Anatomy of an Attack
Using Attack Phases In Your Ransomware Investigation

Brian Carrier, CTO

ResponderCon

Sep 13, 2022

CYBER TRIAGE

BasisTech

Goal of Today's Talk

There are two goals of this opening talk:

1) Provide an overview of ransomware attacks for those here who are not familiar with them.

1) Outline our structure for approaching ransomware attacks to guide our customers in their investigation.

Who Am I?

- Involved with DFIR for 20+ years
- Original author of Autopsy and The Sleuth Kit
- Author of File System Forensic Analysis (now out of print)
- CTO at Basis Technology
- We build Autopsy and Cyber Triage

Autopsy vs Cyber Triage

Open Source Digital Forensics

General Purpose Tool

Focused on Deep Analysis

Tens of Thousands of Downloads

Incident Response Software

Hyper Focused on Intrusions

Focused on Triage

Lots of Automation!

Additional Ransomware Resources

- This talk covers the highlights.
- Many links are given to other sites.
- Great Resources:
  - Book: ‘Ransomware: Understand. Prevent. Recover’ by Allan Liska
  - Case Studies: ‘The DFIR Report’.
    - https://thedfirreport.com/
  - Quarterly Updates: Cove Ware:
    - https://www.coveware.com/

Part 1: Example Intrusions

DFIRReport: Sodinokibi (aka REvil)

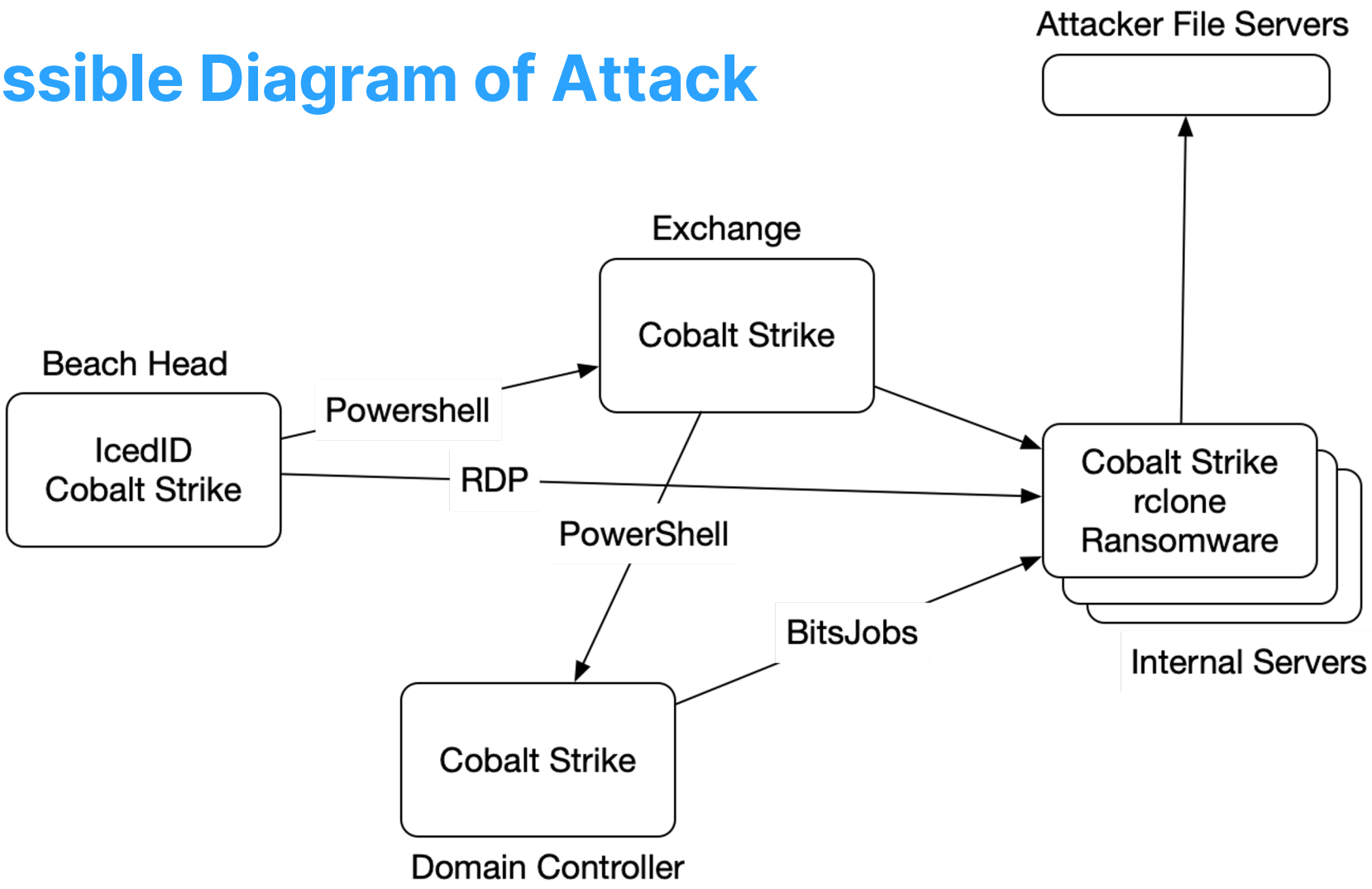
https://thedfirreport.com/2021/03/29/sodinokibi-aka-revil-ransomware/

- Malicious email attachment downloaded IcedID Trojan
- IcedID was added as a scheduled task for persistence
- IcedID was used to download Cobalt Strike (CS)
- Various tools were used to map out the network
- CS was remotely launched on Exchange server (via SMB and Powershell)
- CS was launched on domain controllers and other computers from Exchange server.

DFIRReport: Sodinokibi (aka REvil) (2)

- Credentials were eventually found (dumping lsass) and RDP was used to move around network
- Data was exfiltrated from servers using ‘rclone’
- Ransomware EXE was downloaded to domain controller
- BITSJobs was used to transfer EXE from domain controller to hosts
- Attacker used RDP to start EXE on each host

Possible Diagram of Attack



DFIRReport: Quantum

https://thedfirreport.com/2022/04/25/quantum-ransomware/

- Email was opened with malicious attachment with IcedID (again)
- Beachhead had a scheduled task added and attackers got credentials
- Cobalt Strike (again) was used on beachhead and other servers to perform discovery of the environment
- Remote Desktop was used to log into servers and other systems
- Access to domain controller (DC) and file servers was obtained
- Ransomware was copied to target system via C$ share from DC
- Ransomware was launched on each system using both PsExec and WMI

Differences: How ransomware was deployed.

