National Cyber Security Centre
a part of GCHQ

Advisory.

Further TTPs associated with SVR cyber actors

Version 1.0

7 May 2021

Further TTPs associated with SVR cyber actors

Use of multiple publicly available exploits and Sliver framework to target organisations globally

Introduction

This report provides further details of Tactics, Techniques and Procedures (TTPs) associated with SVR cyber actors. SVR cyber actors are known and tracked in open source as APT29, Cozy Bear, and the Dukes.

UK and US governments recently attributed SVR's responsibility for a series of cyber-attacks, including the compromise of SolarWinds and the targeting of COVID-19 vaccine developers.

Alongside this attribution, the United States' National Security Agency (NSA), Federal Bureau of Investigation (FBI), and Cybersecurity and Infrastructure Security Agency (CISA) released an advisory detailing the exploits most recently used by the group. The FBI, Department of Homeland Security (DHS) and CISA also issued an alert providing information on the SVR's cyber tools, targets, techniques and capabilities.

The SVR is Russia's civilian foreign intelligence service. **The group uses a variety of tools and techniques to predominantly target overseas governmental, diplomatic, think-tank, healthcare and energy targets globally** for intelligence gain. The SVR is a technologically sophisticated and highly capable cyber actor. It has developed capabilities to target organisations globally, including in the UK, US, Europe, NATO member states and Russia's neighbours.

The NCSC, NSA, CISA and CSE previously issued a joint report regarding the group's targeting of organisations involved in COVID-19 vaccine development throughout 2020 using WellMess and WellMail malware.

SVR cyber operators appear to have reacted to this report by changing their TTPs in an attempt to avoid further detection and remediation efforts by network defenders.

These changes included the deployment of the open-source tool Sliver in an attempt to maintain their accesses.

The group has also been observed making use of numerous vulnerabilities, most recently the widely reported Microsoft Exchange vulnerability.

Initial access

Further CVEs in use by SVR

As previously reported, the group frequently uses publicly available exploits to conduct widespread scanning (T1595.002) and exploitation (T1190) against vulnerable systems. The group seeks to take full advantage of a variety of exploits when publicised. The group have used:

- CVE-2018-13379 FortiGate
- CVE-2019-1653 Cisco router
- CVE-2019-2725 Oracle WebLogic Server
- CVE-2019-9670 Zimbra
- CVE-2019-11510 Pulse Secure
- CVE-2019-19781 Citrix
- CVE-2019-7609 Kibana
- CVE-2020-4006 VMWare
- CVE-2020-5902 F5 Big-IP
- CVE-2020-14882 Oracle WebLogic
- CVE-2021-21972 VMWare vSphere

This list should not be treated as exhaustive. The group will look to rapidly exploit recently released public vulnerabilities which are likely to enable initial access to their targets. More information about these exploits can be found in previous NCSC advisories on Citrix and VPN vulnerabilities.

Network defenders should ensure that security patches are applied promptly following CVE announcements for products they manage.

Most recently, the group has also scanned for Microsoft Exchange servers vulnerable to CVE-2021-26855. Such activity is typically followed by the use of further exploits and deployment of a webshell (T1505.003) if successful. Other Microsoft Exchange exploits commonly used in conjunction with this CVE include:

- CVE-2021-26857 (SOAP payload)
- CVE-2021-26858 (Arbitrary files)
- CVE-2021-27065 (Arbitrary files)

More information about these exploits and mitigation advice can be found on the NCSC website.

Supply chain compromises

The SolarWinds campaign demonstrates the actor's willingness to target organisations that supply privileged software (T1195.002), such as network management or security applications, to many users or organisations.

These types of attacks give SVR actors initial access to a large number of organisations. From this initial access, the actors select a much smaller number of victims for follow-on compromise activity. These victims are targeted in line with intelligence priorities.

Enterprise products and applications deployed across multiple organisations will be attractive supply chain targets. Products which require access to a significant portion of user or network data to operate are likely to be especially attractive targets. Earlier this year Mimecast and SolarWinds acknowledged compromises, now known to be conducted by SVR cyber operators.

Post-compromise

Additional malware in use by SVR

NCSC and partner industry analysis shows that on multiple occasions, SVR actors used Cobalt Strike, a commercial Red Team command and control framework, to carry out their operations after initial exploitation (e.g. compromise of SolarWinds platform).

The group also deployed GoldFinder, GoldMax and Sibot malware after compromising a victim via SolarWinds. GoldMax is a custom backdoor, GoldFinder is a custom tool – both are written in Golang. Sibot is a simple custom downloader and, unlike other malware in recent use by the group, is written in VBS (T1059.005). Microsoft's analysis of this malware can be found here.

