

# **Strengthening Your Blue Teaming Skills: Thinking Like an Attacker**

Copyright © 2023 BlueCapeSecurity



# Agenda

- Ransomware Scenario as an Example
- Required Blue Team Skills and Knowledge
- Learning Offense is Your Best Defense





# ***The Anatomy of a Ransomware Attack***



# Organized Cybercrime: Ransomware

## Targets:

Businesses

## Motivations:

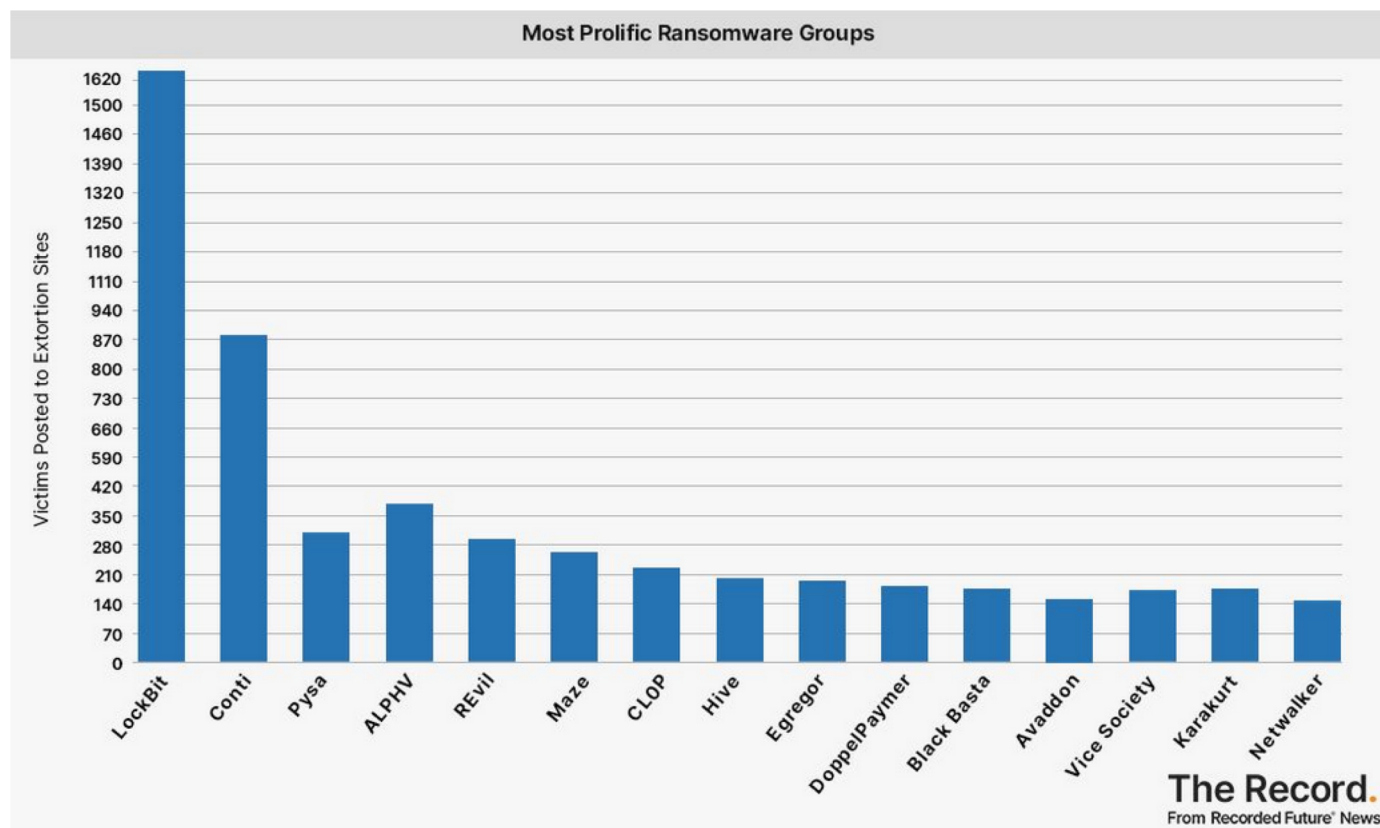
Financial Gain

## Business Model:

Ransomware as a Service (RaaS)

## Ransomware Affiliate:

A person or group who rents access to Ransomware-as-a-Service (RaaS) platforms, orchestrates intrusions into corporate networks, encrypt files with the “rented ransomware,” and then earn a commission from successful extortions.

