Global Information Assurance Certification Paper

The new breed of cracker, verse the next generation of defenses

Andrew Ingle
April 22, 2004

The internet is widely recognized as the tool which facilitated the information age. As with other revolutionary inventions such as the steam engine and the printing press, the impact of the internet will follow a certain pattern: a decade of initial refinement of the invention and commercialized, after which the true social impacts of the invention (which will take decades to unfold), will become clear.[1]

Abstract

The inclusion of the internet in corporate business models has lead to the inclusion of the internet in the business model of organized crime. Professional Hackers are being paid to develop worms for use by these groups or to perform various acts of cyber crime. Tools Security professionals are increasingly facing full time counterparts as opposed to the script kiddiez and crackers of the 90's. This new breed of professional hacker, who is motivated by financial gain as opposed to purely malicious intent, poses new risks for network managers.

[1] For a complete discussion of this theory, please see: Drucker, P.F. (2002) Managing the next Society: New York. Truman Tally Books, St. Martin's Press.

Table of Contents

Introduction

The internet is widely recognized as the tool which facilitated the information age. As with other revolutionary inventions such as the steam engine and the printing press, the impact of the internet will follow a certain pattern: a decade of initial refinement of the invention and commercialized, after which the true social impacts of the invention (which will take decades to unfold), will become clear.[2]

The advent of the internet sparked the information age. To date, we have seen the internet included in corporate business models, including the incorporation of the internet in the business model of organized crime. Hackers are being paid to develop new worms for use by spammers, to perform corporate espionage, and are engaging in extortion/blackmail[3]. Network administrators are increasingly facing this type of activity, opposed to the script kiddiez and crackers of the 90's. This new breed of professional hacker who is motivated by financial gain poses new risks for network managers, particularly for those managers who are tasked with defending the networks of today and tomorrow.

The predominant source of network attacks in 2003 was worm or blended threat base[4]. This trend has continued into 2004 with the on-going competition between the writers of the Gobot and Netsky worms releasing new variants at rates of almost one a day. However, the number of events not related to worm or blended threats has also increased dramatically during the same period. In 2003 as compared to 2002, the rate at which vulnerabilities were reported dropped, but the relative severity of these vulnerabilities increased[5].

Over the past 2 years, we have witnessed a trend in the reduction of the time between the identification of an exploit and the widespread availability of and use of that exploit. The release of the Witty worm only 2 days after the vulnerability in Internet Security Systems Realsecure and BlackIce firewall products is an example of this trend. Continuation of the trend will undoubtedly lead to zero day exploits. In fact, the authors of the Symantec Internet Security Threat Report

---

[2] For a complete discussion of this theory, please see: Drucker, P.F. (2002) Managing the next Society: New York. Truman Tally Books, St. Martin's Press.
[3] Nuttall, Chris. Hackers blackmail internet bookies, (2004, February 23). Financial Times. Retrieved from http://www.equiptechnology.com/newshub/presscuttings/FT-Hackers%20Blackmail%20internet%20bookies%2023.02.04.pdf
[4] Symantec Internet Security Threat Report Volume V. (March 2004). Retrieved from http://enterprisesecurity.symantec.com/content.cfm?articleid=1539&EID=0. page 6.
[5] Ibid. page 4.

release of March 2004, which reports statistics for the second half of 2003, expressed some surprise that a zero-day exploit hadn't already occurred.

This paper will take a brief look at who is perpetrating these computer attacks, and what the most common threat vectors are. Having developed this base, the paper will then examine some of the countermeasures available and explore their effectiveness.

The Threat Arena

Since the early 90's there have been 2 classes of hackers; those with expert knowledge and skills, and those who use tools written by the former or who misuse tools designed for security auditors. More recently, we have witnessed the formation of a new class of hacker, the "professional" hacker. The professional hacker is motivated by profit. To this end, professional hackers have become increasingly organized, sometimes forming links with organized crime gangs or with other professional hackers. The scope of their activities has broadened to include the writing of worms and trojans for use as SPAM relays, various phishing scams using trojaned systems as web servers, extortion, and the theft of trade secrets[6].

The advent of the professional hacker creates an environment in which corporate information officers and network administrators must consider the strong possibility that their organization is being targeted by someone on a full time basis. This has already changed the type of threats that corporations face.

