U.S. Justice Department Charges APT41 Hackers over Global Cyberattacks

By By: Trend Micro Sep 18, 2020 Read time: 4 min (1005 words)

Published: 2020-09-18 · Archived: 2026-04-05 17:55:03 UTC

On September 16, 2020, the United States Justice Department announced that it was charging five Chinese citizens with hacking crimes committed against over 100 institutions in the United States and abroad. The global hacking campaign went after a diverse range of targets, from video game companies and telecommunications enterprises to universities and non-profit organizations. The five individuals were reportedly connected to the hacking group known as APT41. At the time of writing, they remain fugitives, but two Malaysian citizens have been arrested for aiding the hackers.

Three related indictments unsealed by the Justice Department laid out the group's wide range of malicious activities, including crypto-jacking and ransomware attacks. Most of the activities appear to have been done for profit, but some were for espionage purposes.

Justice officials say that the group's intrusions allowed the hackers to steal source code, customer account data, and personally identifiable information (PII). Other notable activities include defrauding video game companies by manipulating in-game resources, and launching a ransomware attack on the network of a non-profit organization dedicated to combating global poverty.

The hackers used publicly available exploits and common vulnerabilities, which are listed in the official report. They also employed sophisticated hacking techniques to gain and maintain access to the victim's computer networks. The official report outlined how the team used "supply chain attacks" in which they compromised software providers and modified the code they were giving their customers. This also allowed the threat actors to compromise the customers and spread their influence further.

This is not the first time that APT41 activities have been scrutinized — the group has been active for some time. Just last May, Trend Micro connected the group to ransomware attacks on Taiwanese organizations. The new ransomware family, which we dubbed ColdLock, is potentially destructive as it appears to target databases and email servers for encryption.

The attack chain of ransomware incidents in Taiwan

The Trend Micro Research team investigated the ColdLock ransomware attack, which actually targeted the energy industry in Taiwan. The ransomware attack chain is outlined in Figure 1; however, we currently do not know the initial arrival vector of this threat into a potential victim's network. Our analysis focused on the way the attacker spreads the ransomware to infect as many machines as possible.

1. The threat actor enters a victim's network environment and obtains the account username and password of the company headquarters' active directory server.

2. After logging in to the active directory server, the threat actor modifies the active directory server group policy object — this includes a request that all domain account members create a scheduled task and execute the malware.
3. In the final step, the other subsidiary active directory servers and all the endpoint machines will download the scheduled task and execute the ransomware.

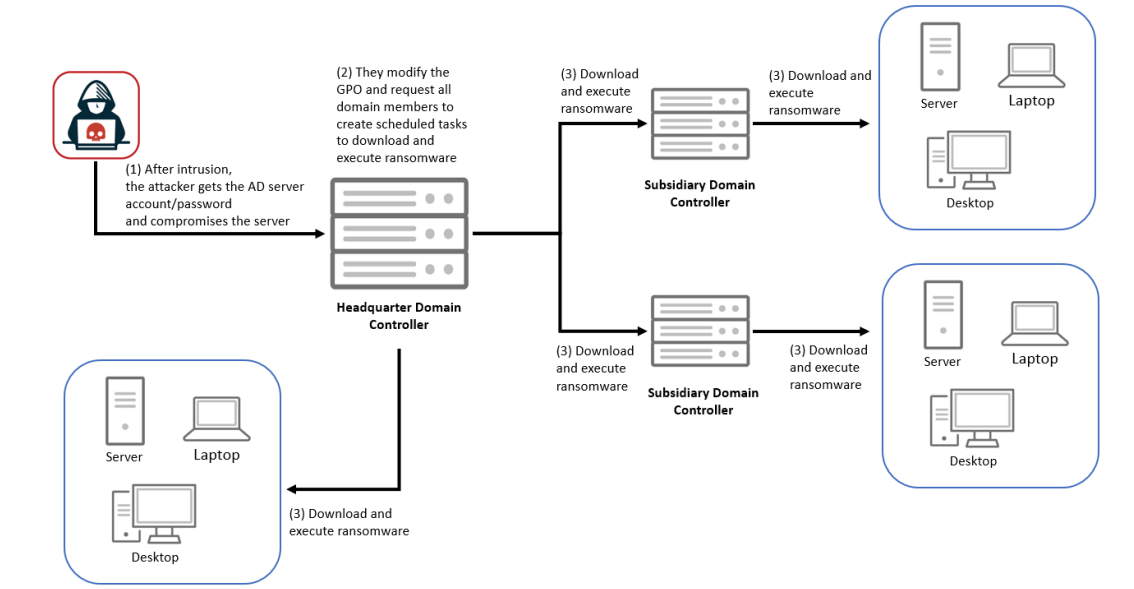

Figure.1 The attacker uses an Active Directory (AD) scheduled task to deploy the ransomware in the customer environment.

Scheduled tasks play a very important role in this incident. The threat actors use a scheduled task command to spread and infect a victim's environment. The screenshot in Figure 2 shows how the threat actor uses SMB and internal IIS Web Service to copy "lc.tmp" (the main ransomware loader in this incident) to other victims' host machines. After that, the PowerShell command executes the main ransomware loader.

