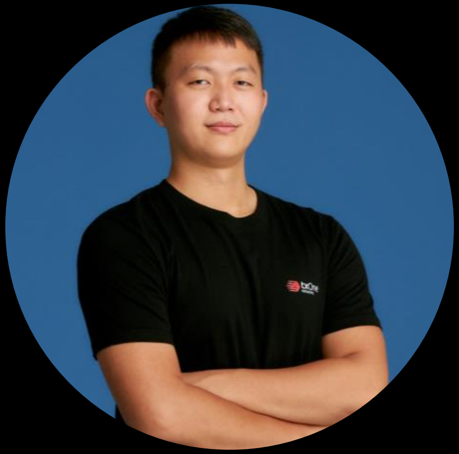
txOne networks *The Leader of OT Zero Trust*

The Endgame for the Ransomware in Critical Infrastructure!

Hank Chen, Mars Cheng

September 15, 2022

Hank Chen and Mars Cheng



Hank Chen

Threat Researcher, PSIRT and Threat Research at TXOne Networks

- Malware Analysis, Product Security and Vulnerability Research
- Teaching Assistant of Cryptography at Taiwan Tsing Hua University (NTHU) and CCoE
- Instructor of the Cyber Security training course for Taiwan Ministry of Defense
- Joined in many CTF competitions with 10sec and TSJ to focus on crypto, reverse, and pwn challenges
- Spoke at several cyber security conferences such as FIRST, BlackHat USA, HITCON, VXCON

Mars Cheng

Manager, PSIRT and Threat Research at TXOne Networks

- Executive Director, Association of Hackers in Taiwan (HIT)
- ICS/SCADA, IoT, Malware Analysis and Enterprise Security
- Spoke at Black Hat, RSA Conference, DEF CON, HITCON, FIRST, SecTor, HITB, SINCON, ICS Cyber Security Conference USA and Asia, CYBERSEC, InfoSec Taiwan and so on
- Instructor of HITCON Training 2022/2021/2020/2019,CCoE Taiwan, Ministry of Education, Ministry of National Defense, Ministry of Economic Affairs in Taiwan, and Listed companies
- General Coordinator of HITCON (Hacks In Taiwan Conference) PEACE 2022 and 2021

TXOne Networks Background

Founded in 2019, a company formed of a joint venture by Trend Micro and Moxa

Concentrated in OT/ICS all-terrain cybersecurity solutions by offering security inspection, endpoint protection, and network defense portfolios

Vertical leader in semiconductors, pharmaceuticals, and other critical infrastructures

Dedicated to OT/ICS threat research and cooperating with Trend Micro ZDI

Expand the perimeter by solution integration with security vendors and GSI

331 worldwide enterprises customers

TXONE NETWORKS
TOP
Enterprise Security
SOLUTION PROVIDERS IN APAC - 2020
SECURITY

GLOBAL INFOSEC AWARDS WINNER
CYBER DEFENSE MAGAZINE
2021

GLOBAL INFOSEC AWARDS WINNER
CYBER DEFENSE MAGAZINE
2022

SC 2022 awards EUROPE
WINNER

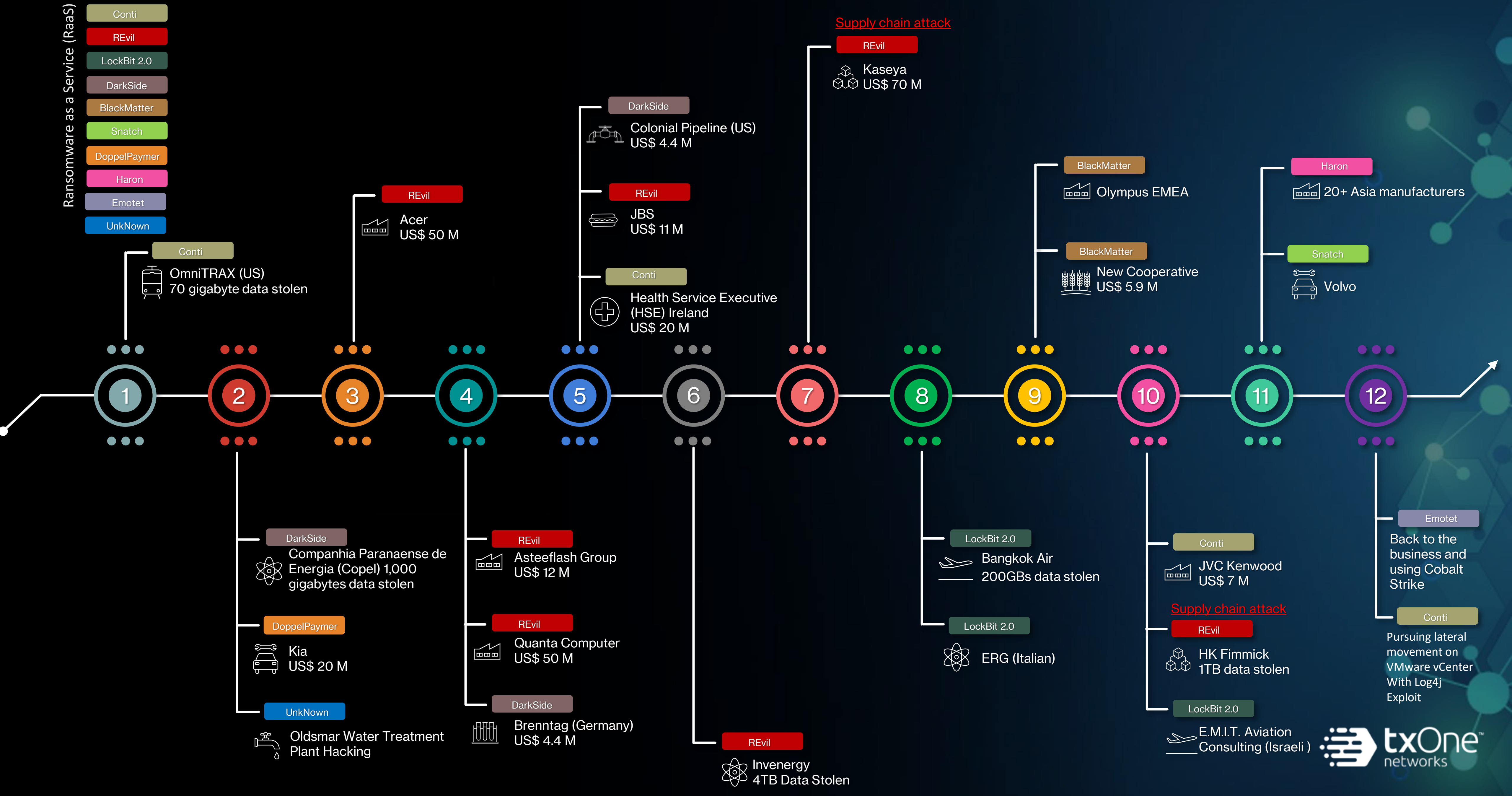
txOne networks

Outline

- Threats in Review
- What are the Characteristics of Ransomware that Affects Critical Infrastructure?
- How can Critical Infrastructure Mitigate the Threat of Ransomware?
- Closing Remarks

Threats in Review

2021 Attack Incidents in Critical Infrastructure



Cyber Criminal Groups

Ransomware as a Service (RaaS)

- Conti
- REvil
- LockBit 2.0
- DarkSide
- BlackMatter
- Snatch
- DoppelPaymer
- Haron
- Emotet
- UnkNown

1

Conti
OmniTRAX (US)
70 gigabyte data stolen

2

DarkSide
Companhia Paranaense de Energia (Copel) 1,000 gigabytes data stolen

DoppelPaymer
Kia
US$ 20 M

UnkNown
Oldsmar Water Treatment Plant Hacking

3

REvil
Acer
US$ 50 M

4

REvil
Asteeflash Group
US$ 12 M

REvil
Quanta Computer
US$ 50 M

DarkSide
Brenntag (Germany)
US$ 4.4 M

5

DarkSide
Colonial Pipeline (US)
US$ 4.4 M

REvil
JBS
US$ 11 M

Conti
Health Service Executive (HSE) Ireland
US$ 20 M

6

REvil
Invenergy
4TB Data Stolen

7

Supply chain attack
REvil
Kaseya
US$ 70 M

8

LockBit 2.0
Bangkok Air
200GBs data stolen

LockBit 2.0
ERG (Italian)

9

BlackMatter
Olympus EMEA

BlackMatter
New Cooperative
US$ 5.9 M

10

Conti
JVC Kenwood
US$ 7 M

Supply chain attack
REvil
HK Fimmick
1TB data stolen

LockBit 2.0
E.M.I.T. Aviation Consulting (Israeli)

11

Haron
20+ Asia manufacturers

Snatch
Volvo

12

Emotet
Back to the business and using Cobalt Strike

Conti
Pursuing lateral movement on VMware vCenter With Log4j Exploit

txOne networks

The Key Observations from Attack Incidents in 2021

Most active criminal groups in 2021

- Conti, Maze, Lockbit, REvil and DarkSide

Targeting the Critical Infrastructure and leverage supply chain attack

- Colonial Pipeline attack in May by DarkSide
- Kaseya supply chain attack by REvil

Running the RaaS business model with the affiliate programs

- Ransom demand less than 500k charge for 25%
- Ransom demand over 5M charge for 10%

Executive Order issued by U.S. President Joe Biden

- Improving the nation’s cybersecurity
- Supply Chain and Software Bills of Materials (SBOMs)

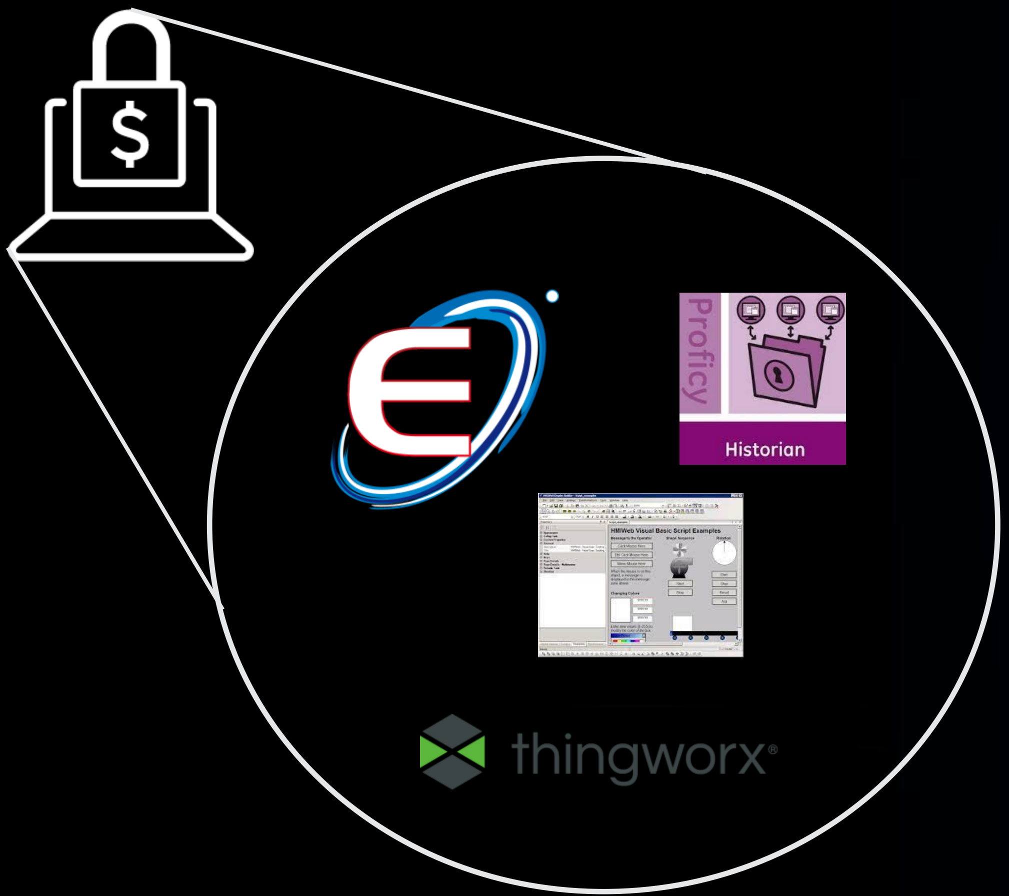
Leverage zero-day vulnerabilities

- CVE-2021-30116, Kaseya VSA vulnerability
- CVE-2021-44228, Log4J vulnerability

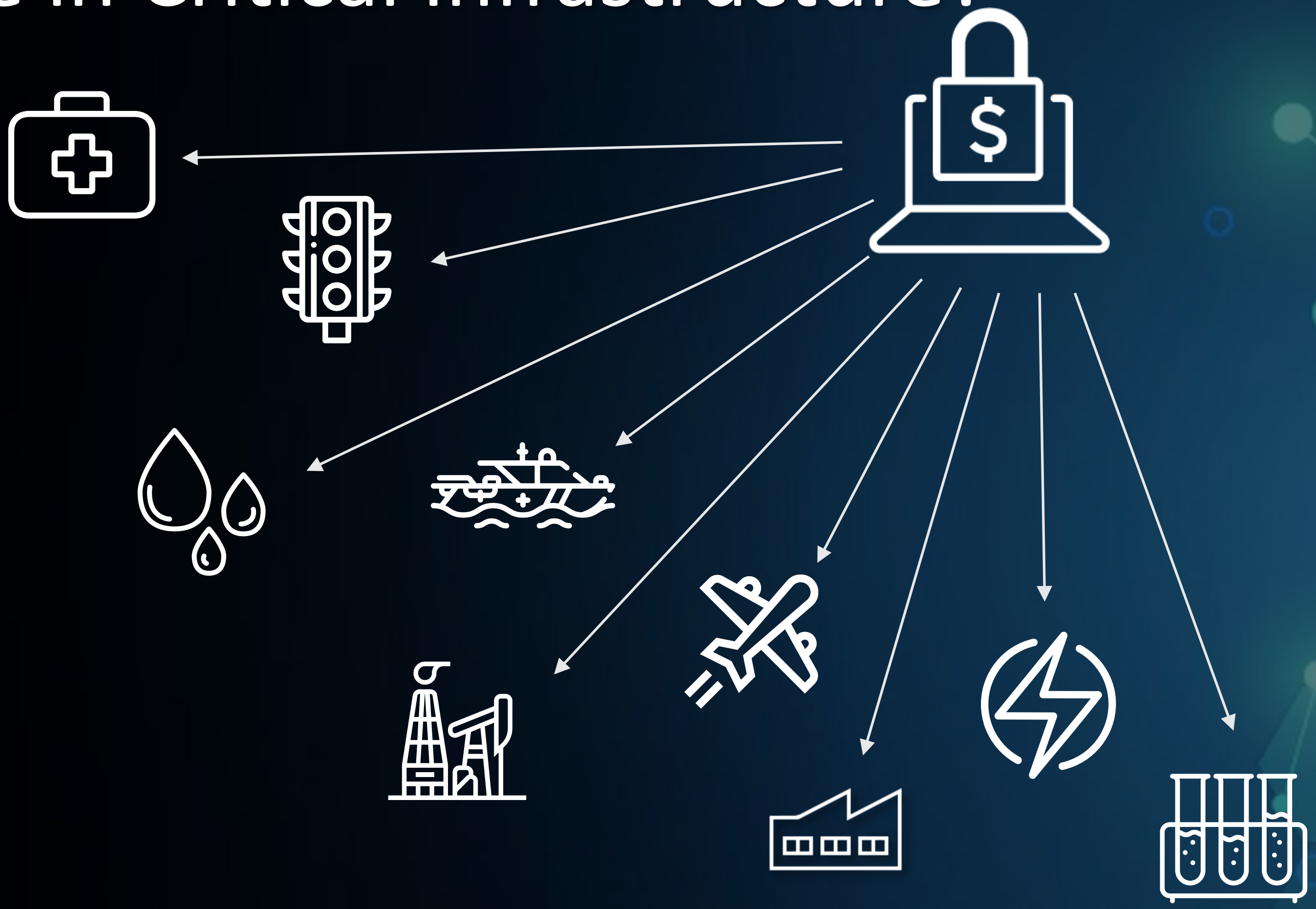
Threat Overview
Recent Attack Trends – Many Ransomware Family

Ransomware Family	2021 Q2	2021 Q3	2021 Q4	2022 Q1	From 2021 Q4 to 2022 Q1
WannaCry	62.38%	46.95%	46.73%	42.23%	↘
Cryptor	4.06%	17.72%	15.91%	13.79%	↘
Locker	10.44%	10.92%	10.57%	13.43%	↗
LockBit	2.10%	4.35%	5.32%	5.89%	↗
Conti	3.49%	3.09%	3.98%	4.34%	↗
Gandcrab	5.03%	5.21%	3.93%	4.19%	↗
Locky	5.59%	3.28%	3.32%	3.69%	↗
Cobra	2.61%	2.83%	2.73%	3.33%	↗
Hive	0.59%	0.79%	1.82%	2.56%	↗
MAZE	1.00%	1.27%	1.69%	2.07%	↗

What Are Ransomware in Critical Infrastructure?



Targeted specific resources in critical infrastructure such as applications and certificates



The ransomware impacted the Critical Infrastructure before

What are the Characteristics of Ransomware that Affects Critical Infrastructure?

The Ransomware Matrix

	WannaCry	Ryuk	Lockergoga	EKANS	RagnarLocker	ColdLock	Egregor	Conti v2
Language Check	No	No	No	No	Yes	No	Yes	No
Kill Process/Services	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Persistence	Yes	Yes	No	No	No	No	No	Yes
Privilege Escalation	Yes	Yes	No	No	Yes	No	No	No
Lateral Movement	Yes	No	No	No	No	No	No	No
Anti-Recovery	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
Atomic-Check	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
File Encryption	R-M-W	R-W-M	M-R-W	R-W-M	R-W-M	R-W-M	R-W-M	R-W-M
Partial Encryption	No	Yes	No	N/A	No	Yes	Yes	Yes
Cipher Suite	AES-128-CBC RSA-2048	AES-256 RSA-2048	AES-128-CTR RSA-1024	AES-256-CTR RSA-2048	Salsa20 RSA-2048	AES-256-CBC RSA	ChaCha8 RSA-2048	ChaCha8 RSA-4096
Configuration File	Yes	No	No	Yes	Yes	No	Yes	No
Command-Line Arguments	Yes	No	Yes	No	Yes	No	Yes	Yes

Claim:
The matrix is only based on the samples we had analyzed. They might add more features in their variants.

