

Table of Contents

Introduction	3
Taking Root	3
The Damage	4
From Wall Street to Main Street: Why Every CIO Should Care	5
“Stealthology” 101	5
Stuxnet: “A worm in the centrifuge” ⁷	5
Zeus: The godfather of botnets	6
Zeus in action	6
Developing a Strong Offense Against Rootkits	7
Defenses must move beyond the operating system	7

Take the stealth, creativity, and patience of Stuxnet. Add the commercialism, wide distribution, and easy-to-use toolkits of Zeus. Consider that despite more than years of activity, as of May 2011, neither of these cybercriminal teams has been exposed. You now understand the recipe—and potency—of today's malware. Start planning now. It will take more than signatures and operating system-level protections to protect your intellectual property and other assets against criminals wielding these weapons.

Introduction

Stealth is the art of travelling undetected, of being invisible. Stealth technology allows military aircraft, Ninjas, and malware to sneak up on the enemy to launch an attack, gain intelligence, or take over systems and data.

Although stealth techniques are used in sophisticated attacks like Conficker and Operation Aurora, the Stuxnet attack offers a new blueprint—and benchmark—for how committed criminals can use stealth techniques to steal data or target computing systems. Stuxnet innovations included a combination of five zero-day vulnerabilities, three rootkits, and two stolen digital certificates.

Powerful toolkits, like what is available in the Zeus Crimeware Toolkit, make stealth malware development a “point- and-click” endeavor, no longer restricted to the most knowledgeable programmers. While there are no definitive industry figures, McAfee Labs estimates that about 15 percent of malware uses sophisticated stealth techniques to hide and spread malicious threats that can cause significant damage.¹ These attacks form the cornerstone—the “persistent” part—of advanced persistent threats (APTs).

When Stuxnet innovations combine with easy-to-use programming toolkits like Zeus, these complex stealth attacks will occur more often and threaten mainstream enterprise targets. This will be the new reality of crimeware, and enterprises will need to adopt new anti-crimeware that moves beyond the traditional operating system.

Taking Root

Stealth techniques allow malware to lock on to vulnerable endpoints in any industry, agency, or organization. When malware takes root inside a system, attackers can take their pick of data assets, computing resources, or covert hiding spots for reconnaissance. From one compromised, or “pwned”² system, an attacker can move through the network looking for vulnerabilities and data assets.

One of the most important things to understand about stealthy malware like Stuxnet and Zeus is that it truly owns the computers it takes over. Through rootkits that operate at the user, kernel, and firmware levels, malware can hide, replicate, protect itself against being overwritten, and deactivate anti-virus protection and other defenses.³ Because the attacker controls the system, he can also use stealth techniques to limit the risk of exposure. Crimeware can minimize system user impact, mask data movement on a LAN, remove and reinstall itself, update itself via the web, and move from machine to machine and back again. By looking innocent when it enters the computer and then lying dormant, the code waits for the right time to activate, download its payload, and corrupt the system.

Perhaps most devastating, many rootkits can self-heal, reinstalling from a hiding place after a system has been cleaned, extending the compromised system's shelf life for the attacker. As long as IT thinks it has solved the problem, they may ignore future alerts from the system. The attacker can use the compromised system as a long-term safe haven.

The Damage

Organizations invest a great deal of time and money tracking down compromised hosts and recovering from the data losses they cause. Today's best practice remediation for any infection of stealthware is to revert to a known good backup or trusted image. When stealth attack code lies dormant for extended periods, however, a backup you believe is safe may not be trustworthy. The safest recourse may be a complete reinstall from manufacturers' images of the operating environment and applications.

Cleanup is costly. Reimaging can take five hours per machine, derailing both the IT technician and the end user from more productive work. As stealth techniques increase in complexity, these cleanup costs can only increase. Because some malware can reincarnate after a reimage, the most cautious approach in use today is to replace infected computers—a high capital and productivity cost.

