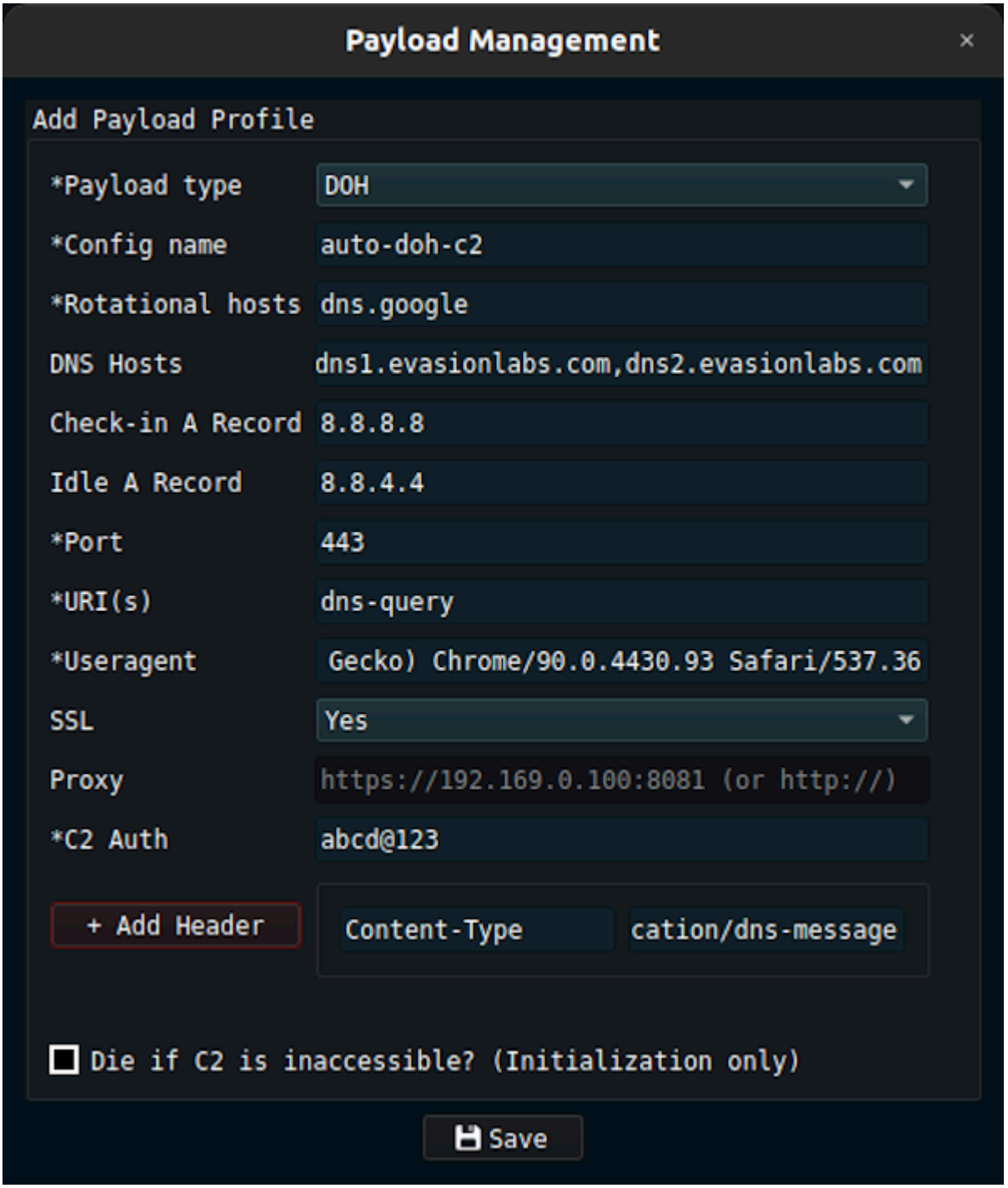
Brute Ratel C4

By Chetan Nayak

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

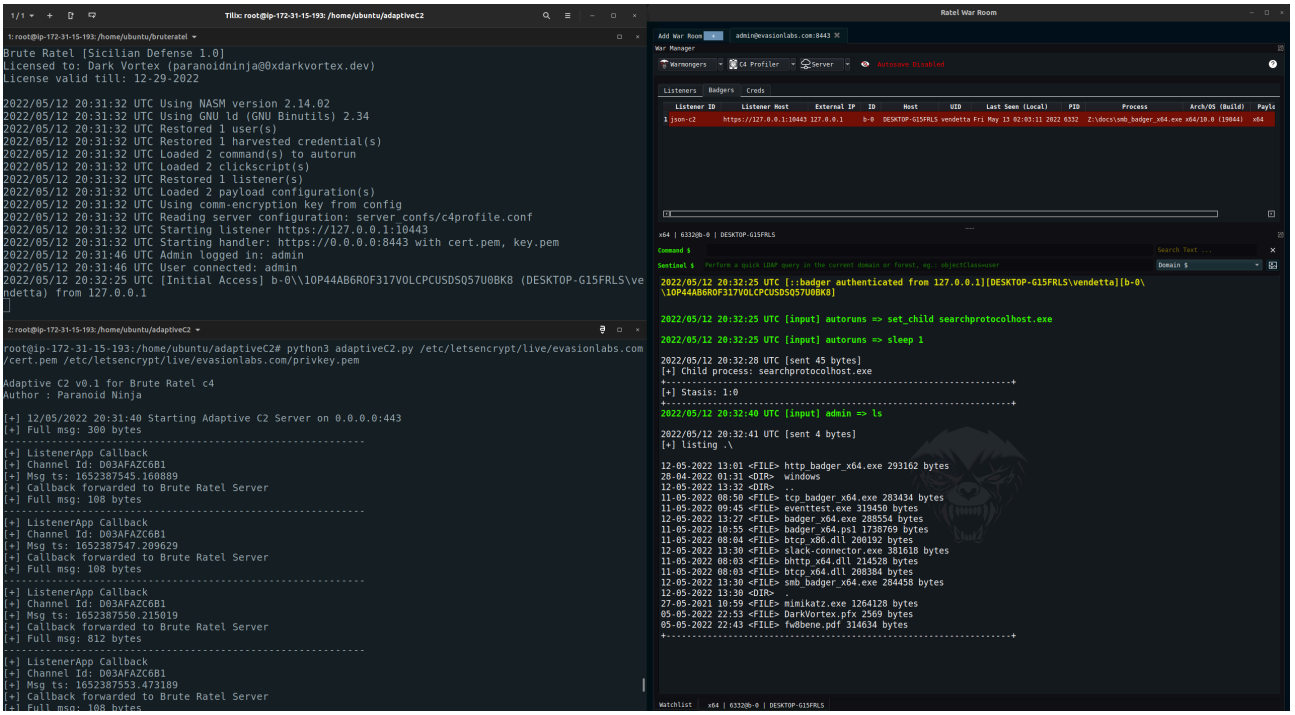
DNS Over HTTPS