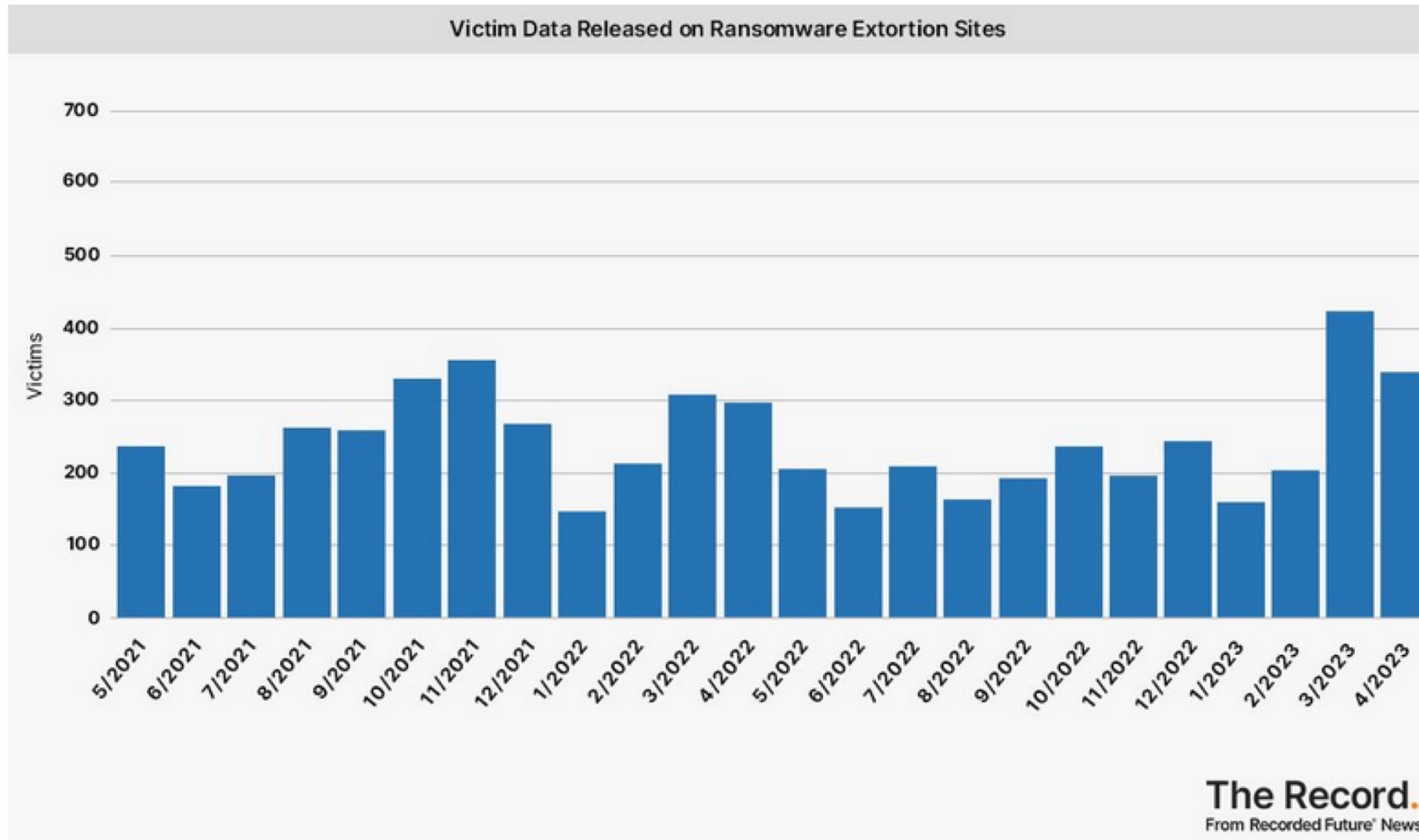


<https://therecord.media/ransomware-tracker-the-latest-figures> (May 2023)





# Organized Cybercrime: Ransomware

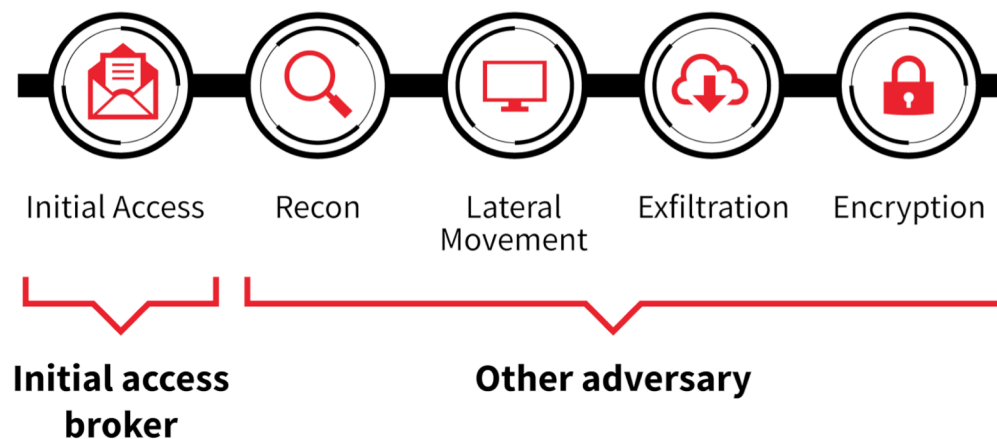


# Access Broker Business Model

## Access Broker Boom Accelerated in 2022

Access brokers are threat actors who acquire access to organizations and provide or sell this access to other actors, including ransomware operators. The popularity of their services increased in 2022, with more than 2,500 advertisements for access identified — a 112% increase compared to 2021.