Most companies only reveal breaches when regulations require disclosure (typically losses of personally identifiable information), so tangible costs can be difficult to gauge. However, a few numbers indicate trends:

- *Fast spreading*—McAfee Labs has detected up to 6 million new botnet infections in a month
- *Increasing data loss rates*—Malicious attacks were the root cause of 31 percent of the data breaches studied in the *2011 Ponemon Cost of a Data Breach Survey*, the highest percentage in the study's five year history⁴
- *Increasing data breach costs*—The average compromised record costs \$214, and the average data breach costs \$7.2 million⁵
- *Compliance in jeopardy*—About three-quarters of the companies surveyed by Evaluateserve in 2011 said that discovering threats and discovering vulnerabilities were their biggest challenges in risk management⁶
- *Tax on productivity*—Costs average five hours for each IT administrator and user per system reimaged (10 hours total), for an approximate cost per endpoint of \$585; at a 5,000 node company, a 1 percent infection rate would equate to \$30,000 in cleanup costs)

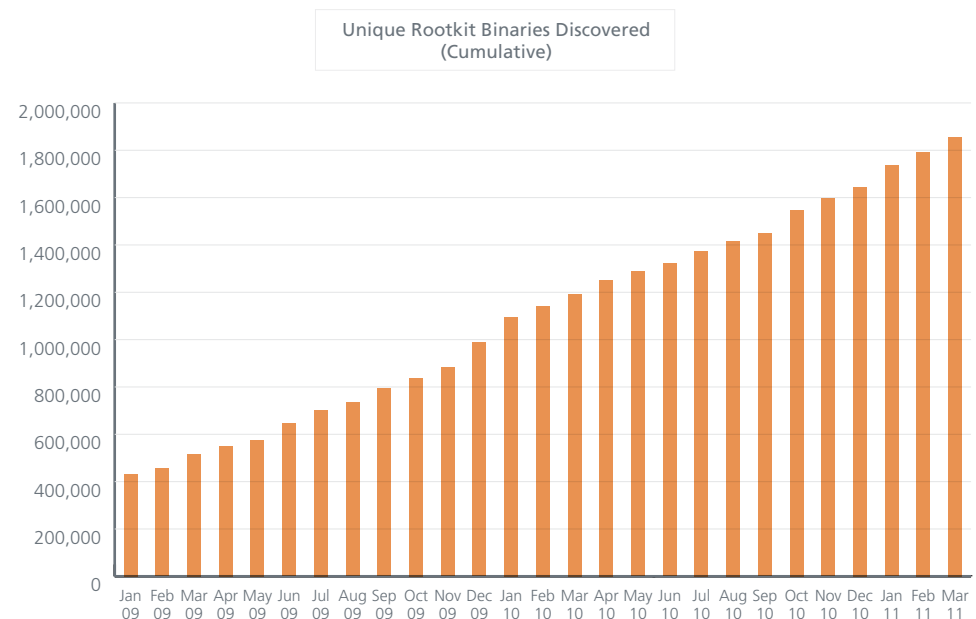


Figure 1: McAfee research has documented steady growth in stealthy rootkit malware, from 42 samples in 2007 to almost 2 million today.

From Wall Street to Main Street: Why Every CIO Should Care

The history of high technology demonstrates that successful techniques migrate from boutique to baseline, from Wall Street to Main Street. Techniques are combined and recombined in endless variations. So if and when Stuxnet and Zeus attack strategies are used together, it won't just be brand names and governments that suffer. A determined hacker may build tools that target any company's crown jewels:

- Credit card data from retailers and transaction processors
- Market launch and promotion campaigns from ad agencies and consumer goods companies
- Employee health records from self-insured companies
- Geographic information mapping (GIS) mapping data for energy exploration companies
- Source code from software development companies
- Product designs from manufacturers

"Stealthology" 101

Professional hackers learn early on to cover their tracks for as long as possible. Rootkits are one of the preferred tools, since rootkits can target any system, from database servers to point-of-sale terminals, from mobile phones to automobile electronics. Because rootkits can operate within and below the operating system, they can disguise or conceal the files, processes, and registry keys touched by other malware. These traits make rootkits a vital component of multistage threat operations.

Let's look at two case studies: Stuxnet and Zeus, which underscore the compelling need for anti-crimeware to move beyond the operating system.

Stuxnet: "A worm in the centrifuge"⁷

The Stuxnet attack appears to have been designed to disrupt industrial control systems within Iranian nuclear programs. Stuxnet used both user- and kernel-mode rootkits, plus a rootkit within the programmable logic controller (PLC)—that had not previously been seen in the wild. The user and kernel-mode rootkits hid files and then decrypted and injected code in running processes. The spring 2010 version of the kernel-mode rootkit included stolen signed device drivers, so that the rootkit would appear to the operating system as legitimate code.

This set of complex malware was teamed with four zero-day Microsoft Windows vulnerabilities to abet distribution and concealment of the payload until it found its target, where the rootkit specific to programmable logic controllers (PLCs) took advantage of a previously unknown Siemens vulnerability.