DFIRReport: Conti

https://thedfirreport.com/2021/09/13/bazarloader-to-conti-ransomware-in-32-hours/

- beachhead had BazarLoader run (not IcedID)
- Discovery was performed and Cobalt Strike downloaded (again)
- Remote processes were launched via WMI. Lateral movement via RDP and Cobalt Strike beacons.
- Gained access to file server and domain controller
- SCPed data from file server to attacker's server for data exfiltration
- Attackers manually launched Conti via RDP on several hosts.
- Conti will mount other hosts C$ drives and remotely encrypt them (self propagation).

Differences: Loader, propagation, SCP exfiltration

DFIRReport: BumbleBee

https://thedfirreport.com/2022/08/08/bumblebee-roasts-its-way-to-domain-admin/

- Initial access via Phishing loads BumbleBee loader
- Cobalt Strike is downloaded to beachhead
- RDP was used to access other hosts.
- AnyDesk was installed on a server for persistence
- Various methods were used to get domain admin credentials. Many hosts were logged into to dump lsass.
- Eventually Kerberoasting was used to get domain service account.
- CS was installed on domain controller. They were detected.

Differences: Loader. Install AnyDesk. Logged into lots of computers.

Microsoft: BlackCat

https://www.microsoft.com/security/blog/2022/06/13/the-many-lives-of-blackcat-ransomware/

- Initial access was via compromised credentials and RDP
- Installs commercial tools Total Deployment Software and ScreenConnect/ConnectWise on various hosts
- Created local admin accounts for persistence
- BlackCat was downloaded via Chrome and launched.
- BlackCat propagates itself using PsExec to other hosts.

Differences: ConnectWise, local account was created, BlackCat self propagates.

That’s Enough For Now…

- There are lots of other examples and variations…That’s the problem.
- There are many ways to achieve the same goals.
- How does the responder know when to stop looking?

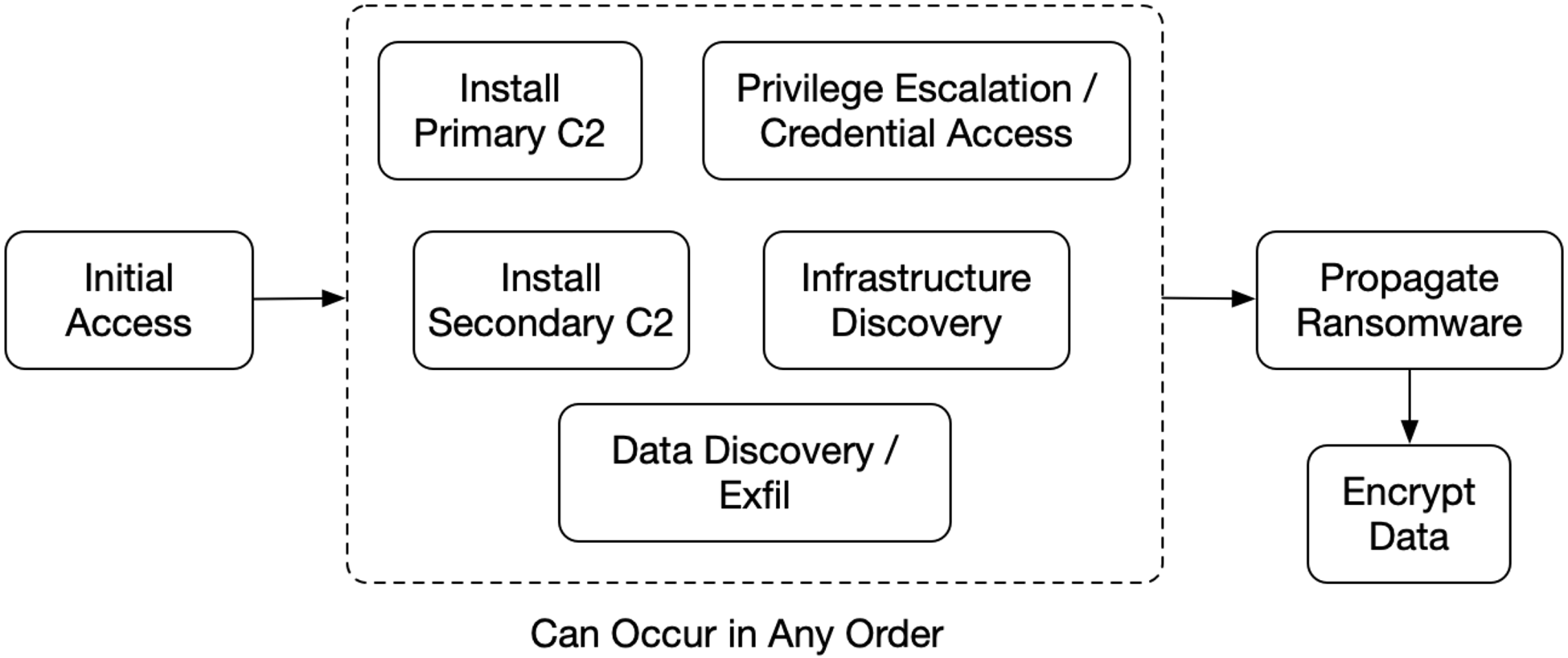
- We wanted to define a Ransomware Framework to help our customers.

Part 2: Frameworks

Our Framework Goals

- Develop a more specific phase-based framework ransomware attacks.
- Responders can use it to ensure they have artifacts for each phase.
- Some phases will be automatic based on the ransomware type.
  - Propagation for example.