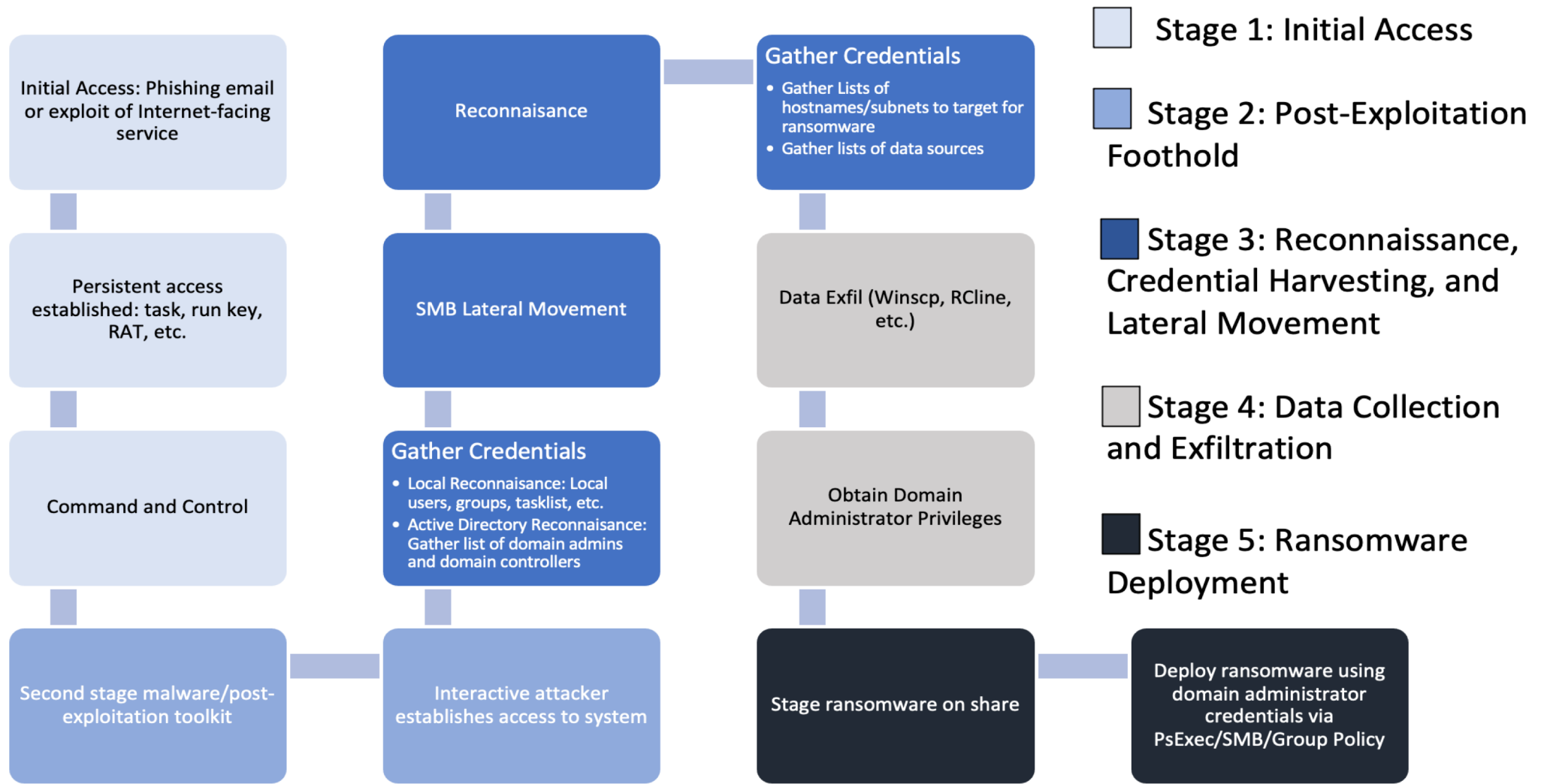
- CrowdStrike 2023 Global Threat Report



<https://redcanary.com/threat-detection-report/trends/ransomware/>



# Ransomware Attack Lifecycle



<https://securityintelligence.com/posts/how-ransomware-attacks-happen/>



18041#-Malicious ISO File Leads to Domain Wide Ransomware

	Tools	Technique	Exploited Vulnerabilities
Initial Access		T1566.001 Phishing: Spearphishing Attachment	
Execution	IcedID Cobalt Strike	T1059.001 Command and Scripting Interpreter: PowerShell T1059.003 Command and Scripting Interpreter: Windows Command Shell T1204.002 User Execution: Malicious File T1569.002 System Services: Service Execution T1047 Windows Management Instrumentation	
Persistence	IcedID	T1053.005 Scheduled Task/Job: Scheduled Task	
Privilege Escalation	Cobalt Strike — GetSystem	T1134.001 Access Token Manipulation: Token Impersonation/Theft T1068 Exploitation for Privilege Escalation	ZeroLogon CVE-2020-1472
Defense Evasion		T1562.001 Impair Defenses: Disable or Modify Tools T1218.010 System Binary Proxy Execution: Regsvr32 T1218.011 System Binary Proxy Execution: Rundll32 T1055 Process Injection T1553.005 Mark-of-the-Web Bypass	
Credential Access	Mimikatz ProcDump	T1003.001 OS Credential Dumping: LSASS Memory T1003.006 OS Credential Dumping: DCSync	
Discovery	<ul style="list-style-type: none"> <li>— ntest</li> <li>— net</li> <li>— chcp</li> <li>— ipconfig</li> <li>— systeminfo</li> </ul>	T1482 Domain Trust Discovery T1082 System Information Discovery T1018 Remote System Discovery T1615 Group Policy Discovery T1614.001 System Location Discovery: System Language Discovery T1124 System Time Discovery T1135 Network Share Discovery T1087.002 Account Discovery: Domain Account T1083 File and Directory Discovery T1033 System Owner/User Discovery	
	<ul style="list-style-type: none"> <li>— net</li> <li>— nslookup</li> <li>— Invoke-ShareFinder</li> <li>— Get-EventLog</li> <li>— Get-ADComputer</li> <li>— Custom PowerShell</li> <li>— Custom Batch Scripts</li> <li>— Adget</li> <li>— WMI Queries</li> <li>— dir</li> </ul>		
	<ul style="list-style-type: none"> <li>— Group Policy</li> <li>— Invoke-ShareFinder</li> <li>— Veeam Backup Console</li> </ul>		
Lateral Movement	Cobalt Strike	T1021.001 Remote Services: Remote Desktop Protocol T1021.002 Remote Services: SMB/Windows Admin Shares T1021.004 Remote Services: Windows Remote Management T1570 Lateral Tool Transfer	
Collection	Local Files Text, TSV, CSV	T1074.001 Data Staged: Local Data Staging	
Command and Control	IcedID Cobalt Strike AnyDesk Atera Splashtop	T1071.001 Application Layer Protocol: Web Protocols	
Exfiltration	Rclone — Mega.io	T1567.002 Exfiltration Over Web Service: Exfiltration to Cloud Storage	
Impact	Quantum Ransomware	T1486 Data Encrypted for Impact	
	net user	T1531 Account Access Removal	