File Encryption:
SF: SetFileInformationByHandle/NtSetInformationFile;
R: ReadFile ; W: WriteFile ; M: MoveFile;
MP: MapViewOfFile, FF: FlushViewOfFile

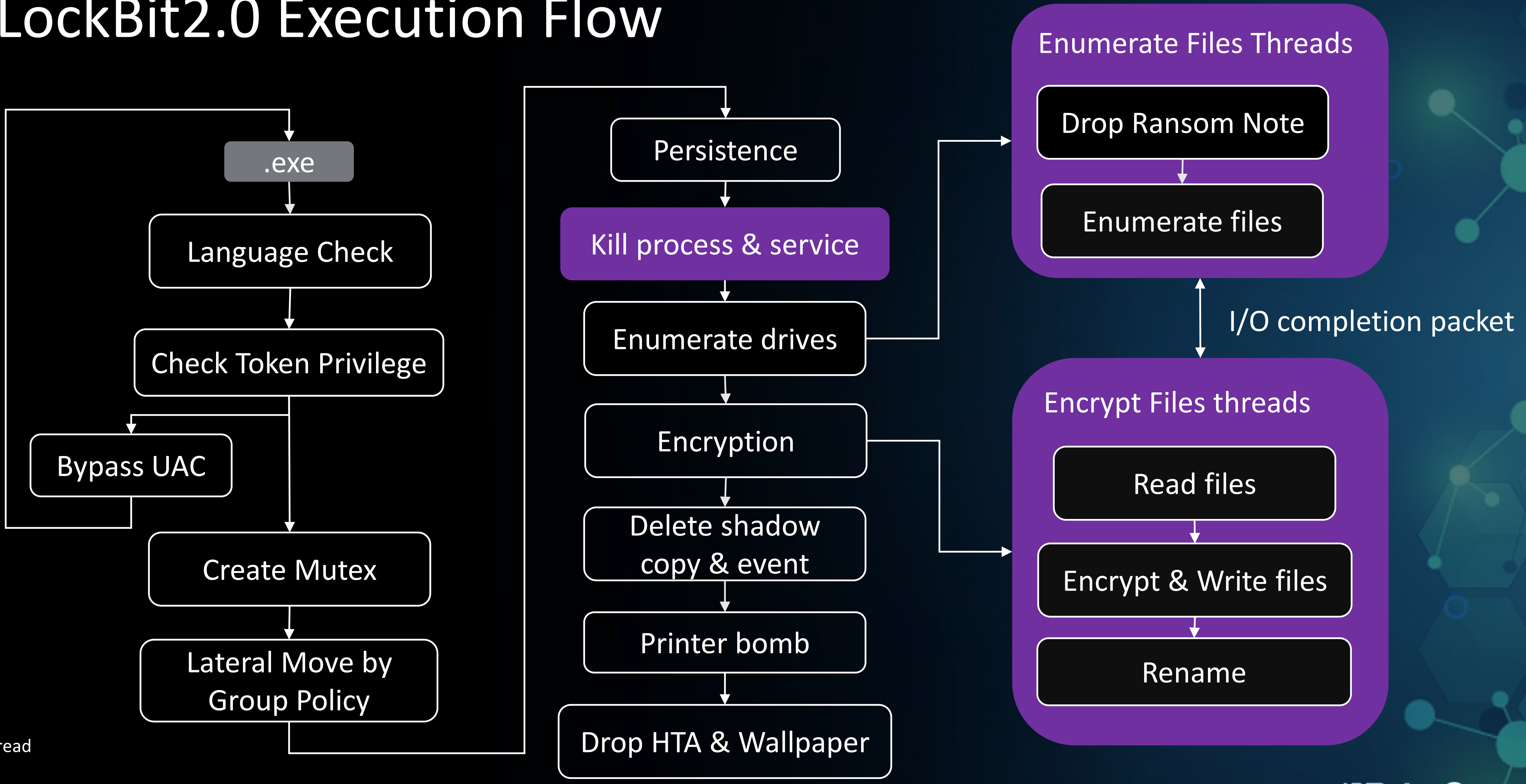
The Ransomware Matrix

	Bad Rabbit	Mount Locker	RansomExx	DoppelPaymer	Darkside	Babuk	REvil	LockBit 2.0
Language Check	No	No	No	No	Yes	No	Yes	Yes
Kill Process/Services	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Persistence	Yes	No	No	Yes	No	No	Yes	Yes
Privilege Escalation	Yes	No	No	Yes	No	No	Yes	Yes
Lateral Movement	Yes	Yes	No	No	No	No	No	Yes
Anti-Recovery	No	No	Yes	Yes	Yes	Yes	Yes	Yes
Atomic-Check	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
File Encryption	MP-FF	R-W-SF	R-W-M	R-W-M	M-R-W	M-R-W	R-W-M	R-W-SF
Partial Encryption	Yes	Yes	No	No	Yes	Yes	Yes	Yes
Cipher Suite	AES-128-CBC RSA-2048	ChaCha20 RSA-2048	AES-256-ECB RSA-4096	AES-256-CBC RSA-2048	Salsa20 RSA-1024	HC256 Curve25519-ECDH	Salsa20 Curve25519-ECDH	AES-128-CBC Curve25519-ECDH
Configuration File	No	No	No	No	Yes	No	Yes	No
Command-Line Arguments	Yes	Yes	No	No	Yes	Yes	Yes	Yes

Claim:
The matrix is only based on the samples we had analyzed. They might add more features in their variants.

File Encryption:
SF: SetFileInformationByHandle/NtSetInformationFile;
R: ReadFile ; W: WriteFile ; M: MoveFile;
MP: MapViewOfFile, FF: FlushViewOfFile

LockBit2.0 Execution Flow



.exe

Language Check

Check Token Privilege

Bypass UAC

Create Mutex

Lateral Move by Group Policy

Persistence

Kill process & service

Enumerate drives

Encryption

Delete shadow copy & event

Printer bomb

Drop HTA & Wallpaper

Enumerate Files Threads

Drop Ransom Note

Enumerate files

I/O completion packet

Encrypt Files threads

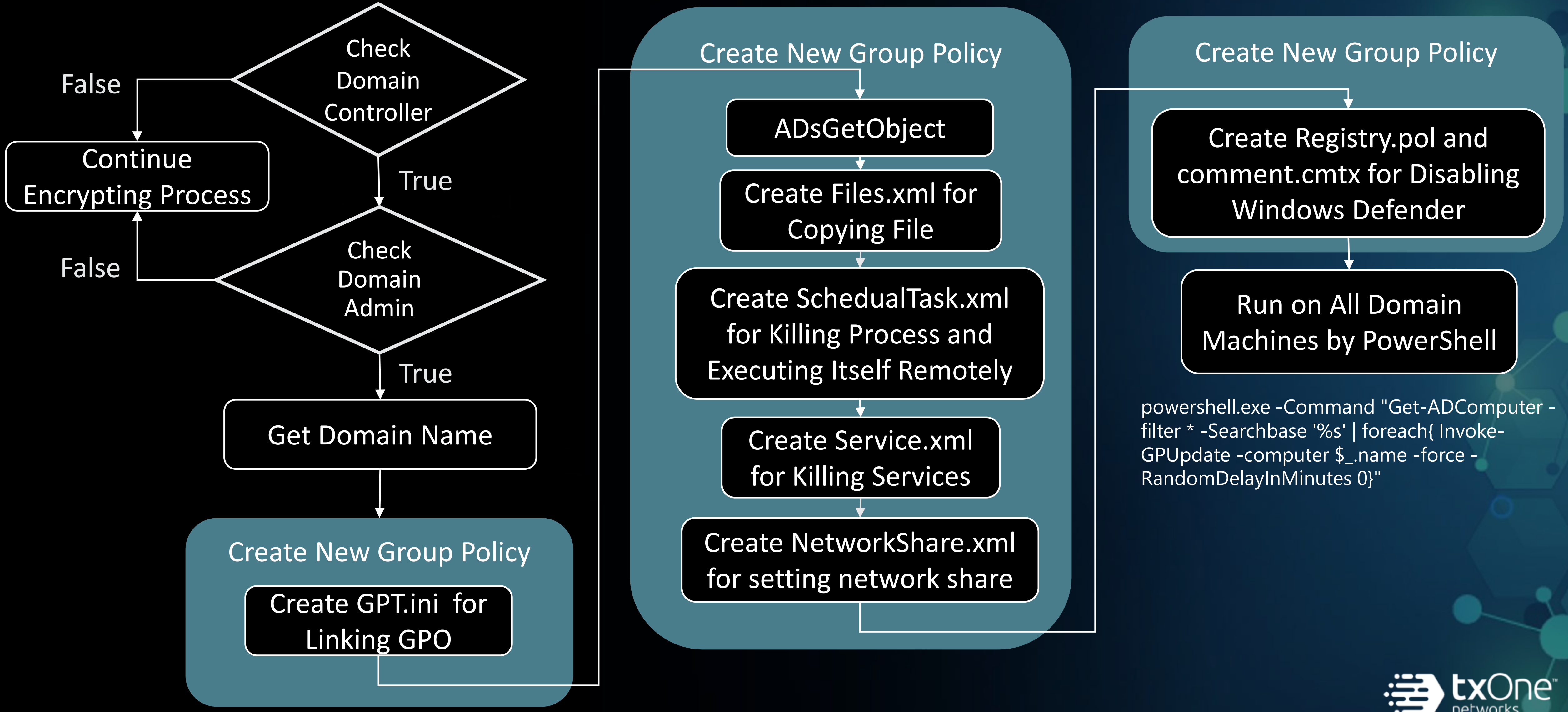
Read files

Encrypt & Write files

Rename

🟪 : new thread
▨ : in disk
🟧 : in memory
🟦 : in zip

AD Group Policy Propagation Techniques in LockBit 2.0



Check Domain Controller

False

Continue Encrypting Process

True

Check Domain Admin

False

True

Get Domain Name

Create New Group Policy

Create GPT.ini for Linking GPO

Create New Group Policy

ADsGetObject

Create Files.xml for Copying File

Create SchedualTask.xml for Killing Process and Executing Itself Remotely

Create Service.xml for Killing Services

Create NetworkShare.xml for setting network share

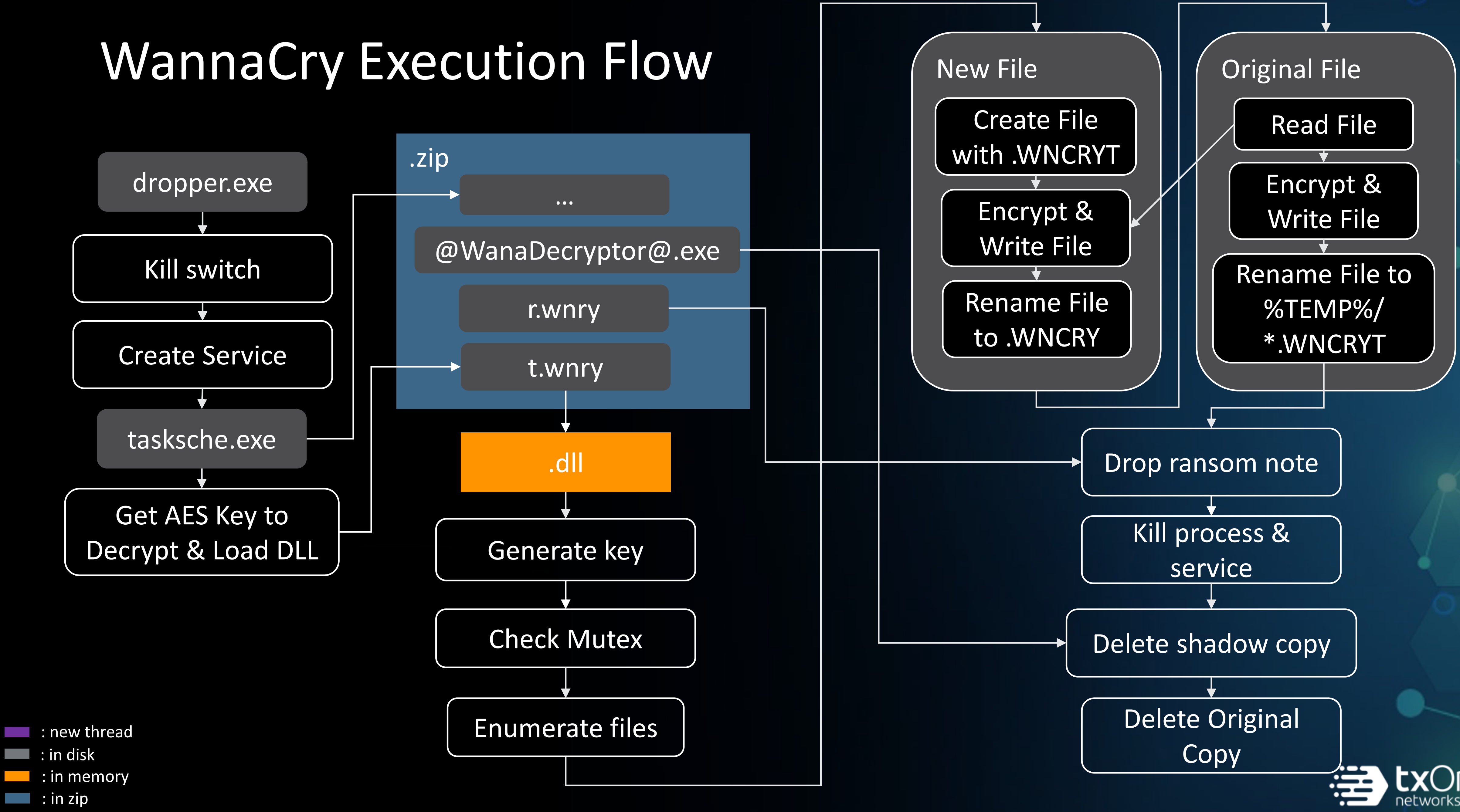
Create New Group Policy

Create Registry.pol and comment.cmtx for Disabling Windows Defender

Run on All Domain Machines by PowerShell

```
powershell.exe -Command "Get-ADComputer -filter * -Searchbase '%s' | foreach{ Invoke-GPUpdate -computer $_.name -force -RandomDelayInMinutes 0}"
```

