THREAT ANALYSIS

BRONZE UNION Cyberespionage Persists Despite Disclosures

TUESDAY, JUNE 27, 2017
BY: COUNTER THREAT UNIT RESEARCH TEAM

Summary

In 2015, the SecureWorks® Counter Threat Unit™ (CTU) research team documented the BRONZE UNION threat group (formerly labeled TG-3390), which CTU™ analysis suggests is based in the People's Republic of China (PRC). Since that analysis, CTU researchers have observed multiple BRONZE UNION threat campaigns that illustrate the evolution of the group's methods and espionage objectives. Despite multiple public disclosures of their activities, BRONZE UNION remains an active and formidable threat as of this publication.

CTU researchers divided the threat intelligence about this group into two sections: strategic and tactical. Executives can use the strategic assessment of the ongoing threat to determine how to reduce risk to their organization's mission and critical assets. Computer network defenders can use the tactical information gathered from incident response investigations and research to reduce the time and effort associated with responding to the threat group's activities.

Key points

- CTU researchers assess it is highly likely that the BRONZE UNION threat group gathers defense, security, and political intelligence from organizations around the world. CTU researchers have observed it targeting organizations in the aerospace, government, defense, technology, energy, and manufacturing verticals.
- CTU researchers assess it is likely that the group is located in the People's Republic of China.
- BRONZE UNION has historically used strategic web compromises (SWCs) in its campaigns, CTU researchers have also observed it exploiting vulnerable Internet-facing services to gain access to targeted networks.
- After accessing a network, the threat actors leverage a range of proprietary, publicly available, and native tools to search for and acquire desirable data.

Strategic threat intelligence

Analysis of a threat group's targeting, origin, and competencies can determine which organizations could be at risk. This information can help organizations make strategic defensive decisions regarding this threat.

Intent

Based on BRONZE UNION's targeting activity, CTU researchers assess it is highly likely that the group focuses on political and defense organization networks. In 2016, the threat actors conducted a strategic web compromise (SWC) on the website of an international industry organization that affected aerospace, academic, media, technology, government, and utilities organizations around the world. During a discrete period of activity, this SWC was used to specifically target Turkish government, banking, and academic networks. These focused attacks suggest a concerted effort to compromise strategically significant networks in Turkey, possibly due to Turkey's political, economic, and military relationships in Europe and the Middle East.

In addition, BRONZE UNION activity on multiple U.S.-based defense manufacturer networks included the threat actors seeking information associated with aerospace technologies, combat processes, and naval defense systems. Third-party analysis suggests that systemic issues in the PRC's defense technology industries could influence demand for this type of information because this type of data could potentially address innovation and supply deficits which exist within this industry sector in the PRC.

Attribution

In 2015, CTU researchers assessed that BRONZE UNION likely originates in the PRC based on factors such as targeting, operating hours, and tool selection. Observed activity since 2015 reinforces that association; for example:

- continued focus on information that would be of interest to individuals or groups living in a country that has a significant manufacturing base and a strategic interest in U.S. military capabilities
- use of web shells that have historically been leveraged by threat groups believed to be operating in the PRC
- connections between a subset of the group's operational infrastructure and PRC-based Internet service companies

Capability

BRONZE UNION has consistently demonstrated the capability to conduct successful large-scale intrusions against high-profile networks and systems. CTU researchers identified evidence of the group exploiting vulnerabilities in Internet-facing service desk software to gain an initial foothold on desirable networks, while concurrently compromising systems of interest via SWCs. During the observed intrusions, the group rapidly collected account credentials, escalated privileges, and deployed multiple web shells presumably to extend its access across the compromised network.

BRONZE UNION is disciplined and takes proactive steps to avoid detection. For example, at the end of 2016 CTU researchers observed the threat actors using native system functionality to disable logging processes and delete logs within a network. The group also manipulated native Windows features on compromised systems to access additional legitimate functionality. These behaviors indicate that the threat actors quickly gain a detailed understanding of the environments they compromise and use this understanding to conceal their activity from network defenders. Although CTU researchers have observed BRONZE UNION modifying its tools, likely in response to public reporting on its activities, there is no evidence that the group's capabilities have changed substantially or that its operations have been deterred.

Tactical threat intelligence

Investigating BRONZE UNION activity and evicting the threat actors from compromised networks have given CTU researchers unique insight into the group's tools and tactics.

Tools

CTU researchers observed BRONZE UNION using the following tools in intrusions since the 2015 analysis, but clients should assume that the threat group still has access to the previously reported tools.

