

Brute Ratel C4

By Chetan Nayak

Archived: 2026-04-05 22:04:48 UTC

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 Management ×

Add Payload Profile

*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

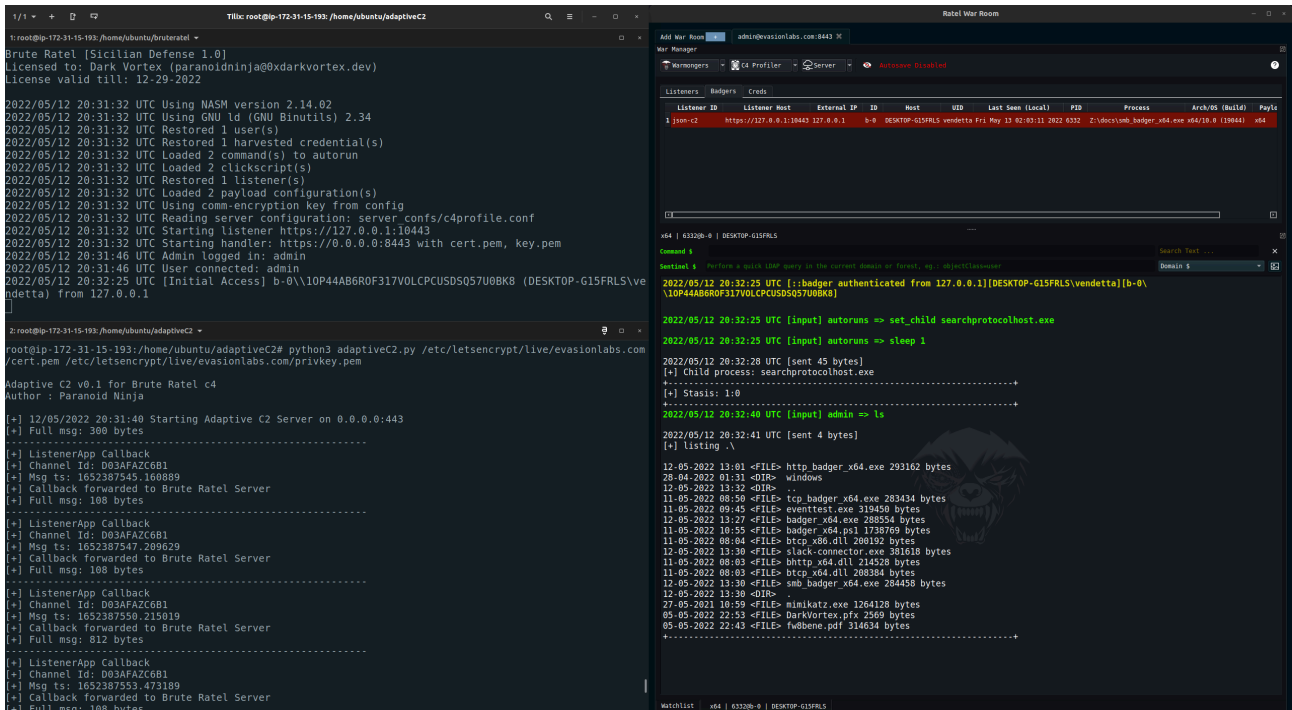
+ Add Header Content-Type cation/dns-message

Die if C2 is inaccessible? (Initialization only)

Save

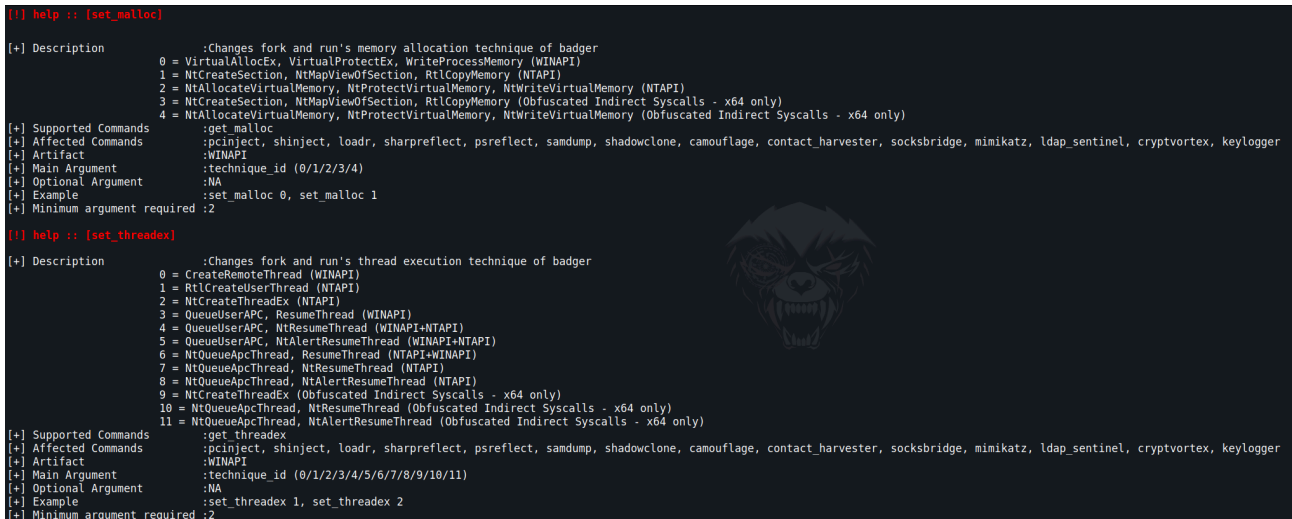
External C2 Channels

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



Indirect Syscalls

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



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

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.

The screenshot shows the Ldap Sentinel application interface. At the top, there is a dropdown menu set to 'b-0'. Below it, several radio buttons are visible: 'SPN Recon', 'User Recon' (which is selected), 'Group Recon', 'Computer Recon', and 'GPO Recon'. Underneath, there are more options: 'Request all user attributes from current domain' (unselected), 'Prebuilt query' (selected) with a dropdown set to 'cn' and a text input field containing '*', and a checkbox for 'Forest (Default action is to run on the current domain)' which is checked. Below the GUI is a terminal window titled 'Command \$' showing the following output:

```
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 Catalog
=====
[+] 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

The screenshot shows a Kali Linux terminal window with the following components:

- Top Bar:** Contains tabs for 'Listeners', 'Badgers', 'Creds', and 'Click Script X'. A dropdown menu shows 'b-0'.
- Click Script Panel:** A table with two columns: 'Click Script' and 'Commands'.

Click Script	Commands
1 Credential Dumping	1 id
2 Discovery	2 pwd
	3 ipstats
	4 psreflect echo \$psversiontable
	5 net users
	6 scquery
- Terminal Output:**

```
x64 | 12912@b-0 | DESKTOP-G15FRLS  
Command $  
Sentinel $ Perform a quick LDAP query in the current domain or forest, eg.: objectClass=us... Domain $  
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
Stack Frame Chaining	Yes	No	No
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
Unhook DLL Load Notifications	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
Advanced Module Stomping with PEB Hooking	Yes	Yes	Yes
In-Memory PE and RDLL Execution	Yes	Yes	Yes
In-Memory BOF Execution	Yes	Yes	Yes
In-Memory Dotnet Execution	Yes	Yes	Yes
Network Malleability	Yes	Yes	Yes
Built-In Anti-Debug Features	Yes	Yes	Yes
Module stomping for BOF/Memexec	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

Source: <https://bruteratel.com/>