In separate incidents, the NCSC observed that once SVR actors had gained initial access to a victim's network, they then made use of the open-source Red Team command and control framework named Sliver.

The use of the Sliver framework was likely an attempt to ensure access to a number of the existing WellMess and WellMail victims was maintained.

Following the publication of the joint WellMess Advisory SVR cyber operators used the Sliver framework. Sliver is an "…open source, cross-platform adversary

simulation/red team platform…" written in Golang that supports command and control mechanisms over a variety of protocols including Mutual-TLS (T1573.002), HTTP/S (T1071.001) and DNS (T1071.004).

The use of the Sliver framework was likely an attempt to ensure access to a number of the existing WellMess and WellMail victims was maintained following the exposure of those capabilities. As observed with the SolarWinds incidents, SVR operators often used separate command and control infrastructure for each victim of Sliver.

SVR actors have used methods other than malware to maintain persistence on high value targets, including the use of stolen credentials.

Mail server persistence

SVR actors often target administrator mailboxes in order to acquire further network information and access. This is likely in an effort to better understand the target network and obtain further privileges or credentials for persistence and/or lateral movement.

In one example identified by the NCSC, the actor had searched for authentication credentials in mailboxes, including passwords and PKI keys (T1552).

In another incident, the actor leveraged access gained from the SolarWinds campaign to compromise a certificate (T1552.004) issued by Mimecast. The actor used that access to authenticate a subset of Mimecast's products with customer systems (T1199). In this way, the actor was able to abuse the Mimecast Azure app in order to compromise the final target.

The Mimecast Azure application's default application permissions allowed the application full access to all mailboxes in the victim organisation's tenant. Once the actor had gained access to this application, they were able to utilise the applications permissions in order to extract emails from any mailbox used by the victim organisation (T1114.002). For reference, the default permissions that were granted to the Mimecast application can be seen below, along with a definition of the permission:

- "full_access_as_app" under Exchange. This is a highly privileged permission and allows the app to use Exchange Web services with full access to all mailboxes.
- "User.Read" under Microsoft Graph. Microsoft Graph is an API that allows custom applications to access Microsoft O365 data and services. This permission grants the app the ability to read the profile of the signed-in user.

As a result, no further privilege escalation or lateral movement was needed by the actor to access emails of interest.

Mandiant FireEye has detailed a number of detection and mitigation strategies that will help organisations proactively harden Microsoft O365 environments against these techniques. This includes recommendations on how to detect suspicious modifications in a user's O365 mailbox permissions.

MITRE ATT&CK®

This advisory 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	Technique	Procedure
Reconnaissance	T1595.002: Active Scanning	SVR frequently scans for publicly available exploits, most recently including Microsoft Exchange servers vulnerable to CVE-2021-26855.
Initial Access	T1190: Exploit Public-Facing Application	SVR frequently uses publicly available exploits to conduct widespread exploitation of vulnerable systems, including against Citrix, Pulse Secure, FortiGate, Zimbra and VMWare.
	T1195.002: Supply Chain Compromise: Compromise Software Supply Chain	SVR target organisations who supply privileged software to intelligence targets.
	T1199: Trusted Relationship	SVR leveraged access gained from the SolarWinds campaign to compromise a certificate issued by Mimecast, which it then used to authenticate a subset of Mimecast's products with customer systems.
Execution	T1059.005: Command and Scripting Interpreter: Visual Basic	SVR deployed Sibot, a simple custom downloader written in VBS, after compromising victims via SolarWinds.
Persistence	T1505.003: Server Software Component: Web Shell	SVR typically deploy a web shell on Microsoft Exchange servers following successful compromise.
	T1078: Valid Accounts	SVR actors have maintained persistence on high value targets using stolen credentials.

Conclusion

The SVR targets organisations that align with Russian foreign intelligence interests, including governmental, think-tank, policy and energy targets, as well as more time-bound targeting, for example COVID-19 vaccine targeting in 2020.

Organisations are advised to follow the mitigation advice and guidance below, as well as the detection rules in the appendix to help protect against this activity.

Organisations should also follow the advice and guidance in the recently published NSA advisory and the FBI and CISA alert, which detail further TTPs linked to SVR cyber actors.

Reporting to the NCSC

UK organisations affected by the activity outlined in should report any suspected compromises to the NCSC via the website.

Mitigation advice

- SVR actors regularly make use of publicly known vulnerabilities (alongside complex supply chain attacks) to gain initial access onto target networks. Managing and applying security updates as quickly as possible will help reduce the attack surface available for SVR actors, and force them to use higher equity tooling to gain a foothold in the networks.