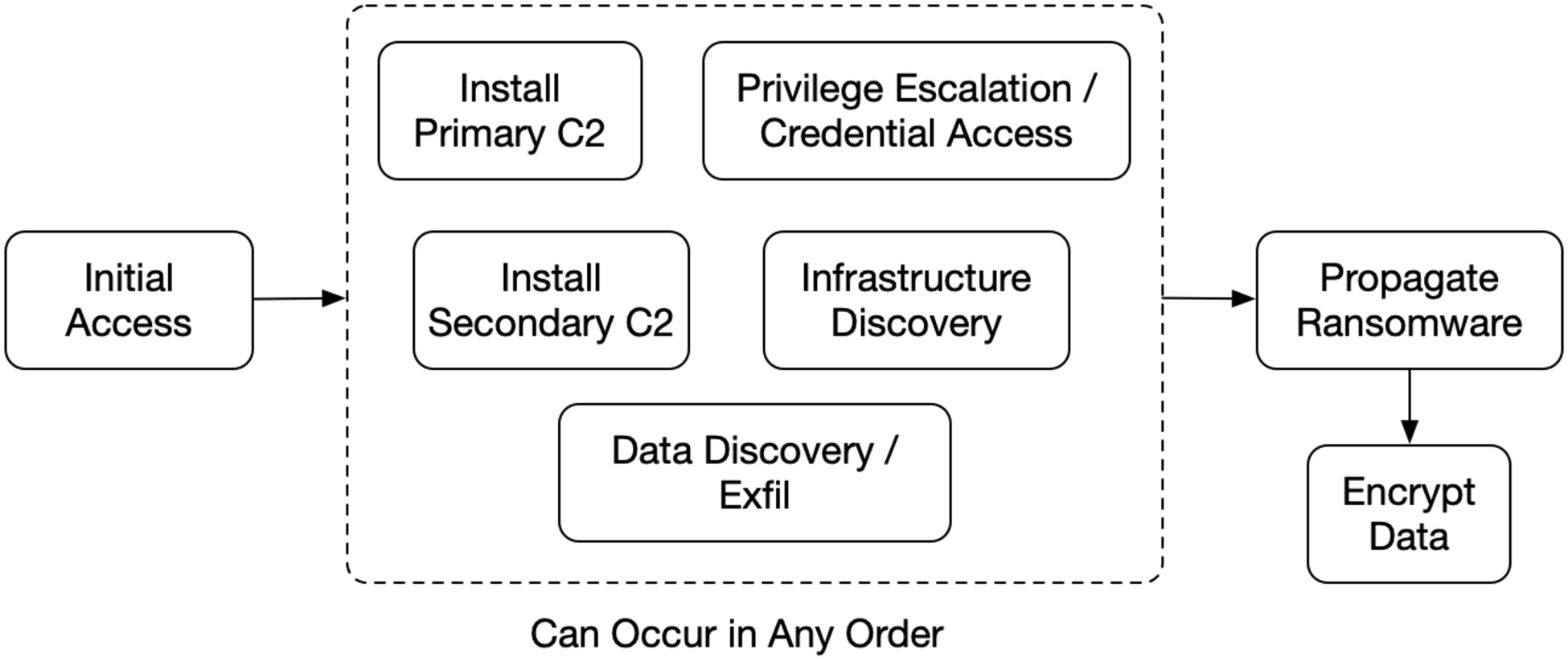
Visual Overview



Initial Access Phase

- The attacker needs initial access into the network.
- It’s important to find this because it tells you want to fix and this host will often have evidence of infrastructure discovery.
- Common techniques include:
  - Phishing
  - Exposed RDP
  - Exploiting vulnerabilities

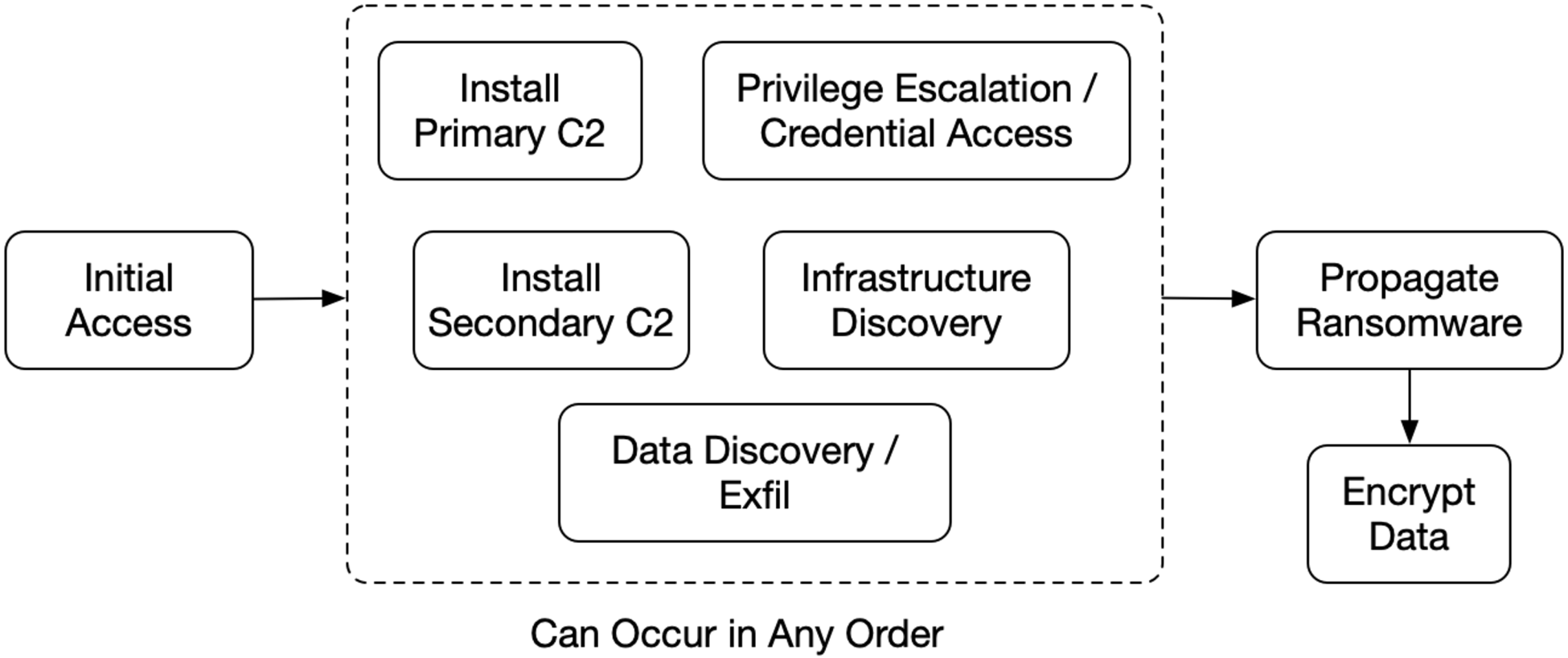
Visual Overview



Install Primary C2 Phase

- Most “Hands On” ransomware requires the attacker to interact with hosts on the network.
- It’s important to find hosts that have C2 so that attacker no longer has access.
- Some are persistent.
- Common techniques include:
  - Loaders, such as IcedID or Bazaar
  - Cobalt Strike
  - Remote access software

