Cyberwarfare: Novel Wipers used in Ukraine 2022

Ashu Sharma

Ryan Estes

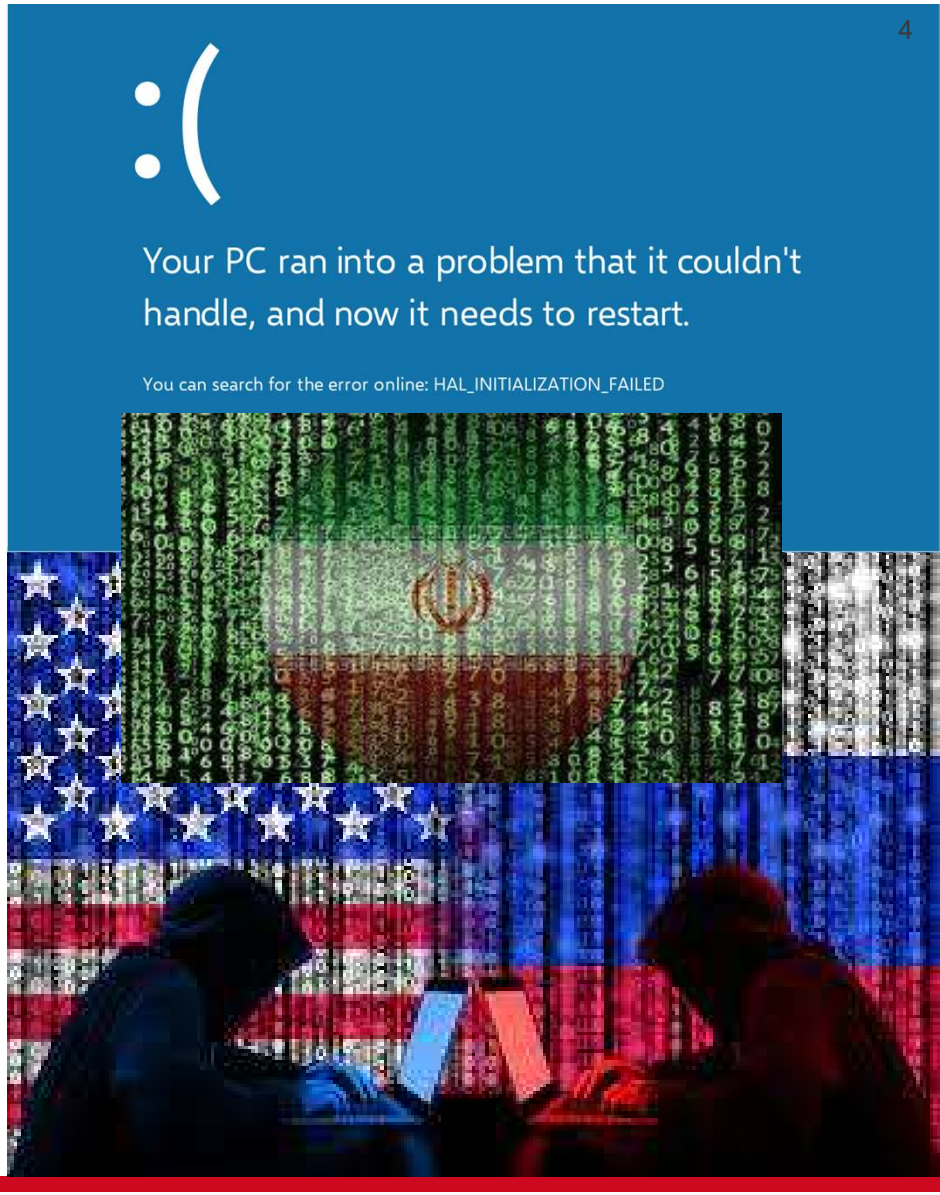
Agenda

- **Introduction**
  - How It Started
  - What is Cyberwarfare?
  - Threat Landscape
  - A New Battlefield
- **The Russian/Ukraine Conflict**
  - Threat Actors
  - Major Malware involved
  - Cyberwarfare Timeline
- **Technical Analysis**
  - ISAACWiper (Ryan)
  - Azov Ransomware (Ashu)
- **Threat Hunting**
  - YARA Rules
  - VirusTotal Query (Azov)
  - Sample Hashes
- **Q&A**
- **References**