WannaCry Execution Flow



dropper.exe

Kill switch

Create Service

tasksche.exe

Get AES Key to Decrypt & Load DLL

.zip

…

@WanaDecryptor@.exe

r.wnry

t.wnry

.dll

Generate key

Check Mutex

Enumerate files

New File

Create File with .WNCRYT

Encrypt & Write File

Rename File to .WNCRY

Original File

Read File

Encrypt & Write File

Rename File to %TEMP%/ *.WNCRYT

Drop ransom note

Kill process & service

Delete shadow copy

Delete Original Copy

🟪 : new thread

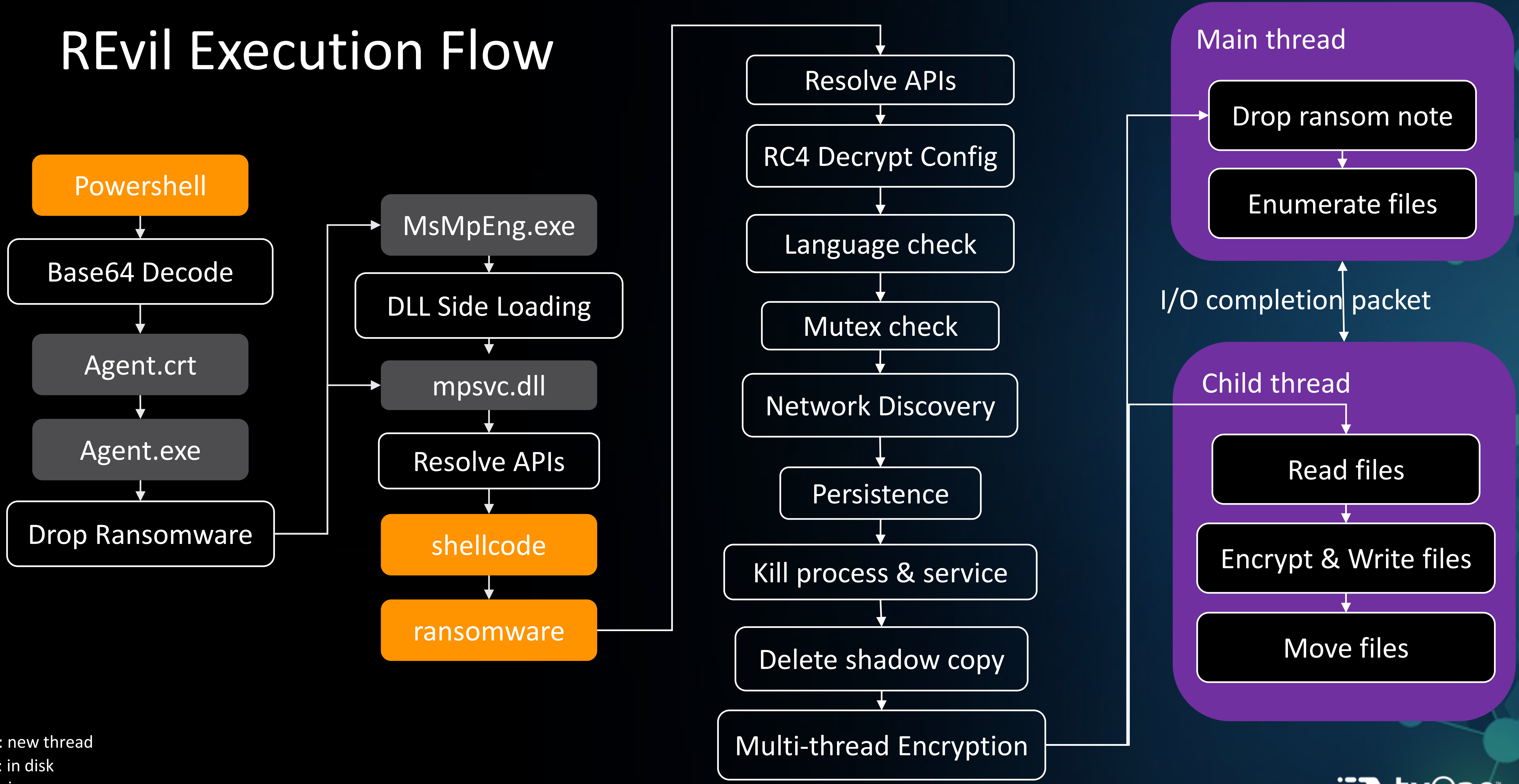
◼ : in disk

🟧 : in memory

🟦 : in zip

txOne networks

REvil Execution Flow



Powershell

Base64 Decode

Agent.crt

Agent.exe

Drop Ransomware

MsMpEng.exe

DLL Side Loading

mpsvc.dll

Resolve APIs

shellcode

ransomware

Resolve APIs

RC4 Decrypt Config

Language check

Mutex check

Network Discovery

Persistence

Kill process & service

Delete shadow copy

Multi-thread Encryption

Main thread

Drop ransom note

Enumerate files

I/O completion packet

Child thread

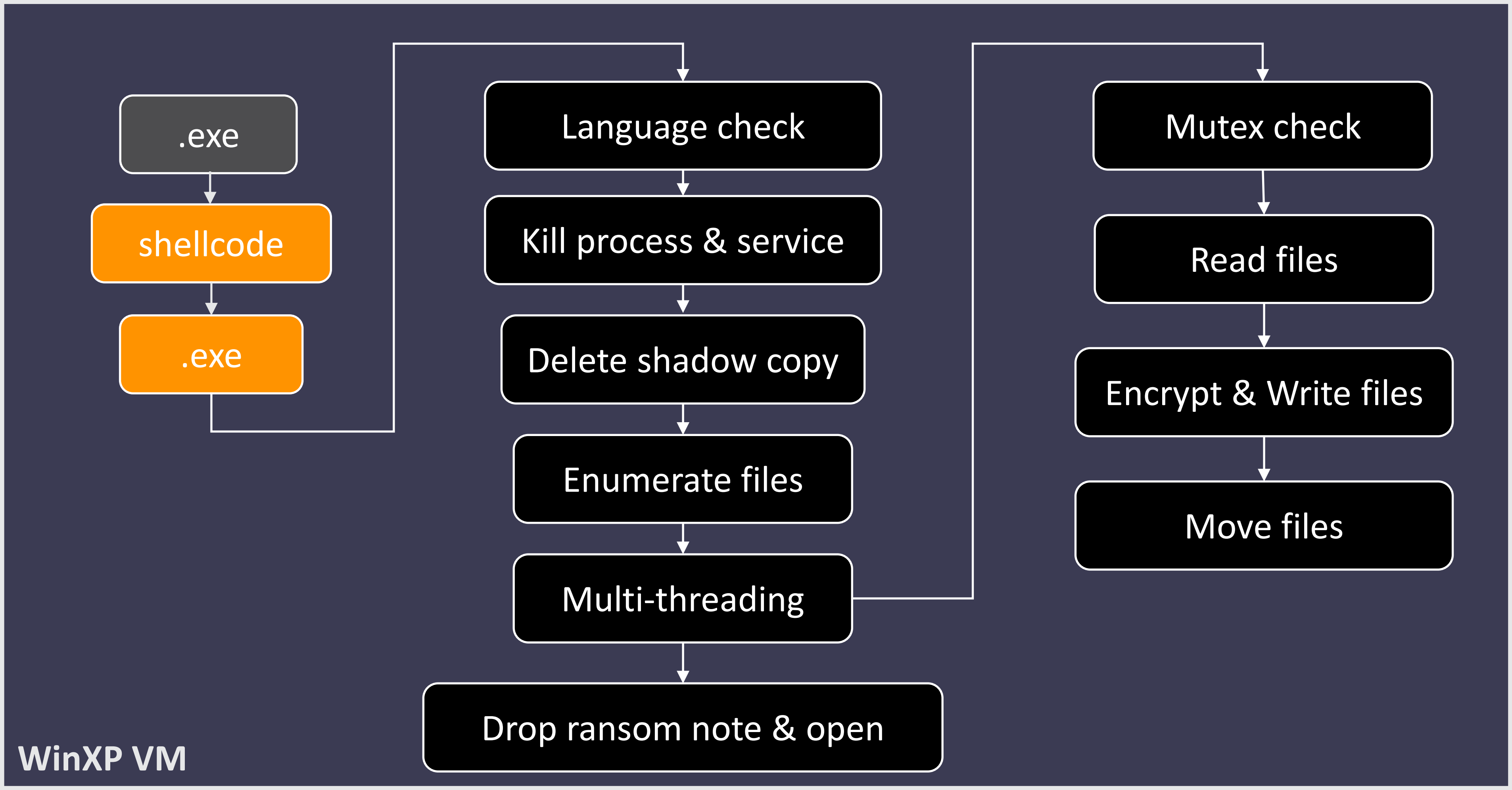
Read files

Encrypt & Write files

Move files

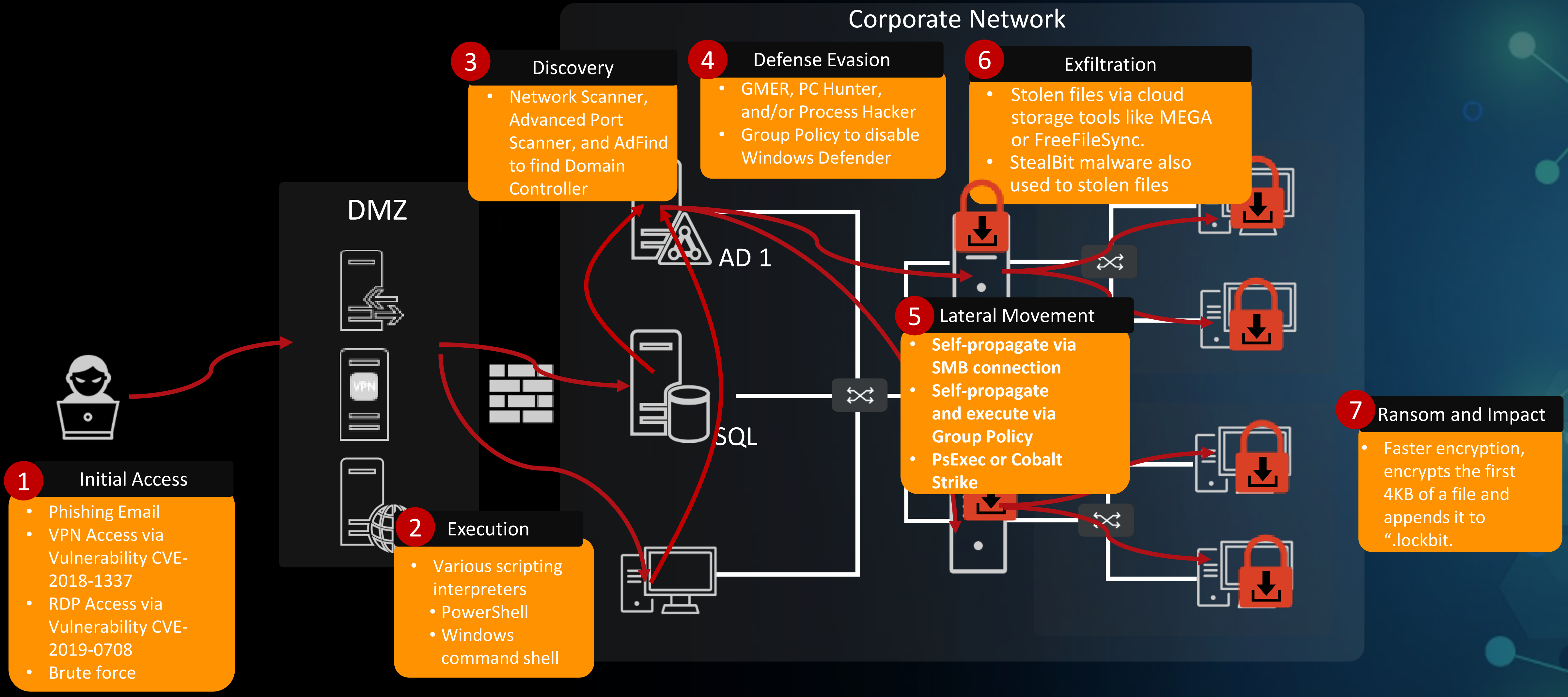
🟪 : new thread
◼ : in disk
🟧 : in memory
🟦 : in zip

RagnarLocker Execution Flow



🟪 : new thread
⬛ : in disk
🟧 : in memory
🟦 : in zip

Common Attack Path of Ransomware in Critical Infrastructure



1 Initial Access

- Phishing Email
- VPN Access via Vulnerability CVE-2018-1337
- RDP Access via Vulnerability CVE-2019-0708
- Brute force

2 Execution

- Various scripting interpreters
  - PowerShell
  - Windows command shell

3 Discovery

- Network Scanner, Advanced Port Scanner, and AdFind to find Domain Controller

4 Defense Evasion

- GMER, PC Hunter, and/or Process Hacker
- Group Policy to disable Windows Defender

5 Lateral Movement

- **Self-propagate via SMB connection**
- **Self-propagate and execute via Group Policy**
- **PsExec or Cobalt Strike**

6 Exfiltration

- Stolen files via cloud storage tools like MEGA or FreeFileSync.
- StealBit malware also used to stolen files

7 Ransom and Impact

- Faster encryption, encrypts the first 4KB of a file and appends it to ".lockbit.

Common Characteristics of Ransomware in Critical Infrastructure

1. Atomic-Check (16)
2. Kill Process/Services (14)
3. Anti-Recovery (13)
4. Command-Line Arguments (11)
5. Partial Encryption (10)
6. Privilege Escalation (7)
7. Persistence (7)
8. Language Check (5)

How can Critical Infrastructure Mitigate the Threat of Ransomware?

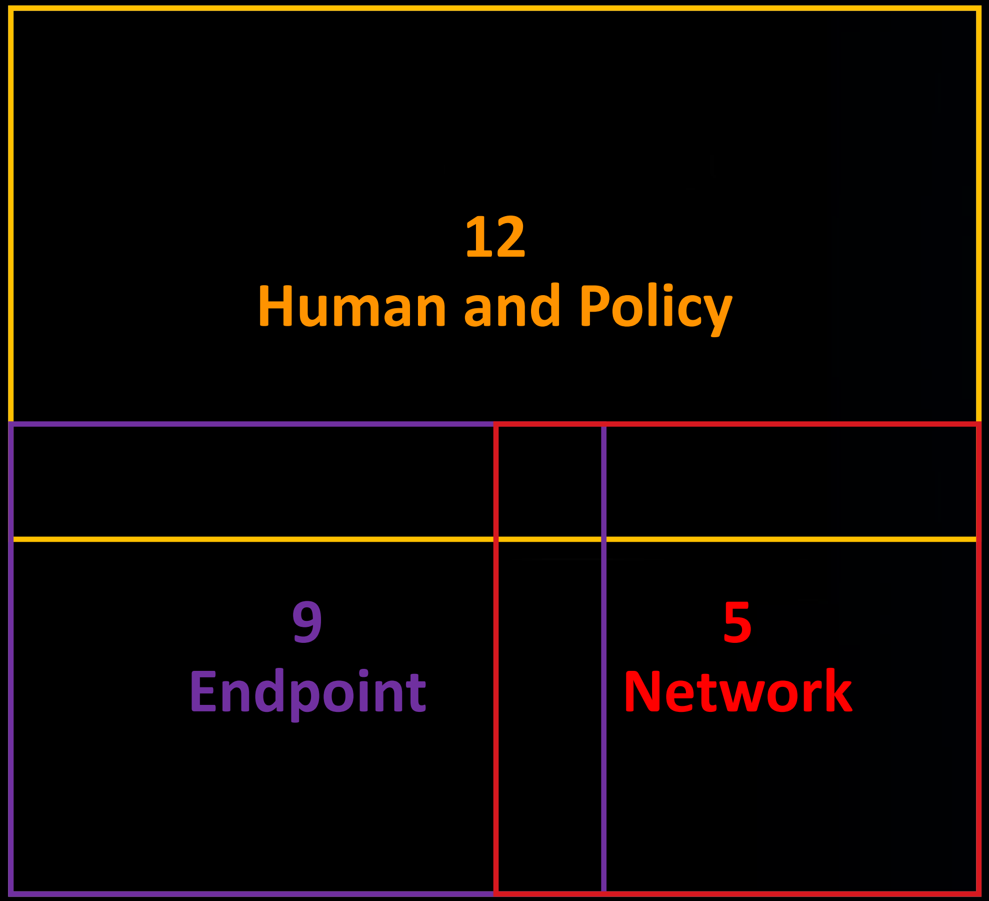
Ransomware Techniques Based on MITRE ATT&CK for ICS

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Drive-by Compromise	Change Operating Mode	Modify Program	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Command-Line Interface	Module Firmware	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Execution through API	Project File Infection		Indicator Removal on Host	Remote System Discovery	Lateral Tool Transfer	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Graphical User Interface	System Firmware		Masquerading	Remote System Information Discovery	Program Download	I/O Image		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Hooking	Valid Accounts		Rootkit	Wireless Sniffing	Remote Services	Man in the Middle		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Modify Controller Tasking			Spoof Reporting Message		Valid Accounts	Monitor Process State		Data Destruction		Loss of Productivity and Revenue
Replication Through Removable Media	Native API						Point & Tag Identification		Denial of Service		Loss of Protection
Rogue Master	Scripting						Program Upload		Device Restart/Shutdown		Loss of Safety
Spearphishing Attachment	User Execution						Screen Capture		Manipulate I/O Image		Loss of View
Supply Chain Compromise							Wireless Sniffing		Modify Alarm Settings		Manipulation of Control
Transient Cyber Asset									Rootkit		Manipulation of View
Wireless Compromise									Service Stop		Theft of Operational Information
									System Firmware		

12 Tactics
78 Techniques

Application of Mitigations

24 mitigations



- Network Segmentation (Network)(4)
- Application Isolation and Sandboxing (Endpoint)(3)
- Network Intrusion Prevention (Network)(3)
- Exploit Protection (Network, Endpoint)(2)
- Restrict Web-Based Content (Endpoint)(2)
- Update Software(Endpoint, Human and Policy)(2)
- Disable or Remove Feature or Program (Endpoint)(2)
- Network Allowlists (Human and Policy)(2)
- Execution Prevention (Endpoint)(2)
- Code Signing (Endpoint)(2)
- Restrict File and Directory Permissions (Human and Policy)(2)
- Restrict Registry Permissions (Human and Policy)(2)
- Privileged Account Management (Human and Policy)
- Vulnerability Scanning(Network, Endpoint)
- Threat Intelligence Program
- Authorization Enforcement (Human and Policy)
- Human User Authentication (Human and Policy)
- Access Management (Human and Policy)
- Software Process and Device Authentication (Human and Policy)
- Password Policies (Human and Policy)
- Filter Network Traffic (Network)
- Antivirus/Antimalware (Endpoint)
- User Training (Human and Policy)
- User Account Management (Human and Policy)

Practical Ransomware Mitigation Strategies in Critical Infrastructure

The Difference between IT and OT

Type	OT Environment	IT Environment
Virus Pattern Update	**Hard**	Usually up to date
The Variability of the Operating Environment	**Low**	High
The Burden of Ransomware Encryption on the System	**High** and may cause operation shutdown	Low to Middle

Malware Detection Methods

Type	Scope
Signature-based	Byte sequence, List of DLL, Assembly Instruction
Behavior-based	API Calls, System calls, CFG, Instruction trace, n-gram, Sandbox
Heuristic-based	API Calls, System call, CFG, Instruction trace, List of DLL, Hybrid featues, n-gram
Cloud-based	Strings, System calls, Hybrid featues, n-gram
Learning-based	API Calls, System call, Hybrid featues
…	

Limitations of Malware Detection

Type	Limitations
Signature-based	Need huge database, Hard to defeat obfuscated samples, Vendor need to spend many people to update the signature
Behavior-based	Need to Run it, have the risk of attacking by 0-day exploits or vulnerabilities. Time-consuming and labor-intensive. Behavior policy can be bypassed
Heuristic-based	will include both of the above
Cloud-based	Immediacy of Internet connections. Adds additional delay to many tasks. Less effective at monitoring/detecting Heuristics
Learning-based	Learning dataset can’t help to identify the variant
…	

txOne networks

Limitations of Malware Detection

- Analysis is time-consuming and labor-intensive
- Vendor need to constantly update the latest malware signature
- Capabilities of identifying new variants is low
- Obfuscated samples are hard to defeat

Deep Dive into Our Symbolic Engine - TCSA

- TCSA (TXOne Code Semantics Analyzer)
  - Malware detection with instruction-level Semantic automata
  - Use Vivisect as the core decompiler engine
    - Support AMD, ARM, x86, MSP430, H8 and many other architectures
    - Support analysis of program files for Windows and Linux systems
  - Pure Python based Engine: Works on any platform able to run Python
  - In TCSA rule, developers can notate the data references between API calls
    - Symbolized return values of Win32 API, function, or unknown API
    - Usage of memory heap, stack, local variables, etc.
    - DefUse: tracing the source of data, memory values, argument values from
  - Support two additional feature extraction systems: YARA and Capa subsystems
  - Developers Orienting Malware Scanning Design
    - Developers can write their own Rules to be installed in the TCSA engine as callbacks
    - The TCSA engine will traverse and explore each function and the instructions in its Code Block
    - In the Callback, each instruction, memory, function name and parameter can be analyzed line by line

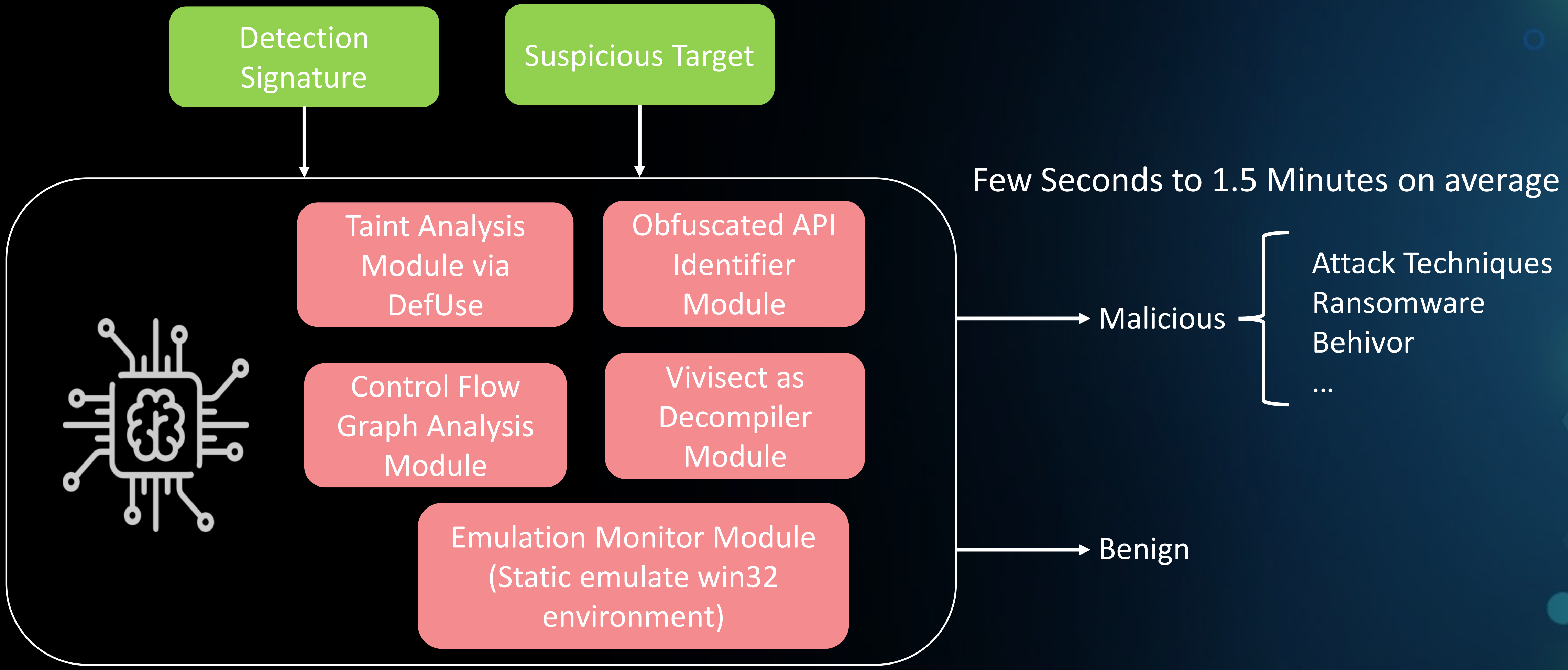
Practical Ransomware Mitigation Strategies in Critical Infrastructure

- IT Environment: **TCSA** + Other Mitigation Strategies
- OT Environment: Multilayer Mitigation Strategies

Related Work

- Three main papers which inspired our research
  - Christodorescu, Mihai, et al. "Semantics-aware malware detection." 2005 IEEE symposium on security and privacy (S&P'05). IEEE, 2005.
  - Kotov, Vadim, and Michael Wojnowicz. "Towards generic deobfuscation of windows API calls." arXiv preprint arXiv:1802.04466 (2018).
  - Ding, Steven HH, Benjamin CM Fung, and Philippe Charland. "Asm2vec: Boosting static representation robustness for binary clone search against code obfuscation and compiler optimization." 2019 IEEE Symposium on Security and Privacy (SP). IEEE, 2019.
- Thanks for their contributions

Deep Dive into Our Symbolic Engine - TCSA



Detection Signature

Suspicious Target

Taint Analysis Module via DefUse

Obfuscated API Identifier Module

Control Flow Graph Analysis Module

Vivisect as Decompiler Module

Emulation Monitor Module (Static emulate win32 environment)

Few Seconds to 1.5 Minutes on average

Malicious

- Attack Techniques
- Ransomware
- Behivor
- …

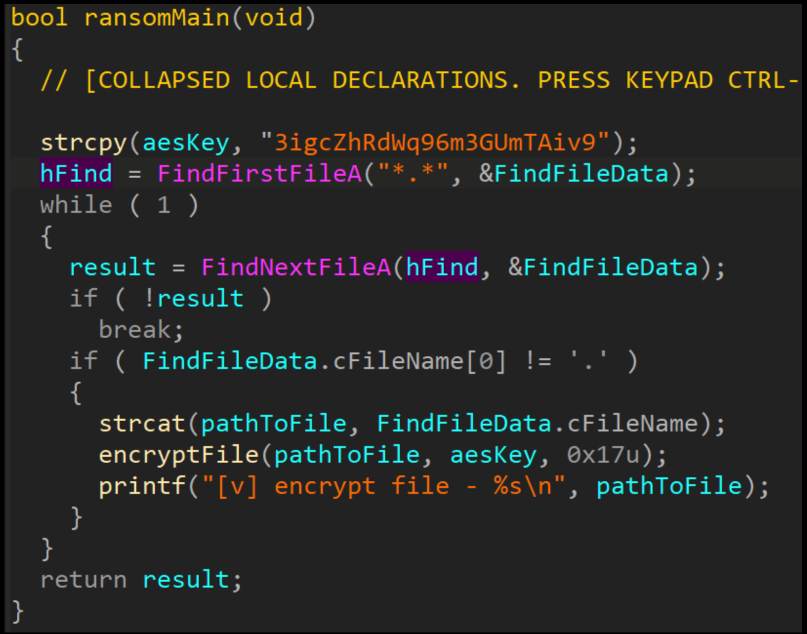
Benign

Real World Ransomware Detection (Cont.)

