black hat® USA 2024

AUGUST 7-8, 2024
BRIEFINGS

Surfacing a Hydra

Unveiling a Multi-Headed Chinese State-Sponsored Campaign Against a Foreign Government

Speakers: Mark Parsons & Morgan Demboski

Image: Taylor James s

Introductions

SOPHOS
Defeat Cyberattacks

Morgan Demboski
Threat Intelligence Analyst
Washington, DC
@Morgan_Demboski 🐦

Mark Parsons
Senior Threat Hunter
Charleston, South Carolina, USA
@security_dumpster 🐦
*@_mcp_* Ⓜ

Agenda

Background

Operation Crimson Palace: Stage 1

Cluster Analysis & Assessing Overlap

Operation Crimson Palace: Stage 2

C2 Gap Analysis

SPADE Tool

Takeaways & Q&A

Background

A years-long cyberespionage campaign tracked by Sophos MDR, attributed to Chinese state-sponsored actors

STAC1248

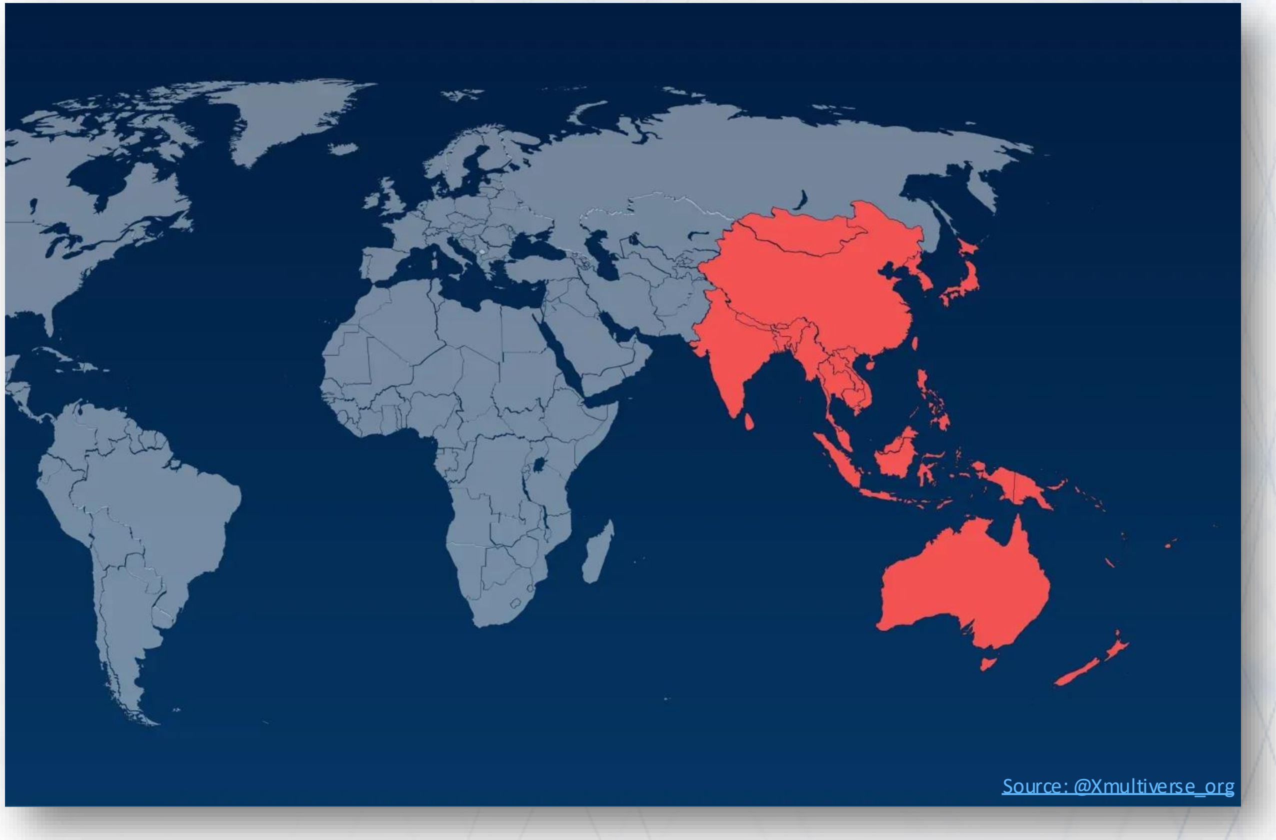
STAC1870

STAC1305

- Two-stage campaign
- Multiple active & coordinated "groups"
- Broad targeting of critical orgs in a SE Asian country

Victimology

- **SE Asian government organization**
  - Campaign later **expanded to other critical organizations** in the country
  - History of conflict with China over South China Sea (SCS)



Source: @Xmultiverse_org

Immediate Challenges

- Onboarded with existing long-term breach
  - Related activity dating back to early 2022
- **Lack of full visibility / major coverage gaps**

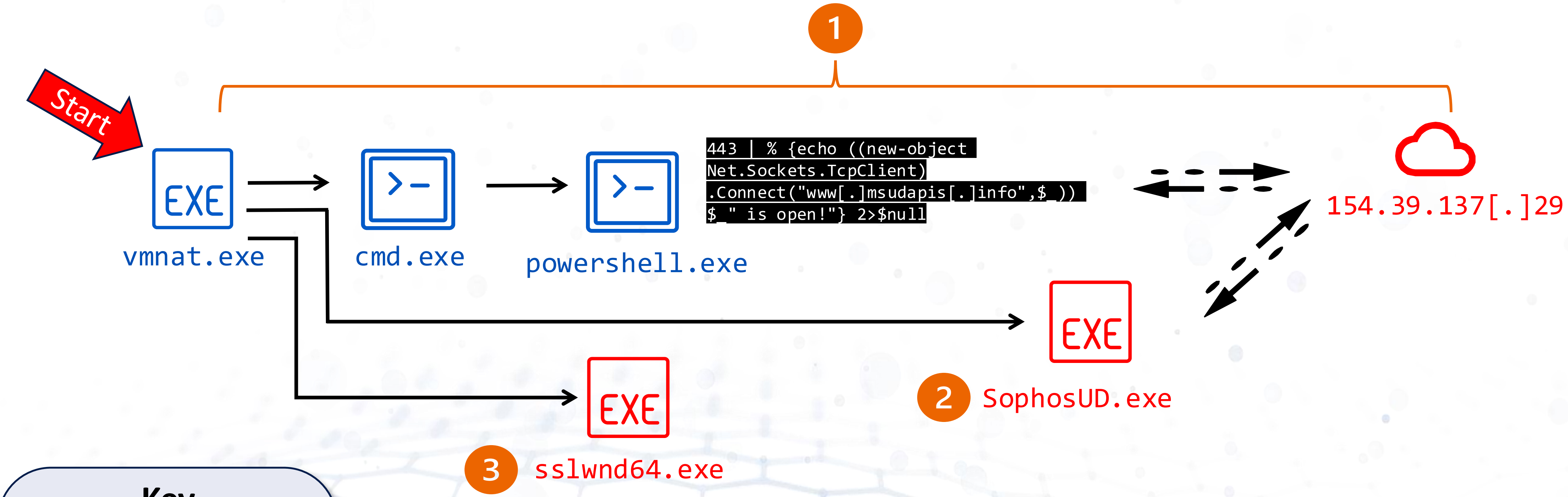
*If we can’t take mitigation actions directly, **what can we as defenders do to make the most of the situation?***

Source: David Truss

Initial Triage

How did it start?

PowerShell TCP Listener



```
443 | % {echo ((new-object
Net.Sockets.TcpClient)
.Connect("www[.]msudapis[.]info",$_))
$_" is open!"} 2>$null
```

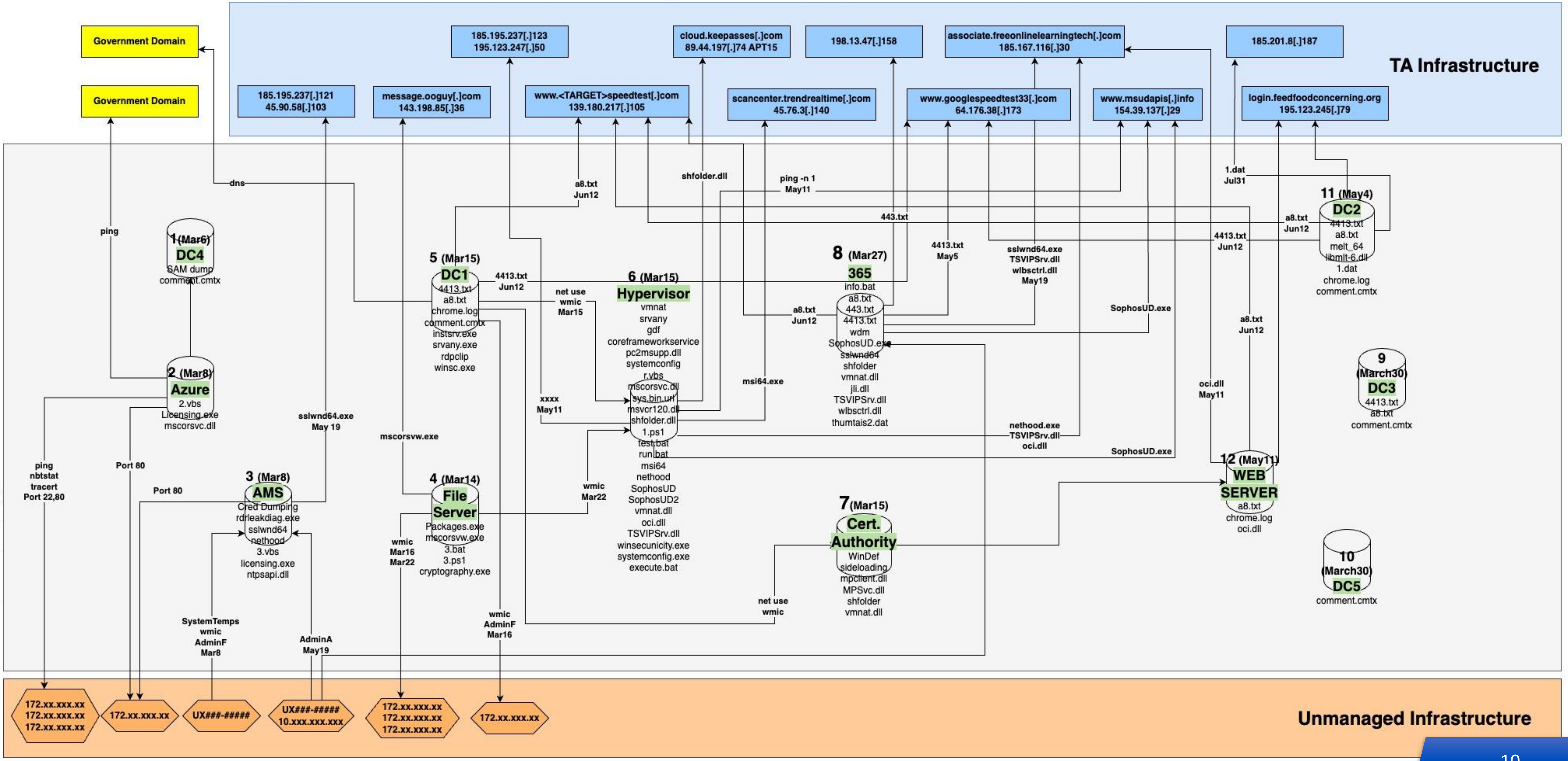
Key

- — Process Action
- >_ LoLBin
- EXE Malicious EXE
- # Execution Order

Execution Context

Host: Office 365 Integrations Server
Path: C:\ProgramData\Microsoft\Vault\vmnat.exe

Within 7 days, we found 13 malware families across ¼ of the org's server infrastructure…



TA Infrastructure

Government Domain

Government Domain

185.195.237[.]123
195.123.247[.]50

cloud.keepasses[.]com
89.44.197[.]74 APT15

198.13.47[.]158

associate.freeonlinelearningtech[.]com
185.167.116[.]30

185.201.8[.]187

185.195.237[.]121
45.90.58[.]103

message.ooguy[.]com
143.198.85[.]36

www.<TARGET>speedtest[.]com
139.180.217[.]105

scancenter.trendrealtime[.]com
45.76.3[.]140

www.googlespeedtest33[.]com
64.176.38[.]173

www.msudapis[.]info
154.39.137[.]29

login.feedfoodconcerning.org
195.123.245[.]79

1 (Mar6) DC4
SAM dump
comment.cmtx

2 (Mar8) Azure
2.vbs
Licensing.exe
mscorsvc.dll

3 (Mar8) AMS
Cred Dumping
rdrleakdiag.exe
sslwnd64
nethood
3.vbs
licensing.exe
ntpsapi.dll

4 (Mar14) File Server
Packages.exe
mscorsvw.exe
3.bat
3.ps1
cryptography.exe

5 (Mar15) DC1
4413.txt
a8.txt
chrome.log
comment.cmtx
instsrv.exe
srvany.exe
rdpclip
winsc.exe

6 (Mar15) Hypervisor
vmnat
srvany
gdf
coreframeworkservice
pc2msupp.dll
systemconfig
r.vbs
mscorsvc.dll
sys.bin.url
msvcr120.dll
shfolder.dll
1.ps1
test.bat
run.bat
msi64
nethood
SophosUD
SophosUD2
vmnat.dll
oci.dll
TSVIPSrv.dll
winsecunicity.exe
systemconfig.exe
execute.bat

7 (Mar15) Cert. Authority
WinDef
sideloading
mpclient.dll
MPSvc.dll
shfolder
vmnat.dll

8 (Mar27) 365
info.bat
a8.txt
443.txt
4413.txt
wdm
SophosUD.exe
sslwnd64
shfolder
vmnat.dll
jli.dll
TSVIPSrv.dll
wlbsctrl.dll
thumtais2.dat

9 (March30) DC3
4413.txt
a8.txt
comment.cmtx

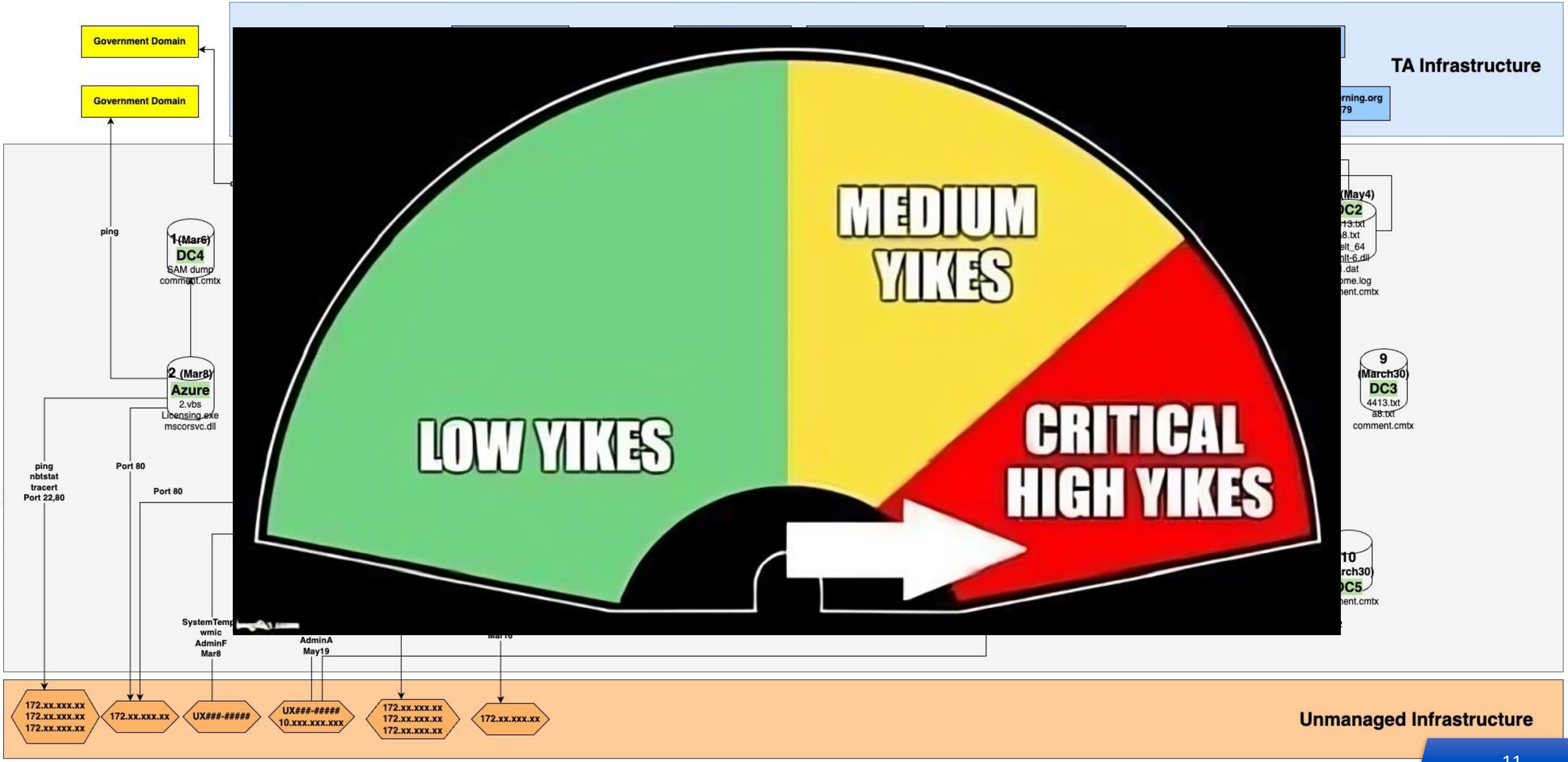
10 (March30) DC5
comment.cmtx

11 (May4) DC2
4413.txt
a8.txt
melt_64
libmlt-6.dll
1.dat
chrome.log
comment.cmtx

12 (May11) WEB SERVER
a8.txt
chrome.log
oci.dll

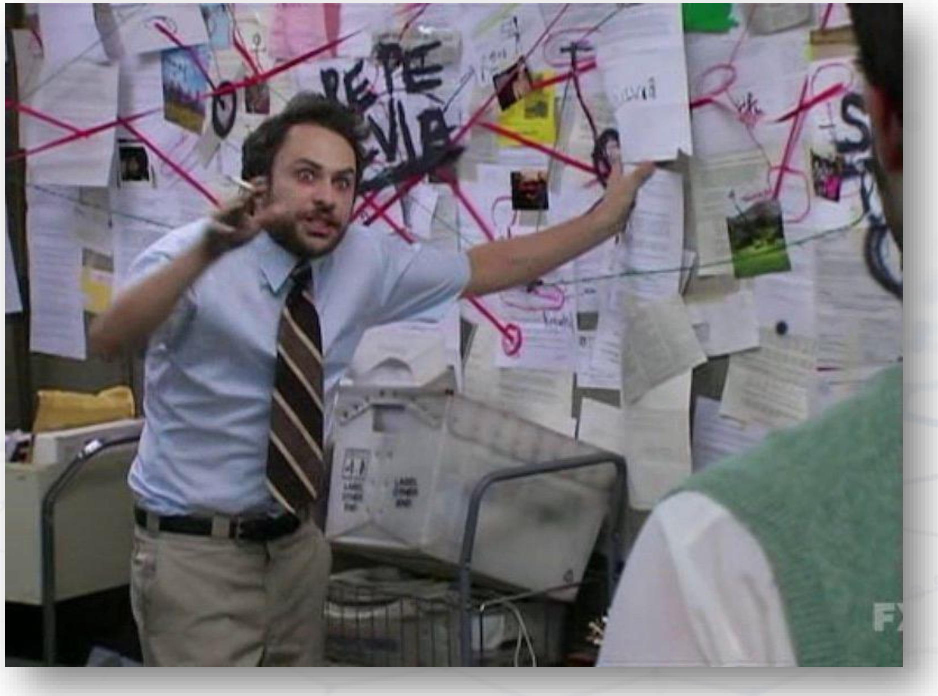
Unmanaged Infrastructure

Within 7 days, we found 13 malware families across ¼ of the org's server infrastructure...



