A Dive into Earth Baku's Latest Campaign

⋮ 8/9/2024

APT & Targeted Attacks

Earth Baku has broadened its scope from the Indo-Pacific region to Europe, the Middle East, and Africa. In this blog entry, we examine the threat actor's latest tools, tactics, and procedures.

By: Ted Lee, Theo Chen August 09, 2024 Read time: 6 min (1512 words)

Summary

- Earth Baku (a threat actor associated with APT41) has expanded its activities beyond the Indo-Pacific region to Europe, the Middle East, and Africa — targeting countries like Italy, Germany, UAE, and Qatar, with suspected threat activity in Georgia and Romania.
- The group uses public-facing applications such as IIS servers as entry points, deploying advanced malware toolsets such as the Godzilla webshell, StealthVector, StealthReacher, and SneakCross.
- StealthVector and StealthReacher are customized loaders that deploy backdoor components while employing techniques such as AES encryption and code obfuscation for stealth. SneakCross, the group's latest backdoor, uses Google services for command-and-control (C&C) activities and boasts a modular design for easer updates.
- During post-exploitation, Earth Baku uses tools like a customized iox tool, Rakshasa, and Tailscale to maintain persistence, along with MEGAcmd for data exfiltration.

Earth Baku, an advanced persistent threat (APT) actor that we previously wrote about in 2021, has expanded its activities to Europe, the Middle East, and Africa (MEA) beginning late 2022. The group has updated its tools, tactics, and procedures (TTPs) in more recent campaigns, making use of public-facing applications such as IIS servers as entry points for attacks, after which they deploy sophisticated malware toolsets on the victim's environment, including the loaders StealthVector and StealthReacher, and the modular backdoor SneakCross.

Victimology

Initially targeting the Indo-Pacific region with their earlier campaigns, Earth Baku started expanding their presence to Europe, the Middle East, and Africa, which includes countries such as Italy, Germany, UAE and Qatar. Furthermore, we also observed connections to the threat actor's infrastructure originating from Georgia, and multiple malware toolsets uploaded from Romania. Hence, we think these two countries are also likely under threat as well. Figure 1 shows all the regions which we believe are potentially under threat from Earth Baku.

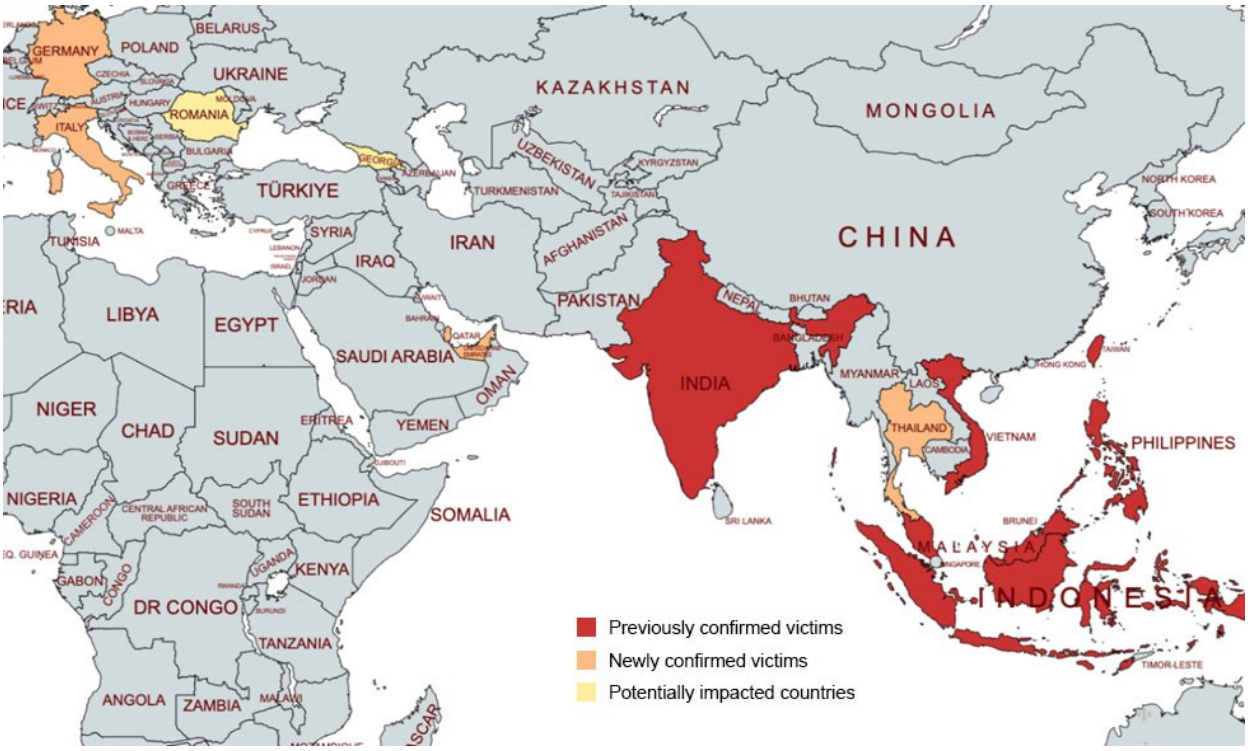

Figure 1. Map chart for Earth Baku's scope of potential impact
download

Based on our investigation, the targeted sectors included the following:

- Government
- Media and Communications
- Telecom
- Technology
- Healthcare
- Education

Infection Vector

In the group's recent operations, Earth Baku's attacks exploited public-facing applications, specifically IIS servers, as an entry point for attacks. Once the perpetrators gain access, they deploy the Godzilla webshell, which allows them to maintain control over the compromised server. Through Godzilla, Earth Baku is then able to deploy the shellcode loader StealthVector and its backdoor components, Cobalt Strike, and a new backdoor named SneakCross.

During the post-exploitation stage, Earth Baku will attempt to build reverse tunnels to maintain control access by using publicly available reverse tunneling tools. In addition, we observed MEGAcmd tool being deployed into the victim's environment, likely for data exfiltration.

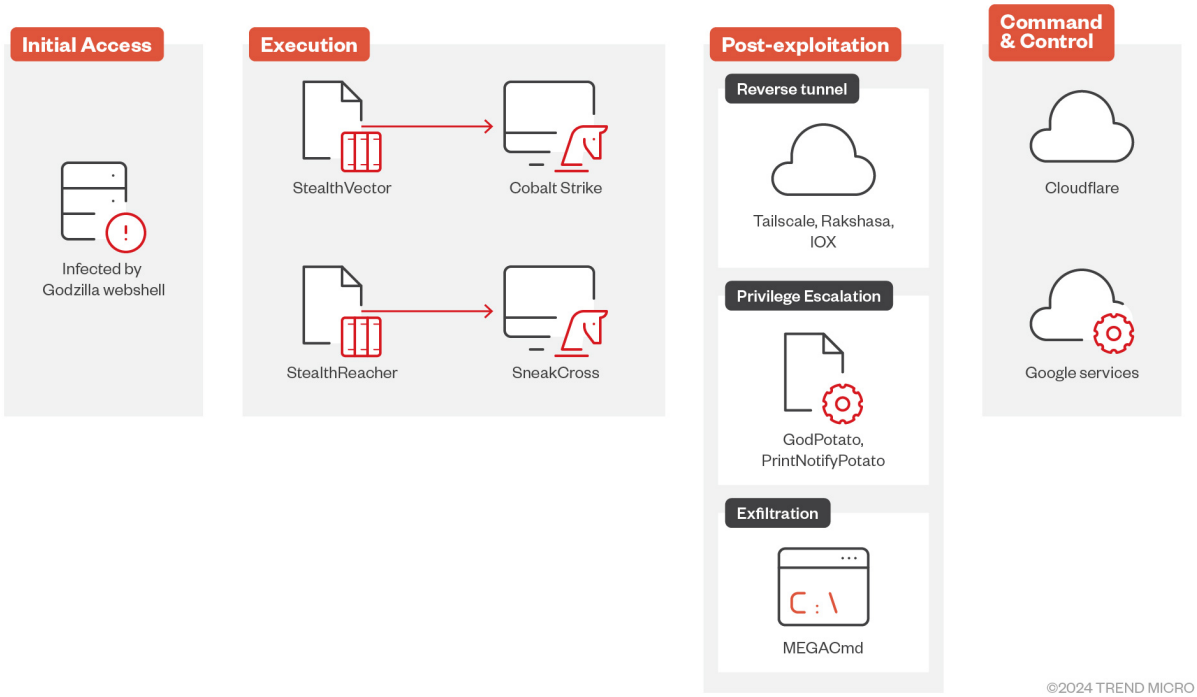

Figure 2. The infection vector of recent campaigns
download

Technical Analysis

Loader: StealthVector and StealthReacher

StealthVector is a customized backdoor loader used to launch Earth Baku's backdoor components in stealth mode. This year, we observed Earth Baku adding two new loaders to launch its backdoor components: CobaltStrike and SneakCross (aka MoonWalk).

New StealthVector

The new StealthVector is very similar to the one found in 2021. Although it has changed little in terms of configuration structure, it now uses AES as its encryption algorithm instead of customized ChaCha20. In some variants, we also observed a code virtualizer being used for code obfuscation, making the malware more difficult to analyze. It also inherited other defense evasion techniques to make sure the backdoor components were executed stealthily.

- **ETW and CFG Disable:** Disabling Event Tracing for Windows (ETW) and Control Flow Guard (CFG) to mitigate footprint and avoid detection.
- **DLL Hollowing:** StealthVector will import a legitimate DLL from the System32 folder and inject malicious code into the section of the legitimate DLL file.

Figure 3. Obfuscated main function by code virtualizer

StealthReacher

StealthReacher (aka DodgeBox) can be considered as an enhanced variant of StealthVector, featuring code obfuscation techniques such as *FNV1-a* and other defense evasion mechanisms. Compared to the older StealthVector, it uses AES algorithms for encryption and MD5 hashing for *checksum*. Based on our observations, StealthReacher is the specified loader to launch the new modular backdoor, SneakCross.