- Despite the complexity of supply chain attacks, following basic cyber security principles will make it harder for even sophisticated actors to compromise target networks. By implementing good network security controls and effectively managing user privileges organisations will help prevent lateral movement between hosts. This will help limit the effectiveness of even complex attacks. Further NCSC advice is available via the links in the guidance section below.

- Detecting supply chain attacks, such as the Mimecast compromise, will always be difficult. An organisation may be able to detect this sort of activity through heuristic detection methodologies such as the volume of emails being accessed or by identifying anomalous IP traffic. However, the actor frequently uses malicious infrastructure located within the target organisation's own country, likely in an effort to frustrate detection efforts.

- Organisations should ensure sufficient logging (both cloud and on premises) is enabled and stored for a suitable amount of time, to identify compromised accounts, exfiltrated material and actor infrastructure. Mail retention and content policies should also be implemented to reduce the amount of sensitive information available upon successful compromise. Particularly sensitive information, including information relating to network architecture and network security, should be safeguarded appropriately.

- As part of Microsoft's 'Advanced Auditing' functionality, Microsoft have introduced a new mailbox auditing action called 'MailItemsAccessed' which helps with investigating the compromise of email accounts. This is part of Exchange mailbox auditing and is enabled by default for users that are assigned an Office 365 or Microsoft 365 E5 license or for organisations with a Microsoft 365 E5 compliance add-on subscription.

- With 'MailItemsAccessed' enabled, administrators are able to identify almost every single email accessed by a user, giving organisations forensic defensibility to help assert which individual pieces of mail were or were not maliciously accessed by an attacker.

Further guidance

A variety of mitigations will be of use in defending against the campaigns detailed in this report:

- **Protect your devices and networks by keeping them up to date**: use the latest supported versions, apply security patches promptly, use anti-virus and scan regularly to guard against known malware threats. See NCSC guidance: https://www.ncsc.gov.uk/guidance/mitigating-malware.
- **Use multi-factor authentication (/2-factor authentication/two-step authentication) 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
- **Treat people as your first line of defence**. Tell staff how to report suspected phishing emails, and ensure they feel confident to do so. Investigate their reports promptly and thoroughly. Never punish users for clicking phishing links or opening attachments. See NCSC guidance: https://www.ncsc.gov.uk/phishing
- **Set up a security monitoring capability** so you are collecting the data that will be needed to analyse network intrusions. See NCSC Guidance: https://www.ncsc.gov.uk/guidance/introduction-logging-security-purposes.
- **Prevent and detect lateral movement in your organisation's networks**. See NCSC guidance: https://www.ncsc.gov.uk/guidance/preventing-lateral-movement

Appendix

Snort rules

Sliver HTTP request URLs are procedurally generated according to a set pattern, as per the implant/sliver/transports/tcp-http.go file.

