RelianceCyber

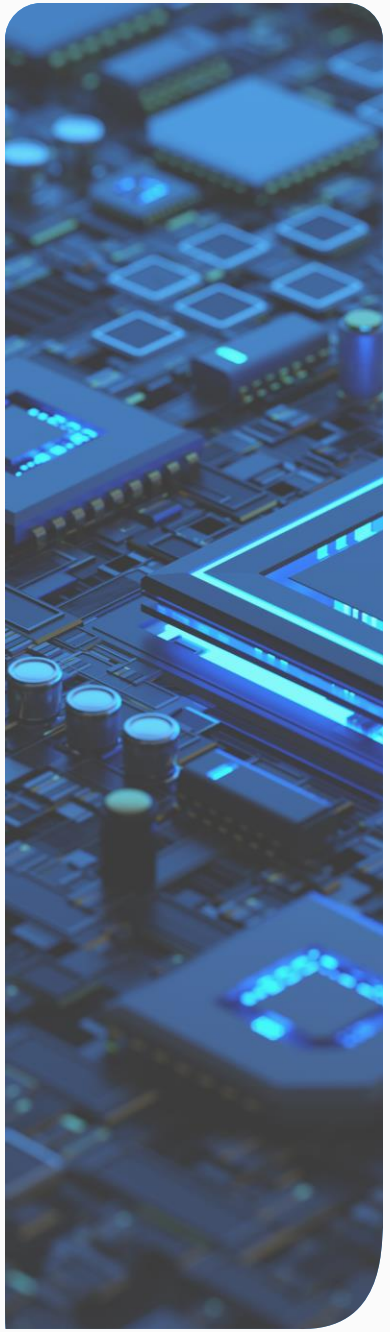
TLP: CLEAR

Threat Intelligence

ATP29 Threat Actor Profile

Written by: Adam Schweizer

Date: 2024-07-02



RelianceCyber

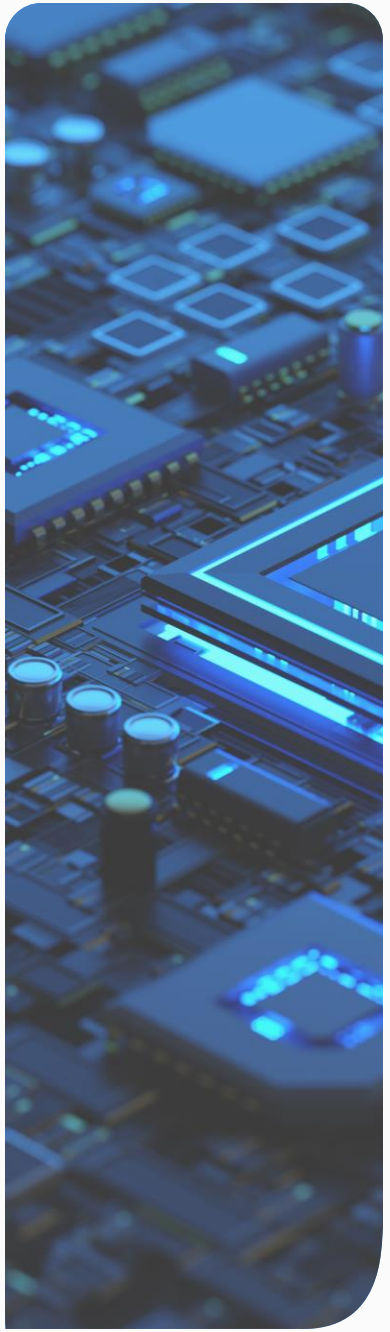
Executive Summary

The Reliance Cyber Threat Actor Profile Report aims to help businesses understand & manage the associated risks by providing the most relevant information and mitigation advisory. If you require any additional information about this report or the advice contained therein; please contact your Customer Success representative.