- Basically, ransomware has the following capabilities
  - Find unfamiliar files (such as FindFirstFile)
  - Read/Write behavior in the same file (such as CreateFile -> ReadFile -> SetFilePointer ->WriteFile)
  - Identify common encrypt function or algorithm (WinCrypt*, AES, ChaCha, RC4…)
- What are our criteria of detection?
  - 3 features (file enumeration, file operations, encryption) detected or
  - One of the chain
    - File enumeration → Encryption
    - File enumeration & File operations → Encryption

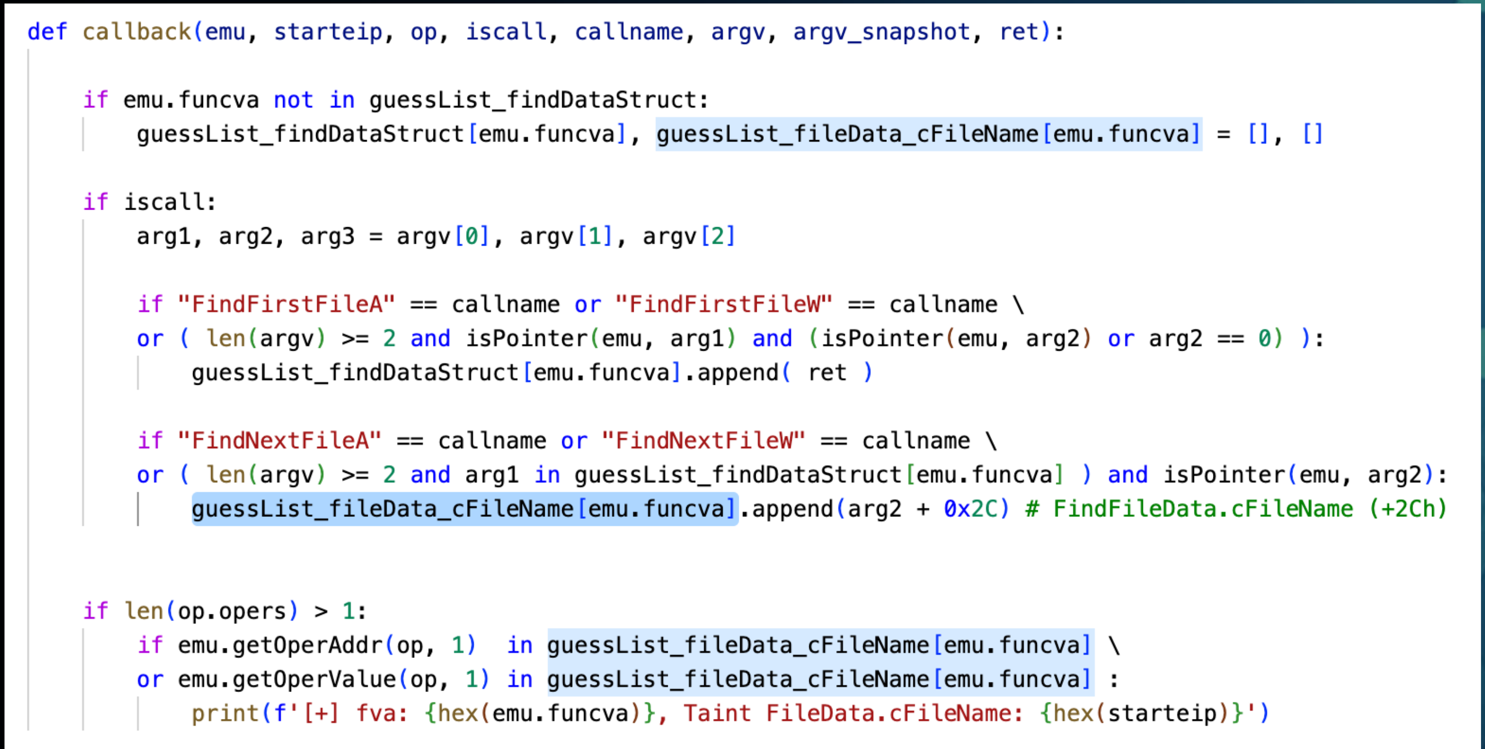
Real World Ransomware Detection (Cont.)

- File Enumeration



```
bool ransomMain(void)
{
  // [COLLAPSED LOCAL DECLARATIONS. PRESS KEYPAD CTRL-

  strcpy(aesKey, "3igcZhRdWq96m3GUmTAiv9");
  hFind = FindFirstFileA("*.*", &FindFileData);
  while ( 1 )
  {
    result = FindNextFileA(hFind, &FindFileData);
    if ( !result )
      break;
    if ( FindFileData.cFileName[0] != '.' )
    {
      strcat(pathToFile, FindFileData.cFileName);
      encryptFile(pathToFile, aesKey, 0x17u);
      printf("[v] encrypt file - %s\n", pathToFile);
    }
  }
  return result;
}
```

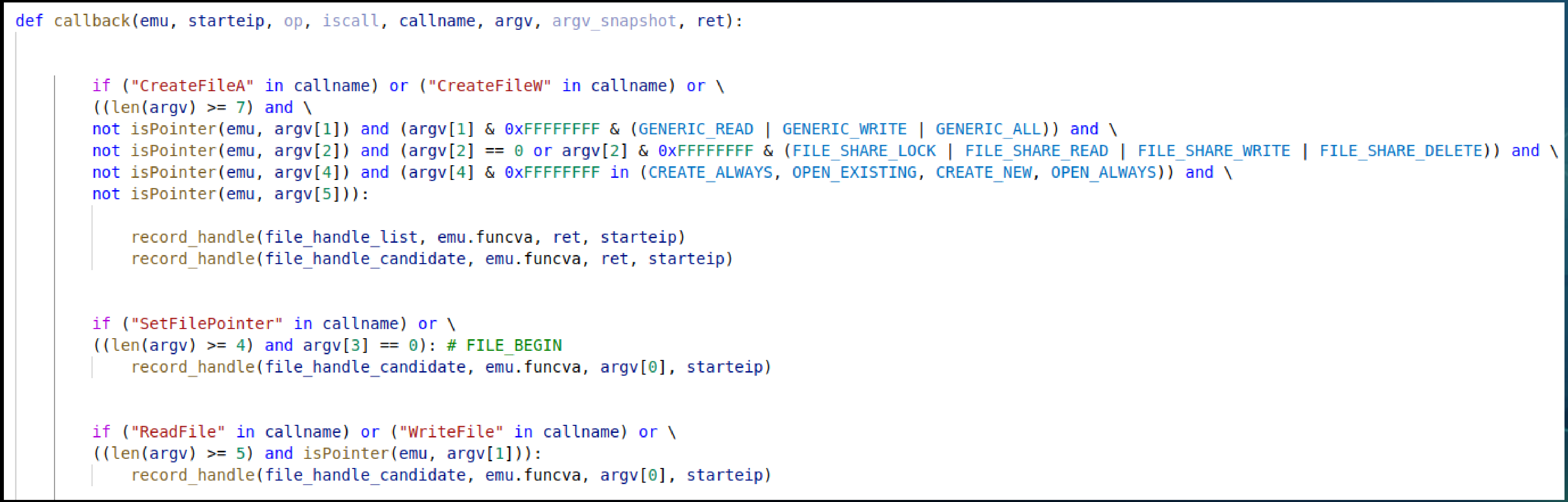
WannaCry Ransomware sample via IDA Pro



```
def callback(emu, starteip, op, iscall, callname, argv, argv_snapshot, ret):

    if emu.funcva not in guessList_findDataStruct:
        guessList_findDataStruct[emu.funcva], guessList_fileData_cFileName[emu.funcva] = [], []

    if iscall:
        arg1, arg2, arg3 = argv[0], argv[1], argv[2]

        if "FindFirstFileA" == callname or "FindFirstFileW" == callname \
        or ( len(argv) >= 2 and isPointer(emu, arg1) and (isPointer(emu, arg2) or arg2 == 0) ):
            guessList_findDataStruct[emu.funcva].append( ret )

        if "FindNextFileA" == callname or "FindNextFileW" == callname \
        or ( len(argv) >= 2 and arg1 in guessList_findDataStruct[emu.funcva] ) and isPointer(emu, arg2):
            guessList_fileData_cFileName[emu.funcva].append(arg2 + 0x2C) # FindFileData.cFileName (+2Ch)


    if len(op.opers) > 1:
        if emu.getOperAddr(op, 1)  in guessList_fileData_cFileName[emu.funcva] \
        or emu.getOperValue(op, 1) in guessList_fileData_cFileName[emu.funcva] :
            print(f'[+] fva: {hex(emu.funcva)}, Taint FileData.cFileName: {hex(starteip)}')
```

Real World Ransomware Detection (Cont.)

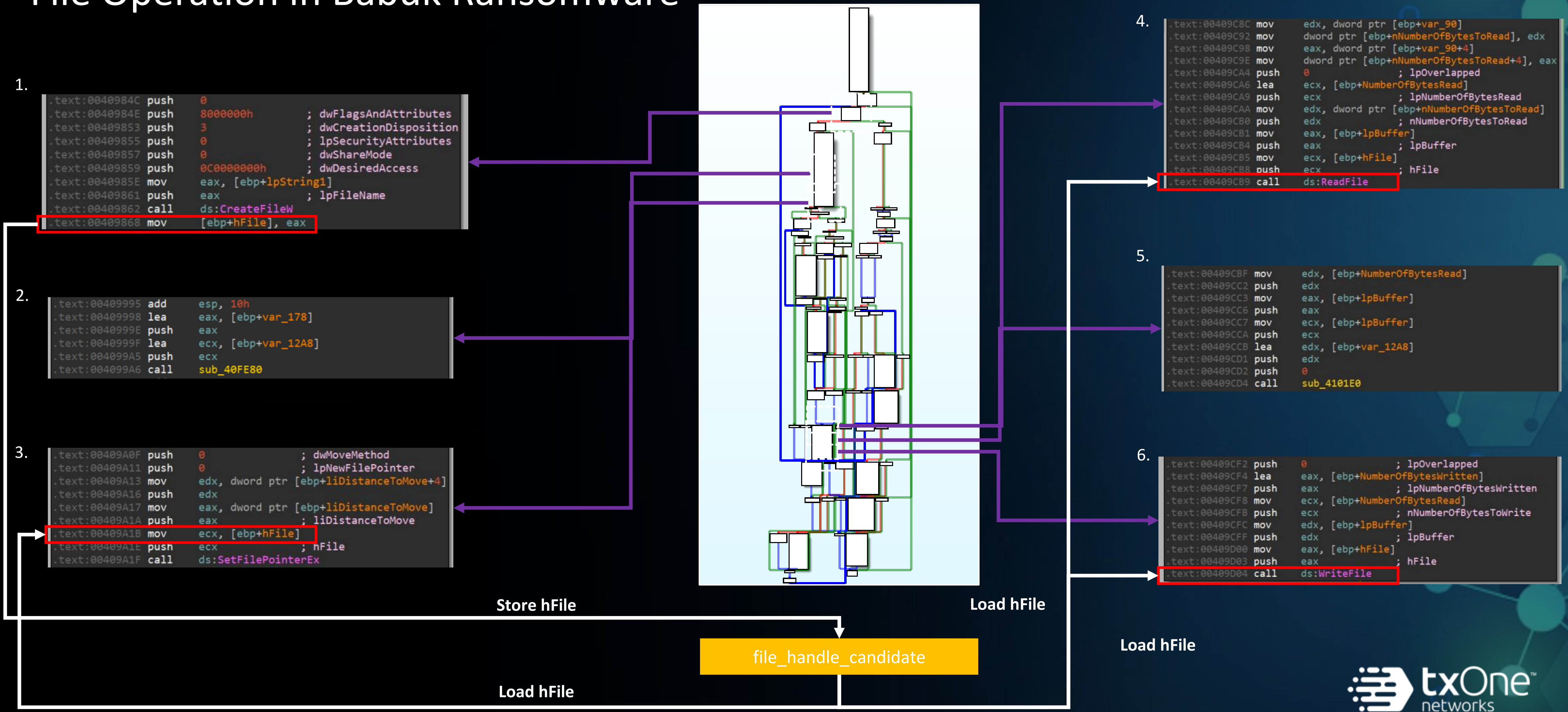
- File Operation
  - Taint file handle generated from CreateFile*
  - Monitor file I/O API usage



```
def callback(emu, starteip, op, iscall, callname, argv, argv_snapshot, ret):


        if ("CreateFileA" in callname) or ("CreateFileW" in callname) or \
        ((len(argv) >= 7) and \
        not isPointer(emu, argv[1]) and (argv[1] & 0xFFFFFFFF & (GENERIC_READ | GENERIC_WRITE | GENERIC_ALL)) and \
        not isPointer(emu, argv[2]) and (argv[2] == 0 or argv[2] & 0xFFFFFFFF & (FILE_SHARE_LOCK | FILE_SHARE_READ | FILE_SHARE_WRITE | FILE_SHARE_DELETE)) and \
        not isPointer(emu, argv[4]) and (argv[4] & 0xFFFFFFFF in (CREATE_ALWAYS, OPEN_EXISTING, CREATE_NEW, OPEN_ALWAYS)) and \
        not isPointer(emu, argv[5])):

            record_handle(file_handle_list, emu.funcva, ret, starteip)
            record_handle(file_handle_candidate, emu.funcva, ret, starteip)


        if ("SetFilePointer" in callname) or \
        ((len(argv) >= 4) and argv[3] == 0): # FILE_BEGIN
            record_handle(file_handle_candidate, emu.funcva, argv[0], starteip)


        if ("ReadFile" in callname) or ("WriteFile" in callname) or \
        ((len(argv) >= 5) and isPointer(emu, argv[1])):
            record_handle(file_handle_candidate, emu.funcva, argv[0], starteip)
```

Real World Ransomware Detection (Cont.)

- File Operation in Babuk Ransomware



1.

```
.text:0040984C push    0
.text:0040984E push    8000000h           ; dwFlagsAndAttributes
.text:00409853 push    3                  ; dwCreationDisposition
.text:00409855 push    0                  ; lpSecurityAttributes
.text:00409857 push    0                  ; dwShareMode
.text:00409859 push    0C0000000h         ; dwDesiredAccess
.text:0040985E mov     eax, [ebp+lpString1]
.text:00409861 push    eax                ; lpFileName
.text:00409862 call    ds:CreateFileW
.text:00409868 mov     [ebp+hFile], eax
```

2.

```
.text:00409995 add     esp, 10h
.text:00409998 lea     eax, [ebp+var_178]
.text:0040999E push    eax
.text:0040999F lea     ecx, [ebp+var_12A8]
.text:004099A5 push    ecx
.text:004099A6 call    sub_40FE80
```

3.

```
.text:00409A0F push    0                  ; dwMoveMethod
.text:00409A11 push    0                  ; lpNewFilePointer
.text:00409A13 mov     edx, dword ptr [ebp+liDistanceToMove+4]
.text:00409A16 push    edx
.text:00409A17 mov     eax, dword ptr [ebp+liDistanceToMove]
.text:00409A1A push    eax                ; liDistanceToMove
.text:00409A1B mov     ecx, [ebp+hFile]
.text:00409A1E push    ecx                ; hFile
.text:00409A1F call    ds:SetFilePointerEx
```

4.

```
.text:00409C8C mov     edx, dword ptr [ebp+var_90]
.text:00409C92 mov     dword ptr [ebp+nNumberOfBytesToRead], edx
.text:00409C98 mov     eax, dword ptr [ebp+var_90+4]
.text:00409C9E mov     dword ptr [ebp+nNumberOfBytesToRead+4], eax
.text:00409CA4 push    0                  ; lpOverlapped
.text:00409CA6 lea     ecx, [ebp+NumberOfBytesRead]
.text:00409CA9 push    ecx                ; lpNumberOfBytesRead
.text:00409CAA mov     edx, dword ptr [ebp+nNumberOfBytesToRead]
.text:00409CB0 push    edx                ; nNumberOfBytesToRead
.text:00409CB1 mov     eax, [ebp+lpBuffer]
.text:00409CB4 push    eax                ; lpBuffer
.text:00409CB5 mov     ecx, [ebp+hFile]
.text:00409CB8 push    ecx                ; hFile
.text:00409CB9 call    ds:ReadFile
```

5.

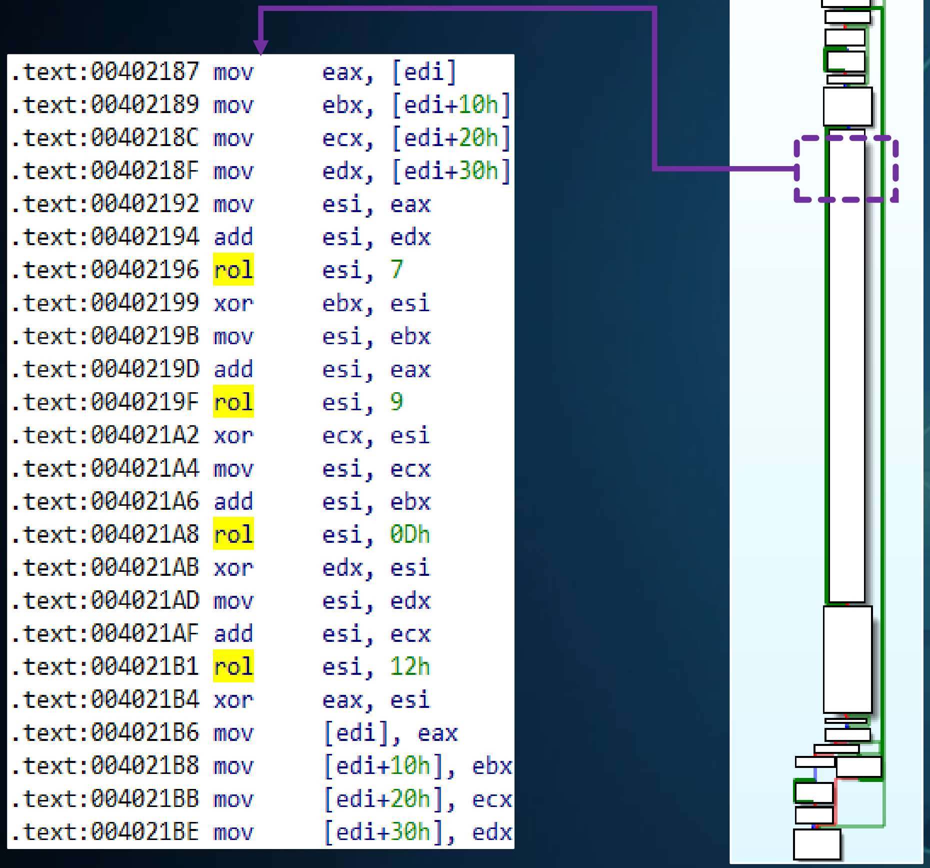
```
.text:00409CBF mov     edx, [ebp+NumberOfBytesRead]
.text:00409CC2 push    edx
.text:00409CC3 mov     eax, [ebp+lpBuffer]
.text:00409CC6 push    eax
.text:00409CC7 mov     ecx, [ebp+lpBuffer]
.text:00409CCA push    ecx
.text:00409CCB lea     edx, [ebp+var_12A8]
.text:00409CD1 push    edx
.text:00409CD2 push    0
.text:00409CD4 call    sub_4101E0
```

6.

```
.text:00409CF2 push    0                  ; lpOverlapped
.text:00409CF4 lea     eax, [ebp+NumberOfBytesWritten]
.text:00409CF7 push    eax                ; lpNumberOfBytesWritten
.text:00409CF8 mov     ecx, [ebp+NumberOfBytesRead]
.text:00409CFB push    ecx                ; nNumberOfBytesToWrite
.text:00409CFC mov     edx, [ebp+lpBuffer]
.text:00409CFF push    edx                ; lpBuffer
.text:00409D00 mov     eax, [ebp+hFile]
.text:00409D03 push    eax                ; hFile
.text:00409D04 call    ds:WriteFile
```

Real World Ransomware Detection (Cont.)

