Texas Council Risk Management Fund

RISK ALERT

February 15, 2022

Cyber Risk Alert - Russian State-Sponsored Cyber Threats to Public Entities

Given the increased focus on the geopolitical landscape, the Russian threat to U.S. public entities and critical infrastructure, including specific tactics, techniques, and procedures associated with Russian actors has reached a high alert status. This alert is urging all public entities to take urgent steps to reduce the likelihood and impact of a potentially damaging compromise.

Public entities need to adopt a heightened state of awareness and to conduct proactive threat hunting. It's strongly urged that network defenders to implement recommendations detailed in this alert. These mitigations will help organizations improve their functional resilience by reducing the risk of compromise or severe business interruption.

SYSTEMS AFFECTED:

- Unpatched Multi-Vendor Operating Systems
- Entities without Multi-Factor Authentication
- Entities without adequate Anti-Virus Software
- Hardware without Surge Protectors or Uninterruptable Power Supplies

RISK:

Government: Large, medium, small government entities: **High**

Businesses: Large, medium, small business entities: **High**

SUMMARY:

Historically, Russian state-sponsored advanced persistent threat (APT) actors have used common but effective tactics, including spear phishing, brute force, and exploiting known vulnerabilities against accounts and networks with weak security to gain initial access to target networks. Vulnerabilities known to be exploited by Russian state-sponsored APT actors for initial access include:

- FortiGate VPNs. [CVE-2018-13379]
- Cisco Routers [CVE-2019-1653)
- Oracle WebLogic Servers [CVE-2019-2725]
- Kibana [CVE-2019-7609]
- Zimbra Software [CVE-2019-9670]
- Exim Simple Mail Transfer Protocol [CVE-2019-10149]
- Pulse Secure [CVE-2019-11510]
- Citrix [CVE-2019-19781]
- Microsoft Exchange [CVE-2020-0688]
- VMWare [CVE-2020-4006]
- F5 Big-IP [CVE-2020-5902]
- Oracle WebLogic {CVE-2020-14882]
- Microsoft Exchange [CVE-2021-26855]

Russian state-sponsored APT actors have also demonstrated sophisticated tradecraft and cyber capabilities by compromising third-party infrastructure, compromising third-party software, or developing and deploying custom malware. The actors have also demonstrated the ability to maintain persistent, undetected, long-term access in compromised environments, including cloud environments, by using legitimate credentials.

In some cases, Russian state-sponsored cyber operations against critical infrastructure organizations have specifically targeted operational technology (OT)/industrial control systems (ICS) networks with destructive malware. Russian state-sponsored APT actors have used sophisticated cyber capabilities to target a variety of U.S. critical infrastructure organizations, including those in the healthcare, public health, energy, and telecommunications. High-profile cyber activity publicly attributed to Russian state-sponsored APT actors by U.S. government reporting and legal action includes:

- Targeting state and local aviation networks
- Targeting energy sector networks

TECHNIQUES BEING USED:

The following techniques are being employed by Russian state-sponsored APT actors:

- Active Vulnerability Scanning to scan in an attempt to find vulnerable servers.

- Phishing for Information to gain credentials of target networks.
- Malware being deployed, including ICS-focused destructive malware.
- Exploit Public-Facing Application vulnerabilities, including zero day, in internet-facing systems.
- Supply Chain Compromise of third-party software, including M.E. Doc and SolarWinds Orion.
- Command and Scripting to execute commands and exfiltrate data on remote machines.
- Valid Accounts and Credentials to maintain long-term access to compromised networks.
- Brute Force attacks such as password guessing and password spraying campaigns.
- OS Credential Dumping to exfiltrate credentials of the Active Directory database.
- Forging Kerberos Tickets to obtain tickets for Active Directory Service Principal Names (SPN).
- Credentials from Password Stores to access Group Managed Service Account (gMSA) passwords.
- Credential Access through Windows Net logon vulnerability to access Active Directory servers.
- Private Encryption Keys from Active Directory (ADFS) to decrypt SAML signing certificates.
- Multi-Hop Proxy and virtual private servers (VPSs) to route traffic to targets.

RECOMMENDATIONS:

The following recommended actions should be taken:

- Implement robust log collection and retention. Without a centralized log collection and monitoring capability, organizations have limited ability to investigate incidents or detect the threat actor behavior.
- Look for behavioral evidence or network and host-based artifacts from know Russian state-sponsored TTPs. Review authentication logs for system and application login failures of valid accounts. Look for multiple, failed authentication attempts across multiple accounts.
- Look for suspicious impossible logins with changing username, user agent strings, and IP address combinations or logins where IP addresses don’t align to geographic location.
- Look for one IP used for multiple accounts, excluding expected logins.
- Look for impossible travel where a user logs in from multiple addresses that are of significant geographical distance apart and not realistic.
- Look for processes and program execution command-line arguments that may indicate credential dumping, especially attempts to copy the ntds.dit file from a domain controller.
- Look for suspicious privileged account use after resetting passwords or applying mitigations.

- Look for unusual activity in typically dormant accounts and unusual user agent strings not typically associated with normal user activity, which may indicate bot activity.
- Notice unexpected equipment behavior such as reboots of controllers and other hardware.
- Look for delays or disruptions in communication with field equipment or other hardware.
- Secure backups and ensure backup data is offline is secured. Scan the backup data with an anti-virus program to ensure it's free of malware.
- Create, maintain, and exercise a cyber incident response plan and business continuity plan.
- Require multi-factor authentication for all users, without any exceptions. Require strong passwords and don't allow general accounts used across multiple users.
- Audit domain controllers to log successful Kerberos TGS requests and ensure events are monitored for anomalous activity. Enforce least privilege on Administrator accounts.
- Identify, detect, and investigate abnormal activity that indicates lateral movement by a threat actor or malware. Use network monitoring tools, log, and endpoint detection and response.
- Enable spam filters to prevent phishing emails and executable from reaching end users. Implement a user training program to not visit malicious websites or open attachments.
- Implement network segmentation to separate network segments based on role and functionality to prevent lateral movement by controlling traffic flows to subnetworks.
- Update software, operating systems, applications, and firmware on network assets.
- User a risk-based asset inventory strategy to determine how network assets are identified and evaluated for the presence of malware. Turn off or disable unnecessary services on devices.
- Disable unnecessary ports and protocols and monitor common ports for command and control activity. Disable unnecessary services within devices and ensure hardware is in read-only mode.

REFERENCES:

CISA:

CISA, FBI, and NSA Release Cybersecurity Advisory on Russian Cyber Threats to U.S. Critical Infrastructure | CISA

CISA:

AA22-011A_Joint_CSA_Understanding_and_Mitigating_Russian_Cyber_Threats_to_US_Critical_Infrastructure_TLP-WHITE_01-10-22_v1.pdf (cisa.gov)

For additional information please contact Lee Cain, IT Risk Consultant at lee.cain@sedgwick.com or by phone at 512-427-2322