1. **Key Recommendations** – List of recommended mitigations to help mitigate threats associated with APT29 known activity. (Pages 3-5)
2. **Threat Actor Profile**– The APT29 introduction, notable attacks timeline, tactics, techniques and procedures and a visualized Tactics, Techniques and Procedures (TTPs) map. (Pages 6-12)
3. **Sources & Additional Resources** – List of sources used to produce this report and additional resources that have detailed information (Page 13)

RelianceCyber

Key Recommendations



RelianceCyber

Key Recommendations

Reliance Cyber have reviewed the threat actor activity and suggest below some of the key mitigations.

APT29 Mitigations

TA.APT29.001 - 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 the NCSC Guide for more details.

TA.APT29.002 - 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.

TA.APT29.003 - 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.

TA.APT29.004 - Ensure device enrollment policies are configured to only permit authorized devices to enroll. Use zero-touch enrollment where possible, or if self-enrollment 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 the NCSC Guide for more details.

Action: Please ensure all of the above actions are either remediated or appropriately risk managed.

RelianceCyber

Key Recommendations

TA.APT29.005 - Consider a variety of information sources such as application events and host-based logs to help prevent, detect and investigate potential malicious behavior. 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 the NCSC Guide for more details.

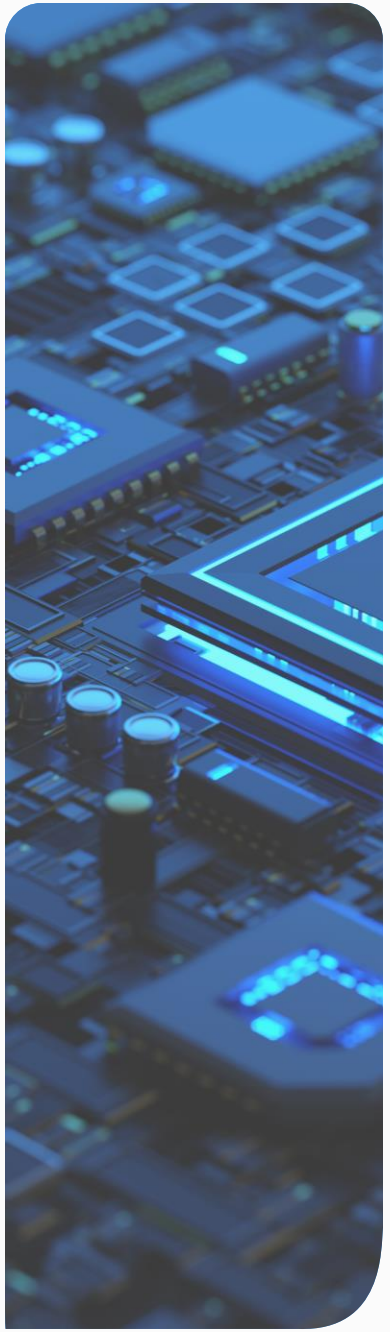
TA.APT29.006 - Session lifetimes should be kept as short as practical to reduce the window of opportunity for an adversary to use stolen session tokens. This should be paired with a suitable authentication method that strikes a balance between regular user authentication and user experience.

Action: Please ensure all of the above actions are either remediated or appropriately risk managed.

RelianceCyber

Threat Intelligence

APT29 Threat Actor Profile



RelianceCyber

APT29 Threat Actor Profile – Introduction

APT29 Alternative Names

BlueBravo, Cozer, Cozy Bear, Cozy Duke, CozyCar, EuroAPT, Midnight Blizzard, NOBELIUM, Office Monkeys, RUS2, The Dukes, UNC2452

About APT29

The threat actor in question is known under various names such as Nobelium, Midnight Blizzard and APT29. They are a highly dedicated cyberespionage group believed to be affiliated with the Russian foreign intelligence service (SVR).

Nobelium has been active since at least October 2020 and has targeted a wide range of organizations globally, including government entities, diplomatic institutions, technology companies, and critical infrastructure providers.