The Symantec Internet Security Threat Report for the second half of 2003 provides us with a snapshot of the current source of threats. In brief:

- 43% of network attacks were worms or blended threat based down from 78% in the same period of 2002[7].

- Of the remaining reports 17% were exploit attempts with the remainder (40%) consisting of reconnaissance to detect potentially vulnerable machines[8].

This represents either a substantial drop in worm activity (35%) or a marked increase in non-worm attacks. During this time period, Symantec reported an increase in the number of systems affected by blended threats while the number of unique threats remained relatively constant[9]. This time period also included

[6] Adam Piore. (2003, December 22), Hacking for Dollars, Newsweek International, Retrieved from http://msnbc.msn.com/Default.aspx?id=3706599&p1=0.
[7] Symantec Internet Security Threat Report Volume V. (March 2004). Retrieved from http://enterprisesecurity.symantec.com/content.cfm?articleid=1539&EID=0. page 6.
[8] Ibid.
[9] Symantec Internet Security Threat Report Volume V. (March 2004). Retrieved from http://enterprisesecurity.symantec.com/content.cfm?articleid=1539&EID=0. page 25.

worms like Blaster. And that during the same period the number of internet based crimes increased dramatically[10]. This suggests that the statistics are describing an increase in non-worm activity.

The threat from "Script Kiddiez" is becoming increasingly severe, as new resources become available for network penetration testing and exploit writing. The speed at which new "push button" exploit tools can be developed and released is increasing. An example of this is the new Metasploit Framework version 2, a tool that can be misused by the black hat community to very quickly produce and package exploit code.

As worm development is now being driven at least in part by organized groups with both knowledge and sizable financial backing, it would seem increasingly likely that we will see a Flash Worm in the wild. The simplified models discussed by Tom Vogt in his paper "Simulating and optimizing worm propagation algorithms" would seem to demonstrate that a Flash Worm is technically possible and not an overly onerous task, although it is likely that many nodes on the internet would fail under the traffic load of the propagation phase, possibly reducing its ability to spread[11].

So why haven't we already seen one? The answer is partly to do with the fact that this type of worm is more complex to write and time consuming to optimize to find the best possible balance between speed and size. This is however secondary to the fact that this type of worm is more suited to deliver a massive DDoS attack, or to destroy/disable a very large number of computers. The traffic caused during the propagation phase of the worm virtually assures that it will be noticed, and action will quickly be taken to curtail its spread. As a result, while a large number of computers may initially be affected, these machines will only be available to the attacker for a relatively short period of time (days at most). This, coupled with the amount of attention that an outbreak of this type would attract not only from the internet community but also from world governments is not something that most organized criminal groups would want. These two factors make the Flash worm inappropriate for the goals of most professional hackers and organized crime.

The propagation algorithms used in worms found in the wild today are adequate for their purposes and do not require further optimization. This is not to say that significant resources have not been put into the development of worms of this type by military, anarchist and terrorist groups, since these are the groups that could most benefit from the ability to shut down or destroy the communications infrastructure of a target country within minutes. In addition, these groups have little or no fear of repercussions.

---

[10] Adam Piore, "Hacking for Dollars", Newsweek International Edition, Dec 22 2003, http://msnbc.msn.com/Default.aspx?id=3706599&p1=0.

[11] Vogt, T. (2003, Sept. 29) Simulating and optimising worm propagation algorithms, Retrieved 2004, April 3 from http://downloads.securityfocus.com/library/WormPropagation.pdf

Instead, professional hackers working with organized crime groups will focus on developing methods to evade detection by current IDS and host based intrusion detection systems like Virus Scanners[12]. The adoption of detection evasion schemes pioneered by virus writers has already begun with worm programmers using packagers to compress and encrypt worms, defense mechanisms to kill the process of firewalls and antivirus software, and measures taken to prevent users from patching their systems. This group is also financially motivated to find and exploit new vulnerabilities, thus making them the most likely to produce a zero day exploit. The Microsoft Internet Explorer ITS zone bypass vulnerability is an excellent example of this as it is technically the first zero day exploit since no patch or work around existed.

