Goodcorp vs APT41

Aimé Fraser

Executive Summary

With a state-of-the-art game in development, Gamecorp is a prime target for APT41. The threat actor's past actions in the gaming industry have proven their ability to disrupt operations and negatively impact brand awareness. They have stolen code in development, poisoned updates to infect end-user systems, installed ransomware, hijacked resources for crypto-mining, and manipulated in-game currency.

Threat Actor APT41

Known as a sophisticated Chinese state-sponsored actor targeting a broad cross-section of industries, including healthcare, tech, telecoms, media, software, education, and travel, APT41 engages in espionage operations in these industries consistent with Chinese national policy priorities. However, the group was first identified in 2012, operating in the gaming industry. Most of their work in this sector has occurred outside regular business hours in China, between 1800 and 0700 (UTC +8). It appears this work is done for personal gain outside their daily work but with the tacit approval of their government employers.

The Initial Compromise

APT41 often gains access to systems through spear-phishing and prefers to use attachments. One of their favored methods of running a phishing campaign is to tease current industry buzz in the subject line of emails. Their thorough research allows them to send emails from spoofed addresses of people likely known to the recipient. They are not only content to target employees but also phish supply chain partners who may not enforce stringent security measures.

To these ends, they have exploited vulnerabilities in Microsoft Office, Atlassian Confluence, and TeamViewer and have used compiled HTML in attachments. These are relatively complex methods, and APT41 has also been known to take a more direct approach. They can bypass the social interactions required for phishing and attack unpatched or misconfigured web services directly.

Foothold and Escalation

APT41 uses various remote administration techniques to gain control of a system. They've used Cobalt Strike Beacon as well as PowerShell and Accessibility exploits. They have also used bootkits and rootkits to establish persistence in physical memory before the operating system loads. The group often initially installs its backdoors to a temp file and creatively names its files and domains to appear to be connected with legitimate antivirus programs.

APT 41 escalates privileges with similarly diverse tactics. They might run a brute force attack and use keylogging or the Sticky Keys exploit to remove access or abuse network shares. They use Windows Credential Editor or Mimikatz to obtain login credentials from LSSAS memory.

Repurposing APT39 Controls

Goodcorp's experience defending against APT39 at its travel subsidiary is valuable, as the two groups share many tactics, and all controls used to protect against APT39 should be implemented at Gamecorp.

However, APT41 is a more experienced and sophisticated operator; additional measures are required. In particular, APT41 is known to use administrator tools to install services and evade detection by using bootkits and DLL sideloading into legitimate processes. They dump credentials using Mimikatz or Windows Credential Editor and may exfiltrate data via FTP. Below is a list of defensive strategies against APT41. It does not include defensive actions against APT39, as Gamecorp can leverage our subsidiary’s experience.

Defensive Strategies: APT41

- Ensure all systems are current with updates and patches
- Remove or update unused dependencies, unmaintained or previously vulnerable dependencies, and unnecessary features
- Monitor for abnormal processes spawning from a potentially exploited application and look for anomalous behavior of browser or Office processes that might indicate website compromise
- Collect authentication logs, analyze for unusual access patterns, and follow best practices for detecting adversary use of valid accounts for authenticating to remote services
- Use multi-factor authentication and refer to NIST guidelines when creating passwords
- Use Trusted Platform Module technology and a secure boot process to prevent compromise of system integrity
- Turn off UAC's privilege elevation for standard users
- Enable LSSAS as a protected process to prevent credential dumping
- Implement the MimiKatz’s developer’s Yara rule to detect the application (see Appendix for link)
- Monitor command executions and WMI processes; consider using application control to block execution of wmic.exe and disallowing all users remote connection to WMI