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



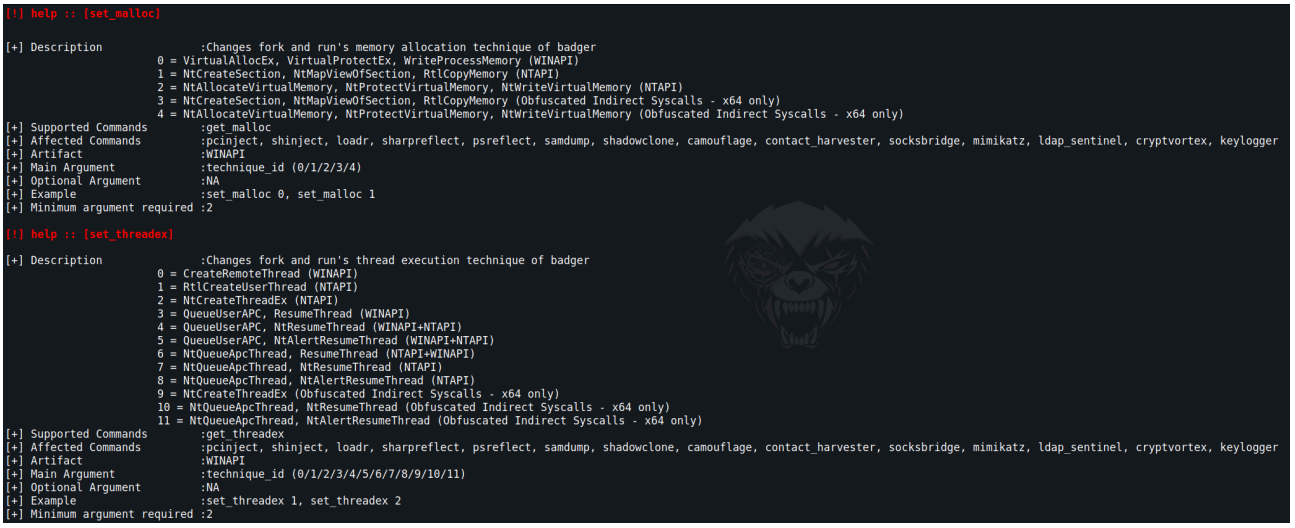
External C2 Channels

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

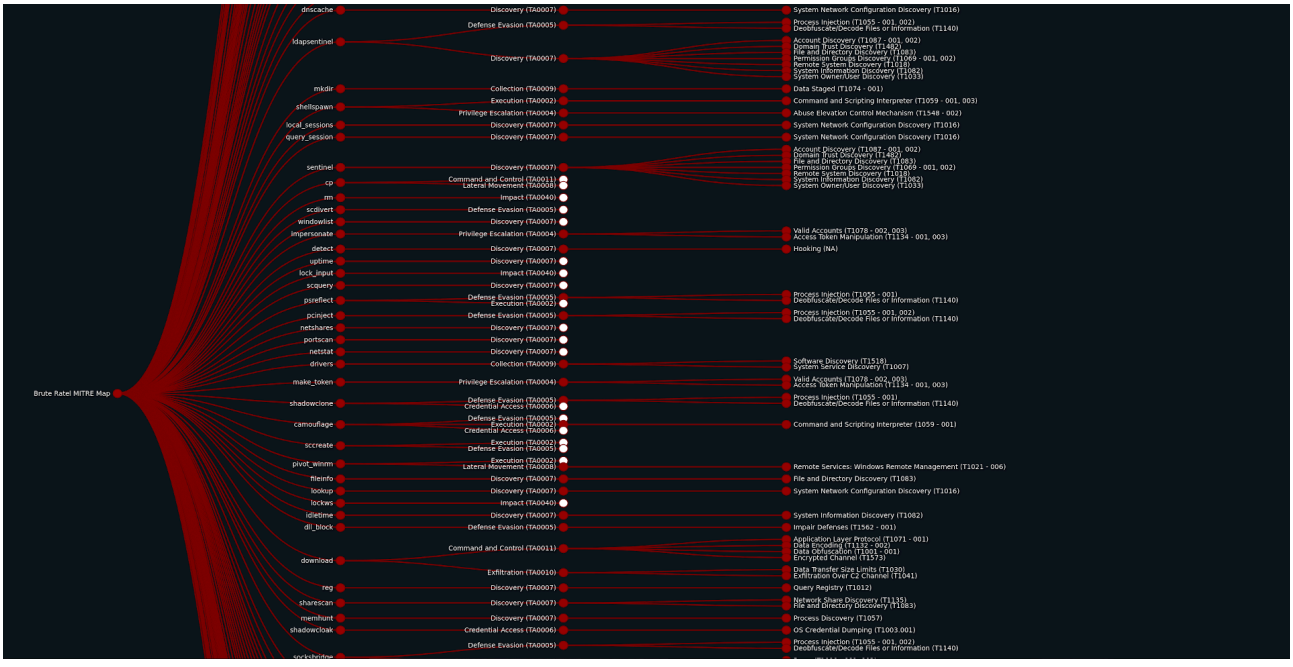
Badger provides various techniques to hunt EDR userland hooks and DLL, and avoid triggering them using various syscall obfuscation and debugging techniques

```
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
```

