txOne networks *The Leader of OT Zero Trust*

No More Ransomware in Critical Infrastructure!

不要再讓勒索軟體肆虐關鍵基礎設施了！

Mars Cheng, Hank Chen

September 22, 2022

Mars Cheng and Hank Chen

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

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

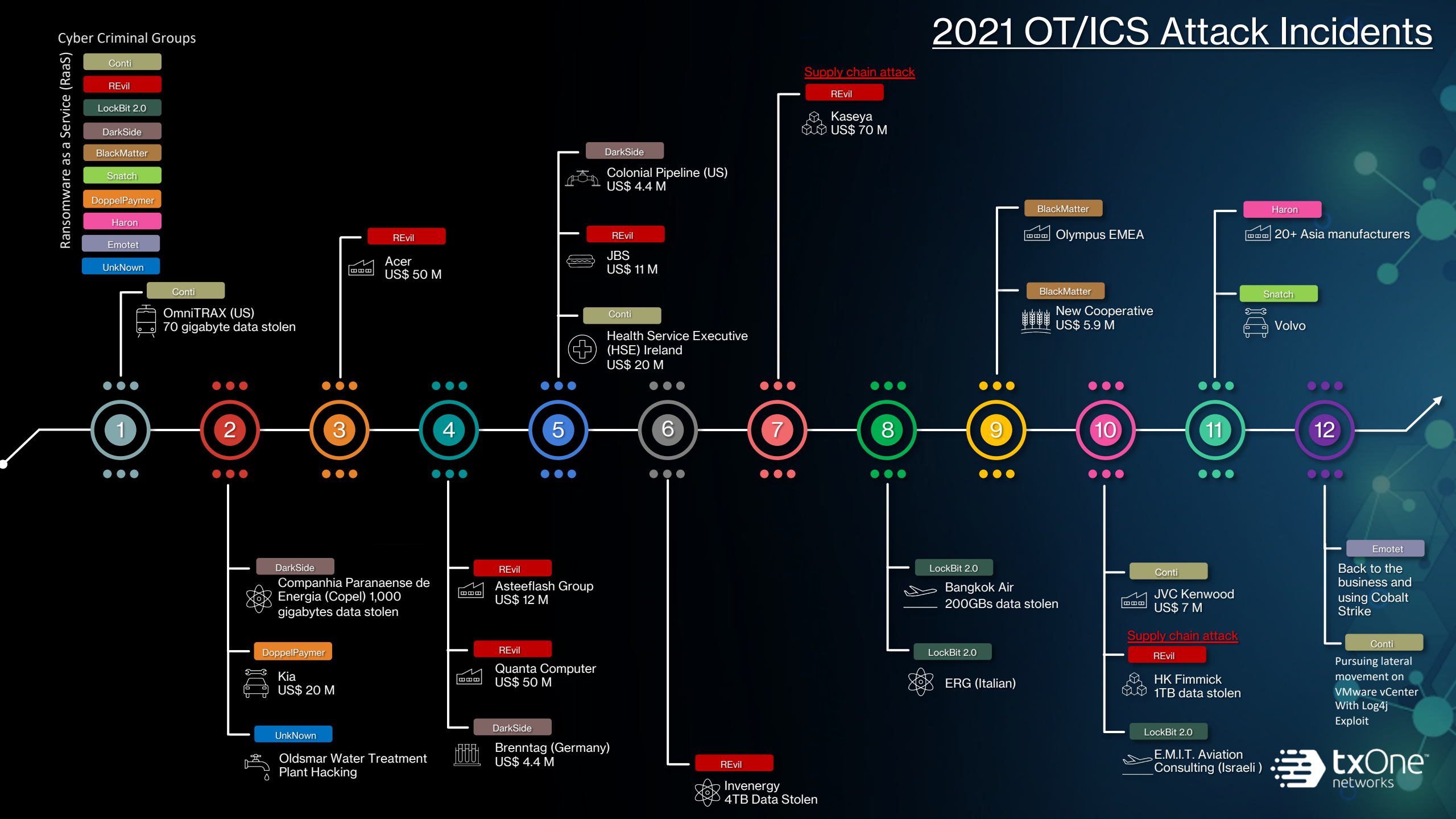
txOne networks

Outline

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

ICS Threat in Review

2021 OT/ICS Attack Incidents



2021 OT/ICS Attack Incidents Highlights

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

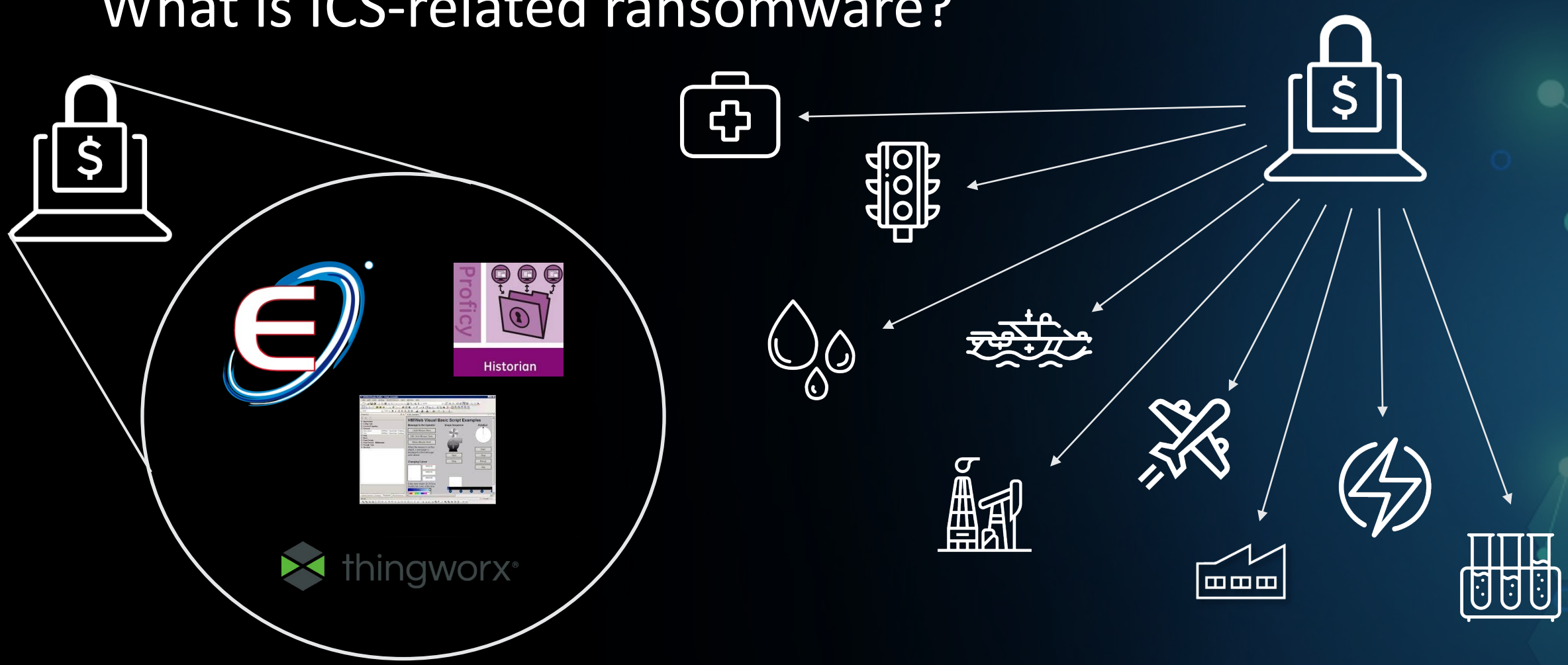
- Improving the nation’s cybersecurity
- Supply Chain and Software Bills of Materials (SBOMs)

Leverage zero-day vulnerabilities

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

txOne networks

What is ICS-related ransomware?



Targeted ICS-Specific resources such as applications and certificates

The ransomware impacted the ICS environment before

txOne networks

What are the Characteristics of Ransomware that Affects Critical Infrastructure?

