ORNA™

Cybersecurity Advisory

Dear ORNA Customer,

We are sending you this advisory to provide situational awareness about the Chinese State Sponsored threat group **APT41** an identified increase in targeted attacks across our customer sector landscape.

Summary

APT41, also known by aliases such as **Barium**, **Wicked Panda**, and **Winnti**, has been active since at least 2007 and is known for its dual-role operations that combine state-sponsored espionage with financially motivated intrusions.

Recently, **APT41** has intensified its cyber operations, targeting multiple sectors including shipping and logistics, media and entertainment, technology, and automotive in countries such as Italy, Spain, Taiwan, Thailand, Turkey, and the United Kingdom. This sustained campaign, ongoing since 2021, has seen **APT41** successfully infiltrate and maintain unauthorized access to numerous networks, allowing for the extraction of sensitive data over extended periods.

Timeline

- **August 2021:** TrendMicro documented the use of StealthVector by APT41, describing it as a shellcode loader used to deliver Cobalt Strike Beacon and the shellcode implant named ScrambleCross (aka SideWalk).
- **May 2022:** APT41 compromised at least six U.S. state government networks by exploiting vulnerable internet-facing web applications.
- **2023:** APT41 infiltrated multiple organizations' networks, extracting sensitive data over extended periods using sophisticated malware and techniques.
- **2024:** Zscaler ThreatLabz discovered DodgeBox, an advanced version of StealthVector, which is used to load the backdoor MoonWalk.

Malware Capabilities

DUSTPAN / **DodgeBox**: Acts as a shellcode loader that decrypts and loads additional malware, establishes C2 communication, and evades detection using techniques such as call stack spoofing and DLL side-loading.

DUSTTRAP / **MoonWalk**: A multi-stage plugin framework capable of executing shell commands, capturing keystrokes and screenshots, gathering system information, and modifying the Windows Registry. It employs Windows Fibers for evasion and uses Google Drive for C2 communication.

Attack Methodology

- **Persistence:** Web Shells like ANTSWORD and BLUEBEAM are deployed for persistence.
- **Custom Droppers:** DUSTPAN (aka StealthVector) and DUSTTRAP (aka MoonWalk) are used for payload delivery and lateral movement.
- **Public Tools:** SQLULDR2 and PINEGROVE are used for data extraction and exfiltration.
- **C2 Communication**: Cobalt Strike Beacon and compromised Google Workspace accounts are used for C2 communication.

- **Data Exfiltration**: SQLULDR2 exports data from Oracle Databases, and PINEGROVE transmits data using Microsoft OneDrive.