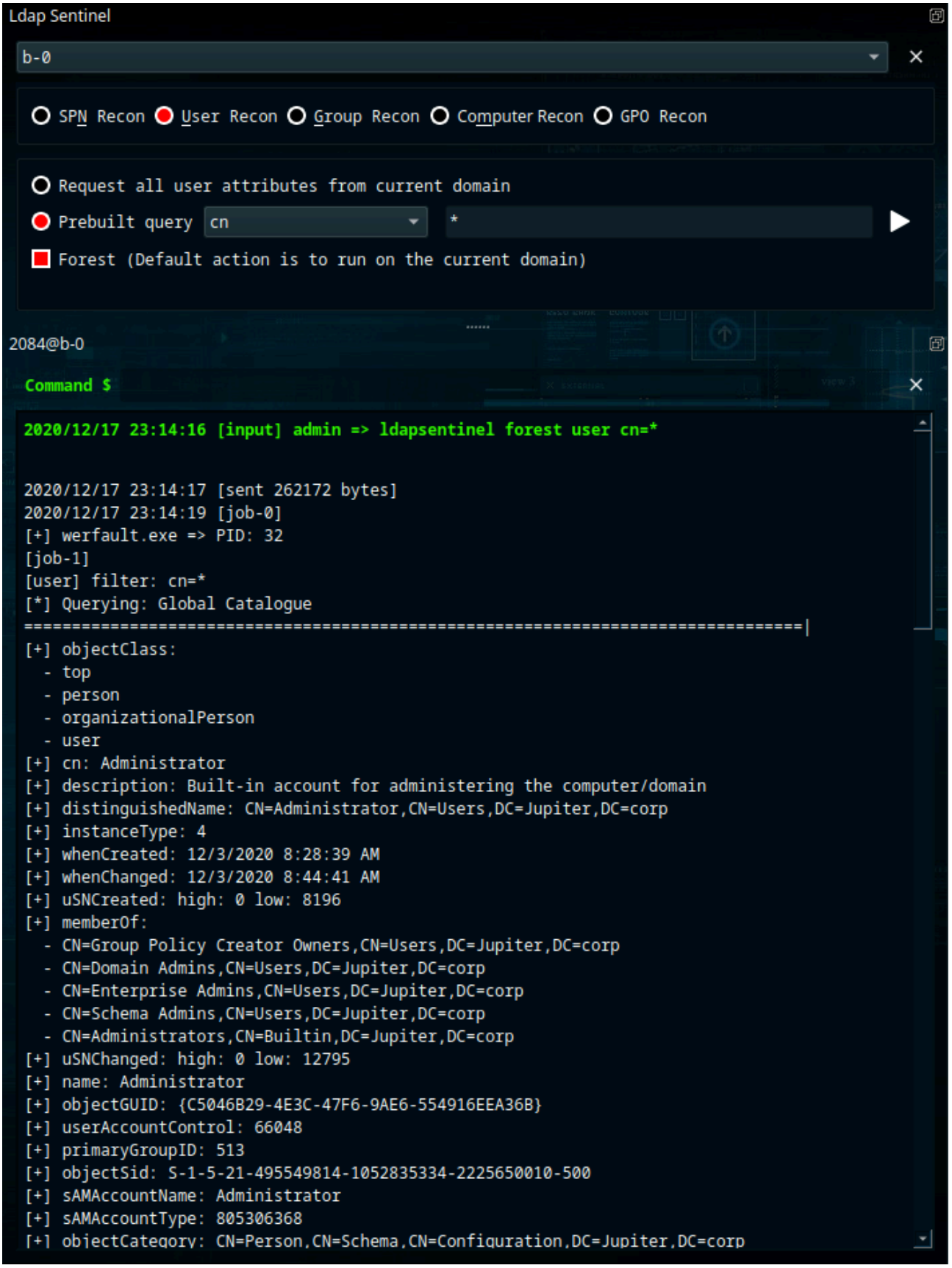
Brute Ratel MITRE graph

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