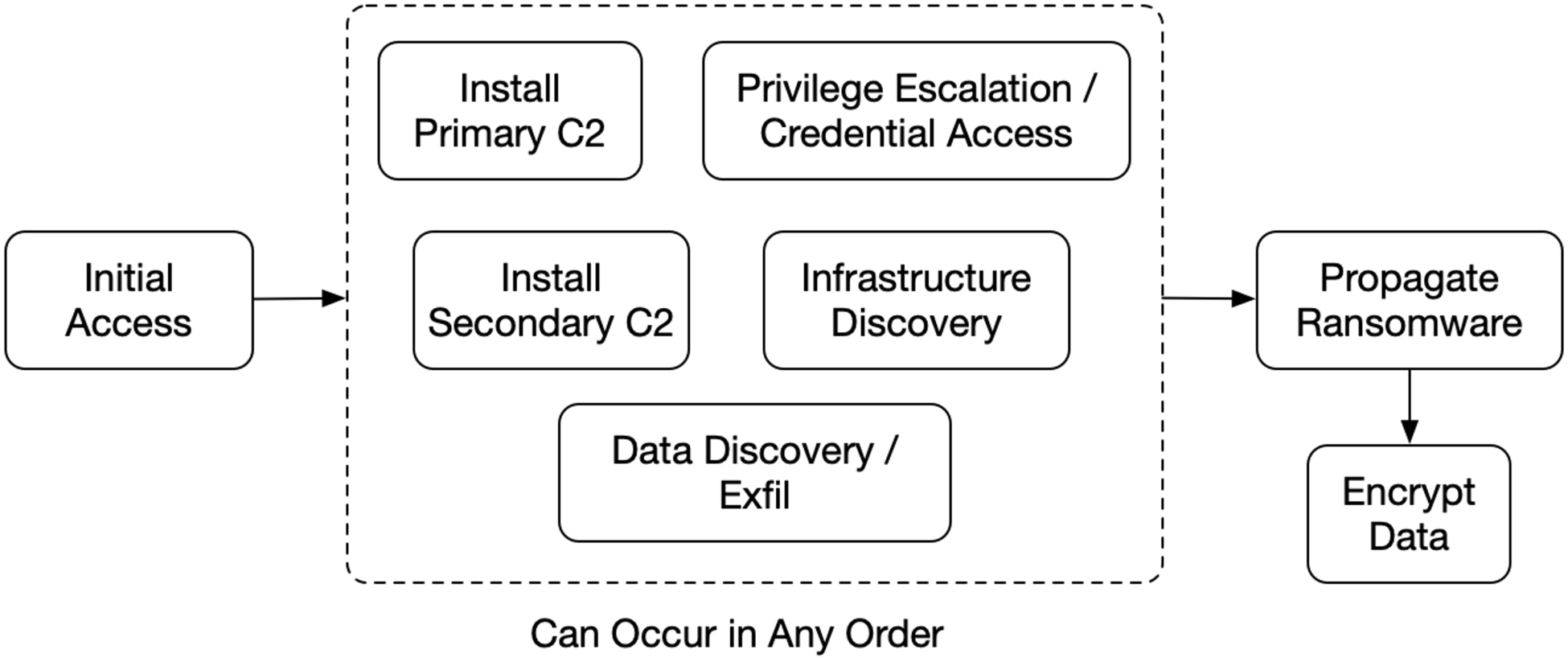
Visual Overview



Install Secondary C2 Phase

- Some attackers will install additional persistence and C2 in case the primary methods are removed.
- An initial access broker could have also installed something.
- Example:
  - Create user account
  - Persistence on a random system

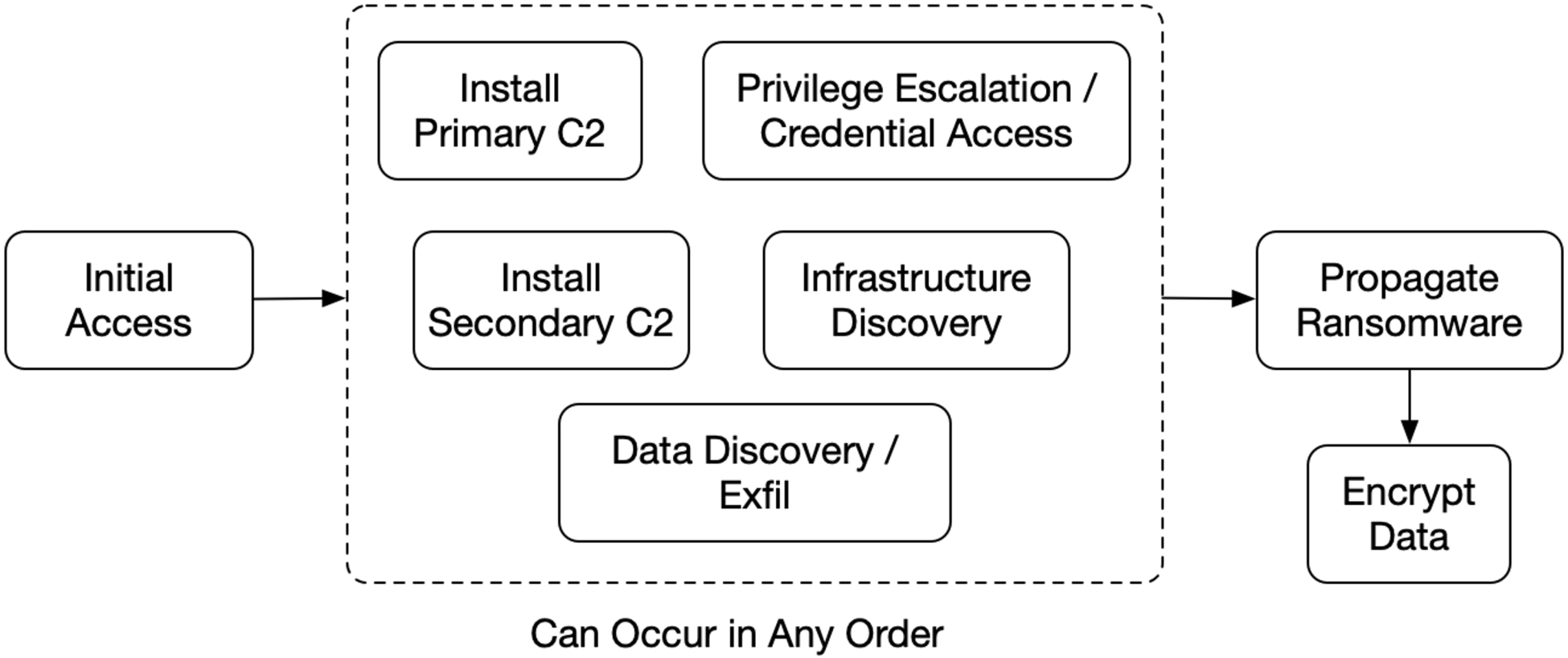
Visual Overview



Privilege Escalation / Credential Access Phase

- Privileged accounts are needed to gain access to domain controller and file servers.
- Important to find out where they got access and which accounts.
- This could occur on several hosts during the attack.
- Examples:
  - Dump lsass memory
  - mimikatz
  - Kerberoasting