- The resource file extension defines the beacon type.
- A random number generator decides whether to include a parent folder in the URL path.
- The parent folder and resource filename are randomly chosen from predefined lists per beacon type.
- The URL query parameter underscore _ is a numeric value which specifies the payload encoding format.
- Results can be further filtered by User-Agent, Accept-Language and PHPSESSID Cookie headers.

```
alert tcp any any -> any any (msg: "Sliver HTTP implant beacon -
robots.txt getPublicKey"; content:"/robots.txt?_="; pcre:"/\AGET
(?:\/(?:static|www|assets|text|docs|sample))?\/robots\.txt\?_=[0-9]{1,9}
HTTP/";)

alert tcp any any -> any any (msg: "Sliver HTTP implant beacon -
sample.txt getPublicKey"; content:"/sample.txt?_="; pcre:"/\AGET
(?:\/(?:static|www|assets|text|docs|sample))?\/sample\.txt\?_=[0-9]{1,9}
HTTP/";)

alert tcp any any -> any any (msg: "Sliver HTTP implant beacon - info.txt
getPublicKey"; content:"/info.txt?_="; pcre:"/\AGET
(?:\/(?:static|www|assets|text|docs|sample))?\/info\.txt\?_=[0-9]{1,9}
HTTP/";)

alert tcp any any -> any any (msg: "Sliver HTTP implant beacon -
example.txt getPublicKey"; content:"/example.txt?_="; pcre:"/\AGET
(?:\/(?:static|www|assets|text|docs|sample))?\/example\.txt\?_=[0-9]{1,9}
HTTP/";)

alert tcp any any -> any any (msg: "Sliver HTTP implant beacon - .jsp
getSessionID"; content:".jsp?_="; pcre:"/\APOST
(?:\/(?:app|admin|upload|actions|api))?\/(?:login|admin|session|action)\.
jsp\?_=[0-9]{1,9} HTTP/";)

alert tcp any any -> any any (msg: "Sliver HTTP implant beacon -
login.php Send"; content:"/login.php?_="; pcre:"/\APOST
(?:\/(?:api|rest|drupal|wordpress))?\/login\.php\?_=[0-9]{1,9} HTTP/";)
```

```
alert tcp any any -> any any (msg: "Sliver HTTP implant beacon -
signin.php Send"; content:"/signin.php?_="; pcre:"/\APOST
(?:\/(?:api|rest|drupal|wordpress))?\/signin\.php\?_=[0-9]{1,9} HTTP/";)

alert tcp any any -> any any (msg: "Sliver HTTP implant beacon - api.php
Send"; content:"/api.php?_="; pcre:"/\APOST
(?:\/(?:api|rest|drupal|wordpress))?\/api\.php\?_=[0-9]{1,9} HTTP/";)

alert tcp any any -> any any (msg: "Sliver HTTP implant beacon -
samples.php Send"; content:"/samples.php?_="; pcre:"/\APOST
(?:\/(?:api|rest|drupal|wordpress))?\/samples\.php\?_=[0-9]{1,9} HTTP/";)

alert tcp any any -> any any (msg: "Sliver HTTP implant beacon -
underscore.min.js Poll"; content:"/underscore.min.js?_="; pcre:"/\AGET
(?:\/(?:js|static|assets|dist|javascript))?\/underscore\.min\.js\?_=[0-
9]{1,9} HTTP/";)

alert tcp any any -> any any (msg: "Sliver HTTP implant beacon -
jquery.min.js Poll"; content:"/jquery.min.js?_="; pcre:"/\AGET
(?:\/(?:js|static|assets|dist|javascript))?\/jquery\.min\.js\?_=[0-
9]{1,9} HTTP/";)
```

YARA Rules

The following Yara rules will aid network defenders in detecting Sliver. It should be noted that other frameworks may rely on code from the Sliver project (e.g. WireGost). Sliver is also used to conduct legitimate pen-testing activity. Therefore a Sliver detection does not necessarily indicate a compromise by APT29.

```
rule sliver_github_file_paths_function_names {

    meta:

        author = "NCSC UK"

        description = "Detects Sliver Windows and Linux implants based on paths
and function names within the binary"

    strings:

        $p1 = "/sliver/"

        $p2 = "sliverpb."
```

```
        $fn1 = "RevToSelfReq"

        $fn2 = "ScreenshotReq"

        $fn3 = "IfconfigReq"

        $fn4 = "SideloadReq"

        $fn5 = "InvokeMigrateReq"

        $fn6 = "KillSessionReq"

        $fn7 = "ImpersonateReq"

        $fn8 = "NamedPipesReq"

    condition:

        (uint32(0) == 0x464C457F or (uint16(0) == 0x5A4D and
uint16(uint32(0x3c)) == 0x4550)) and (all of ($p*) or 3 of ($fn*))

}
```

```
rule sliver_proxy_isNotFound_retn_cmp_uniq {

    meta:

        author = "NCSC UK"

        description = "Detects Sliver implant framework based on some unique
CMPs within the Proxy isNotFound function. False positives may occur"

    strings:

        $ = {C644241800C381F9B3B5E9B2}

        $ = {8B481081F90CAED682}

    condition:

        (uint32(0) == 0x464C457F or (uint16(0) == 0x5A4D and
uint16(uint32(0x3c)) == 0x4550)) and all of them

}
```

```
rule sliver_nextCCServer_calcs {

    meta:

        author = "NCSC UK"

        description = "Detects Sliver implant framework based on instructions
from the nextCCServer function. False positives may occur"

    strings:

        $ = {4889D3489948F7F94839CA????48C1E204488B0413488B4C1308}

    condition:

        (uint32(0) == 0x464C457F or (uint16(0) == 0x5A4D and
uint16(uint32(0x3c)) == 0x4550)) and all of them

}
```

About this document

This advisory is the result of a collaborative effort by United Kingdom's National Cyber Security Centre (NCSC), the United States' National Security Agency (NSA), the Federal Bureau of Investigation (FBI), and Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA).

The United States' National Security Agency (NSA) agrees with this attribution and the details provided in the report.

This advisory 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.

Disclaimer

This report draws on information derived from NCSC and industry sources. Any NCSC findings and recommendations made have not been provided with the intention of avoiding all risks and following the recommendations will not remove all such risk. Ownership of information risks remains with the relevant system owner at all times.