Moving From Wild Hunches to Evidence Driven Theories

How do we go from:



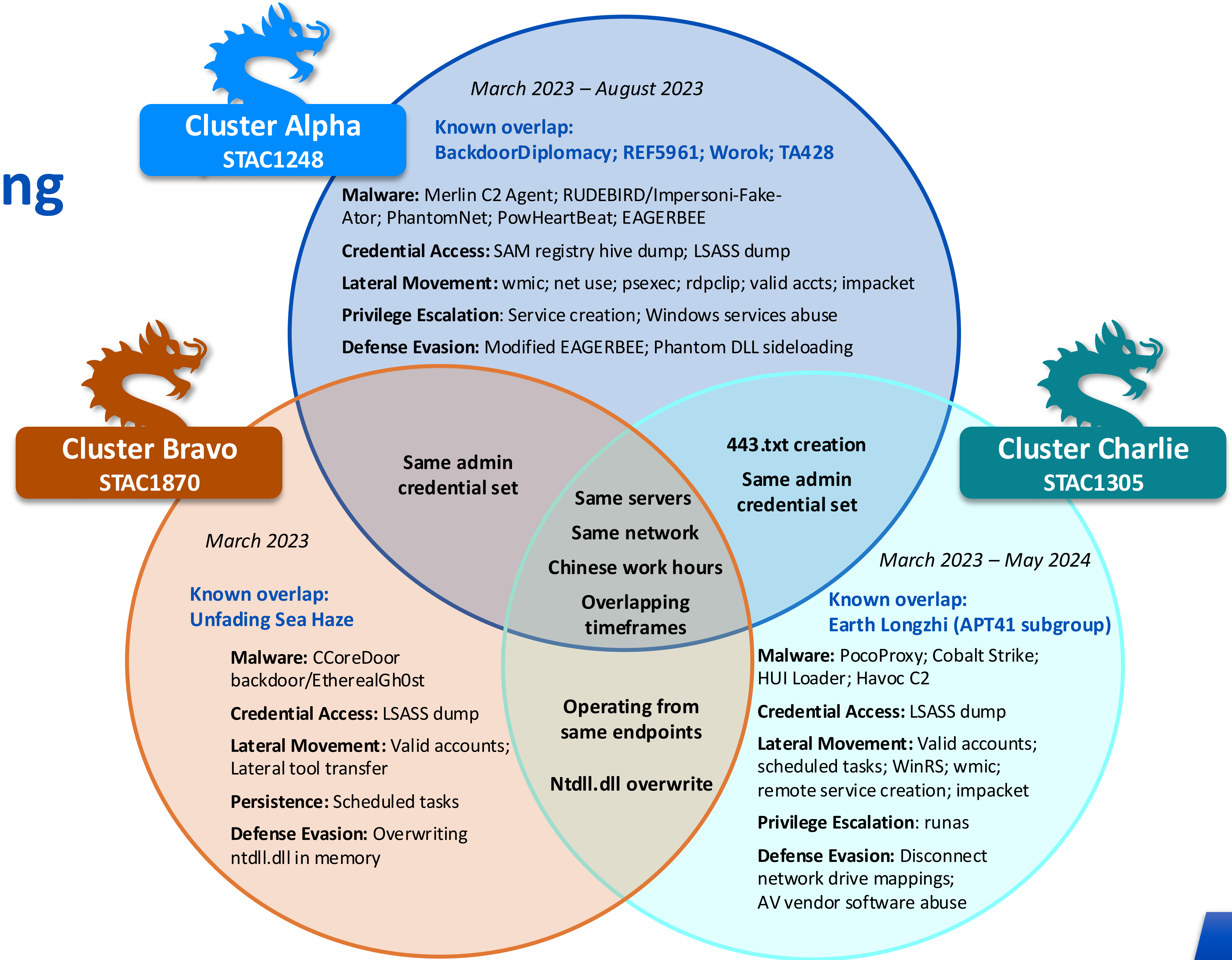
Uncovering the Threat Clusters

Clustering Methodology

Noticed anomalous patterns in several factors:

- ☑ Authentication data, including source subnet, workstation hostname, & account usage
- ☑ Repeat use of techniques, including specific commands & options
- ☑ Unique tools & the paths they were deployed to
- ☑ Targeted user accounts & hosts
- ☑ Timing of the observed activity
- ☑ Attacker C2 infrastructure

Overlapping Behaviors



Cluster Alpha
STAC1248

March 2023 – August 2023

Known overlap:
BackdoorDiplomacy; REF5961; Worok; TA428

Malware: Merlin C2 Agent; RUDEBIRD/Impersoni-Fake-Ator; PhantomNet; PowHeartBeat; EAGERBEE

Credential Access: SAM registry hive dump; LSASS dump

Lateral Movement: wmic; net use; psexec; rdpclip; valid accts; impacket

Privilege Escalation: Service creation; Windows services abuse

Defense Evasion: Modified EAGERBEE; Phantom DLL sideloading

Cluster Bravo
STAC1870

March 2023

Known overlap:
Unfading Sea Haze

Malware: CCoreDoor backdoor/EtherealGh0st

Credential Access: LSASS dump

Lateral Movement: Valid accounts; Lateral tool transfer

Persistence: Scheduled tasks

Defense Evasion: Overwriting ntdll.dll in memory

Cluster Charlie
STAC1305

March 2023 – May 2024

Known overlap:
Earth Longzhi (APT41 subgroup)

Malware: PocoProxy; Cobalt Strike; HUI Loader; Havoc C2

Credential Access: LSASS dump

Lateral Movement: Valid accounts; scheduled tasks; WinRS; wmic; remote service creation; impacket

Privilege Escalation: runas

Defense Evasion: Disconnect network drive mappings; AV vendor software abuse

Same admin credential set

443.txt creation

Same admin credential set

Same servers

Same network

Chinese work hours

Overlapping timeframes

Operating from same endpoints

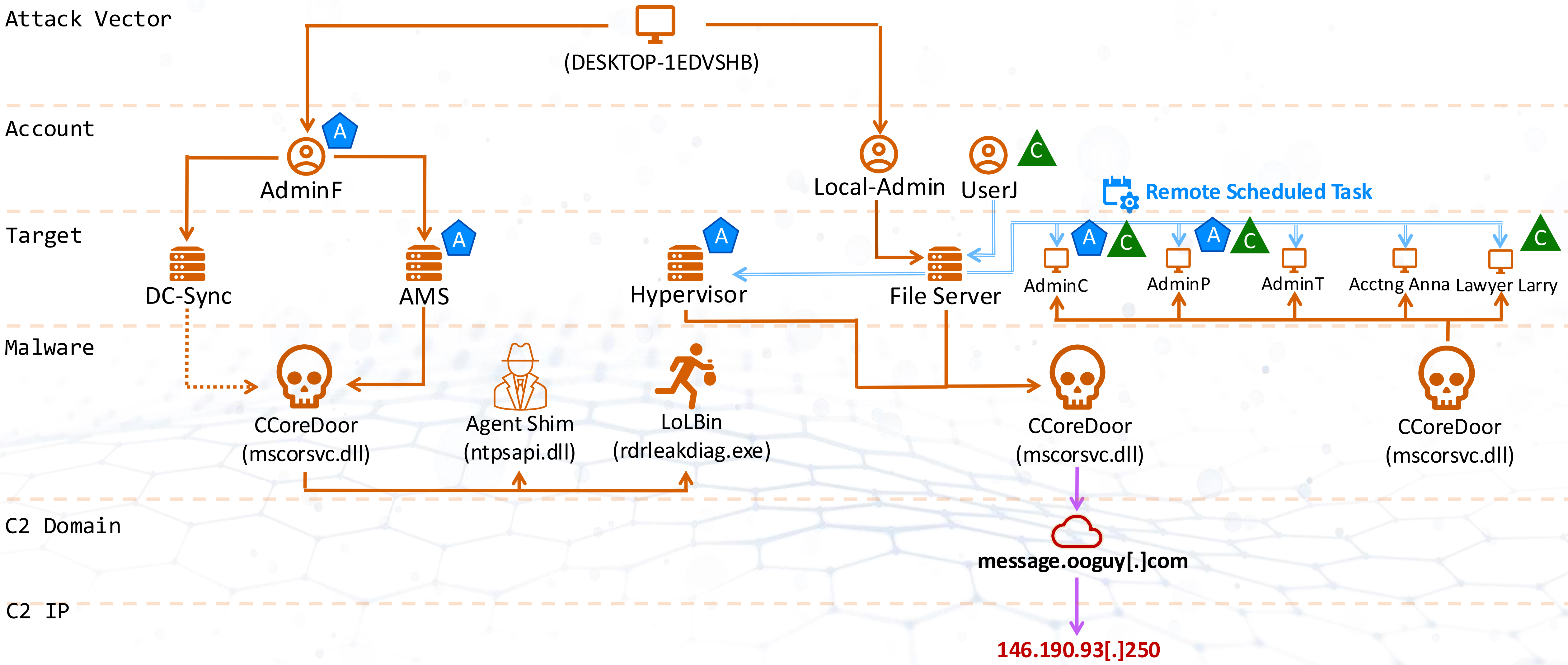
Ntdll.dll overwrite

Spotlight on Cluster Attack Flows

Pattern of Life: BRAVO

Key

Action	—	Cluster Alpha Overlap	A
Lateral Movement	—	Cluster Charlie Overlap	C
Network Comm.	—		



Attack Vector

(DESKTOP-1EDVSHB)

Account

A AdminF

Local-Admin

UserJ C

Remote Scheduled Task

Target

DC-Sync

A AMS

A Hypervisor

File Server

A C AdminC

A C AdminP

AdminT

Acctng Anna

Lawyer Larry C

Malware

CCoreDoor (mscorsvc.dll)

Agent Shim (ntpsapi.dll)

LoLBin (rdrleakdiag.exe)

CCoreDoor (mscorsvc.dll)

CCoreDoor (mscorsvc.dll)

C2 Domain

message.ooguy[.]com

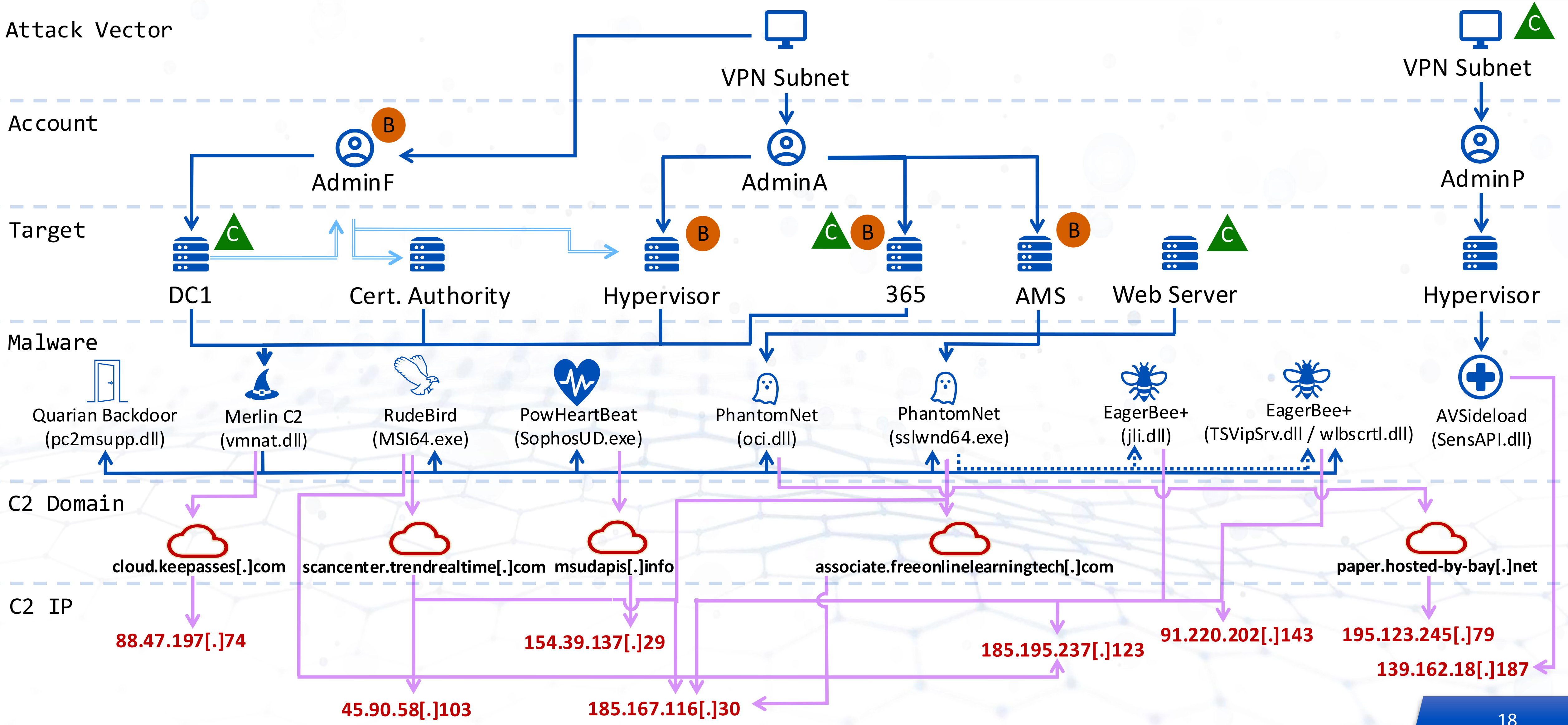
C2 IP

146.190.93[.]250

Pattern of Life: ALPHA

Key

Action	—	Cluster Bravo Overlap	B
Lateral Movement	—	Cluster Charlie Overlap	C
Network Comm.	—		



Attack Vector

Account

Target

Malware

C2 Domain

C2 IP

VPN Subnet

VPN Subnet C

AdminF B

AdminA

AdminP

DC1 C

Cert. Authority

Hypervisor B

C B 365

AMS B

Web Server C

Hypervisor

Quarian Backdoor (pc2msupp.dll)

Merlin C2 (vmnat.dll)

RudeBird (MSI64.exe)

PowHeartBeat (SophosUD.exe)

PhantomNet (oci.dll)

PhantomNet (sslwnd64.exe)

EagerBee+ (jli.dll)

EagerBee+ (TSVipSrv.dll / wlbscrtl.dll)

