Sniper Incident Response

Chris Brewer
Consulting Director at Palo Alto Networks / Unit 42

Cactus Con

Agenda

- Shocking statement
- Core concepts
- The Big 4
- Finding wins - FAST
- Case study

Many incident response investigations can be solved within **72 hours**

Background

Sniper Forensics (Created by Chris Pogue)

The process of taking a targeted, deliberate approach to forensic investigations

- Create an investigation plan
- Apply sound logic
  - Alexiou
  - Occam
  - Locard
- Extract what needs to be extracted, nothing more
- Allow the data to provide the answers

Guiding Principles

Locard
Every contact by a criminal leaves a trace

Occam

The simplest explanation is often the right one

OR

Let the data be the data

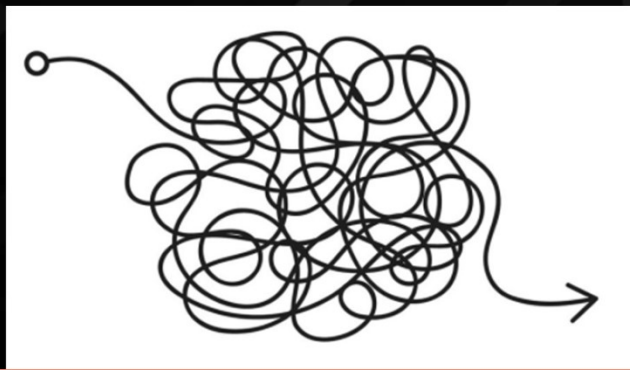
Alexiou Principal

- What questions are you trying to answer?
- What data do you need to answer that question?
- How do you analyze that data?
- What does the data tell you?

Cactus Con

The Problem

- Current way of conducting IR investigations is slow
- One (1) host at a time approach to IR can miss quick wins
- Doesn’t prioritize the key questions from counsel or C-Suite



The Solution

Sniper Incident Response

Fast targeted hunt of data

- Prioritize answering **The Big 4** questions to drive the case
- Task analysts with answering these questions. Assign “workstream leads”
- Sweep multiple hosts at once to drive investigation forward and get quick wins

Questions are the answer

The Big 4

1. What did they take?
2. Are they still here?
3. Where did they go?
4. How did they get in?

Strike Team

Team of people who are skilled at incident response. Primarily utilized for the first 24 - 72 hours of a case.

Incident response! = forensics

- Incident response is focused on fast analysis of the data
- Focuses on quick wins that the forensics team can use for their case
- Strike Team focuses on creating a Hunt Plan and answering The Big 4 questions

Cactus Con

Step 1 - Investigation Plan

Having a plan in place keeps the investigation focused

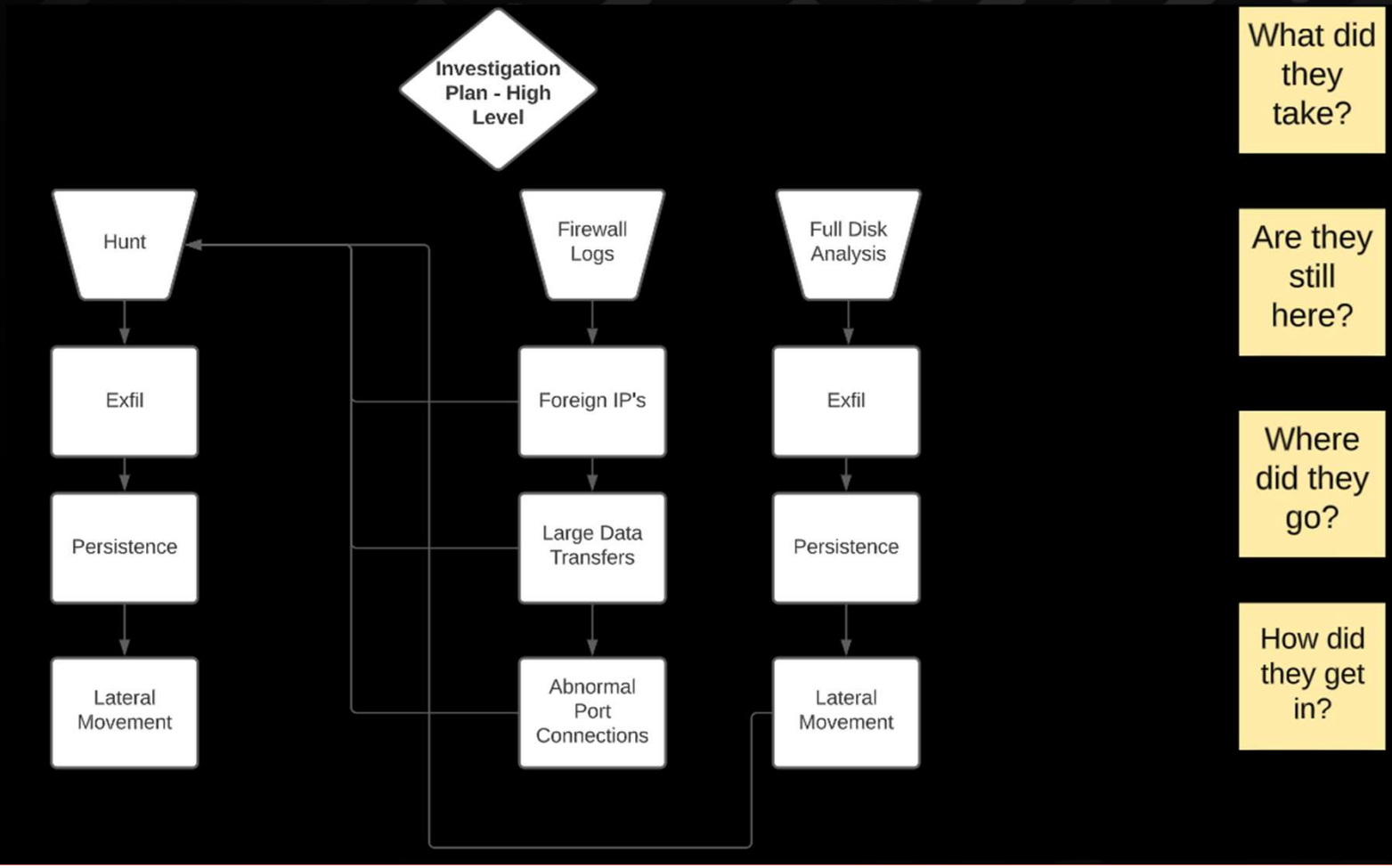
- What are the goals? Write them down
- Focus on the questions counsel / execs need answers for
- What do those answers look like? Have clear criteria for answering them
- If an answer can't be found, show negative evidence