The rootkit in the PLC came with an extra layer of stealth, a malicious wrapper that insulated the PLC from the control systems that were running a number of centrifuges used to enrich nuclear fuel. The wrapper intercepted calls to the PLC and told the control that all systems were functioning correctly, when, in fact, the malware had reprogrammed the centrifuges to make them useless.

The Stuxnet combination of low-level rootkits and unknown vulnerabilities—plus assorted other enablers—may be the most complex threat security researchers have been able to dissect publicly.⁸

What a botnet does

- Distribute spam (zombies on top 10 botnets send out more than 25,400 spams/day/ zombie; ~ 134 billion/day)
- Initiate distributed denial-of-service (DDoS) attacks against targeted enterprises
- Access files on a compromised network, including source code for new products
- Log keystrokes (keylogging) to discover personal information and steal identities
- Steal legitimate software for resale
- Steal pay-per-click ad dollars

Zeus: The godfather of botnets

Historically, stealth malware has been difficult to write and thus relatively rare. However, commercial crimeware operations like Zeus have changed everything. Where McAfee found 43 rootkit samples in the month of January 2007, we found 133,090 unique samples in July 2010, perhaps only coincidentally when Stuxnet was revealed to the public.

The Zeus organization operates like many a commercial software tool developer. In addition to a formal release process that includes beta testing, Zeus offers its rocket science in a graphical toolkit so straightforward a high school computer class could use it. Franchisees of Zeus can quickly create custom kernel-mode rootkits to build a botnet of “pwned,” or “compromised” hosts.

The cloud phenomenon has come to Zeus as well. The programming-averse can rent or purchase working Zeus botnets to run spam campaigns, execute DDoS attacks, or scout for specific data types, such as proprietary information.



Figure 2: The Zeus/SpyEye toolkit helps malware writers easily create hidden, stealthy malware.

Like drugs, Mrs. Field’s cookie samples, and a test drive of a Tesla electric car, the first Zeus toolkit hit is free. It leaves many wanting more. Would you like virtual network computing (VNC) so that you can control the host remotely and see the screen, mouse clicks, and keystrokes? That’s a \$500 surcharge. With that option, you also get a Firefox injection upgrade, allowing you to add fields to any browser application. Originally, software designed to steal banking credentials, this feature of Zeus means it can be used to capture other valuable data, such as logins for administrative accounts and in-house applications, or social security, credit card, and mobile phone numbers. Zeus is now a tool of first resort for data thieves.^{9,10}

Zeus in action

Zeus usually spreads through compromised websites or email. Criminals will drive traffic to a phishing site (a spoofed website), where a drive-by download will install the Trojan without user action. To zero in on a specific user community, the attacker might plant a custom Zeus Trojan on a genuine, legitimate site. For example, if you were looking to find design blueprints at a car manufacturer, you might install your code at www.carsdesignnews.com, a website claiming to be the leading online resource for automotive design.

Attackers can also embed their Zeus Trojans in email attachments, such as corrupt PDFs. The use of spear phishing emails—personalized through social engineering or social media—will increase as attackers strive to extract specific information or take over vulnerable systems inside specific organizations.

The Zeus toolkit is just one example. In Q4 2010, at least three other low-cost exploit toolkits were available for building botnets using precompiled exploits. The wealth of readily available web-based and server-side toolkits help explain why McAfee Labs detects about 60,000 new pieces of malware every day.

Just recently, the source code of the Zeus Trojan was posted to several underground sites. This release of malware source code creates an opportunity for crimeware developers to build derivative works for their own malicious goals. As any programmer knows, starting with a working program is a great boost to a project. With source code in hand, a savvy developer can modify Zeus to better target specific users or specific data while incorporating more devious stealth tactics. This portends an even greater wave of new (zero-day) exploits to come.

Developing a Strong Offense Against Rootkits

Enterprises have deployed many layers of security tools against traditional hacks and malware. These tools remain important because no malicious technique is ever retired. The black hats' tool arsenal only expands, so the white hats must bolster their arsenal as well.

Rootkits are especially challenging because rootkit developers thoroughly grasp the workings of the operating system, its device drivers, and other software components. Through this deep understanding, they can outwit security software built into most operating systems.