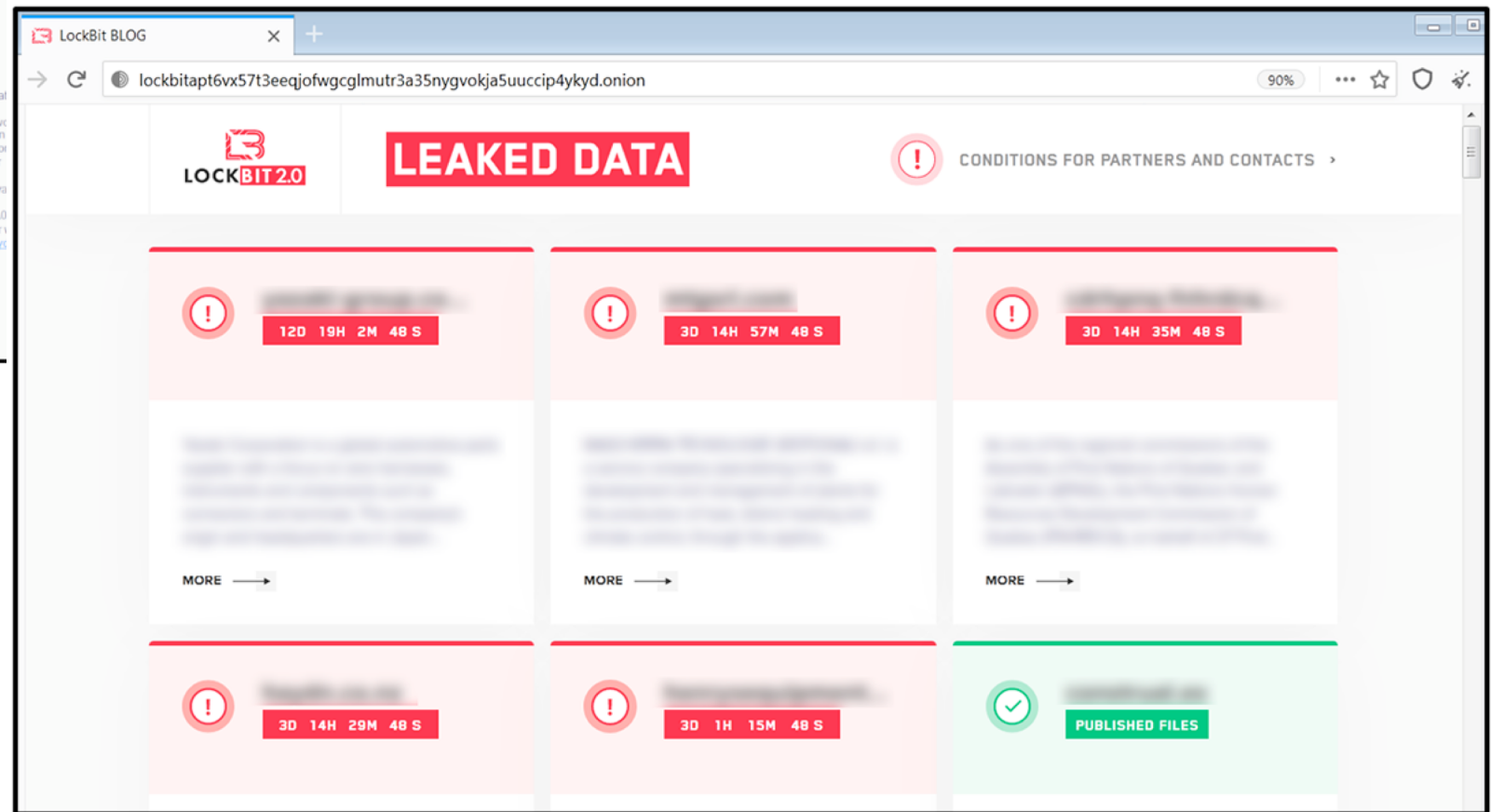
# Ransomware DFIR Report

- 🔥 Initial Access: IcedID ISO
- 🔥 Credentials: DCsync
- 🔥 PrivEsc: ZeroLogon
- 🔥 Lateral: RDP, SMB/Remote Service, WMI
- 🔥 C2: IcedID, Cobalt Strike, Anydesk
- 🔥 Exfil: Rclone to Mega
- 🔥 Impact: Quantum Ransomware

This case was analyzed and published by “The DFIR Report”:  
<https://thedfirreport.com/2023/04/03/malicious-iso-file-leads-to-domain-wide-ransomware/>




# BOOM!



<https://blogs.blackberry.com/en/2021/08/threat-spotlight-lockbit-2-0-ransomware-takes-on-top-consulting-firm>







