SecurityRisk ADVISORS

CyberSOC Threat Notification

CISA Advisory on Russian Foreign Intelligence Service (SVR) Cyber Operations

Executive Summary

The Federal Bureau of Investigation (FBI), Department of Homeland Security (DHS), and CISA have released a joint Cybersecurity Advisory addressing the Russian Foreign Intelligence Service (SVR) continuing to target the U.S. and foreign entities.

Description

Also known as APT (Advance Persistent Threat) 29, the SVR activity primarily targets government networks, think tank and policy analysis organizations, and information technology companies to gather intelligence. In previous attacks, APT 29 utilized password spraying attacks to gain access to an administrator account with a weak password, compromising a large network. The threat actor also leveraged CVE-2019-19781 against a Virtual Private Network (VPN) appliance to gain control of a victim's network. SVR was also attributed to releasing malware that targeted COVID-19 vaccine development. Once deployed, this malware targeted Active Directory and repositories containing vaccine research within the organizations affected. Additionally, APT 29 has been observed in other organizations that exhibit similar post-infection tactics as was exhibited in the SolarWinds compromise, including how the actors purchased and managed infrastructure used in the intrusions.

Safeguards/Recommendations

CISA provides several recommendations in their advisory including implementing and improving Multi-Factor Authentication, placing improved security controls on administrative accounts, enforcing strong passwords, monitoring and auditing networks for anomalous shell commands, and ensuring endpoint monitoring solutions are configured properly.

Version History

Version 1. Initial Report

Published: 04-26-2021

Attribution Metrics

Threat Actor: Cozy Bear

Origin: Russian Nation-State

Associations: SolarWinds

Other Aliases: APT29, Yttrium, The Dukes

Technique Metrics

Vulnerabilities: CVE-2019-19781

Tactics: Password Spraying, Leveraging Zero-Day Vulnerabilities, WELLMESS Malware, Supply Chain Intrusions

Industries: Government, Information Technology, Think Tank and Policy Analysis Organizations

Contact Us

24x7 SOC Phone: 215.867.9051
Email: soc@sra.io
Website: https://sra.io