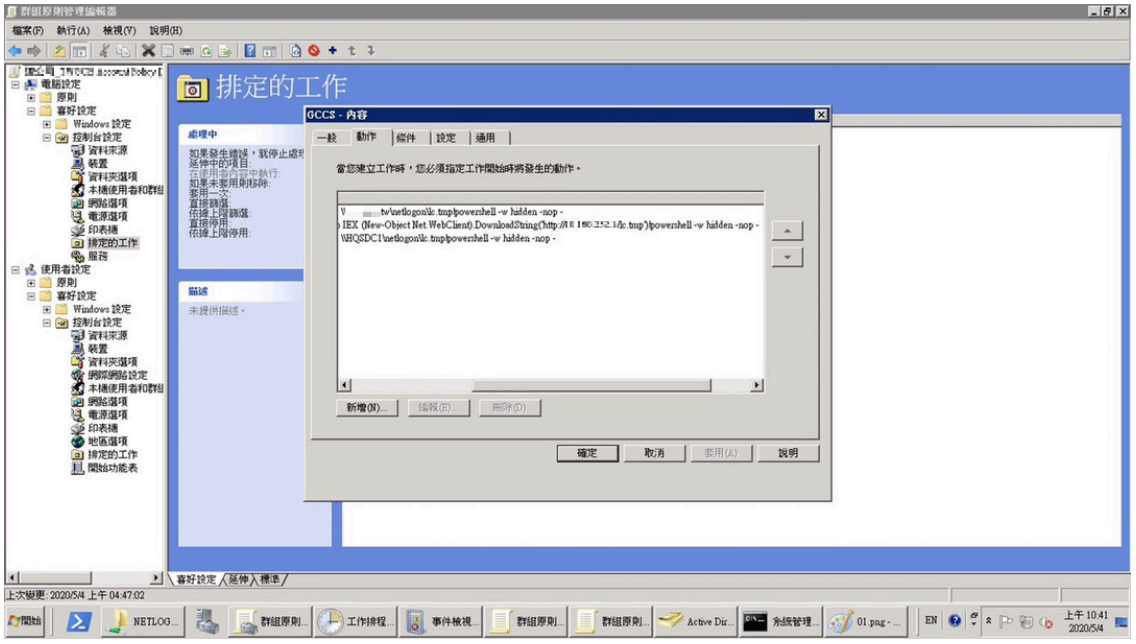

Figure 2. How a scheduled task delivers the malware to a victim's environment

The right tool for the job

Before the ransomware attack, the attacker was likely already hiding in the victims' environments for some time. We found the same customized loaders installed as Windows services in every victim's environment, and those infected machines were in positions that allowed them to reach other machines under the subnets.

The loaders decrypted the next-stage payloads, which were either embedded inside itself or stored on the disk as separate files. The next-stage payloads were CobaltStrike in this series of incidents. After the loader and payload pairs were successfully installed, the attacker started poking around the environments with tools like password dumpers and HTTP tunneling tools — then the ransomware attacks were launched one month later.

More than just a single occurrence

During the investigation, we discovered more incidents that are possibly related to the one discussed above. We did this by checking the indicator overlap and the C&C infrastructure overlap. Based on the distribution of the linked indicators, the attacker(s) appears to be interested in energy, retail, and telecom companies, mainly in Southeast Asia. They mostly conduct espionage activities — lurking in the environments for a long period and packing the data that interested them. They also seem to be updating the backdoors and toolsets they use.

Possible link to Chinese espionage

The C&C server 104[.]233[.]224[.]227 was hosted under a small hosting service with only 64 IPs under it. The IP range was registered to an address in Inner Mongolia, China. The C&C server was abandoned several days after the incidents, and now the IP is hosting a Simplified-Chinese site.

Trend Micro Solutions

Sophisticated hacking groups have versatile tools and are persistent threats. Users should deploy more robust and proactive defenses to be adequately protected against these groups. The following Trend Micro Solutions are recommended:

- Trend Micro XDR for Users: Applies AI and analytics for earlier detection of threats across endpoints and other layers of the system
- Trend Micro Apex One™: Provides actionable insights, expanded investigative capabilities, and centralized visibility across the network.
- Trend Micro™ Deep Discovery™ Email Inspector: Detects, blocks, and analyzes malicious email attachments through custom sandboxing and other detection techniques

To help defend users against APT41 specifically, we have developed an assessment tool that can scan endpoints for file-based indicators collected from global intelligence sources.

Indicators of Compromise

SHA-1	*Malware Family*

2367326f995cb911c72baadc33a3155f8f674600	NTDSDump
75e49120a0238749827196cebb7559a37a2422f8	COLDLOCK
5b9b7fb59f0613c32650e8a3b91067079bcb2fc2	COLDLOCK
e7aa8f55148b4548ef1ab9744bc3d0e67588d5b7	COLDLOCK
ad6783c349e98c2b4a8ce0b5c9207611309adca7	COBALTSTRIKE
29cc0ff619f54068ce0ab34e8ed3919d13fa5ee9	COLDLOCK
2051f0a253eced030539a10ebc3e6869b727b8a9	COLDLOCK
a2046f17ec4f5517636ea331141a4b5423d534f0	COLDLOCK
03589dffe2ab72a0de5e9dce61b07e44a983d857	COBALTSTRIKE
9d6feb6e246557f57d17b8df2b6d07194ad66f66	COLDLOCK
28d172e374eebc29911f2152b470528fc695662e	PWDDUMPER
574fb6a497c032f7b9df54bc4669d1eb58d78fb4	ASPSHELL

*One of the sources for this table is the original report from the U.S. Justice Department

Tags
