Malware Threats and Mitigation Strategies

US-CERT

Informational Whitepaper

May 16, 2005

Produced by:
Multi-State Information Sharing and Analysis Center and
United States Computer Emergency Readiness Team

Current Malware Threats and Mitigation Strategies

OVERVIEW

The nature of malicious code, or malware, (e.g., viruses, worms, bots) shifted recently from disrupting service to actively seeking financial gain. In the past, worms were designed primarily to propagate. The impact on victims and organizations was primarily a disruption of service resulting in loss of productivity and sometimes a loss in revenue. Now, many of the significant worms are designed to steal sensitive information such as credit card numbers, social security numbers, pin codes, and passwords and send the information to the attacker for nefarious purposes including identity theft.

Unfortunately, attackers have become very adept at circumventing traditional defenses such as anti-virus software and firewalls. Even encrypted web transactions may not protect sensitive information if the user's computer has been infected.

Botnets are often the focal point for collecting the confidential information, launching Denial of Service attacks and distributing SPAM. A ***bot,*** short for *ro**bot**,* is an automated software program that can execute certain commands. A ***botnet,*** short for *ro**bot net**work**,* is an aggregation of computers compromised by bots that are connected to a central "controller." Botnet controllers are often controlled from chat rooms and can be linked together to form even larger botnets. Botnets controlling tens of thousands of compromised hosts are common.

Because malware writers are circumventing the basic security controls many organizations have implemented, the community needs to increase user awareness regarding cyber security issues in order to minimize the opportunity for sensitive information from "leaking out" of an organization. If a system is compromised, organizations need to improve the ability to minimize their damage. The purpose of this paper is to inform organizations of this rapidly growing problem and provide best-practice defense tactics.

WHAT SYSTEMS ARE AFFECTED?

The current primary targets are Windows 98/ME/XP/2000/2003 systems. Unix, Linux and Mac systems are still vulnerable, but at the present time are not as highly targeted.

WHAT IS THE RISK?

Because the detection of these threats is difficult and the data that they may send out of the internal network may be sensitive, the risk to governments, businesses, and home users is *high*.

WHAT IS BEHIND THESE NEW THREATS?

In the past, the intent of malware authors was to disrupt service, advertise political statements, for "fun" or for "bragging rights" among their peers. In most cases, these attacks resulted in disruptions of services, embarrassments for the victims and many hours of lost productivity.

However, the intent behind recent malicious code attacks has shifted with the focus on invasion of privacy, financial gain and identity theft using spam, phishing attacks, spyware, adware, rootkits and keystroke loggers to capture passwords, credit card and social security numbers as well as other proprietary and sensitive information. The new forms of malware conceal themselves in order to hide their existence from personal firewalls, anti-virus programs, anti-spyware software and the operating system (OS) itself.

WON'T ANTI-VIRUS SOFTWARE PROTECT ME?

Botnet worm infections can occur *even when the impacted organization has the very latest anti-virus (AV) signatures and is automatically pushing out OS and application patches*. The MS ISAC

received three reports in the past six months where major system infections were caused by a newly discovered worm variant that was undetectable by current anti-virus signatures.

Attackers take advantage of "windows of opportunities" between vendor creation and organization implementation of the following:

- Vulnerability alerts
- Operating system and application software patches
- Anti-virus signatures
- Intrusion detection signatures

Applying vendor patches and implementing newly released signatures as soon as possible are essential to lowering the risk to your organization.

Because today's malware uses multiple vectors to spread including infecting file shares and brute-forcing weak passwords, organizations need to implement comprehensive information security policies and procedures that address all areas of potential compromise and vectors of attack.

WILL A FIREWALL PROTECT ME?

An enterprise firewall between your internal network and the Internet provides one layer of protection for the internal computers. However, not all threats come through the "front door" of your organization's network and through that firewall. Employee and consultant laptops that have been connected to public or home networks can become infected with malware. Once these users connect their computers, physically or through VPN connections, to your organization's internal network they have effectively circumvented the Internet-facing firewall.