AVSideload (SensAPI.dll)

cloud.keepasses[.]com

scancenter.trendrealtime[.]com

msudapis[.]info

associate.freeonlinelearningtech[.]com

paper.hosted-by-bay[.]net

88.47.197[.]74

154.39.137[.]29

185.195.237[.]123

91.220.202[.]143

195.123.245[.]79

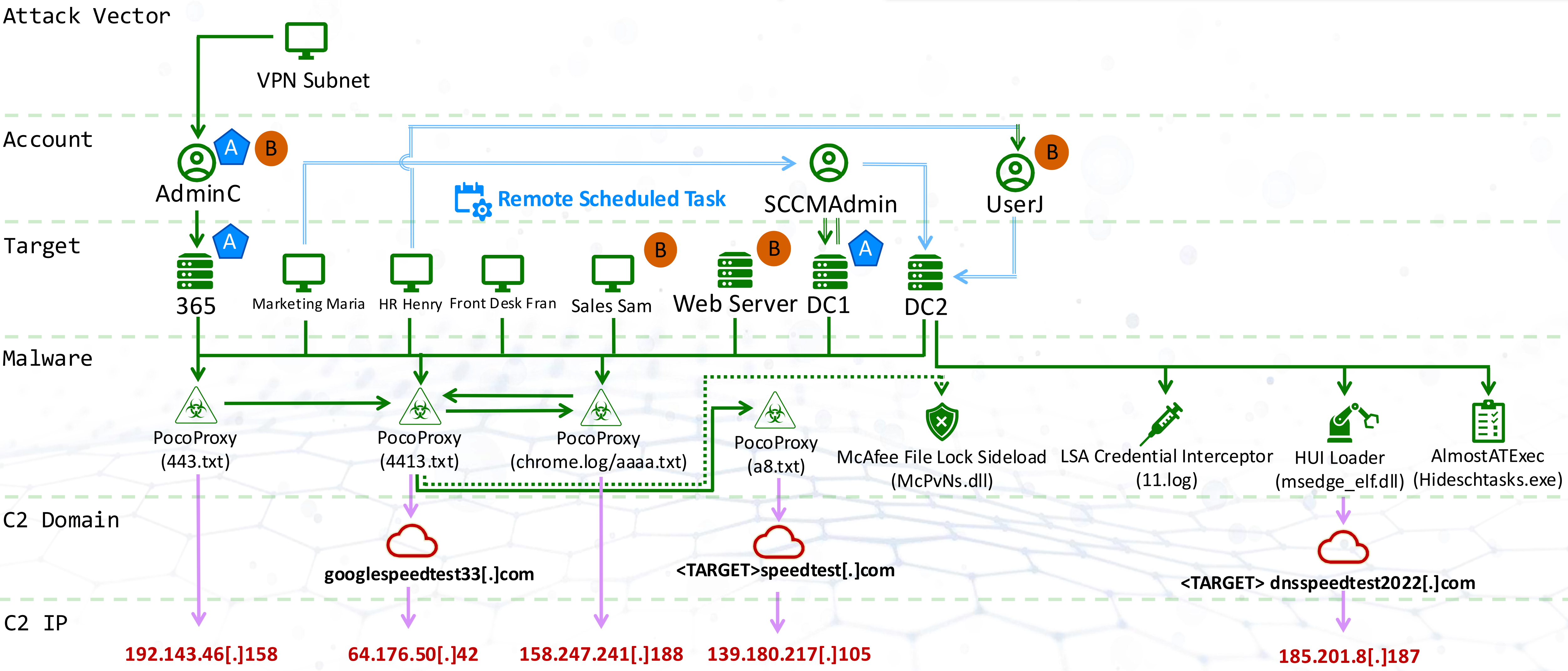
139.162.18[.]187

45.90.58[.]103

185.167.116[.]30

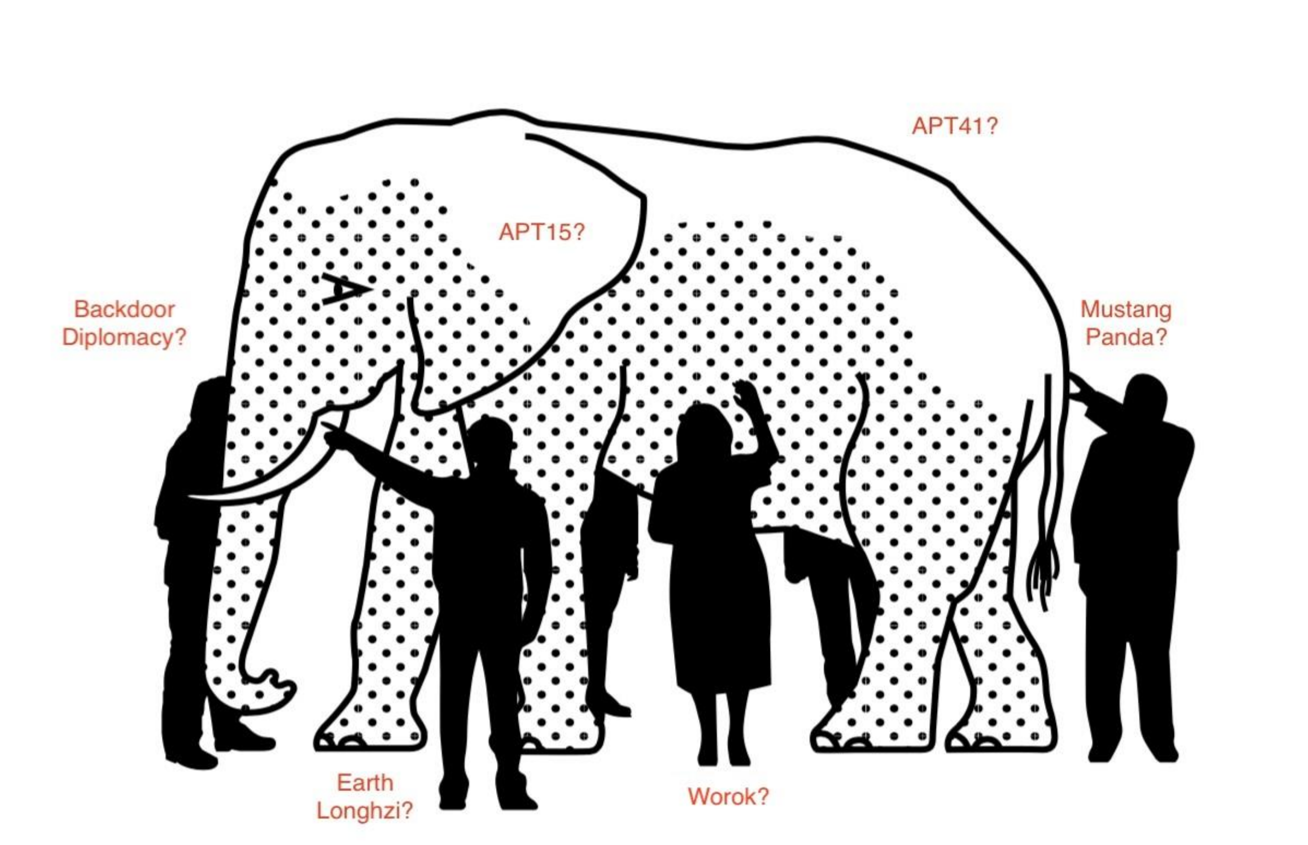
Pattern of Life: CHARLIE

Key		
Action	🟧	Cluster Alpha Overlap A
Lateral Movement	🟦	Cluster Charlie Overlap C
Network Comm.	🟪	



Cluster Analysis & Assessing Overlap

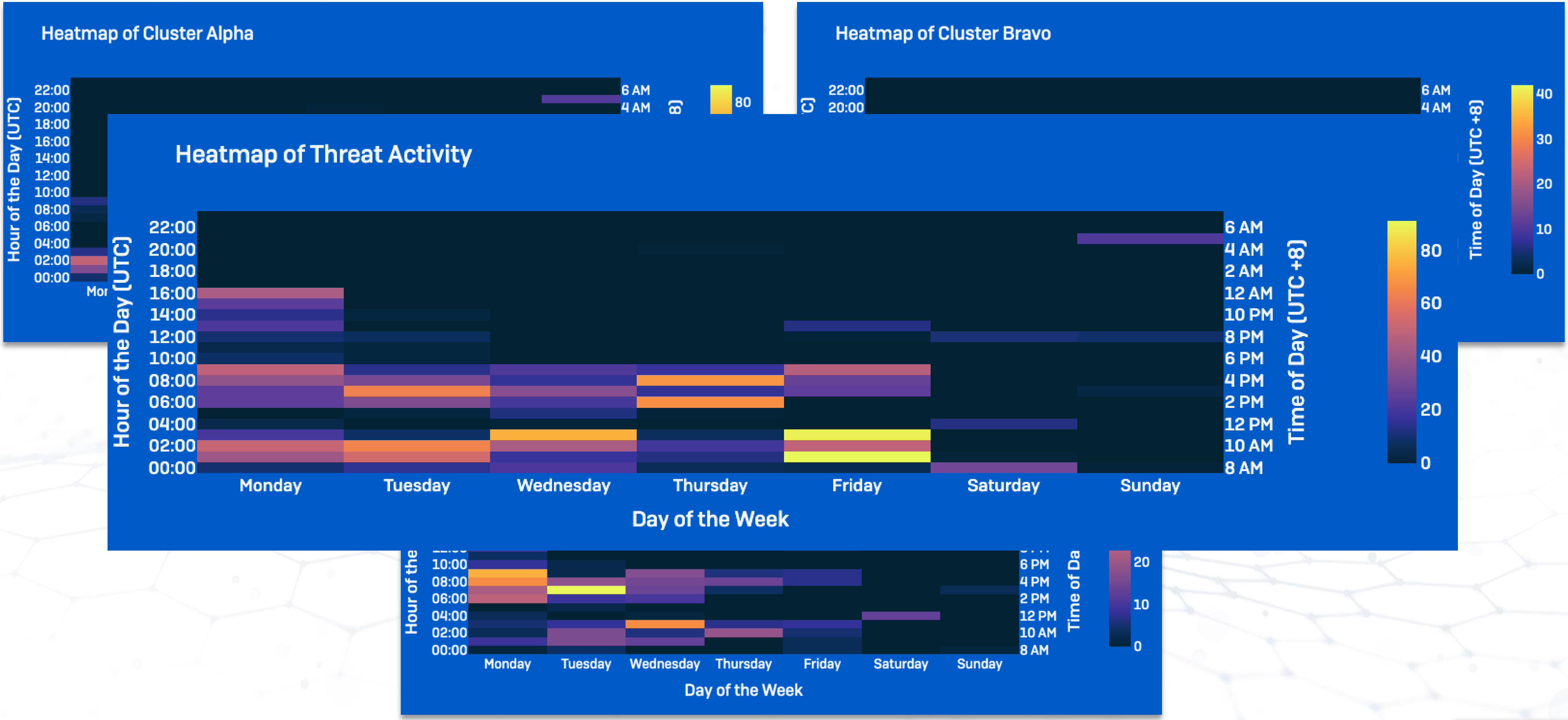
Initial Attribution is Puzzling



Source: FS

- Industry tends to liberally create new threat groups vs campaigns
- **PRC-Aligned Activity: Assumptions**
  - Known to have multiple APTs targeting SE Asia
  - Tool sharing & infrastructure reuse
- **Observed overlap with:**
  - Mustang Panda (Legacy)
  - Backdoor Diplomacy / APT15
  - REF5961
  - Earth Longzhi (APT 41 Subgroup)
  - Worok / TA428
  - Unfading Sea Haze

Time of Day Analysis



Heatmap of Cluster Alpha

Heatmap of Cluster Bravo

Heatmap of Threat Activity

Adversary Patterns

Cluster Alpha | STAC1248

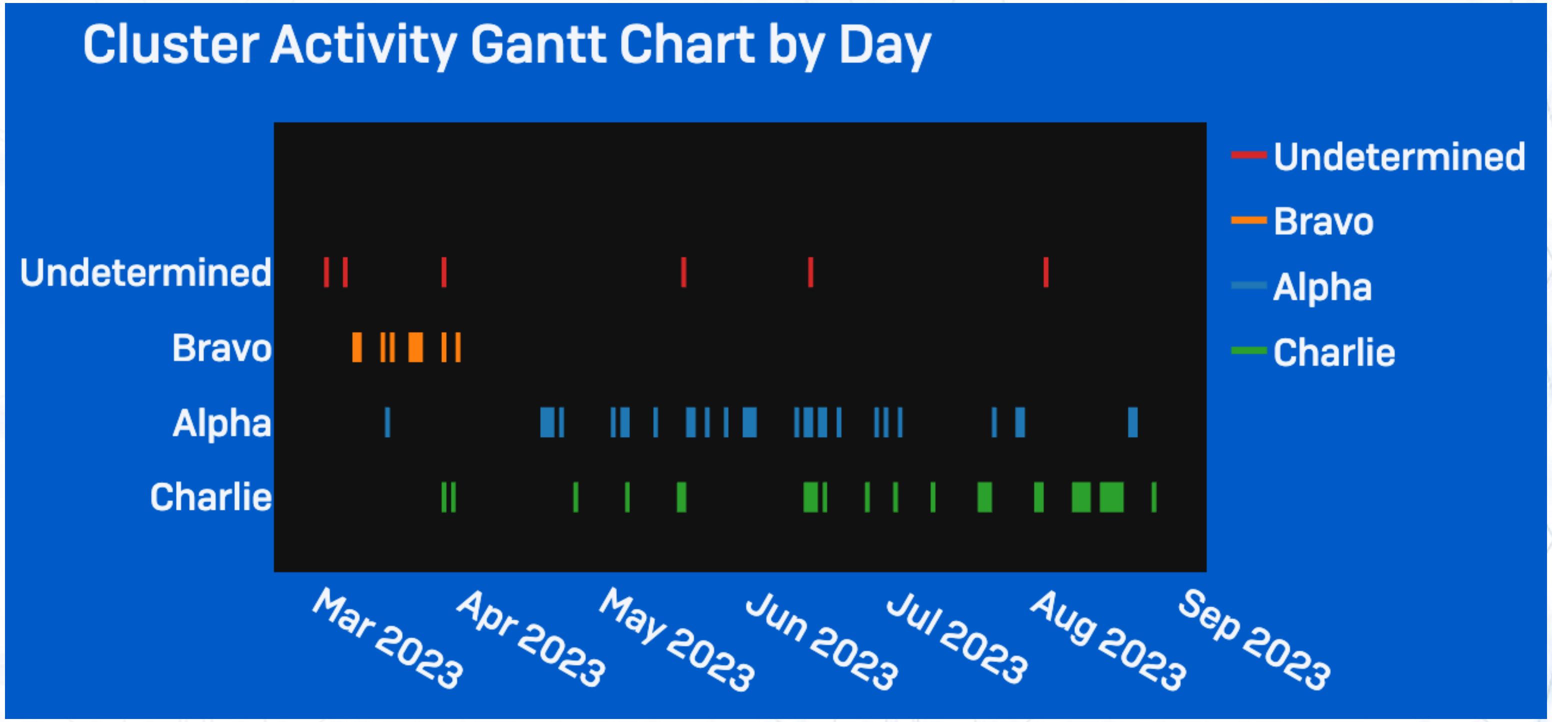
- Month 1 – Month 6
- Often occurred within the traditional working hours of 8am to 5pm CST
- Peaked on Friday

Cluster Bravo | STAC1870

- Mini-cluster from Month 1
- Often occurred within traditional working hours of 8am to 5pm CST
- Peaked on Tuesday, Wednesday, & Thursday

Cluster Charlie | STAC1305

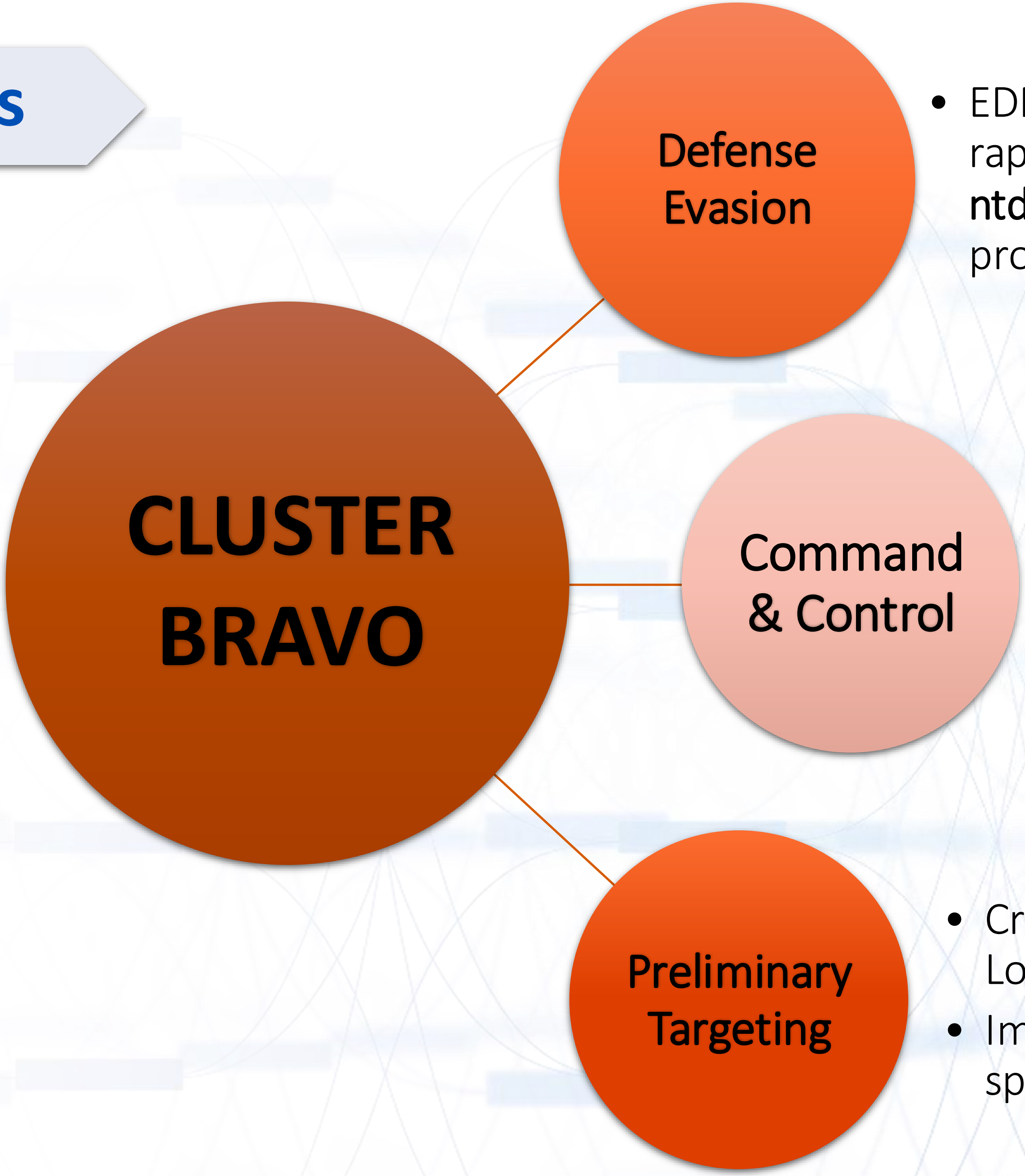
- Month 2 – Month 6
- Varied the most outside standard working hours
- Peaked Monday through Wednesday 12pm to 6pm CST
- Spike of activity on holiday in June