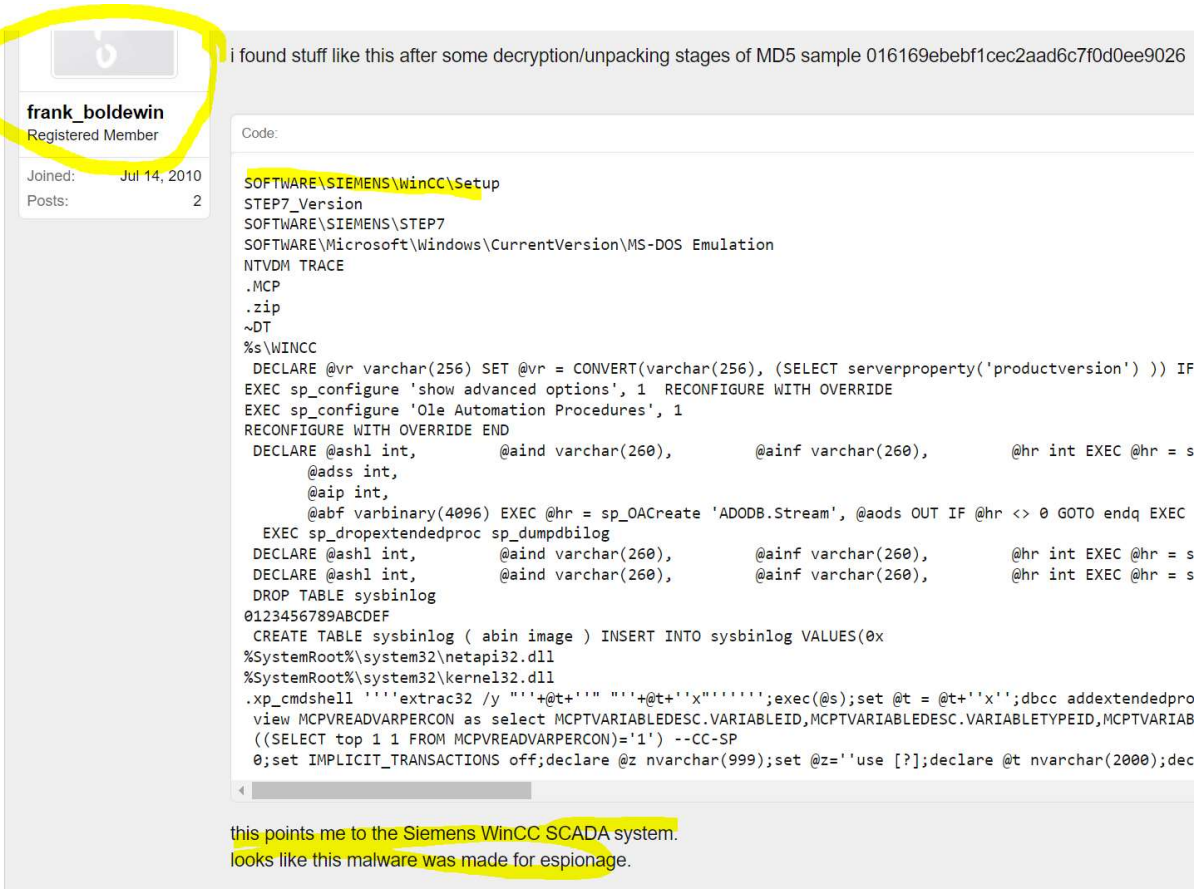

Introduction

How a New Era of Warfare Started

- A customer in Iran reported arbitrary BSODs and computer reboots and Responded with a Windows OS misconfiguration.
- Observed persistence.
- 58% of devices in Iran were infected and Nobody knew what this code was intended to do.
- Highly skilled hackers used Zero-day vulnerabilities.