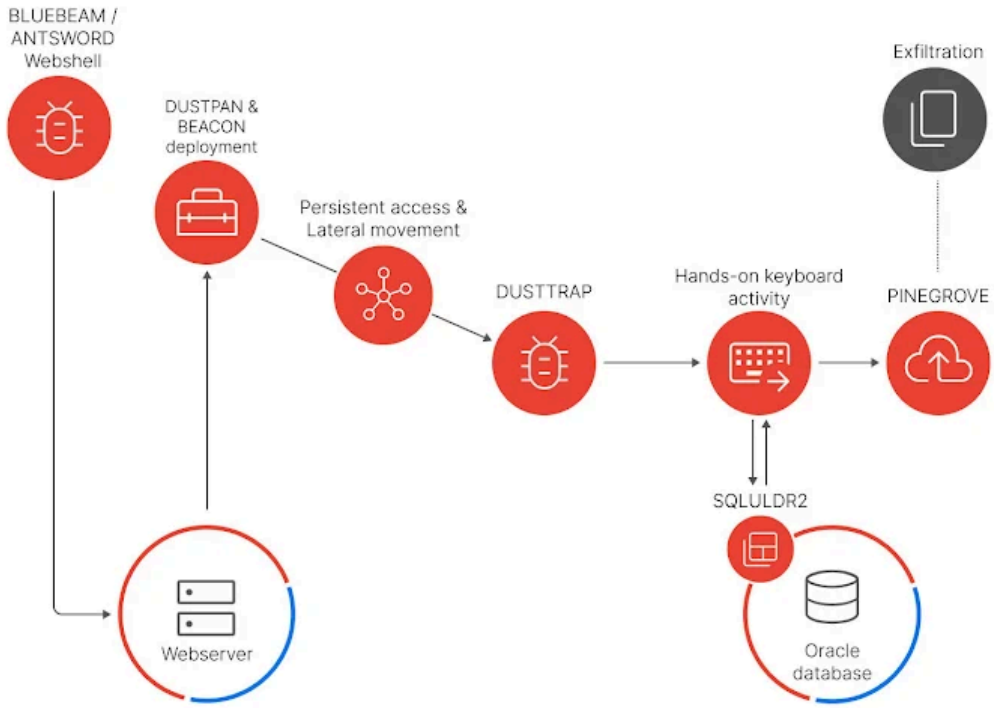

Image 1: Attack path.

Analysis Under Diamond Model

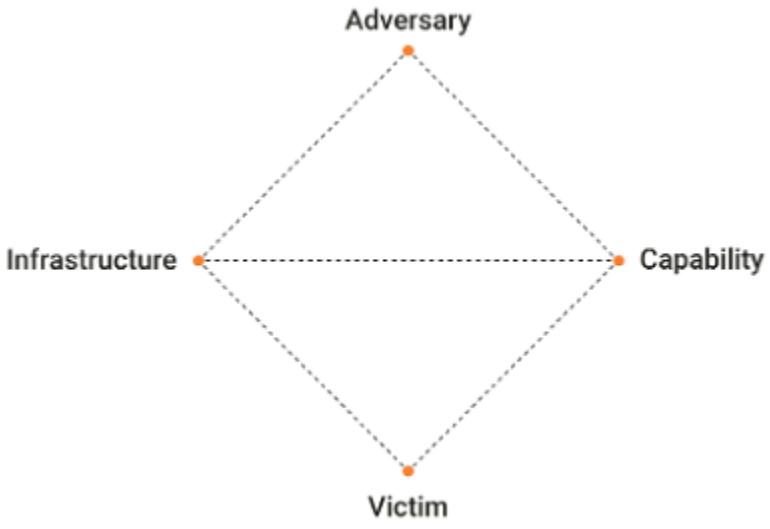

Image 2. Diamond Model.

- **Adversary**
    - **APT41** is a prolific and sophisticated threat actor known for combining state-sponsored espionage with financially motivated activities.
    - The group demonstrates advanced capabilities in exploiting vulnerabilities and orchestrating multi-stage cyber attacks.
    - Attribution: Tracked by numerous cybersecurity firms, including Mandiant and Google TAG, APT41 is suspected to be state-backed due to the resources and coordination required for their campaigns.
    - Origin: China.

- **Infrastructure**
    - Utilizes a complex and multi-tier C2 infrastructure, including compromised Google Workspace accounts and Microsoft OneDrive for data exfiltration.
    - Deploys ANTSWORD and BLUEBEAM web shells on compromised servers to maintain persistence and execute commands.
    - Utilizes compromised legitimate accounts and cloud services to blend malicious activities with regular traffic, enhancing operational security and avoiding detection.
    - Custom droppers DUSTPAN and DUSTTRAP.
    - Publicly available tools SQLULDR2 and PINEGROVE.

- **Capability**
    - **APT41** leverages a variety of techniques:
        - Exploiting public-facing applications
        - Using supply chain compromises
        - Employing web shells for persistence
        - Obfuscating files and using DLL side-loading for defense evasion
        - Dumping credentials and escalating privileges
        - Conducting detailed system and file discovery
        - Capturing input and screen data
        - Using C2 communications over HTTP/S and other protocols
    - Capable of executing arbitrary code, establishing persistent access, and conducting extensive data exfiltration.
    - Demonstrates proficiency in using sophisticated tools like ANTSWORD and BLUEBEAM web shells, DUSTPAN and DUSTTRAP droppers, and publicly available tools like SQLULDR2 and PINEGROVE.

- **Victim**
    - Organizations across various sectors, including shipping and logistics, media and entertainment, technology, and automotive industries, particularly in the U.S., U.K., Italy, Spain, Taiwan, Thailand, and Turkey, are targeted.

      .

