Winnti. More than just a game

Authors

Expert GReAT

Kaspersky Lab began this ongoing research in the autumn of 2011. The subject is a series of targeted attacks against private companies around the world.

In the course of our research we uncovered the activity of a hacking group which has Chinese origins. This group was named “Winnti”.

According to our estimations, this group has been active for several years and specializes in cyberattacks against the online video game industry. The group’s main objective is to steal source codes for online game projects as well as the digital certificates of legitimate software vendors. In addition, they are very interested in how network infrastructure (including the production of gaming servers) is set up, and new developments such as conceptual ideas, design and more.

We weren’t the first to focus on this group and investigate their attacks. In 2010 US-based HBGary investigated an information security incident related to the Winnti group at one of HBGary’s customers – an American video game company.

In the Beginning Was …

In the autumn of 2011, a Trojan was detected on a huge number of computers – all of them linked by the fact that they were used by players of a popular online game. It emerged that the piece of malware landed on users' computers as part of a regular update from the game's official update server. Some even suspected that the publisher itself was spying on players. However, it later became clear that the malicious program ended up on the users' computers by mistake: the cybercriminals were in fact targeting the companies that develop and release computer games.

The computer game publisher whose servers spread the Trojan asked Kaspersky Lab to analyze the malicious program that was found on its update server. It turned out to be a DLL library compiled for a 64-bit Windows environment and even had a properly signed malicious driver.

The malicious DLL landed on gamers' computers running under either 32-bit or 64-bit operating systems. It couldn't start in 32-bit environments, but it could, under certain conditions, launch without the user's knowledge or consent in 64-bit environments, though no such accidental launches have been detected.

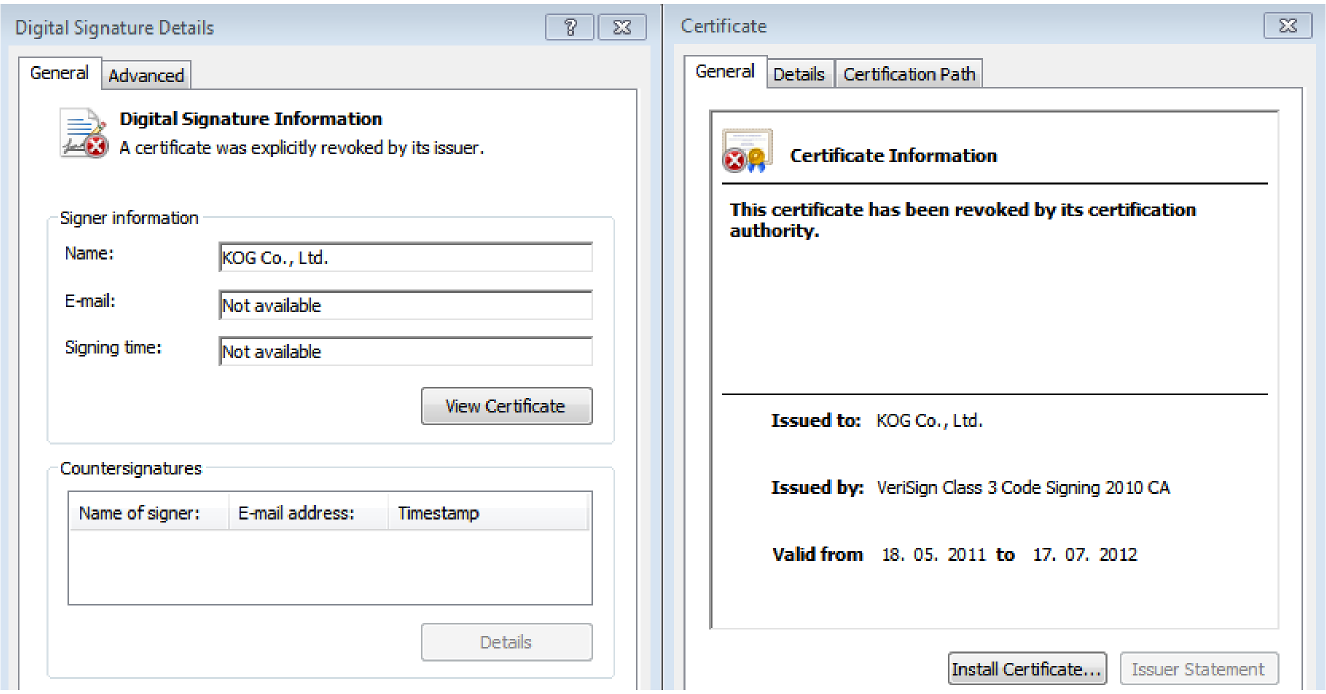
The DLL contained a backdoor payload, or, to be exact, the functionality of a fully-fledged Remote Administration Tool (RAT), which gave cybercriminals the ability to control the victim computer without the user's knowledge.