How a New Era of Warfare Started



frank_boldewin
Registered Member

Joined: Jul 14, 2010
Posts: 2

i found stuff like this after some decryption/unpacking stages of MD5 sample 016169ebebf1cec2aad6c7f0d0ee9026

Code:

```
SOFTWARE\SIEMENS\WinCC\Setup
STEP7_Version
SOFTWARE\SIEMENS\STEP7
SOFTWARE\Microsoft\Windows\CurrentVersion\MS-DOS Emulation
NTVDM TRACE
.MCP
.zip
~DT
%s\WINCC
 DECLARE @vr varchar(256) SET @vr = CONVERT(varchar(256), (SELECT serverproperty('productversion') )) IF
EXEC sp_configure 'show advanced options', 1  RECONFIGURE WITH OVERRIDE
EXEC sp_configure 'Ole Automation Procedures', 1
RECONFIGURE WITH OVERRIDE END
 DECLARE @ashl int,         @aind varchar(260),         @ainf varchar(260),         @hr int EXEC @hr = s
       @adss int,
       @aip int,
       @abf varbinary(4096) EXEC @hr = sp_OACreate 'ADODB.Stream', @aods OUT IF @hr <> 0 GOTO endq EXEC
  EXEC sp_dropextendedproc sp_dumpdbilog
 DECLARE @ashl int,         @aind varchar(260),         @ainf varchar(260),         @hr int EXEC @hr = s
 DECLARE @ashl int,         @aind varchar(260),         @ainf varchar(260),         @hr int EXEC @hr = s
 DROP TABLE sysbinlog
0123456789ABCDEF
 CREATE TABLE sysbinlog ( abin image ) INSERT INTO sysbinlog VALUES(0x
%SystemRoot%\system32\netapi32.dll
%SystemRoot%\system32\kernel32.dll
.xp_cmdshell ''''extrac32 /y "''+@t+'" "''+@t+''x"''''''';exec(@s);set @t = @t+''x'';dbcc addextendedpro
 view MCPVREADVARPERCON as select MCPTVARIABLEDESC.VARIABLEID,MCPTVARIABLEDESC.VARIABLETYPEID,MCPTVARIAB
 ((SELECT top 1 1 FROM MCPVREADVARPERCON)='1') --CC-SP
 0;set IMPLICIT_TRANSACTIONS off;declare @z nvarchar(999);set @z=''use [?];declare @t nvarchar(2000);dec
```

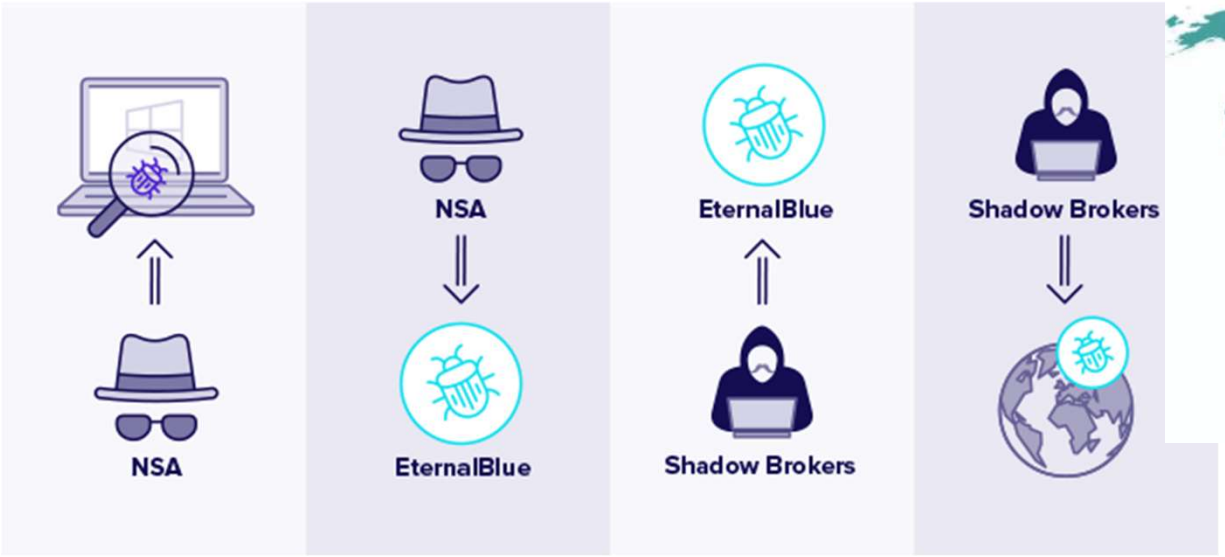
this points me to the Siemens WinCC SCADA system.
looks like this malware was made for espionage.