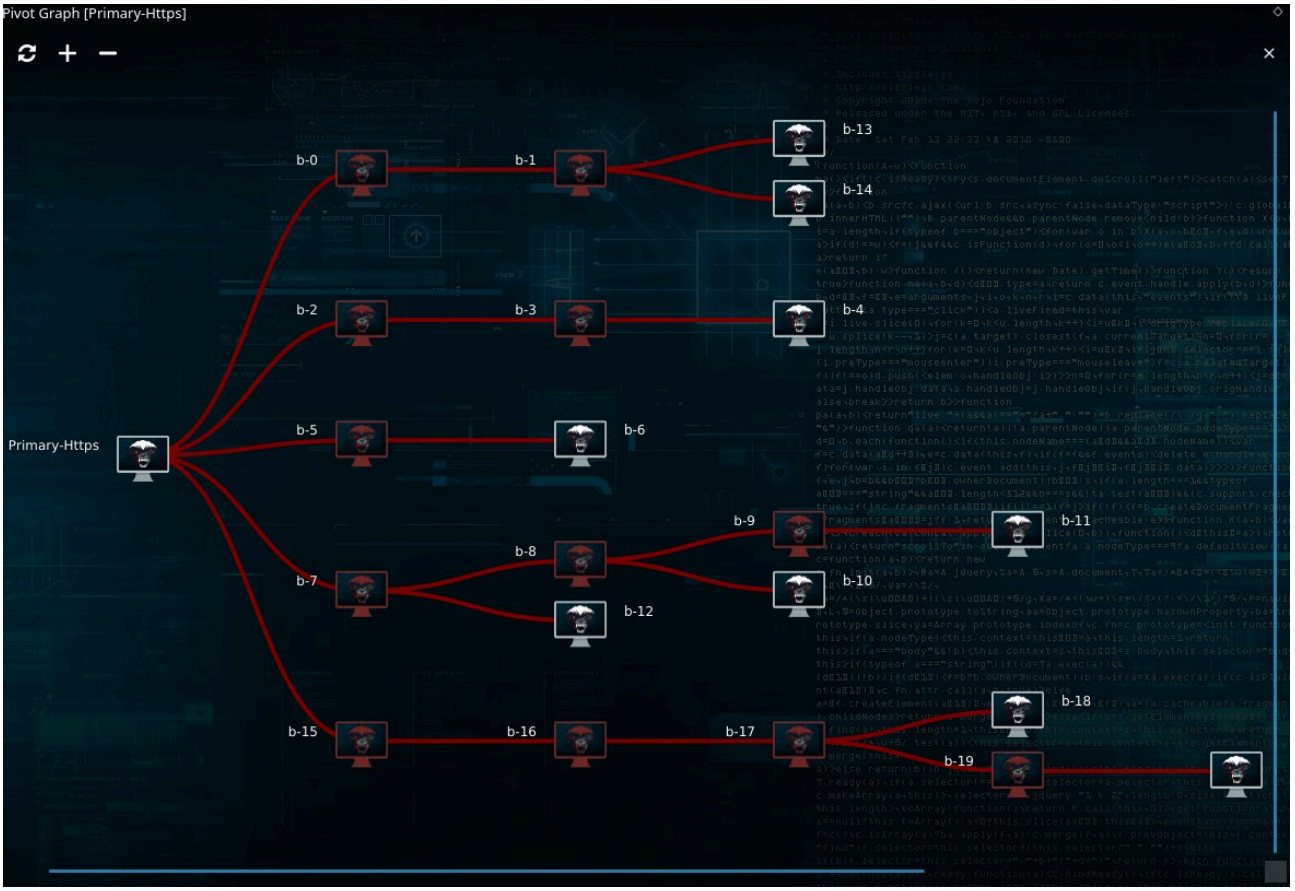
One stop for all your LDAP queries

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.