The malicious module turned out to be the first time we saw Trojan applications for the 64-bit version of Microsoft Windows with a valid digital signature. We had seen similar cases before, but all previous incidents where digital signatures were abused affected only 32-bit applications.

At an early stage of our research, we identified a fair number of similar backdoors, both 32-bit and 64-bit, in our collection of malware samples that were detected under various verdicts. We grouped them together into a separate family. Symantec appears to be the first to name these malicious programs; we kept Symantec's name – Winnti – in the name of the malware family we created: Backdoor.Win32(Win64).Winnti. As for the people behind these attacks involving this remote administration tool, we ended up calling them "the Winnti group".

Interestingly, the digital signature belonged to another video game vendor – a private company known as KOG, based in South Korea. This company's main business was MMRPG games, exactly the same area as the first victim.

We contacted KOG, whose certificate was used to sign the malicious software, and notified Verisign, which issued the certificate for KOG. As a result the certificate was revoked.



Digital Signature Information
A certificate was explicitly revoked by its issuer.

Signer information

Name: KOG Co., Ltd.

E-mail: Not available

Signing time: Not available

Countersignatures

Name of signer:	E-mail address:	Timestamp

Certificate Information

This certificate has been revoked by its certification authority.

Issued to: KOG Co., Ltd.

Issued by: VeriSign Class 3 Code Signing 2010 CA

Valid from 18. 05. 2011 **to** 17. 07. 2012

Digital Certificates

When we discovered the first stolen digital certificate we didn't realize that stealing the certificates and signing malware for future attacks against other targets was the preferred method of this group. Over the next 18 months we discovered more than a dozen similar compromised digital certificates.

Moreover, we found that those digital certificates seemed to have been used in attacks organized by other hacking groups, presumably coming from China.

For example, in an attack against South Korean social networks Cyworld and Nate in 2011 the attackers used a Trojan that was digitally signed using a certificate of from the gaming company YNK Japan Inc.

A digital certificate of the same company was used recently (March 2013) in Trojans deployed against Tibetan and Uyghur activists. In fact, this story dates back to 2011. We highly recommend this Norman blogpost about a similar incident: http://blogs.norman.com/2011/security-research/invisible-ynk-a-code-signing-conundrum .

At the same time, in March 2013, Uyghur activists were targeted by other malware, which was digitally signed by another gaming company called MGAME Corp.

We believe that the source of all these stolen certificates could be the same Winnti group. Either this group has close contacts with other Chinese hacker gangs, or it sells the certificates on the black market in China.

Below is the list of known compromised companies and digital certificates used by the Winnti group in different campaigns:

Company	Serial number	Country
ESTsoft Corp	30 d3 fe 26 59 1d 8e ac 8c 30 66 7a c4 99 9b d7	South Korea

Kog Co., Ltd.	66 e3 f0 b4 45 9f 15 ac 7f 2a 2b 44 99 0d d7 09	South Korea
LivePlex Corp	1c aa 0d 0d ad f3 2a 24 04 a7 51 95 ae 47 82 0a	South Korea/ Philippines
MGAME Corp	4e eb 08 05 55 f1 ab f7 09 bb a9 ca e3 2f 13 cd	South Korea
Rosso Index KK	01 00 00 00 00 01 29 7d ba 69 dd	Japan
Sesisoft	61 3e 2f a1 4e 32 3c 69 ee 3e 72 0c 27 af e4 ce	South Korea
Wemade	61 00 39 d6 34 9e e5 31 e4 ca a3 a6 5d 10 0c 7d	Japan/South Korea/US
YNK Japan	67 24 34 0d db c7 25 2f 7f b7 14 b8 12 a5 c0 4d	Japan
Guangzhou YuanLuo	0b 72 79 06 8b eb 15 ff e8 06 0d 2c 56 15 3c 35	China
Fantasy Technology Corp	75 82 f3 34 85 aa 26 4d e0 3b 2b df 74 e0 bf 32	China
Neowiz	5c 2f 97 a3 1a bc 32 b0 8c ac 01 00 59 8f 32 f6	South Korea