A few of today's security tools work against some of today's rootkits. Tools like virus scanners and host intrusion prevention systems operate at the operating system and above. They can examine memory and monitor user-mode privileges to detect and remediate the relatively high-level, user-mode rootkits. However, stealth techniques that operate at the kernel level and below fly under the radar of traditional operating system, vulnerability, and virus scanning tools. Kernel-mode rootkits have system-level privileges, so they are harder to detect and repair.

Stuxnet and Zeus demonstrate how today's cybercrime is much more sophisticated compared to just a few years ago.

Defenses must move beyond the operating system

Today's criminals know how software works. They know how protective tools work. They increasingly use this knowledge to circumvent security solutions.

With two decades and more of experience playing chess with cybercriminals, McAfee and Intel researchers believe that we need to re-envision how to detect and block stealthy malware. We must apply our knowledge of computers and criminals and step beyond the operating system, using our detective powers and protective tools in new ways. To fend off these rootkit-style threats, enterprise defenses will need to move out of the traditional software operating stack to monitor operations from a new vantage point closer to and integral with the hardware.

We know we need to move quickly. Zeus already reflects mobile use cases. We have uncovered rootkits for Android devices and attacks on this operating system are on the rise. It's only a matter of time before this sort of malware routinely targets the full range of interconnected embedded and mobile devices.

Until recently, most security vendors targeted the software stack, since that is where the threats occurred. As rootkits drop from the user and kernel levels into the boot, hypervisor, and firmware levels, security researchers are working with hardware developers to migrate security lower in the platform.

When the McAfee Embedded Security Program and product plans with WindRiver were announced, McAfee advised organizations to begin looking at establishing trust relationships that allow approved software—and only approved software—to execute or alter code. McAfee and Intel are working now to apply our collective body of knowledge in security, software, and systems to stay ahead of crimeware innovations like stealthy malware even as it moves from personal computers to smartphones to industrial controls and all manner of intelligent devices.

Over the next few years, your enterprise will upgrade and adopt new endpoint devices, building out higher bandwidth networks and extending infrastructure to mobile devices. In order to provide your organization, enterprise, or agency with protection from infections of stealth malware, your choice of security solutions must include products that embed security beyond the operating system. In every layer of security you deploy—from authentication to encryption to inspection to trust—your most effective protection against stealthy malware will take greater advantage of and extend to the platform components. The next generation of security solutions will initiate from the very first compute cycle and provide protection throughout.

Learn more at www.mcafee.com/labs

About the Authors

Dave Marcus currently serves as director of security research and communications for McAfee Labs, focusing on bringing extensive McAfee security research and global threat intelligence to McAfee customers and the greater security community. Mr. Marcus formerly served as senior security evangelist and strategist for McAfee, with more than 10 years of technical experience in information technology security, network performance and integration, and e-learning solutions in addition to management and consulting.

Thom Sawicki is the senior product strategist for the recently established Endpoint Security Software and Services organization within Intel's Software and Services Group, a team that is creating a pipeline of new and innovative products for Intel. Mr. Sawicki was most recently with Intel Labs where he was a senior technology strategist combining strengths in strategy development, market analysis, and technology communications to establish a record of accomplishment in forging the path from research innovation to product development.

About McAfee

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ:INTC), is the world's largest dedicated security technology company. McAfee delivers proactive and proven solutions and services that help secure systems, networks, and mobile devices around the world, allowing users to safely connect to the Internet, browse, and shop the web more securely. Backed by its unrivaled global threat intelligence, McAfee creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. McAfee is relentlessly focused on constantly finding new ways to keep our customers safe. <http://www.mcafee.com>

¹ McAfee Labs

² In online gaming circles, pwning means to conquer; to gain ownership. We use it here to mean taking over control of a host computer.

³ <http://blogs.mcafee.com/mcafee-labs/exploring-stealthmbr-defenses>

⁴ <http://www.ponemon.org/blog/post/cost-of-a-data-breach-climbs-higher>

⁵ Ibid

⁶ Evaluate Risk and Compliance Outlook 2011, sponsored by McAfee

⁷ <http://www.economist.com/node/17147818>

⁸ This paper concentrates on the rootkit facets of Stuxnet. There are many comprehensive analyses of Stuxnet, from *Vanity Fair* to McAfee blogs: <http://blogs.mcafee.com/mcafee-labs/stuxnet-update>.

⁹ *The New Era of Botnets*, McAfee Labs

¹⁰ <http://blogs.mcafee.com/mcafee-labs/the-first-combined-zeusspyeye-toolkit>