***Required  
Blue Team Skills  
and Knowledge***



# Ransomware: Tactics, Tools and Techniques

Initial Access	Post-Exploitation	Impact
<ul style="list-style-type: none"><li>➤ TA001 Initial Access Phishing (MalDoc Attachment)</li></ul>	<ul style="list-style-type: none"><li>➤ TA003 Persistence Scheduled Tasks, Run Keys, Accounts creation</li><li>➤ TA007 Discovery net, whoami, ipconfig, wmic</li><li>➤ TA004 Privilege Escalation UAC bypass</li><li>➤ TA0006 Credential Access LSASS, SAM, Mimikatz</li><li>➤ TA0008 Lateral Movement Pass-the-hash, Pass-the-ticket</li><li>➤ TA0005 - Defensive Evasion Process injection (rundll32.exe), DLL hijacking</li><li>➤ TA007 Discovery AdFind</li><li>➤ TA0011 Command and Control Cobalt Strike, Empire</li></ul>	<ul style="list-style-type: none"><li>➤ TA0010 Exfiltration 7zip, RClone, WinSCP</li><li>➤ TA0040 Impact Deleting data Data Encryption (via PsExec, WMIC, RunDll32)</li></ul>



# Blue Team Knowledge & Skills You Need!

## Fundamentals

Active Directory Domain Services

Group Policy Objects

Living off the Land Tools

Windows System Internals

Windows and Domain Authentication

## Intermediate

Evidence Acquisition Techniques

Windows Forensic Analysis

Malware Analysis

Network Traffic Analysis

Cloud Forensic Analysis

## Advanced

Red Team Attack Operations

Enterprise Incident Response

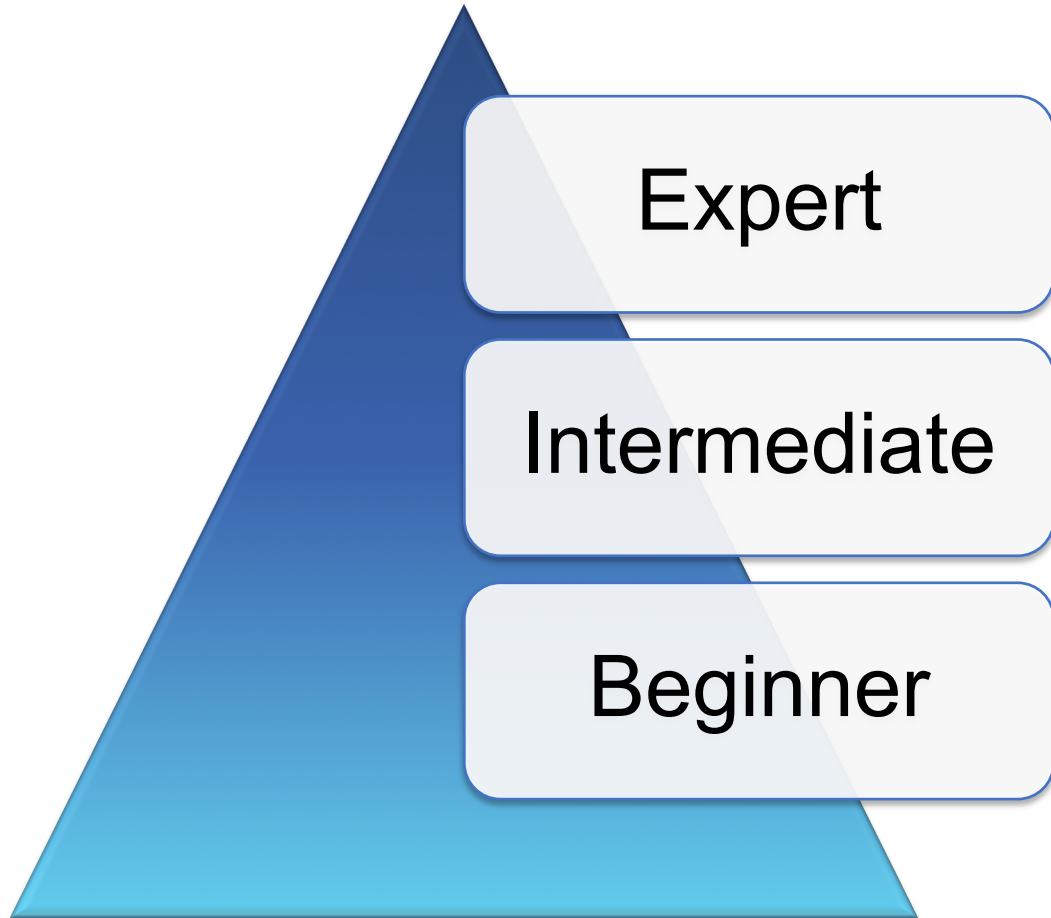
Threat Hunting

Cyber Threat Intelligence

On top of ever changing platforms, applications and infrastructures!



# Blue Team Skills Development



- You lead real-world investigations
  - You simulate real threats and attacker TTPs
  - You practice enterprise incident response, using realistic lab environments including enterprise tools such as SIEMs, EDRs, etc.
- 
- You set up your own labs and domain environments
  - You start attacking and investigating your lab
  - You investigate the attack patterns using forensic tools
  - You gain some real world experience e.g. as a SOC Analyst
- 
- You do a little bit of ethical hacking
  - You explore your first forensic artifacts
  - You read/watch some tutorials, books and follow along
  - You train up on foundational IT skills and practice some malware / network / system analysis

