CTO Roundtable: Malware Defense Overview

The Internet has enabled malware to progress to a much broader distribution model and is experiencing a huge explosion of individual threats. There are automated tools that find vulnerable sites, attack them, and turn them into distribution sites. As commerce and the business of daily living migrate online, attacks to leverage information assets for ill-gotten benefit have increased dramatically. Security professionals are seeing more sophisticated and innovative profit models on par with business models seen in the legitimate world.

Often a machine's infection signature is unique and completely different from any other, making effective defense all the more difficult to achieve. Some studies have shown that 12 percent of all PCs on the Internet are malware infected, while the infection rate of the consumer-facing PC sector is closer to 25 percent. This difference reflects successful security efforts by IT professionals to secure the nonconsumer PC sector and shows that there are mechanisms to reduce overall infection risk. Though not intended to replace the in-depth discussion of malware defense by the ACM CTO Roundtable, the following overview should help readers understand the basic scope of the threats in play today and provide a framework to address them and minimize the overall risk of compromise.

—*Mache Creeger*

Many types of malware and payloads exist, but two types in particular cause concern in the consumer and enterprise space. Both capture personal information; some are opportunistic in nature, do not target any specific individual, and are designed to go after anyone who happens to be ensnared, while others focus on specific “high-value” targets. By far the majority of common security issues for end users are the former, and these types of threats typically try to make money by stealing information or resources from the end-user machine. Standard practices such as patching, an up-to-date security suite, and strong passwords go a long way toward protecting against these threats.

As in any other business, attackers attempt to extract the highest value available from the computers they compromise. As the supply of raw Social Security numbers or credit card numbers increases, the demand drops and those assets become less valuable on the open criminal market. Refining stolen assets from their raw, low-value state to high-value, specialized content is a growing trend requiring a great deal of additional context. A full set of medical information for a specific individual is an example of high-value, specialized content.

While security awareness is becoming more of a background issue, paradoxically the actual threat space is increasing. A common perception is that malware is not a problem because end users do not see direct evidence of its effects. Malware writers have learned that if they minimize direct impact to computing platforms so the effects of an attack are not directly visible to the user, then they can extract maximum value from compromised machines over a longer period of time.

OBVIOUS SECURITY RISKS

- Running older and unsupported operating systems such as Windows 2000, Windows 98, and Windows 95 poses a very high risk for infection.
- A common misperception is that the operating system and a single AV (antivirus) product fully

address PC security. Most people are also ill informed about the status of their patch level and AV effectiveness (is it installed correctly and is its subscription current?). Moreover, there is fake AV malware that tricks you into thinking you are installing a real AV product and are protected when you are not.

INFECTION AVOIDANCE PRACTICES THAT ARE NO LONGER VALID

- Avoiding dodgy Web sites such as pornography or file-sharing (warez) sites was once a good approach to keep you safe from malware infection. Because of the rise of XSS (cross-site scripting) attacks that inject malicious code into otherwise normal Web pages, however, infection can just as easily occur from respectable Web sites.
- Downloading and executing unsigned software from a reputable Web site used to be reasonably safe. Today that practice carries significant risk, as you have no way of guaranteeing that the software has not been tampered with on the server. Ad hoc experiments have shown that unsigned applications from well-known server sites carry a risk of infection. Moreover, you should accept signatures only from organizations that you trust.

A BASIC HYGIENE SET OF SECURITY PRACTICES

- Protect your passwords and keep different passwords for different sites.
- Keep your PC safe by running a modern operating system and keeping up with its patch releases.
- Run a current client-based security suite (antivirus, firewall, intrusion prevention,...) with the latest updates and patches.
- Don't enable file shares in directories that are going to attract malicious code.
- Avoid downloading and executing unsigned executables, and accept signatures only from organizations you trust.
- Pay attention to Web-site validation cues such as the extended validation icon that appears on the PayPal site.
- Avoid dubious Web sites, such as pornography or pirated software (warez).
- Don't fall for those pesky phishing e-mails. Generally don't follow login links from e-mails.

