National Cyber Security Centre
a part of GCHQ

National Cyber Security Centre
PART OF THE GCSB

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Communications Security Establishment
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité

Advisory

SVR cyber actors adapt tactics for initial cloud access

February 2024

SVR cyber actors adapt tactics for initial cloud access

How SVR-attributed actors are adapting to the move of government and corporations to cloud infrastructure

Overview

This advisory details recent tactics, techniques and procedures (TTPs) of the group commonly known as APT29, also known as Midnight Blizzard, the Dukes or Cozy Bear.

The UK National Cyber Security Centre (NCSC) and international partners assess that APT29 is a cyber espionage group, almost certainly part of the SVR, an element of the Russian intelligence services. The US National Security Agency (NSA), the US Cybersecurity and Infrastructure Security Agency (CISA), the US Cyber National Mission Force (CNMF), the Federal Bureau of Investigation (FBI), Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC), the Canadian Centre for Cyber Security (CCCS) and the New Zealand National Cyber Security Centre (NCSC) agree with this attribution and the details provided in this advisory.

This advisory provides an overview of TTPs deployed by the actor to gain initial access into the cloud environment and includes advice to detect and mitigate this activity.

Previous actor activity

The NCSC has previously detailed how Russian Foreign Intelligence Service (SVR) cyber actors have targeted governmental, think tank, healthcare and energy targets for intelligence gain. It has now observed SVR actors expanding their targeting to include aviation, education, law enforcement, local and state councils, government financial departments and military organisations.

SVR actors are also known for:

- the supply chain compromise of SolarWinds software

- activity that targeted organisations developing the COVID-19 vaccine

Evolving TTPs

As organisations continue to modernise their systems and move to cloud-based infrastructure, the SVR has adapted to these changes in the operating environment.

They have to move beyond their traditional means of initial access, such as exploiting software vulnerabilities in an on-premise network, and instead target the cloud services themselves.

To access the majority of the victims' cloud hosted network, actors must first successfully authenticate to the cloud provider. Denying initial access to the cloud environment can prohibit SVR from successfully compromising their target. In contrast, in an on-premise system, more of the network is typically exposed to threat actors.

Below describes in more detail how SVR actors are adapting to continue their cyber operations for intelligence gain. These TTPs have been observed in the last 12 months.

Access via service and dormant accounts

Previous SVR campaigns reveal the actors have successfully used brute forcing (T1110) and password spraying to access service accounts. This type of account is typically used to run and manage applications and services. There is no human user behind them so they cannot be easily protected with multi-factor authentication (MFA), making these accounts more susceptible to a successful compromise. Service accounts are often also highly privileged depending on which applications and services they're responsible for managing. Gaining access to these accounts provides threat actors with privileged initial access to a network, to launch further operations.

SVR campaigns have also targeted dormant accounts belonging to users who no longer work at a victim organisation but whose accounts remain on the system. (T1078.004).

Following an enforced password reset for all users during an incident, SVR actors have also been observed logging into inactive accounts and following instructions to reset the password. This has allowed the actor to regain access following incident response eviction activities.

Cloud-based token authentication

Account access is typically authenticated by either username and password credentials or system-issued access tokens. The NCSC and partners have observed SVR actors using tokens to access their victims' accounts, without needing a password (T1528).

The default validity time of system-issued tokens varies dependant on the system, however cloud platforms should allow administrators to adjust the validity time as appropriate for their users. More information can be found on this in the mitigations section of this advisory.

Enrolling new devices to the cloud

On multiple occasions, the SVR has successfully bypassed password authentication on personal accounts using password spraying and credential reuse. SVR actors have also then bypassed MFA through a technique known as 'MFA bombing' or 'MFA fatigue', in which the actors repeatedly push MFA requests to a victim's device until the victim accepts the notification (T1621).

Once an actor has bypassed these systems to gain access to the cloud environment, SVR actors have been observed registering their own device as a new device on the cloud tenant (T1098.005). If device validation rules are not set up, SVR actors can successfully register their own device and gain access to the network.

By configuring the network with device enrolment policies, there have been instances where these measures have defended against SVR actors and denied them access to the cloud tenant.