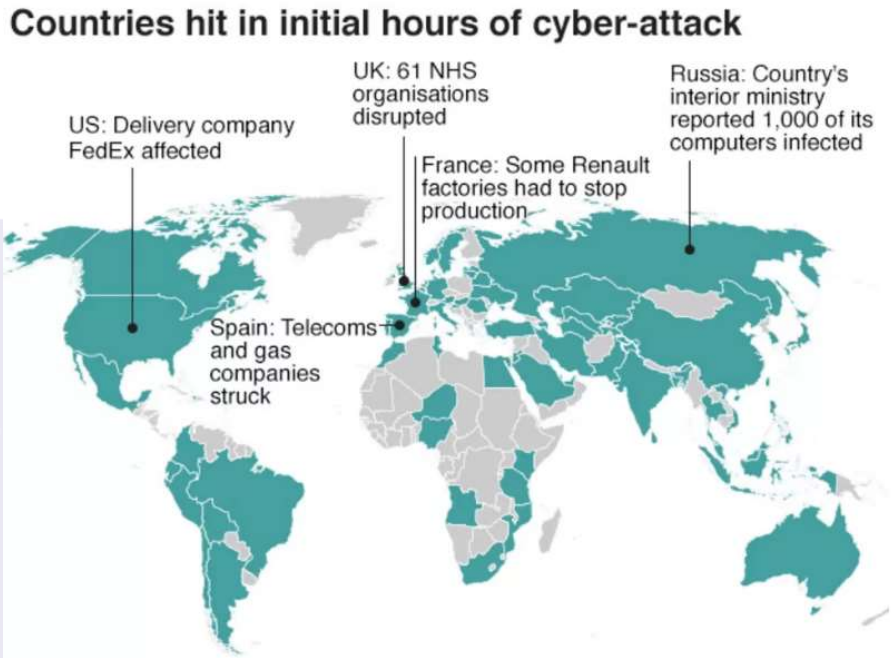
Early Days of Cyberwarfare

- The Stuxnet drivers were signed with genuine digital certificates from respected companies.
- Said; It was an option.
- And then Estates comes in business.
- Detections were delayed.
- Pay Exploit hackers; buy exploits and keep zero days.

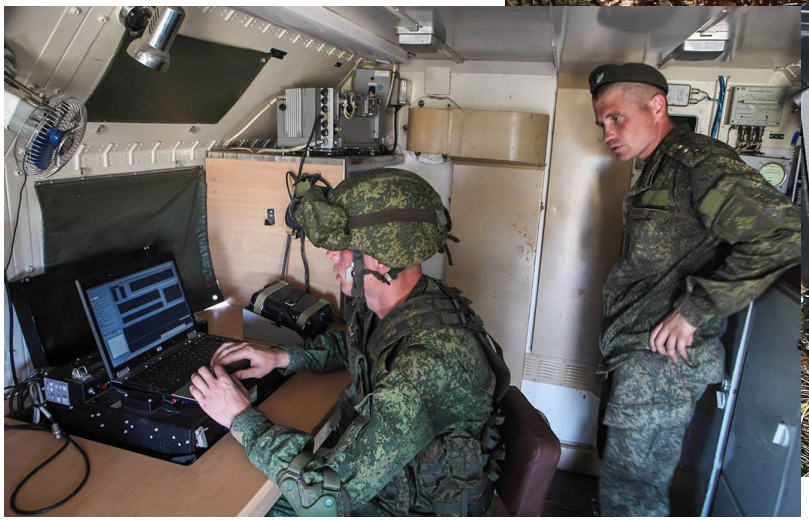
A Game of Exploits

> **Before it leaked, EternalBlue was one of the most useful exploits in the NSA's cyber arsenal ... used in countless intelligence-gathering and counterterrorism missions.**
>
> — New York Times