Cactus Con

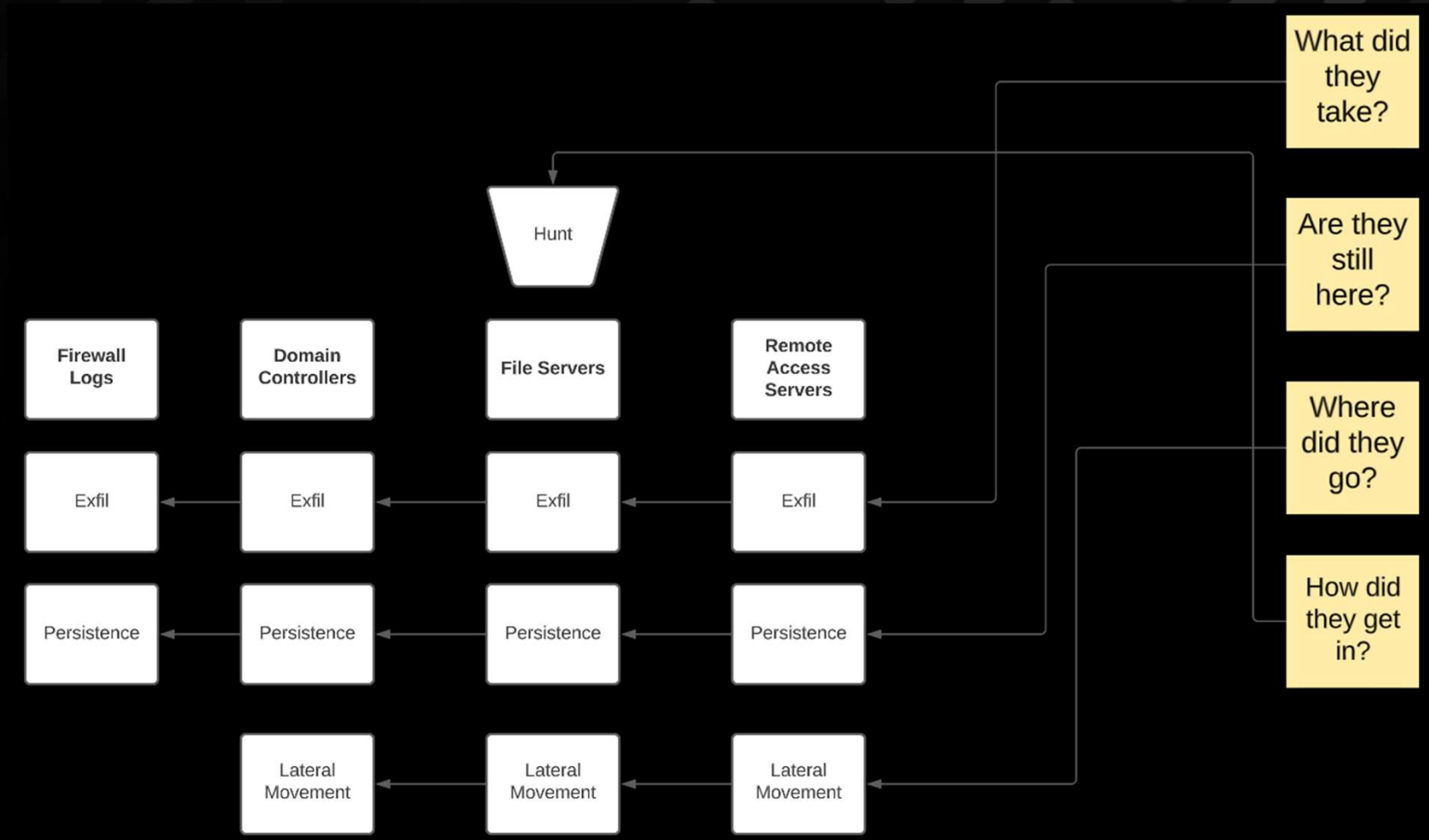
The first 36 hours

- Build your investigation plan
- Deploy tools and collect evidence
- Identify persistence
- Identify exfil