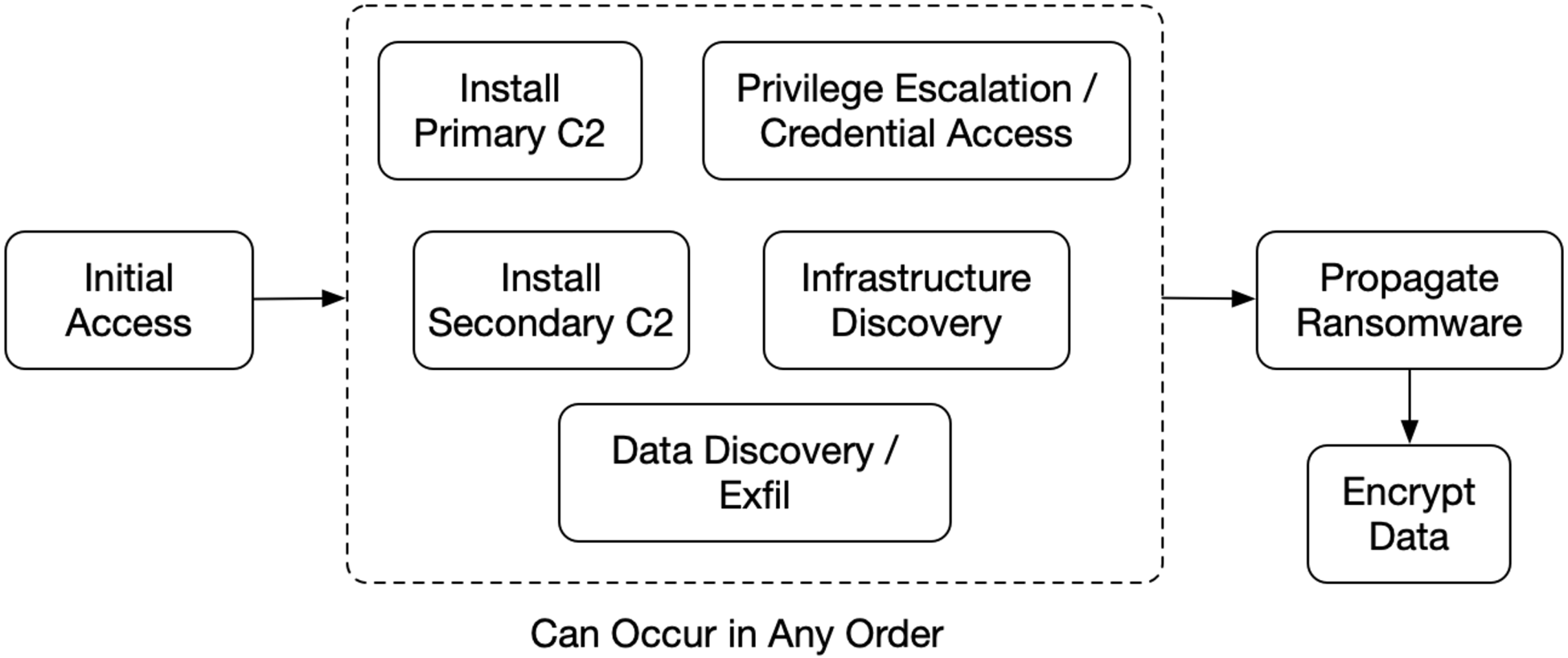
Visual Overview



Infrastructure Discovery Phase

- Attackers want to find domain controllers and file servers to maximize impact.
- Want to understand what the beachhead gives them.
- This could occur on several hosts during the attack.
- Examples:
  - adfind and ADRecon
  - ping.exe
  - net.exe
  - etc.