The ICS-Related Ransomware Matrix

	WannaCry	Ryuk	Lockergoga	EKANS	RagnarLocker	ColdLock	Egregor	Conti v2
First Seen	2017/1/16	2018/8/22	2019/3/8	2019/12/26	2020/4/13	2020/5/4	2020-12-06	2021/1/29
Code-Signed	No	No	Yes	No	No	No	No	No
Anti-Analysis	Yes	N/A	N/A	N/A	Yes	N/A	Yes	Yes
Language Check	No	N/A	N/A	N/A	Yes	N/A	Yes	N/A
Kill Process/Services	Yes	Yes	Yes	Yes	Yes	Yes	Yes	N/A
Persistence	Yes	Yes	N/A	No	N/A	N/A	N/A	N/A
Privilege Escalation	N/A	Yes	N/A	N/A	Yes	N/A	N/A	N/A
Lateral Movement	Yes	N/A	No	No	N/A	N/A	N/A	N/A
Anti-Recovery	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
Atomic-Check	Yes	Yes	Yes	Yes	Yes	Yes	N/A	Yes
File Encryption	R-M-W	R-E-W-M	M-R-W	R-W-W-M	R-E-W-M	R-E-W-M	R-E-W-M	R-E-W-M
Partial Encryption	N/A	N/A	N/A	N/A	N/A	Yes	N/A	Yes
Cipher Suite	AES 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
Configuration File	Yes	No	No	No	Yes	No	Yes	No
Command-Line Arguments	Yes	No	Yes	No	Yes	No	Yes	Yes

File Encryption Flags:
SF: SetFileInformationByHandle/NtSetInformationFile
R: ReadFile ; W: WriteFile ; M: MoveFile
E: Encrypt ; MP: MapViewOfFile

txOne networks

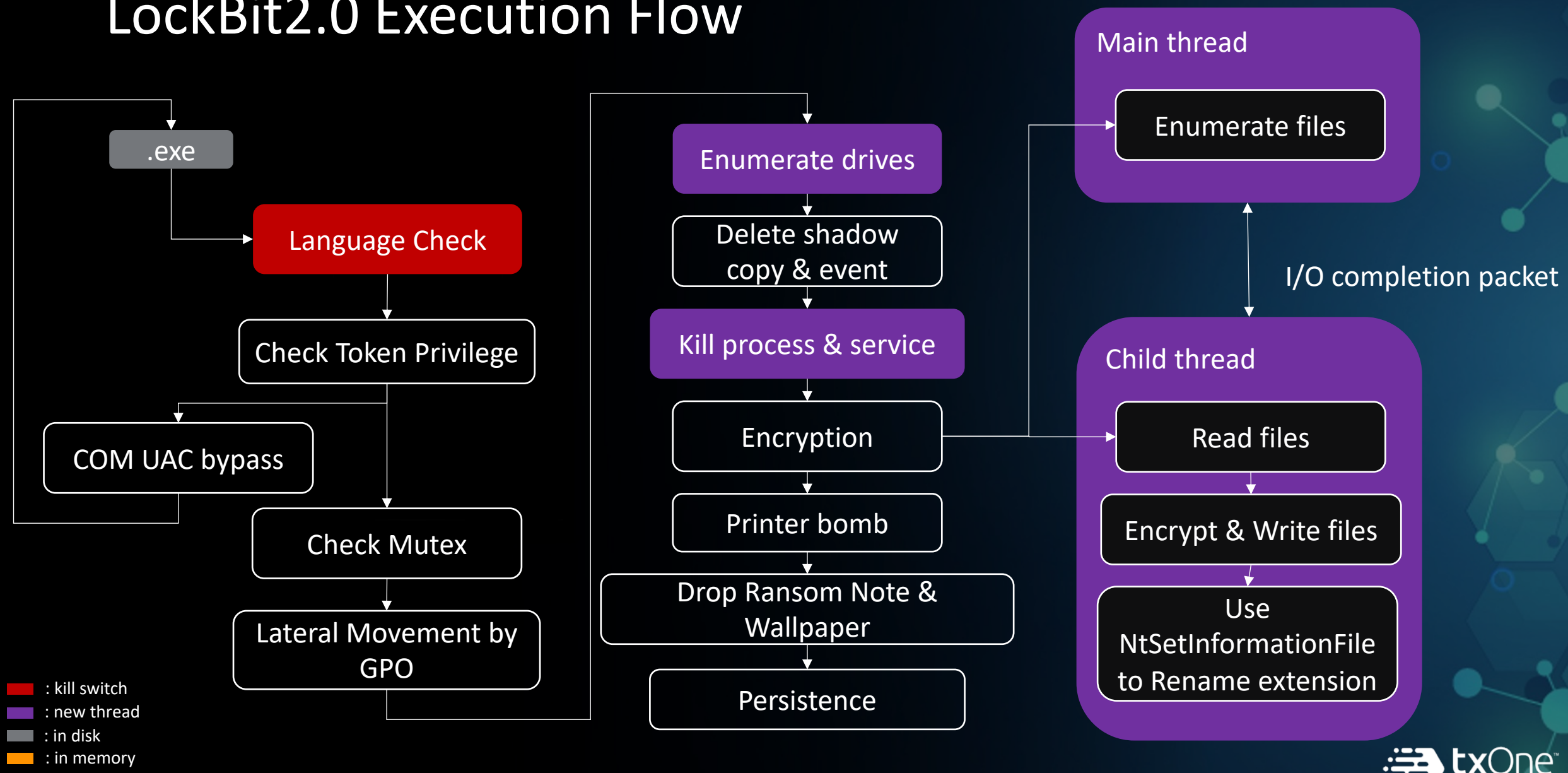
The ICS-Related Ransomware Matrix

	Bad Rabbit	Mount Locker	RansomExx	DoppelPaymer	Darkside	Babuk Locker	REvil	LockBit 2.0
First Seen	2020/10/25	2021/05/11	2020/06/14	2019/10/15	2021/02/03	2021/09/06	2021/7/3	2021/8/3
Code-Signed	Yes	No	No	Yes	No	No	No	No
Anti-Analysis	N/A	N/A	N/A	Yes	N/A	N/A	N/A	Yes
Language Check	No	N/A	No	No	Yes	N/A	N/A	Yes
Kill Process/Services	N/A	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Persistence	Yes	N/A	N/A	N/A	N/A	No	Yes	Yes
Privilege Escalation	N/A	N/A	N/A	Yes	N/A	No	Yes	Yes
Lateral Movement	Yes	Yes	N/A	No	N/A	N/A	N/A	Yes
Anti-Recovery	N/A	N/A	Yes	Yes	N/A	N/A	Yes	Yes
Atomic-Check	N/A	Yes	N/A	N/A	Yes	N/A	Yes	Yes
File Encryption	MP-E	R-E-W-SF	R-E-W-M	R-E-W-M	M-R-E-W	M-R-E-W	R-E-W-M	R-E-W-SF
Partial Encryption	No	Yes	N/A	N/A	Yes	N/A	Yes	Yes
Cipher Suite	AES RSA	ChaCha20 RSA-2048	AES-256-ECB RSA-4096	AES-256-CBC RSA-2048	Salsa20 RSA-1024	HC128 Curve25519-ECDH	Salsa20 RSA	AES-128-CBC Curve25519-ECDH
Configuration File	N/A	No	No	N/A	Yes	No	Yes	No
Command-Line Arguments	Yes	Yes	No	N/A	Yes	Yes	Yes	Yes