They are known for their use of phishing campaigns, leveraging compromised email accounts to infiltrate their targets. The group has been attributed to several high-profile attacks, including the 2015 attack against the American Democratic National Committee and the 2020 Sunburst attack targeting SolarWinds products.

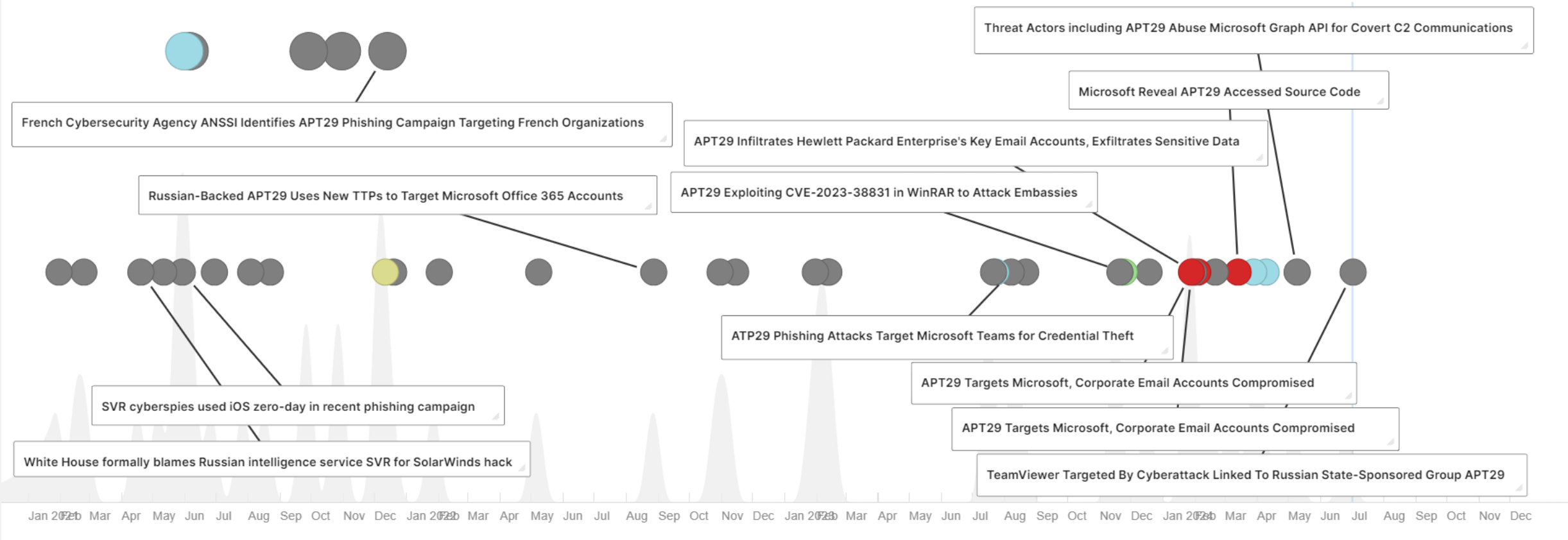
Their most common TTPs include leveraging commercially available residential proxy networks, exploiting misconfigurations in cloud resources, and utilizing the Microsoft Graph API for command-and-control communication.

Recent events involving Nobelium include their targeting of French diplomatic entities and public organizations, a cyberattack against remote software provider TeamViewer, and their exploitation of information stolen from Microsoft's corporate email systems.

Action: Informational only. No actions needed.

RelianceCyber

APT29 Attacks Timeline



Action: Informational only. No actions needed.

RelianceCyber

APT29 Threat Actor Tactics, Techniques and Procedures

Reliance Cyber have reviewed the latest observed activities attributed to the APT29 Threat Actor and below provide a summary of the most important activity.

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 organization but whose accounts remain on the system [T1078.004]. 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.

Action: See page 4 for recommendations.

RelianceCyber

APT29 Threat Actor Tactics, Techniques and Procedures

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 dependent on the system; however, cloud platforms should allow administrators to adjust the validity time as appropriate for their users.

