Trend Micro Incorporated
Research Paper
2012

The Crimeware Evolution

Loucif Kharouni

Contents

Introduction

The crimeware landscape continuously evolved, particularly in the past few years. Cybercriminals are spending more time securing their malicious creations and the servers where they are stored to prevent leakage or security researchers from getting hold of them.

ZeuS, Citadel, Ice IX, SpyEye, and the Blackhole Exploit Kit—some of the most notorious crimeware today—have been enhanced to better evade detection by security solutions. This research paper discusses some of the notable changes that have been made to the aforementioned crimeware. It specifically talks about two types of crimeware—toolkits and exploit kits—commonly sold underground and used by bad guys for their own malicious purposes.

Toolkits help cybercriminals create and manage malicious programs as well as run networks of interconnected infected computers called "botnets." Examples of these include ZeuS, Citadel, Ice IX, and SpyEye.

Exploit kits, meanwhile, help cybercriminals spread malicious programs using exploits that take advantage of well-known application vulnerabilities. The Blackhole Exploit Kit is one of the most popular exploit kits sold underground.

Crimeware like toolkits and exploit kits make life easy for cybercriminals. Their use makes malware creation and deployment a breeze in a sense. Because if there is anything we can be sure of, it is that the better security companies do at their job, the more cybercriminals will improve their wares.

Figure 1: Timeline showing when each crimeware emerged

Toolkits

ZeuS

ZeuS, from the beginning, has always been secure. In fact, skilled cybercriminals often used ZeuS because its creator—Monstr, aka Slavik—has been very selective of his customers. He often dealt with buyers only via instant or chat messages.[1] Chats were easy to encrypt and keep away from prying eyes compared with emails. All Monstr had to do was ensure that he used strong passwords for his instant-messaging accounts and that the said accounts could not be easily traced back to him.

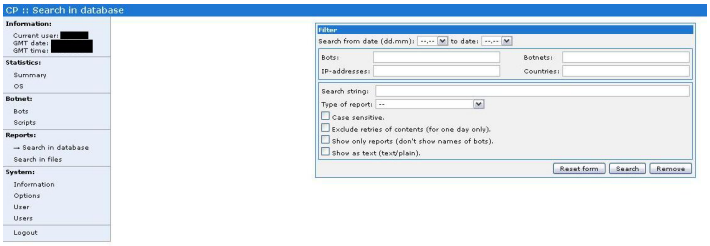

Figure 2: ZeuS control panel

Part of the reason for ZeuS's infamy was its reliability. It was coded well, which is a plus for interested buyers, as this made them harder to catch. Though ZeuS remains in use today, its code has not been updated since its creator disappeared sometime in October 2010. Monstr was said to have passed on the source code of his creation before he vanished though to SpyEye creator, Gribodemon, aka harderman.

Citadel and Ice IX

Citadel and Ice IX could be considered by-products of ZeuS. Both took advantage of ZeuS's popularity and the leakage of its code to become known in the cybercriminal underground. Prior to being publicly leaked in May 2011 though, ZeuS's source code was already privately available a month before. And though how the code was made public remains unclear, some believe this was intentional while others speculate that Gribodemon may have shared it with a few people who may have caused the leak in the process.

1 http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp__file-partching-zbot-varians-zeus-2-9.pdf

Aquabox—Citadel's creator—improved ZeuS's code mainly by making its control panel more user-friendly. It was released in the Russian underground in January 2012 and since then took a life of its own with the support of a skillful and relentless development team. It is the only crimeware of its grade being marketed to fraudsters in open underground venues.[2]

Figure 3: Citadel control panel

Ice IX, meanwhile, boasted of protection from trackers. Its creator, nvidiag, claimed that only bots could download its configuration file. This was, however, not the case, as researchers could still download the configuration file without encountering any problem.[3]

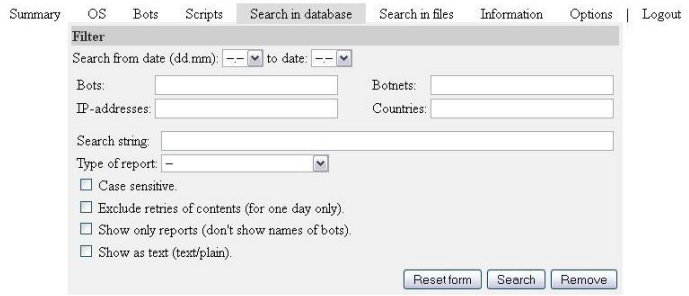

Figure 4: Ice IX control panel

SpyEye

SpyEye has not been updated since version 1.3.48, which came out in October 2011. Gribodemon—its creator—disappeared around the same time Monstr did. Other cybercriminals seem to have continued his work though, as we continue to see installation service and server offerings underground.