- OwaAuth — This web shell and credential stealer deployed to Microsoft Exchange servers is installed as an ISAPI filter. Captured credentials are DES-encrypted using the password "12345678" (see Figure 1), and are written to a text file (log.txt) in the system's root directory.

```
 ' Microsoft.Exchange.Clients.OwaAuth
Public Sub Init(Application As HttpApplication)
    Me.SP = "[redacted]ExhhangeOwaauths"
    Me.Key = "12345678"
    Me.Log = "c:\log.txt"
    Me._application = Application
    Me._application.BeginRequest += New EventHandler(Me.Application_BeginRequest)
    Me._application.EndRequest += New EventHandler(Me.Application_EndRequest)
End Sub
```

Figure 1. Configuration file from OwaAuth.dll. (Source: SecureWorks)

- China Chopper web shell — This web-based executable script communicates with a full-featured user interface to allow threat actors to transfer and create files, open a command terminal, and interact with database servers.
- Rcmd — This lateral movement tool facilitates the execution of commands on systems across the target environment.
- Wrapikatz — This tool wraps Mimikatz code in a custom loader to evade antivirus detection, and changes the command-line usage to evade process-telemetry detection and make the tool easier to use. This tool is not exclusive to BRONZE UNION. CTU researchers have observed various threat groups leveraging Wrapikatz binaries with different usage options.
- Netview — This publicly available host-enumeration tool presents details about IP addresses, network shares, remote sessions, and logged-on users.
- Kekeo — This publicly available toolset manipulates the Kerberos authentication protocol. CTU researchers identified BRONZE UNION actors using a file named ms.exe that was likely a credential-abuse tool from the Kekeo toolset.

Tactics, techniques, and procedures

Observations of BRONZE UNION activity during several network compromises gave CTU researchers insight into the tactics the group employs.

Access vectors and command and control

CTU researchers observed BRONZE UNION delivering malware to systems via SWCs and scan-and-exploit techniques. The threat actors appear to be able to create and leverage multiple SWCs in parallel. They have also demonstrated the ability to create SWCs and malware-staging sites by leveraging websites linked to networks previously compromised by the group. Apparent overlap between existing compromises and new campaigns suggests that the group considers leveraging existing network compromises when planning infrastructure requirements. Figure 2 shows a BRONZE UNION infection chain leveraging an SWC.

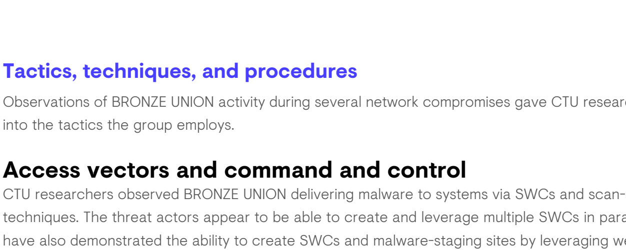

Figure 2. Likely BRONZE UNION infection chain observed in 2016. (Source: SecureWorks)

In multiple instances, CTU researchers observed artifacts from unsuccessful attempts to create a web shell on web-accessible JBOSS-based service desk software, followed by use of a functional shell to gain access to the environment. These events strongly suggest that the threat actors leveraged the web application as part of the initial compromise vector.

BRONZE UNION appears to use a combination of self-registered IP addresses and commercial VPN services in its command and control (C2) and operational infrastructure. The threat actors also integrate infrastructure they likely previously compromised for espionage purposes. For example, CTU researchers identified the group using IP addresses owned by several, presumably compromised, research organizations to interact with web shells in other target environments.

Host enumeration and lateral movement

After gaining an initial foothold in a compromised environment, the threat actors quickly identify and explore accessible systems. In one example, BRONZE UNION actors leveraged initial web shell access on Internet-facing systems to conduct internal reconnaissance, including domain enumeration and network state, via ipconfig, net use, net user, and net view commands. In a separate incident, CTU researchers identified a file named s.txt, which is consistent with the output of the Netview host-enumeration tool.

Knowledge of the compromised environment allows the threat actors to move laterally between systems. CTU researchers identified ten compromised hosts in one environment that contained artifacts associated with the Rcmd lateral-movement tool. Use of the tool leaves a small helper script (read.vbs) on the target system. This script relays commands and output between the controller and the system.

