22] So if there is no choice, the next question becomes how can we make the Internet a safer place. The following are several suggestions that could potentially decrease the risk of information warfare in today's online society.

First and foremost, educating the non-technical users on the risks of interconnectivity is a must. One idea would be to require users to have a license to connect. This concept may sound silly, but think about it, if your system is vulnerable to the latest exploits and gets compromised, you are not the only one that will suffer the consequences. Attackers will use your system to spread malicious code, mount distributed denial of service attacks, or worse as a jumping point for targeted attacks. If you were made aware, through a licensing process, of simple security measures such as patching your system regularly, strong passwords, or using anti-virus protection, the likelihood of several million vulnerable computers would decrease.

A second suggestion is to have a global organization responsible for tracking down those that participate in information warfare as well as being in charge of prevention measures. This organization could be part of the United Nations or a separate entity. The responsibilities of this "Cyber-Center for Disease Control"[23] would be three-fold, prevention, worldwide incident response and prosecution of those found guilty. Today, there is no legal recourse for a company if the perpetrator is outside the reach of their countries legal system. This allows attackers great freedoms, as well as the capability of hiring outsiders to perform targeted attacks. By creating a global organization, this would centralize resources to prevent and fight outbreaks, as well as prosecute those responsible.

Lastly, there needs to be financial liability for making vulnerable code as well as not patching systems in a timely matter. "There is no standards for quality or security, and there is no liability for insecure software. Hence, there is no economic incentive to create high quality."[24] A toy company is liable if their product harms children, and yet the harm that is caused by lack of security in software is far greater to a society as a whole. Among other things, financial information, social security numbers, or classified data could be compromised, and yet the fault does not lie on those that have produced the software that has the vulnerability. Unfortunately, even if there is a patch, this is no guarantee that systems will be patched in a timely manner. Liability also has to be assessed on the part of upper management or non-technical users that not do what they can to prevent their systems from being compromised. This will provide the financial consequences necessary to create both more secure products as well as a more secure networking environment.

6. Conclusion

The increasing number of incidents, be they viruses or compromised systems, will not cease until the factors that provide an ease of information warfare are reduced. These factors are both technological and human-related in nature. The technological factors include, but are not limited to, a consolidation of Internet services such as DNS, a monopoly of one operating system, and the lack of patch management in the corporate environment as well as in the home. Human factors far outweigh those of technology though when it comes to this increase of information warfare. These include, the automation and increased sophistication of hacking tools, the drastic increase of non-technical users connecting to the Internet and the lack of enforcement and diligence of upper management when it comes to security policies. If action is not taken to prevent the increase of information warfare, it will become too dangerous to do business on the Internet.

7. Notes

[1] Goldberg, Ivan K, Dr. “Glossary of Information Warfare Terms.” 27 October 2003. URL: http://www.psycom.net/iwar.2.html

[2] ”CERT/CC Statistics 1988-2004: Vulnerabilities reported.” 3 August 2004. URL: http://www.cert.org/stats/cert_stats.html#vulnerabilities

[3] ”2004 E-Crime Watch Survey Shows Significant Increase in Electronic Crimes.” 25 May 2004. URL: http://www.cert.org/about/ecrime.html

[4] Doval, Diego. “((no single == many) && no single != no)) point(s) of failure.” 15 June 2004. URL: http://www.dynamicobjects.com/d2r/archives/002829.html

[5] Ibid

[6] Ibid

[7] United Press International “Hackers go after DoubleClick.” 28 July 2004. The Washington Times. URL: http://washingtontimes.com/upi-breaking/20040728-020846-8483r.htm

[8] Geer, Dan et al. “CyberInsecurity: The Cost of Monopoly – How the Dominance of Microsoft’s Products Pose a Risk to Security.” 24 September 2003. URL: http://www.ccianet.org/papers/cyberinsecurity.pdf, p. 3

[9] Ibid, p. 12

[10] Edall, Gordon and Senf, David. “Patch Management Strategies for Proactive Defense.” IDC Customer Needs and Strategies. January 2004. IDC#30678, Volume 1. Title page

[11] Ibid, p. 1

[12] Beighton, Nigel. “Early Alerting – the key to proactive security.” 30 March 2004. URL : http://www.securitypark.co.uk/pfv.asp?articleid=22297

[13] Drake, Stephen D., Broussard, Frederick W., Kolodgy, Charles J., and Hudson, Sally. “Mobile Patch Management: Addressing Corporate Security Threats Beyond the Firewall.” IDC Technology Assessment. July 2004. IDC# 31530, Volume 1. p. 4