Other possible "backdoors" that may allow worms to infect computers inside an Internet-facing firewall include users reading and downloading attachments from personal, external web-based email, employees using Instant Messaging (IM) or Internet Relay Chat (IRC) and users visiting web sites with malicious code.

Phishing schemes (a combination of social engineering and HTML hyperlink trickery), spyware/adware, and DNS (Domain Name Service) cache poisoning can be used to trick users into visiting malicious web sites unintentionally. Upon visiting one of these web sites, the user's web browser could automatically download or run malicious code, infecting the host computer and possibly other systems on the internal network.

WILL AN INTRUSION DETECTION/Prevention SYSTEM HELP ME?

Yes. AnIDS (OR Intrusion Prevention System (IPS)) should be deployed on the network in an effort to find network attacks, to analyze and correlate these anomalies, and to react as needed. The use of IDS/IPS devices can help to answer the following questions:

- Is the organization under attack?
- What IP/network is the source?
- What IP/network is the target?
- Which attack, if known, is being executed?

In a sense, an Intrusion Detection/Prevention System provides an ability to see the traffic coming and going across the network wires. Although an IDS/IPS is only as effective as the signatures it

uses to detect intrusions, the network placement of the IDS/IPS sensors, and the analyst examining the IDS/IPS alerts, it is still a necessary and corroborative network device to add to an organization's defense in depth strategy.

HOW HARD IS IT TO FIND ACTIVE MALCODE AND THE REMOTE COMPUTER CONTROLLING IT?

Today's malware uses multiple methods to hide and disguise itself making identification and eradication extremely difficult. From hiding processes from the Operating System to using encrypted network traffic over common out-bound network ports (e.g. HTTP, DNS, FTP), malware coders are building their software smarter and more stealthy with each new version.

Some worms attempt to disable or corrupt anti-virus and personal firewall software so that when a new vendor signature file is pushed out, it may fail to detect and clean the malware.

Infected computers may attempt to join a botnet using IRC or web-based protocols to get instructions from the controlling server(s) of that network. These directions can include installing hidden key-logging software, performing covert network scans, performing a DoS (denial of service) attack, or participating in a DDoS (distributed denial of service) attack, and installing other malicious code onto that computer that may act as a "middle-man" hiding evidence of the compromise from AV scanners, firewalls and even experienced administrators.

Worms may hide outgoing communications to its controlling computer by using random or nonstandard outbound ports for service protocols such as: IRC, FTP (File Transfer Protocol) and TFTP (Trivial File Transfer Protocol). It is not sufficient for an organization to block IRC traffic by only blocking ports 6666/TCP and 6667/TCP (the well-known ports for IRC). In fact, some recent variants have begun using port 80/TCP, which is the same port used for browsing web sites. Selecting a port used for normal business, combined with the trend for worms to encrypt their communications, makes it even more difficult for administrators to identify network traffic as malicious.

Botnets typically contact a controller via its domain name (e.g., controller.no-ip.info). These network names are usually registered through a DDNS (Dynamic Domain Name System) service, making it difficult to trace the attacker. In responding to an infection, it is not sufficient to block the IP address of the bot-controlling server since the infected system(s) are trying to access the controller via its domain name (e.g. controller.no-ip.info). When a botnet controller is discovered and taken off-line, the attacker attaches a different IP address to the controlling domain name. Therefore, the bots previously attached to discovered controller can establish a connection to the new controlling host. In most cases, the controlling computers are machines that were previously compromised by the attacker.

WHAT CAN I DO?

Protecting your organization from these growing threats can be difficult and requires multiple layers of defenses, otherwise known as defense in depth. As every organization is different, this strategy should therefore be based on a balance between protection, capability, cost, performance, and operational considerations. Defense in depth for most organizations should at least consider the following two areas: (1) protecting the enclave boundaries and (2) protecting the computing environment.