Cluster Activity Gantt Chart by Day

Connecting the Dots

Connecting the Dots



CLUSTER BRAVO

Defense Evasion

- EDR unhooking through rapid loading of renamed **ntdll.dll** into a malicious process

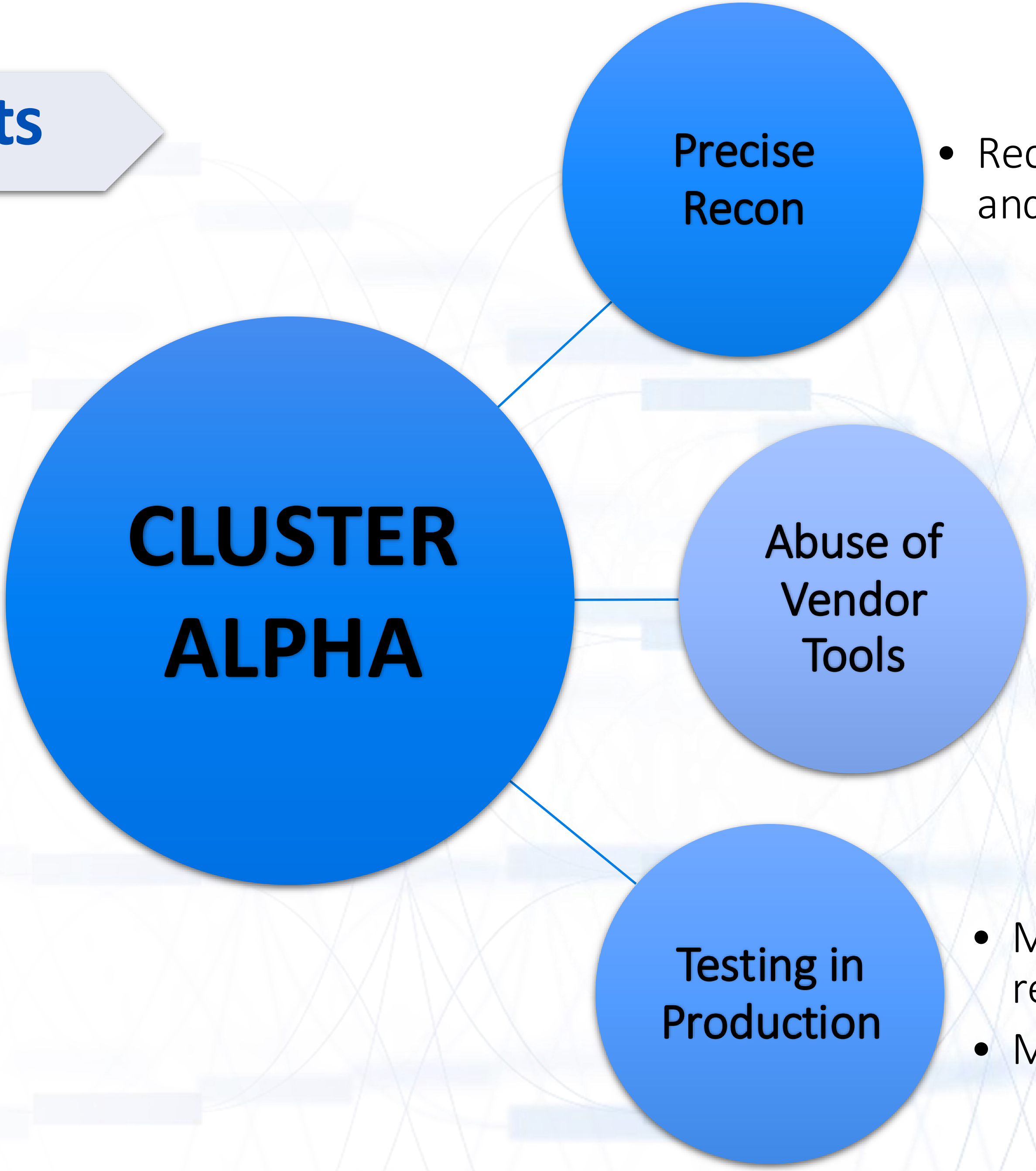
Command & Control

- Novel backdoor in the form of CCoreDoor/Ethereal-Gh0st

Preliminary Targeting

- Credential Capture via LoLBin **RDRLeakDiag**
- Implant deployment to specific users & systems

Connecting the dots



CLUSTER ALPHA

Precise Recon

- Recon of specific users and systems

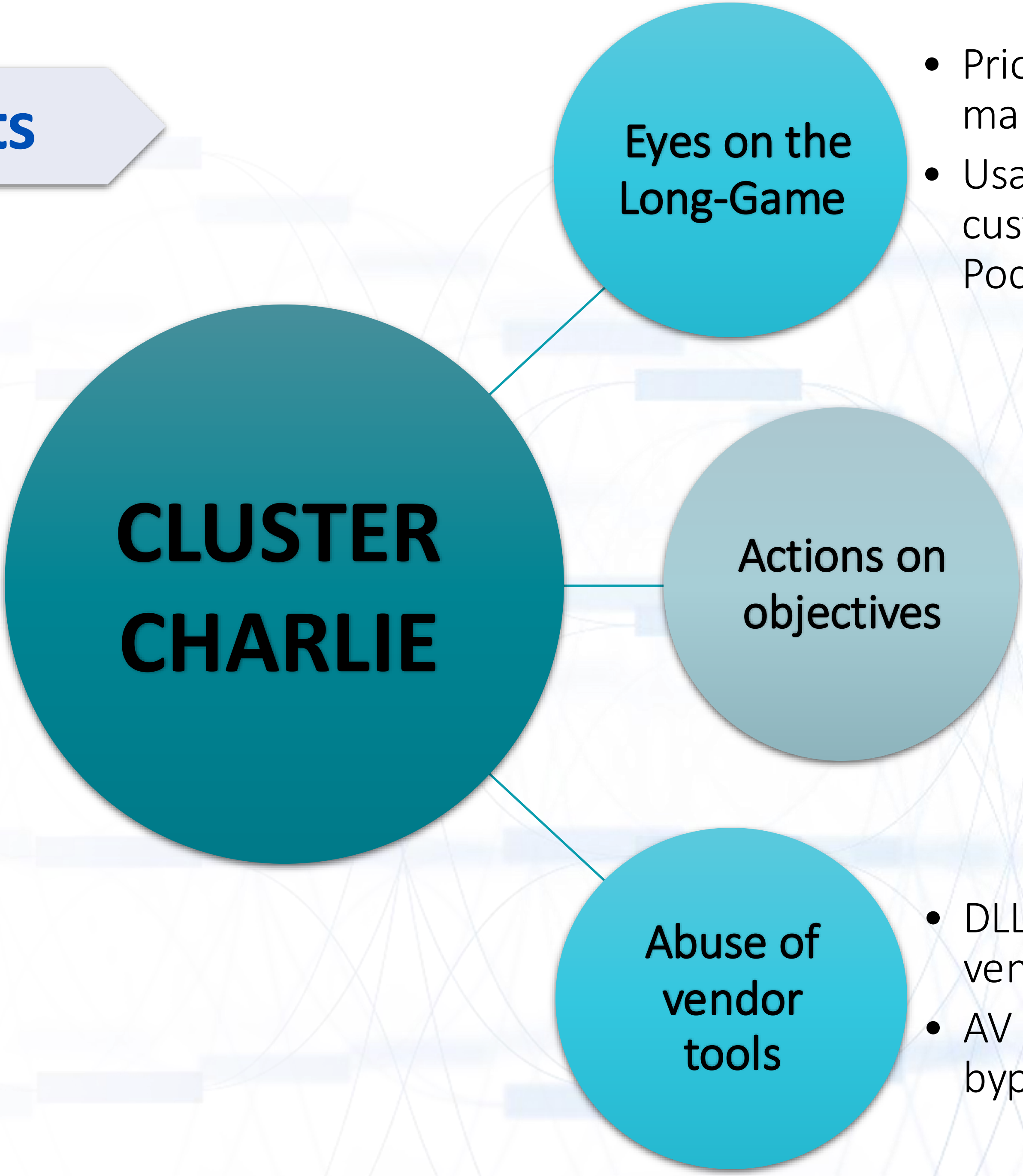
Abuse of Vendor Tools

- DLL sideloading of AV vendor binaries
- Evading EDR through DNS Blackhole

Testing in Production

- Multiple methods to reach same goal
- Making mistakes

Connecting the dots



CLUSTER CHARLIE

Eyes on the Long-Game

- Prioritizing access management
- Usage of unreported custom malware - PocoProxy for C2

Actions on objectives

- Exfiltration
- Keyloggers
  - TattleTale Malware

Abuse of vendor tools

- DLL sideloading of AV vendor binaries
- AV Vendor Drivers for EDR bypass

Cluster Overlap – Targets of Interest

Assumption: We are observing isolated malicious events against targets of interest

Admin C
🐞 🔭

Admin P
🐞 🔭 🪪 📂

Sales Sam
🐞 🔭 ⌨

Acctng Anna
🐞 📂 ⌨

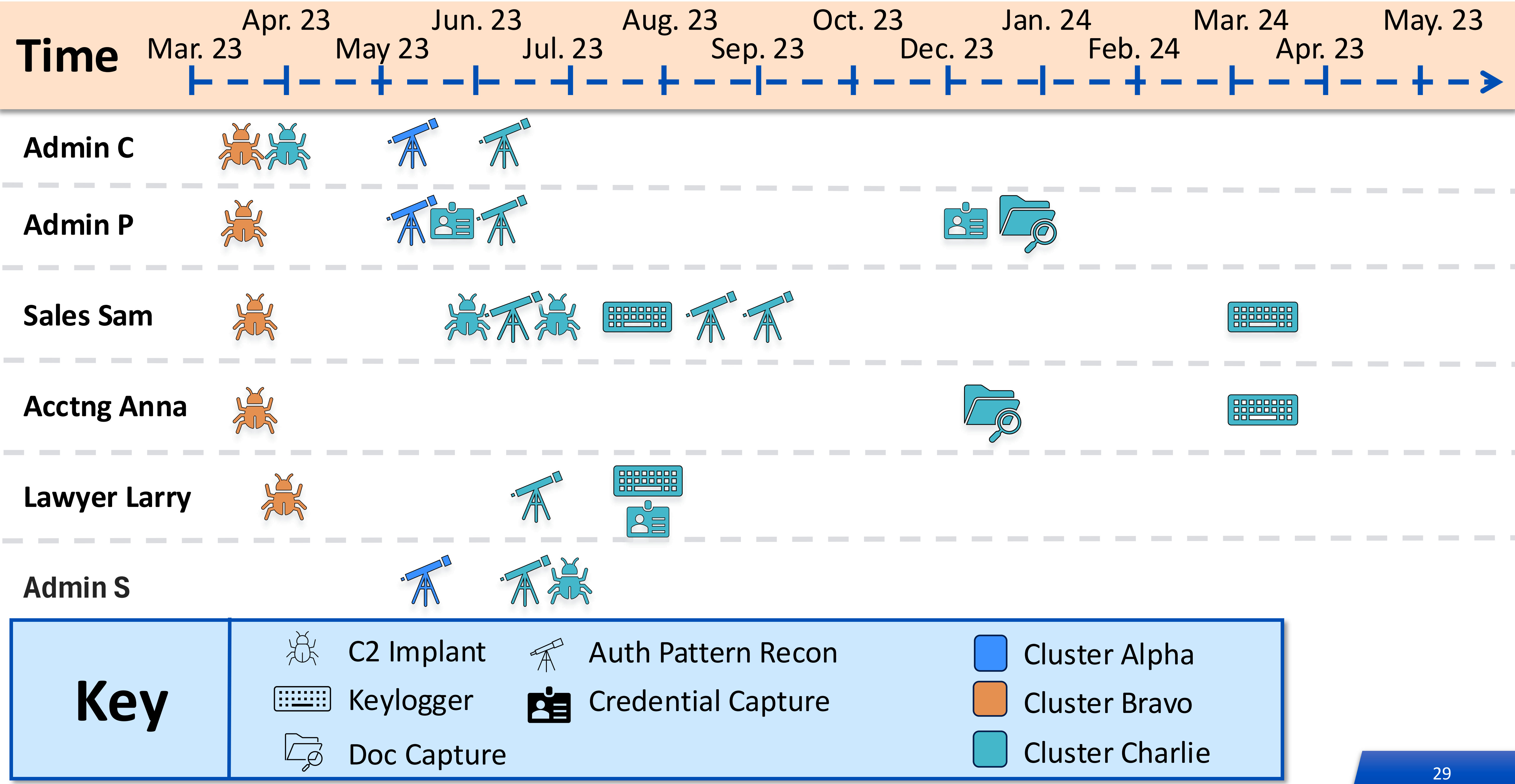
Lawyer Larry
🐞 🔭 🪪 ⌨

Admin S
🔭 🐞

Key

🐞	C2 Implant	🔭	Auth Pattern Recon
⌨	Keylogger	🪪	Credential Capture
📂	Doc Capture		

Cluster Overlap – Targets of Interest



Division of Labor – Cluster Objectives

Cluster Bravo

- Developing initial foothold by deploying CCoreDoor backdoor to specific users & admins

Cluster Alpha

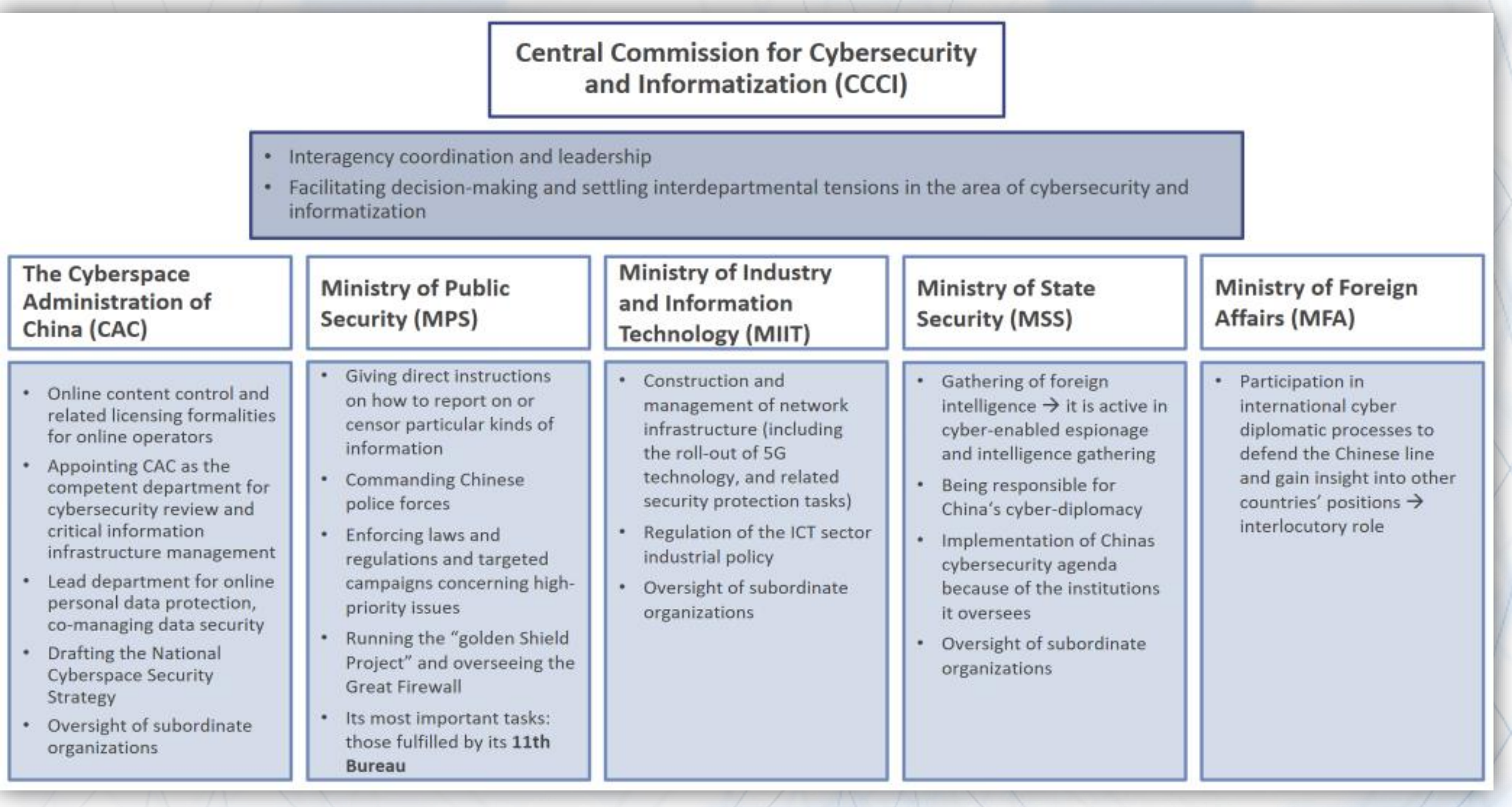
- Mapping victim domain, focusing on infrastructure & programs
- Identifying admins & directors of key applications
- Testing out different payloads & techniques

Cluster Charlie

- Capture and Exfiltration of Confidential Documents & IT Infrastructure Documentation & Key Material
- Gaining & maintaining access throughout network

Timing and overlaps indicate a level of coordination and awareness

We have moderate confidence these activity clusters were part of **a coordinated campaign under the direction of a single organization**



Central Commission for Cybersecurity and Informatization (CCCI)

- Interagency coordination and leadership
- Facilitating decision-making and settling interdepartmental tensions in the area of cybersecurity and informatization

The Cyberspace Administration of China (CAC)

- Online content control and related licensing formalities for online operators
- Appointing CAC as the competent department for cybersecurity review and critical information infrastructure management
- Lead department for online personal data protection, co-managing data security
- Drafting the National Cyberspace Security Strategy
- Oversight of subordinate organizations

Ministry of Public Security (MPS)

- Giving direct instructions on how to report on or censor particular kinds of information
- Commanding Chinese police forces
- Enforcing laws and regulations and targeted campaigns concerning high-priority issues
- Running the "golden Shield Project" and overseeing the Great Firewall
- Its most important tasks: those fulfilled by its **11th Bureau**

