

SpecterOps Blog

Filters



Q Search Blog

```
└─$ ./ghostsurf -t https://passwordstate.ludus.domain -dkr | tee output.txt

NTLM relay browser session hijacking

[+] Impacket Library Installation Path: /home/kali/ghostsurf/venv/lib/python3.13/site-packages/impacket
[*] Target: https://passwordstate.ludus.domain
[*] SOCKS proxy started. Listening on 127.0.0.1:1080
[*] HTTP Socks Plugin loaded..
[*] HTTPS Socks Plugin loaded..
[*] SOCKS proxy: 127.0.0.1:1080
[*] Kernel-mode auth workaround ENABLED
[*] Keep-relaying mode ENABLED (will reload targets after success)
[*] Setting up SMB Server on port 445
[*] Setting up HTTP Server on port 80
  * Serving Flask app 'lib.relay.servers.sockserver'
  * Debug mode: off
[*] Setting up WCF Server on port 9389
[*] Setting up RAW Server on port 6666

[*] Servers started, waiting for connections
Type help for list of commands
```

RESEARCH & TRADECRAFT

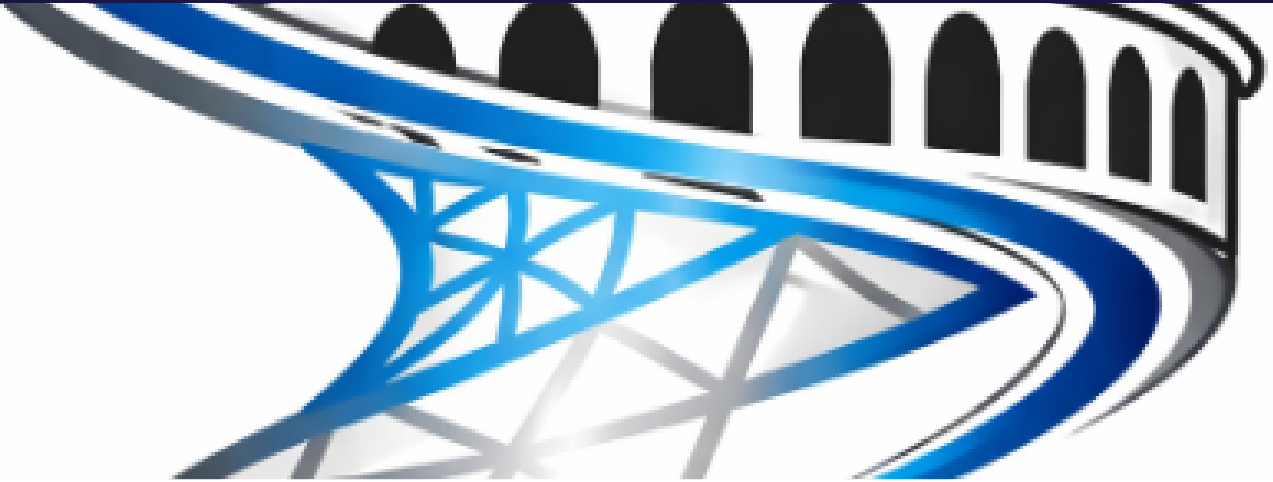
ghostsurf: From NTLM Relay to Browser Session Hijacking

TL;DR: ntlmrelay's SOCKS proxy works great for SMB and MSSQL but fails when you try to browse a web application...

By: Allen DeMoura

17 mins





RESEARCH & TRADECRAFT

^ Saved Queries

Auto-run selected query

```

1 MATCH p=(:jamf_Account)-[r]->(:jamf_Computer)
2 WHERE r.traversable
3 RETURN p

```

Tag Save Run

BLOODHOUND

Expanding Attack Path Management to macOS Environments

Introduction Attack path management has historically focused on identity systems like Active Directory and Entra ID. That focus made sense....