Victims

It's tempting to assume that Advanced Persistent Threats (APTs) primarily target high-level institutions: government agencies, ministries, the military, political organizations, power stations, chemical plants, critical infrastructure networks and so on. In this context it seems unlikely that a commercial company would be at risk unless it was operating on the scale of Google, Adobe or The New York Times, which was recently targeted by a cyberattack, and this perception is reinforced by the publicity that attacks on corporations and government organizations usually receive. However, any company with data that can be effectively monetized is at risk from APTs. This is exactly what we encountered here: it was not a governmental, political, military, or industrial organization but gaming companies that were targeted.

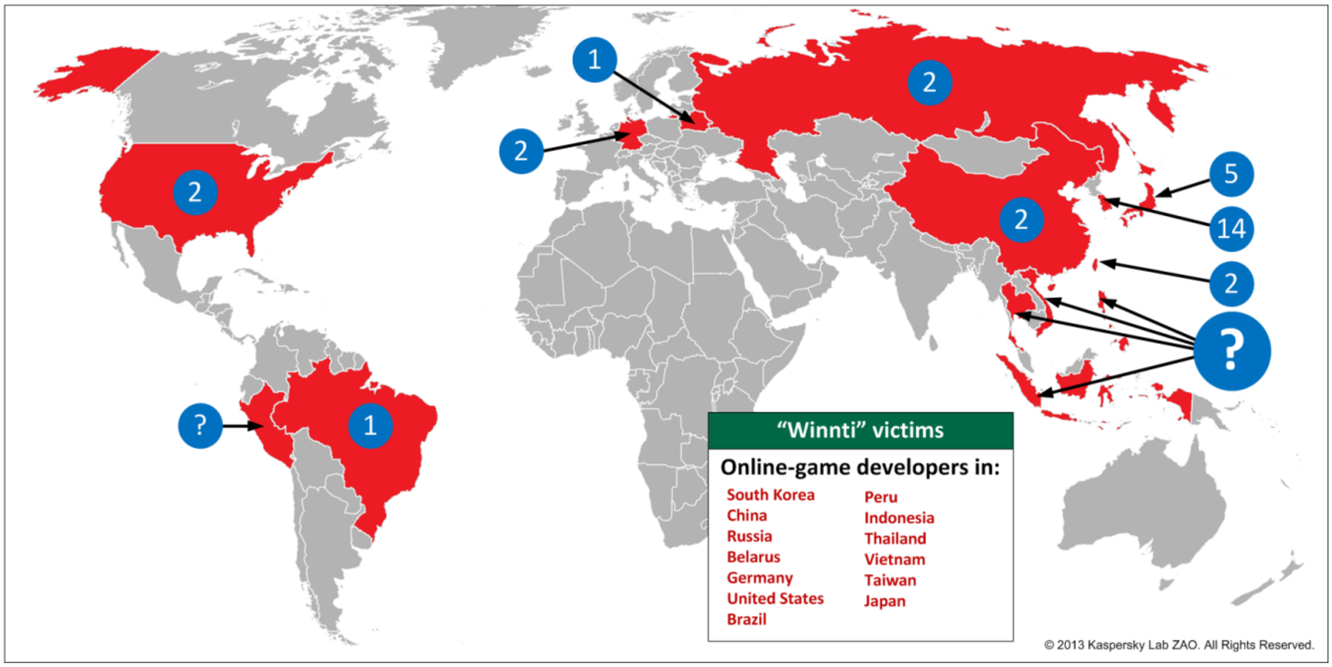
It's difficult to name all the victims of the Winnti team. Judging by the information that we have at our disposal – namely the tags within malicious programs, the names of the C&C domains, the companies whose digital certificates were stolen to sign malware, and the countries where detection notifications came from – we can say that at least 35 companies have been infected by Winnti malware at some time.

Countries where the affected companies are located:

Asia	Europa	South America	North America
Vietnam	Belarus	Brazil	USA
India	Germany	Peru	
Indonesia	Russia		
China			
Taiwan			
Thailand			

Phillipines
S. Korea
Japan

This data demonstrates that the Winnti team is targeting gaming companies located in various parts of the world, albeit with a strong focus on SE Asia.