Ministry of Industry and Information Technology (MIIT)

- Construction and management of network infrastructure (including the roll-out of 5G technology, and related security protection tasks)
- Regulation of the ICT sector industrial policy
- Oversight of subordinate organizations

Ministry of State Security (MSS)

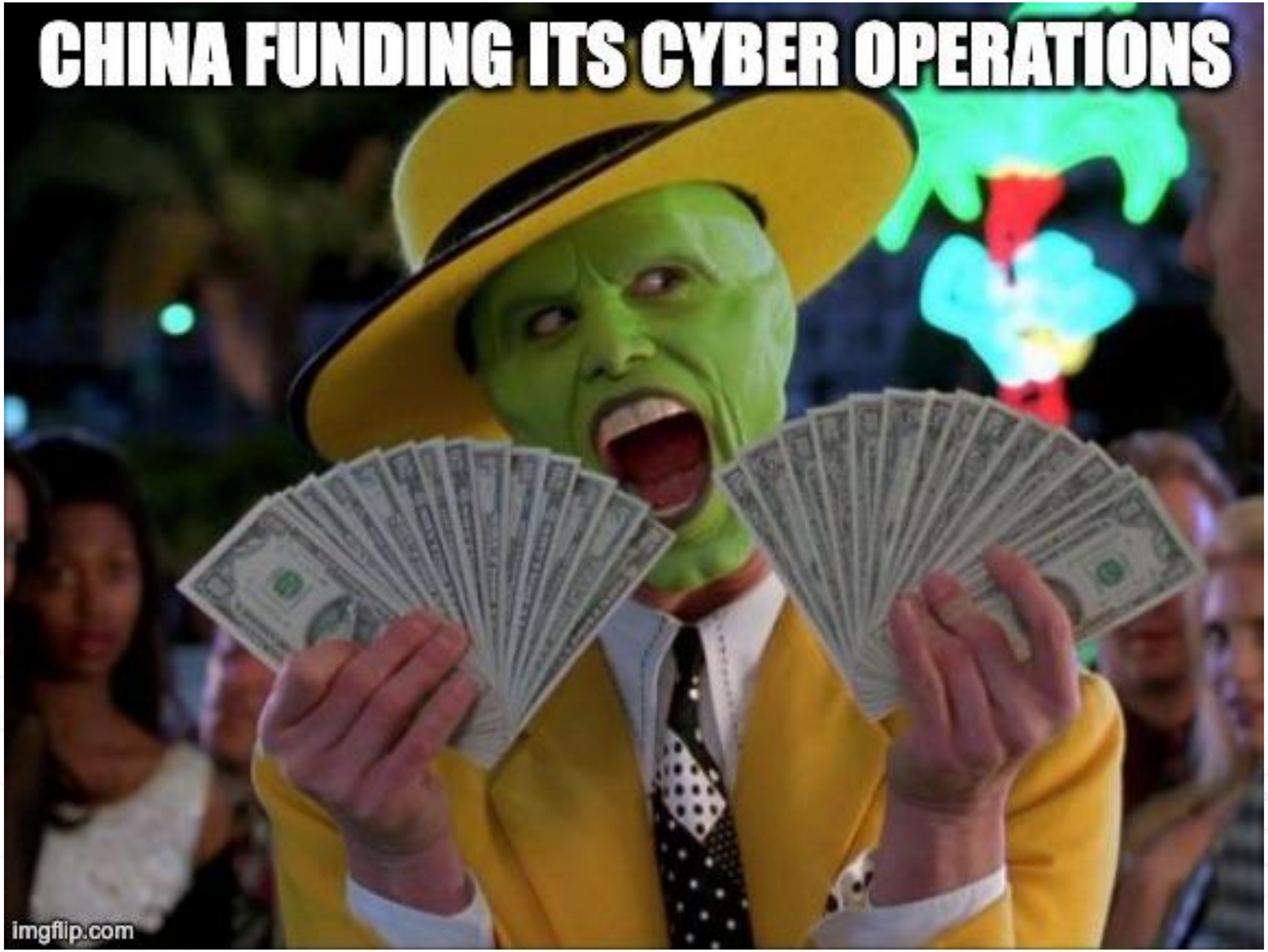
- Gathering of foreign intelligence → it is active in cyber-enabled espionage and intelligence gathering
- Being responsible for China's cyber-diplomacy
- Implementation of Chinas cybersecurity agenda because of the institutions it oversees
- Oversight of subordinate organizations

Ministry of Foreign Affairs (MFA)

- Participation in international cyber diplomatic processes to defend the Chinese line and gain insight into other countries' positions → interlocutory role

Source: ESMT Berlin

BH Asia 2024: China's Military Cyber Operations – Pukhraj Singh


CHINA FUNDING ITS CYBER OPERATIONS
imgflip.com

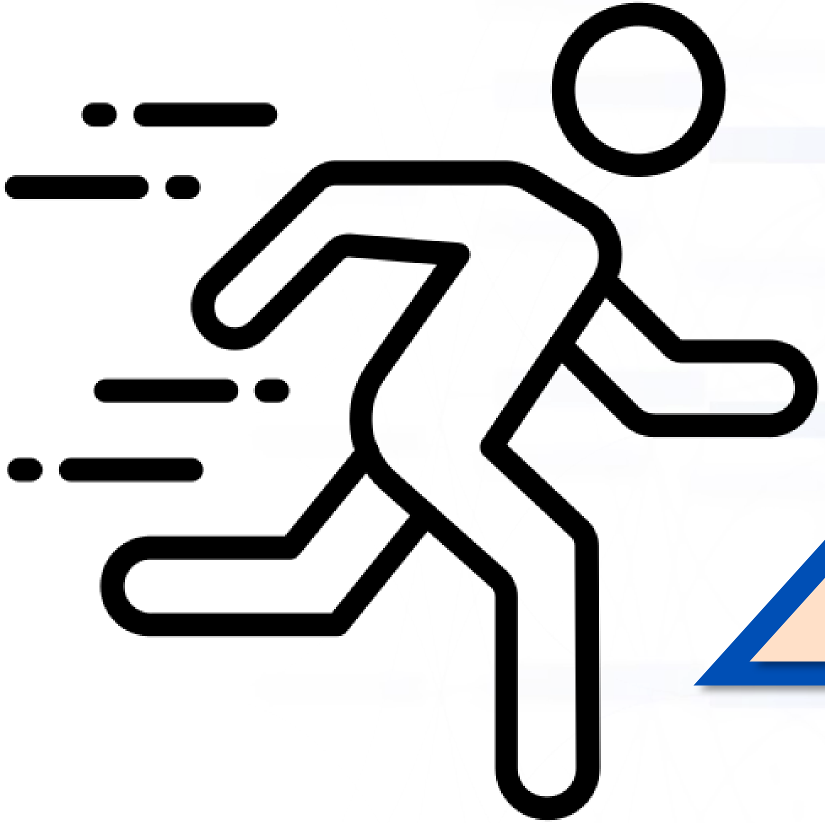
Cluster Charlie Returns with a Vengeance: Stage 2

(September 2023 - April 2024)

Catching our breath? (or so we thought)

CLUSTER CHARLIE PREPPING DOZENS OF NEW BACKDOORS
OUR TEAM BLOCKING THEIR IMPLANTS
imgflip.com

A Change of Pace



Stage 2 = Begins at the end of September 2023 as Cluster Charlie re-penetrates the network via a web shell and performs recon on the victim's confidential docs webserver

A Change of Pace

Actions on Objective

- Document capture
- Keyloggers
- Tattletale malware

Starting to deploy open-source & custom tooling

- Shadow Copy Service DLL

Continuing to make mistakes

- Service DLL sideloading

Taking masquerading to the next level

- Targets Sophos binaries
- Abuses AV vendor tools

Actions on Objectives

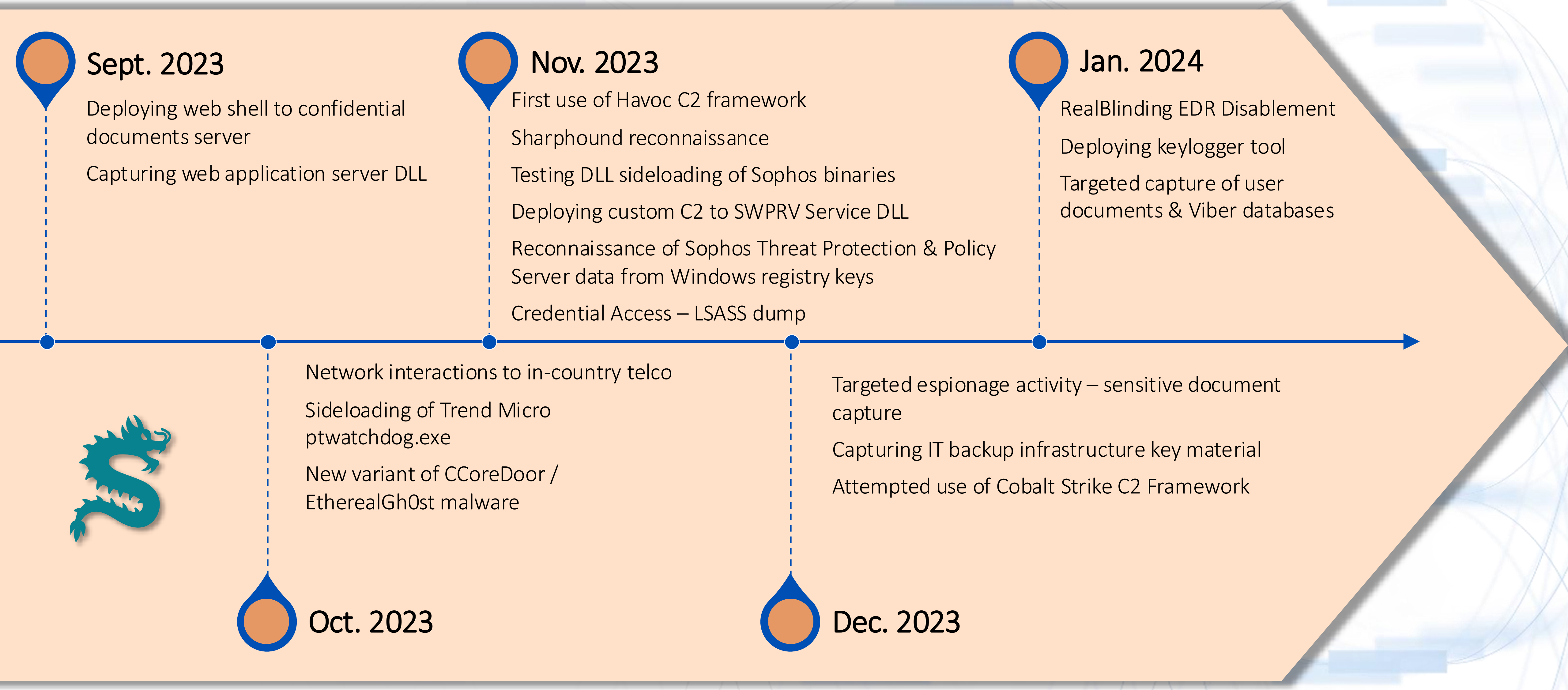
In November, Cluster Charlie began to exfiltrate highly sensitive info for espionage purposes

- Docs related to military, cybersecurity, and economic interests – many related to military strategy in the SCS
- The Windows and Web Credential Store of several admins
- Individual VoIP phone databases
- Cloud OpenVpn certs and configs, data backup project documentation, and switching infrastructure
- Disaster recovery data, network data, email data
- Services data (IP block assignments, server blade configurations, DMZ configurations, server/backups inventory, network diagrams, and domain user lists)
- Extensive data from the Mobile Device Manager (MDM) solution

Other Actions on Objectives:

- Keylogger deployments
  - TattleTale malware
- Ensuring full access to entire environment

Cluster Charlie Stage 2: Timeline



Sept. 2023

Deploying web shell to confidential documents server

Capturing web application server DLL

Oct. 2023

Network interactions to in-country telco

Sideloading of Trend Micro ptwatchdog.exe

New variant of CCoreDoor / EtherealGh0st malware

Nov. 2023

First use of Havoc C2 framework

Sharphound reconnaissance

Testing DLL sideloading of Sophos binaries

Deploying custom C2 to SWPRV Service DLL

Reconnaissance of Sophos Threat Protection & Policy Server data from Windows registry keys

Credential Access – LSASS dump

Dec. 2023

Targeted espionage activity – sensitive document capture

Capturing IT backup infrastructure key material

Attempted use of Cobalt Strike C2 Framework

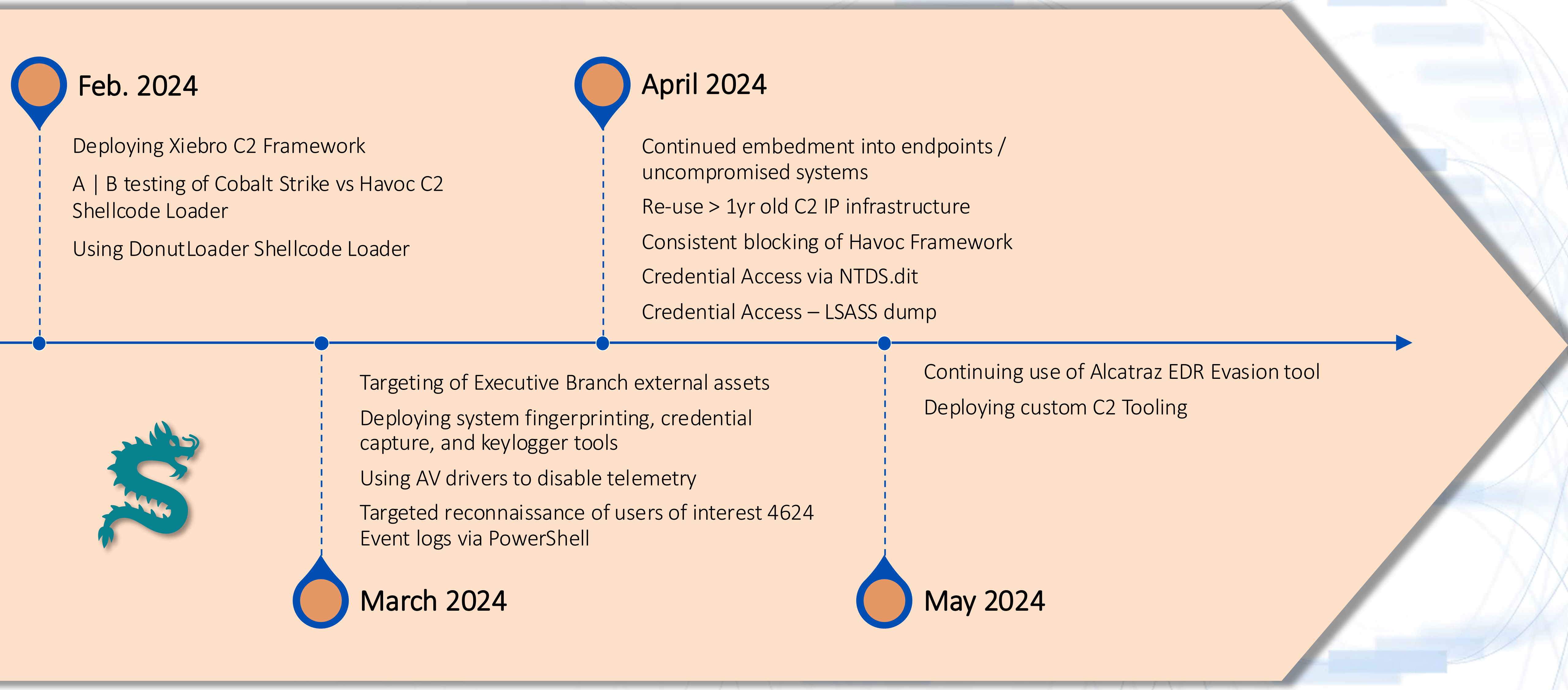
Jan. 2024

RealBlinding EDR Disablement

Deploying keylogger tool

Targeted capture of user documents & Viber databases

Cluster Charlie Stage 2: Timeline (cont.)



