Earth Preta’s Cyberespionage Campaign Hits Over 200

By Trend Micro (words)

Published: 2023-03-27 · Archived: 2026-04-06 03:09:20 UTC

We used a qualitative approach to identify the collection requirements, methods, and objectives of the operational groups and their respective places in the organization. We established links between the operational threat groups by grouping overlaps in victimology and identifying core indicators, such as implants or payloads.

Case studies

Overlaps

Throughout our investigation, we observed several instances where victims were compromised by two groups simultaneously, indicating possible overlaps in collection requirements between these groups. While there are no indications of overlaps in individual devices, there are strong indications of targets intersecting, suggesting these groups are pursuing similar objectives. Additionally, the overlaps among victims indicate a lack in targeting coordination and/or planning within the overall groups' leadership or management.

These targeting overlaps have been observed in multiple groups, such as Groups 724, 1358, and 5171. Since these groups operate across a variety of sectors, it is likely that the overlap in collection requirements is the result of similar objectives rather than coordination between the toolset and collected materials. However, we have not been able to identify any evidence of coordination between these groups or a shared toolset.

Infection and exfiltration vectors

Group 5171's exfiltration methods are sophisticated and designed to avoid detection. Several victims in key countries, such as Singapore, Vietnam, Netherlands, Ghana, and Myanmar, have indications of files exfiltrated via a dedicated USB mass storage device. For instance, in January 2023, a device from Vietnam loaded the Adobe CEF Helper under the path <*C:\Users\XXX\AAM UpdatesXXX\AAM Updates.exe*> and exfiltrated documents to drive F:. The same device also carried out another collection in December 2022, where data was copied from folder <*C\:$RECYCLE.BIN\S-XXXXX$XXXH.pdf*>, indicating that the user deleted the collected data.

Roaming endpoint attacks

In contrast to Group 5171, Group 1358’s uses malicious USB mass storage devices as its primary method of compromise. Our analysis indicated that toward the end of 2022 and early 2023, all documented intrusions from Group 1358 used USB mass storage devices. In addition, there were multiple instances where initial compromise occurred while the assets of the target were roaming abroad through a technique known as the “traveling laptop attack.”

This mix of traditional intelligence trade craft and cyber techniques could mean that these groups have access to advanced resources and support from nation states, since such techniques are not typically available to

independent hackers. Moreover, this approach could signify the growing convergence of cyber- and physical security as cyberattacks continue to move beyond digital systems and into the physical world.

Operation groups

While this is not a comprehensive list, we summarize and attribute the operational functions to specific groups as contributing units to Earth Preta's cyberespionage activities and deployments. As we continue following this campaign and track its activities, these group names will be updated accordingly once analyses and attribution are confirmed.

Group 724

Group 724 is possibly related to Earth Preta. The group utilizes sideloading with Adobe CEF Helper to establish a persistent foothold in the user's home directory, employing a naming convention with one of the following patterns:

- AcroRD32XXX
- AAM UpdatesXXX
- AcrobatXXX
- Eset Malware ProtectionXXX

"XXX" denotes three random letters. The group uses a USB drive as an entry point into a target's system, indicating its preference for leveraging physical vectors for intrusion. This group is considered one of the most dangerous in the Southeast Asian region and has been known to target a myriad of organizations.

Group 724 also appears to be focused on compromising targets in specific industries and countries. The group has been observed targeting sectors such as finance, government, manufacturing, fabrication, construction, energy, transportation, air traffic, and food production. This targeted approach indicates that the group has developed a clear understanding of the vulnerabilities and high-value assets present in these industries. The significant level of proliferation suggests that it is well-funded and includes a large team of skilled individuals, likely enabling it to carry out attacks on multiple targets simultaneously.

The group uses customized USB storage devices tailored to individual targets as part of their intrusion tactics. These customized devices appear to be carefully crafted to bypass security measures and appear legitimate to the target. With this preference for a physical entry vector, the group can increase the chances of a successful intrusion and maintain its covert operations. This technique highlights the level of sophistication and planning that goes into Group 724's attacks.

Group 1358

Group 1358 is a highly sophisticated threat actor that employs advanced tactics and techniques to infiltrate and compromise a wide range of targets worldwide. The group has been observed utilizing Avast's WSC DLL for sideloading, a technique leveraging the Windows Management Instrumentation (WMI) service to execute malicious code. This group is potentially composed of several operating groups utilizing the same tools and techniques. Persistence is established at *ProgramData\AvastSvcXXX*, where "XXX" represents three random

letters. The group uses generic USB mass storage devices as an entry point, suggesting that they prioritize ease of access over customization.

This group's choice of malware is PlugX, an older and well-known remote access tool. Despite its age, PlugX remains an effective tool for threat actors due to its flexibility and evasion capabilities. The group's victimology is extensive, targeting organizations across various sectors globally. However, recent observations suggest that the group has shifted its collection efforts towards maritime-related information since December 2022. Targets have included shipping information, sea vessel movements, border and immigration control, export-related government agencies, food production, and humanitarian groups. While some of the targets are related to maritime research and development, most of the information we found as targeted pertain to operational maritime information, even to the extent of compromising specific vessels or tugboat companies.

Exfiltration methods utilized involve the use of USB sticks that are plugged in, enabling the PlugX tool to copy all collected data into a previously known and expected USB stick. This technique allows the group to remain undetected and avoid detection by traditional security measures.

Group 5171

Group 5171 is a threat actor that utilizes advanced techniques to infiltrate and compromise targets across the Middle East and Europe. The group uses DLL sideloading with Adobe CEF Helper and establishes persistence in the *RECYCLERS.BIN* folder. In addition, the group also employs USB-based data exfiltration as part of their tactics.

Group 5171 differentiates itself from other threat actors with their use of the travelling laptop attack. This technique involves infecting a laptop with malicious code in transit. Usually, the device will be travelling as part of a routine work travel and upon return to the origin country, a more elaborate exploitation and lateral movement can be initiated. This method allows the group to bypass traditional security measures and gain access to their targets undetected.

Sectoral targets of Group 5171 are spread out, indicating that the group does not focus on specific sectors but rather adopts a more opportunistic approach. However, observing victims' business verticals and sectors indicate that Group 5171's collection efforts show a high level of interest in research and development related to IT solutions, materials manufacturing and fabrication, energy production and synthetization, air travel, and space.

Conclusion

We deem the findings of this research on Earth Preta's cyberespionage operations have significant implications for international security and intellectual property. There are strong indications of intertwined traditional intelligence tradecraft and cyber collection efforts, indicative of a highly coordinated and sophisticated cyberespionage operation. We identified several distinct operational groups, each with unique TTPs and objectives, which reveals a highly specialized and organized cyberespionage operation.

This study also suggests that Earth Preta's cyberespionage operations have a broad reach and have the capacity to target high value targets. The shift in collection priorities toward intelligence regarding specific areas also indicates that Earth Preta is targeting critical infrastructure and key institutions that can affect national and international relations, economies, and securities.

Given the scale and sophistication of Earth Preta's cyberespionage operations, the international community needs to take proactive measures to defend against this significant threat. This includes robust cybersecurity measures, effective countermeasures against cyberespionage, and increased international cooperation in combating this threat. The international community must raise awareness on the threats posed by Earth Preta's cyberespionage operations, promote information sharing, and develop effective countermeasures. It is essential to have a coordinated response to this threat, with the support of the private sector, academia, and civil society, to ensure the safety and security of critical infrastructure and intellectual property.

Indicators of Compromise (IOCs)

For a list of the IOCs, download the appendix hereopen on a new tab.
