مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Earth Baxia Threat Campaign

Tracking #:432316309

Date:20-09-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed the threat actor group known as Earth Baxia has been observed executing sophisticated cyber-attacks targeting government organizations and critical sectors across the Asia-Pacific (APAC) region.

TECHNICAL DETAILS:

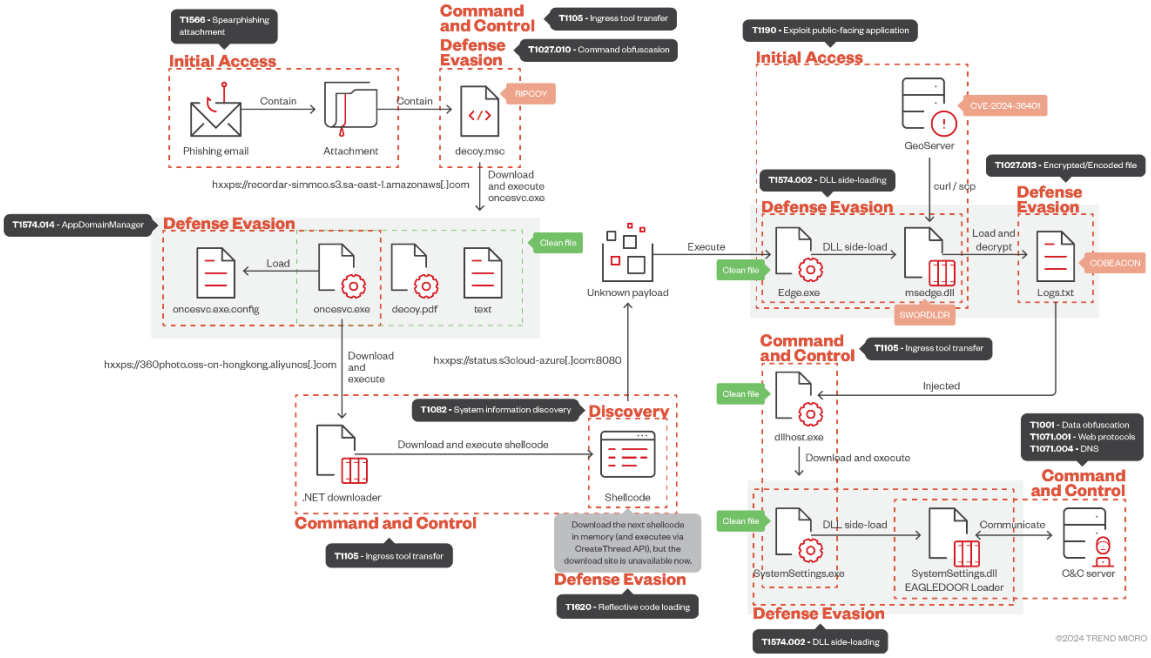
The threat actor group known as Earth Baxia has been observed executing sophisticated cyber-attacks targeting government organizations and critical sectors across the Asia-Pacific (APAC) region.Utilizing advanced techniques such as spear-phishing and exploiting the GeoServer vulnerability (CVE-2024-36401), they have successfully infiltrated networks to deploy customized malware, including modified Cobalt Strike components and a new backdoor named EAGLEDOOR.

Attack Vector Overview:

Earth Baxia has leveraged spear-phishing emails as a primary vector for initial access, often sending tailored messages with malicious attachments designed to trick users into executing harmful payloads. The exploitation of CVE-2024-36401 allows attackers to execute arbitrary commands on vulnerable GeoServer instances, facilitating the download of malicious components into targeted environments.

Malware Analysis:

- Cobalt Strike Modifications: The group employs a customized version of Cobalt Strike that has been altered to evade detection mechanisms. This includes modifications to internal signatures and configuration structures.
- EAGLEDOOR Backdoor: This new backdoor supports multiple communication protocols (DNS, HTTP, TCP, Telegram) for data exfiltration and command-and-control (C&C) operations. Its capabilities include gathering system information and delivering subsequent payloads.



The Earth Baxia threat campaign exemplifies the evolving landscape of cyber threats facing organizations in the APAC region. By employing sophisticated tactics and leveraging vulnerabilities in widely-used software, this group poses a significant risk to sensitive data and operational integrity. Organizations must adopt proactive measures outlined in this advisory to enhance their security posture against such advanced threats.

Indicators of Compromise:
Attached File.

RECOMMENDATIONS:

- Review the Indicators of Compromise (IOCs) and implement the necessary security measures.
- Regularly update and patch systems, particularly those running GeoServer or similar applications, to mitigate the risk of exploitation through known vulnerabilities.
- Deploy comprehensive security solutions that include email filtering, endpoint protection, and intrusion detection systems to identify and block threats at various stages of the attack lifecycle.
- Implement continuous training programs for employees to enhance their ability to recognize and respond to phishing attempts. Regular simulations can help reinforce this training.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.trendmicro.com/en_us/research/24/i/earth-baxia-spear-phishing-and-geoserver-exploit.html