Pyramid of Pain

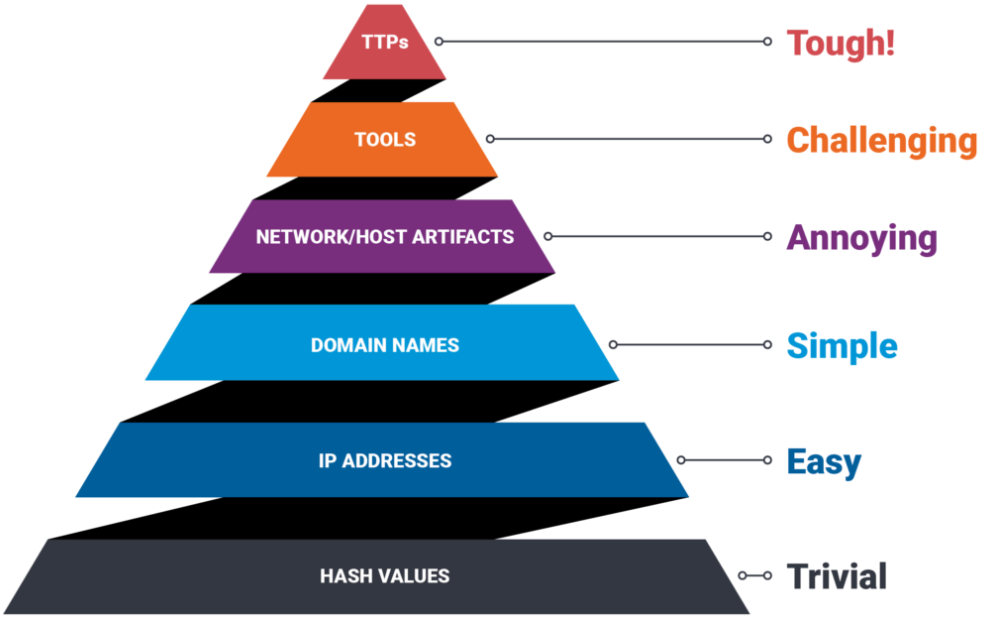

Image 3. Pyramid of Pain.

The Pyramid of Pain is a framework used to illustrate the increasing difficulty for an attacker when defenders detect and disrupt different types of indicators of compromise. The idea is that the higher an indicator is on the pyramid, the more it will frustrate and impact the attacker when it's detected or blocked. Lower-level indicators like hash values can be easily modified by attackers, while higher-level indicators such as their TTPs are much harder to change and cause greater disruption.

1. **Hash Values:** APT41 can frequently modify malware hash values, allowing them to bypass simple hash-based detection mechanisms.
    - Hashes from malware variants like DUSTPAN or DUSTTRAP can change quickly with each new build.
2. **IP Addresses:** APT41 can rotate and update IP addresses associated with their C2 infrastructure, limiting the effectiveness of IP-based blocking.
    - C2 infrastructure frequently relies on disposable IP addresses that can be swapped out as needed.
3. **Domain Names:** APT41 regularly registers new domain names for malicious activity. Blocking domains they use can be somewhat effective but requires continuous monitoring.
    - Domains used in their campaigns often reflect spoofed or newly created names to mask malicious intent.
4. .**Network/Host Artifacts:** These artifacts are more persistent and harder to modify, such as specific registry keys, file paths, or traffic patterns tied to malware execution.
    - Unique file paths and registry keys left behind by StealthVector or MoonWalk make these indicators useful for detection.
5. **Tools:** Disrupting APT41's toolset, such as custom malware or public hacking tools, can greatly increase the difficulty of continuing an attack.

- Key tools used by APT41 include DUSTPAN and DUSTTRAP, alongside publicly available tools like SQLULDR2.

6. **TTPs:** TTPs represent the overall strategies and methods used by APT41 in their attacks. When defenders target these, it causes significant disruption since modifying them requires rethinking their entire approach.
    - APT41 relies on techniques like deploying web shells for persistence and using DLL side-loading to evade defenses. These core behaviors are challenging to change quickly, making them the most impactful layer to target.

Initial Access

APT41 employs multiple initial access techniques to infiltrate their targets, often exploiting public-facing vulnerabilities or leveraging supply chain compromises. They are known for using the following techniques:

- **Exploiting Public-Facing Applications:** APT41 exploits vulnerabilities in internet-facing systems to gain access. For instance, they have targeted USAHerds and Log4j vulnerabilities in various campaigns.
    - MITRE ATT&CK ID: T1190 - Exploiting unpatched vulnerabilities in web applications or VPNs to gain initial access.