Investigation Plan



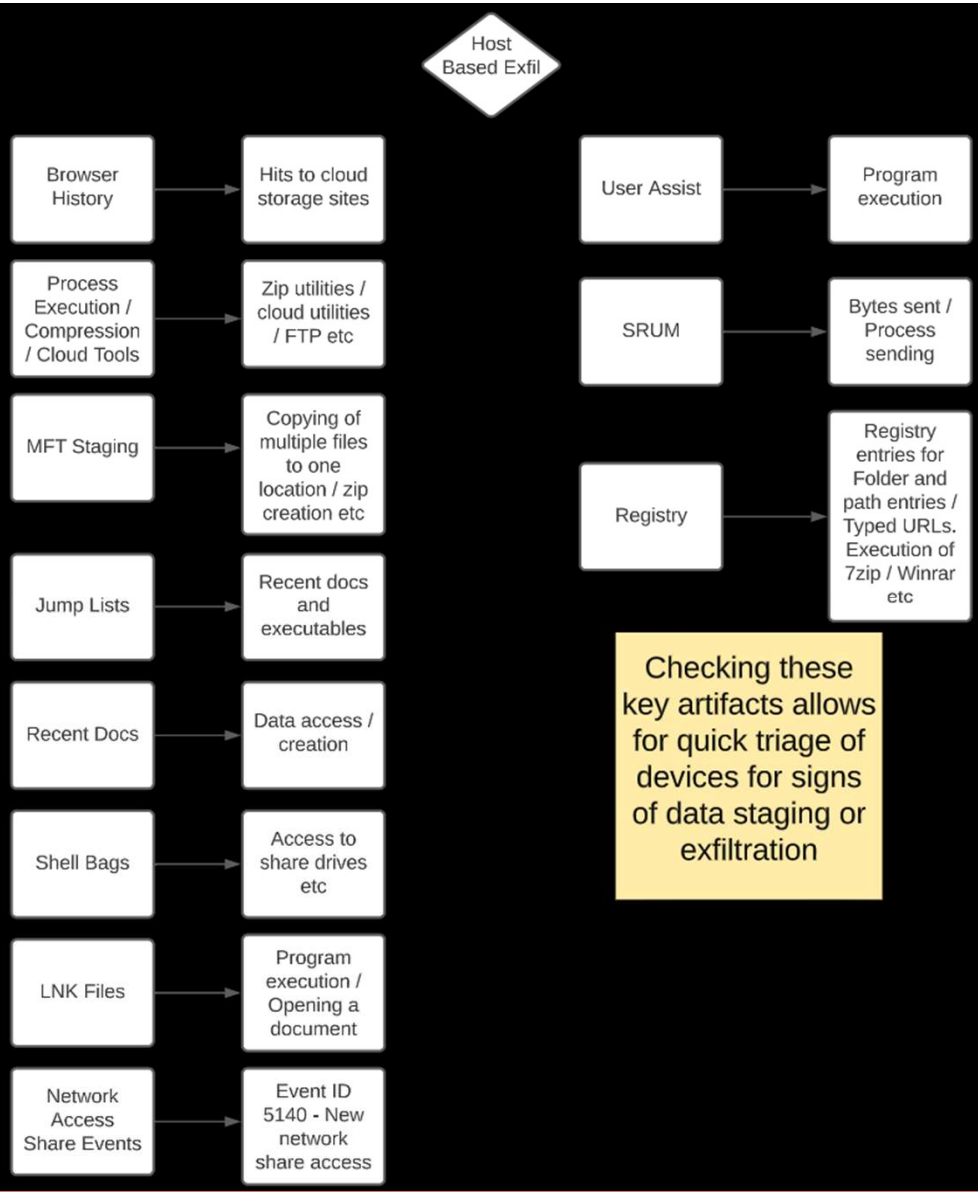
Hunt Plan



Cactus Con

Finding exfil

What did they take?