Residential proxies

As network-level defences improve detection of suspicious activity, SVR actors have looked at other ways to stay covert on the internet. A TTP associated with this actor is the use of residential proxies (T1090.002). Residential proxies typically make traffic appear to originate from IP addresses within internet service provider (ISP) ranges used for residential broadband customers and hide the true source. This can make it harder to distinguish malicious connections from typical users. This reduces the effectiveness of network defences that use IP addresses as indicators of compromise, and so it is important to consider a variety of information sources such as application and host-based logging for detecting suspicious activity.

Conclusion

The SVR is a sophisticated actor capable of carrying out a global supply chain compromise such as the 2020 SolarWinds, however the guidance in this advisory shows that a strong baseline of cyber security fundamentals can help defend from such actors.

For organisations that have moved to cloud infrastructure, a first line of defence against an actor such as SVR should be to protect against SVR's TTPs for initial access. By following the mitigations outlined in this advisory, organisations will be in a stronger position to defend against this threat.

Once the SVR gain initial access, the actor is capable of deploying highly sophisticated post compromise capabilities such as MagicWeb, as reported in 2022. Therefore, mitigating against the SVR's initial access vectors is particularly important for network defenders.

CISA have also produced guidance through their Secure Cloud Business Applications (SCuBA) Project which is designed to protect assets stored in cloud environments.

Some of the TTPs listed in this report, such as residential proxies and exploitation of system accounts, are similar to those reported as recently as January 2024 by Microsoft.

MITRE ATT&CK®

This report has been compiled with respect to the MITRE ATT&CK® framework, a globally accessible knowledge base of adversary tactics and techniques based on real-world observations.

Tactic	ID	Technique	Procedure
Credential Access	T1110	Brute forcing	The SVR use password spraying and brute forcing as an initial infection vector.
Initial Access	T1078.004	Valid Accounts: Cloud Accounts	The SVR use compromised credentials to gain access to accounts for cloud services, including system and dormant accounts.
Credential Access	T1528	Steal Application Access Token	The SVR use stolen access tokens to login to accounts without the need for passwords.
Credential Access	T1621	Multi-Factor Authentication Request Generation	The SVR repeatedly push MFA requests to a victim's device until the victim accepts the notification, providing SVR access to the account.
Command and Control	T1090.002	Proxy: External Proxy	The SVR use open proxies in residential IP ranges to blend in with expected IP address pools in access logs.
Persistence	T1098.005	Account Manipulation: Device Registration	The SVR attempt to register their own device on the cloud tenant after acquiring access to accounts.

Mitigation and Detection

A number of mitigations will be useful in defending against the activity described in this advisory:

- **Use multi-factor authentication** (/2-factor authentication/two-step verification) to reduce the impact of password compromises. See NCSC guidance: https://www.ncsc.gov.uk/guidance/multi-factor-authentication-online-services and https://www.ncsc.gov.uk/guidance/setting-two-factor-authentication-2fa
- Accounts that cannot use 2SV should have strong, unique passwords. User and system accounts should be disabled when no longer required with a 'joiners, movers and leavers' process in place and regular reviews to identify and disable inactive/dormant accounts. See NCSC guidance: https://www.ncsc.gov.uk/collection/10-steps/identity-and-access-management
- System and service accounts should implement the principle of least privilege, providing a tightly scoped access to resources required for the service to function.
- Canary service accounts should be created which appear to be valid service accounts but are never used by legitimate services. Monitoring and alerting on the use of these account provides a high confidence signal that they are being used illegitimately and should be investigated urgently.
- Session lifetimes should be kept as short as practical to reduce the window of opportunity for an adversary to use stolen session tokens. This should be paired with a suitable authentication method that strikes a balance between regular user authentication and user experience.
- Ensure device enrolment policies are configured to only permit authorised devices to enrol. Use zero-touch enrolment where possible, or if self-

enrolment is required then use a strong form of 2SV that is resistant to phishing and prompt bombing. Old devices should be prevented from (re-)enrolling when no longer required. See NCSC guidance: https://www.ncsc.gov.uk/collection/device-security-guidance/getting-ready/provisioning-and-distributing-devices

- Consider a variety of information sources such as application events and host-based logs to help prevent, detect and investigate potential malicious behaviour. Focus on the information sources and indicators of compromise that have a better rate of false positives. For example, looking for changes to user agent strings that could indicate session hijacking may be more effective than trying to identify connections from suspicious IP addresses. See NCSC guidance: https://www.ncsc.gov.uk/guidance/introduction-logging-security-purposes