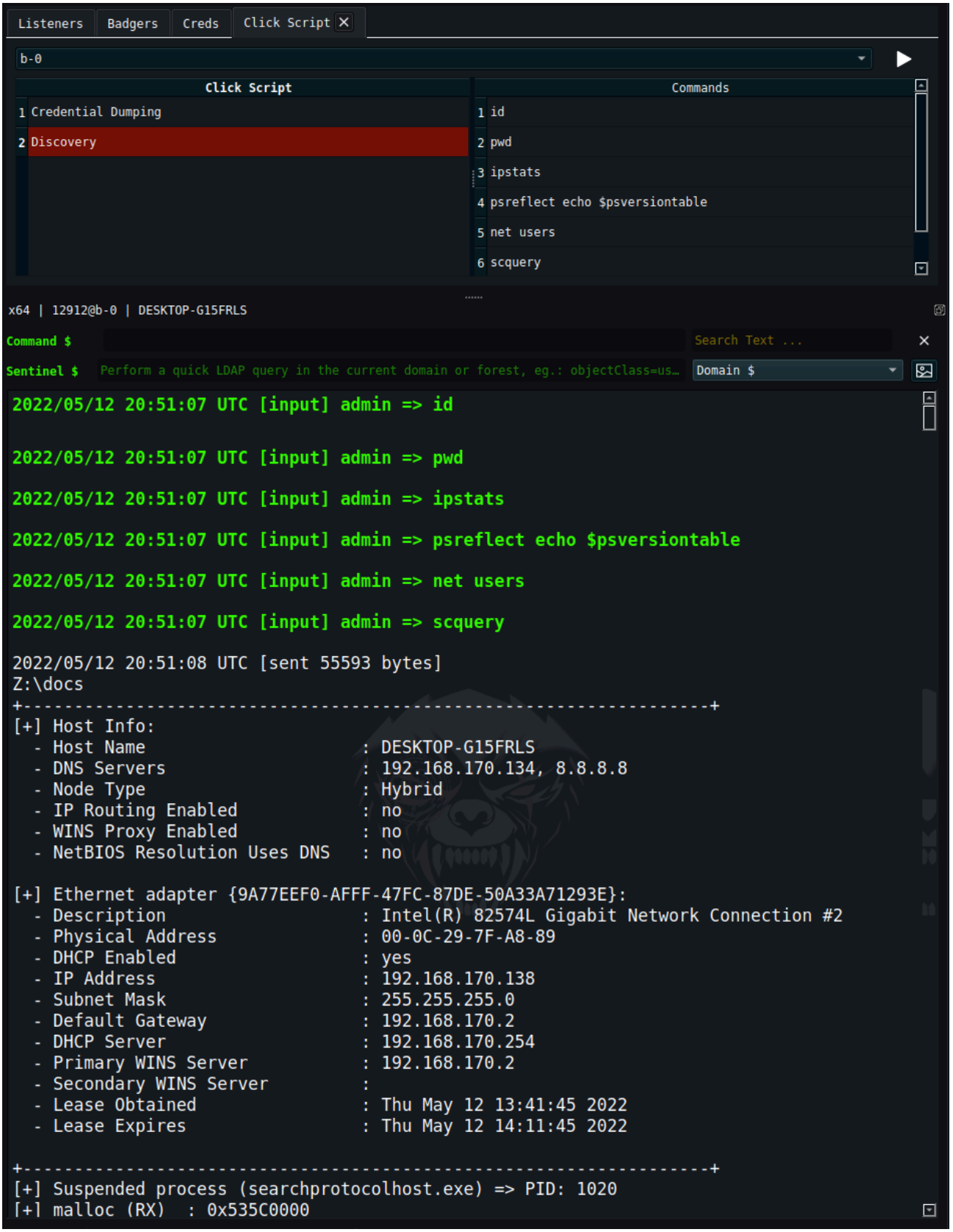
Multiple Command and Control Channels

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



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/