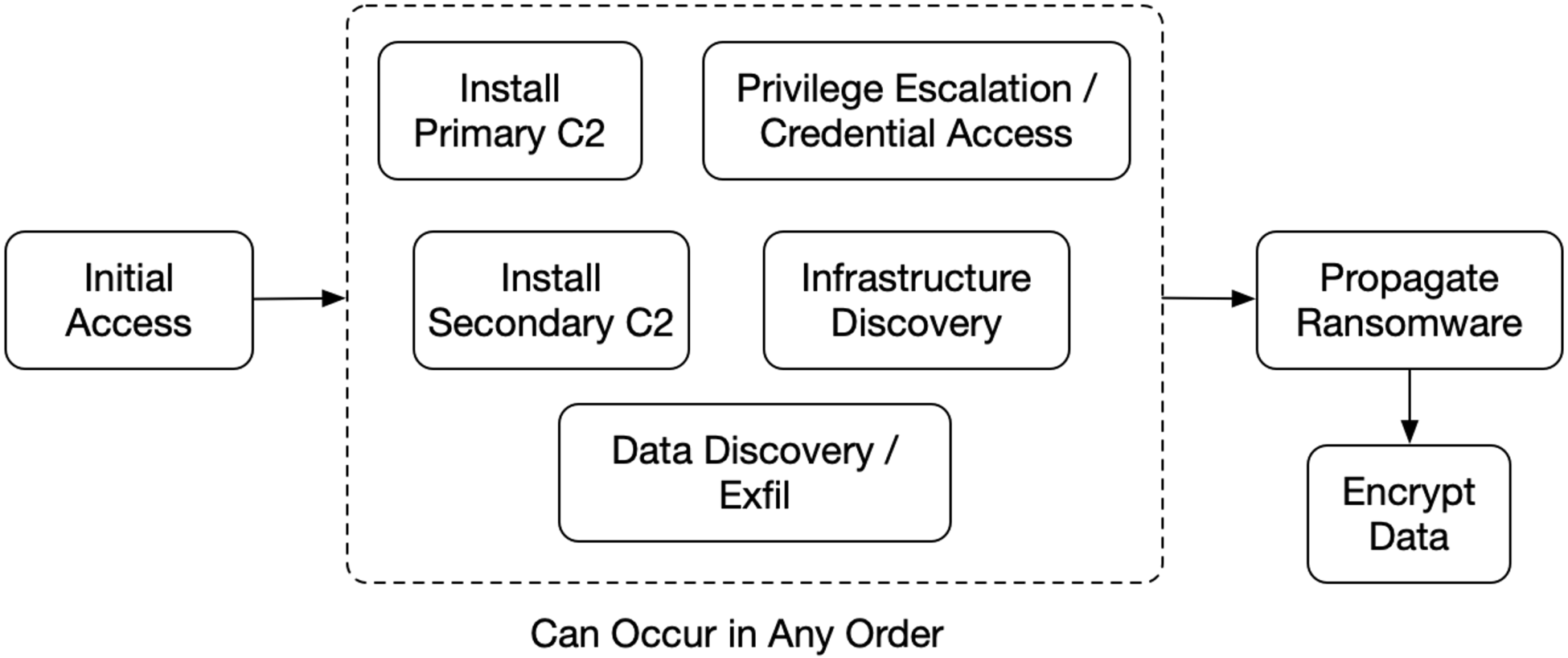
Visual Overview



Data Discovery / Exfil Phase

- Attackers want to make sure they copy and encrypt critical data.
- Seek out file servers and computers with important data.
- Examples:
  - Focus on file servers
  - Look at usage and login activity of endpoints
  - Copy via rclone, scp, sftp, etc.

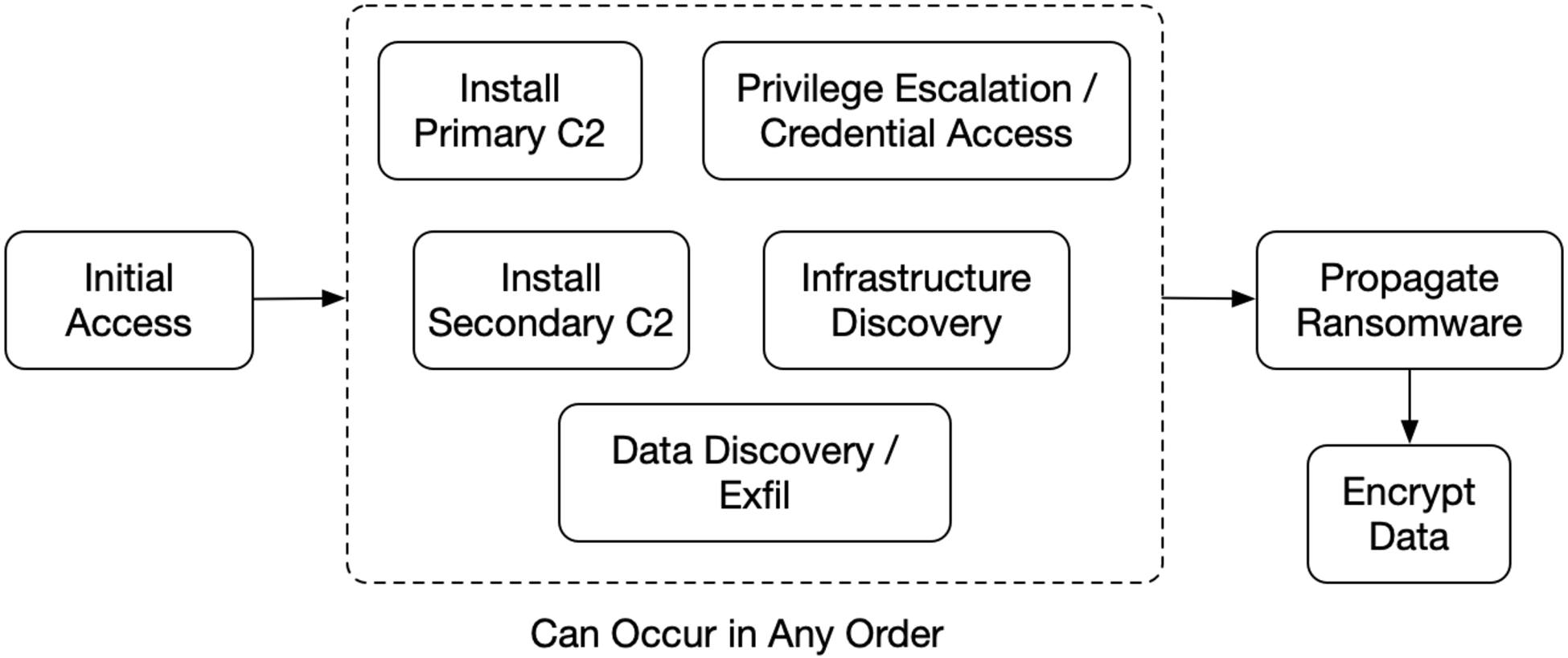
Visual Overview



Propagate Ransomware Phase

- Ransomware needs to be copied onto victims and launched.
- Some propagate themselves.
- Knowing how this happened is critical to tracing back.
- Examples:
  - Manual via RDP
  - PsExec
  - Group Policy Objects

