Operation Diplomatic Specter

Date: 28th May 2024 | Severity: High

Summary

The Operation Diplomatic Specter campaign, first reported by Palo Alto's Unit 42 in May 2024, has been active since at least late 2022. The cyberespionage campaign, operated by Chinese state-sponsored threat actors (tracked as TGR-STA-0043), targets diplomatic and economic missions, embassies, military operations, political meetings, ministries, and high-ranking officials, in the Middle East, Africa, and Asia. The threat actors specifically target their victims' email inboxes, exfiltrating sensitive emails and files, sometimes while using keyword searches to filter information related to military, telecommunications, and geopolitical affairs.

Attack Vectors

The threat actors behind Operation Diplomatic Specter gain initial access through the exploitation of known vulnerabilities in Microsoft Exchange and public-facing web servers (for example, ProxyLogon and ProxyShell). Then, they deploy in-memory VBScript implants and perform extensive reconnaissance using both custom and commodity network scanners (such as Nbtscan and Portscan). In addition, the attackers use various publicly available tools like JuicyPotatoNG for privilege escalation and Mimikatz for credential dumping. For lateral movement, the threat actors use Yasso, a Chinese pen-testing tool that supports brute forcing, network scanning, remote interactive shell capabilities, and arbitrary command execution.

Indicator of compromise

INDICATOR TYPE	INDICATORS
Domains	• govm.tk • update.microsoft-ns1.com • labour.govu.ml • api.microsoft-ns1.com • cloud.microsoft-ns1.com • home.microsoft-ns1.com • static.microsoft-ns1.com
IP Addresses	• 103.108.67.153 • 103.149.90.235 • 103.108.192.238 • 194.14.217.34 • 192.225.226.217

File Hashes	• 22d556db39bde212e6dbaa154e9bcf57527e7f51fa2f8f7a60f6d7109b94048e • 8198c8b5eaf43b726594df62127bcb1a4e0e46cf5cb9fa170b8d4ac2a4dad179 • 0f72e9eb5201b984d8926887694111ed09f28c87261df7aab663f5dc493e215f • 0b980e7a5dd5df0d6f07aabd6e7e9fc2e3c9e156ef8c0a62a0e20cd23c333373 • d5a44380e4f7c1096b1dddb6366713aa8ecb76ef36f19079087fc76567588977 • 62dec3fd2cdbc1374ec102d027f09423aa2affe1fb40ca05bf742f249ad7eb51 • 0e0b5c5c5d569e2ac8b70ace920c9f483f8d25aae7769583a721b202bcc0778f

Recommendation

- Email Security Enhancements: Implement advanced email security measures such as email authentication protocols (e.g., SPF, DKIM, DMARC), email encryption, and advanced threat protection solutions to detect and block phishing attempts and malicious attachments.
- Employee Training and Awareness: Conduct regular cybersecurity training sessions for employees to educate them about the threat of phishing attacks and social engineering tactics used by threat actors. Encourage employees to exercise caution when handling sensitive information and to report any suspicious emails or activities promptly.
- Endpoint Detection and Response (EDR): Deploy EDR solutions on endpoints to monitor for suspicious behavior and indicators of compromise. EDR solutions can help detect and respond to advanced threats, including those associated with state-sponsored cyber espionage campaigns.
- Threat Intelligence Sharing: Share threat intelligence with relevant government agencies, international partners, and cybersecurity organizations to facilitate a coordinated response to the threat posed by Chinese state-sponsored threat actors. Collaborate with trusted partners to exchange information about observed TTPs (Tactics, Techniques, and Procedures) and indicators of compromise.
- Incident Response Planning: Develop and regularly update incident response plans to ensure a swift and coordinated response in the event of a cyber attack or data breach. Conduct tabletop exercises and simulations to test the effectiveness of response procedures and identify areas for improvement.
- Supply Chain Security: Assess and enhance the security of third-party vendors and suppliers that have access to sensitive information or provide services to targeted organizations. Implement stringent security requirements and conduct regular audits to ensure compliance with security standards.
- Regulatory Compliance: Ensure compliance with relevant cybersecurity regulations and standards, such as GDPR, CCPA, or industry-specific regulations. Implement controls to protect sensitive data and mitigate the risk of regulatory penalties in the event of a data breach.
- Continuous Monitoring and Threat Hunting: Implement continuous monitoring and threat hunting capabilities to detect and respond to advanced threats in real-time. Leverage threat hunting teams or third-party security providers to proactively identify and neutralize threats before they can cause damage.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Link

- https://dashboard.ti.insight.rapid7.com/#/tip/cyber-term/664f46f39ced5c7a988314f9