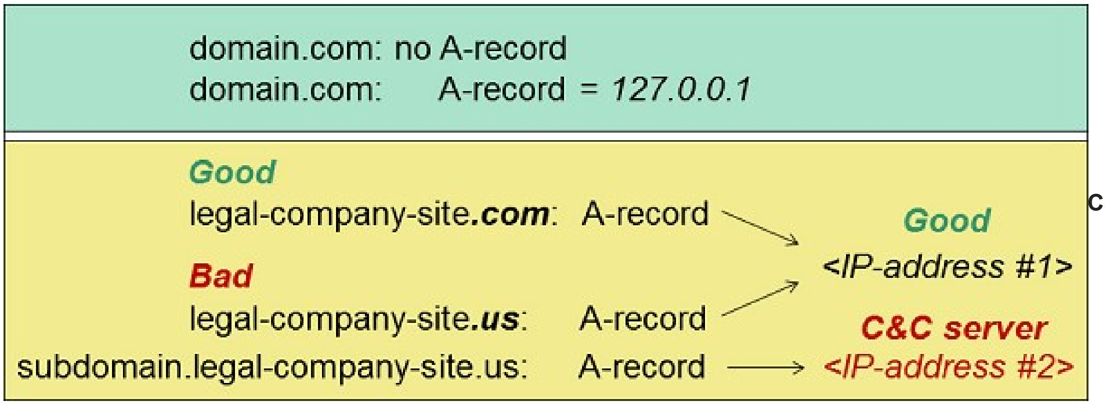
Countries where gaming companies have been affected

Such geographic diversity is hardly surprising. Often, gaming companies (both publishers and developers) are international, having representatives and offices worldwide. Also, it is common practice for gaming companies from various regions to cooperate. The developers of a game may be located in a different country from its publisher. When a game later reaches markets in regions away from its initial ‘home’, it is often localized and published by other publishers. In the course of this cooperation, the partner companies often grant each other access to network resources to exchange data associated with the gaming content, including distribution kits, gaming resources, resource assembly kits, etc. If one company in the network gets infected, it’s easy for the cybercriminals to spread the infection throughout the partnership chain.

Winnti C&Cs Structure

During the investigation, we identified over a hundred malicious programs, every single one compiled to attack a particular company. Typically, separate C&C domains were assigned to each targeted company. Virtually all the C&C domains were arranged as follows: a second-level domain was created without a DNS A-record, i.e., there was no IP address assigned to it.

In case there was an A-record, the assigned IP address was typically 127.0.0.1. It is also noteworthy that some of the second-level domains that the cybercriminals created for their C&C had very similar names to the domain hosting the site of a certain real gaming company. And the malicious users’ domain was resolved to the same IP address which the site of the real gaming company used. In any case, the third-level domains resolved to IP addresses assigned to the attackers' actual C&C servers.


domain.com: no A-record
domain.com: A-record = 127.0.0.1
Good
legal-company-site.com: A-record
Good
<IP-address #1>
Bad
legal-company-site.us: A-record
C&C server
subdomain.legal-company-site.us: A-record
<IP-address #2>

C&C domain naming and resolution

Sometimes the Winnti team registered their C&C units with public hosts. Judging by the samples identified, these C&C centers were subdomains of such domains as 6600.org, 8866.org, 9966.org or ddns.net.

From the names of the C&C domains or subdomains, the attack targets or countries of residence could be guessed, as in:

```
 ru.gcgame.info
kr.zzsoft.info
jp.xxoo.co
us.nhntech.com
fs.nhntech.com
as.cjinternet.us
```

The subdomains "ru", "kr", "jp" and "us" most probably mean that these C&C servers manage bots hosted on the computers of companies located in Russia, South Korea, Japan and the US respectively, while "fs" and "as" are acronyms for the names of the companies being attacked.

Sometimes Winnti's malicious programs had a local IP address, such as 192.168.1.136, specified in their settings for the C&C. This could mean that at some point of time there was an infected computer that did not have a connection to the Internet, but the cybercriminals needed control over it (it may have been infected while malware was spread via a corporate network). In this case, the cybercriminals deployed a dedicated local C&C server on another compromised computer within the same local network which did have an Internet connection; via that C&C, the first victim computer could be controlled. System administrators often try to isolate critical computers from the outside world. This decreases the probability of haphazard infection, but, apparently, does not always help in a targeted attack.