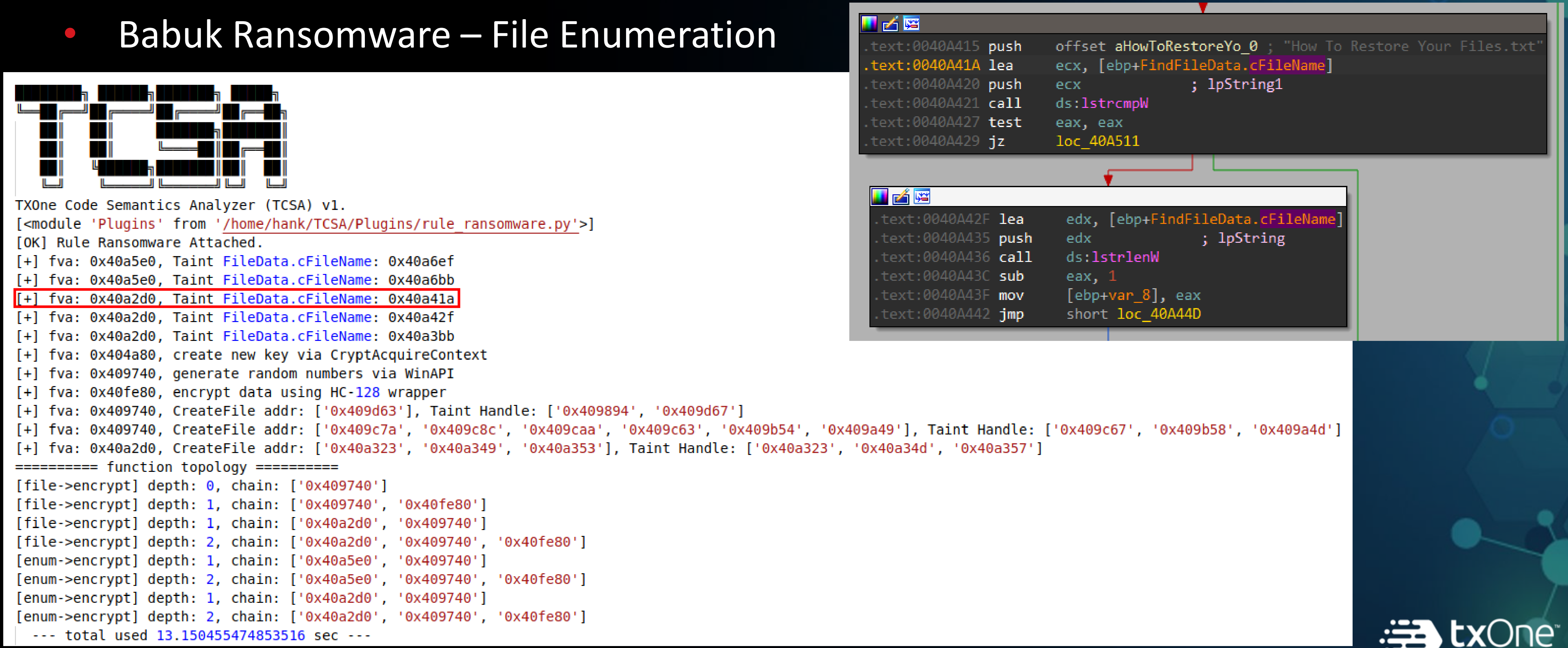
- File Encryption
  - Darkside
    - Customized Salsa20 matrix and encryption
    - 4 rounds of linear shifting
  - 7ev3n
    - R5A Encryption
  - …



```
.text:00402187 mov     eax, [edi]
.text:00402189 mov     ebx, [edi+10h]
.text:0040218C mov     ecx, [edi+20h]
.text:0040218F mov     edx, [edi+30h]
.text:00402192 mov     esi, eax
.text:00402194 add     esi, edx
.text:00402196 rol     esi, 7
.text:00402199 xor     ebx, esi
.text:0040219B mov     esi, ebx
.text:0040219D add     esi, eax
.text:0040219F rol     esi, 9
.text:004021A2 xor     ecx, esi
.text:004021A4 mov     esi, ecx
.text:004021A6 add     esi, ebx
.text:004021A8 rol     esi, 0Dh
.text:004021AB xor     edx, esi
.text:004021AD mov     esi, edx
.text:004021AF add     esi, ecx
.text:004021B1 rol     esi, 12h
.text:004021B4 xor     eax, esi
.text:004021B6 mov     [edi], eax
.text:004021B8 mov     [edi+10h], ebx
.text:004021BB mov     [edi+20h], ecx
.text:004021BE mov     [edi+30h], edx
```

Real World Ransomware Detection (Cont.)

- Babuk Ransomware – File Enumeration



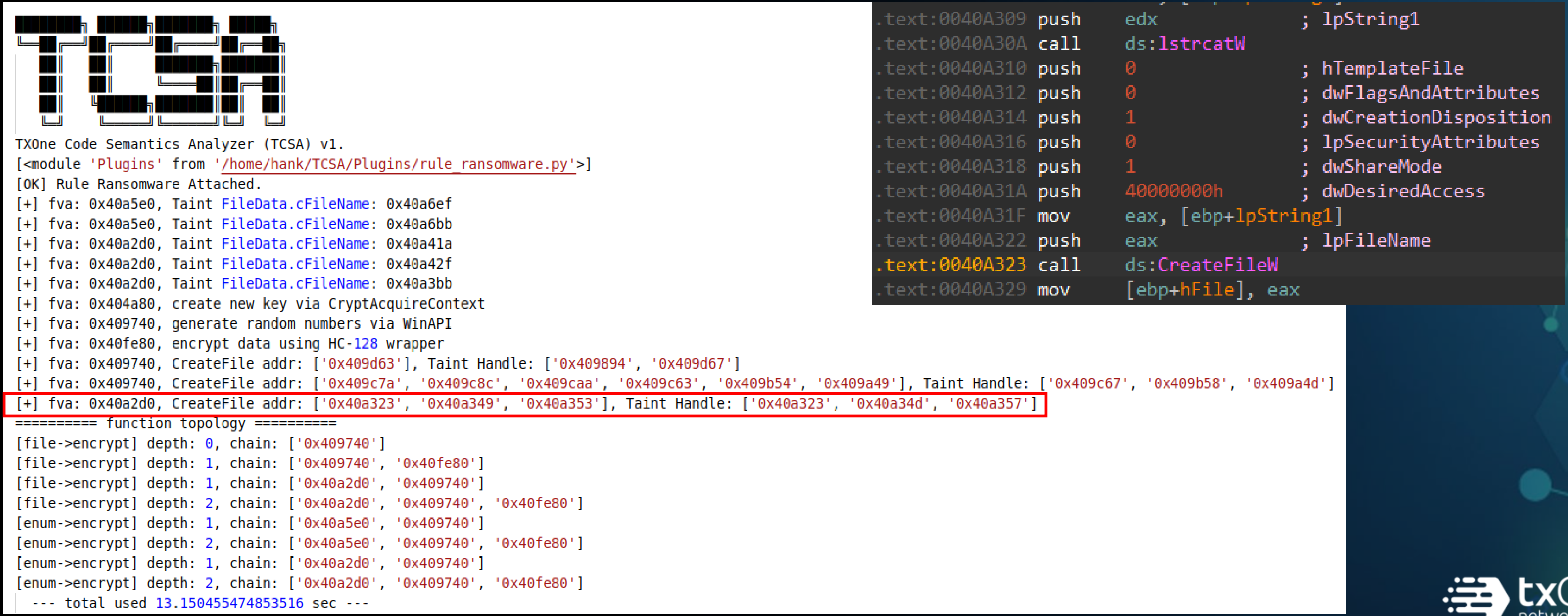
```
.text:0040A415 push    offset aHowToRestoreYo_0 ; "How To Restore Your Files.txt"
.text:0040A41A lea     ecx, [ebp+FindFileData.cFileName]
.text:0040A420 push    ecx             ; lpString1
.text:0040A421 call    ds:lstrcmpW
.text:0040A427 test    eax, eax
.text:0040A429 jz      loc_40A511
```

```
.text:0040A42F lea     edx, [ebp+FindFileData.cFileName]
.text:0040A435 push    edx             ; lpString
.text:0040A436 call    ds:lstrlenW
.text:0040A43C sub     eax, 1
.text:0040A43F mov     [ebp+var_8], eax
.text:0040A442 jmp     short loc_40A44D
```

```
TXOne Code Semantics Analyzer (TCSA) v1.
[<module 'Plugins' from '/home/hank/TCSA/Plugins/rule_ransomware.py'>]
[OK] Rule Ransomware Attached.
[+] fva: 0x40a5e0, Taint FileData.cFileName: 0x40a6ef
[+] fva: 0x40a5e0, Taint FileData.cFileName: 0x40a6bb
[+] fva: 0x40a2d0, Taint FileData.cFileName: 0x40a41a
[+] fva: 0x40a2d0, Taint FileData.cFileName: 0x40a42f
[+] fva: 0x40a2d0, Taint FileData.cFileName: 0x40a3bb
[+] fva: 0x404a80, create new key via CryptAcquireContext
[+] fva: 0x409740, generate random numbers via WinAPI
[+] fva: 0x40fe80, encrypt data using HC-128 wrapper
[+] fva: 0x409740, CreateFile addr: ['0x409d63'], Taint Handle: ['0x409894', '0x409d67']
[+] fva: 0x409740, CreateFile addr: ['0x409c7a', '0x409c8c', '0x409caa', '0x409c63', '0x409b54', '0x409a49'], Taint Handle: ['0x409c67', '0x409b58', '0x409a4d']
[+] fva: 0x40a2d0, CreateFile addr: ['0x40a323', '0x40a349', '0x40a353'], Taint Handle: ['0x40a323', '0x40a34d', '0x40a357']
========== function topology ==========
[file->encrypt] depth: 0, chain: ['0x409740']
[file->encrypt] depth: 1, chain: ['0x409740', '0x40fe80']
[file->encrypt] depth: 1, chain: ['0x40a2d0', '0x409740']
[file->encrypt] depth: 2, chain: ['0x40a2d0', '0x409740', '0x40fe80']
[enum->encrypt] depth: 1, chain: ['0x40a5e0', '0x409740']
[enum->encrypt] depth: 2, chain: ['0x40a5e0', '0x409740', '0x40fe80']
[enum->encrypt] depth: 1, chain: ['0x40a2d0', '0x409740']
[enum->encrypt] depth: 2, chain: ['0x40a2d0', '0x409740', '0x40fe80']
  --- total used 13.150455474853516 sec ---
```

Real World Ransomware Detection (Cont.)

- Babuk Ransomware – File Operation

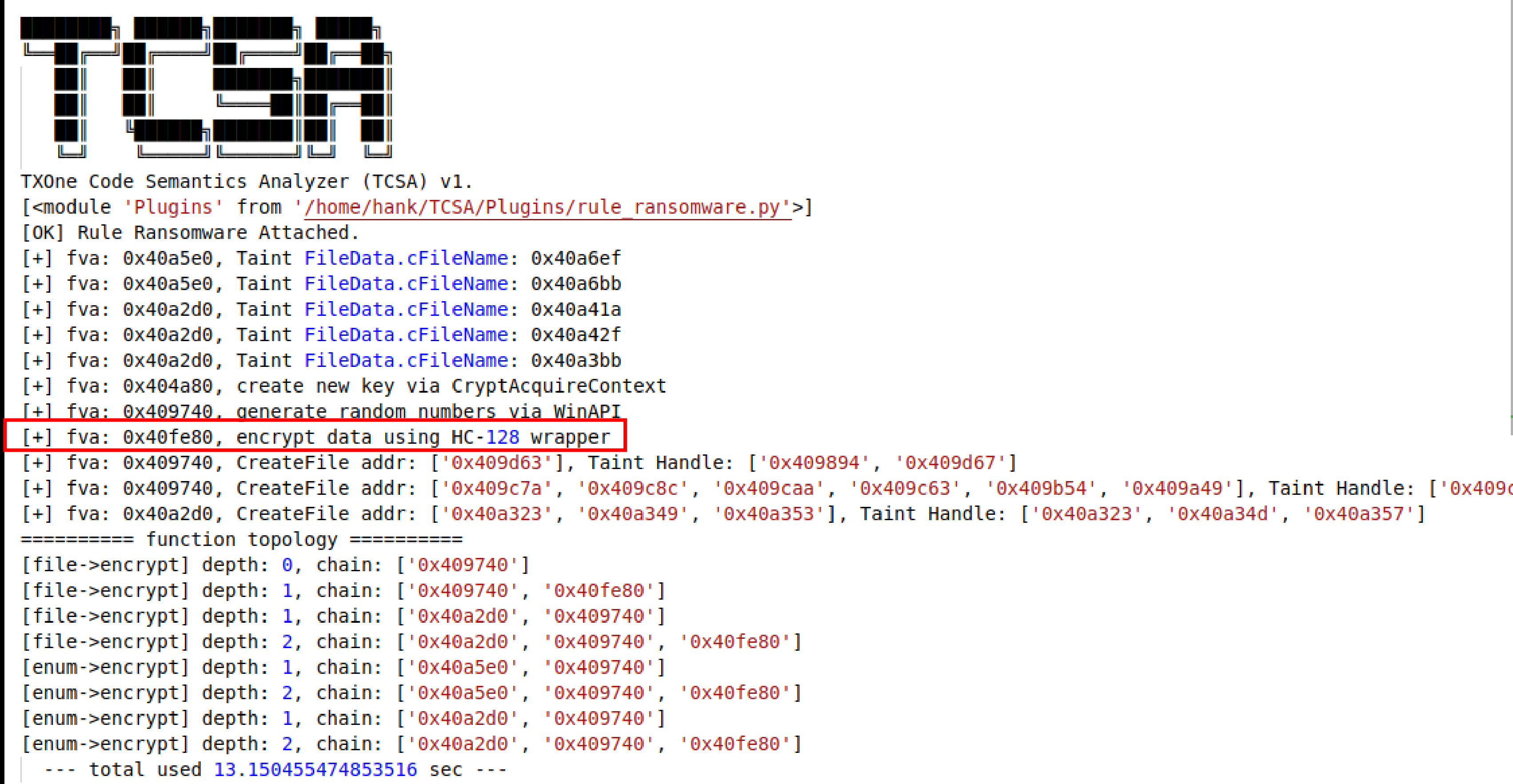


```
TXOne Code Semantics Analyzer (TCSA) v1.
[<module 'Plugins' from '/home/hank/TCSA/Plugins/rule_ransomware.py'>]
[OK] Rule Ransomware Attached.
[+] fva: 0x40a5e0, Taint FileData.cFileName: 0x40a6ef
[+] fva: 0x40a5e0, Taint FileData.cFileName: 0x40a6bb
[+] fva: 0x40a2d0, Taint FileData.cFileName: 0x40a41a
[+] fva: 0x40a2d0, Taint FileData.cFileName: 0x40a42f
[+] fva: 0x40a2d0, Taint FileData.cFileName: 0x40a3bb
[+] fva: 0x404a80, create new key via CryptAcquireContext
[+] fva: 0x409740, generate random numbers via WinAPI
[+] fva: 0x40fe80, encrypt data using HC-128 wrapper
[+] fva: 0x409740, CreateFile addr: ['0x409d63'], Taint Handle: ['0x409894', '0x409d67']
[+] fva: 0x409740, CreateFile addr: ['0x409c7a', '0x409c8c', '0x409caa', '0x409c63', '0x409b54', '0x409a49'], Taint Handle: ['0x409c67', '0x409b58', '0x409a4d']
[+] fva: 0x40a2d0, CreateFile addr: ['0x40a323', '0x40a349', '0x40a353'], Taint Handle: ['0x40a323', '0x40a34d', '0x40a357']
========== function topology ==========
[file->encrypt] depth: 0, chain: ['0x409740']
[file->encrypt] depth: 1, chain: ['0x409740', '0x40fe80']
[file->encrypt] depth: 1, chain: ['0x40a2d0', '0x409740']
[file->encrypt] depth: 2, chain: ['0x40a2d0', '0x409740', '0x40fe80']
[enum->encrypt] depth: 1, chain: ['0x40a5e0', '0x409740']
[enum->encrypt] depth: 2, chain: ['0x40a5e0', '0x409740', '0x40fe80']
[enum->encrypt] depth: 1, chain: ['0x40a2d0', '0x409740']
[enum->encrypt] depth: 2, chain: ['0x40a2d0', '0x409740', '0x40fe80']
 --- total used 13.150455474853516 sec ---
```

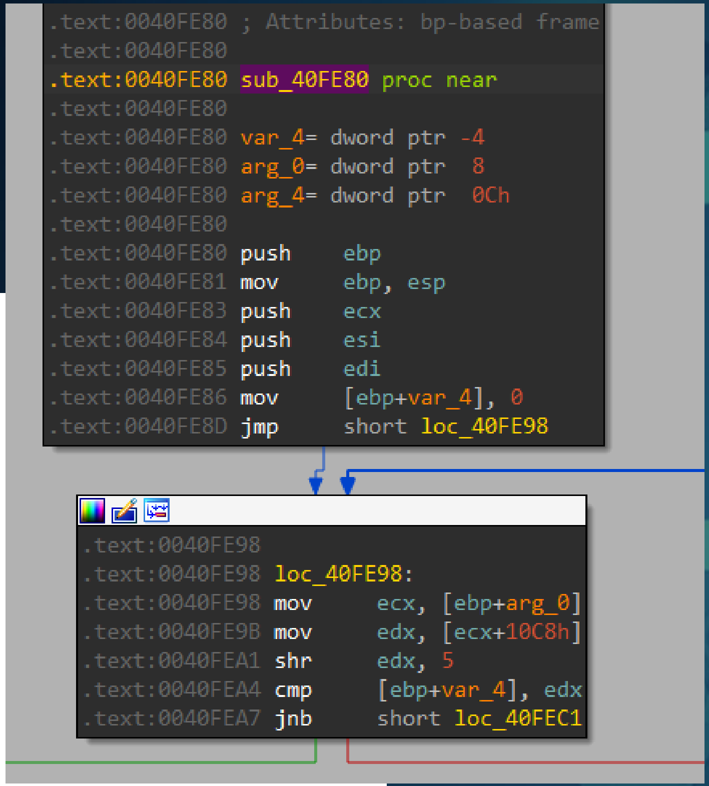
```
.text:0040A309 push    edx                 ; lpString1
.text:0040A30A call    ds:lstrcatW
.text:0040A310 push    0                   ; hTemplateFile
.text:0040A312 push    0                   ; dwFlagsAndAttributes
.text:0040A314 push    1                   ; dwCreationDisposition
.text:0040A316 push    0                   ; lpSecurityAttributes
.text:0040A318 push    1                   ; dwShareMode
.text:0040A31A push    40000000h           ; dwDesiredAccess
.text:0040A31F mov     eax, [ebp+lpString1]
.text:0040A322 push    eax                 ; lpFileName
.text:0040A323 call    ds:CreateFileW
.text:0040A329 mov     [ebp+hFile], eax
```

Real World Ransomware Detection (Cont.)

- Babuk Ransomware – File Encryption



```
TXOne Code Semantics Analyzer (TCSA) v1.
[<module 'Plugins' from '/home/hank/TCSA/Plugins/rule_ransomware.py'>]
[OK] Rule Ransomware Attached.
[+] fva: 0x40a5e0, Taint FileData.cFileName: 0x40a6ef
[+] fva: 0x40a5e0, Taint FileData.cFileName: 0x40a6bb
[+] fva: 0x40a2d0, Taint FileData.cFileName: 0x40a41a
[+] fva: 0x40a2d0, Taint FileData.cFileName: 0x40a42f
[+] fva: 0x40a2d0, Taint FileData.cFileName: 0x40a3bb
[+] fva: 0x404a80, create new key via CryptAcquireContext
[+] fva: 0x409740, generate random numbers via WinAPI
[+] fva: 0x40fe80, encrypt data using HC-128 wrapper
[+] fva: 0x409740, CreateFile addr: ['0x409d63'], Taint Handle: ['0x409894', '0x409d67']
[+] fva: 0x409740, CreateFile addr: ['0x409c7a', '0x409c8c', '0x409caa', '0x409c63', '0x409b54', '0x409a49'], Taint Handle: ['0x409c67', '0x409b58', '0x409a4d']
[+] fva: 0x40a2d0, CreateFile addr: ['0x40a323', '0x40a349', '0x40a353'], Taint Handle: ['0x40a323', '0x40a34d', '0x40a357']
========== function topology ==========
[file->encrypt] depth: 0, chain: ['0x409740']
[file->encrypt] depth: 1, chain: ['0x409740', '0x40fe80']
[file->encrypt] depth: 1, chain: ['0x40a2d0', '0x409740']
[file->encrypt] depth: 2, chain: ['0x40a2d0', '0x409740', '0x40fe80']
[enum->encrypt] depth: 1, chain: ['0x40a5e0', '0x409740']
[enum->encrypt] depth: 2, chain: ['0x40a5e0', '0x409740', '0x40fe80']
[enum->encrypt] depth: 1, chain: ['0x40a2d0', '0x409740']
[enum->encrypt] depth: 2, chain: ['0x40a2d0', '0x409740', '0x40fe80']
 --- total used 13.150455474853516 sec ---
```



```
.text:0040FE80 ; Attributes: bp-based frame
.text:0040FE80
.text:0040FE80 sub_40FE80 proc near
.text:0040FE80
.text:0040FE80 var_4= dword ptr -4
.text:0040FE80 arg_0= dword ptr  8
.text:0040FE80 arg_4= dword ptr  0Ch
.text:0040FE80
.text:0040FE80 push    ebp
.text:0040FE81 mov     ebp, esp
.text:0040FE83 push    ecx
.text:0040FE84 push    esi
.text:0040FE85 push    edi
.text:0040FE86 mov     [ebp+var_4], 0
.text:0040FE8D jmp     short loc_40FE98
```

```
.text:0040FE98
.text:0040FE98 loc_40FE98:
.text:0040FE98 mov     ecx, [ebp+arg_0]
.text:0040FE9B mov     edx, [ecx+10C8h]
.text:0040FEA1 shr     edx, 5
.text:0040FEA4 cmp     [ebp+var_4], edx
.text:0040FEA7 jnb     short loc_40FEC1
```

Real World Ransomware Detection (Cont.)

- Experiment
- How we collect Ransomware samples?
  - Time interval: 2021.06-2022.06
  - Filter process
    - Found in VirusTotal, more than 3 antivirus vendors identify ransomware, and it is Windows executable
    - Automated dynamic analysis (commercial sandbox)
    - Final check samples
    - Get ransomware sample dataset
  - Results
    - 1153 / 1206 (95.60%) !!!