ENROLLING NEW DEVICES TO THE CLOUD

On multiple occasions, the SVR have 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.

Action: See page 4 for recommendations.

RelianceCyber

APT29 Threat Actor Tactics, Techniques and Procedures

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

RESIDENTIAL PROXIES

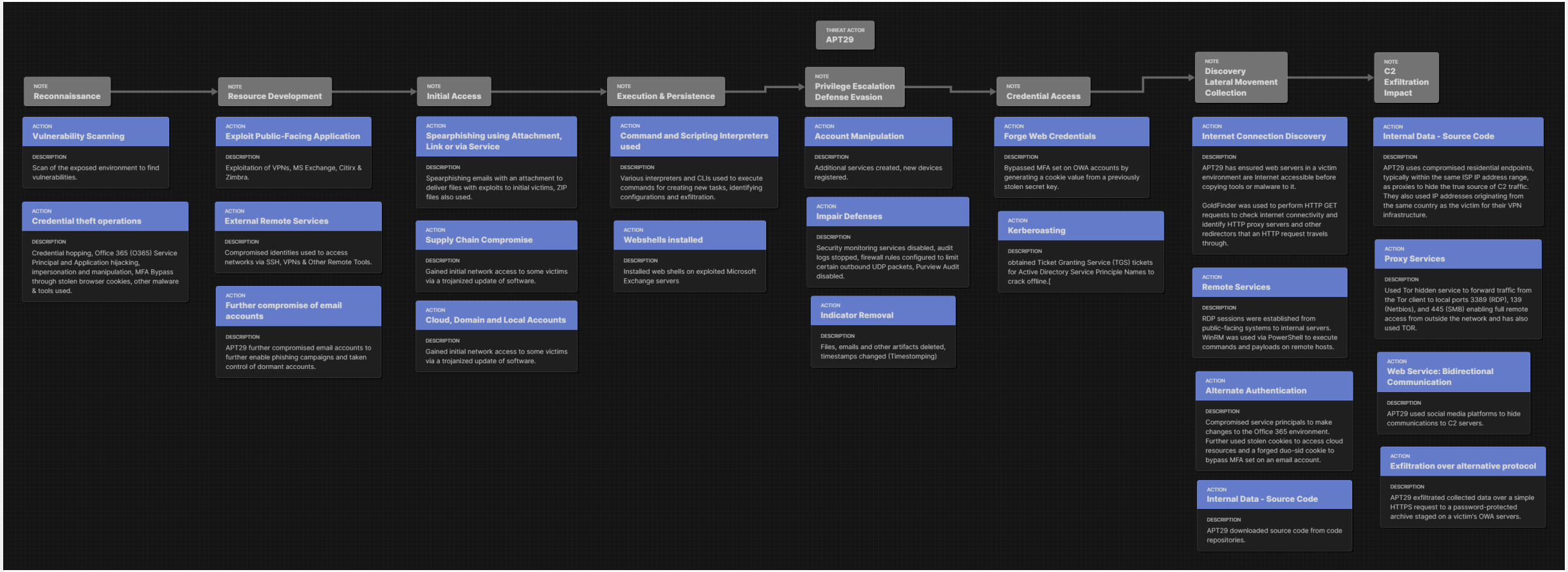
As network-level defenses improve detection of suspicious activity, SVR actors have looked at other ways to stay covert on the internet. A TTP associated with this actor is the use of residential proxies [T1090.002]. Residential proxies typically make traffic appear to originate from IP addresses within 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 defenses 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.

Action: See page 4 for recommendations.

RelianceCyber

APT29 Threat Actor Profile – Notable Observed TTPs



Action: Informational only. No actions needed.

RelianceCyber

Sources & Additional Resources

SVR Cyber Actors Adapt Tactics for Initial Cloud Access

Mitre Attack APT29 Profile

RELIANCECYBER.COM