AL2023_65 Researchers from ESET found a cyberespionage operation against a Guyana government organization (October 10, 2023)

Description

Cybersecurity researchers from ESET uncovered a sophisticated cyberespionage campaign named "Operation Jacana" targeting a government entity in Guyana. This incident highlights the growing concerns of state-sponsored cyberattacks on critical infrastructure and sensitive government information. Operation Jacana has been identified as an Advanced Persistent Threat (APT) but has not been definitively attributed to any specific group.

Details

According to the researchers, Operation Jacana commenced with a spear phishing campaign targeting the Guyana government entity. The attackers sent meticulously crafted emails with subject lines related to Guyanese public affairs, showing that they were closely monitoring the political landscape in Guyana. The emails contained links that, when clicked, downloaded a ZIP file from a Vietnamese government website, indicating that the attackers may have compromised another government entity to host their malware samples.

The ESET researchers determined that the core tool used by the threat actors in Operation Jacana is a previously undocumented C++ backdoor named DinodasRAT. This remote access trojan exhibits a wide range of capabilities, including file exfiltration, Windows registry manipulation, execution of CMD commands, and more. DinodasRAT employs the Tiny Encryption Algorithm (TEA) to encrypt the information it sends to the C&C server. This encryption adds an extra layer of obfuscation to the malicious activities, making it more challenging to detect and analyze. After gaining initial access through spear phishing, the attackers proceeded to move laterally within the victim's internal network. They used tools like Impacket, a WMI-based lateral movement tool, to execute various commands on the network, including manipulating files and Windows registry keys.

To communicate with the C&C server, DinodasRAT uses the Winsock library to create a socket, primarily using the TCP protocol but also capable of switching to UDP. The malware creates multiple threads for different tasks, ensuring synchronized communication with the C&C server. DinodasRAT is equipped with a

range of commands for executing actions on the victim's machine or the malware itself. These commands include listing directory contents, deleting files, modifying file attributes, sending files to the C&C server, and more. The backdoor allows attackers to execute various actions, providing them with extensive control over the compromised system. However, in addition to DinodasRAT the attackers deployed a variant of Korplug (also known as PlugX), a well-known backdoor commonly associated with China-aligned threat groups.

Indicators of Compromise

Please see the link for a list of IOCs including domains, IP addresses and email addresses associated with this malicious campaign:

https://github.com/eset/malware-ioc/tree/master/operation_jacana

Remediation

To protect yourself against this campaign, it is recommended to practice proper cyber security hygiene when navigating the internet. Here are some tips to consider:

1. **Email Security Enhancements**: Implement robust email filtering and security solutions to detect and block phishing emails.
2. **Patch and Update Management:** Ensure all operating systems, software, and security tools are up to date with the latest patches and updates to mitigate vulnerabilities that attackers might exploit.
3. **Multi-Factor Authentication (MFA):** Enforce MFA for accessing critical systems and sensitive information. This adds an extra layer of security, even if login credentials are compromised.
4. **Network Segmentation:** Isolate critical systems and sensitive data from less secure parts of the network. This can limit lateral movement if attackers gain access.
5. **Threat Intelligence Sharing:** Participate in threat intelligence sharing with industry peers and government agencies to stay informed about emerging threats and attacker tactics.

6. **Incident Response Plan:** Develop and regularly update an incident response plan that outlines steps to take in case of a security breach.

7. S**ecurity Awareness Training:** Continuously educate employees about cybersecurity best practices, including the dangers of phishing and social engineering attacks.

8. **Backup and Recovery Planning:** Regularly back up critical data and test the restoration process to ensure business continuity in case of a ransomware attack or data breach.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- The Hacker News. (2023, October 5). *Guyana governmental entity hit by DinodasRAT in cyber espionage attack*. https://thehackernews.com/2023/10/guyana-governmental-entity-hit-by.html
- Tavella, F. (2023, October 5). *Operation Jacana: Foundling hobbits in Guyana*. Retrieved from Welivesecurity. https://www.welivesecurity.com/en/eset-research/operation-jacana-spying-guyana-entity/