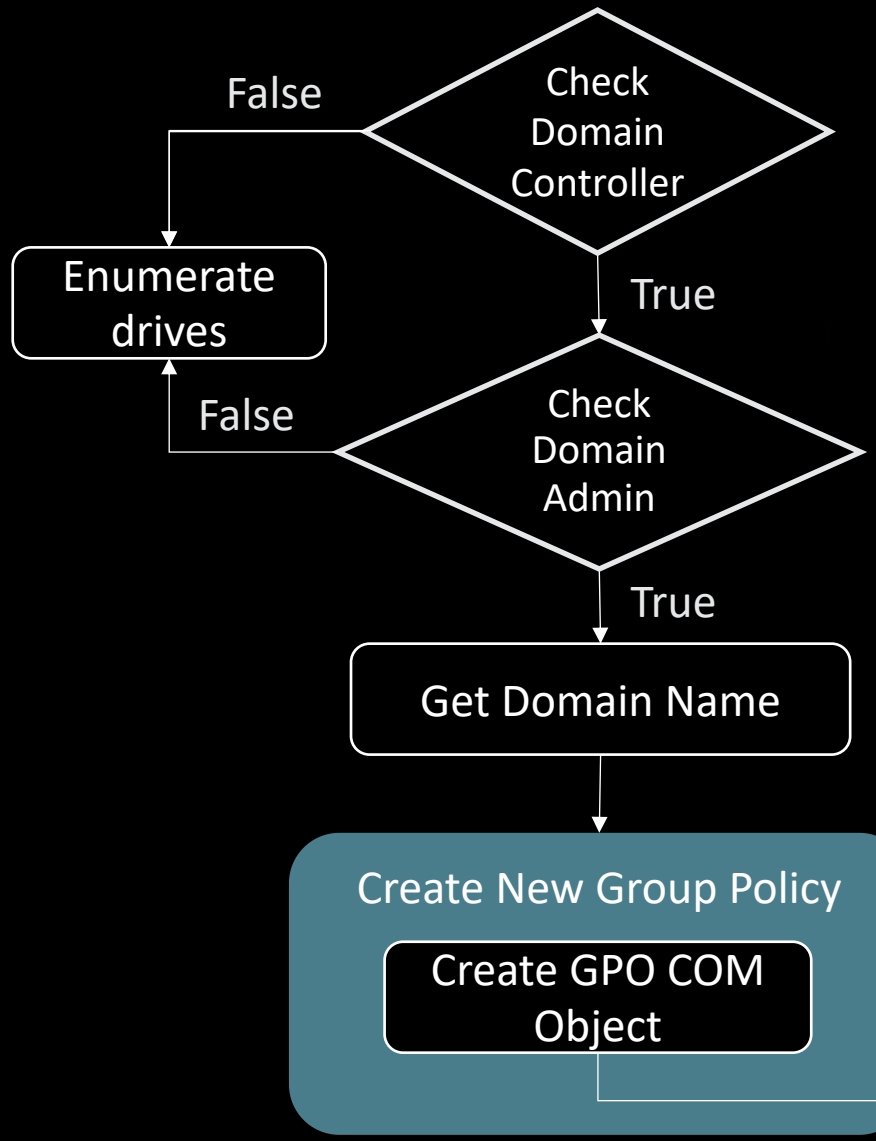
File Encryption Flags:
SF: SetFileInformationByHandle/NtSetInformationFile
R: ReadFile ; W: WriteFile ; M: MoveFile
E: Encrypt ; MP: MapViewOfFile