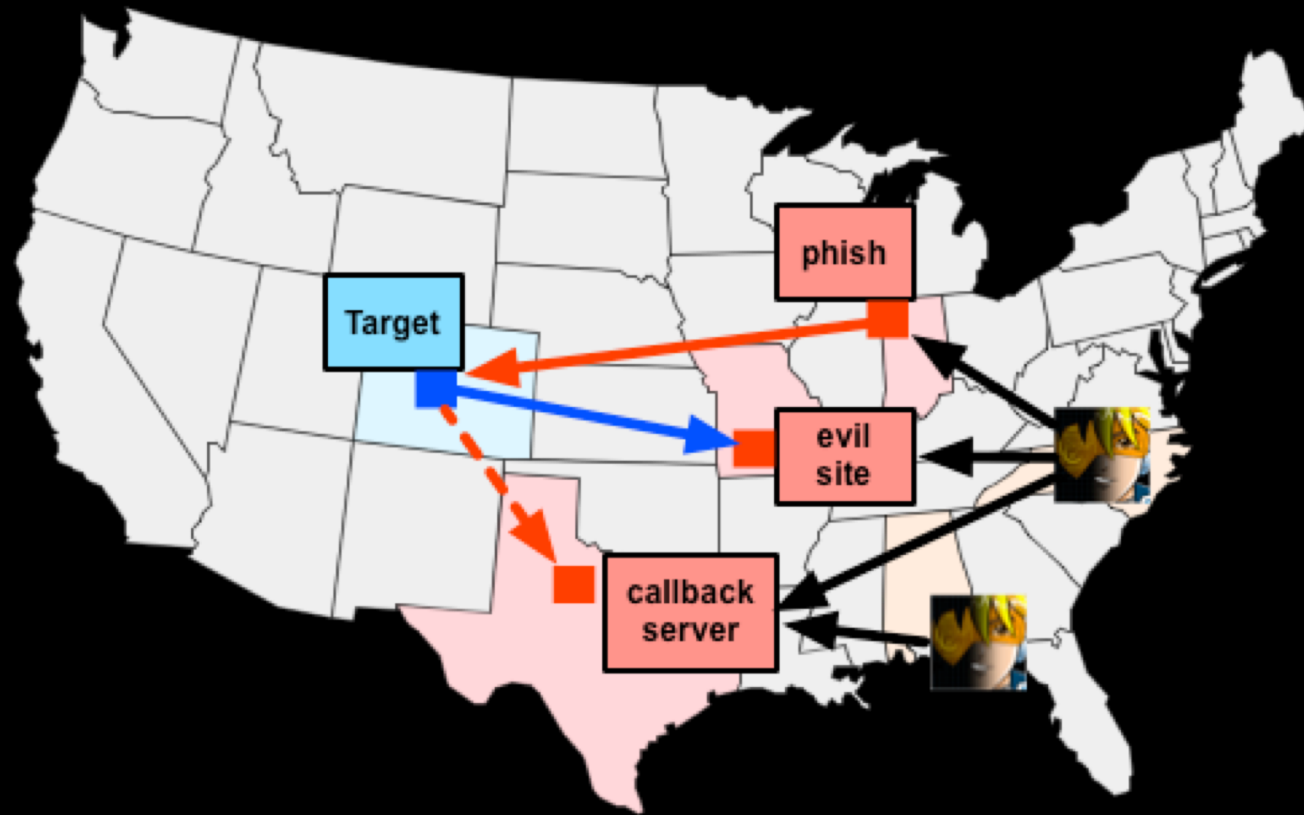


***Understanding  
Offense is Your  
Best Defense!***





# Think Like the Attacker: C2 Attack Infrastructure

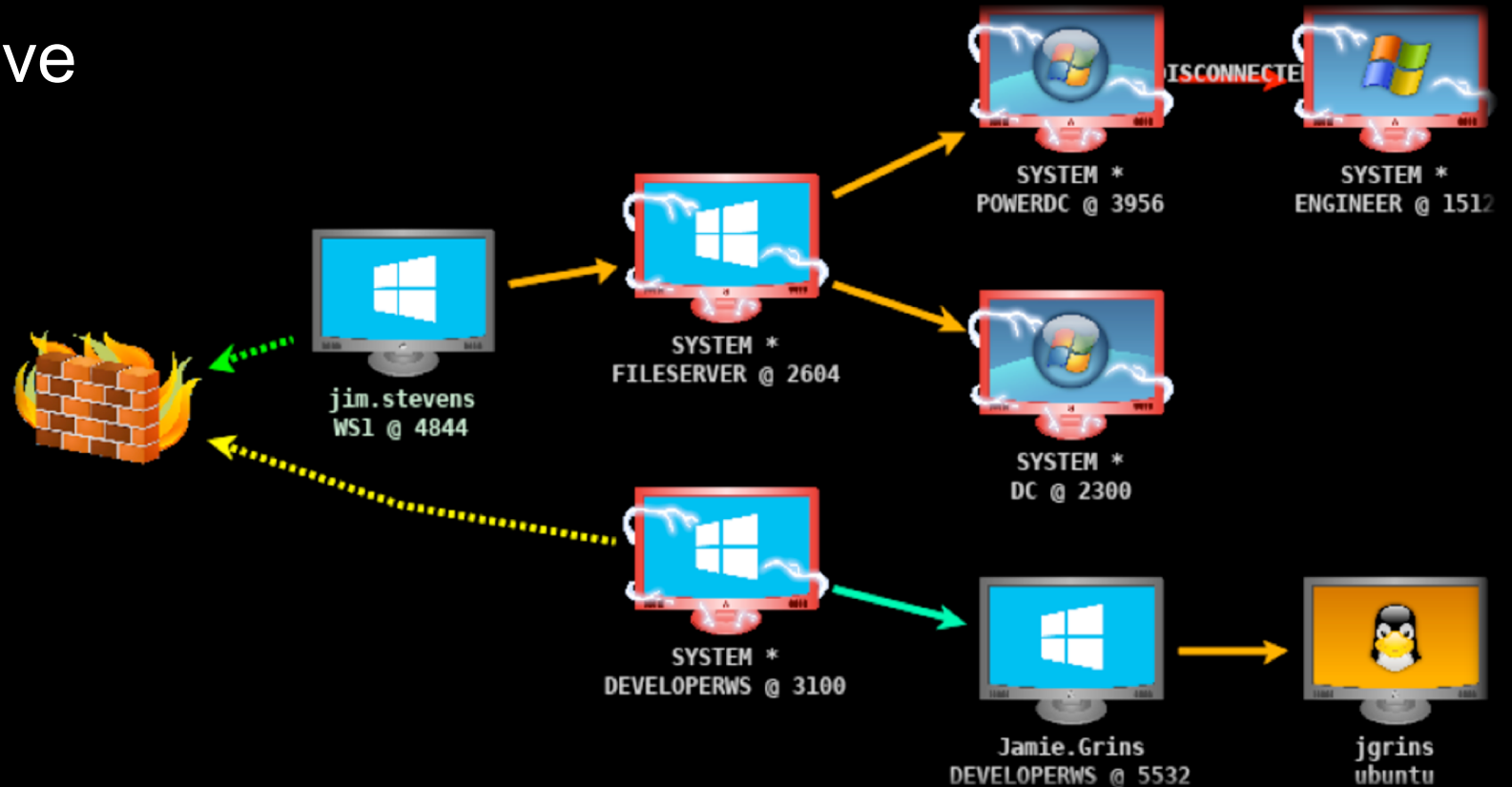


<https://www.cobaltstrike.com/blog/infrastructure-for-ongoing-red-team-operations/>



# Think Like the Attacker: Post-Exploitation

TTPs needed to achieve objectives?

