Russian Foreign Intelligence Service (SVR) Cyber Operations: Trends and Best Practices for Network Defenders


us-cert.cisa.gov/ncas/alerts/aa21-116a

Summary

The Federal Bureau of Investigation (FBI), Department of Homeland Security (DHS), and Cybersecurity and Infrastructure Security Agency (CISA) assess Russian Foreign Intelligence Service (SVR) cyber actors—also known as Advanced Persistent Threat 29 (APT 29), the Dukes, CozyBear, and Yttrium—will continue to seek intelligence from U.S. and foreign entities through cyber exploitation, using a range of initial exploitation techniques that vary in sophistication, coupled with stealthy intrusion tradecraft within compromised networks. The SVR primarily targets government networks, think tank and policy analysis organizations, and information technology companies. On April 15, 2021, the White House released a statement on the recent SolarWinds compromise, attributing the activity to the SVR. For additional detailed information on identified vulnerabilities and mitigations, see the National Security Agency (NSA), Cybersecurity and Infrastructure Security Agency (CISA), and FBI Cybersecurity Advisory titled “Russian SVR Targets U.S. and Allied Networks,” released on April 15, 2021.

The FBI and DHS are providing information on the SVR’s cyber tools, targets, techniques, and capabilities to aid organizations in conducting their own investigations and securing their networks.

Click here for a PDF version of this report.

Threat Overview

SVR cyber operations have posed a longstanding threat to the United States. Prior to 2018, several private cyber security companies published reports about APT 29 operations to obtain access to victim networks and steal information, highlighting the use of customized tools to maximize stealth inside victim networks and APT 29 actors’ ability to move within victim environments undetected.

Beginning in 2018, the FBI observed the SVR shift from using malware on victim networks to targeting cloud resources, particularly e-mail, to obtain information. The exploitation of Microsoft Office 365 environments following network access gained through use of modified SolarWinds software reflects this continuing trend. Targeting cloud resources probably reduces the likelihood of detection by using compromised accounts or system misconfigurations to blend in with normal or unmonitored traffic in an environment not well defended, monitored, or understood by victim organizations.

Technical Details

SVR Cyber Operations Tactics, Techniques, and Procedures

Password Spraying

In one 2018 compromise of a large network, SVR cyber actors used password spraying to identify a weak password associated with an administrative account. The actors conducted the password spraying activity in a “low and slow” manner, attempting a small number of passwords at infrequent intervals, possibly to avoid detection. The password spraying used a large number of IP addresses all located in the same country as the victim, including those associated with residential, commercial, mobile, and The Onion Router (TOR) addresses.

The organization unintentionally exempted the compromised administrator’s account from multi-factor authentication requirements. With access to the administrative account, the actors modified permissions of specific e-mail accounts on the network, allowing any authenticated network user to read those accounts.

The actors also used the misconfiguration for compromised non-administrative accounts. That misconfiguration enabled logins using legacy single-factor authentication on devices which did not support multi-factor authentication. The FBI suspects this was achieved by spoofing user agent strings to appear to be older versions of mail clients, including Apple’s mail client and old versions of Microsoft Outlook. After logging in as a non-administrative user, the actors used the permission changes applied by the compromised administrative user to access specific mailboxes of interest within the victim organization.

While the password sprays were conducted from many different IP addresses, once the actors obtained access to an account, that compromised account was generally only accessed from a single IP address corresponding to a leased virtual private server (VPS). The FBI observed minimal overlap between the VPSs used for different compromised accounts, and each leased server used to conduct follow-on actions was in the same country as the victim organization.

During the period of their access, the actors consistently logged into the administrative account to modify account permissions, including removing their access to accounts presumed to no longer be of interest, or adding permissions to additional accounts.

Recommendations

To defend from this technique, the FBI and DHS recommend network operators to follow best practices for configuring access to cloud computing environments, including:

- Mandatory use of an approved multi-factor authentication solution for all users from both on premises and remote locations.

- Prohibit remote access to administrative functions and resources from IP addresses and systems not owned by the organization.
- Regular audits of mailbox settings, account permissions, and mail forwarding rules for evidence of unauthorized changes.
- Where possible, enforce the use of strong passwords and prevent the use of easily guessed or commonly used passwords through technical means, especially for administrative accounts.
- Regularly review the organization's password management program.
- Ensure the organization's information technology (IT) support team has well-documented standard operating procedures for password resets of user account lockouts.
- Maintain a regular cadence of security awareness training for all company employees.

Leveraging Zero-Day Vulnerability

In a separate incident, SVR actors used CVE-2019-19781, a zero-day exploit at the time, against a virtual private network (VPN) appliance to obtain network access. Following exploitation of the device in a way that exposed user credentials, the actors identified and authenticated to systems on the network using the exposed credentials.

The actors worked to establish a foothold on several different systems that were not configured to require multi-factor authentication and attempted to access web-based resources in specific areas of the network in line with information of interest to a foreign intelligence service.

Following initial discovery, the victim attempted to evict the actors. However, the victim had not identified the initial point of access, and the actors used the same VPN appliance vulnerability to regain access. Eventually, the initial access point was identified, removed from the network, and the actors were evicted. As in the previous case, the actors used dedicated VPSs located in the same country as the victim, probably to make it appear that the network traffic was not anomalous with normal activity.

