APT41 Resurfaces as Earth Baku With New Cyberespionage Campaign

By Ted Lee (words)

Published: 2021-08-24 · Archived: 2026-04-06 00:52:39 UTC

We have uncovered a cyberespionage campaign being perpetrated by Earth Baku, an advanced persistent threat (APT) group with a known history of carrying out cyberattacks under the alias APT41. This is not the group’s first foray into cyberespionage, and its long list of past cybercrimes also includes ransomware and cryptocurrency mining attacksopen on a new tab.

Earth Baku deploys its ongoing campaign, which can be traced to as far back as July 2020, through multiple attack vectors that are designed based on different exploits or the infrastructure of its targeted victim's environment:

- • SQL injection to upload a malicious file
- • Installment through *InstallUtil.exe* in a scheduled task
- • Possibly a malicious link (LNK) file sent as an email attachment
- • Exploitation of the ProxyLogon vulnerability CVE-2021-26855 to upload a China Chopper web shell

This campaign uses previously unidentified shellcode loaders, which we have named StealthVector and StealthMutant, and a backdoor, which we have dubbed ScrambleCross. Earth Baku has developed these new malware tools to facilitate targeted attacks on public and private entities alike in specific industries that are located in the Indo-Pacific region. Thus far, the affected countries include India, Indonesia, Malaysia, the Philippines, Taiwan, and Vietnam.

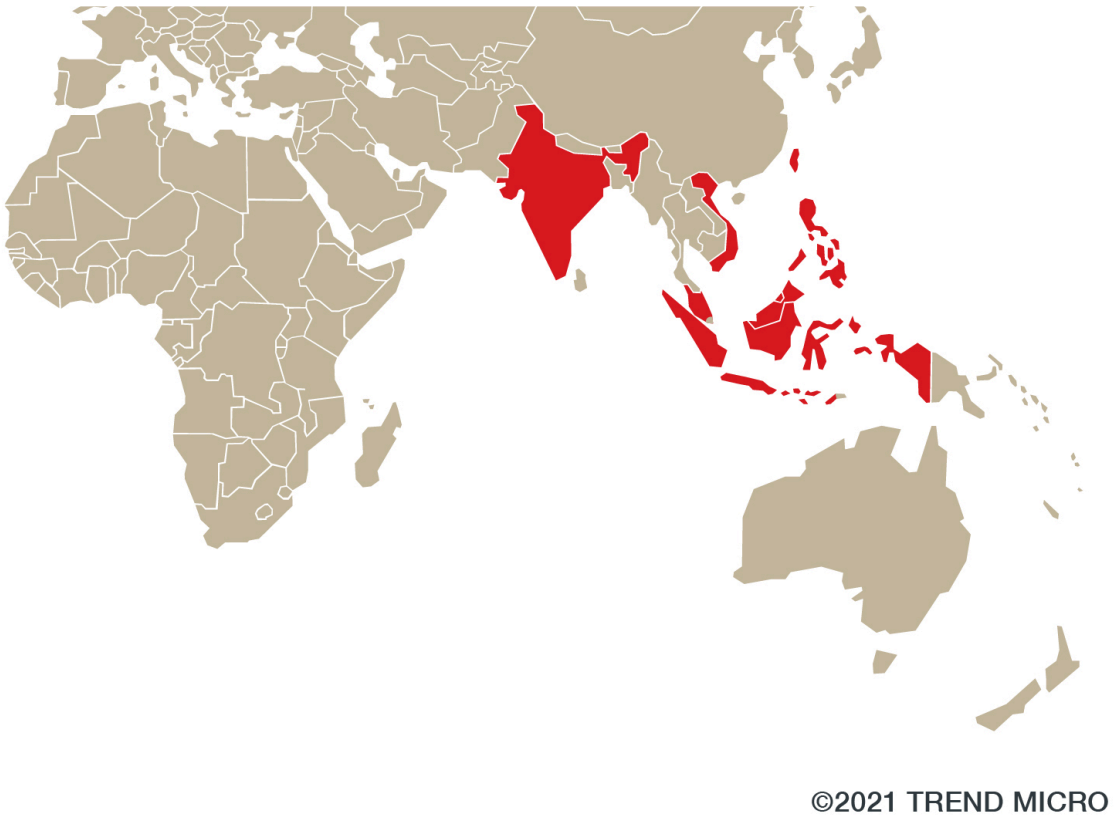

Figure 1. Countries affected by Earth Baku's new campaign

Source: Trend Micro™ Smart Protection Network™ infrastructure

StealthVector

We initially observed StealthVector, a shellcode loader written in C/C++, in October 2020. StealthVector is designed with various configurable features that make it easy for malicious actors to modify and tailor it to their needs, including a feature that disables Event Tracing for Windows (ETW), allowing the malware to run in stealth mode. This loader can stealthily run its payload in various ways, such as using the *CreateThread* function, bypassing Microsoft's Control Flow Guard (CFG), module stomping, and phantom dynamic link library (DLL) hollowing.