It's noting that both StealthVector and StealthReacher will perform re-encryption after the first initiation via XOR encryption, with the key being the victim's computer name. From a digital forensics' aspect, it is

challenging to decrypt and analyze the collected payload even though all the components (loader and payload) were collected at the same time.

Backdoor: SneakCross

SneakCross is a new modular backdoor that uses Google services for its command-and-control (C&C) communication. It employs Windows Fibers to evade detection from network protection products and EDR solutions. We believe it to be the successor to their previous modular backdoor, ScrambleCross, which was mentioned in our previous report. The modular design allows attackers to easily update its capabilities, modify its behavior, and customize functionality for different scenarios.

In Google Cloud's report, they mentioned that they successfully found at least 15 plugins that support various backdoor functions including:

- Shell Operations
- File System Operations
- Process Operations
- Network Probing
- Network Store Interface Operations
- Screen Operations
- System Information Discovery
- File Manipulation Operations
- Keylogger
- Active Directory Operations
- File Uploader
- RDP
- DNS Operations
- DNS Cache Operations
- Registry Operations

Post-Exploitation routine

During the post-exploitation stage, Earth Baku will deploy various tools on the victim's environment for persistence, privilege escalation, discovery and exfiltration. In this section, we 'll examine the most noteworthy of these tools.

Persistence: reverse-tunnel

We found the threat actors attempting to build reverse tunnels with the following tools for persistent control access to compromised machines:

Customized iox tool

The perpetrators built their own *iox tunneling tool* based on its public source code. Changes include simplified required arguments (local IP/Port) and an additional special argument *-ggg*. To launch the tool, the user needs to input this special argument, after which the tool works properly.

Rakshasa

Rakshasa is a powerful proxy tool written in Go, designed specifically for multi-level proxying and internal network penetration.

Tailscale

Tailscale is a Virtual Private Network (VPN) service created to enable secure connectivity between devices within a unified virtual network. Recently, we have identified threat actors attempting to incorporate compromised systems into their virtual networks using the Tailscale platform. Additionally, these threat actors have been using legitimate Tailscale servers as intermediaries, significantly complicating the process of tracing the origins of their activities.

Exfiltration

Within the victim's environment, we found many MEGAcmd tools dropped onto infected machines. MEGAcmd is a command-line tool used for interacting with the MEGA cloud storage service. We infer that the threat actors attempted to use this tool for exfiltrating stolen data to MEGA, hoping to capitalize on its ability to efficiently upload large volumes of data. This procedure was also observed with an associated group, Earth Lusca.

Conclusion

Earth Baku has significantly expanded its reach from the Indo-Pacific to Europe and MEA since late 2022. Their recent operations showcase advanced techniques, including the use of public-facing applications like IIS servers for initial access and the deployment of the Godzilla webshell for control. The group has employed new loaders such as StealthVector and StealthReacher, to stealthily launch backdoor components, and added SneakCross as their latest modular backdoor. Earth Baku also used several tools during its post-exploitation including a customized iox tool, Rakshasa, TailScale for persistence, and MEGAcmd for efficient data exfiltration. These developments underscore Earth Baku's evolving and increasingly sophisticated threat profile, which can potentially pose significant challenges for cybersecurity defenses.

Recommendations

To defend against cyberespionage tactics and minimize the risk of compromise, both individual users and organizations implement the following best practices:

- **Implementing the principle of least privilege:** Restricting access to sensitive data and closely monitoring user permissions makes it more challenging for attackers to move laterally within a corporate network.
- **Addressing security gaps:** Regularly updating systems and applications and enforcing strict patch management policies allows organizations to address security gaps within their system. Furthermore, employing virtual patching can help secure legacy systems for which patches are unavailable.

- **Developing a proactive incident response strategy:** Deploying defensive measures designed to identify and mitigate threats in the event of a breach, and conducting regular security drills improves the effectiveness of an organization’s incident response plan.
- **Adopting the 3-2-1 backup rule:** Maintaining at least three copies of corporate data in two different formats, with one air-gapped copy stored off-site ensures that data remains intact even in the event of a successful attack. Regularly updating and testing these backups helps ensure the integrity of the data.

Trend solutions

Organizations looking to defend themselves from sophisticated attacks can consider powerful security technologies such as Trend Vision One™, which allows security teams to continuously identify attack surfaces, including both known and unknown, plus managed and unmanaged cyber assets.

It assists organizations in prioritizing and addressing potential risks and vulnerabilities by evaluating critical factors, such as the likelihood and impact of possible attacks, providing a comprehensive set of prevention, detection, and response capabilities, all supported by advanced threat research, intelligence, and AI. Vision One enhances an organization's overall security posture and effectiveness, offering robust protection against all types of attacks.

Indicators of Compromise

The indicators of compromise for this entry can be found here.