By: Jared Atkinson

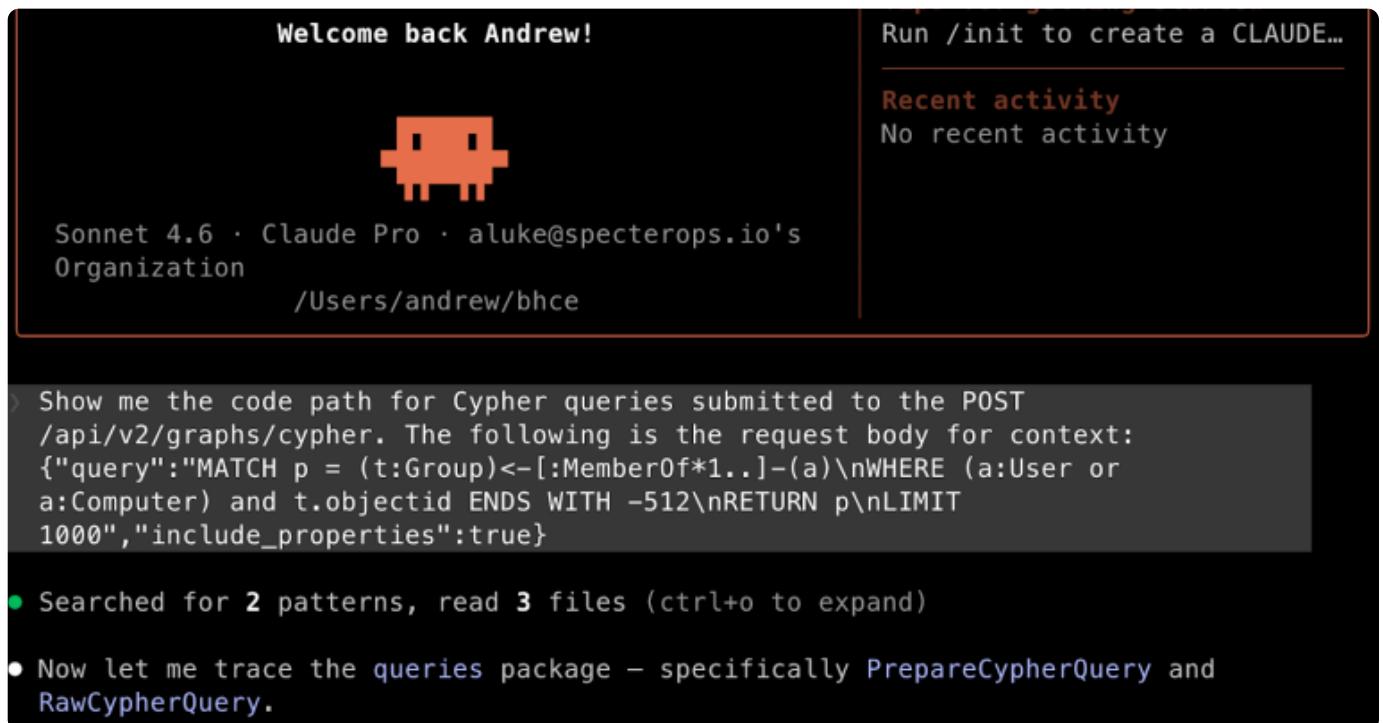
11 mins

JamfHound v1.1

RESEARCH & TRADECRAFT

JamfHound v1.1 Update: SSO Attack Paths and Okta Additions

TL;DR : New SSO Attack Paths and Okta Edges in JamfHound: Updates have been added to the JamfHound OpenGraph collector...



RESEARCH & TRADECRAFT

Leveling Up Secure Code Reviews with Claude Code

TL;DR: Claude Code is a force multiplier when performing secure code reviews during an assessment. In this post, we discuss...

By: Andrew Luke

18 mins



RESEARCH & TRADECRAFT

Attack Paths Don't Stop at Identity Providers

Modeling Okta in BloodHound Enterprise to uncover cross-platform identity risk Introduction Identity is no longer confined to a single system....