Defensive evasion

CTU researchers observed BRONZE UNION actors reconfiguring legitimate Windows features to establish PowerShell remoting and WinRM (see Figure 3). These remote management technologies allow a full range of configuration, data transfer, and remote execution capabilities over HTTP/HTTPS channels. Enabling these features gives the threat actor a remote control channel to persistently access the victim's environment without using malicious software that could be detected.

```
"cmd" /c cd /d "C:\inetpub\wwwroot\"&ver&echo [S]&cd&echo [E]
"cmd" /c cd /d "C:\inetpub\wwwroot\"&powershell Set-ExecutionPolicy RemoteSigned&echo [S]&cd&echo [E]
"cmd" /c cd /d "C:\inetpub\wwwroot\"&powershell Get-ExecutionPolicy&echo [S]&cd&echo [E]
"cmd" /c cd /d "C:\inetpub\wwwroot\"&powershell Enable-WSManCredSSP =2013Role Server -force&echo [S]&cd&ec
"cmd" /c cd /d "C:\inetpub\wwwroot\"&powershell winrm quickconfig -transport:https&echo [S]&cd&echo [E]
"cmd" /c cd /d "C:\inetpub\wwwroot\"&powershell winrm set winrm/config/service/Auth @{Kerberos=003D"true"}
"cmd" /c cd /d "C:\inetpub\wwwroot\"&powershell winrm set winrm/config/service/auth @{Basic=003D"true"}&ec
```

Figure 3. PowerShell commands. (Source: SecureWorks)

Some payloads leveraged DLL side loading, a technique that involves running a legitimate, typically digitally signed, program that loads a malicious DLL. The DLL acts as a stub loader, which loads and executes shell code. BRONZE UNION previously used this technique to enable execution of PlugX and HttpBrowser tools in a way that is challenging for network defenders to detect.

In 2016, CTU researchers observed the group using native system functionality to disable logging processes and delete logs within a compromised environment. The threat actors used the appcmd command-line tool to unlock and disable the default logging component on the server (systsm.webServer/httplogging) and then delete existing logs from the system (see Figure 4).

```
"cmd" /c cd /d "C:\inetpub\wwwroot\"&ver&echo [S]&cd&echo
"cmd" /c cd /d "C:\inetpub\wwwroot\"&c:\windows\system32\inetsrv\appcmd unlock config -section:system.webServer/httplogging&echo [S]&cd&echo
"cmd" /c cd /d "C:\inetpub\wwwroot\"&c:\windows\system32\inetsrv\appcmd set config "Default Web Site/" /section:httplogging /dontLog:true&echo [S]&cd&echo
"cmd" /c cd /d "C:\inetpub\wwwroot\"&del C:\inetpub\logs\LogFiles\W3SVC1\*.log /q&echo [S]&cd&echo
```

Figure 4. Threat actor using appcmd to delete logs and disable logging. (Source: SecureWorks)

Credential access

BRONZE UNION uses various tools for credential theft. In one incident, the threat actor used the Wrapikatz tool (w.exe) with a usage statement that retrieves various passwords and Windows credentials from memory and compiles them in w.txt:

```
c:\programdata\w.exe -w -l -c>>c:\programdata\w.txt
```

In a separate incident, the threat actor used access provided by extensive web shell deployment to harvest account credentials:

```
2016-10-03T09:27:47 dir
2016-10-03T09:28:11 w64.log >ppp.log
2016-10-03T09:30:10 PowerShell.exe -ExecutionPolicy Bypass -File getpwd.ps1
>iistail.log
```

In another example, BRONZE UNION leveraged the Kekeo credential abuse tool to exploit CVE-2014-6324, a vulnerability in Microsoft's implementation of the Kerberos network authentication protocol. Exploitation of this vulnerability allows an attacker to escalate privileges on the affected system.

Exfiltration

BRONZE UNION has also leveraged various web shells to collect and stage data for exfiltration. In one instance, the threat actor gained remote access to a high-value system in a compromised network, ran quser.exe to identify existing RDP sessions on the device, immediately ran a command to compile a RAR archive that specified file types the threat actor did not want, and used a password to encrypt the archive:

```
YYYY-MM-DD hh:mm:ss quser
YYYY-MM-DD hh:mm:ss C:\windows\temp\svchost.exe a -m5 -v2000m -hp{password} -
inul -r "{destination_file.rar}" "{multiple user directories linked to the
victim's projects}" -x*.exe -x*.msi -x*.cab -x*.inc -x*.dll -x*.db -x*.mdb -
x*.htm -x*.html -x*.css -x*.jar -x*.js -x*.tmp -x*.bak -x*.dat -x*.log -
x*.xml -x*.dmp -x*.dbf -x*.avi -x*.mp3 -x*.mp4 -x*.mpg -x*.mpeg -x*.asp -
x*.aspx -x*.gif -x*.jpg -x*.mpp -x*.pst
```

The threat actors typically rename the encrypted RAR archives. In the following example, archives for exfiltration were renamed as .tmp files:

```
move \\{FILE PATH}\c$\programdata\AT.part01.rar \\{FILE
PATH}\c$\programdata\at01.tmp
```

The TMP files were then staged for exfiltration on Internet-facing servers that had previously been compromised with the China Chopper web shell. From those servers the threat actor could use a web shell to retrieve the encrypted archives:

```
copy \\{FILE PATH}\c$\programdata\*.tmp \\{FILE PATH}\ServiceDesk\custom\style
```