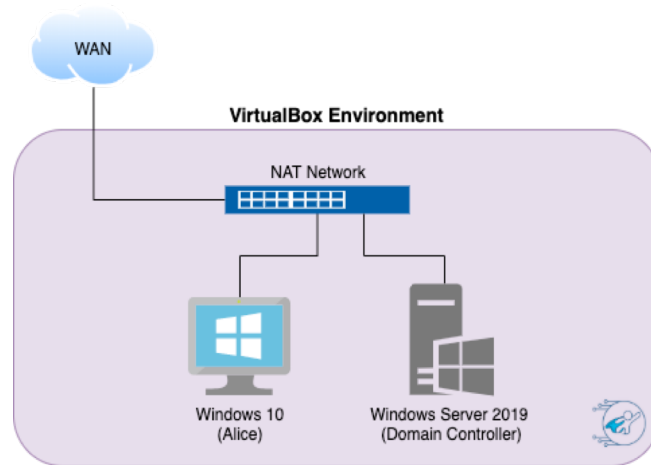


<https://www.mandiant.com/resources/blog/defining-cobalt-strike-components>

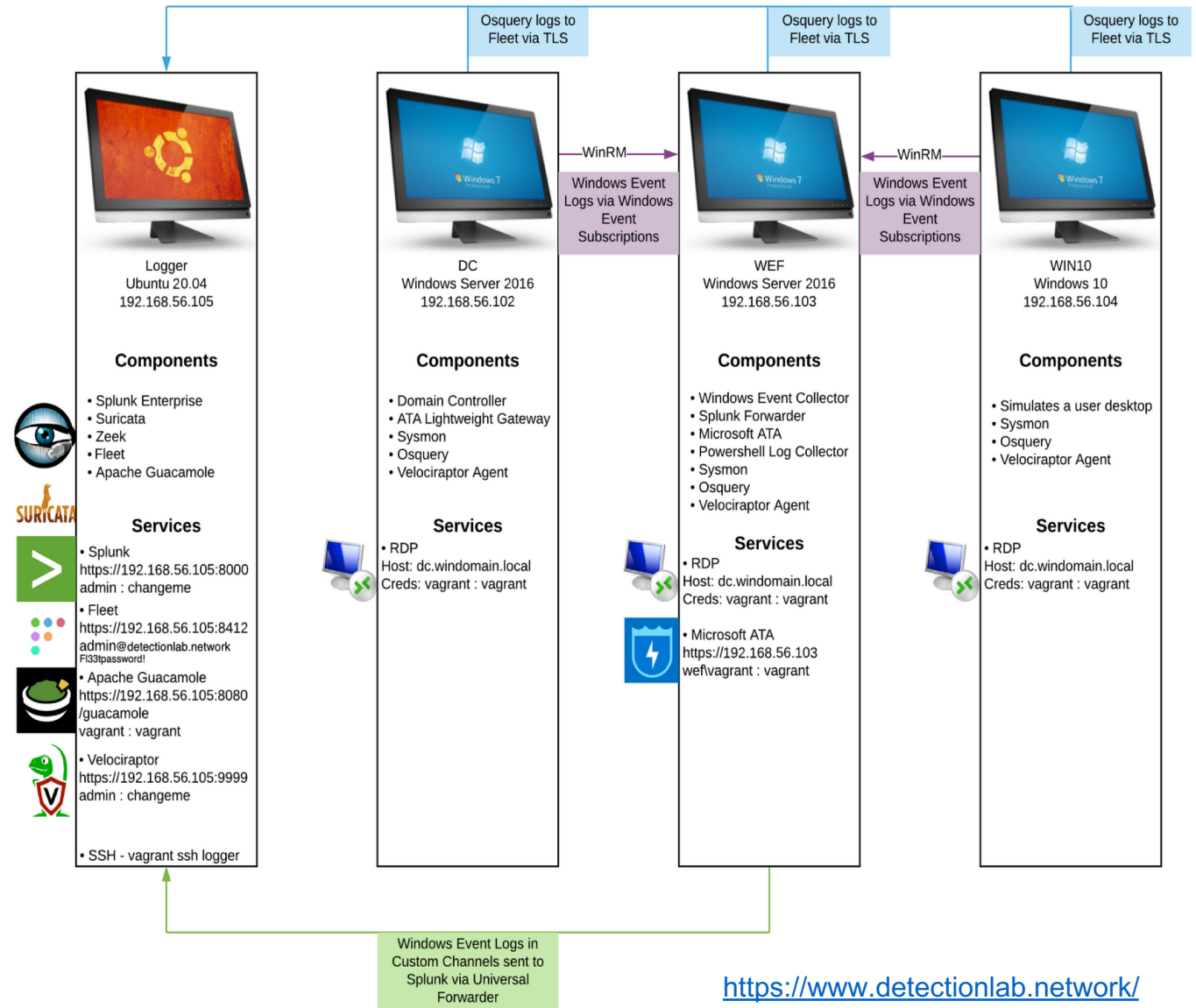


# Simple Lab Setup

Beginner => DIY 😊



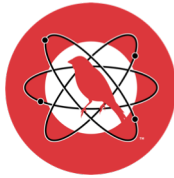
<https://bluecapesecurity.com/build-your-lab>



<https://www.detectionlab.network/>

# DIY: Attack & Investigate Scenario

## Simulating Attack Techniques



Atomic Red Team™ is a library of simple tests that every security team can execute to test their controls.

<https://atomicredteam.io/>

```
Select Administrator: Windows PowerShell

Starting ART attack simulation
=====