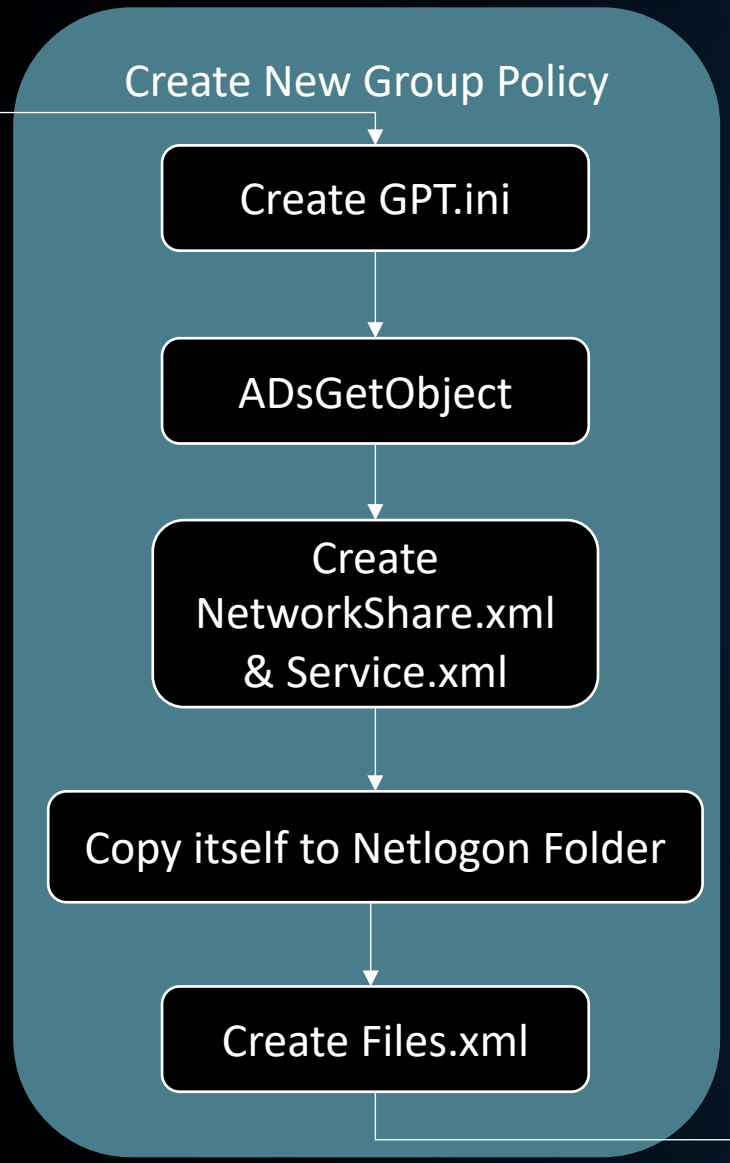
txOne networks

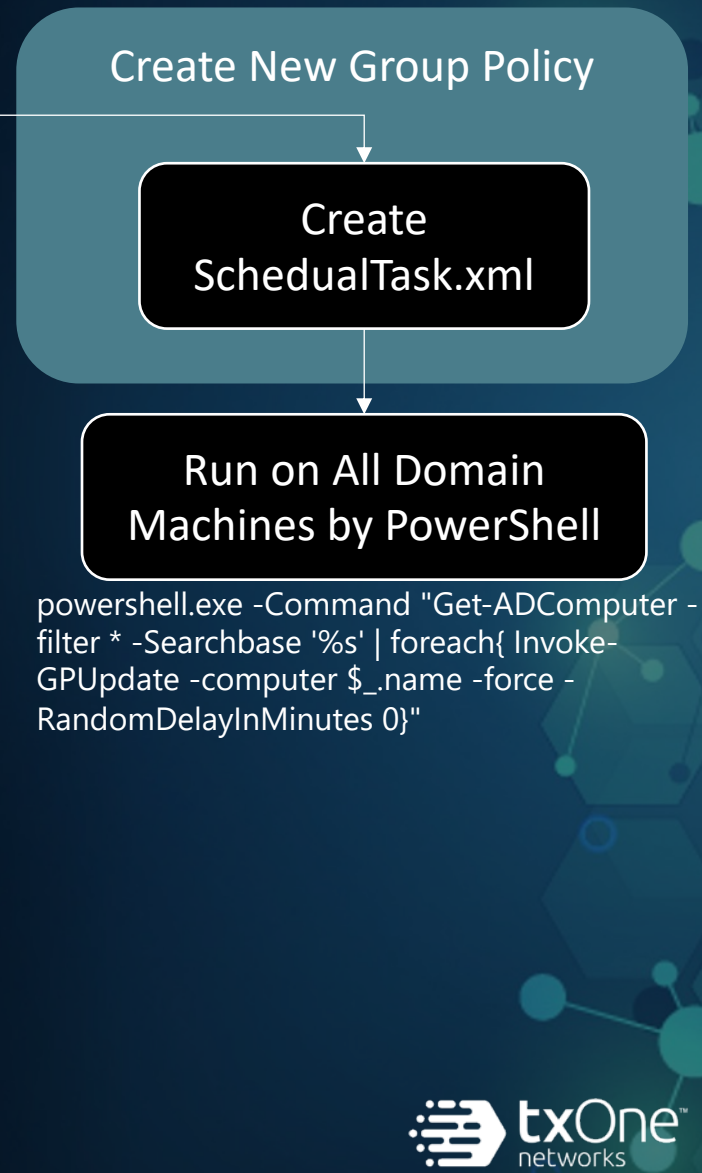
LockBit2.0 Execution Flow



AD GPO Propagation Techniques in LockBit 2.0



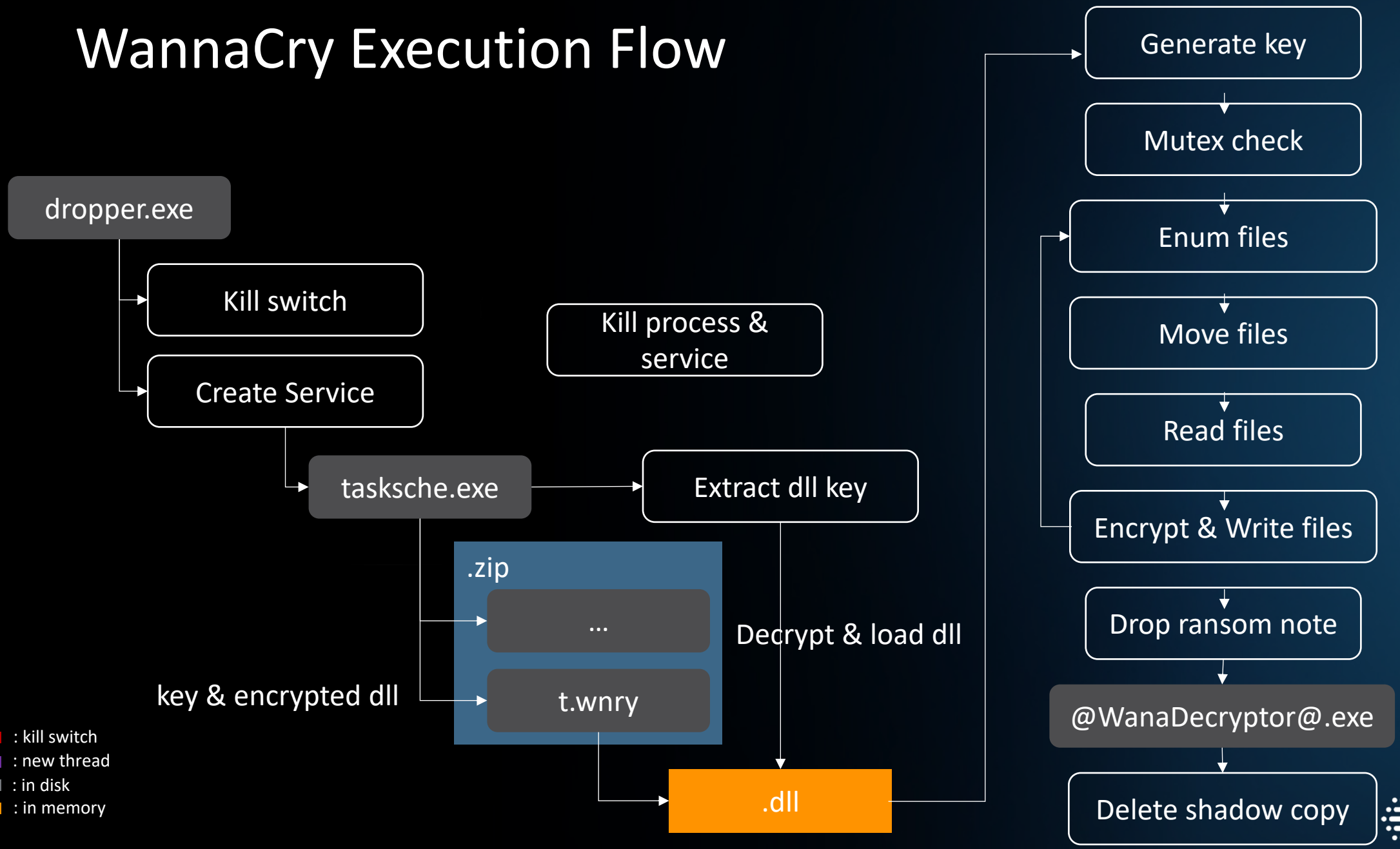





```
powershell.exe -Command "Get-ADComputer -filter * -Searchbase '%s' | foreach{ Invoke-GPUpdate -computer $_.name -force -RandomDelayInMinutes 0}"
```