Counter Measures looking forward

An often talked about, but under-emphasized, component of the fight to secure the corporate network is user education. The end user is still one of the weakest links in the defenses of most networks as demonstrated by the continued success of email based worms like Beagle and Blackmal. While this user education may improve in the future, user naïveté will continue to be a major weakness for years to come. Surprisingly it maybe hardware venders that capitalize on the market for secure desktop platforms, for example NVidia's new nForce 250Gb chipset includes a hardware accelerated firewall. This firewall ships in a reasonably safe default configuration with all inbound connections blocked but allowing all outbound connections. While this is not the safest solution it is a massive step in the right direction, and turns a default install of any flavor of Windows or Unix/Linux operating system greatly increasing the security of the platform.

Touching on the subject of firewalls, best practices dictate that firewall and router access control lists should be written to restrict both inbound and outbound traffic to only commonly used ports. For example, many office nodes are not operating any local servers that require access from outside the node. In these cases, routers/firewalls bordering this node can be configured to block all inbound connection requests and to allow outbound connections only to specific ports such as 25 (SMTP), 110 (POP3), 995(POP3s), 80(HTTP), and 443(HTTPS) denying all others. Rules for ports 25, 110, and 995 should also be limited to the URL's or IP's of the corporate mail servers. This way, in the event that a worm or exploit does successfully compromise one or more of the local machines, its ability to call home, to transmit pilfered data out, or to accept remote commands is likely to be blocked. This restrictive rule set will also help to deter or at least slow professional hackers as they will have to breach multiple layers of firewalls.

[12] Symantec Internet Security Threat Report Volume V. (March 2004). Retrieved from http://enterprisesecurity.symantec.com/content.cfm?articleid=1539&EID=0. page 27.

Slowing the attacker and forcing them to perform additional network probing will similarly increase the chances of an IDS (Intrusion Detection System) detecting the attack. However, IDS's do not respond automatically. So the speed at which worms transit the internet with low latency high bandwidth connections means that system administrators have a very short period of time to react to the alert raised by their IDS. Similarly, after weeks of preparations, attacks by professional hackers are often very swift leaving even alert administrators only a short period of time to react to the intrusion. The operator must also contend with the large number of false positives that most IDS systems generate. As a result, much like the little boy who cried wolf, the value of the IDS is reduced but the doubt in the minds of the administrative staff as to the validity of an alert. This often leads to situations where the IDS is more useful in forensic investigation after a security breach has been identified, than as a proactive defensive mechanism.

Advanced Counter Measures

The latest generation of IDS systems includes devices such as Q1 Labs, QRadar. These products "learn" normal network behavior over a defined period of time and later use this, combined with a database of historical attack patterns, to detect unauthorized network activity. The expectation is that this learning phase will reduce the number of false positives and the number of errors produced by hand crafting rules. One particular feature worth noting is that QRadar accepts external event feeds from third party vendors' products. This aggregating of data from multiple sensors increases an administrator's ability to "see" the threat status of their entire network from a single interface, thereby improving response times. Since QRadar is a new product (released on March 9th, 2004), there are as of yet no independent reviews of its real-world performance. A further drawback to this technology is the $25,000 price tag for a basic system, thus putting it out of the reach of many small and mid sized companies.

Intrusion Prevention Systems include features to stop or help contain attacks in progress in an automated manor. Features such as rate limiting are used to reduce the impact of unknown threats until such time as an operator can evaluate the threat. This technology should be capable of containing the spread of worms and blended threats, and may also be able to provide some defense against zero day exploits by spotting abnormal traffic.

The remaining counter measures fall into a legal grey zone. None of the attached legal questions have, as of this writing, been tested in court.

The first HoneyPots are a passive means of drawing or redirecting attacks onto safe systems. These systems have several advantages including the capture of hackers' methods, tools, or worm code for later analysis and possible prosecution. Since HoneyPots are completely passive and there should be no legitimate connections to them, any connection is highly suspect. This reduces the number of false positives to near zero.

The HoneyPot is configured to appear as a server running unpatched or otherwise vulnerable services, making it a very tempting target for hackers. Of course most HoneyPots are configured to be less vulnerable than they appear to be requiring the hacker to expend additional resources once the assault has begun. These resources can be additional skills or tools, both of which will also expend time. Every additional minute the attacker spends attacking the HoneyPot give the administrative team one additional minute to analyze and respond to the assault.