- **Supply Chain Compromise:** APT41 also compromises third-party software suppliers to distribute malware to targets, a tactic often used to gain access to multiple victims simultaneously.
    - MITRE ATT&CK ID: T1195 - Injecting malware into legitimate software updates to infiltrate organizations that use the compromised software.

By exploiting these vectors, APT41 gains initial footholds in networks and proceeds to escalate privileges, establish persistence, and move laterally.

MITRE ATT&CK Mapping

Tatic	Technique	ID	Description
Initial Access	Exploit Public-Facing Application	T1190	Exploiting vulnerabilities in internet-facing applications.
Initial Access	Supply Chain Compromise	T1195	Compromising third-party software to distribute malware.
Execution	Command and Scripting Interpreter	T1059	Using scripts and shell commands for execution.
Persistence	Web Shell	T1505.003	Deploying web shells like ANTSWORD and

			BLUEBEAM.
Persistence	Create Account	T1136	Creating new user accounts to maintain access.
Persistence	Boot or Logon Autostart Execution	T1547	Setting up persistence mechanisms that execute at boot/logon.
Privilege Escalation	Exploitation for Privilege Escalation	T1068	Exploiting vulnerabilities to gain higher privileges.
Defense Evasion	Obfuscated Files or Information	T1027	Using obfuscation techniques to avoid detection.
Defense Evasion	DLL Side-Loading	T1574.002	Loading malicious DLLs through legitimate executables.
Credential Access	Credential Dumping	T1003	Extracting credentials from memory, SAM, or LSASS.
Discovery	System Information Discovery	T1082	Gathering detailed system information.
Discovery	File and Directory Discovery	T1083	Exploring the file system to find sensitive data.
Lateral Movement	Remote Services	T1021	Using remote services like RDP or SMB for lateral movement.
Collection	Screen Capture	T1113	Capturing screenshots to gather information.
Collection	Input Capture	T1056	Capturing keystrokes and other input data.
Exfiltration	Exfiltration Over Web Service	T1567.002	Using web services like OneDrive for data exfiltration.
Command and Control	Application Layer Protocol	T1071	Communicating using protocols like HTTP/S.
Command and Control	Non-Application Layer Protocol	T1095	Communicating using lower-level protocols.

Indicators of Compromise

Web Shells: ANTSWORD, BLUEBEAM
Droppers: DUSTPAN (StealthVector), DUSTTRAP (MoonWalk)
Tools: SQLULDR2, PINEGROVE
C2 Infrastructure: Compromised Google Workspace accounts, Microsoft OneDrive
Exploits: Vulnerable internet-facing applications, zero-day vulnerabilities (e.g., USAHerds, Log4j)

Conclusion

APT41's recent activities demonstrate their continued capability to conduct sophisticated cyberattacks across multiple sectors and regions. Organizations must remain vigilant and adopt robust cybersecurity measures to protect against these persistent threats. The sharing of IOCs and threat intelligence is crucial in mitigating the impact of **APT41's** campaigns and safeguarding sensitive data.

Recommendations

Recommendation #1: Stay up do date

Stay informed through threat intelligence feeds and news updates on cyber attacks regarding APT41.

Recommendation #2: Multi Factor Authentication

Ensure that multiple forms of verification are required to access sensitive systems and data.

Recommendation #3: Conduct Regular Security Audits

Perform regular security assessments and audits to identify and remediate vulnerabilities.

Recommendation #4: Users Awareness

Conduct simulated attack scenarios to make sure that the employees are well aware of phishing and other risks, and also to make sure that they report the incident to the internal cybersecurity team.

Recommendation #5: Prepare for the Worst

ORNA strongly recommends that organizations ensure that all critical systems are backed up appropriately and that incident response plans are rehearsed regularly so that all participants understand their role.

References

1. The Hacker News: https://thehackernews.com/2024/07/chinese-apt41-upgrades-malware-arsenal.html https://thehackernews.com/2024/07/apt41-infiltrates-networks-in-italy.html
2. Cybernews: https://cybernews.com/security/chinese-apt41-back-in-action-compromising-companies/

If you have any additional questions, please reach out to your ORNA representative at sme@orna.app.

Sincerely,
ORNA Team