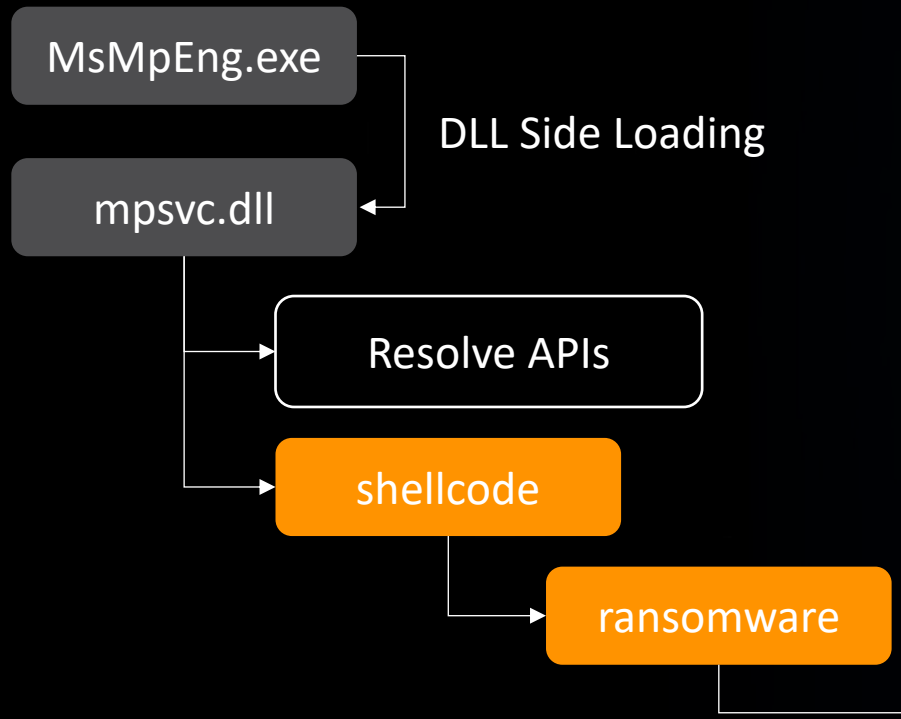
txOne networks

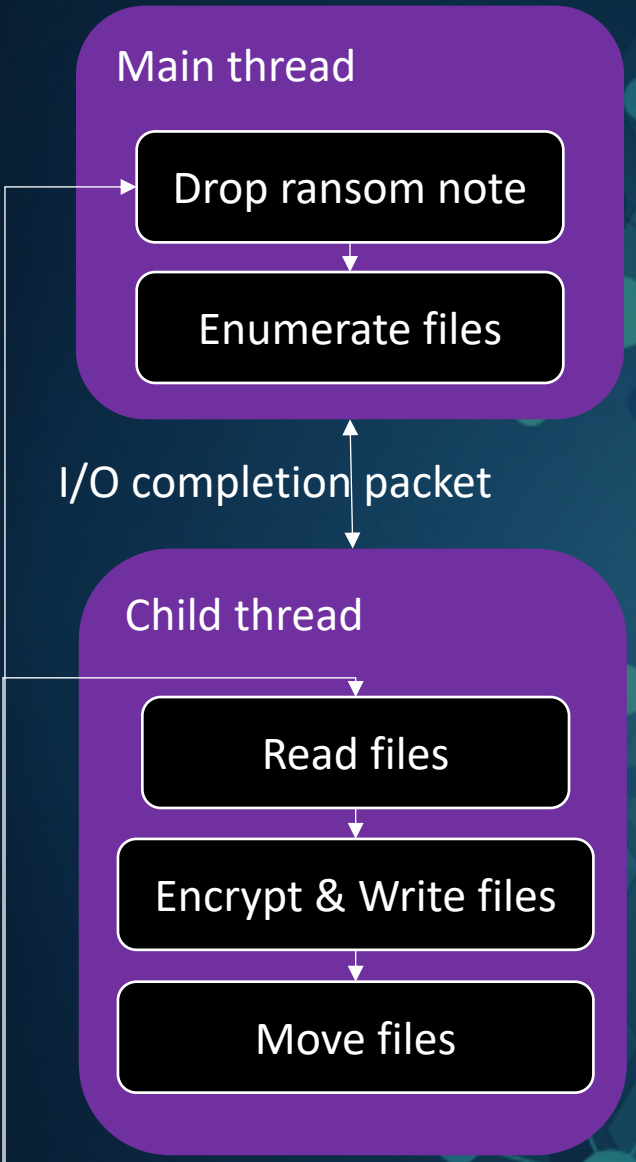
WannaCry Execution Flow



txOne networks

REvil Execution Flow

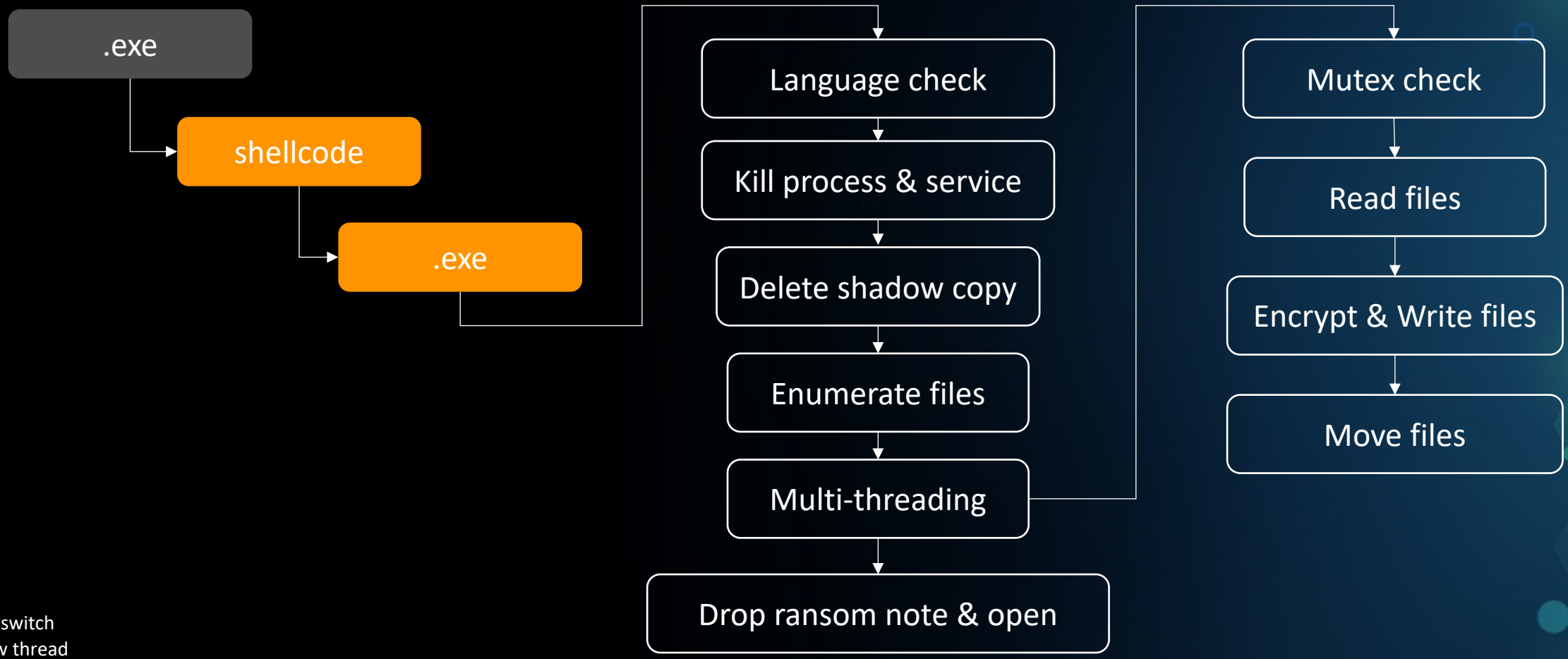




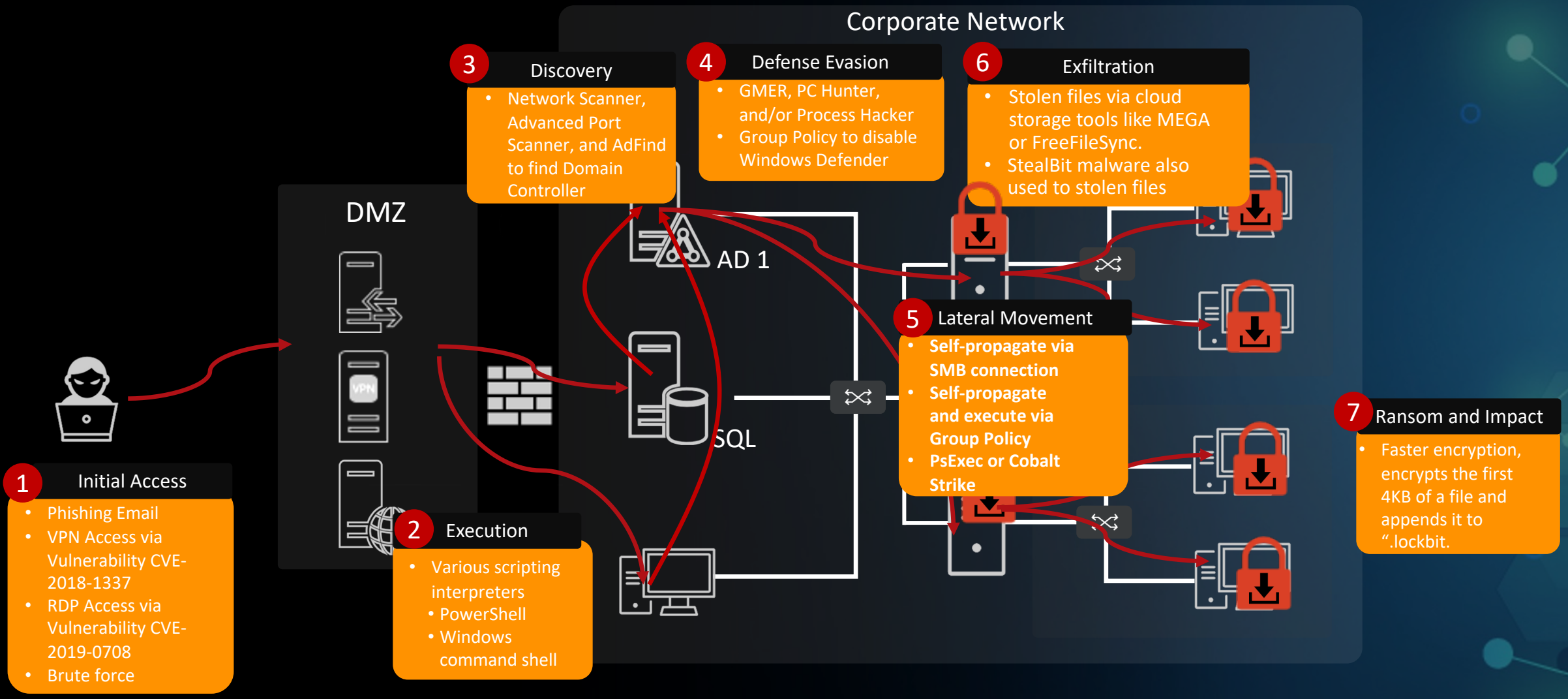
: kill switch
: new thread
: in disk
: in memory

txOne networks

RagnarLocker Execution Flow



Common Attack Path of ICS-Related Ransomware



txOne networks

The Common Characteristics of ICS-Related Ransomware

1. Kill Process/Services
2. Anti-Recovery
3. Atomic-Check
4. Command-Line Arguments
5. Anti-Analysis
6. Partial Encryption
7. Privilege Escalation
8. Persistence
9. Language Check
10. Code-Signed

txOne networks

How can Critical Infrastructure Mitigate the Threat of Ransomware?