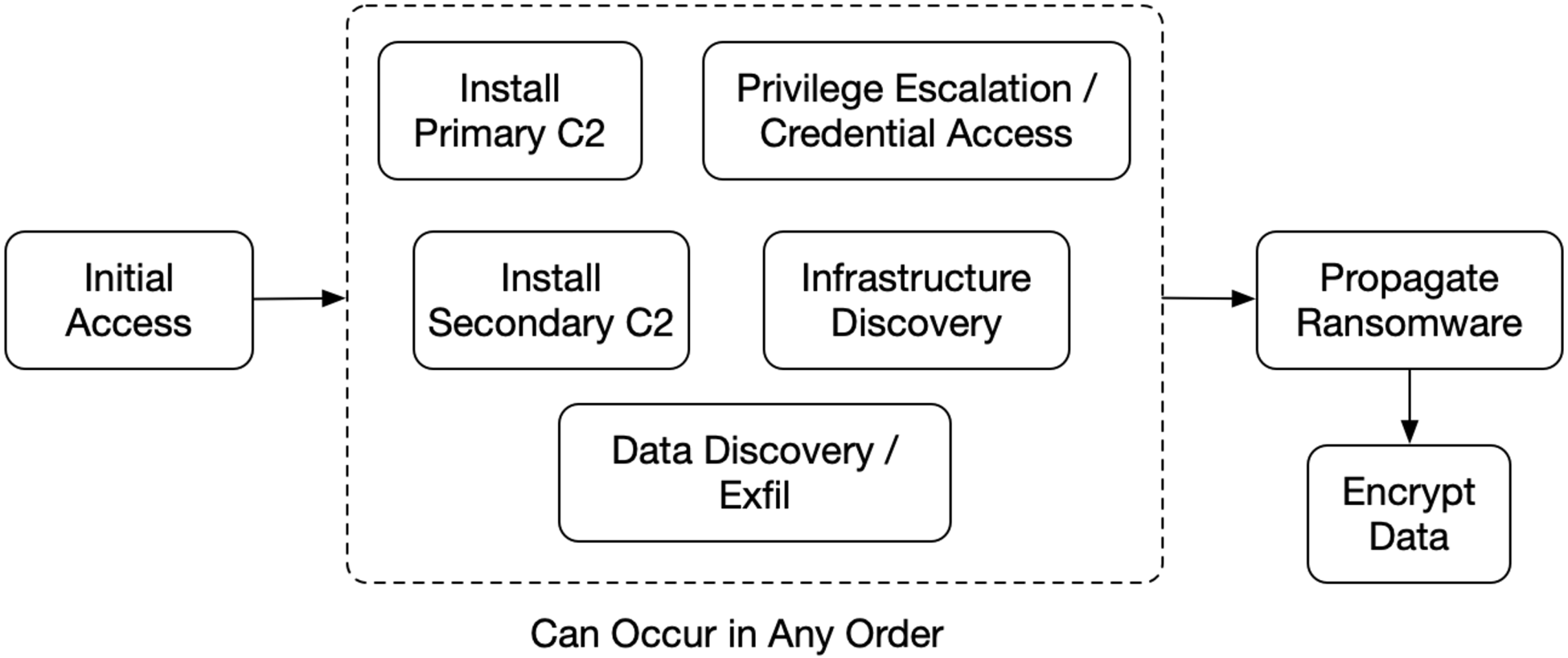
Visual Overview



Encrypt Data Phase

- Ultimately, data gets encrypted.
- Can happen from EXE running locally or by drive being mounted by another system.
- Ransom notes are created.
- It’s important to know where the EXE ran from.

Visual Overview



Phases vs Hosts

- A host can be used during multiple phases.
- When reviewing a host, consider all phases.
- For example, the beachhead could be:
  - Initial Access
  - Primary C2
  - Infrastructure Discovery
  - Privilege Escalation

Part 3: Using the Framework

Checklist

- Keep track of which phases you've discovered.
- Work backwards.
- Learn about the ransomware family to determine which phases are relevant.

☐ Infrastructure Discovery

☑ Propagate Ransomware

Via GPO from Domain Controller
Copied from file share
Scheduled task launched it

Start With an Encrypted System

- Find out how it was encrypted.
  - Get timestamps from ransomware notes and encrypted files.
  - Identify the family based on extensions / notes.
  - Did the ransomware run on that host?
    - Are there signs of execution before the encryption?
    - Is Volume Shadow deleted?
    - Were services disabled?
  - Was its drive mounted?
    - Are there network logins before the encryption?
    - Does the ransomware family mount network drives?

CYBER TRIAGE

Dashboard

Bad Items 5

Suspicious Items 14

Users

Accounts 1

Inbound Logons

Outbound Logons 4

Network Shares

Programs Run 2

Bad Items

Incid

Group Items | Suspicious Items Only | Include Items on Good List | Search

Item	Type	Description
/Temp/54896b1f9ca22.exe	Program Run	Malware detected: Yes
/temp/54896b1f9ca22.exe	File	Malware detected: Yes
/users/jdoe/appdata/local/temp/java/javaperformancetester.exe	File	Malware detected: Yes
/users/jdoe/appdata/local/temp/java/javaPerformanceTester.exe	Program Run	Malware detected: Yes
/windows/system32/cmd.exe	Startup Program	Accessibility feature backdoor detected
/programdata/intel/readme.txt	File	Ransomware note suspected
/users/jdoe/appdata/local/microsoft/edge/user data/default/servic	File	Ransomware note suspected

Cyber Triage - ReversingLabs Results

Item Details | File | Process | User | Execution History | Startup Items | Data Accessed | Host Info | Logon Session | Sources

File details for /Temp/54896b1f9ca22.exe

/temp/54896b1f9ca22.exe

File Details | Malware Scan Results | Bad List | Strings | PE Header

Threat Level:	Bad
Scanner Results:	28 of 28 (100.00%) identified as malicious
Threat Name:	Win32.Ransomware.Conti
Last Seen:	10/11/21, 2:24:17 AM EDT
First Seen:	7/27/21, 2:52:40 AM EDT
Possible Impact:	High
File Source:	Uploads to Reversing Labs
Classification Generic:	False

Cyber Triage - Recorded Future Sandbox Results

Signature Matches

Name	Score
Conti Ransomware	10
Modifies extensions of user files	8
Reads user/profile data of web browsers	7
Drops desktop.ini file(s)	6
Drops file in Program Files directory	4
Suspicious behavior: EnumeratesProcesses	0
Suspicious use of AdjustPrivilegeToken	0
Suspicious use of WriteProcessMemory	0

Processes Created

PID	Parent	Process
1772	1268	"C:\Users\Admin\AppData\Local\Temp\54896b1f9ca22.exe"
1752	464	C:\Windows\system32\vssvc.exe
2036	1772	cmd.exe /c C:\Windows\System32\wbem\WMIC.exe shadowcopy

Ransomware Notes Details

Item Details | File | Process | User | Execution History | Startup Items | Data Accessed | Host Info | Logon Session | Sources | Other Occurrences | Analysis Results

Item details for /users/jdoe/appdata/local/microsoft/edge/user data/default/service worker/cachestorage/readme.txt

Item Type: File

Highest Scoring Results:

Score: Suspicious

Analysis Result Type: Ransomware note suspected

Justification: Found more than 150 copies of file with same name and size (Newest of 1975 files, size = 1,173 bytes, created = 9/17/21, 4:22:30 PM EDT)

Path: /users/jdoe/appdata/local/microsoft/edge/user data/default/service worker/cachestorage/readme.txt