ENTERPRISE SECURITY

Small to mid-market companies typically spend less than one hour per month on security and do not perceive it to be a priority. Businesses with fewer than 50 employees usually work with a single-stop, local IT provider; those with more than 250 employees have many viable alternatives for security services; but those in the 50- to 250-employee range have very limited security options from IT providers.

Small business-owned Web sites are increasingly being compromised and used to attack Web-site visitors, making it not just the desktop owner's problem but also the Web-site owner's. Because small businesses usually have no idea what Web-site security entails, fixing this problem is a major challenge. Some hosting companies will do security scans as a service for Web sites run by small business, but these products face significant challenges and most likely will not be comprehensive.

Security investments should be governed by the business you are in and the impact of having a breach. If you handle valuable user information such as Social Security numbers, bank information, medical records, gaming information—anything of value on the open criminal market—you should

address those security issues immediately.

In protecting against the loss of valuable enterprise assets, it is important to remember that you are defending against a highly adaptable and dynamic adversary. This makes assessing risk very difficult. When one hole is plugged, attackers can move to new areas. You are trying to plug as many leaks as you can with a fixed budget, and there's no real guarantee that what you leave out isn't the critical item that will cause major damage.

A security policy has many fragmented and specialized pieces and does not lend itself to a single comprehensive approach. For the home you should implement what most client-side security suites already have: antivirus, firewall, and intrusion prevention. For stricter enterprise security, determining the level of risk you are willing to take and the amount of time and money you are willing to spend to minimize that risk is really hard to do. You need to do a risk/reward security analysis to determine which holes are really worth plugging.

Security is very different from other more predictable areas of computing. In the technology world people tend to look for definitive fixes to problems. Security and malware, however, are more like influenza, where every year there's another strain no matter what you do, and you can never implement a fully comprehensive solution to resolve the problem definitively.

CLOUD COMPUTING AND SECURITY

Commodity-based clouds will provide an inexpensive and available platform with a base level of security. For more security, you will either go to a more specialized public vendor or build a private cloud on your own.

Check SAS 70 certifications when shopping for public cloud vendors. If your industry specifies certain types of security, you will need to ask more specific questions before running your application on a particular public cloud environment.

ATTACK SCENARIOS

- Attacker walks up to a bank ATM, opens up its maintenance port, inserts a USB stick, and loads malware to take it over.
- Attacker disguised as a service representative installs malware on debit-card point-of-sale devices for six to eight local San Francisco Bay area gas stations and captures debit-card financial information.
- In October 2008, people visiting the Macys.com retail site were unknowingly rerouted to a Web site that looked just like Macys.com but wasn't.

EMERGING INTEREST AREAS

- Reputation-based security is an emerging area that began being showcased in products in 2009. Example features might be a vendor assessment of files and Web sites (green, yellow, or red) available to end users. Eventually reputation-based security will evolve into the application control quantifying and enforcing user risk tolerance.
- Researchers are letting machines get infected by malware so they can work out what the malware is being used for, how it's engineered, and what greater purpose it serves.
- A lot of the work being done involves looking at the malware ecosystem and every part of the crime life cycle—not just the technology pieces, but also who benefits.
- In a process called negative externalities, security decisions made by a single computer user

have significant impact on Web sites, ISPs, and other users. By browsing dubious Web sites on unprotected machines and getting infected, that user's browsing behavior has real and measurable costs to those other businesses.

The argument for the greater good of the Internet community is: What are the set of economic and regulatory policies that will motivate users to align their decisions more closely with the cost impact on the rest of the community? It's the same argument that surrounds public health.

LOVE IT, HATE IT? LET US KNOW

feedback@queue.acm.org

© 2010 ACM 1542-7730/10/0200 \$10.00