In the Winnti samples that were detected and analyzed, we found 36 unique C&C domains. Most probably, this is only a small portion of all existing Winnti C&C domains, as we only managed to obtain some of the samples from this malware family. This is hardly surprising since these malicious programs are used to execute targeted attacks, so no information is available about many instances of infection; for this reason, we have no way of obtaining samples of the malware used in these undisclosed attacks.

Domain names used in the attacks we discovered:		
newpic.dyndns.tv	lp.zzsoft.info	ru.gcgame.info
update.ddns.net	lp.gasoft.us	kr.jcrsoft.com
nd.jcrsoft.com	eya.jcrsoft.com	wm.ibm-support.net
cc.nexoncorp.us	ftpd.9966.org	fs.nhntech.com
kr.zzsoft.info	kr.xxoo.co	docs.nhnclass.com
as.cjinternet.us	wi.gcgame.info	rh.jcrsoft.com
ca.zzsoft.info	tcp.nhntech.com	wm.nhntech.com
sn.jcrsoft.com	ka.jcrsoft.com	wm.myxxoo.com
lp.apanku.com	my.zzsoft.info	ka.zzsoft.info
sshd.8866.org	jp.jcrsoft.com	ad.jcrsoft.com
ftpd.6600.org	su.cjinternet.us	my.gasoft.us
tcpiah.googleclick.net	vn.gcgame.info	
rss.6600.org	ap.nhntech.com	

Knowing the 2nd level domains used by Winnti, we brute forced through all 3rd level subdomains up to 4 symbols long, and identified those that have the IP addresses of real servers assigned to them. Having searched through subdomains for a total of 12 2nd level domains, we identified 227 “live” 3rd level domains. Many of them are C&C servers for Winnti-class malware that have hitherto remained unidentified.

Analyzing the WHOIS data for the 12 2nd level domains, we found the following list of email addresses used for registration:

```
evilsex@gmail.com
jslee.jcr@gmail.com
whoismydns@gmail.com
googl3@live.com
wzcc@cnkker.com
apanku2009@gmail.com
```

For some of these domains, registration data proved to be the same as those for the domain google.com:

```
Registrant: Google Inc.
1600 Amphitheatre Parkwa
Mountain Vie, California 94043
United States
+1.6503300100
```

Judging by the domain registration data, the Winnti team started their criminal activities at least in 2007. Their early domains were involved in spreading rogue antiviruses (FakeAV). From 2009 onwards, domains began to emerge hosting C&C servers for bots used to infect gaming companies. Apparently, the cybercriminals graduated to relatively large-scale penetrations into the corporate networks of gaming companies starting from 2010.

Known Malware

The attackers' favorite tool is the malicious program we called "Winnti". It has evolved since its first use, but all variants can be divided into two generations: 1.x and 2.x. Our publication describes both variants of this tool.

In our report we publish an analysis of the first generation of Winnti.

The second generation (2.x) was used in one of the attacks which we investigated during its active stage, helping the victim to interrupt data transfer and isolate infections in the corporate network. This incident and our investigation is described in detail here.

In addition to that, we have observed the use of a popular backdoor known as PlugX, which is believed to have Chinese origins. Previously, this had only been used in attacks against Tibetan activists.

The Commercial Interest

As has been stated above, APTs can target any commercial company if cybercriminals find a way to make a profit from the attack.

So which methods do cybercriminals use to generate illicit earnings from attacks on gaming companies?

Based on the available information, we have singled out three main monetization schemes that could be used by the Winnti team.

- **The unfair accumulation of in-game currency/"gold" in online games and the conversion of virtual funds into real money.**
- **Theft of source code from the online games server to search for vulnerabilities in games – often linked to point 1.**
- **Theft of source code from the server part of popular online games to further deploy pirate servers.**

Let's look at an example. During our investigation of an infection at a computer game company, we found that malware had been created for a particular service on the company's server. The malicious program was looking for a specific process running on the server, injected code into it, and then sought out two places in the process code where it could conceal call commands for its function interceptors. Using these function interceptors, the malicious programs modified process data which was processed in those two places, and returned control back. Thus, the attackers change the normal execution of the server processes. Unfortunately, the company was not able to share its targeted application with us, and we cannot say exactly how this malicious interference affected gaming processes. The company concerned told us that the attackers' aim was to acquire gaming "gold" illegally.