There are some legality issues surrounding the deployment of a HoneyPot. Most of these legal issues stem from privacy legislation that restricts the recording of communications. The legality of recording communications to the HoneyPot is fairly clear, and is permissible under Canadian law as long as one party has consented to the recording. This is also true for most States in the United States there are however a few states which require both parties to consent to the recording. The issue becomes less clear under United States law when a hacker who has compromised the box contacts a third party and carries on a conversation[13]. At this point, the HoneyPot is a carrier and neither the intended recipient nor the originator. The rights of the third party must now be taken into account. The Canadian Criminal Code, Part VI Section 184 Subsection 2.c.iii allows for the interception "if the interception is necessary to protect the person's rights or property directly related to providing the service". This would appear to give HoneyPot operators the legal right to intercept all communications to and from the computer as this is both protecting their property and directly related to "offering" the service.

Depending on the use of the HoneyPot, legislation in the United States provides a possible exemption under the federal Service Provider Protection, allowing network security tools to monitor and record network traffic to detect intrusions or unauthorized usage[14]. This exemption is not afforded to HoneyPots being used for research. In any case, best practices strongly recommend that all machines in a network containing HoneyPots present a banner on standard service ports. The banner needs to cover the following points:

- All transmissions to and from this system are monitored maybe recorded
- Any transmission logs or recordings maybe shared with third parties
- Use of the system indicates acceptance of these terms

Most legal issues are resolved by this simple step, as the user has consented to the monitoring and subsequent disclosure of the data waiving their privacy rights. It should be noted that this is still insufficient in dual consent States where the

[13] Spitzner, L. (June 12, 2003). Honeypots: Are They Legal?. Retrieved April 9, 2004 from http://www.securityfocus.com/infocus/1703
[14] Ibid.

hacker is communicating with a third party as only the hacker on the HoneyPot will ever see the banner.

In addition to privacy issues, there is the issue of liability should a compromised HoneyPot be used to successfully attack a third party's computer. Although there is some risk here, as of the time of this writing I have been unable to find any court rulings attributing liability to HoneyPot operators.

At the opposite end of the spectrum is the issue of hacking back, or active counter hacking. For years security practitioners have itched to strike back instead of applying another patch and turning the other cheek. Recently, products such as Enforcer and Simbiot have become available which have the potential to offer exactly this capability. The argument for this capability is that a static defense is insufficient to defeat a determined and knowledgeable attacker, and the strike back features offer a deterrence or threat elimination capability that is otherwise absent.

Currently, worms are still the most common source of attack. Counter attacks against infected machines scanning or attacking protected networks would seem to have the potential to speed the elimination of worms and blended threats. At the same time this could also substantially reduce the virtual army of zombie machines that hackers have been using as platforms for their illegal activities. Obviously this would make the internet a safer place. However, there are a few bumps and twists in the road. The first hurdle that has to be overcome is the legal issue of hacking what is probably a third party's computer. In the case of a worm the owner of the infected system probably doesn't know the system is infected. In the case of a hacker attack, the attack is probably being launched through several intermediate computers scattered through multiple countries. In either case its possible or even likely that the offending system is not in North America, further complicates the issue. Most of the 191 countries that are a member of the United Nations do not have explicit computer crime laws, and only few of those that do, have co-operation agreements between law enforcement. The net effect of this is that a network operator using one of these tools in North America is more likely to be charged with hacking than the individual who initiated the attack. Having said that several defenses have been raised, the most common is self defense. Curtis E.A. Karnow summed up the use of self defense as:

> "…not an impossible thing; expert testimony might help, but because the consequences of guessing wrongly here are so onerous, for example, conviction of a federal felony, the absence of directly relevant case authority should give pause, a long pause."[15]

Using strikeback technologies to control worm outbreaks is the goal of Enforcer, a program designed to neutralize worms on internal networks. There is no legal

[15] Karnow, C. E.A. Launch on Warning: Aggressive Defense of Computer Systems. Retrieved April 2, 2004 from http://www.gcwf.com/gcc/GrayCary-C/News--Arti/Journal/0703_JIL.doc_cvt.htm

issue with using this type of tool on your own equipment as long as proper authorization is granted from management. Surprisingly, counter attacking a worm infected machine out side of your network isn't quite the same legally as counter attacking a hacker. The difference is that a virus has no intent and no desire; as such it falls loosely under the definition of nuisance[16]. Karnow postulates that under United States law the doctoring of nuisance has an attached concept of "self help" whereby:

> "A person affected by a private nuisance, or a person who is especially affected by a public nuisance, may use self-help and abate the nuisance and then sue the malefactor for the costs of the abatement"[17].