Some exfil statistics

ID: T1567.002
Typical data exfil occurs over web to cloud sites

- Services:
  - Mega
  - pCloud
  - DropMeFiles
  - Sendspace
  - Files.io
  - OneDrive
  - Google Drive

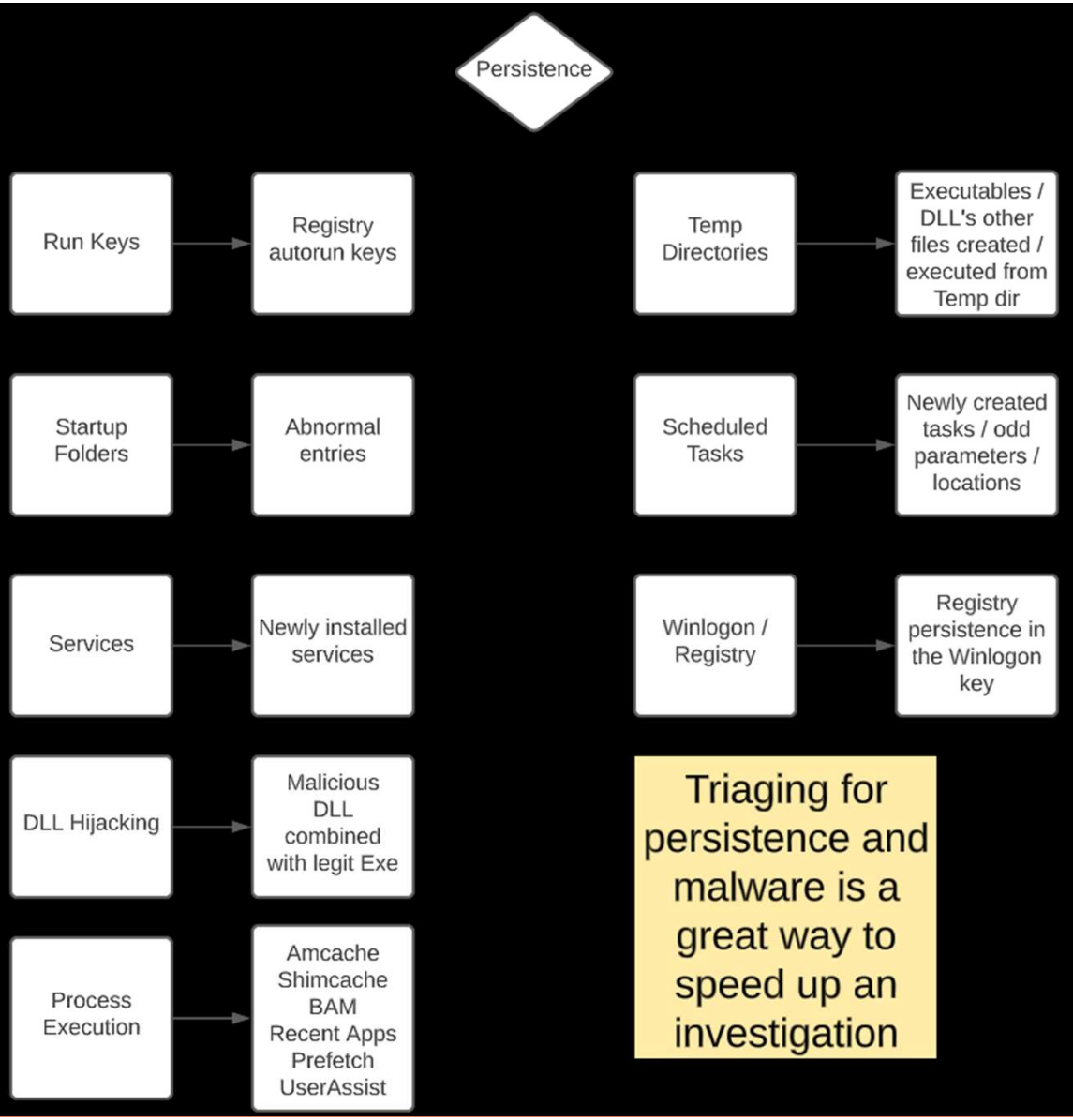
- Tools:
  - Rclone
  - WinSCP
  - FileZilla
  - Cloud-service-specific tools (e.g., MEGAsync, pCloud App, Google Drive for desktop, etc.)

Rclone - quick fact

The rclone.conf file typically contains the bad guys username and password for the site they exfiltrated your data to other common files included filter.txt and rclone.bat

Persistence

Are they still here?



Common persistence mechanisms

- T1053.005: Scheduled Task/Job: Scheduled Task
  - scheduled tasks created by the TA to recurrently execute malicious code.
- T1098: Account Manipulation
  - TA's modified account permissions and/or credentials.
- T1136: Create Account
  - Threat actors create accounts, including local (T1136.001) or domain (T1136.002) accounts, in order to retain persistent access to systems or other resources in victims' environments.
- T1547.001: Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
  - Windows Registry "run keys" are frequently modified to automatically launch malicious programs or scripts.
- T1505.003: Server Software Component: Web Shell
  - TA's leverage web shells as a means of obtaining persistent, backdoor access to victims' internet-facing servers—particularly Microsoft Exchange servers. China Chopper web shells in cases involving Microsoft Exchange vulnerabilities.
- T1543.003: Create or Modify System Process: Windows Service
  - TA's install malicious services or modify existing processes on Windows systems.