Initially thought to be a ZeuS competitor, SpyEye first reared its ugly head in 2009. Monstr was said to have passed on the source code of his creation before he vanished though to SpyEye creator, Gribodemon. Gribodemon then started providing support to existing ZeuS customers and offered them discounted versions of SpyEye as an alternative to ZeuS. Since then, Gribodemon kept updating his creation until, like Monstr, he disappeared.[4]

Figure 5: SpyEye control panel

2 http://blogs.rsa.com/hurry-citadel-is-going-off-the-open-market/
3 http://blog.trendmicro.com/trendlabs-security-intelligence/zeus-gets-another-update/
4 http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_turning-the-tables_spyeye-cibercrime-ring.pdf

Exploit Kits

Blackhole Exploit Kit

The Blackhole Exploit Kit allows an attacker to take advantage of most known vulnerabilities in popular applications like Internet Explorer as well as Adobe Acrobat, Reader, and Flash Player. It has been a cybercriminal favorite since 2011.

To ensure its security, Paunch—its creator—does not directly provide the kit to customers. It is instead installed in a web server somewhere that is connected to a database for logging and reporting. This server, which uses web technologies like PHP and database products like MySQL, is also used as an administrative interface. Its PHP source code at the server is also encrypted and protected by IONCube.[5]

More recently, underground forum and Pastebin posts announced the availability of Blackhole Exploit Kit 2.0—an even stealthier and more lethal version—most likely created after the success of its predecessor.[6]

Figure 6: Blackhole Exploit Kit 1.0 control panel

Conclusion

Dealing with cybercrime is a daily battle. Cybercriminals continuously improve their tools to keep up with security companies' efforts to thwart threats. This research paper covered just a few of the most notorious crimeware we have seen to date. As shown, ZeuS, Citadel, Ice IX, SpyEye, and the Blackhole Exploit Kit have all undergone various enhancements since they were first released in the cybercriminal underground. They have become well-known because of their reliability and stability.

All of the crimeware mentioned in this paper, except the Blackhole Exploit Kit, are mainly used for banking fraud and stealing personally identifiable information (PII). Most of the stories you hear about banking fraud may involve malware created with any of the aforementioned crimeware. The Blackhole Exploit Kit, meanwhile, has been known for distributing malware via drive-by-downloads. As such, the simple act of visiting a compromised site is enough to get your computer infected with a banking Trojan, a FAKEAV malware, or a ransomware, more specifically a Police Trojan.

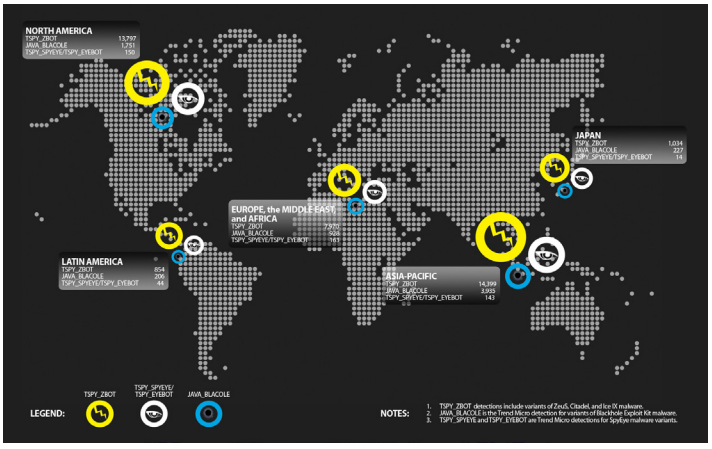

Figure 7: Regional distribution of the crimeware discussed in this paper

5 http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_blackhole-exploit-kit.pdf

6 http://blog.trendmicro.com/trendlabs-security-intelligence/blackhole-2-0-beta-tests-in-the-wild/

Cybercriminals will continue to create and improve malicious wares, including crimeware, because selling and using these is profitable. Crimeware will continue to be used as long as they remain effective, otherwise cybercriminals will find better tools.

One thing is for sure though, we will continue to monitor and stay on top of underground activities to protect customers with the help of our products backed by the Trend Micro™ Smart Protection Network™.

The Trend Micro Smart Protection Network cloud security infrastructure rapidly and accurately identifies new threats, delivering global threat intelligence to secure data wherever it resides. We look in more places to collect massive amounts of threat-specific data from multiple sources including our global network of sensors. We use data mining and big data analytics to identify, correlate, and analyze new threats, producing actionable threat intelligence across mobile, physical, virtual, and cloud environments. We deliver this intelligence to our products and services through our proven cloud infrastructure to ensure our customers' data is protected.

TREND MICRO INCORPORATED

Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years' experience, we deliver top-ranked client, server and cloud-based security that fits our customers' and partners' needs, stops new threats faster, and protects data in physical, virtualized and cloud environments. Powered by the industry-leading Trend Micro™ Smart Protection Network™ cloud computing security infrastructure, our products and services stop threats where they emerge—from the Internet. They are supported by 1,000+ threat intelligence experts around the globe.

TREND MICRO INCORPORATED

10101 N. De Anza Blvd.
Cupertino, CA 95014

U.S. toll free: 1 +800.228.5651
Phone: 1 +408.257.1500
Fax: 1 +408.257.2003
www.trendmicro.com

TREND MICRO™

Securing Your Journey to the Cloud