After exfiltrating the files, the threat actor used web shell access on the staging server to delete the staged RAR archives and detach their network shares, likely to avoid detection. Figure 5 shows the commands used to perform these activities on a RAR archive renamed with a *.jpg extension.

```
NewServiceDesk    2016-09-29T15:10:45    net use * /d /y
NewServiceDesk    2016-09-29T15:10:44    dir
NewServiceDesk    2016-09-29T15:10:42    del *.jpg"
NewServiceDesk    2016-09-29T15:10:42    dir
NewServiceDesk    2016-09-29T15:10:41    cd /d "E:\ManageEngine\ServiceDesk
\server\default\deploy\common-libraries.war
```

Figure 5. BRONZE UNION commands. (Source: SecureWorks)

Reentry attempt

After BRONZE UNION was evicted from a compromised environment, which involved blocking the group's known infrastructure, CTU researchers observed the group attempting to reconnect to its OWA web shells and a backup web shell it had deployed during the intrusion. The threat actor also attempted to use OWA account credentials likely acquired during an earlier phase of the intrusion. BRONZE UNION appeared to leverage other compromised infrastructure, presumably to make reentry attempts seem legitimate. This attempt illustrates the importance of thorough planning when conducting an eviction and the need for continuous vigilance for evidence of reentry.

Conclusion

As of this publication, BRONZE UNION remains a formidable threat group that targets intellectual property and executes its operations at a swift pace. Its activities indicate a preference for leveraging SWCs and scan-and-exploit techniques to compromise target systems. To mitigate these threats, CTU researchers recommend that clients conduct regular internal vulnerability scanning, patching, and upgrading of priority systems, particularly Internet-facing systems and users' devices. Advanced endpoint threat detection (AETD) can help detect activity associated with web shells and lateral movement, and network technologies that use sandboxing techniques to detonate binaries in network traffic can prevent malicious traffic from reaching internal systems. Early detection and response can minimize exposure and damage.

Threat indicators

The threat indicators in Table 1 are associated with BRONZE UNION activity. Note that IP addresses can be reallocated. The IP addresses may contain malicious content, so consider the risks before opening them in a browser.

Indicator	Type	Context
198.56.185.179	IP address	Used by BRONZE UNION to connect to China Chopper web shell
211.255.155.194	IP address	Likely associated with VPN used by BRONZE UNION to connect to China Chopper web shell
211.255.155.199	IP address	Likely associated with VPN used by BRONZE UNION to connect to China Chopper web shell
211.255.155.202	IP address	Likely associated with VPN used by BRONZE UNION to connect to China Chopper web shell
211.255.155.204	IP address	Likely associated with VPN used by BRONZE UNION to connect to China Chopper web shell
211.255.155.215	IP address	Likely associated with VPN used by BRONZE UNION to connect to China Chopper web shell
211.255.155.218	IP address	Likely associated with VPN used by BRONZE UNION to connect to China Chopper web shell
211.255.155.219	IP address	Likely associated with VPN used by BRONZE UNION to connect to China Chopper web shell
211.255.155.224	IP address	Likely associated with VPN used by BRONZE UNION to connect to China Chopper web shell
104.130.244.126	IP address	Used by BRONZE UNION to connect to web shells
96.90.63.57	IP address	Used by BRONZE UNION to connect to web shells
117.136.63.145	IP address	Used by BRONZE UNION to connect to web shells
cd5aaa37ee165071f914ceec8fd09e0f	MD5 hash	OwaAuth web shell used by BRONZE UNION
2b5aa30f8f0575bdfe1ddebc8dac8c56a91137a8	SHA1 hash	OwaAuth web shell used by BRONZE UNION
0e823a5b64ee761b70315548d484b5b9c4b61968b5068f9a8687c612ddbfeb80	SHA256 hash	OwaAuth web shell used by BRONZE UNION
javaws.exe	Filename	Malware used in BRONZE UNION SWC that downloads and executes a second-stage payload
98c5f2a680fe9de19683120be90ea75c	MD5 hash	Malware used in BRONZE UNION SWC (javaws.exe)F
daa03d4aa72a16fff910142982b057b195018e6d	SHA1 hash	Malware used in BRONZE UNION SWC (javaws.exe)
ec60e57419f24fabbe67451cb1055b3d2684ab2534cd55c4a88cc395f9ed1b09	SHA256 hash	Malware used in BRONZE UNION SWC (javaws.exe)
45.114.9.174	IP address	Used by BRONZE UNION to host second-stage payload for SWC

Table 1. BRONZE UNION indicators.