Command and Control (TA0011)

- **Post-exploitation tools:**
  - Cobalt Strike
  - Metasploit
  - Sliver – Hi Bishop Fox
  - Brute Ratel C4

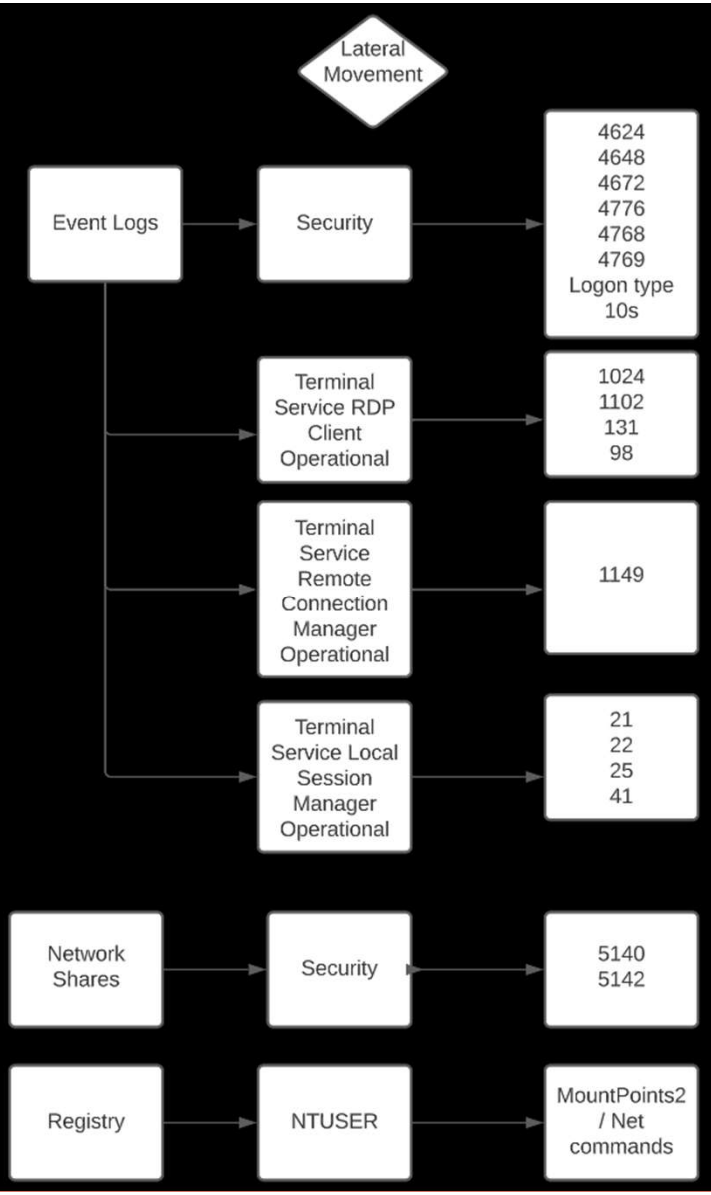
- **Administrative tools (abused by threat actors)**
  - AnyDesk
  - ConnectWise / ScreenConnect
  - LogMeIn
  - PuTTY
  - Splashtop
  - TeamViewer
  - TightVNC

Hours 36 - 52

- Regular client / counsel updates
- Team should ensure C2's are blocked
- Continue hunting for any new / missed persistence
- Identify all systems with interactive access by the TA

Where did they go?

- Use the answers from **“Are they still here?”**
- Compromised accounts / IOC sweeps for malware



Once we have a compromised account, it is easy to query event logs and registry information to see where an attacker went on the network.

Cactus Con

Quick tips for examining event logs

- Parsing / Collection
  - Zimmerman EVTX
  - Logparser
  - Nirsoft
  - Powershell
  - Velociraptor
- Examining
  - Chainsaw - https://github.com/WithSecureLabs/chainsaw
  - Log Parser 2.2 - https://www.microsoft.com/en-us/download/details.aspx?id=24659

PowerShell (not the fastest or prettiest - but it works)
Get-WinEvent -Path C:\someplace\log.evt | Export-CSV C:\someplace\log.csv

Discovery (TA0007)

- Advanced IP Scanner
- Advanced Port Scanner
- AdFind
- BloodHound (and related variants, e.g., SharpHound)
- Cobalt Strike
- net
- nltest
- nmap
- ping
- whoami

Credential Access (TA0006)