Feb. 2024

Deploying Xiebro C2 Framework

A | B testing of Cobalt Strike vs Havoc C2 Shellcode Loader

Using DonutLoader Shellcode Loader

March 2024

Targeting of Executive Branch external assets

Deploying system fingerprinting, credential capture, and keylogger tools

Using AV drivers to disable telemetry

Targeted reconnaissance of users of interest 4624 Event logs via PowerShell

April 2024

Continued embedment into endpoints / uncompromised systems

Re-use > 1yr old C2 IP infrastructure

Consistent blocking of Havoc Framework

Credential Access via NTDS.dit

Credential Access – LSASS dump

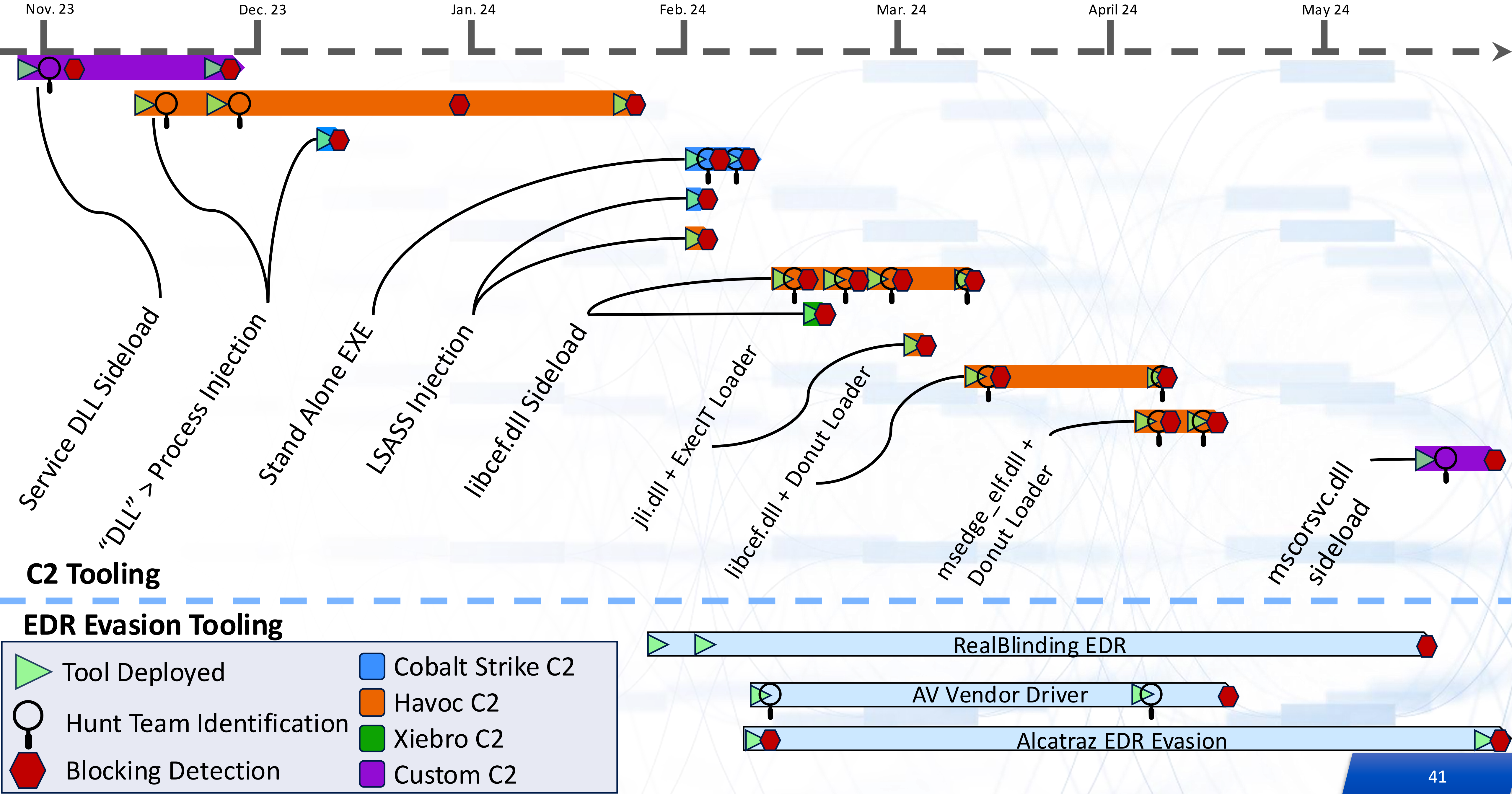
May 2024

Continuing use of Alcatraz EDR Evasion tool

Deploying custom C2 Tooling

C2 Gap Analysis

Open-Source Tooling & C2 Framework Analysis



C2 Tooling

EDR Evasion Tooling

▷	Tool Deployed	🟦	Cobalt Strike C2
○	Hunt Team Identification	🟧	Havoc C2
⬣	Blocking Detection	🟩	Xiebro C2
		🟪	Custom C2

C2 Framework Analysis

- Conducting 'A | B' testing
  - Deploying Cobalt Strike Reflective Loader alongside Havoc Loader, samples maintained same DLL name, and same C2 infrastructure

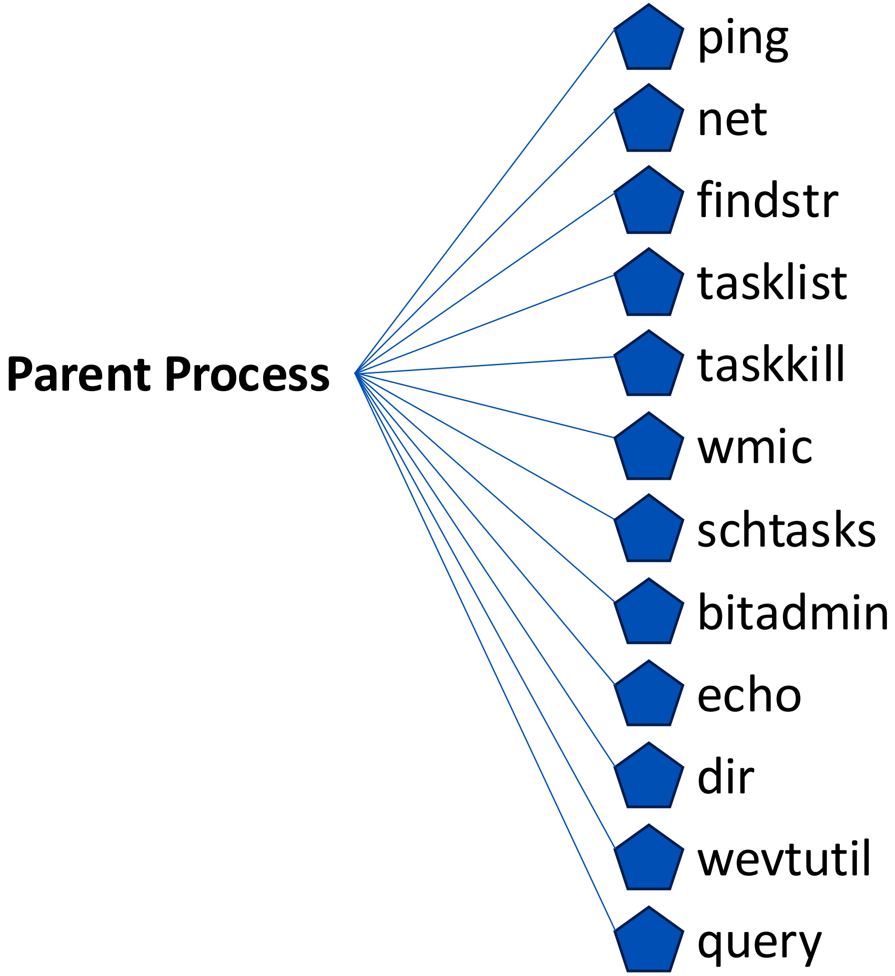
- Taking a tactical approach
  - Cluster Charlie actors relied on open-source tooling & did not shift back to custom tooling until multiple iterations of open-source frameworks were blocked

Source: BigMailer

WHEN THE THREAT ACTORS DON'T SHOW UP LIKE YOU PREDICTED
imgflip.com
MthruF.com

Creating the Session Process Anomaly and Discovery Examination (SPADE) Tool

SPADE Tool



Parent Process

ping

net

findstr

tasklist

taskkill

wmic

schtasks

bitadmin

echo

dir

wevtutil

query

What does C2 look like?

Typically, discovery commands are executed from a sideloaded or injected process over a short time span, which generates network connections to a small number of external IPs

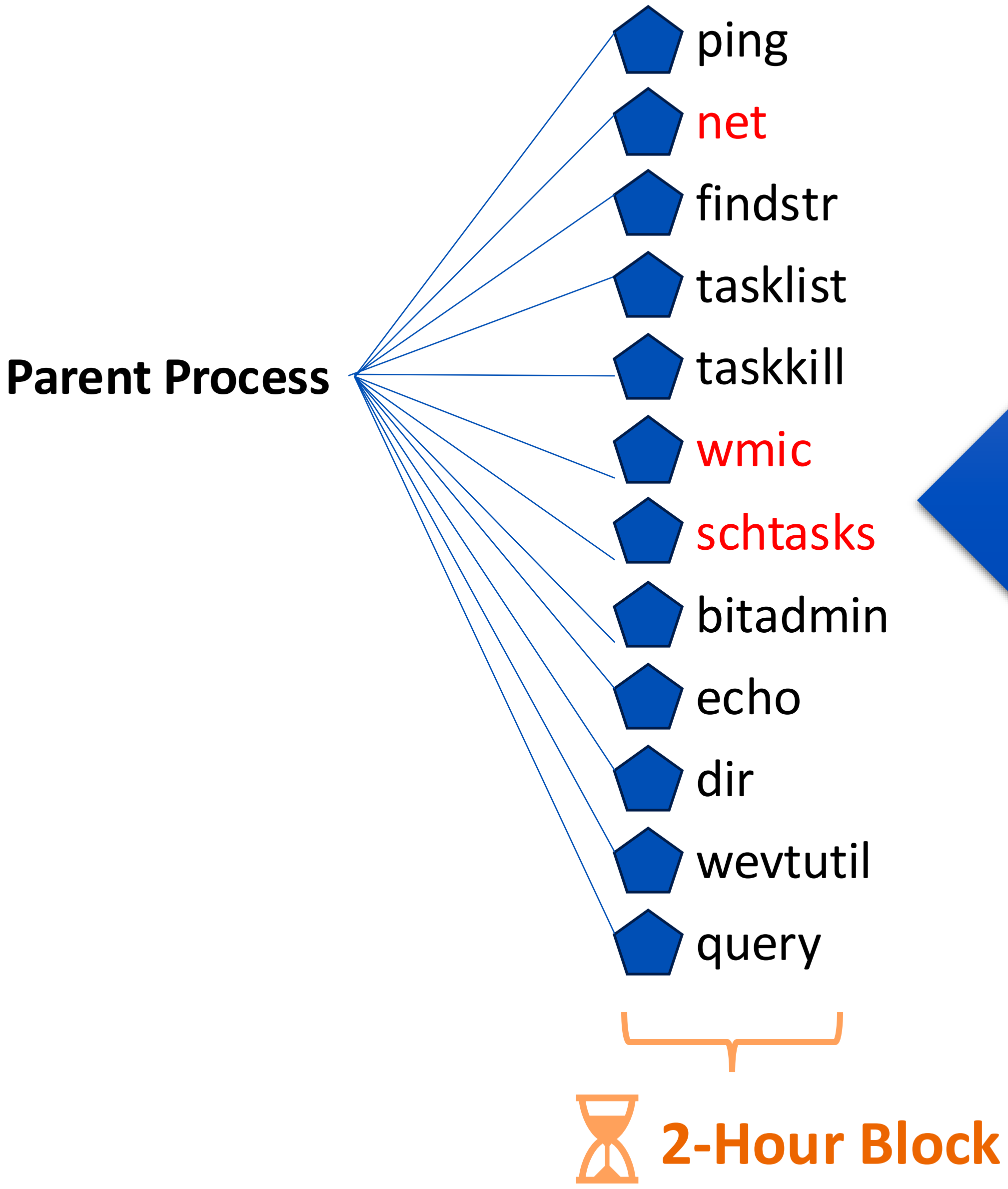
Problem

It's hard to find malicious discovery commands from a single parent to child relationship because of the volume of processes & programs executing typically benign binaries

Solution

Come up with a way to look **for a process from a specific path executing more than one discovery process** = ***The SPADE Tool***

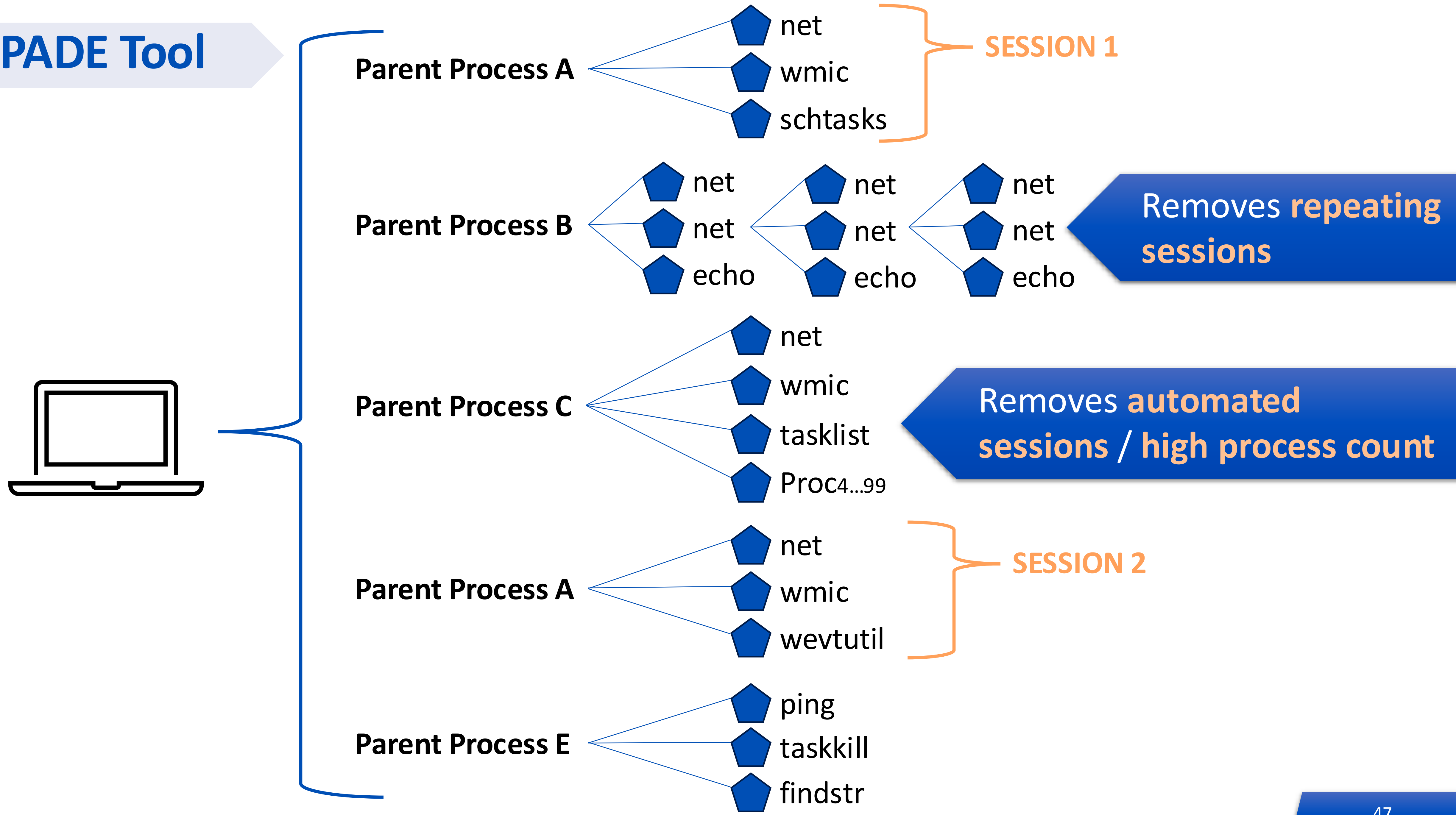
SPADE Tool



The SPADE tool looks for more than **2 discovery commands** from a parent process over a **2-hour session**