[14] Knight, Will. “Handheld PC virus holds ominous promise.” 20 July 2004. The New Scientist. URL: http://www.newscientist.com/news/news.jsp?id=ns99996181

[15] Schneier, Bruce. “Fixing Network Security by Hacking the Business Climate.” June 2002. URL: http://www.counterpane.com/presentation4.pdf. p. 13

[16] Christiansen, Christian A. and Kolodgy, Charles J. “Security in a World Without Secrets.” IDC Special Study. April 2003. IDC #29235, Volume 1. Title page

[17] “The enemy within (part 2).” 22 February 2004. The Guardian Observer. URL: http://observer.guardian.co.uk/review/story/0,6903,1153305,00.html

[18] Higginbotham, Ian. “Common Sense – the Ultimate AV Tool reviewed…” 2000. URL: http://www.itsecurity.com/papers/norman1.htm

[19] Hinson, Gary. “Human factors in information security.” 22. February 2004. URL: http://www.itsecurity.com/papers/hinson1.htm

[20] Staniford, Stuart, Paxson, Vern, and Weaver, Nicohas. “How to 0wn the Internet in Your Spare Time.” 14 May 2002. URL: http://www.icir.org/vern/papers/cdc-usenix-sec02

[21] Schneier, Bruce. “Fixing Network Security by Hacking the Business Climate.” June 2002. URL: http://www.counterpane.com/presentation4.pdf. p. 8

[22] Ibid, p. 2

[23] Staniford, Stuart, Paxson, Vern, and Weaver, Nicohas. “How to 0wn the Internet in Your Spare Time.” 14 May 2002. URL: http://www.icir.org/vern/papers/cdc-usenix-sec02

[24] Schneier, Bruce. “Fixing Network Security by Hacking the Business Climate.” June 2002. URL: http://www.counterpane.com/presentation4.pdf. p. 7

8. Bibliography

”2004 E-Crime Watch Survey Shows Significant Increase in Electronic Crimes.” 25 May 2004. URL: http://www.cert.org/about/ecrime.html

Beighton, Nigel. “Early Alerting – the key to proactive security.” 30 March 2004. URL : http://www.securitypark.co.uk/pfv.asp?articleid=22297

”CERT/CC Statistics 1988-2004: Vulnerabilities reported.” 3 August 2004. URL: http://www.cert.org/stats/cert_stats.html#vulnerabilities

Christiansen, Christian A. and Kolodgy, Charles J. “Security in a World Without Secrets.” IDC Special Study. April 2003. IDC #29235, Volume 1

Doval, Diego. “((no single == many) && no single != no)) point(s) of failure.” 15 June 2004. URL: http://www.dynamicobjects.com/d2r/archives/002829.html

Drake, Stephen D., Broussard, Frederick W., Kolodgy, Charles J., and Hudson, Sally. “Mobile Patch Management: Addressing Corporate Security Threats Beyond the Firewall.” IDC Technology Assessment. July 2004. IDC# 31530, Volume 1

Edall, Gordon and Senf, David. “Patch Management Strategies for Proactive Defense.” IDC Customer Needs and Strategies. January 2004. IDC#30678, Volume 1

Geer, Dan et al. “CyberInsecurity: The Cost of Monopoly – How the Dominance of Microsoft’s Products Pose a Risk to Security.” 24 September 2003. URL: http://www.ccianet.org/papers/cyberinsecurity.pdf

Goldberg, Ivan K, Dr. “Glossary of Information Warfare Terms.” 27 October 2003. URL: http://www.psycom.net/iwar.2.html

Higginbotham, Ian. “Common Sense – the Ultimate AV Tool reviewed…” 2000. URL: http://www.itsecurity.com/papers/norman1.htm

Hinson, Gary. “Human factors in information security.” 22. February 2004. URL: http://www.itsecurity.com/papers/hinson1.htm

Knight, Will. “Handheld PC virus holds ominous promise.” 20 July 2004. The New Scientist. URL: http://www.newscientist.com/news/news.jsp?id=ns99996181

Schneier, Bruce. “Fixing Network Security by Hacking the Business Climate.” June 2002. URL: http://www.counterpane.com/presentation4.pdf.

Staniford, Stuart, Paxson, Vern, and Weaver, Nicohas. “How to 0wn the Internet in Your Spare Time.” 14 May 2002. URL: http://www.icir.org/vern/papers/cdc-usenix-sec02

“The enemy within (part 2).” 22 February 2004. The Guardian Observer. URL: http://observer.guardian.co.uk/review/story/0,6903,1153305,00.html

United Press International “Hackers go after DoubleClick.” 28 July 2004. The Washington Times. URL: http://washingtontimes.com/upi-breaking/20040728-020846-8483r.htm