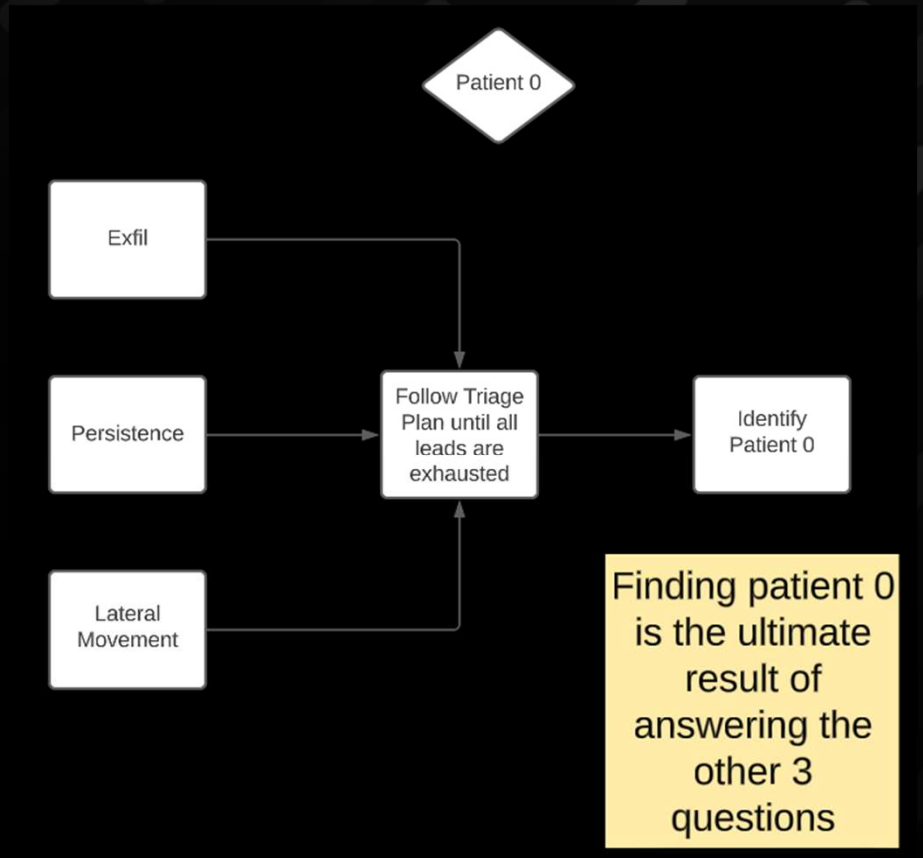
- Mimikatz
- LaZagne
- Impacket secretsdump
- Procdump targeting the LSASS process
- Multifunctional post-exploitation tools (e.g., Cobalt Strike)

Hours 52 - 72

- Continue hunting for any missed malicious activity
- Block C2
- Work the lateral movement backwards to identify first compromised host
- If software vulnerability identified - patch it
- If data exfiltrated - consider bringing in breach counsel

Finding patient 0

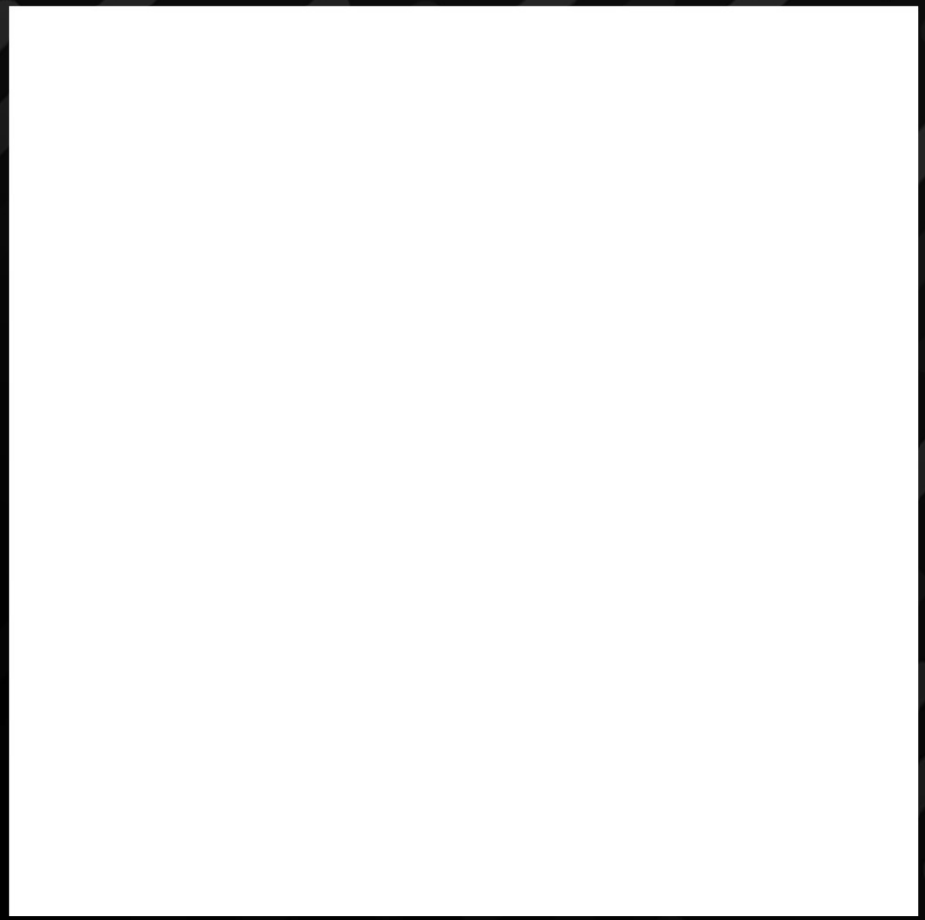
How did they get in?



