IMPORTANT CYBERSECURITY NEWS: FIN7's NEW STEALTH WEAPON ANUBISBACKDOOR EMERGES IN THE WILD

Vairav Cyber Security News Report

Date: March 20th, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Thirbam Sadak 148
Baluwatar, Kathmandu

EXECUTIVE SUMMARY

A recent cybersecurity development unveiled a new Python-based backdoor, dubbed AnubisBackdoor, attributed to the notorious FIN7 group, also known as Savage Ladybug. This malware grants attackers full control over infected systems, enabling remote command execution and data theft. Notably, AnubisBackdoor employs mild obfuscation techniques, allowing it to evade detection by most antivirus solutions, thereby posing significant risks to targeted organizations.

DETAILS OF THE INCIDENT

Description of the Cyber Threat: AnubisBackdoor is a Python-based malware designed to provide attackers with remote access, command execution capabilities, and data exfiltration functionalities. Its obfuscation techniques, though not highly sophisticated, are effective enough to bypass many security tools, rendering it fully undetected (FUD) by most antivirus solutions.

Identification: Threat intelligence company PRODAFT uncovered AnubisBackdoor, analyzing its capabilities and distribution methods.

Affected Entities/Industries: While specific targets of AnubisBackdoor have not been publicly disclosed, FIN7 has a history of targeting sectors such as hospitality, retail, and financial services.

Potential Impact:

- **Financial Losses**: Unauthorized access and data theft can lead to significant financial repercussions.
- **Operational Downtime**: Compromised systems may experience disruptions, affecting business continuity.
- **Data Exposure**: Sensitive information could be exfiltrated, leading to data breaches.

- **Reputational Damage**: Public disclosure of such incidents can harm an organization's reputation.

Exploitation Methods:

- **Mal-spam Campaigns**: Attackers use malicious emails to deliver the malware payload.
- **Compromised SharePoint Instances**: Hosting and serving the malware through compromised SharePoint servers to evade detection.

RELATED THREAT INTELLIGENCE & IOCs

Malicious IPs

- 38.134.148.20
- 5.252.177.249
- 212.224.107.203
- 195.133.67.35

Malware Hashes (SHA256)

- 03a160127cce3a96bfa602456046cc443816af7179d771e300fec80c5ab9f00f
- 5203f2667ab71d154499906d24f27f94e3ebdca4bba7fe55fe490b336bad8919

RECOMMENDED ACTIONS

Immediate Mitigation Steps

- Update antivirus definitions to recognize AnubisBackdoor indicators.
- Block identified malicious IPs and monitor network traffic for connections to these addresses.
- Scan systems for known malware hashes to detect infections.

Security Best Practices

- Educate employees on recognizing phishing emails to prevent mal-spam attacks.
- Regularly update and patch software to mitigate vulnerabilities.

- Implement robust access controls and network segmentation to limit lateral movement.

For Advanced Security Teams

- Deploy intrusion detection systems (IDS) to monitor for suspicious activities.
- Conduct threat-hunting exercises focusing on the identified IOCs.
- Analyze network traffic for anomalies associated with AnubisBackdoor's communication patterns.

ADDITIONAL RESOURCES AND OFFICIAL STATEMENTS

- https://securityonline.info/bitdefender-gravityzone-small-business-security-review-enterprise-grade-protection-without-the-enterprise-headache/
- https://catalyst.prodaft.com/public/report/anubis-backdoor/overview
- https://github.com/prodaft/malware-ioc/blob/master/SavageLadybug/AnubisBackdoor.md

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com