T1566.001 Atomic Test #1 - Download Macro-Enabled Phishing Attachment
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

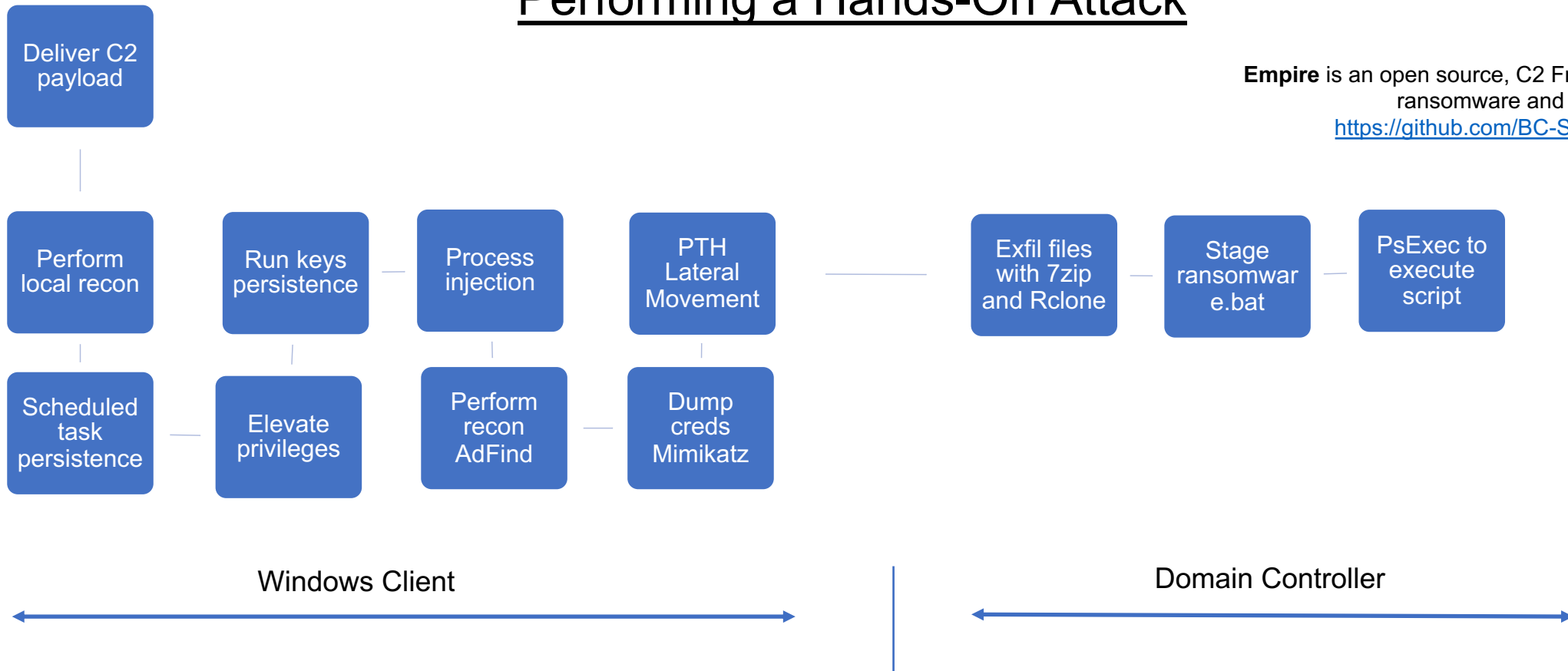
Executing test: T1566.001-1 Download Macro-Enabled Phishing Attachment
Done executing test: T1566.001-1 Download Macro-Enabled Phishing Attachment
T1078.003 Atomic Test #1 - Create local account with admin privileges
PathToAtomicsFolder = C:\AtomicRedTeam\atomics
```



# DIY: Attack & Investigate Scenario

## Performing a Hands-On Attack

Empire is an open source, C2 Framework used by ransomware and APT groups alike.  
<https://github.com/BC-SECURITY/Empire>





Q & A