txOne networks

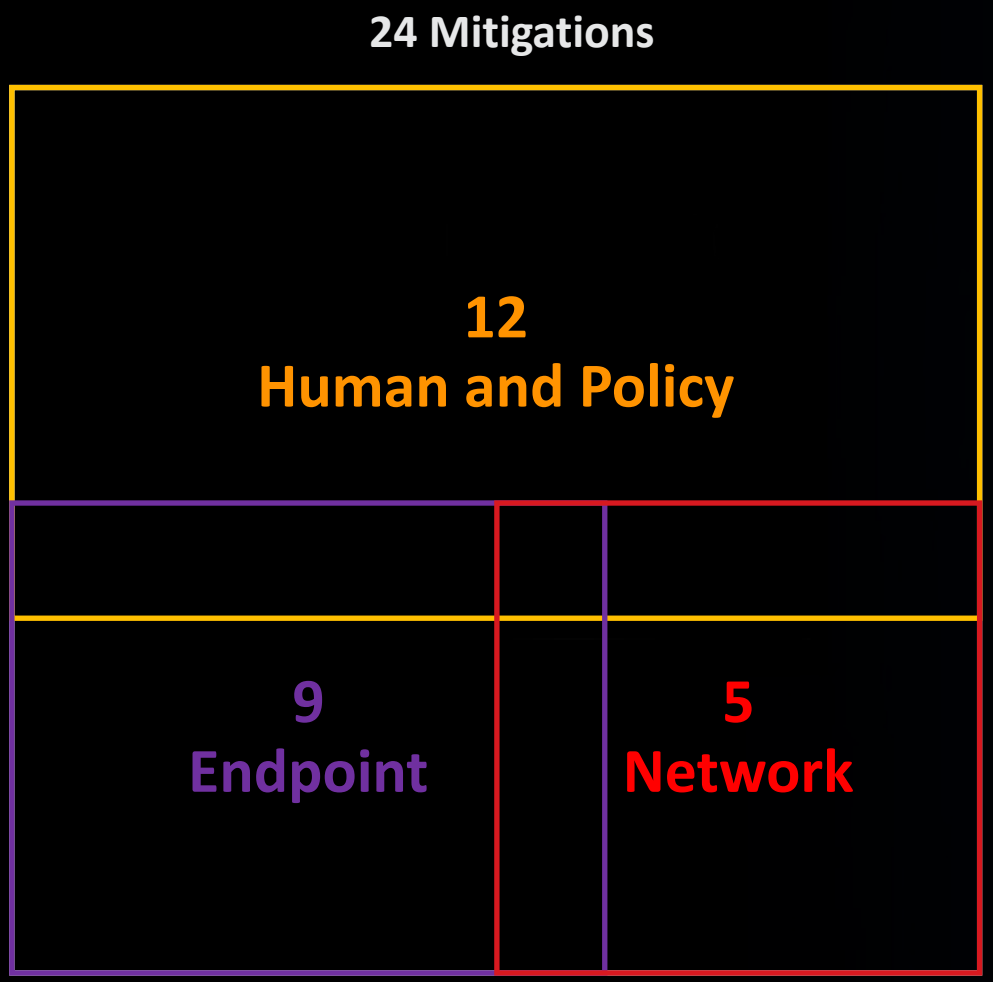
Ransomware Techniques Based on MITRE ATT&CK for ICS

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

txOne networks

Apply the 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)

txOne networks

The Practical Ransomware Mitigation Strategies in the ICS World

The Difference of Enterprise and ICS

Type	ICS Environment	Enterprise Environment
Virus Pattern Update	**Hardly**	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

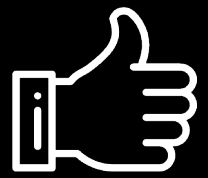
txOne networks

The Practical Ransomware Mitigation Strategies in the ICS World

Known Ransoware Scanning

ICS-Related 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

txOne networks

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 language check failed

```
int __stdcall main_language_check()
{
  int count; // esi
  int KeyboardLayoutList; // eax
  int nBuff; // edi
  _WORD *lpList; // eax
  _WORD *keyboard_layouts; // ebx
  int LANG_CHECK; // ecx

  count = 0;
  check_UI_language();
  KeyboardLayoutList = mw_GetKeyboardLayoutList(0, 0);
  nBuff = KeyboardLayoutList;
  if ( !KeyboardLayoutList )
    return 0;
  lpList = (_WORD *)safe_RtlAllocateHeap(4 * KeyboardLayoutList);
  keyboard_layouts = lpList;
  if ( !lpList )
    return 0;
  if ( !mw_GetKeyboardLayoutList(nBuff, (HKL *)lpList) || nBuff <= 0 )
  {
LABEL_8:
    w_w_RtlFreeHeap((int)keyboard_layouts);
    return 0;
  }
  while ( !check_keyboard_layout(keyboard_layouts[2 * count]) || !LANG_CHECK )
  {
    if ( ++count >= nBuff )
      goto LABEL_8;
  }
  return 1;
```

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

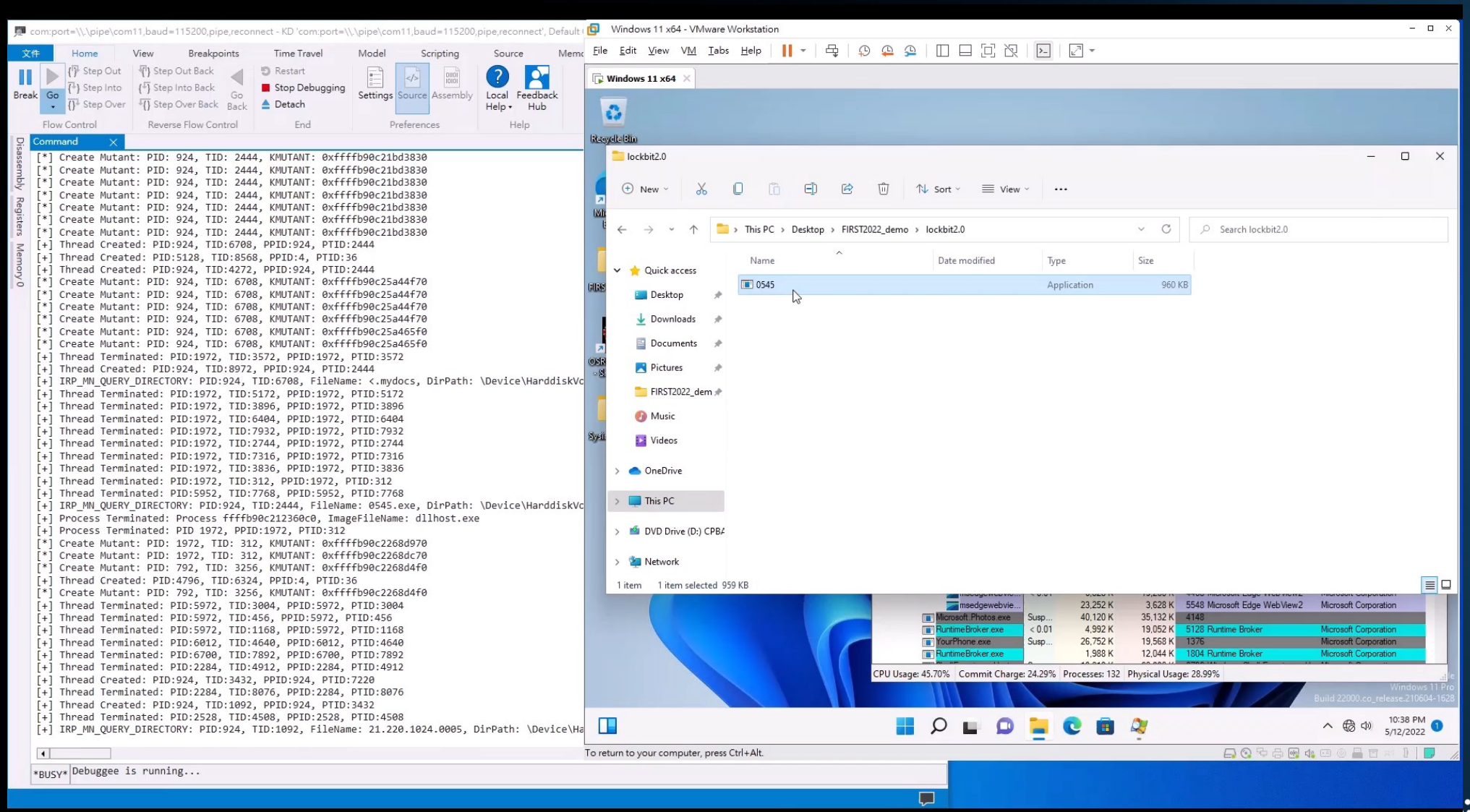
If delete shadow copy failed

```
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
```