Enclave Boundary

The enclave boundary is the point at which the organization's network interacts with the Internet. For the purpose of this article, the focus will center on firewall and intrusion detection/prevention systems usage.

1. ***Firewalls***

   The main purpose of a firewall is access control. By limiting inbound (from the Internet to the internal network) and outbound communications (from the internal network to the Internet), various attack vectors can be reduced. Acceptable inbound communication types for the organization need to be explicitly defined in the firewall policies. As the firewall is usually one of the first lines of defense, access to the firewall device itself needs to be strictly controlled.

   Conversely, the firewall also needs to be configured for authorized outbound network traffic. In the case of a compromised host inside the network, outbound or egress filtering can contain that system and prevent it from communicating outbound to their controller – as in the case with bot-nets. Often times, firewalls default to allowing any outbound traffic, therefore, organizations may need to explicitly define the acceptable outbound communication policies for their networks.

   In most cases the acceptable outbound connections would include:

   - SMTP to any address from only your SMTP mail gateway(s);
   - DNS to any address from an internal DNS server to resolve external host names;
   - HTTP and HTTPS from an internal proxy server for users to browse web sites;
   - NTP to specific time server addresses from an internal time server(s);
   - Any ports required by AV, spam filtering, web filtering or patch management software to only the appropriate vendor address(es) to pull down updates; and
   - Anything else where the business case is documented and signed off by appropriate management.

2. ***Intrusion Detection Systems***

   The goal of an IDS (intrusion detection system) is to identify network traffic in near real time. Most IDSs use signatures to detect port scans, malware, and other abnormal network communications. The ideal placement of an IDS is external to the organization as well as internally, just behind the firewall. This way, an organization will have visibility to the traffic approaching the organization as well as the traffic that successfully passed through the firewall. Conversely, there will be visibility on internal traffic trying to communicate external to the network – particularly useful for situations where malicious activity originates from inside the firewall.

Computing Environment

Defending computing hardware and software from attack may be the first line of defense against the malicious insider — or it may be the last line of defense against the outsider who penetrates the enclave boundary defenses. In either case, defending the computing environment is necessary to establish an adequate information assurance posture.[1]

[1] Information Assurance Technical Framework – Chapter 7. http://www.iatf.net/framework_docs/version-3_1/docfile.cfm?chapter=ch07

1. ***Authorized Local Network Devices***
   Ensure that the only devices connected to the organization's network are those items provided by the organization. USB thumb-drives, MP3 players, personal or consultant laptops may be a threat to your environment, therefore if an exception is required by business case, the owner should ensure the device is free of malware before being allowed to connect to the network.

2. ***Operating System Patching/Updating***
   Organizations should have a documented patching policy as well as a systematic, accountable, and documented set of processes and procedures for handling patches. The patching policy should specify what techniques an organization will use to monitor vendor sites for new patches and vulnerabilities and which personnel will be responsible for monitoring, retrieving and implementing those patches. It should also include a methodology for testing and safely installing patches.[2] Pay particular attention to vendor reboot requirements as part of the patch process. Failure to execute this requirement can leave your systems vulnerable.

3. ***Operating System Hardening***
   Operating systems should be hardened to improve the ability to withstand attacks. Various hardening scripts and checklists are available from NIST (National Institute of Standards and Technology), NSA (National Security Agency), and CIS (Center for Information Security).

4. ***Anti-Virus Updating***
   New viruses are discovered everyday. It is therefore recommended to set anti-virus applications to automatically update signature files and scan engines whenever the vendor publishes updates. Mobile and remote users should be required to connect at least weekly and if possible daily to obtain updated signatures. The organization should monitor anti-virus console logs to correct any systems that failed to be updated.

5. ***Change Control Process***
   Implement a change control process to document and review firewall and other network changes before they are implemented.