This is by no means a certain defense, as proof of good intent and the lack of a suitable alternative must be proved. The use of a computer program with well defined logic and a well designed payload to neutralize the virus without damaging the system, thus minimizing any damage caused, would go a long way to satisfying these requirements.

Canadian laws, on the other hand, take a very dim view of any vigilantism. It is likely that users of software of this type would find themselves facing both civil and criminal charges.

Until there is additional legal clarification of this issue, it is unclear as to how many companies would be willing to place their managers, and IT staff in a position where they could be charged with a Federal crime.

The same lack of cyber security legislation in most of the world may lead to the development of off-shore security firms. These companies operating in countries lacking cyber laws would be free to employ counter attacks and aggressive countermeasures in response to any attack on systems in networks under their protection. Since these companies would not be restrained by local laws they would be unconstrained in their selection of the type of or the amount of "force" applied in the counter attack. While the employment of companies of this type may not be ethical, it would be no less illegal than the current practices of garment companies who subcontract to avoid Canadian and United States labor laws.

Aside from the legality of strike-back tools, there is the question of their effectiveness. Can a tool like this control or eliminate a virus outbreak? Tom Vogt first model of worm propagation suggests that[18]: The worm in this model is not multi threaded, does not use advanced scanning techniques, and uses a random propagation method. In this scenario it takes approximately four hours

---

[16] Ibid.
[17] Karnow, C. E.A. Launch on Warning: Aggressive Defense of Computer Systems. Retrieved April 2, 2004 from http://www.gcwf.com/gcc/GrayCary-C/News--Arti/Journal/0703_JIL.doc_cvt.htm
[18] Vogt, T. (2003, Sept. 29) Simulating and optimizing worm propagation algorithms, Retrieved 2004, April 3 from http://downloads.securityfocus.com/library/WormPropagation.pdf. Page 5

before the worm begins to spread exponentially. Multiplying this by 2.4 (to estimate for the internet) results in 9.6 or 10 hours. It is during these initial hours that the virus is most vulnerable to countermeasures as once the exponential growth phase is entered, the worm will be nearly impossible to stop. In this case, it is entirely possible that the worm could be detected, captured, analyzed, and a countermeasure developed and deployed if an automated push update mechanism was used. However, there would still have to be a very large number of systems running strikeback software, as only infected systems that attacked such a network would be knocked out. If each infected machine infected just one other system prior to being neutralized, the size of the outbreak would at the very least remain stable. As the rate of infection increases and networks hosting strikeback systems come under increasing attack, the number of counter attacks will similarly rise. The amount of bandwidth consumed by the counter attack would be greater than that of the attack, for example because of the need to be careful to not cause unintended data loss. This suggests that the point at which network nodes become saturated will be reached more rapidly, which would in turn smooth out and extend the worms' growth phase. This may give administrators a chance to patch or otherwise protect vulnerable systems.

These new strains of worms will be increasingly intelligent and able to evade detection, will modify their attack vector, and will eventually implement elements of basic artificial intelligence enabling them to learn and share new exploits with others of its kind.[19] Tools such as MetaSploit are also lowering the level of knowledge required to write a worm, and at the same time giving worm developers a framework which can be leveraged to quickly deploy new exploit code.

Summary

The recent incursion of organized crime into the wired economy has begun another revolution in the digital world. This new revolution is quickly swinging the balance of power from the defender to that of the attacker, and while there are new and increasingly sophisticated tools available to defend networks, these tools are also out of the reach of most small and mid sized businesses. Even if the legal issues surrounding active countermeasures are resolved, it is unlikely that they will provide significant deterrence to professional hackers given the motivation, dedication, and resources of some of the organized crime groups. Especially in cases where the network is perceived to be of high value, such as banks. In the event that active defensive measures are deployed they are likely to have the largest impact on small business and home users. Unable to purchase the more advanced tools and lacking the skills sets to administer their systems and network they will be caught in a virtual no mans land.