Recommendations

To defend from this technique, the FBI and DHS recommend network defenders ensure endpoint monitoring solutions are configured to identify evidence of lateral movement within the network and:

- Monitor the network for evidence of encoded PowerShell commands and execution of network scanning tools, such as NMAP.
- Ensure host based anti-virus/endpoint monitoring solutions are enabled and set to alert if monitoring or reporting is disabled, or if communication is lost with a host agent for more than a reasonable amount of time.
- Require use of multi-factor authentication to access internal systems.

- Immediately configure newly-added systems to the network, including those used for testing or development work, to follow the organization's security baseline and incorporate into enterprise monitoring tools.

WELLMESS Malware

In 2020, the governments of the United Kingdom, Canada, and the United States attributed intrusions perpetrated using malware known as WELLMESS to APT 29. WELLMESS was written in the Go programming language, and the previously-identified activity appeared to focus on targeting COVID-19 vaccine development. The FBI's investigation revealed that following initial compromise of a network—normally through an unpatched, publicly-known vulnerability—the actors deployed WELLMESS. Once on the network, the actors targeted each organization's vaccine research repository and Active Directory servers. These intrusions, which mostly relied on targeting on-premises network resources, were a departure from historic tradecraft, and likely indicate new ways the actors are evolving in the virtual environment. More information about the specifics of the malware used in this intrusion have been previously released and are referenced in the 'Resources' section of this document.

Tradecraft Similarities of SolarWinds-enabled Intrusions

During the spring and summer of 2020, using modified SolarWinds network monitoring software as an initial intrusion vector, SVR cyber operators began to expand their access to numerous networks. The SVR's modification and use of trusted SolarWinds products as an intrusion vector is also a notable departure from the SVR's historic tradecraft.

The FBI's initial findings indicate similar post-infection tradecraft with other SVR-sponsored intrusions, including how the actors purchased and managed infrastructure used in the intrusions. After obtaining access to victim networks, SVR cyber actors moved through the networks to obtain access to e-mail accounts. Targeted accounts at multiple victim organizations included accounts associated with IT staff. The FBI suspects the actors monitored IT staff to collect useful information about the victim networks, determine if victims had detected the intrusions, and evade eviction actions.

Recommendations

Although defending a network from a compromise of trusted software is difficult, some organizations successfully detected and prevented follow-on exploitation activity from the initial malicious SolarWinds software. This was achieved using a variety of monitoring techniques including:

- Auditing log files to identify attempts to access privileged certificates and creation of fake identify providers.
- Deploying software to identify suspicious behavior on systems, including the execution of encoded PowerShell.

- Deploying endpoint protection systems with the ability to monitor for behavioral indicators of compromise.
- Using available public resources to identify credential abuse within cloud environments.
- Configuring authentication mechanisms to confirm certain user activities on systems, including registering new devices.

While few victim organizations were able to identify the initial access vector as SolarWinds software, some were able to correlate different alerts to identify unauthorized activity. The FBI and DHS believe those indicators, coupled with stronger network segmentation (particularly “zero trust” architectures or limited trust between identity providers) and log correlation, can enable network defenders to identify suspicious activity requiring additional investigation.

General Tradecraft Observations

SVR cyber operators are capable adversaries. In addition to the techniques described above, FBI investigations have revealed infrastructure used in the intrusions is frequently obtained using false identities and cryptocurrencies. VPS infrastructure is often procured from a network of VPS resellers. These false identities are usually supported by low reputation infrastructure including temporary e-mail accounts and temporary voice over internet protocol (VoIP) telephone numbers. While not exclusively used by SVR cyber actors, a number of SVR cyber personas use e-mail services hosted on cock[.]li or related domains.

The FBI also notes SVR cyber operators have used open source or commercially available tools continuously, including Mimikatz—an open source credential-dumping too—and Cobalt Strike—a commercially available exploitation tool.

Mitigations

The FBI and DHS recommend service providers strengthen their user validation and verification systems to prohibit misuse of their services.

Resources

- NSA, CISA, FBI Joint Cybersecurity Advisory: Russian SVR Targets U.S. and Allied Networks
- CISA: Remediating Networks Affected by the SolarWinds and Active Directory/M365 Compromise
- CISA Alert AA21-008A: Detecting Post-Compromise Threat Activity in Microsoft Cloud Environments
- FBI, CISA, ODNI, NSA Joint Statement: Joint Statement by the Federal Bureau of Investigation, the Cybersecurity and Infrastructure Security Agency, the Office of the Director of National Intelligence (ODNI), and the National Security Agency

- CISA Alert AA20-352A: Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations
- CISA Insights: What Every Leader Needs to Know about the Ongoing APT Cyber Activity
- FBI, CISA Joint Cybersecurity Advisory: Advanced Persistent Threat Actors Targeting U.S. Think Tanks
- CISA: Malicious Activity Targeting COVID-19 Research, Vaccine Development
- NCSC, CSE, NSA, CISA Advisory: APT 29 targets COVID-19 vaccine development

Revisions

April 26, 2021: Initial Version

Please share your thoughts.

We recently updated our anonymous product survey; we'd welcome your feedback.