- Ensure proper permissions are set for Registry hives to prevent users from modifying keys for system components that may lead to privilege escalation
- Enable Safe DLL Search Mode and disallow loading of remote DLLs
- Make the environment variables associated with command history read-only to preserve the history
- Automatically forward events to a log server or data repository to prevent manipulation of Windows Event Logs
- Test software and updates before deployment while taking note of potentially suspicious activity and verify distributed binaries through hash checking or other integrity-checking mechanisms
- Enable Attack Surface Reduction rules to block ransomware files
- Monitor network data for abnormal inbound/outbound patterns
- Ensure that frequent backups are tested and stored securely off-site

Technical References

CVE-2012-0158

CVE-2015-1641

CVE-2017-0199

CVE-2017-11882

CVE-2019-3396

Detailed Analysis on APT41 https://content.fireeye.com/apt-41/rpt-apt41

Mimikatz Yara Rule written by the developer:
https://github.com/gentilkiwi/mimikatz/blob/master/kiwi_passwords.yar

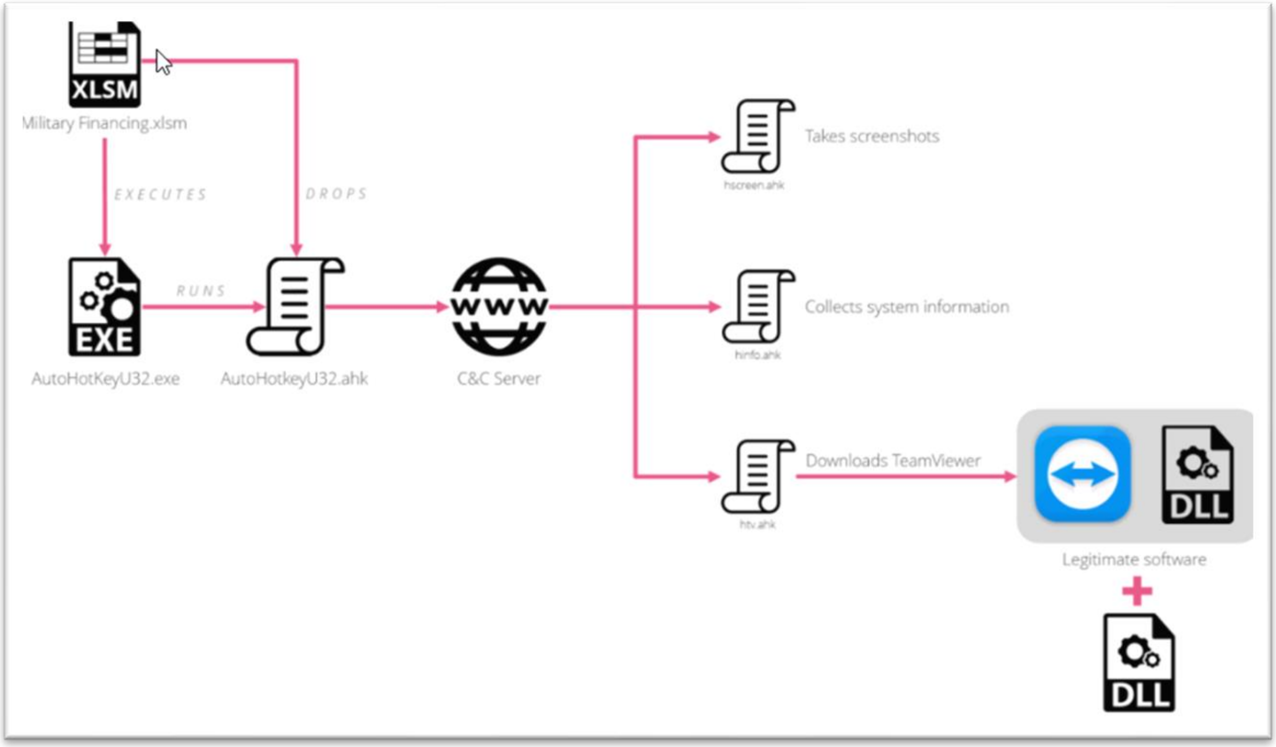
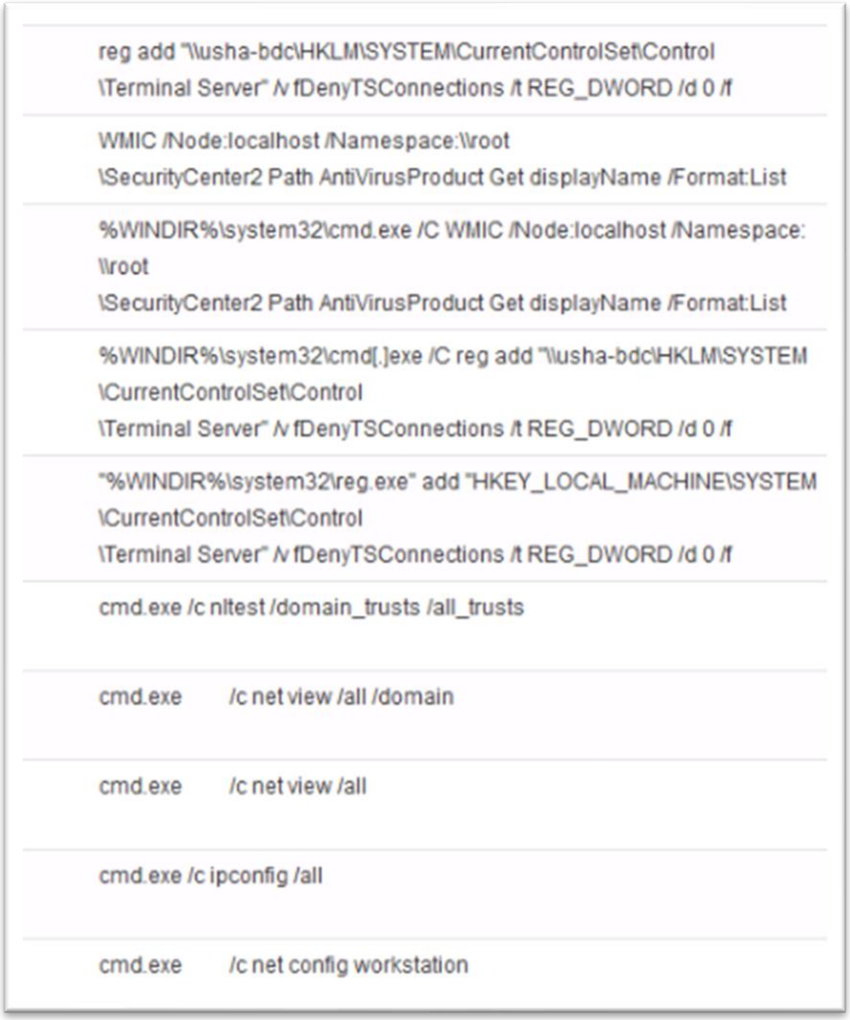


Figure 1. APT41's previous use of malicious attachments delivered via TeamViewer to infect legitimate software



```
reg add "\\usha-bdc\HKLM\SYSTEM\CurrentControlSet\Control
\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f

WMIC /Node:localhost /Namespace:\\root
\SecurityCenter2 Path AntiVirusProduct Get displayName /Format:List

%WINDIR%\system32\cmd.exe /C WMIC /Node:localhost /Namespace:
\\root
\SecurityCenter2 Path AntiVirusProduct Get displayName /Format:List

%WINDIR%\system32\cmd[.]exe /C reg add "\\usha-bdc\HKLM\SYSTEM
\CurrentControlSet\Control
\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f

"%WINDIR%\system32\reg.exe" add "HKEY_LOCAL_MACHINE\SYSTEM
\CurrentControlSet\Control
\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f

cmd.exe /c nltest /domain_trusts /all_trusts

cmd.exe       /c net view /all /domain

cmd.exe       /c net view /all

cmd.exe /c ipconfig /all

cmd.exe       /c net config workstation
```

Figure 2 Some Possible Cobalt Strike Beacon Commands

--End--