Real World Ransomware Detection (Cont.)

- Purge
- Rents
- Conti
- Sorikrypt
- Nemty
- Avaddon
- Phoenix
- Deltalocker
- Seven
- Medusalocker
- Crysis
- Higuniel
- Fakeglobe
- Netfilm
- Spora
- Karmalocker
- Phobos
- Cryptolocker
- Filecoder
- Paradise
- Emper
- Wana
- Babuklocker
- Genasom
- Lockbit
- Makop
- Crypren
- Cryptor
- Quantumlocker
- Garrantdecrypt
- Lockergoga
- Thundercrypt
- Agent
- Redeemer
- Hydracrypt
- Wixawm
- Blackmatter
- Smar
- Buhtrap
- Wcry
- Explus
- Sodinokibi
- Avoslocker
- Zcrypt
- Revil
- Akolocker
- Ryuk
- Hkitty
- Taleb
- Garrantycrypt
- Sevencrypt
- Sodinokib
- Bastacrypt
- Cryptlock
- Nemisis
- Swrort
- Hive
- Tovicrypt
- Crypmod
- Xorist
- Ranzylocker
- Wadhrama
- Netwalker
- Babuk

Real World Ransomware Detection (Cont.)

- Conti variants

  Ransom.Win32.CONTI.SM.hp
  Ransom.Win32.CONTI.SMTH.hp
  Ransom.Win32.CONTI.SMYXBBU
  Ransom.Win32.CONTI.SMYXBFD.hp
  Ransom.Win32.CONTI.YACCA
  Ransom.Win32.CONTI.YXCAAZ
  Ransom.Win32.CONTI.YXCBSZ

- LockBit variants

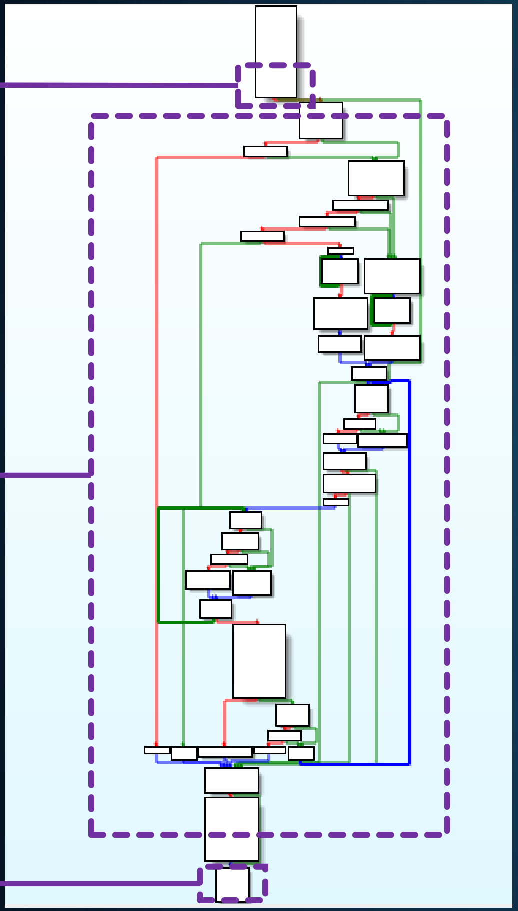
  Ransom.Win32.LOCKBIT.SMCET
  Ransom.Win32.LOCKBIT.SMDS
  Ransom.Win32.LOCKBIT.SMYEBGW
  Ransom.Win32.LOCKBIT.YXBHC-TH
  Ransom_LockBit.R002C0CGI21
  Ransom_Lockbit.R002C0DCO22
  Ransom_Lockbit.R002C0DHB21
  Ransom_Lockbit.R002C0DHD21

- 7ev3n variants

  Ransom_Seven.R002C0DA422
  Ransom_Seven.R002C0DA522
  Ransom_Seven.R002C0DA922
  Ransom_Seven.R002C0DAA22
  Ransom_Seven.R002C0DAF22
  Ransom_Seven.R002C0DAP22
  Ransom_Seven.R002C0DAR22
  Ransom_Seven.R002C0DAS22
  Ransom_Seven.R002C0DAT22
  Ransom_Seven.R002C0DAV22
  Ransom_Seven.R002C0DB122
  Ransom_Seven.R002C0DB222
  Ransom_Seven.R002C0DB322
  Ransom_Seven.R002C0DB822
  Ransom_Seven.R002C0DB922
  Ransom_Seven.R002C0DBA22
  Ransom_Seven.R002C0DBM22
  Ransom_Seven.R002C0DC222
  Ransom_Seven.R002C0DC922
  Ransom_Seven.R002C0DCB22
  Ransom_Seven.R002C0DCC22
  Ransom_Seven.R002C0DCE22
  Ransom_Sodin.R002C0PGM21
  Ransom_EMPER.SM

Real World Ransomware Detection (Cont.)

- For some of undetected samples
  - Prolock / PwndLocker
    - Unknown Encryption Algorithm



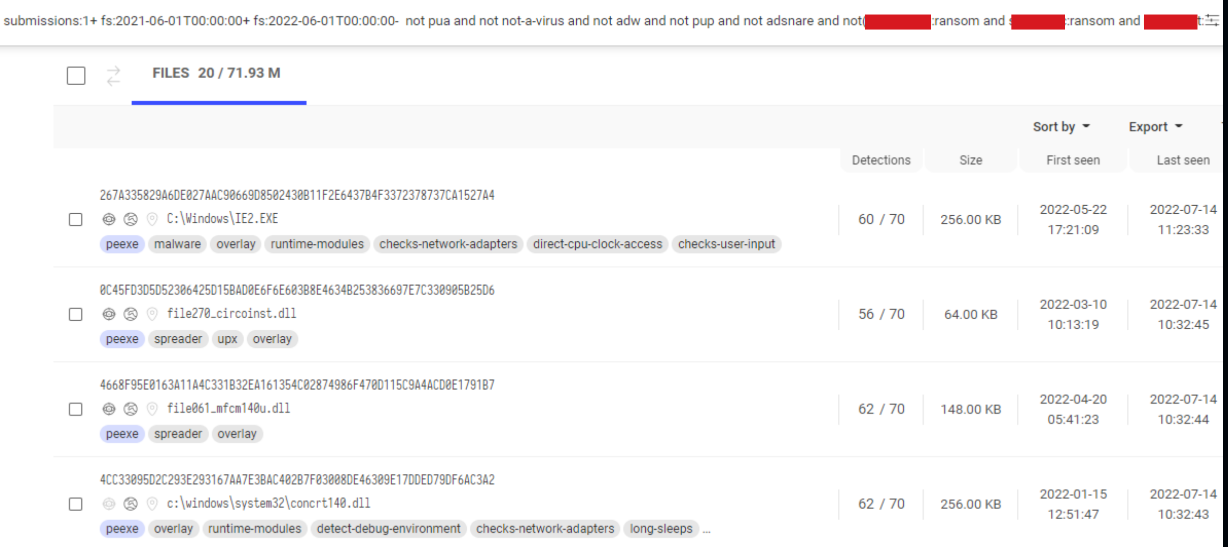
CreateFileW

Customized File Encryption

MoveFileW

Real World Ransomware Detection (Cont.)

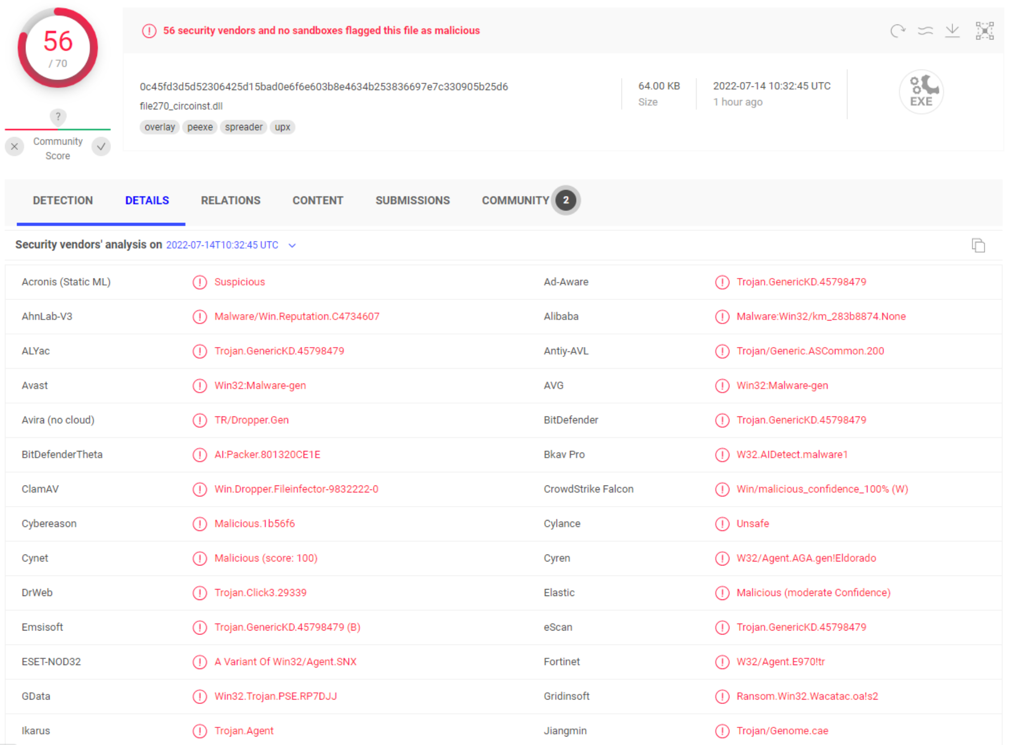
- Experiment
    - By randomly finding 200 non-ransom samples from VirusTotal (2021/06/01 - 2022/06/01)
        - False Positive: 0%



submissions:1+ fs:2021-06-01T00:00:00+ fs:2022-06-01T00:00:00- not pua and not not-a-virus and not adw and not pup and not adsnare and not([redacted]:ransom and [redacted]:ransom and [redacted]t:

FILES 20 / 71.93 M

	Detections	Size	First seen	Last seen
□ 267A335829A6DE027AAC90669D8502430B11F2E6437B4F3372378737CA1527A4 C:\Windows\IE2.EXE peexe malware overlay runtime-modules checks-network-adapters direct-cpu-clock-access checks-user-input	60 / 70	256.00 KB	2022-05-22 17:21:09	2022-07-14 11:23:33
□ 0C45FD3D5D52306425D15BAD0E6F6E603B8E4634B253836697E7C330905B25D6 file270_circoinst.dll peexe spreader upx overlay	56 / 70	64.00 KB	2022-03-10 10:13:19	2022-07-14 10:32:45
□ 4668F95E0163A11A4C331B32EA161354C02874986F470D115C9A4ACD0E1791B7 file061_mfcm140u.dll peexe spreader overlay	62 / 70	148.00 KB	2022-04-20 05:41:23	2022-07-14 10:32:44
□ 4CC33095D2C293E293167AA7E3BAC402B7F03008DE46309E17DDED79DF6AC3A2 c:\windows\system32\concrt140.dll peexe overlay runtime-modules detect-debug-environment checks-network-adapters long-sleeps ...	62 / 70	256.00 KB	2022-01-15 12:51:47	2022-07-14 10:32:43



56 / 70

56 security vendors and no sandboxes flagged this file as malicious

0c45fd3d5d52306425d15bad0e6f6e603b8e4634b253836697e7c330905b25d6
file270_circoinst.dll
overlay peexe spreader upx

64.00 KB Size

2022-07-14 10:32:45 UTC
1 hour ago

Security vendors' analysis on 2022-07-14T10:32:45 UTC

Acronis (Static ML)	Suspicious	Ad-Aware	Trojan.GenericKD.45798479
AhnLab-V3	Malware/Win.Reputation.C4734607	Alibaba	Malware:Win32/km_283b8874.None
ALYac	Trojan.GenericKD.45798479	Antiy-AVL	Trojan/Generic.ASCommon.200
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Avira (no cloud)	TR/Dropper.Gen	BitDefender	Trojan.GenericKD.45798479
BitDefenderTheta	AI:Packer.801320CE1E	Bkav Pro	W32.AIDetect.malware1
ClamAV	Win.Dropper.Fileinfector-9832222-0	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cybereason	Malicious.1b56f6	Cylance	Unsafe
Cynet	Malicious (score: 100)	Cyren	W32/Agent.AGA.gen!Eldorado
DrWeb	Trojan.Click3.29339	Elastic	Malicious (moderate Confidence)
Emsisoft	Trojan.GenericKD.45798479 (B)	eScan	Trojan.GenericKD.45798479
ESET-NOD32	A Variant Of Win32/Agent.SNX	Fortinet	W32/Agent.E970!tr
GData	Win32.Trojan.PSE.RP7DJJ	Gridinsoft	Ransom.Win32.Wacatac.oa!s2
Ikarus	Trojan.Agent	Jiangmin	Trojan/Genome.cae

Practical Ransomware Mitigation Strategies in Critical Infrastructure

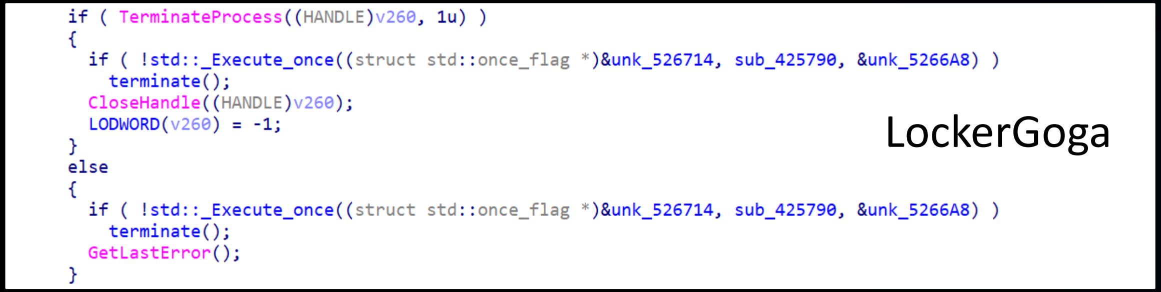
- IT Environment: TCSA + Other Mitigation Strategies
- OT Environment: **Multilayer Mitigation Strategies**

Practical Ransomware Mitigation Strategy for OT environment

	Known Ransonware Scanning ▷	Ransomware Pre-detection Mechanism ▷	Ransomware Encrypted Sequence Detection
👍	Hardly cause any burden on the ICS system	Detect ransomware family common features and block before encryption	Detect ransomware encrypted sequences can prevent excessive burden on the ICS machine and block encryption process
👎	Unable to detect and block new/variant ransomware attacks	False-Positive	Nothing found so far

ICS-Related Ransomware Pre-detection Mechanism

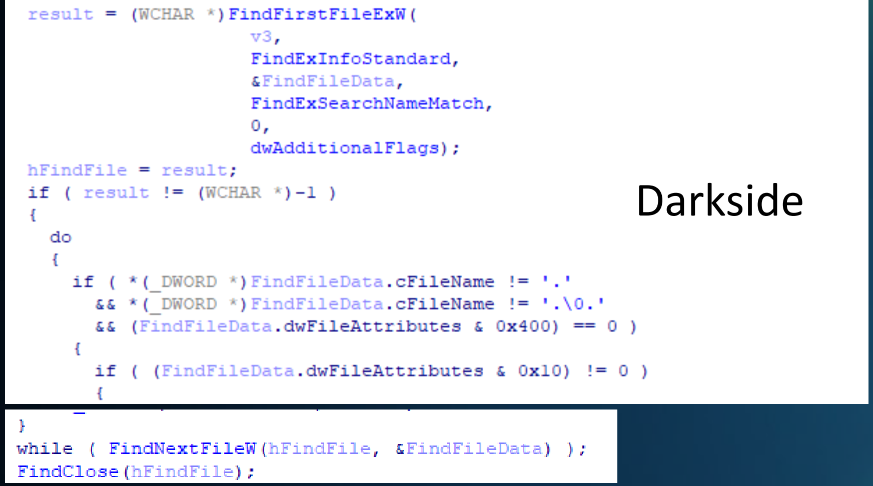
If prevent process be terminated



```
if ( TerminateProcess((HANDLE)v260, 1u) )
{
  if ( !std::_Execute_once((struct std::once_flag *)&unk_526714, sub_425790, &unk_5266A8) )
    terminate();
  CloseHandle((HANDLE)v260);
  LODWORD(v260) = -1;
}
else
{
  if ( !std::_Execute_once((struct std::once_flag *)&unk_526714, sub_425790, &unk_5266A8) )
    terminate();
  GetLastError();
}
```

LockerGoga

If enumerate files failed

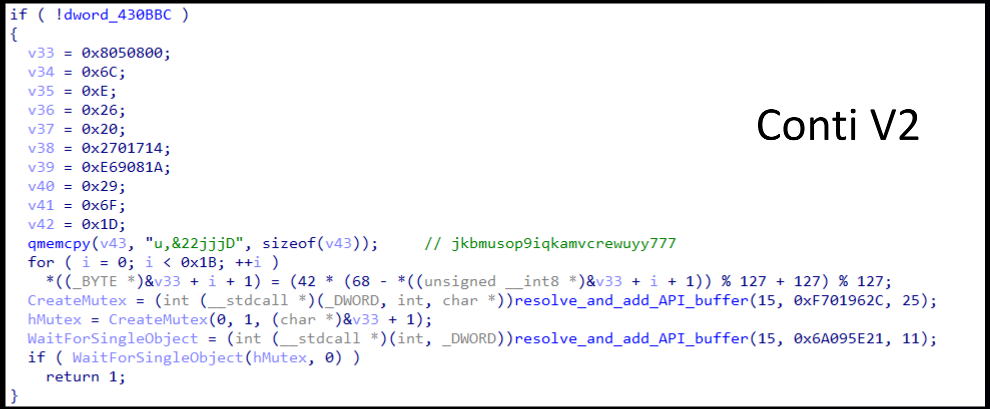


```
result = (WCHAR *)FindFirstFileExW(
                    v3,
                    FindExInfoStandard,
                    &FindFileData,
                    FindExSearchNameMatch,
                    0,
                    dwAdditionalFlags);
hFindFile = result;
if ( result != (WCHAR *)-1 )
{
  do
  {
    if ( *(_DWORD *)FindFileData.cFileName != '.'
      && *(_DWORD *)FindFileData.cFileName != '.\0.'
      && (FindFileData.dwFileAttributes & 0x400) == 0 )
    {
      if ( (FindFileData.dwFileAttributes & 0x10) != 0 )
      {
```

```
}
while ( FindNextFileW(hFindFile, &FindFileData) );
FindClose(hFindFile);
```

Darkside

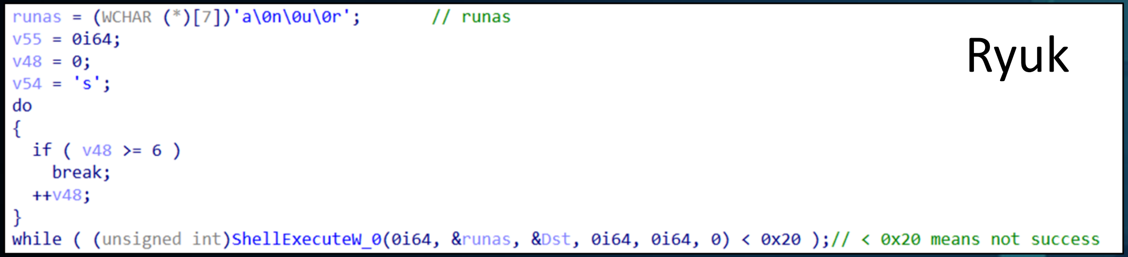
If atomic check failed



```
if ( !dword_430BBC )
{
  v33 = 0x8050800;
  v34 = 0x6C;
  v35 = 0xE;
  v36 = 0x26;
  v37 = 0x20;
  v38 = 0x2701714;
  v39 = 0xE69081A;
  v40 = 0x29;
  v41 = 0x6F;
  v42 = 0x1D;
  qmemcpy(v43, "u,&22jjjD", sizeof(v43));     // jkbmusop9iqkamvcrewuyy777
  for ( i = 0; i < 0x1B; ++i )
    *((_BYTE *)&v33 + i + 1) = (42 * (68 - *((unsigned __int8 *)&v33 + i + 1)) % 127 + 127) % 127;
  CreateMutex = (int (__stdcall *)(_DWORD, int, char *))resolve_and_add_API_buffer(15, 0xF701962C, 25);
  hMutex = CreateMutex(0, 1, (char *)&v33 + 1);
  WaitForSingleObject = (int (__stdcall *)(int, _DWORD))resolve_and_add_API_buffer(15, 0x6A095E21, 11);
  if ( WaitForSingleObject(hMutex, 0) )
    return 1;
}
```