- Takes into account human patterns

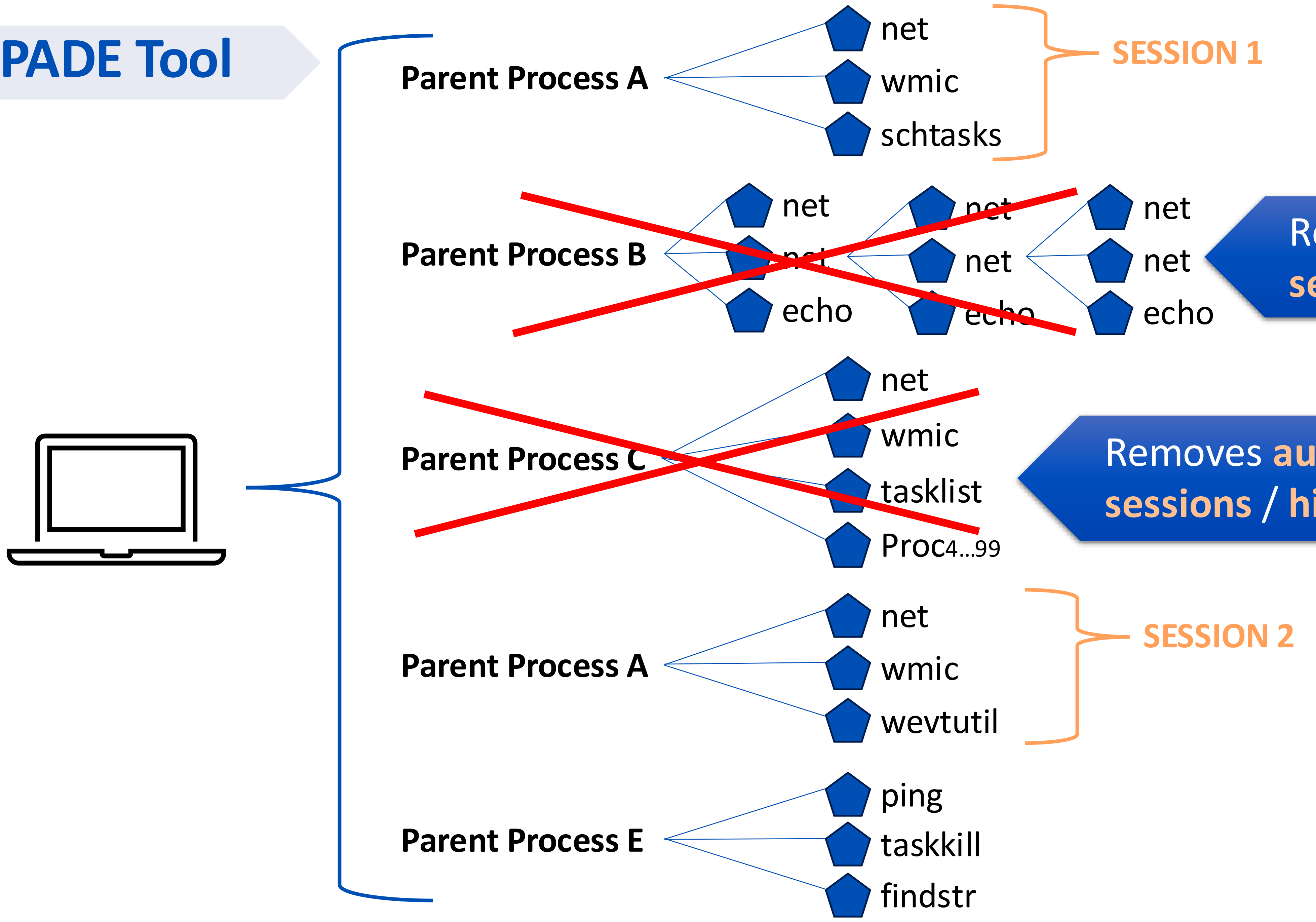
SPADE Tool



Removes **repeating sessions**

Removes **automated sessions / high process count**

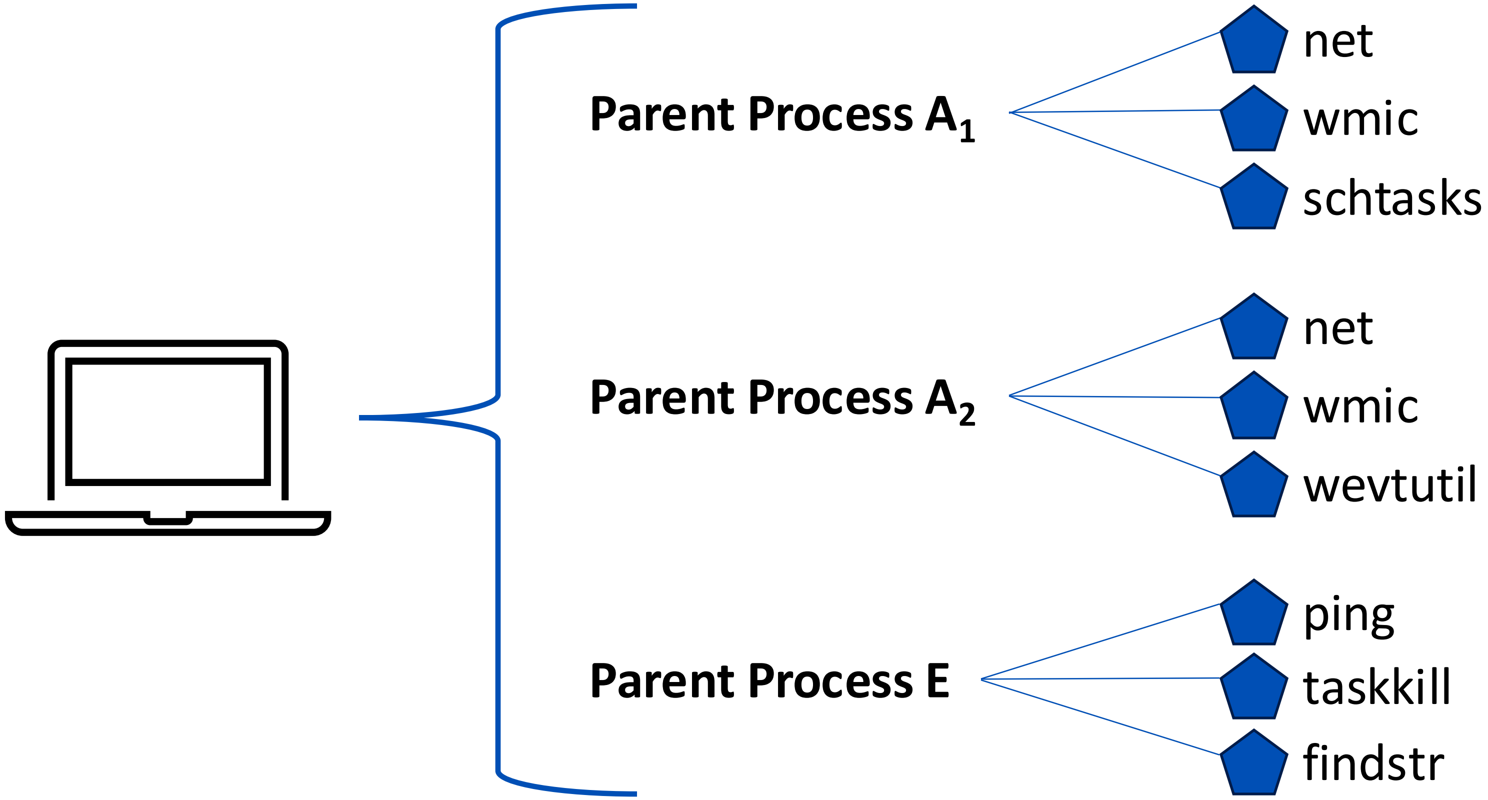
SPADE Tool



Removes **repeating sessions**

Removes **automated sessions / high process count**

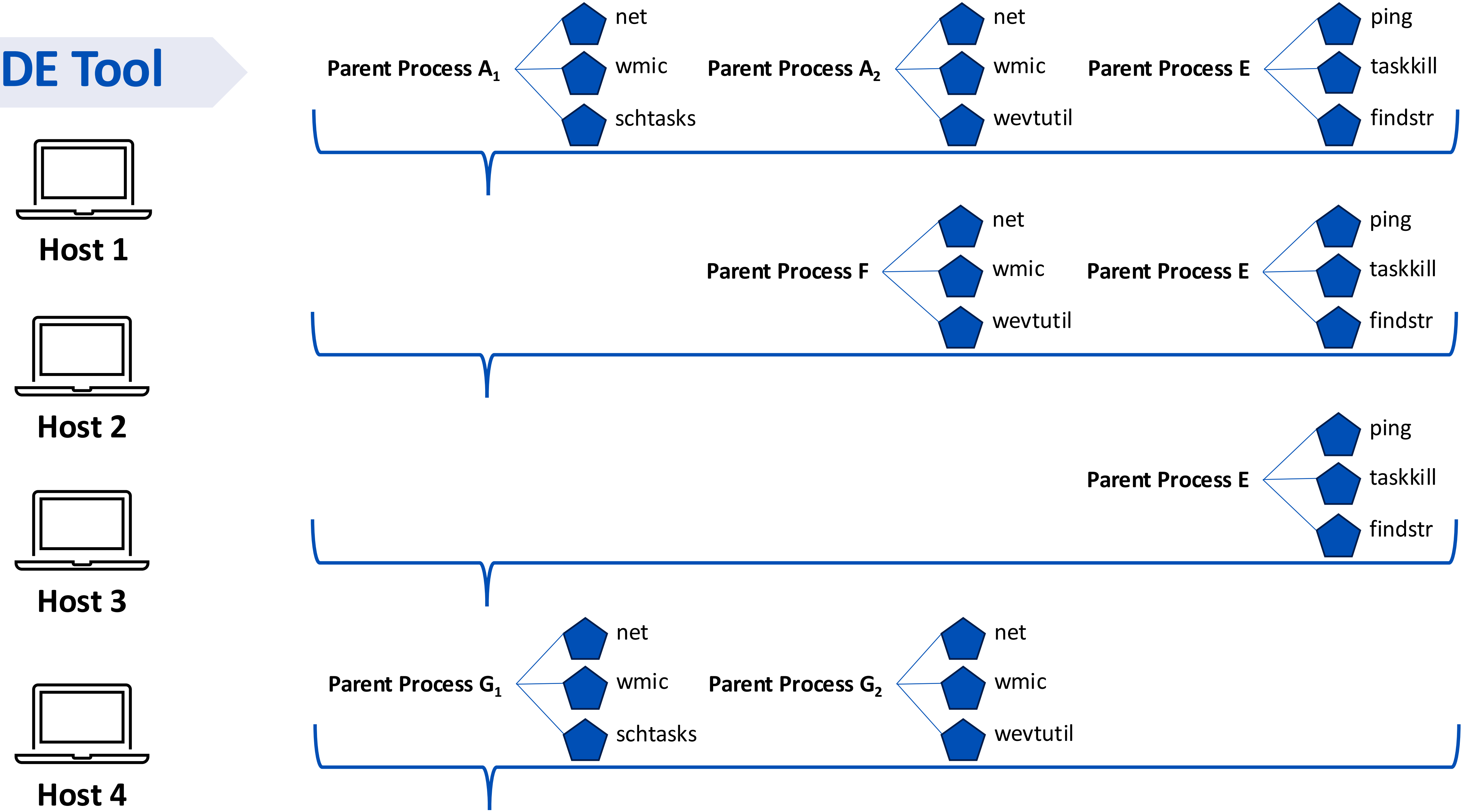
SPADE Tool



Removes **repeating sessions**

Removes **automated sessions / high process count**

SPADE Tool



Host 1

Parent Process A_1: net, wmic, schtasks

Parent Process A_2: net, wmic, wevtutil

Parent Process E: ping, taskkill, findstr

Host 2

Parent Process F: net, wmic, wevtutil

Parent Process E: ping, taskkill, findstr

Host 3

Parent Process E: ping, taskkill, findstr

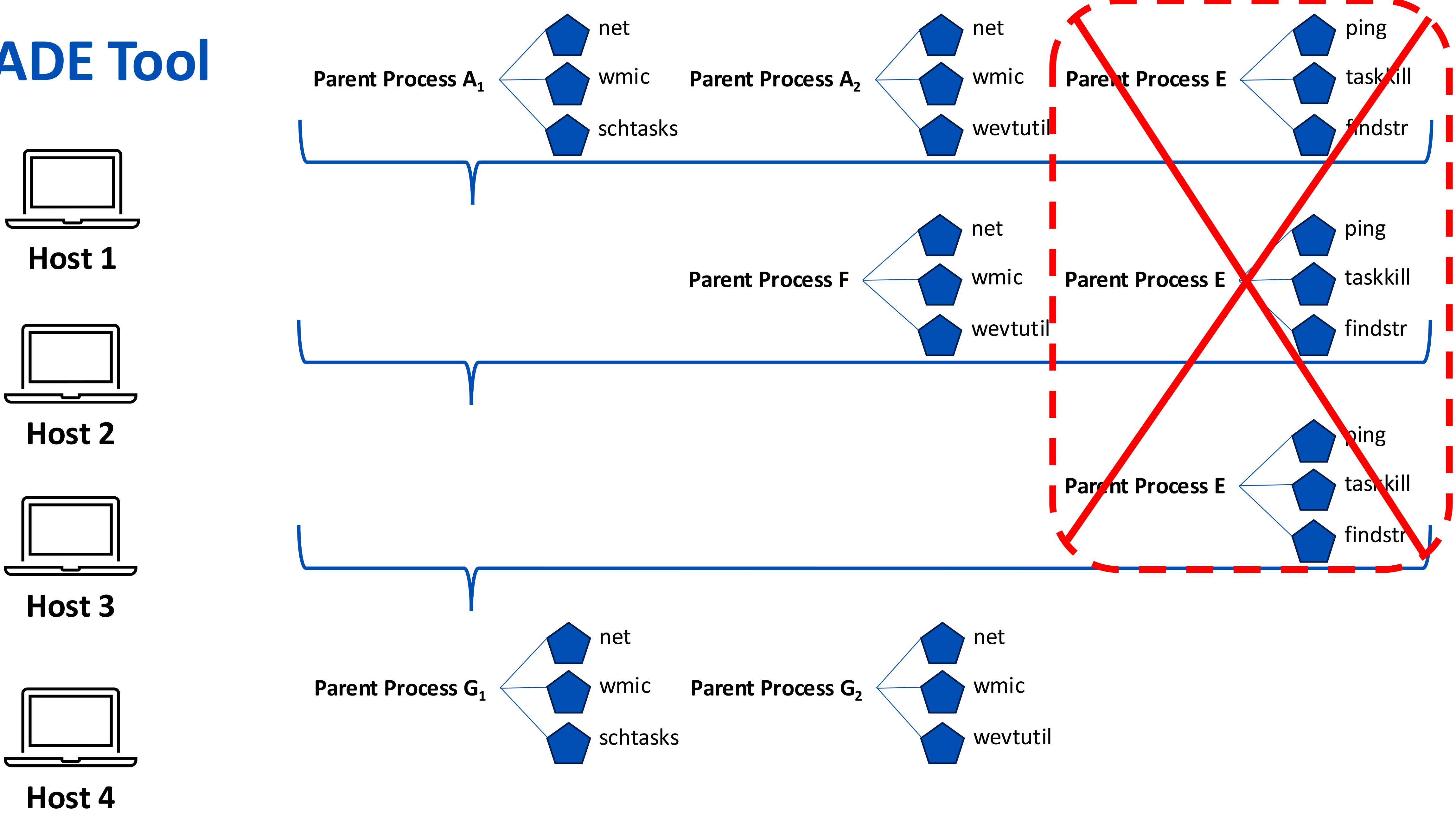
Host 4

Parent Process G_1: net, wmic, schtasks

Parent Process G_2: net, wmic, wevtutil

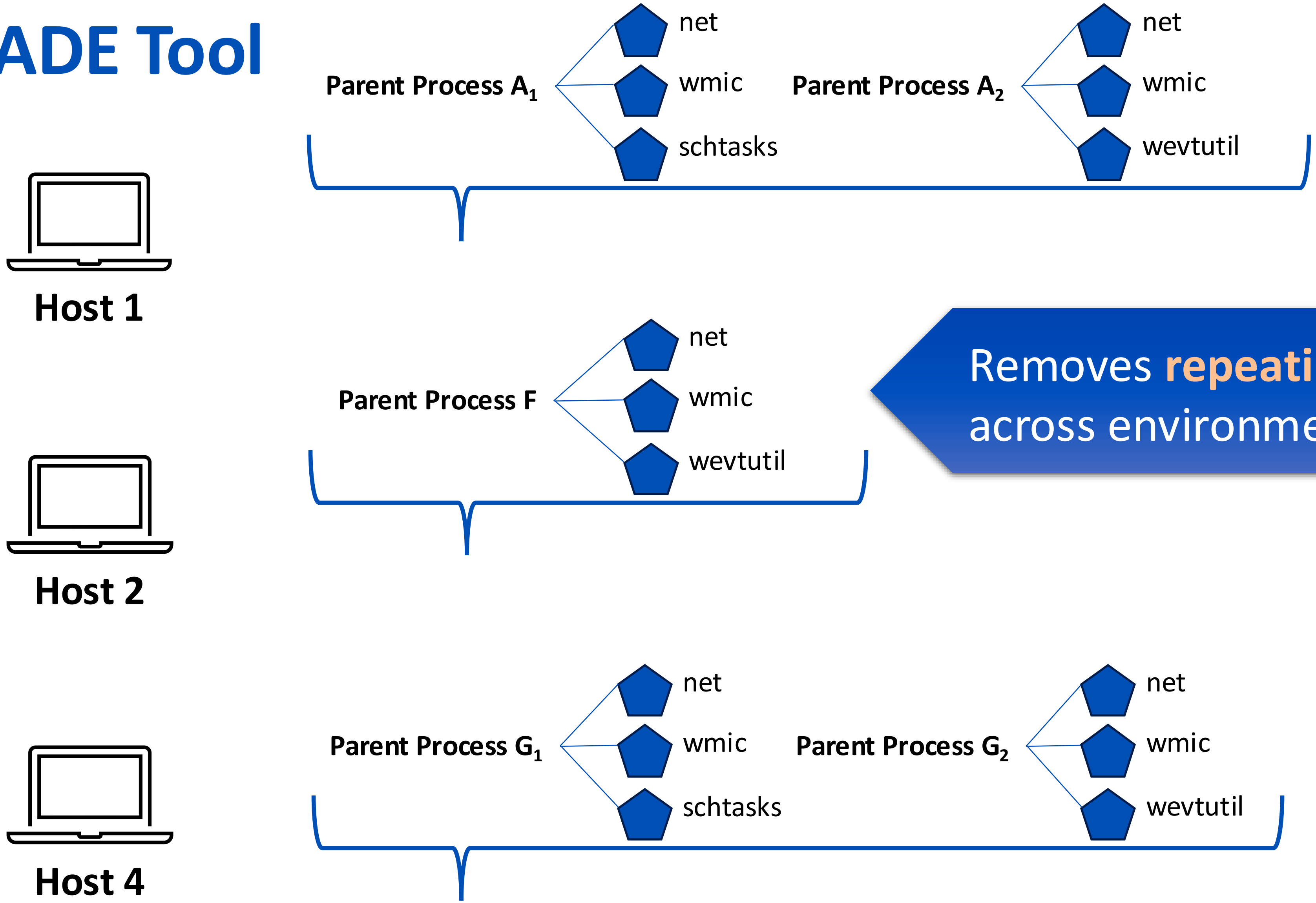
Removes **repeating parent process paths** across environment