KEY TAKEAWAYS: ATTACKERS ARE LOOKING FOR EASY WAYS IN

~70%

Phishing and software vulnerabilities cause majority of cyber incidents (overall)



Cactus Con

But what about new data?

- The process of solving The Big 4 is not a one time search. Searches can be re-ran as new hosts come in and there is no need to exclude hosts that have already been analyzed.

- Targeted searches are fast. Minimal impact to hours used for rescanning data if new hosts added.

1. What did they take?
2. Are they still here?
3. Where did they go?
4. How did they get in?

Sidebar - Adaptability

Mindset

- Failures are opportunities to learn
- Challenges are opportunities to learn
- Failure leads to growth
- Be comfortable with the uncomfortable

Flexibility

- Multiple plans to achieve a goal
- Plan ahead
- Ask questions, listen and observe

Case Study

How to Fail at Everything

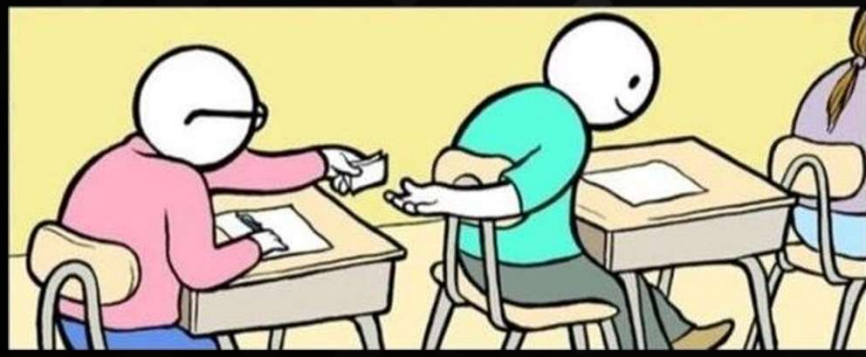
and still not get fired from your job!

Background

- Very large financial company on the east coast
- Over 1 billion in revenue

Scoping notes

- O365 exchange
    - Client experiencing brute force attempts on accounts leading to lockouts - April 10th ish
- 3k endpoints - Windows / Linux / Unix
- Developer team in India (outsourced to 3rd party)
- Went onsite to clients location and had a team supporting remotely



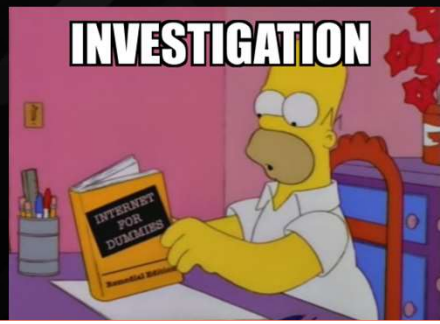
Cactus Con

Initial investigation

- Confirmed brute force attacks originating from IP addresses owned by Choopa LLC (Vultr.com hosting)
- Discovered a few successful logons to outsourced IT supports corporate mailboxes
- 3rd party in India was likely compromised with additional downstream victims

It's important to not stop!

- Looked at the IP addresses connecting to these mailboxes against the VPN logs and discovered several successful authentication events....



Cactus Con

Applying the Sniper IR methodology

- Develop the investigation plan - Answer the Big 4
- Focus on what matters
  - Identify key artifacts / ignore the rest
  - Hunt lateral movement
  - Identify persistence
  - Identify p0

Lots of activity

IP Address	Country	Country_ISO	Organization
.115.3	United States	US	Eqservers LLC
.167.5	India	IN	Jio
76.42.	Netherlands	NL	Choopa, LLC
100.18	Netherlands	NL	HIVELOCITY
76.139	United Kingdom	GB	Choopa, LLC
.61.21	Australia	AU	Choopa, LLC
17.98.	Netherlands	NL	Hostkey B.v.
100.18	Netherlands	NL	HIVELOCITY
17.98.	Netherlands	NL	Hostkey B.v.
17.98.	Netherlands	NL	Hostkey B.v.
100.18	Netherlands	NL	HIVELOCITY
76.81.	Germany	DE	Choopa, LLC
17.98.	Netherlands	NL	Hostkey B.v.
63.21.	United States	US	Choopa, LLC
55.37.	Iran	IR	Mobile Communication Company of Iran PLC
17.98.	Netherlands	NL	Hostkey B.v.
2.187.	Iran	IR	Mobile Communication Company of Iran PLC
2.210.	Iran	IR	Mobile Communication Company of Iran PLC
14.216	Iran	IR	Iran Cell Service and Communication Company
15.221	Iran	IR	Iran Cell Service and Communication Company
6.42.2	Kazakhstan	KZ	JSC Kazakhtelecom
141.38	Italy	IT	Seflow S.N.C. Di Marco Brame' & C.
10.250	Iran	IR	Mobile Communication Company of Iran PLC
06.154	Iran	IR	Mobile Communication Company of Iran PLC
112.141.	Iran	IR	Iran Cell Service and Communication Company