6. ***Host-based Firewall***
   Consider implementing host-based firewalls running on each internal computer and especially laptops assigned to mobile users. Aside from the primary firewall functionality, many host-based firewalls have application hashing capabilities. This is helpful to identify applications that may have been trojanized after initial installation. It is also useful to validate whether an application has been legitimately updated or modified.

7. ***Vulnerability Scanning***
   Routine vulnerability scanning is a valuable practice for every organization. Host scanning mimics the malicious network activity that networked hosts may encounter. Consequently, scan results can indicate which hosts are vulnerable to various types of attacks. These devices should be targeted by system administrators for immediate patching and remediation.

[2] NIST SP 800-40 (Handling Security Patches). http://csrc.nist.gov/publications/nistpubs/800-40/sp800-40.pdf

8. Use Of Proxy Servers and Web Content Filters

Implement outbound application layer proxy servers and web content filters to prevent users from inadvertently being directed to malicious web sites. This includes an outbound web proxy server that is the only computer allowed by the firewall to connect outbound using HTTP and HTTPS. If any of your systems become infected, the combination of proxy servers and firewall egress filtering will help contain the infection and hinder it from connecting to a host outside of your organization.

9. Email Attachment Filtering

Filter the following attachment types at your email gateway unless required for business use: .ade .cmd .eml .ins .mdb .mst .reg .url .wsf .adp .com .exe .isp .mde .pcd .scr .vb .wsh .bas .cpl .hlp .js .msc .pif .sct .vbe .bat .crt .hta .jse .msi .pl .scx .vbs .chm .dll .inf .lnk .msp .pot .shs .wsc. This list continues to grow. Organizations should consider only allowing file extensions with a documented business case and filtering all others.

10. Monitor Logs

Administrators should not rely solely on AV software and email filtering to detect worm infections. Logs from firewalls, intrusion detection and prevention sensors, DNS servers and proxy server logs should be monitored on a daily basis for signs of worm infections including but not limited to:

- Outbound SMTP connection attempts from anything other than your SMTP mail gateways
- Excessive or unusual scanning on TCP and UDP ports 135-139 and 445 Outbound connection attempts on IRC or any other ports that are unusual for your environment
- Excessive attempts from internal systems to access non-business web sites
- Excessive traffic from individual or a group of internal systems
- Excessive DNS queries from internal systems to the same host name and for known "non-existent" host names

Using a centralized means such as a syslog host to collect logs from various devices and systems can help in the analysis of the information.

WHAT IF I AM COMPROMISED?

The notion of becoming compromised is not really a question of "if"; but more a question of "when." No one system or network is completely impenetrable, so it is extremely important to have sound incident response procedures in place so that when the inevitable happens, all parties involved know how to handle the situation.

The manner in which an organization handles an incident will be highly tailored to that organization. Procedures should be based on the incident response policy inside the SOPs (Standard Operating Procedures) of that organization. An SOP delineates the specific technical processes, techniques, checklists, and forms used by the incident response team and the organization as a whole. SOPs should be comprehensive and detailed to ensure that the priorities of the organization are reflected in response operations. In addition, following these standardized responses should minimize errors, particularly those that might be caused by the increased tempo and stress occurring while responding to an incident. Finally, SOPs should be tested to validate their accuracy and usefulness, and then distributed to all team members.[3]

[3] NIST SP 800-61 (Computer Security Incident Handling Guide). http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf

If you don't have an SOP below are some recommended, although not exclusive, steps you may want to consider incorporating into an SOP to minimize sensitive information from being exposed. Note that taking appropriate action quickly is essential.

