WHITE PAPER: SYMANTEC REPORT ON ATTACK KITS AND MALICIOUS WEBSITES

Symantec Report on Attack Kits and Malicious Websites

Executive Summary

Symantec Report on Attack Kits and Malicious Websites

Executive Summary

Contents

Executive summary

Attack toolkits are bundles of malicious code tools used to facilitate the launch of concerted and widespread attacks on networked computers. Also known as crimeware, these kits are usually composed of prewritten malicious code for exploiting vulnerabilities along with various tools to customize, deploy, and automate widespread attacks, such as command-and-control (C&C) server administration tools. As with a majority of malicious code in the threat landscape, attack kits are typically used to enable the theft of sensitive information or to convert compromised computers into a network of zombie bots (botnet) in order to mount additional attacks. These kits are advertised and sold in the online underground economy—a black market of servers and forums where cybercriminals advertise and trade stolen information and services. Symantec has found that attack kits are significantly advancing the evolution of cybercrime into a self-sustaining, profitable, and increasingly organized economic model worth millions of dollars.

Although rudimentary exploit kits were used in attacks as far back as 1992, Symantec has detected significant growth in the development, sale, and use of highly sophisticated attack kits in the threat landscape in the past few years. While some of these kits have relatively simple capabilities—containing limited exploits that target a specific program or operating system—many kits are considerably more robust and include a number of tools with multiple exploits that target a range of applications across various operating systems.

Symantec has found that the relative simplicity and effectiveness of using attack toolkits has contributed to the upward trends observed in cybercrime and that these kits are being used in a majority of malicious attacks online. For example, one major kit, ZeuS, alone accounted for more than 90,000 unique malicious code variants as of August 2009.[1] This is significant because, at that point, there was an estimated 1,400 ZeuS C&C servers operating and it is likely that attack toolkits such as ZeuS have been responsible for infecting millions of computers.[2]

With the growing ability of these kits to generate profitable attack campaigns, there are regular releases of increasingly robust and sophisticated kits that are yet relatively easy to use. One of the first fully capable kits that helped to launch this trend is the MPack attack kit. When MPack first appeared in May 2007, it represented a new model for kits.[3] Not only did it allow its users to exploit website visitors through Web browser vulnerabilities, but in some cases the kit was also reportedly being sold for $1,000—with the purchase even including a one-year support contract.[4] Thus, not only were attackers profiting from the use of MPack—by using it to install keystroke loggers on computers in order to steal sensitive information, for example—but the creators were also profiting from sales of the kit.

This maturing market is also evident in the service-based secondary economy that has emerged around attack kits. A range of secondary services has evolved to provide additional support and profit-seeking ventures for users of these kits. For example, many of these attack kits are sold on a subscription-based model and attackers can obtain regular updates for the exploits in the kits or purchase additional components to extend the capabilities of the kits. This modular capacity also lets attackers stay current with new exploits for the latest vulnerabilities and attack techniques that can be added to the kit as the threat landscape evolves. Many of these kits also include what amounts to customer support services. Symantec has also observed advertisements offering to help install and set up purchased attack kits for a fee.

1-http://www.symantec.com/connect/blogs/zeus-king-underground-crimeware-toolkits
2-https://zeustracker.abuse.ch/monitor.php
3-http://www.symantec.com/connect/blogs/mpack-packed-full-badness
4-http://www.symantec.com/connect/blogs/mpack-clearance-sale; all currency USD

Earliest attack kits

Of the earliest kits identified by Symantec in the early 1990s, most were limited to creating MS-DOS binary and batch viruses. The Virus Creation Lab (VCL) kit was likely the first such kit released, in 1992, and it only allowed users to create viruses and Trojans.[5]Perhaps one of the most well known attacks produced with one of these early kits was the so-called "Anna Kournikova worm".[6]This worm was created using the Visual Basic Script Worm Generator (VBSWG)—a simple kit that allowed the less technically savvy to create mass-mailing worms written in VBS.