Conti V2

If prevent shadow copy be deleted

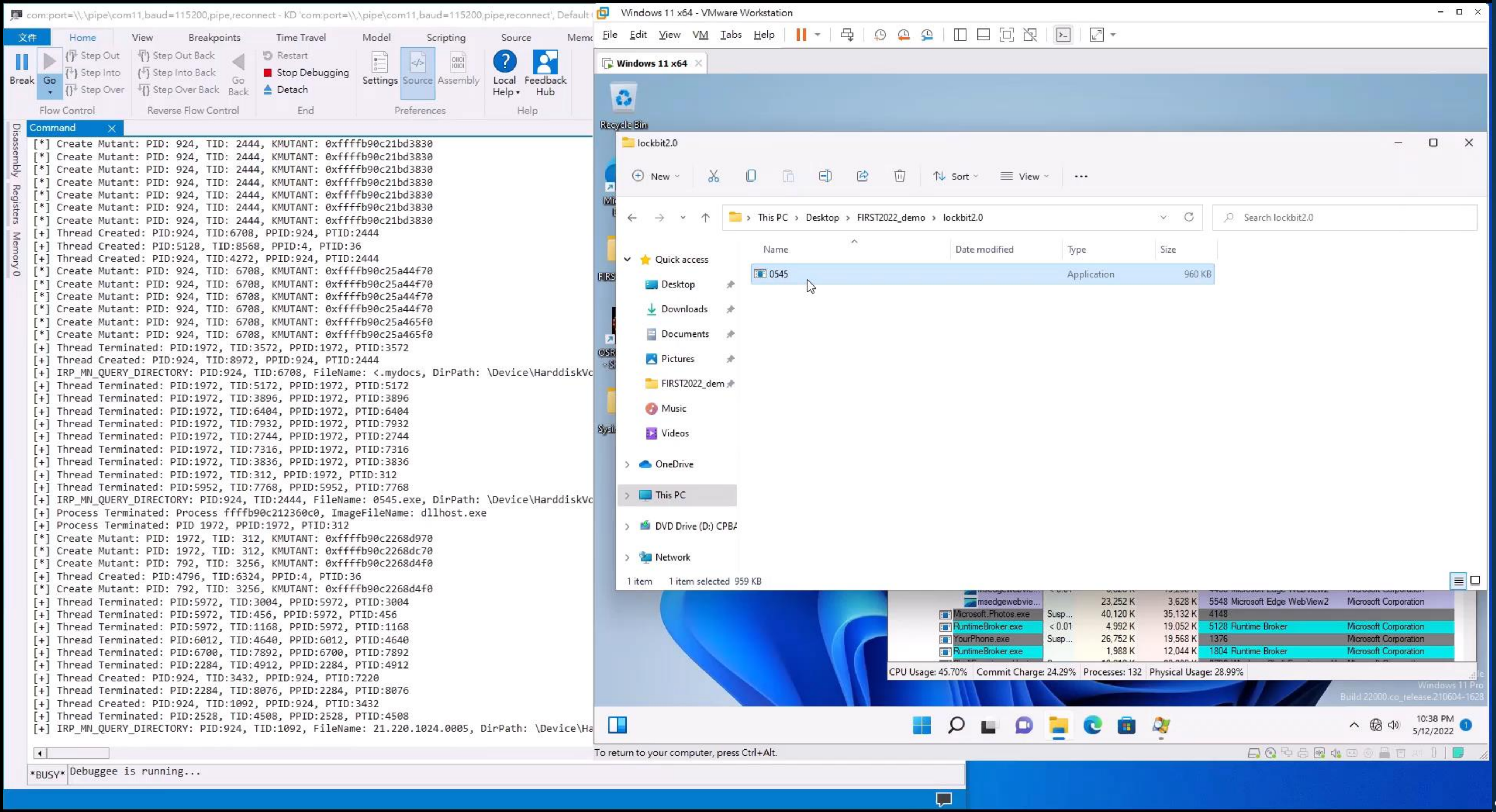


```
runas = (WCHAR (*)[7])'a\0n\0u\0r';       // runas
v55 = 0i64;
v48 = 0;
v54 = 's';
do
{
  if ( v48 >= 6 )
    break;
  ++v48;
}
while ( (unsigned int)ShellExecuteW_0(0i64, &runas, &Dst, 0i64, 0i64, 0) < 0x20 );// < 0x20 means not success
```

Ryuk

txOne networks

ICS-Related Ransomware Pre-detection Mechanism



```
[*] Create Mutant: PID: 924, TID: 2444, KMUTANT: 0xffffb90c21bd3830
[*] Create Mutant: PID: 924, TID: 2444, KMUTANT: 0xffffb90c21bd3830
[*] Create Mutant: PID: 924, TID: 2444, KMUTANT: 0xffffb90c21bd3830
[*] Create Mutant: PID: 924, TID: 2444, KMUTANT: 0xffffb90c21bd3830
[*] Create Mutant: PID: 924, TID: 2444, KMUTANT: 0xffffb90c21bd3830
[*] Create Mutant: PID: 924, TID: 2444, KMUTANT: 0xffffb90c21bd3830
[*] Create Mutant: PID: 924, TID: 2444, KMUTANT: 0xffffb90c21bd3830
[+] Thread Created: PID:924, TID:6708, PPID:924, PTID:2444
[+] Thread Created: PID:5128, TID:8568, PPID:4, PTID:36
[+] Thread Created: PID:924, TID:4272, PPID:924, PTID:2444
[*] Create Mutant: PID: 924, TID: 6708, KMUTANT: 0xffffb90c25a44f70
[*] Create Mutant: PID: 924, TID: 6708, KMUTANT: 0xffffb90c25a44f70
[*] Create Mutant: PID: 924, TID: 6708, KMUTANT: 0xffffb90c25a44f70
[*] Create Mutant: PID: 924, TID: 6708, KMUTANT: 0xffffb90c25a44f70
[*] Create Mutant: PID: 924, TID: 6708, KMUTANT: 0xffffb90c25a465f0
[*] Create Mutant: PID: 924, TID: 6708, KMUTANT: 0xffffb90c25a465f0
[+] Thread Terminated: PID:1972, TID:3572, PPID:1972, PTID:3572
[+] Thread Created: PID:924, TID:8972, PPID:924, PTID:2444
[+] IRP_MN_QUERY_DIRECTORY: PID:924, TID:6708, FileName: <.mydocs, DirPath: \Device\HarddiskVc
[+] Thread Terminated: PID:1972, TID:5172, PPID:1972, PTID:5172
[+] Thread Terminated: PID:1972, TID:3896, PPID:1972, PTID:3896
[+] Thread Terminated: PID:1972, TID:6404, PPID:1972, PTID:6404
[+] Thread Terminated: PID:1972, TID:7932, PPID:1972, PTID:7932
[+] Thread Terminated: PID:1972, TID:2744, PPID:1972, PTID:2744
[+] Thread Terminated: PID:1972, TID:7316, PPID:1972, PTID:7316
[+] Thread Terminated: PID:1972, TID:3836, PPID:1972, PTID:3836
[+] Thread Terminated: PID:1972, TID:312, PPID:1972, PTID:312
[+] Thread Terminated: PID:5952, TID:7768, PPID:5952, PTID:7768
[+] IRP_MN_QUERY_DIRECTORY: PID:924, TID:2444, FileName: 0545.exe, DirPath: \Device\HarddiskVc
[+] Process Terminated: Process ffffb90c212360c0, ImageFileName: dllhost.exe
[+] Process Terminated: PID 1972, PPID:1972, PTID:312
[*] Create Mutant: PID: 1972, TID: 312, KMUTANT: 0xffffb90c2268d970
[*] Create Mutant: PID: 1972, TID: 312, KMUTANT: 0xffffb90c2268dc70
[*] Create Mutant: PID: 792, TID: 3256, KMUTANT: 0xffffb90c2268d4f0
[+] Thread Created: PID:4796, TID:6324, PPID:4, PTID:36
[*] Create Mutant: PID: 792, TID: 3256, KMUTANT: 0xffffb90c2268d4f0
[+] Thread Terminated: PID:5972, TID:3004, PPID:5972, PTID:3004
[+] Thread Terminated: PID:5972, TID:456, PPID:5972, PTID:456
[+] Thread Terminated: PID:5972, TID:1168, PPID:5972, PTID:1168
[+] Thread Terminated: PID:6012, TID:4640, PPID:6012, PTID:4640
[+] Thread Terminated: PID:6700, TID:7892, PPID:6700, PTID:7892
[+] Thread Terminated: PID:2284, TID:4912, PPID:2284, PTID:4912
[+] Thread Created: PID:924, TID:3432, PPID:924, PTID:7220
[+] Thread Terminated: PID:2284, TID:8076, PPID:2284, PTID:8076
[+] Thread Created: PID:924, TID:1092, PPID:924, PTID:3432
[+] Thread Terminated: PID:2528, TID:4508, PPID:2528, PTID:4508
[+] IRP_MN_QUERY_DIRECTORY: PID:924, TID:1092, FileName: 21.220.1024.0005, DirPath: \Device\Ha
```

```
*BUSY* Debuggee is running...
```

Name	Date modified	Type	Size
0545		Application	960 KB

1 item 1 item selected 959 KB

msedgewebvie...		23,252 K	3,628 K	5548 Microsoft Edge WebView2	Microsoft Corporation
Microsoft.Photos.exe	Susp...	40,120 K	35,132 K	4148	
RuntimeBroker.exe	< 0.01	4,992 K	19,052 K	5128 Runtime Broker	Microsoft Corporation
YourPhone.exe	Susp...	26,752 K	19,568 K	1376	Microsoft Corporation
RuntimeBroker.exe		1,988 K	12,044 K	1804 Runtime Broker	Microsoft Corporation

CPU Usage: 45.70% Commit Charge: 24.29% Processes: 132 Physical Usage: 28.99%

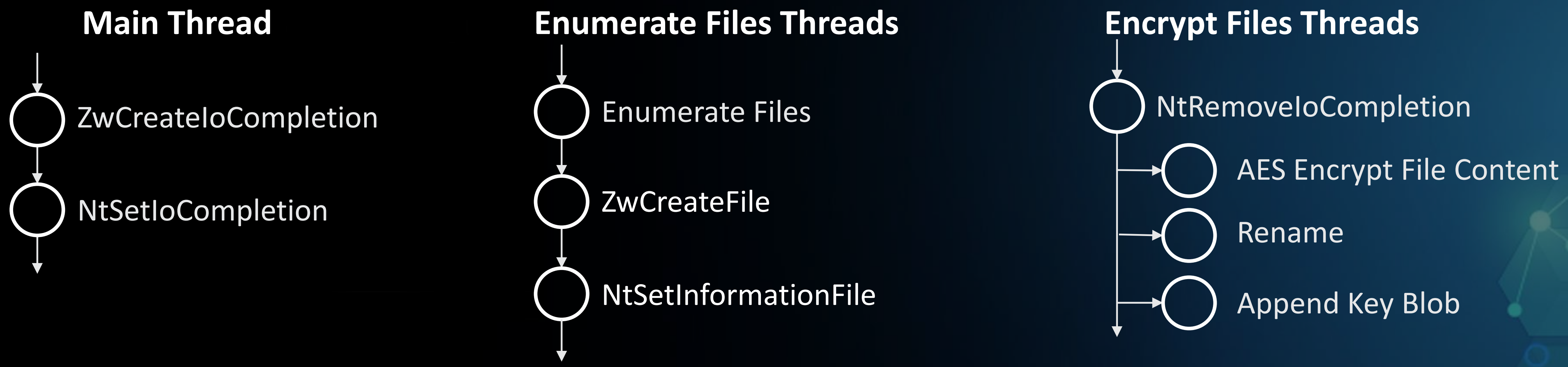
Windows 11 Pro
Build 22000.co_release.210604-1628

10:38 PM
5/12/2022

To return to your computer, press Ctrl+Alt.

txOne networks

Ransomware Encrypted Sequence Detection – LockBit2.0



Main Thread

- ZwCreateIoCompletion
- NtSetIoCompletion

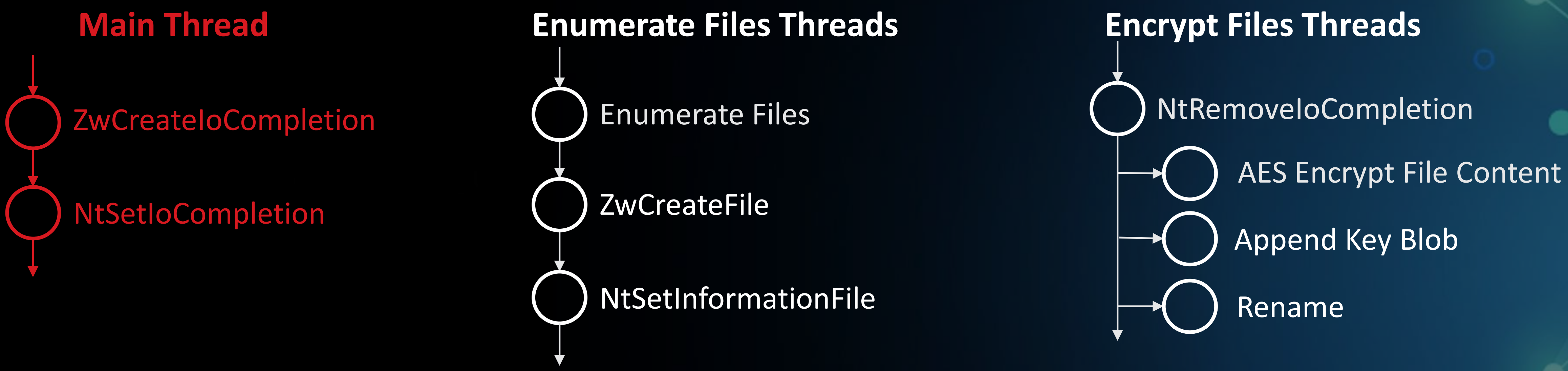
Enumerate Files Threads

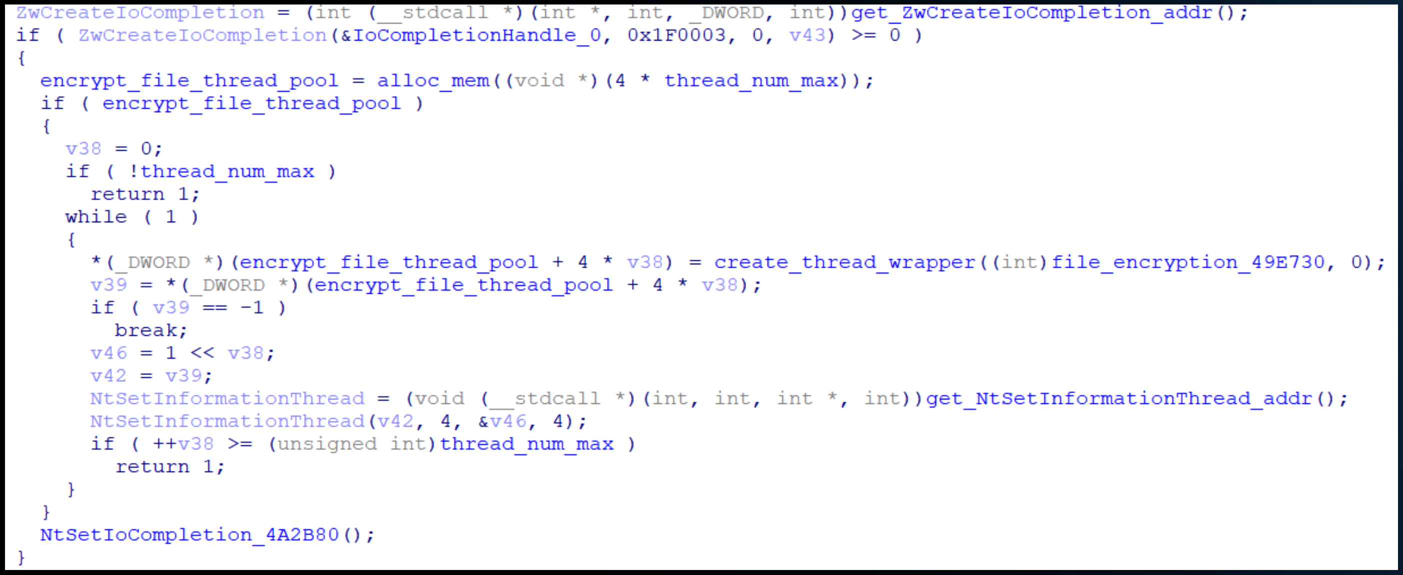
- Enumerate Files
- ZwCreateFile
- NtSetInformationFile

Encrypt Files Threads

- NtRemoveIoCompletion
  - AES Encrypt File Content
  - Rename
  - Append Key Blob

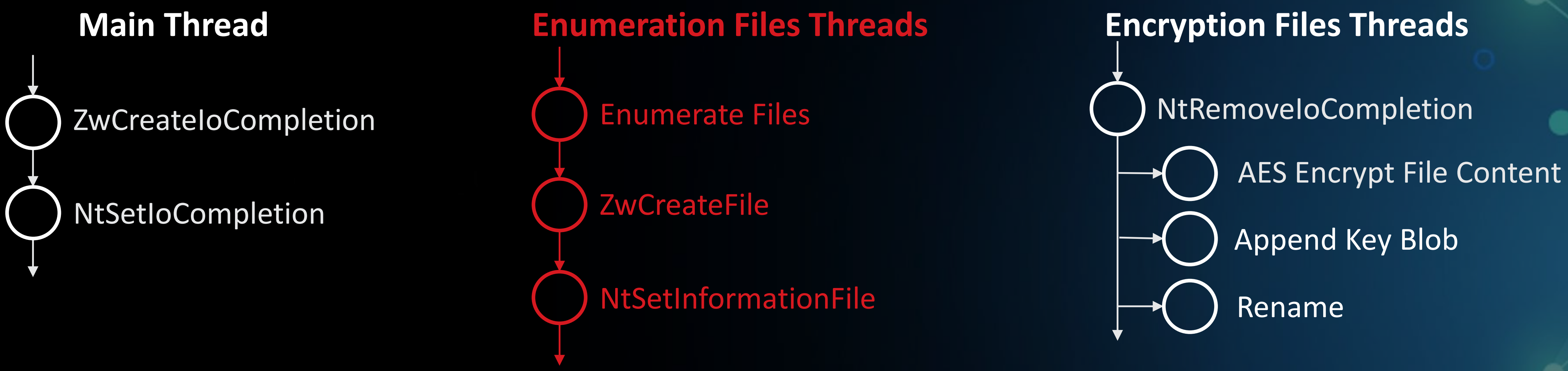
Ransomware Encrypted Sequence Detection – LockBit2.0





```
ZwCreateIoCompletion = (int (__stdcall *)(int *, int, _DWORD, int))get_ZwCreateIoCompletion_addr();
if ( ZwCreateIoCompletion(&IoCompletionHandle_0, 0x1F0003, 0, v43) >= 0 )
{
  encrypt_file_thread_pool = alloc_mem((void *)(4 * thread_num_max));
  if ( encrypt_file_thread_pool )
  {
    v38 = 0;
    if ( !thread_num_max )
      return 1;
    while ( 1 )
    {
      *(_DWORD *)(encrypt_file_thread_pool + 4 * v38) = create_thread_wrapper((int)file_encryption_49E730, 0);
      v39 = *(_DWORD *)(encrypt_file_thread_pool + 4 * v38);
      if ( v39 == -1 )
        break;
      v46 = 1 << v38;
      v42 = v39;
      NtSetInformationThread = (void (__stdcall *)(int, int, int *, int))get_NtSetInformationThread_addr();
      NtSetInformationThread(v42, 4, &v46, 4);
      if ( ++v38 >= (unsigned int)thread_num_max )
        return 1;
    }
  }
  NtSetIoCompletion_4A2B80();
}
```