By: Jared Atkinson

10 mins



RESEARCH & TRADECRAFT

RTFM: Read The Fatal Manual – When Vendor Documentation Creates Critical Attack Paths

TL;DR: Trusted vendor documentation across 16 major technology companies were actively guiding administrators to deploy critical misconfigurations (often Active Directory...)

By: Martin Sohn Christensen

55 mins



BLOODHOUND

Discovering Unexpected Okta Attack Paths with BloodHound

TL;DR: OktaHound is a new data collector for the Okta Platform that ingests information about entities and their relationships within...

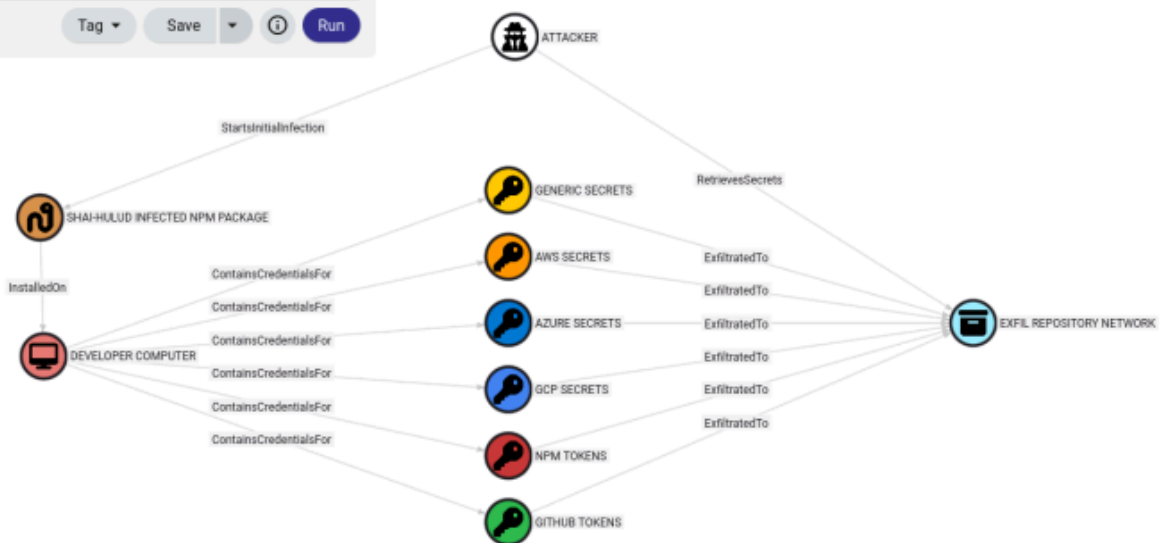
By: Michael Grafnetter

15 mins

```

1 match p=(:Attacker)-[:]->(:InfectedNPMPackage)-
  [:InstalledOn]->(:Computer)-[:ContainsCredentialsFor]-
  >()-[:]->(:GHRepository)
2 where a.name = 'EXFIL REPOSITORY NETWORK'
3 match q=(:Attacker)-[:RetrievesSecrets]-
  (:GHRepository)
4 return p,q

```



Sign up for the latest updates

Email*

Submit

By clicking Sign Up you're confirming that you agree with our Terms and Conditions.



Email:

Submit

Platform

- BloodHound Enterprise
- BloodHound Community Edition

Services and Tradecraft

- Offensive Services
- TRAINING
- Red Team Operations
- Identity-Driven Offensive Tradecraft
- Detection
- Tradecraft Analysis
- Active Directory
- Azure

Solutions

 SOLUTIONS

INDUSTRIES

SpecterOps expands Identity Attack Path Management to Okta, GitHub, and Mac.

[Learn More](#)



Resources

[Research](#)

[Blog](#)

[Events](#)

[Podcasts](#)

[Open Source Tools](#)

Company

[Why SpecterOps](#)

[News](#)

[Careers](#)

[Contact](#)



Copyright 2026 Specter Ops, Inc. All Rights Reserved.

[Terms of Service](#) | [Privacy Policy](#) | [Security](#) | [Trust Center](#) | [Premera Transparency Files](#)