The rise of exploit kits

Vulnerability exploits that allow an attacker to install malicious code onto a victim's computer are the foundation of today's attack kits. These exploits pose a serious threat to organizations and end users because the automated nature of attack toolkits facilitates the attack process so that even novice cybercriminals can successfully mount complex attacks. Attack kits have increased the proliferation of new exploits across the threat landscape and—because most malicious attacks are designed to occur without the victim's knowledge—are a major reason why attempted malicious code infections through the use of malicious websites have dramatically risen over the past several years.

Many current attack kits are available with a range of exploits and a wide array of attack vectors. Increasingly, attack toolkits include exploits for vulnerabilities that encompass multiple applications and technologies. This increases the likelihood that an attack will succeed because there is a greater chance that the victim will be using one of the vulnerable applications and that one of the applications is unpatched.

The exploits used in these attacks predominantly target Web browsers and browser plug-in applications. This is because the Web continues to be the preferred route for malicious attacks. The result is a large number of malicious websites being launched that are designed to facilitate concerted attacks. One reason that attackers have shifted to client-side vulnerabilities (such as those in Web browsers and browser plug-ins) in the past several years is because newer operating system releases have not been including as many network services as in the past, reducing the effectiveness of attacking server-side vulnerabilities. By targeting client-side vulnerabilities, attackers also minimize their attack footprint, thereby increasing their ability to gain surreptitious access to computers located behind firewalls and other network security devices. The automated effectiveness of attack kits used to exploit client-side vulnerabilities may be the primary reason that Web users are at greater risk of being silently infected with malicious code.

ZeuS: king of malicious code kits

Attackers who rely on exploit kits to install malicious code on computers have two main options: they can locate an existing Trojan or bot that incorporates the features they want, or they can use a malicious code kit to generate a unique binary that they can tailor to their needs. ZeuS is the most well known kit that allows attackers to create customized malicious code.

First seen in 2007, ZeuS allows attackers to generate customized Trojans with a higher degree of sophistication than previous kits. Like many other Trojan generators, ZeuS is designed primarily to steal financial details, such as the online banking credentials of a victim. While the cost of ZeuS is steep—early versions were advertised for $4,000 and the recently released ZeuS 2.0 is advertised for as much as $8,000—its ease of use and ability to generate income makes it an appealing purchase for even novice cybercriminals.

5-http://www.textfiles.com/virus/DOCUMENTATION/vcl.txt
6-http://www.symantec.com/security_response/writeup.jsp?docid=2001-021219-1830-99

ZeuS in action

The profitability of malicious code attacks using ZeuS is exemplified by the September 2010 arrests of dozens of people in the United States, the United Kingdom, and Ukraine as part of Operation Trident Breach.[7]This one ring of cybercriminals using a ZeuS botnet allegedly stole over $70 million from online banking and trading accounts over an 18-month period.

Using targeted email attacks and other social engineering ploys, the group allegedly focused on hundreds of small- and medium-sized businesses. Once computers were infected with the Trojan, the attack would then transfer funds from the victims' online bank accounts into accounts operated by money mules. The mules would then transfer the majority of the stolen funds into accounts owners by the attackers, while keeping a portion for themselves. This process also gives the attackers a degree of separation from the actual fund transfer, which could possibly insulate them from prosecution. In some cases, funds from a single account may be transferred through a succession of mules, making the trail to the source more difficult to follow.

Why it matters

While there are other ways to infect computers and steal money without using attack toolkits, these kits allow those with little or no programming knowledge to launch customized attacks using sophisticated pieces of malicious code. This results in a much larger pool of attackers entering the space, which will lead to a higher likelihood of the average user being victimized. A greater number of attackers can lead not only to more malicious code samples in the wild, but also to a greater number of attacks or exploit attempts.

In the past, many cybercriminals also operated alone or in smaller groups. They were also more likely to be computer programmers who used their skills for illegal purposes. However, kits allow those experienced with organized criminal schemes to enter a new market without the need to obtain advanced programming skills or hire those with that skill set. As a result malicious computer programmers can concentrate on creating toolkits and experienced criminals can take advantage of their work, making for a dangerous combination.

7-http://krebsonsecurity.com/tag/operation-trident-breach/

About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

Symantec helps organizations secure and manage their information-driven world with **security management**, **endpoint security**, **messaging security**, and **application security** solutions.

1/2011 21169172