Malicious activity like this has an adverse impact on the game itself, tilting the balance in favor of cheats. But any changes the Winnti team introduces into the game experience are unlikely to be very noticeable. After all, maintaining a skillful balance is the main attribute of online games! Users will simply stop playing if they feel that other players are using non-standard methods to create an advantage beyond normal gameplay or if the game loses its intrinsic competitiveness due to resources or artifacts appearing in the game without the developers' knowledge. At the same time the attackers are keen for the game to remain popular; otherwise, they would be unable to effectively turn all the time and effort of infecting a gaming company into financial gain.

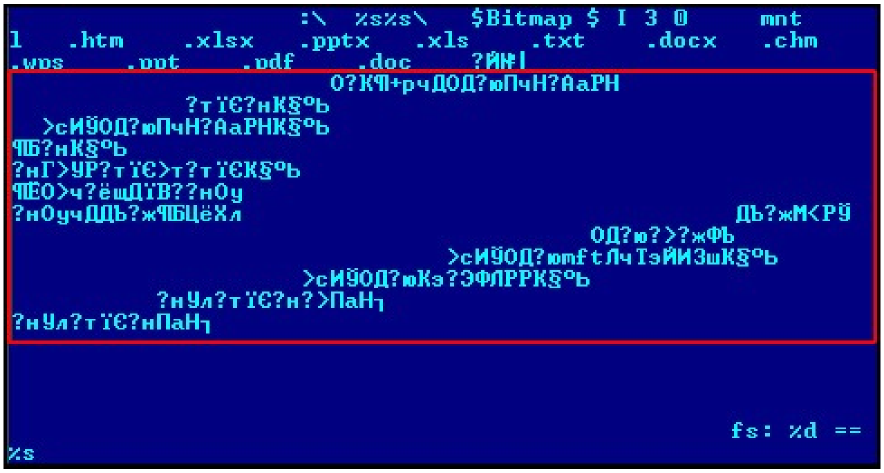
Members of the Winnti team are patient and cautious. Cybercriminals have affected the processes of the online games from the infected companies and stolen money from them for years, but they have found ways of doing this without attracting attention to themselves.

Source of Attacks

So, who is behind Winnti? While analyzing the malicious files that we detected during our investigation we found some details which may cast some light on the source of the attacks.

As part of our investigation, we monitored exactly what the cybercriminals did on an infected PC. In particular, they they downloaded an auxiliary program ff._exe to the Config.Msi folder on the infected machine. This code searches for HTML, MS Excel, MS Word, Adobe, PowerPoint and MS Works documents and text files (.txt) on the hard drive.

Debugging lines were found in ff._exe_ that possibly point to the nationality of the cybercriminals. They were not immediately noticeable because they looked like this in the editor:

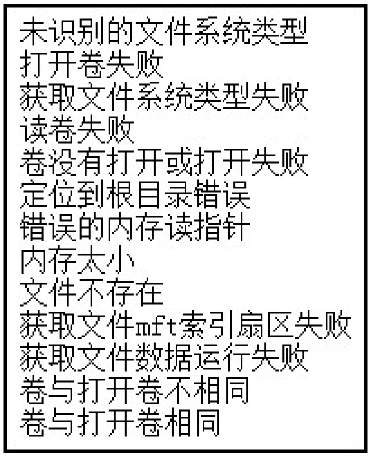


```
                    :\   %s%s\    $Bitmap $ I 3 0      mnt
l    .htm     .xlsx    .pptx    .xls     .txt     .docx    .chm
.wps     .ppt     .pdf     .doc     ?ЙЊ|
                      O?К¶+рчДОД?юПчН?АаРН
            ?тЇЄ?нК§ºь
  >сИЎОД?юПчН?АаРНК§ºь
¶Б?нК§ºь
?нГ>УР?тЇЄ>т?тЇЄК§ºь
¶ЕО>ч?ёшДЇВ??нОу
?нОучДДь?ж¶БЦёХл                                        Дь?жМ<РЎ
                                              ОД?ю?>?жФь
                                    >сИЎОД?юmftЛчТэЙИЗшК§ºь
                    >сИЎОД?юКэ?ЭФЛРРК§ºь
          ?нУл?тЇЄ?н?>ПаН┐
?нУл?тЇЄ?нПаН┐



                                                 fs: %d ==
%s
```

However, during a detailed analysis it emerged that the text is in Chinese Simplified GBK coding. This is what these lines look in Chinese:



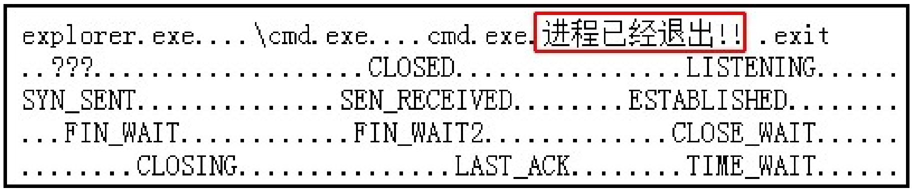
```
未识别的文件系统类型
打开卷失败
获取文件系统类型失败
读卷失败
卷没有打开或打开失败
定位到根目录错误
错误的内存读指针
内存太小
文件不存在
获取文件mft索引扇区失败
获取文件数据运行失败
卷与打开卷不相同
卷与打开卷相同
```

Below is a machine translation of this text into English:

```
 Not identify the type of file system
Below is a translation of the text by interpreter
Open the volume failed
Failed to get the file system type
Failed to read volume
Volumes do not open or open failed
Navigate to the root directory of the error
Error memory read pointer
Memory is too small
File does not exist
Failed to get the file mft index sector
Access to file data fail
Volume and open volumes are not the same
The same volume and open volume
```

In addition, cybercriminals used the AheadLib program to create malicious libraries (for details, see the second part of the article). This is a program with a Chinese interface.

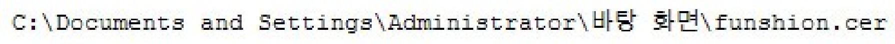
Chinese text was also found in one of the components of the malicious program CmdPlus.dll plug-in:



```
explorer.exe....\cmd.exe....cmd.exe.进程已经退出!! .exit
..???..................CLOSED...............LISTENING.....
SYN_SENT..............SEN_RECEIVED.......ESTABLISHED.......
...FIN_WAIT...........FIN_WAIT2............CLOSE_WAIT.....
........CLOSING..............LAST_ACK........TIME_WAIT.....
```

Translation: ***The process is complete!!***

It would appear that the attackers can at least speak Chinese. However, not everything is so clear cut: because the file transfer plug-in has not been implemented entirely safely, a command which includes the attackers' local path (where the file comes from and where it is saved to) arrives during the process of downloading/uploading files on the infected system. While monitoring the cybercriminals' activity on the infected machine, we noticed they uploaded the certificate they found in the infected system, and the network traffic reflected the local path indicating the place where they saved the file on their computer:



```
C:\Documents and Settings\Administrator\바탕 화면\funshion.cer
```

These characters appear to be Korean, meaning “desktop”. This means the attackers were working on a Korean Windows operating system. Therefore, we can presume that the attack is not the exclusive work of Chinese-speaking cybercriminals.

Conclusions

Our research revealed long-term oriented large scale cyberespionage campaign of a criminal group with Chinese origins. These attacks are not new, many other security researchers have published details of various cybercriminal groups coming from China. However, current hacking group has distinguishable features that make it stand out among others:

- massive abuse of digital signatures; the attackers used digital signatures of one victim company to attack other companies and steal more digital certificates;
- usage of kernel level 64-bit signed rootkit;
- abusing great variety of public Internet resources to store control commands for the malware in an encrypted form;
- sharing/selling stolen certificates to other groups that had different objectives (attacks against Uyghur and Tibetan activists);
- stealing source codes and other intellectual property of software developers in online gaming industry.

The malicious program which we call “Winnti” has evolved significantly since it first emerged; however we classify all its variants in two main generations: 1.x and 2.x.

We have published the technical description of the first generation of Winnti in a separate article .

The second generation (2.x) was used to conduct an attack which we investigated during its active stage. We successfully prevented data transfer to the cybercriminals’ server and isolated the infected systems in the company’s local network. The incidents, as well as results of our investigation, are described in the full report on the Winnti group (PDF).

In addition, we discovered that the Winnti group uses a popular backdoor known as PlugX which also has Chinese origins. This backdoor had previously been seen almost exclusively in attacks targeting Tibetan activists.

Read further

- APT
- Certificate authorities
- Cyber espionage
- Online Games
- Rootkits
- Spear phishing
- Targeted attacks
- Winnti

Authors

Expert GReAT

Winnti. More than just a game

Your email address will not be published. Required fields are marked *