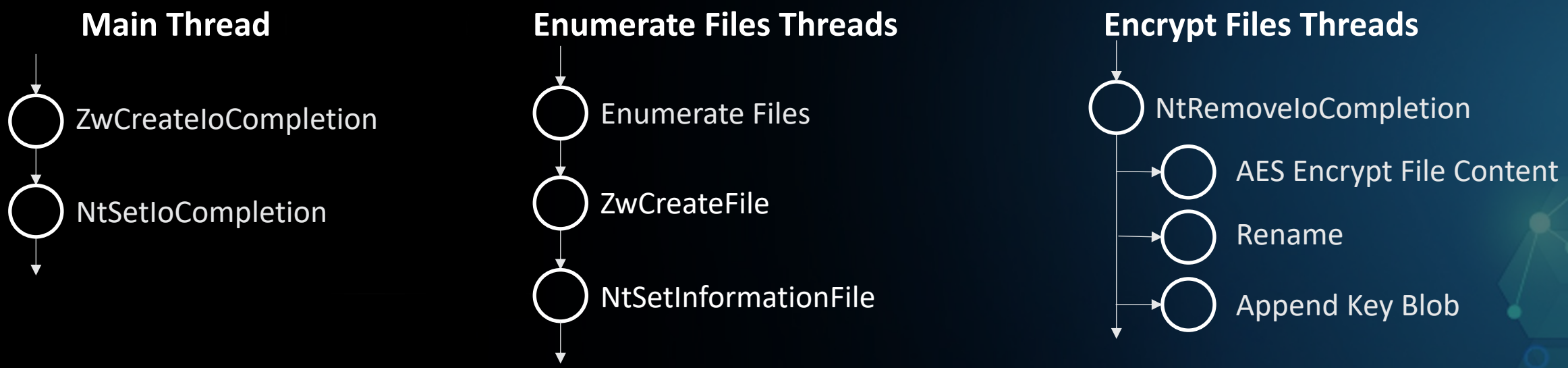
Ryuk

txOne networks

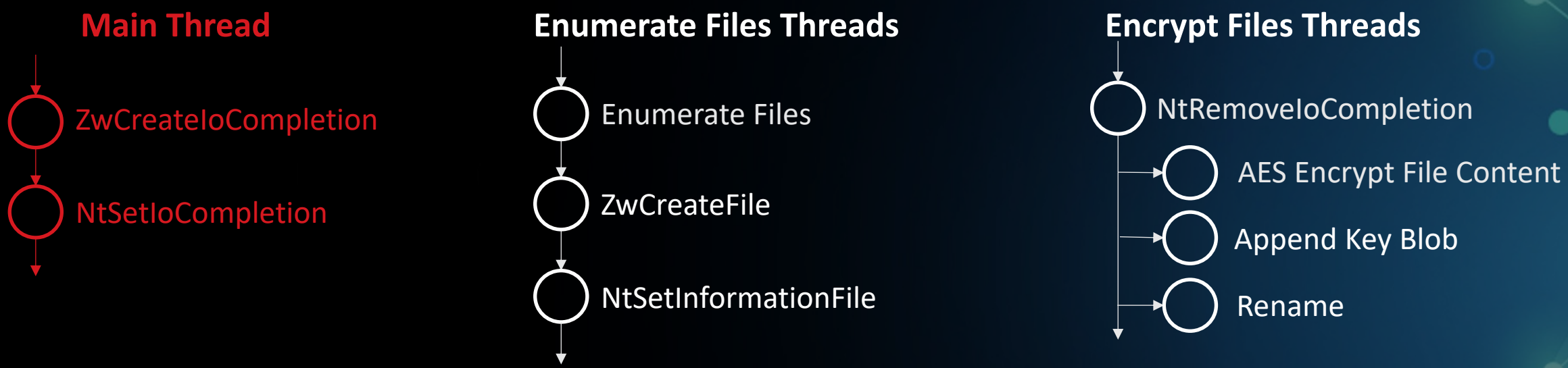
ICS-Related Ransomware Pre-detection Mechanism



Ransomware Encrypted Sequence Detection – LockBit2.0



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();
}
```

txOne networks

Ransomware Encrypted Sequence Detection – LockBit2.0

Main Thread

- ZwCreateIoCompletion
- NtSetIoCompletion

Enumerate Files Threads

- Enumerate Files
- ZwCreateFile
- NtSetInformationFile

Encrypt Files Threads

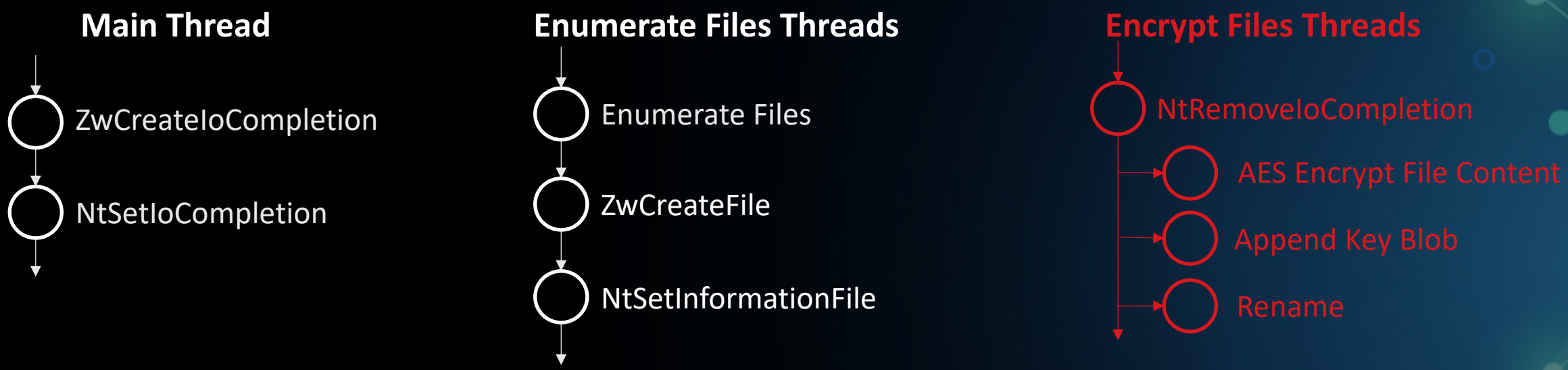
- NtRemoveIoCompletion
  - AES Encrypt File Content
  - Append Key Blob
  - Rename

Folders WhiteList

```
if ( (FindFileData.dwFileAttributes & 0x10) != 0 )// FILE_ATTRIBUTE_DIRECTORY
{
  v17 = (_DWORD *)user32_dll;
  if ( !user32_dll )
  {
    v17 = (_DWORD  else if ( (FindFileData.dwFileAttributes & 4) == 0 )// FILE_ATTRIBUTE_SYSTEM
    user32_dll =   {
  }                  if ( (int)cFileName_len > 4 )
  wsprintfw = (ch    {
```

```
ZwCreateFil v339[0] = IoCompletionHandle_0;                                                    et_ZwCreateFile_addr();
if ( ZwCrea 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\0d      v334 = 0;
              v285[3] = 's\0w';
              v285[4] = '~\0.';
              v285[5] = 't\0b';
              v286 = 0;
```

Ransomware Encrypted Sequence Detection – LockBit2.0