Next, Focus on Propagation

- What launched the executable?
  - Scheduled Task from Group Policy?
  - Interactive login?
  - PsExec?
- Use logs (if available) and work backwards.
  - Go to domain controller
  - Go to source of interactive login

Show Logon Session For Event

CYBER TRIAGE

Dashboard
Bad Items 5
Suspicious Items 13
Users
Accounts 1
Inbound Logons
Outbound Logons 4
Network Shares
Programs Run 2
Web Artifacts
Data Accessed
Malware
Startup Items 1
Triggered Tasks 1
Processes

Bad Items

Group Items | Suspicious Items Only | Include Items on Good List | Search

Item	Type	Description
/Temp/54896b1f9ca22.exe	Program Run	Malware detected: Yes
/temp/54896b1f9ca22.exe	File	Malware detected: Yes
/users/jdoe/appdata/local/temp/java/javaPerformanceTester.exe	Program Run	Malware detected: Yes
/users/jdoe/appdata/local/temp/java/javaperformancetester.exe	File	Malware detected: Yes
/windows/system32/cmd.exe	Startup Program	Accessibility feature backdoor detected

Mark item as a: Bad Item | Suspicious Item | Good Item | Unknown | Add Comment

Item Details | File | Process | User | Execution History | Startup Items | Data Accessed | Host Info | Logon Session | Sources | Other Occurrences | Analysis Results

Related logon session

User: jdoe, start time: 9/17/21, 1:15:52 PM EDT, end time: Unknown, type: Remote Interactive

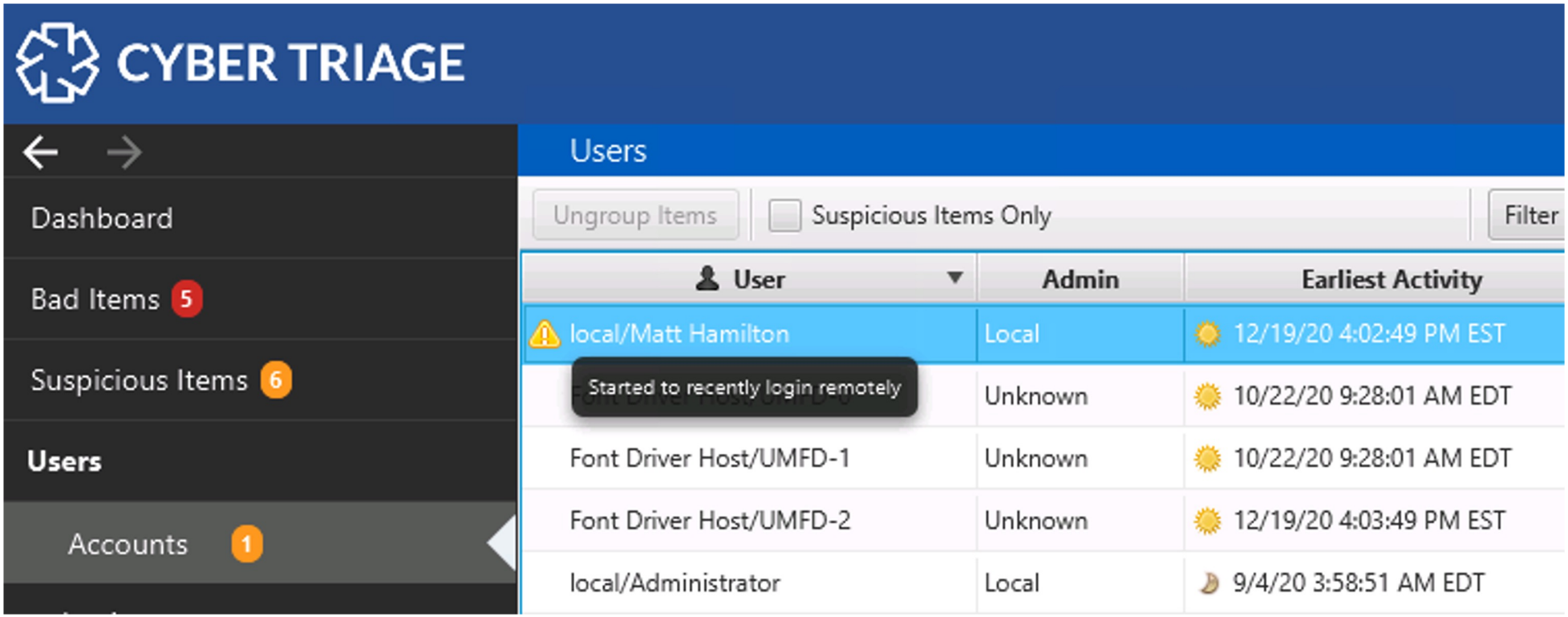
Name: Success: acme/jdoe from 10.1.2.15 @ Start=9/17/21, 1:15:52 PM EDT, End=Unknown
Item Type: Logon Session
User: acme/jdoe
Host: 10.1.2.15
Country: Local

Dive Into Each Host

Anything could be on that host. Look for all phases.

- Inbound and Outbound Logons
- Suspicious processes
- Connections / DNS cache to suspicious hosts
- Infrastructure discovery commands
- New users
- Backdoors
- Follow up on all inbound and outbound hosts
- Search for indicators as they are found

Cyber Triage Flags with New Remote Logins



Back To The First Example - REvil

- Initial Access
  - XLSX attachment with macro on host A.
  - Downloaded IcedID trojan
- Install Primary C2
  - Cobalt Strike on many systems
- Install Backup C2 / Persistence
  - None found
- Privilege Escalation
  - Exploited UAC Bypass
  - Dumped credentials on several systems
- Perform Data Discovery / Exfil
  - Rclone from host X to server Y
- Propagate Ransomware
  - BITSJobs to copy from domain controller
  - Launched via RDP from host X
- Encrypt Data
  - EXE encrypted local data

Summary

- A framework can provide some structure around your investigation and making sure you've considered possible evidence.
- You may not find all evidence, but it's good to make sure you've tried.
- Cyber Triage has and is building in automation to help with this process.
  - Check out the booth in the lobby!

BTW - We're Hiring

We're looking for a Director of Training if you'd like to help make front line responders as efficient as possible!

https://www.cybertriage.com/about/careers/

Contact

Brian Carrier

brianc@basistech.com

LinkedIn: https://www.linkedin.com/in/carrier4n6/

Twitter: @carrier4n6