StealthMutant

Like StealthVector, StealthMutant, which supports both 32-bit and 64-bit operating systems, can disable ETW. This loader, written in C#, has been used by malicious actors since July 2020. Many of the StealthMutant samples we have analyzed use AES-256-ECB for decryption; alternatively, an earlier variant of the loader uses XOR. After its payload is decrypted, StealthMutant performs process hollowing to execute its payload in a remote process.

ScrambleCross

Both StealthMutant and StealthVector contain a payload of either the Cobalt Strike beacon or ScrambleCross, a newly discovered backdoor. ScrambleCross receives instructions from its command-and-control (C&C) server that allow it to receive and manipulate plug-ins. However, we have yet to retrieve and study one of these plug-ins. It has many of the same capabilities as another backdoor, Crosswalk, which has also been used by Earth Baku. For example, both calculate the hash of the code section as an anti-bugging technique, both are designed as fully position-independent code, and both support various kinds of network communication protocols.

Connections to other campaigns

Earth Baku's recent activities are related to another campaign that has been active since at least November 2018, as reported by FireEyeopen on a new tab and Positive Technologiesopen on a new tab. While the older campaign uses a different shellcode loader, which we have named LavagokLdr, we have observed similar code and procedures between LavagokLdr and StealthVector. In the same vein, we have observed that LavagokLdr's payload, Crosswalk, and one of StealthVector's payloads, ScrambleCross, perform similar techniques for decryption and signature checking. But because Earth Baku has updated its toolset with StealthVector, StealthMutant, and ScrambleCross for this new campaign, we have identified it as its own separate operation.

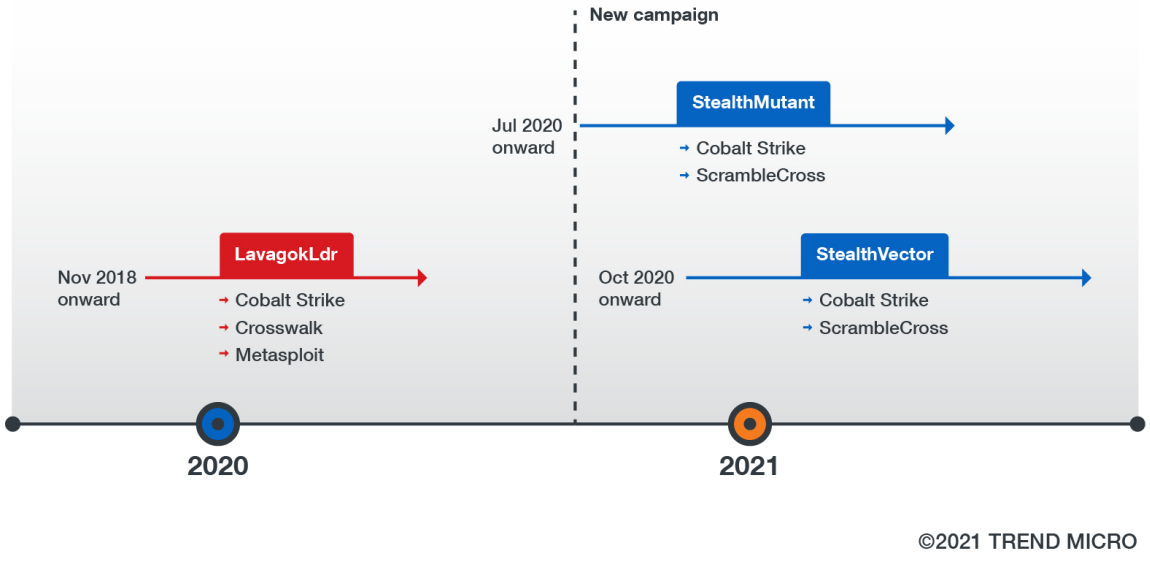

Figure 2. A timeline of Earth Baku's previous campaign as APT41 and its new campaign

How Earth Baku creates its malware tools

Earth Baku is known for its use of self-developed toolsopen on a new tab. To continue doing so, it appears to be filling its ranks with malicious actors who are pooling their diverse skills. Interestingly, the new malware tools involved in Earth Baku's new campaign indicates that the APT group has likely recruited members who specialize in low-level programming, software development, and red-team techniques.

For more details about Earth Baku's new campaign, read our research paper "Earth Baku: An APT Group Targeting Indo-Pacific Countries With New Stealth Loaders and Backdoor."open on a new tab

---