Ransomware Encrypted Sequence Detection – LockBit2.0



Main Thread

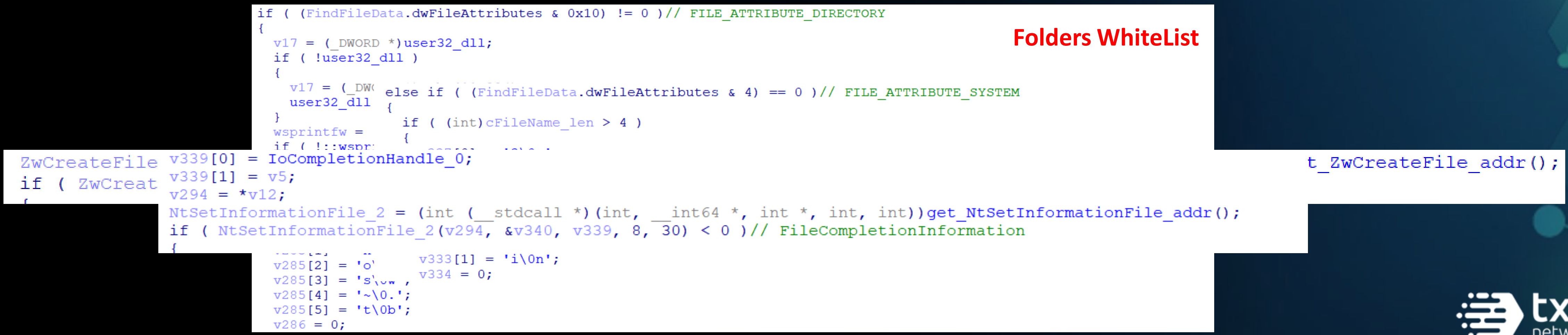
- ZwCreateIoCompletion
- NtSetIoCompletion

Enumeration Files Threads

- Enumerate Files
- ZwCreateFile
- NtSetInformationFile

Encryption Files Threads

- NtRemoveIoCompletion
  - AES Encrypt File Content
  - Append Key Blob
  - Rename



Folders WhiteList

```
if ( (FindFileData.dwFileAttributes & 0x10) != 0 )// FILE_ATTRIBUTE_DIRECTORY
{
  v17 = (_DWORD *)user32_dll;
  if ( !user32_dll )
  {
    v17 = (_DW
    user32_dll
  }
  wsprintfw =
  if ( !::wspr
```

```
else if ( (FindFileData.dwFileAttributes & 4) == 0 )// FILE_ATTRIBUTE_SYSTEM
{
  if ( (int)cFileName_len > 4 )
  {
```

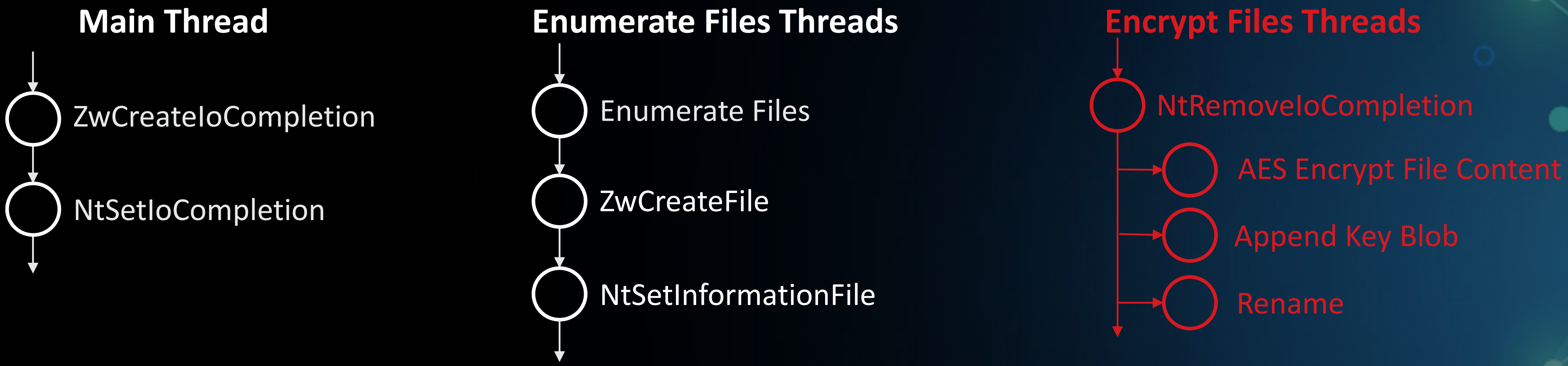
```
ZwCreateFile                                                t_ZwCreateFile_addr();
if ( ZwCreat
```

```
v339[0] = IoCompletionHandle_0;
v339[1] = v5;
v294 = *v12;
NtSetInformationFile_2 = (int (__stdcall *)(int, __int64 *, int *, int, int))get_NtSetInformationFile_addr();
if ( NtSetInformationFile_2(v294, &v340, v339, 8, 30) < 0 )// FileCompletionInformation
{
```

```
v285[2] = 'o'
v285[3] = 's\
v285[4] = '~\0.';
v285[5] = 't\0b';
v286 = 0;
```

```
v333[1] = 'i\0n';
v334 = 0;
```

Ransomware Encrypted Sequence Detection – LockBit2.0



Main Thread

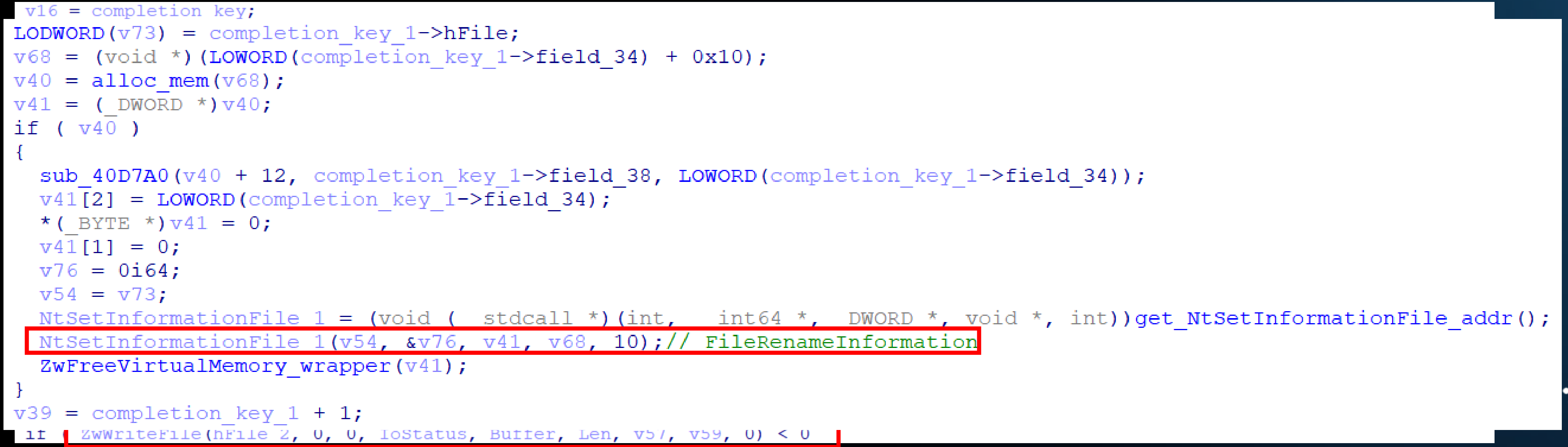
- ZwCreateIoCompletion
- NtSetIoCompletion

Enumerate Files Threads

- Enumerate Files
- ZwCreateFile
- NtSetInformationFile

Encrypt Files Threads

- NtRemoveIoCompletion
  - AES Encrypt File Content
  - Append Key Blob
  - Rename



```
 v16 = completion_key;
LODWORD(v73) = completion_key_1->hFile;
v68 = (void *)(LOWORD(completion_key_1->field_34) + 0x10);
v40 = alloc_mem(v68);
v41 = (_DWORD *)v40;
if ( v40 )
{
  sub_40D7A0(v40 + 12, completion_key_1->field_38, LOWORD(completion_key_1->field_34));
  v41[2] = LOWORD(completion_key_1->field_34);
  *(_BYTE *)v41 = 0;
  v41[1] = 0;
  v76 = 0i64;
  v54 = v73;
  NtSetInformationFile_1 = (void (__stdcall *)(int, __int64 *, _DWORD *, void *, int))get_NtSetInformationFile_addr();
  NtSetInformationFile_1(v54, &v76, v41, v68, 10);// FileRenameInformation
  ZwFreeVirtualMemory_wrapper(v41);
}
v39 = completion_key_1 + 1;
 if ( ZwWriteFile(hFile_2, 0, 0, IoStatus, Buffer, Len, v57, v59, 0) < 0
```

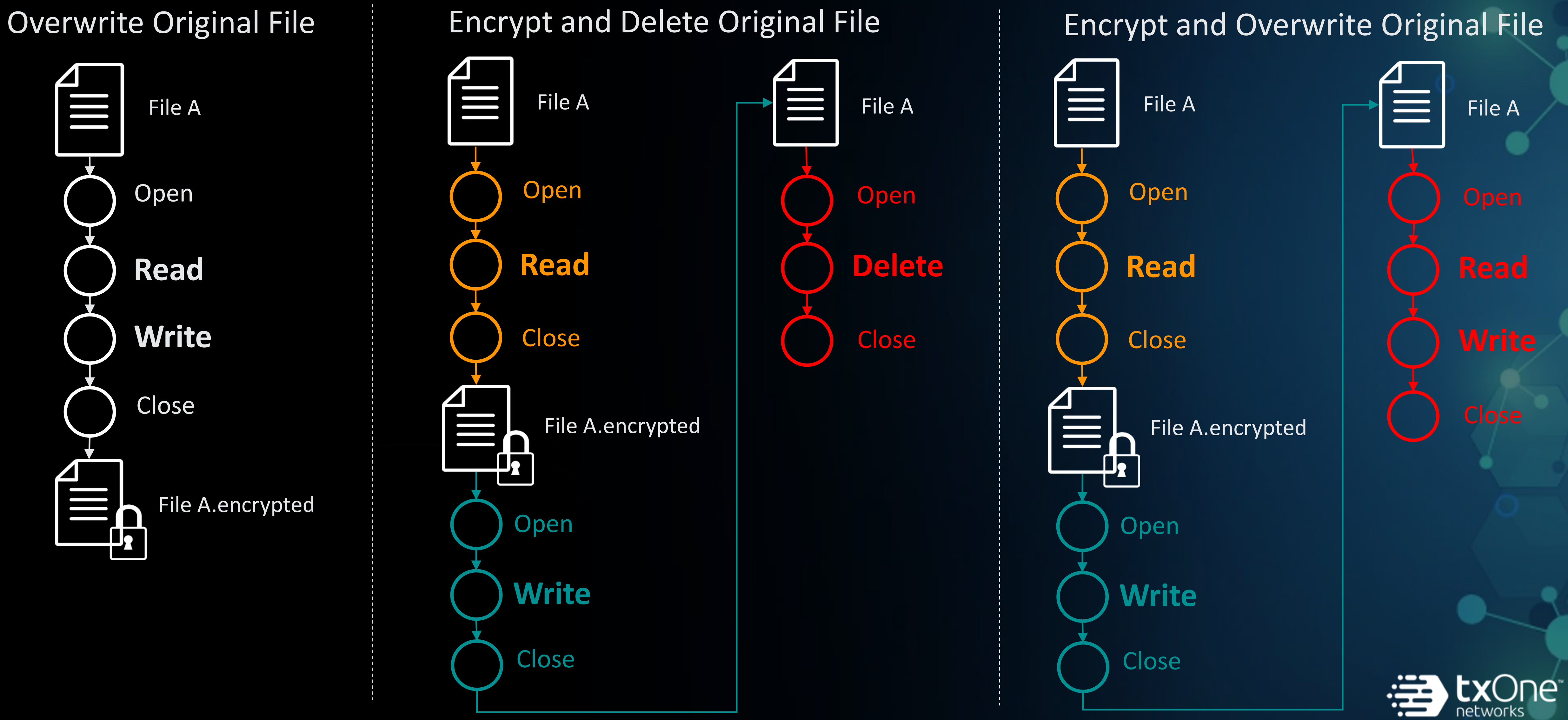
Ransomware Encryption Sequence Detection

Sequence	Ransomware
R-M-W	WannaCry
R-W-M	Ryuk , RagnarLocker, ColdLock , Egregor, Conti v2, RansomExx, DoppelPaymer, Revil, EKANS
R-W-SF	Mount Locker, LockBit 2.0
M-R-W	Darkside, Babuk Locker, Lockergoga
MP-FF	Bad Rabbit

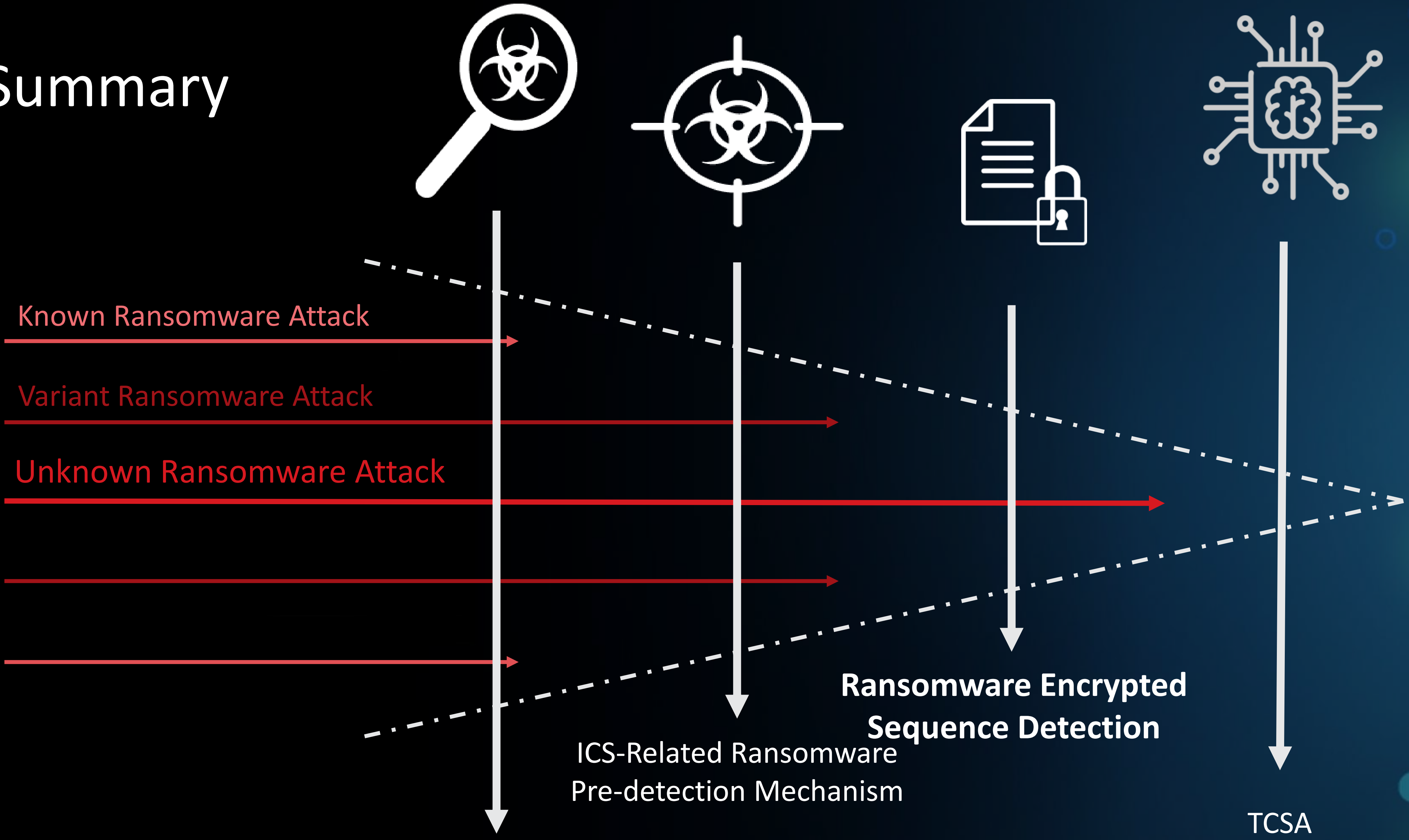
File Encryption Flags:

SF: SetFileInformationByHandle/NtSetInformationFile
R: ReadFile ; W: WriteFile ; M: MoveFile
MP: MapViewOfFile, FF: FlushViewOfFile

Ransomware Encrypted Sequence Detection



Summary

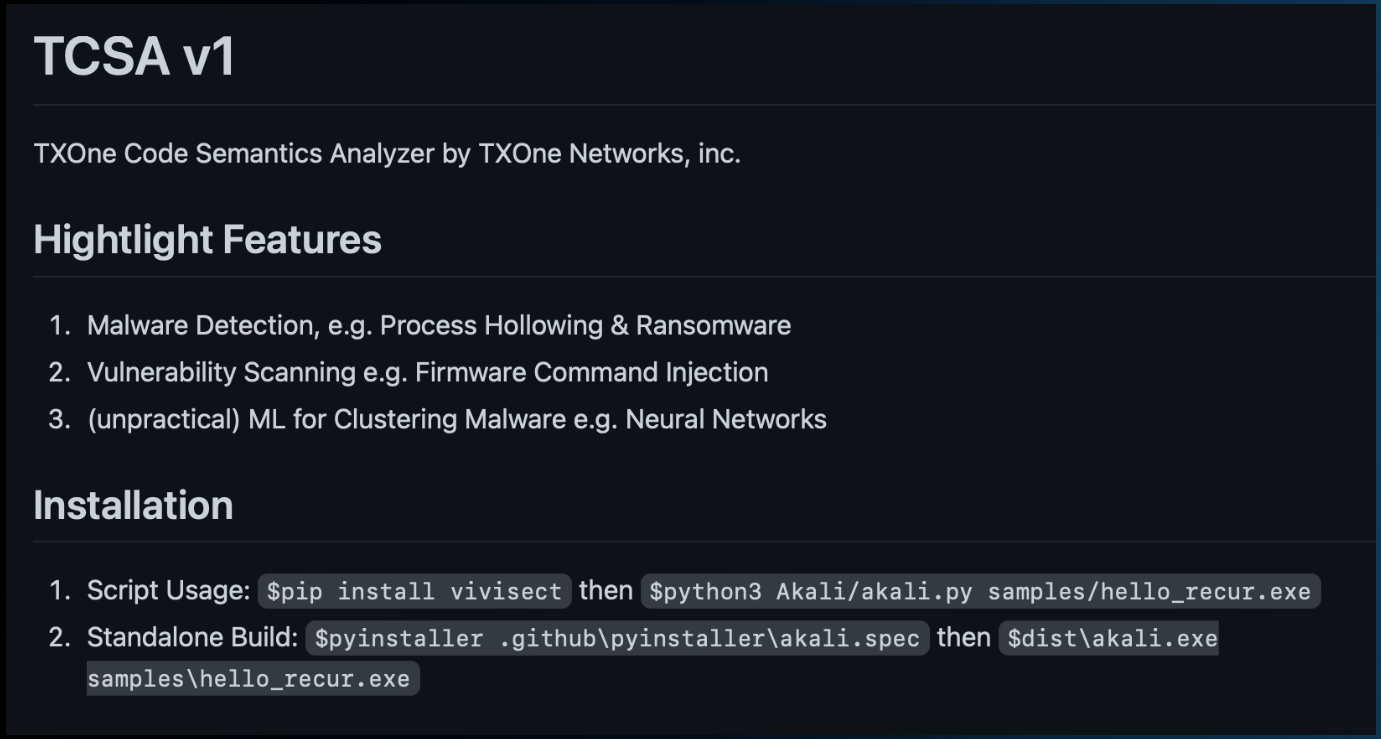


Known Ransomware Attack
Variant Ransomware Attack
Unknown Ransomware Attack
Ransomware Encrypted Sequence Detection
ICS-Related Ransomware Pre-detection Mechanism
TCSA
Known Ransonware Scanning

Protect mission-critical Assets in order to keep Operation running with ZERO TRUST approach

"**NEVER TRUST, ALWAYS VERIFY**"

Opensource to Infosec Community



TCSA v1

TXOne Code Semantics Analyzer by TXOne Networks, inc.

Hightlight Features

1. Malware Detection, e.g. Process Hollowing & Ransomware
2. Vulnerability Scanning e.g. Firmware Command Injection
3. (unpractical) ML for Clustering Malware e.g. Neural Networks

Installation

1. Script Usage: `$pip install vivisect` then `$python3 Akali/akali.py samples/hello_recur.exe`
2. Standalone Build: `$pyinstaller .github\pyinstaller\akali.spec` then `$dist\akali.exe samples\hello_recur.exe`

https://github.com/TXOne-Networks/TCSA

txOne™
networks