```
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 Encrypted Sequence Detection

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

File Encryption Flags:

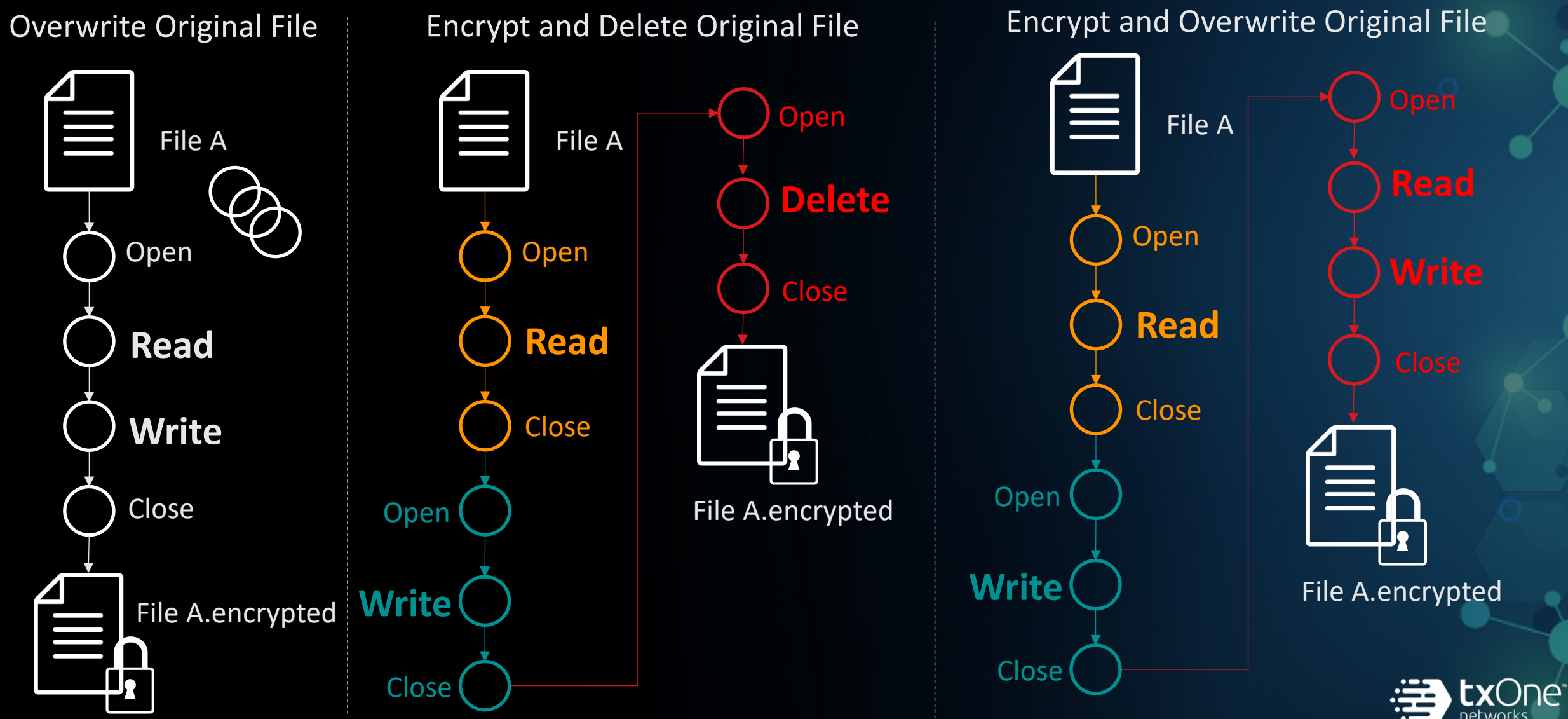
SF: SetFileInformationByHandle/NtSetInformationFile

R: ReadFile ; W: WriteFile ; M: MoveFile

E: Encrypt ; MP: MapViewOfFile

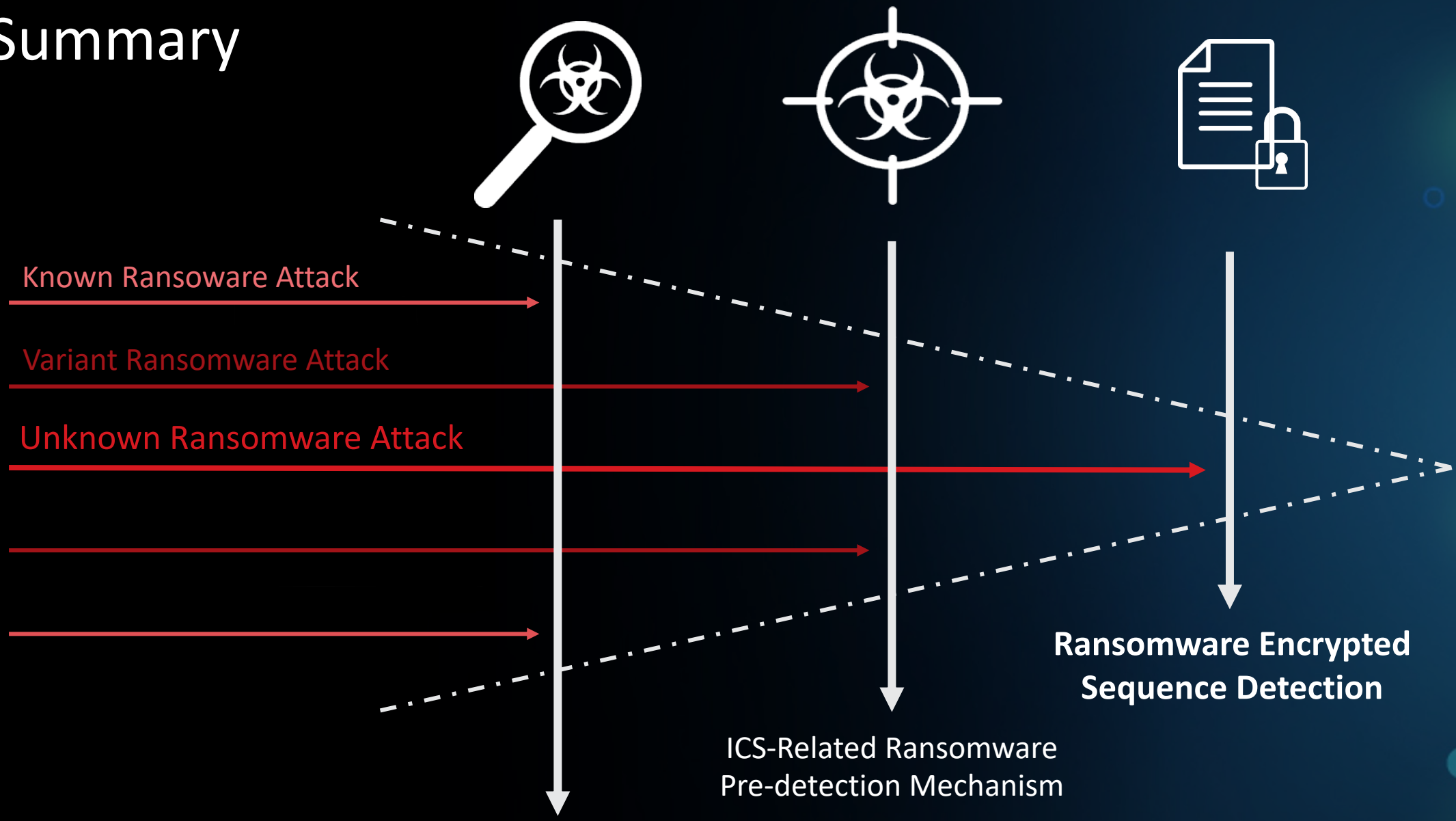
txOne networks

Ransomware Encrypted Sequence Detection



txOne networks

Summary



txOne networks


Protect mission-critical Assets in order to keep Operation running with ZERO TRUST approach
“NEVER TRUST, ALWAYS VERIFY”

txOne™
networks