[19] Strassmann, P. A. (2003, December 1). New Weapons of Information Warfare, Retrieved March 7, 2004 from http://www.computerworld.com/securitytopics/security/story/0,10801,87554,00.html

The inability to track down and prosecute cyber criminals is and will continue to be a major problem for years to come. Increased international co-operation not only between governments and law enforcement agencies but also between corporations is crucial to the long term usability of the internet as a place of business. Over the long term this will hopefully lead to a harmonization of cyber law. In the short term increased co-operation between corporations, possibly through third parties, will enable the identification and blocking of rogue systems and networks.

References

1. Drucker, P.F. (2002) Managing the next Society: New York. Truman Tally Books, St. Martin's Press.

2. Nuttall, Chris. Hackers blackmail internet bookies. Financial Times. Retrieved April 8 2004 from http://www.equiptechnology.com/newshub/presscuttings/FT-Hackers%20Blackmail%20internet%20bookies%2023.02.04.pdf

3. Symantec Internet Security Threat Report (V). Retrieved March 2004, from http://enterprisesecurity.symantec.com/content.cfm?articleid=1539&EID=0. page 6.

4. Piore, A. Hacking for Dollars. Newsweek International. Retrieved December 22, 2003, from http://msnbc.msn.com/Default.aspx?id=3706599&p1=0.

5. Tom Vogt, Simulating and optimizing worm propagation algorithms. Retrieved Sept. 29 2003, fromhttp://downloads.securityfocus.com/library/WormPropagation.pdf

6. Spitzner, L. (June 12, 2003). HoneyPots: Are They Legal? Retrieved April 9, 2004 from http://www.securityfocus.com/infocus/1703

7. Karnow, C. E.A.. Launch on Warning: Aggressive Defense of Computer Systems. Retrieved April 2, 2004, from http://www.gcwf.com/gcc/GrayCary-C/News--Arti/Journal/0703_JIL.doc_cvt.htm

8. Strassmann, P. A. (2003, December 1). New Weapons of Information Warfare. Retrieved March 7, 2004 from http://www.computerworld.com securitytopics/security/story/0,10801,87554,00.html

9. Gaudin, S. (2004, April 1). Study: Virus Attacks Up But Infections Hold Steady. Retrieved April 3 2004 from http://www.internetnews.com/article.php/3334481

10. Holdaway, E. J. (2001, April 1). Active Computer Network Defense: An Assessment. Retrieved March 20 2004 from http://www.iwar.org.uk/iwar/resources/usaf/maxwell/students/2001/01-055.pdf

11. Bussiere, D. (2003, November 3). Worms – Their Spread and Mitigation, Network Computing Asia. Retrieved March 3 2003 from http://www.ncasia.com/ViewArt.cfm?Artid=21975&catid=4&subcat=50

12. Chua, L. & Pappalardo, D. (2003, December 15). Denying DDOS [Electronic Version]. Computer World. Retrieved March 23 2004 from http://www.computerworld.com.sg/pcwsg.nsf/unidlookup/A75CBB9804F0DC1A48256DFA00175F48?OpenDocument

13. Richmond, R. (2004, March 22). PC Worm's Attack on Security Software Sparks Extra Worry. Dow Jones Newswires. 201-938-5670. Retrieved April 5, 2004 from http://news.morningstar.com/news/DJ/M03/D22/200403221913DOWJONESDJONLINE001014.html

14. McCullagh, D. (2003, June 13). Senator OK with zapping pirates' PCs. CNET News.com. Retrieved March 23 2004, from http://news.com.com/2100-1028_3-1018845.html

15. Loomis, C. (2001, November 28). Appropriate Response: More Questions Than Answers. Retrieved, March 10, 2004 from http://www.securityfocus.com/infocus/1516

16. Evers, J. (2004, FEBRUARY 13). Secret Windows code leaked on Internet. ComputerWorld. Retrieved April 9, 2004 from http://www.computerworld.com/softwaretopics/os/story/0,10801,90200,00.html

17. Leyden, J. (2004, April 5). Extortionists take out UK gambling site. The Register. Retrieved April 6, 2004 from http://www.theregister.co.uk/2004/04/05/sporting_options_ddosed/