SPADE Tool



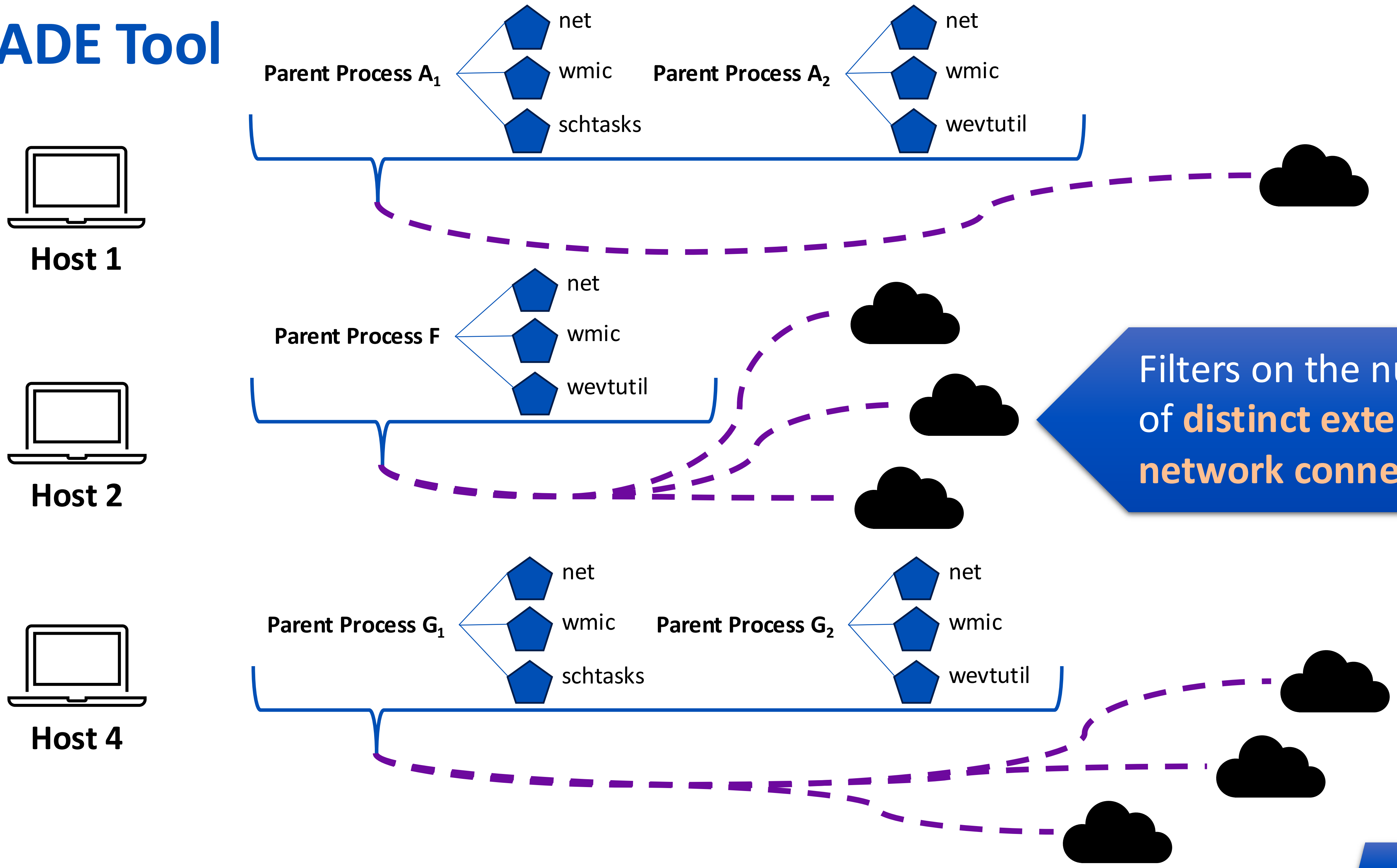
Removes **repeating parent process paths** across environment

SPADE Tool



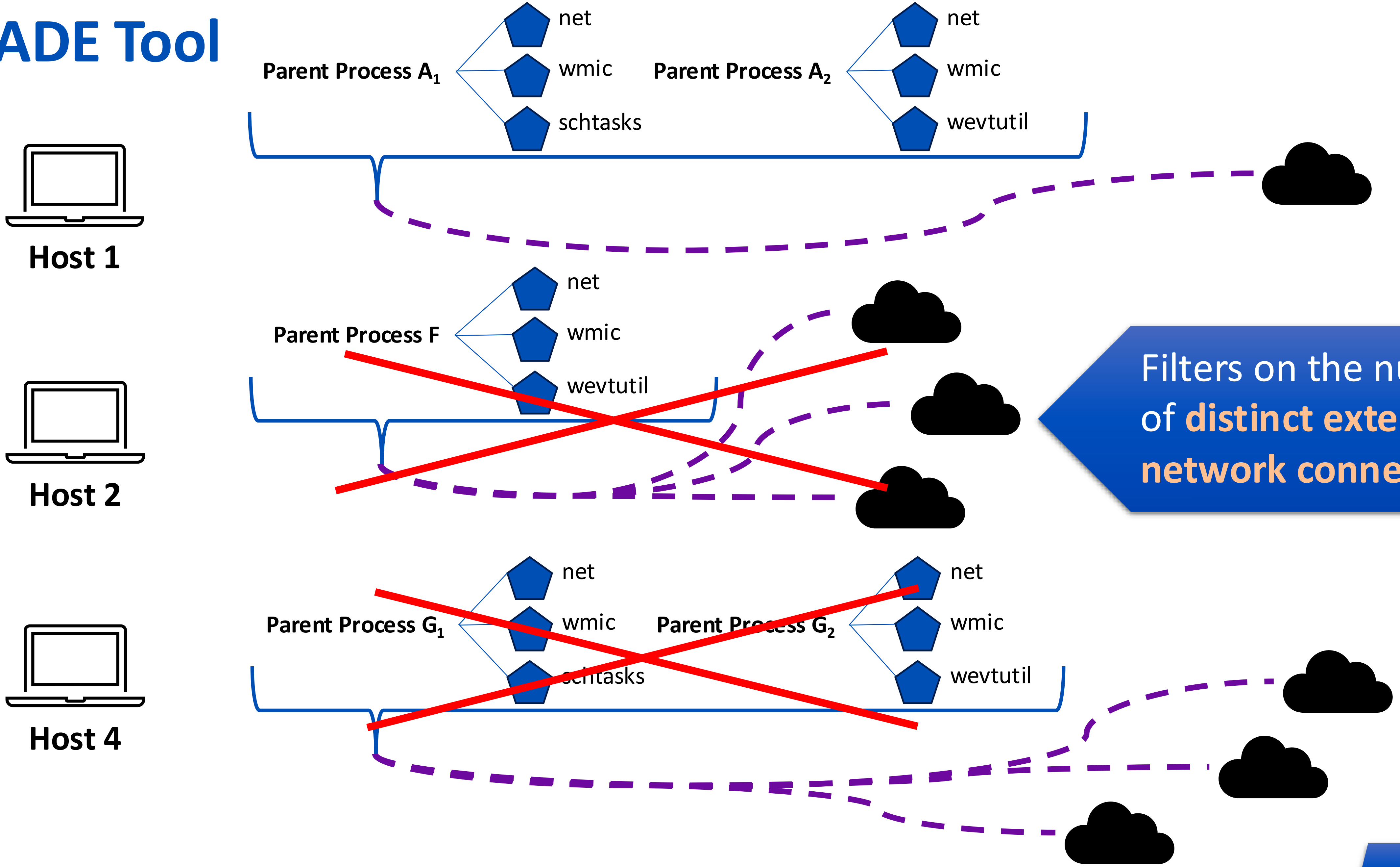
Removes **repeating parent process paths** across environment

SPADE Tool



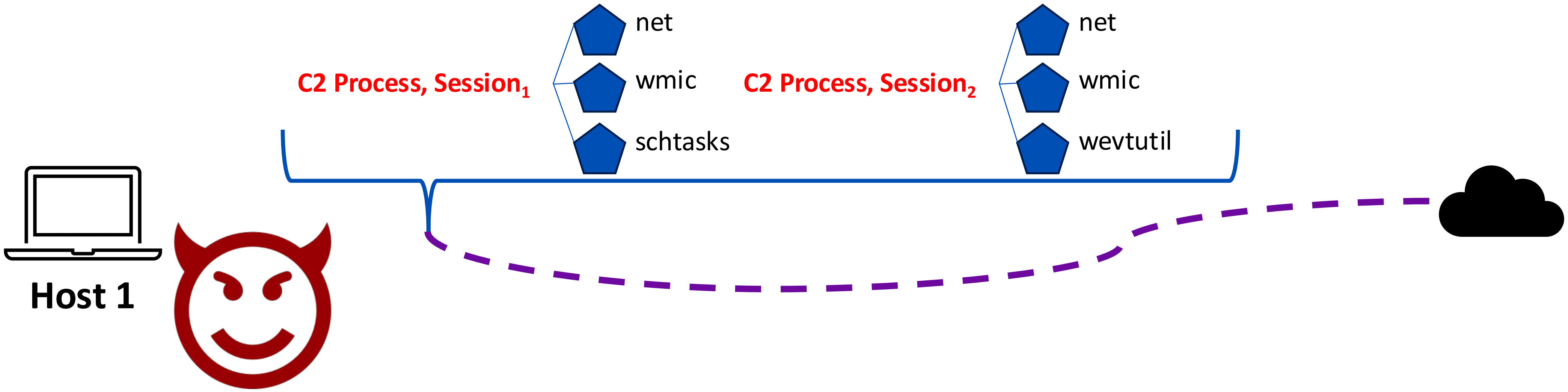
Filters on the number of **distinct external network connections**

SPADE Tool



Filters on the number of **distinct external network connections**

SPADE Tool



Leaves us with **malicious C2 session data & infrastructure**

Operation Crimson Palace Expands

Compromising other victims

Cluster Bravo Activity Expands

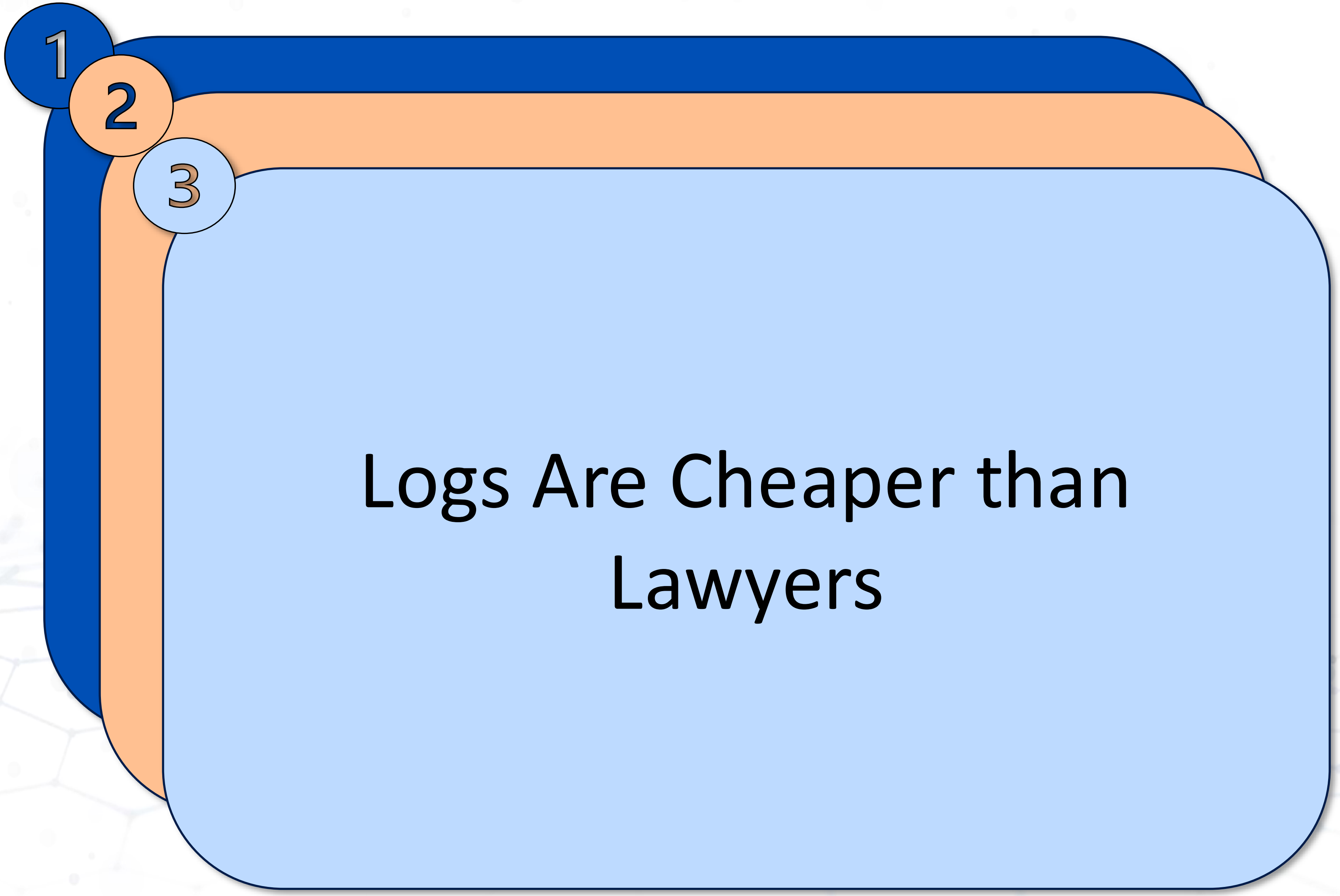
Since January 2024, Sophos has detected activity associated with Cluster Bravo on the networks of **at least 11 other organizations & agencies** in the same country

Using **previously compromised government agencies** for malware staging & C2 (command & control)

Takeaways

THERE IS NO HAPPY ENDING
imgflip.com

Takeaways



Logs Are Cheaper than Lawyers

Acknowledgments

- Paul Jaramillo
- Sean Gallagher
- Colin Cowie
- Jordon Olness
- Greg Iddon
- Hunter Neal
- Andrew Jaeger
- Kostas Tsialemis
- Gabor Szappanos
- Andrew Ludgate
- Steeve Gaudreault
- Daniel Souter
- Pavle Culum
- Peter Mackenzie
- Elida Leite
- Lee Kirkpatrick

...as well as many other members of the Sophos MDR APT, Operations, Rapid Response, and LABS teams for their work

Q
A

Appendix – Read More About Operation Crimson Palace: Stage 1

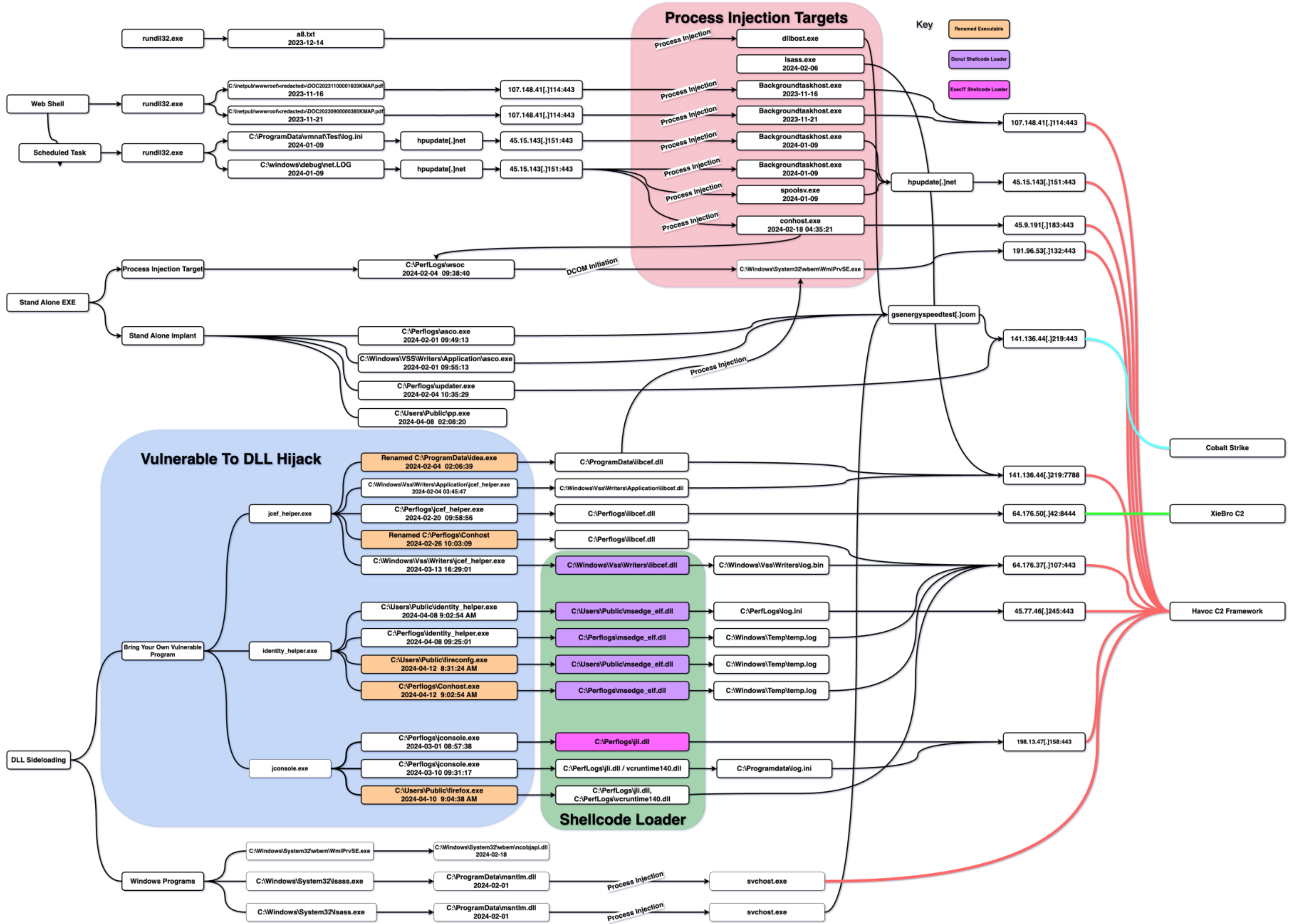
SOPHOS NEWS

Operation Crimson Palace: Overview

SOPHOS NEWS

Operation Crimson Palace: A Technical Deep Dive

Appendix - Cluster Charlie C2 Channel Mind Map



Appendix – Spade C2 Detection Tool

Appendix – Further Reading

- ChamelGang & Friends | Cyberespionage Groups Attacking Critical Infrastructure with Ransomware
  - "Threat actors in the cyberespionage ecosystem are engaging in an increasingly disturbing trend of using ransomware as a final stage in their operations for the purposes of financial gain, disruption, distraction, misattribution, or removal of evidence."
- IOC Extinction? China-Nexus Cyber Espionage Actors Use ORB Networks to Raise Cost on Defenders
  - "China-nexus cyber espionage operations where advanced persistent threat (APT) actors utilize proxy networks known as 'ORB networks' (operational relay box networks) to gain an advantage when conducting espionage operations."
- Is CNVD ≥ CVE? A Look at Chinese Vulnerability Discovery and Disclosure
  - "The US is still lagging behind China in terms of vulnerability discovery and disclosure. While the gap between the US National Vulnerability Database (NVD) and the Chinese NVD (CNNVD) has slightly shrunk over the last 5 years, there are still hundreds of vulnerabilities registered in China that are yet to be listed on the US NVD. Based on information collected, it was determined that the 151 companies providing the MSS vulns employ 1,190 vulnerability researchers and that they provide at least 1,955 vulnerabilities to the MSS each year."