Hive Pro

THREAT ADVISORY

Russian state-sponsored cyber actors targeting U.S. critical infrastructure

TA2022036

Threat Level RED

Publish Date – Feb 18, 2022

In a joint cybersecurity advisory, the Federal Bureau of Investigation (FBI), the National Security Agency (NSA), the Cybersecurity and Infrastructure Security Agency (CISA) revealed that Russian state-sponsored threat actors targeted U.S. defense contractors from January 2020 to February 2022. The threat actors exfiltrated sensitive data from small and large companies in the U.S. working on defense and intelligence contracts, including missile development, vehicle & aircraft and software development.

Threat actors gain initial access by using brute force to identify valid account credentials for domain and M365 accounts. Using compromised M365 credentials, including global admin accounts, the threat actors can gain access to M365 resources such as SharePoint pages user-profiles and user emails. They further used harvested credentials in conjunction with known vulnerabilities CVE-2020-0688 & CVE-2020-17144 in the Microsoft exchange server to escalate privileges and gain remote code execution (RCE) on the exposed applications. In addition, they have exploited CVE-2018-13379 on FortiClient to obtain credentials to access networks. After gaining access to networks, the threat actors map the Active Directory (AD) and connect to domain controllers, from which they exfiltrated credentials and export copies of the AD database "ntds.dit". In multiple breaches, they maintained persistence for at least 6 months in the network continuously exfiltrating sensitive emails and data.

Organizations can mitigate the risk by following the recommendations:

- Monitor the use of stolen credentials.
- Keep all operating systems and software up to date.
- Enable multifactor authentication (MFA) for all users, without exception.

The Techniques commonly used by Russian cyber actor, APT28 are:

TA0043: Reconnaissance
TA0001: Initial Access
TA0004: Privilege Escalation
TA0005: Defense Evasion
TA0006: Credential Access
TA0007: Discovery
TA0009: Collection
TA0003: Persistence
TA0008: Lateral Movement
TA0011: Command and Control
T1027: Obfuscated Files or Information
T1133: External Remote Services
T1190: Exploit Public-Facing Application
T1083: File and Directory Discovery
T1482: Domain Trust Discovery
T1213.002: Data from Information Repositories: SharePoint
T1090.003: Proxy: Multi-hop Proxy
T1589.001: Gather Victim Identity Information: Credentials
T1003.003: OS Credential Dumping: NTDS
T1110.003: Brute Force: Password Spraying
T1566.002: Phishing: Spearphishing Link
T1078.002: Valid Accounts: Domain Accounts
T1078.004: Valid Accounts: Cloud Accounts

Hive Pro

THREAT ADVISORY

Actor Details

Name	Target Locations	Target sectors	Motive
APT28	Afghanistan, Armenia, Australia, Azerbaijan, Belarus, Belgium, Brazil, Bulgaria, Canada, Chile, China, Croatia, Cyprus, France, Georgia, Germany, Hungary, India, Iran, Iraq, Japan, Jordan, Kazakhstan, Latvia, Malaysia, Mexico, Mongolia, Montenegro, Netherlands, Norway, Pakistan, Poland, Romania, Slovakia, South Africa, South Korea, Spain, Sweden, Switzerland, Tajikistan, Thailand, Turkey, Uganda, UAE, UK, Ukraine, USA, Uzbekistan	Automotive, Aviation, Chemical, Construction, Defense, Education, Embassies, Engineering, Financial, Government, Healthcare, Industrial, IT, Media, NGOs, Oil and gas, Think Tanks and Intelligence organizations.	Information theft and espionage

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2018-13379	Fortinet FortiOS 6.0.0 to 6.0.4, 5.6.3 to 5.6.7 and 5.4.6 to 5.4.12	cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*	Fortinet FortiOS VPN web portal directory traversal	CWE-22
CVE-2020-0688	Microsoft Exchange Server 2010, 2013, 2016, 2019	cpe:2.3:a:microsoft:exchange_server:2010:sp3_rollup_30:*:*:*:*:*:*:*, cpe:2.3:a:microsoft:exchange_server:2013:cumulative_update_23:*:*:*:*:*:*:*, cpe:2.3:a:microsoft:exchange_server:2016:cumulative_update_14:*:*:*:*:*:*:*, cpe:2.3:a:microsoft:exchange_server:2016:cumulative_update_15:*:*:*:*:*:*:*, cpe:2.3:a:microsoft:exchange_server:2019:cumulative_update_3:*:*:*:*:*:*:*, cpe:2.3:a:microsoft:exchange_server:2019:cumulative_update_4:*:*:*:*:*:*:*	Microsoft Exchange validation key remote code execution	CWE-798
CVE-2020-17144	Microsoft Exchange Server: 2010 - 2010 Update Rollup 5	cpe:2.3:a:microsoft:exchange_server:2010:sp3_rollup_31:*:*:*:*:*:*	Microsoft Exchange remote code execution vulnerability	CWE-20

Reference

https://www.cisa.gov/uscert/ncas/alerts/aa22-047a