Cactus Con

Sharma logons

- REDACTEDintdc04 - DC - 10.69.130.116
- REDACTEDwadsdcv6 - DC - .208.119
- REDACTEDwcazapp03 - Citrix - 10.69.130.221
- REDACTEDwgqactv01 - Citrix - .157.53
- REDACTEDwgqactv02 - Citrix - .152.128
- REDACTEDwextapv01 - Exchange - 10.69.130.123
- REDACTEDwextapv02 - Exchange - 10.69.130.143
- Alex-pc

Tools deployed and Targets

- PsExec
- ntdsutil
- Powershell
- Mimikatz (64.exe)
- Winrar
- M.bat
- m.zip

Within the same day the threat actor had domain admin credentials
Set additional persistence by creating a privileged account named “Helpdesk”
Pivoted from Windows systems to Linux / Unix servers as well

Lateral movement

TypedURLs
Software\Microsoft\Internet Explorer\TypedURLs
LastWrite Time Thu Jun 22 09:30:12
url1 ->
http://search.live.com/results.aspx?q=connect+to+the+office+365+Security+%26+Compliance+Center+Using+Remote+Powershell&src=IE-SearchBox&Form=IE8SRC
url2 -> http://login.microsoft.com/
url3 -> http://www.google.com/
url4 -> C:\
url5 -> C:\Users[redacted]-pad\AppData
url6 -> \\[redacted]INTDC04\c$
url7 -> \\[redacted]3TK001\c$\WINDOWS
url8 -> \\[redacted]3TK001\c$\WINDOWS\adfs
url9 -> \\[redacted]3TK001\c$
url10 -> [redacted]ADSDCV31\c$\Users
url11 -> [redacted]ADSDCV31\c$
url12 -> [redacted]ADSDCV29\c$
url13 -> [redacted]ADSDCV21\c$
url14 -> [redacted]ADSDCV20\c$
url15 -> [redacted]ADSDCV19\c$
url16 -> [redacted]ADSDCV18\c$
url17 -> [redacted]ADSDC16\c$
url18 -> [redacted]ADSDC15\c$
url19 -> [redacted]ADSDC14\c$
url20 -> [redacted]ADSDC13\c$
url21 -> [redacted]ADSDC12\c$
url22 -> [redacted]ADSDC11\c$
url23 -> [redacted]ADSDC10\c$
url24 -> [redacted]ADSDC09\c$
url25 -> [redacted]ADSDC08\c$

Cactus Con

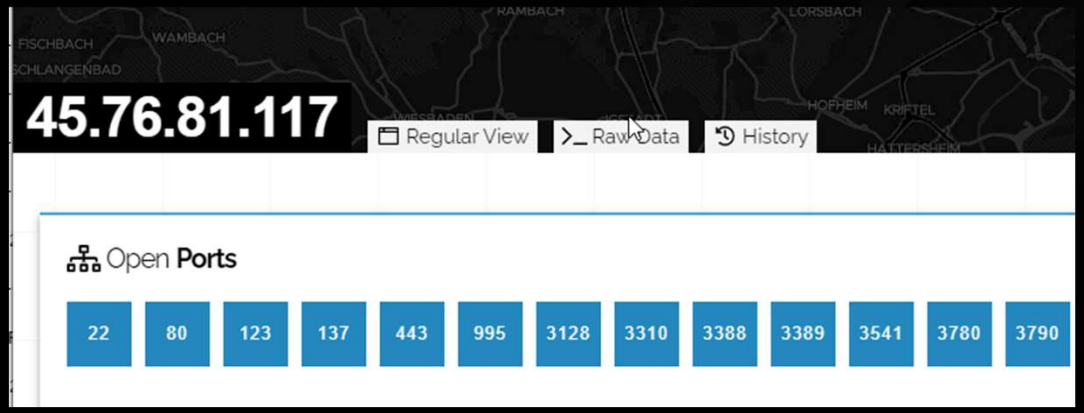
Impact

- **43!** accounts compromised
- Shared secret keys for routers / switches compromised
- Golden tickets and DC's compromised
- Unix/Linux environments compromised
- 3rd party development team was also likely compromised (they are a very large MSP and IT provider)
- Evidence showed admin credentials from the data center administrators also compromised
- Additional lateral movement into partner networks from victim
- Unrelated DIB space networks under attack by the same APT at same time

Hunting

Remember Alex-PC?

- Shodan hunting also returned hits on admin-pc
- Just happened to be running metasploit pro with a self signed cert



At this point....

- TA was reading daily updates
- Bypass the CISO
- Spam phone calls abound
- Revenge!

Cactus Con

Thank you

@br0kenbit

brokenbit.io@protonmail.com

https://www.linkedin.com/in/cebrewer/

https://github.com/br0kenbit ←-- slides will be here

Unit 42 has several open roles - see me for info!

Cactus Con