1. If only a few systems are infected, physically disconnect them from your internal network immediately to contain the infection and prevent infected systems from connecting to the Internet.
2. If step #1 can not be accomplished in a timely manner or more than a few systems are infected and you have not implemented strong firewall egress filtering and proxy servers, immediately block *ALL* outbound traffic to external networks.
3. Implement filters on internal routers, firewalls and other networking equipment as appropriate to isolate infected segments and to monitor network traffic to ensure internal containment or identify how this infection is spreading and which hosts are infected. Monitor all network traffic in order to address possible multifaceted attacks.
4. Review appropriate log files to attempt to identify the first system infected and what the attack vector was if possible.
5. It is vital to determine if any of the infected systems successfully connected to any site on the Internet and what information, if any, was exposed.
6. Conduct a forensic examination of the system identified in step 4 to determine the extent of the compromise and remediation steps. Note that it is important not to trust any software and utilities that already exist on this system since they may also have been compromised or subverted. The examination should be conducted by loading fresh copies of the utilities, running them from good copies on write-protected, removable media or booting from good, write-protected media containing the utilities.
7. If the results of the forensic exam indicate a rootkit was installed, we then recommend for each infected system:
    a) Ensure any needed data is backed up.
    b) Reformat the hard drive.
    c) Rebuild the system.
    d) Ensure all security patches are applied.
    e) Ensure the most current AV signatures are applied.
    f) Restore the system to the network.
    g) Change local administration passwords and the passwords for any user of the infected system.
    h) Change any network share passwords for users of the infected system.
    i) Notify your information security team.
8. If the results of the forensic exam indicate a worm infection, we then recommend for each infected system:
    a) Apply the appropriate security patches to the system.
    b) Clean the infected machine using AV signatures that are verified to detect this variant.
    c) Change local administration passwords and the passwords for any user of the infected system.
    d) Change any network share passwords for users of the infected system.
    e) Restore the system to the network.
    f) Notify your information security team.
9. Once all the systems are cleaned, closely monitor for re-infection for the next week.
10. If identifying personal information has been compromised, the individual(s) should be notified.

11. When deemed appropriate, the information security team should recommend to management that law enforcement officials be contacted.

SUM IT UP FOR ME.

While some malware writers are becoming more skillful in the code they are developing, there are protections that organizations can deploy prior to an infection to mitigate this threat. Organizations that develop, deploy, monitor, and test security tools throughout their network and information security policies that govern these devices, will be better able to avoid compromises and, in the event they do get infected, a faster recovery.

***REFERENCES*:**

NIST: Guidelines on Firewalls and Firewall Policy
http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf

NIST: Computer Security Incident Handling Guide
http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf

SANS: Bots and Botnet: An Overview
http://www.sans.org/rr/whitepapers/malicious/1299.php

IATF: Information Assurance Technical Framework Manual
http://www.iatf.net/framework_docs/version-3_1/zipfile.cfm?chapter=version-3_1

SANS: Incident handler's diary on DNS cache poisoning
http://www.incidents.org/diary.php?date=2005-03-04
http://www.incidents.org/diary.php?date=2005-03-07
http://www.incidents.org/diary.php?date=2005-03-11
http://www.incidents.org/diary.php?date=2005-03-13

TechWeb: Botnet Definition
http://www.techweb.com/encyclopedia/defineterm.jhtml?term=botnet

Microsoft: Help: I Got Hacked. Now What Do I Do?
http://www.microsoft.com/technet/community/columns/secmgmt/sm0504.mspx

CERT®: Home Computer Security Information
http://www.cert.org/homeusers/HomeComputerSecurity/

HoneyNet Project: Tracking Botnets
http://www.honeynet.org/papers/bots/

ComputerWorld: The State of Malware Today – And Tomorrow
http://www.itnetcentral.com/computerworld/article.asp?id=14319&leveli=0&info=Computerworld

TechWeb: Botnet Definition
http://www.techweb.com/encyclopedia/defineterm.jhtml?term=botnet

SANS: Bots and Botnet: An Overview
http://www.sans.org/rr/whitepapers/malicious/1299.php

Published by:
MS-ISAC
30 South Pearl Street, Suite P2
Albany, NY 12207
(518) 474-0865
7x24 CSAC 1-866-787-4722

US-CERT
Department of Homeland Security
Mail Stop 8500
245 Murray Lane, SW, Building 410
Washington, DC 20528
1-888-282-0870