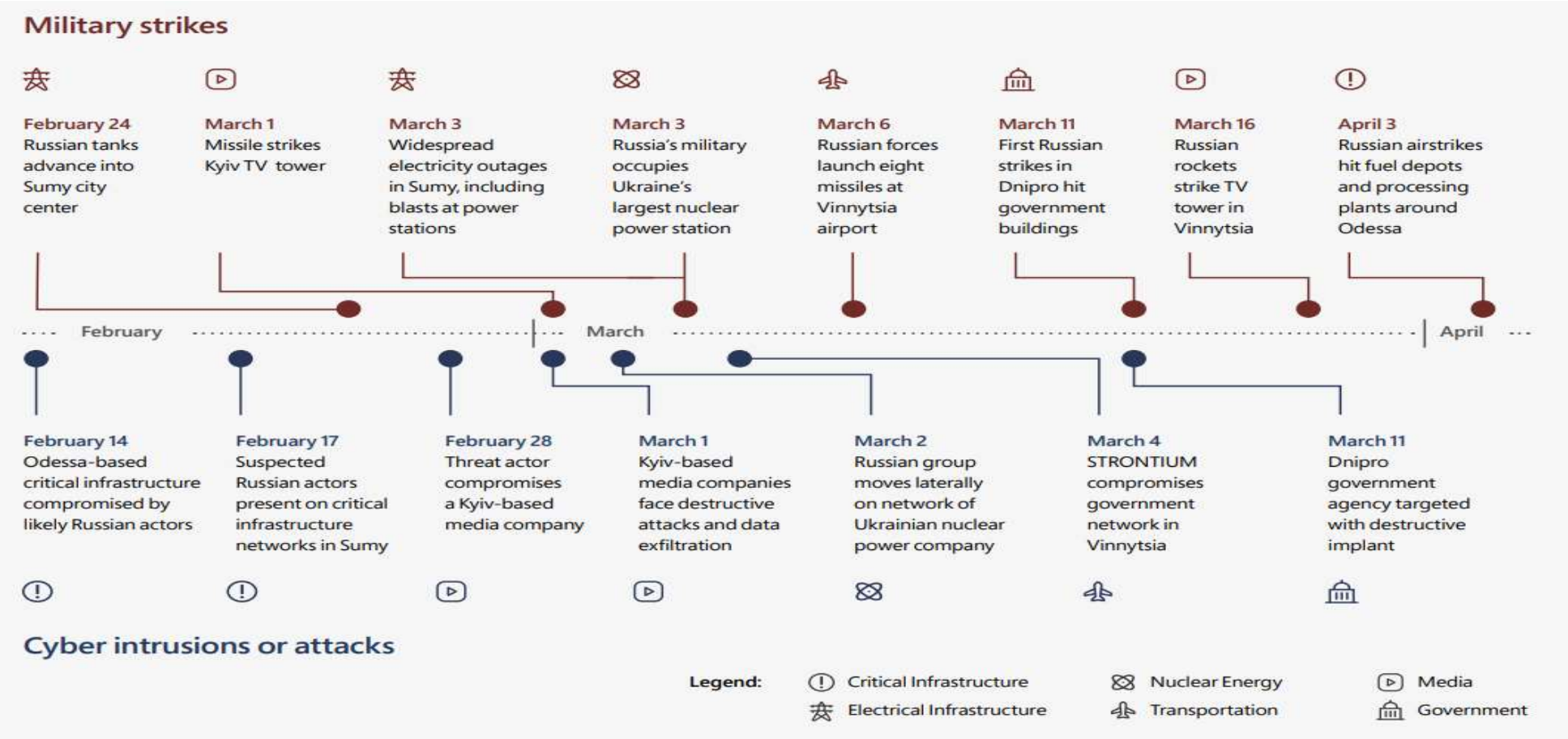


A New Battlefield



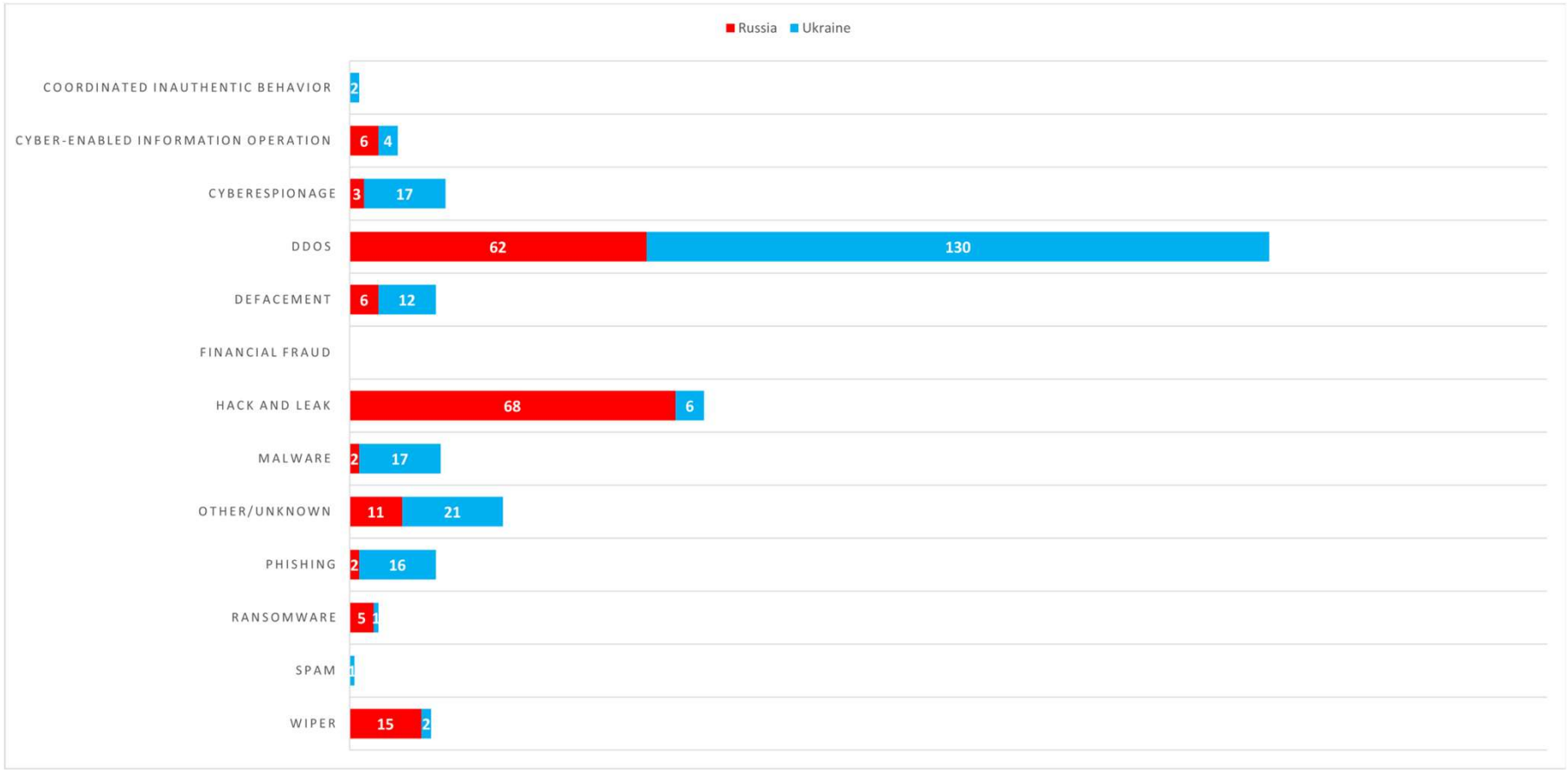
1) #https//www.imperva.com/learn/application-security/cyber-warfare/#~text=Cyber%20warfare%20is%20usually%20defined,and%20even%20loss%20of%20life.

Early Attacks in the Conflict



1) https//query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

Cyberwarfare Attack Types



Threat Actors (Russia)

Allegiance to Russia			
Name	Type	Country	Attacks
NoName057(16)	Collective	Russia	171
Anonymous Russia	Nation State	Russia	100
Killnet	Collective	Russia	85
People's CyberArmy	Collective	Russia	64
Russian Hackers Team	Collective	Unknown	19
Phoenix	Collective	Russia	18
Sandworm	Nation State	Russia	16
Xaknet	Individual	Russia	14
DEV-0586	Collective	Russia	10
Legion Cyber Spetsnaz	Collective	Russia	8
Fancy Bear	Collective	Russia	8
UNC1151	Collective	Belarus	7
Gamaredon	Collective	Russia	6
Nation State - Russian Federation	Collective	Russia	5
Cold River	Collective	Russia	3
KillMilk	Collective	Russia	3
RADIS	Cybercriminal	Unknown	3
UAC-0098	Unknown	Russia	2
UAC-0041	Collective	Russia	2
Zarya	Collective	Russia	2
ICC_H@ckTeam	Collective	Russia	2
Many more …	Collective	…	…

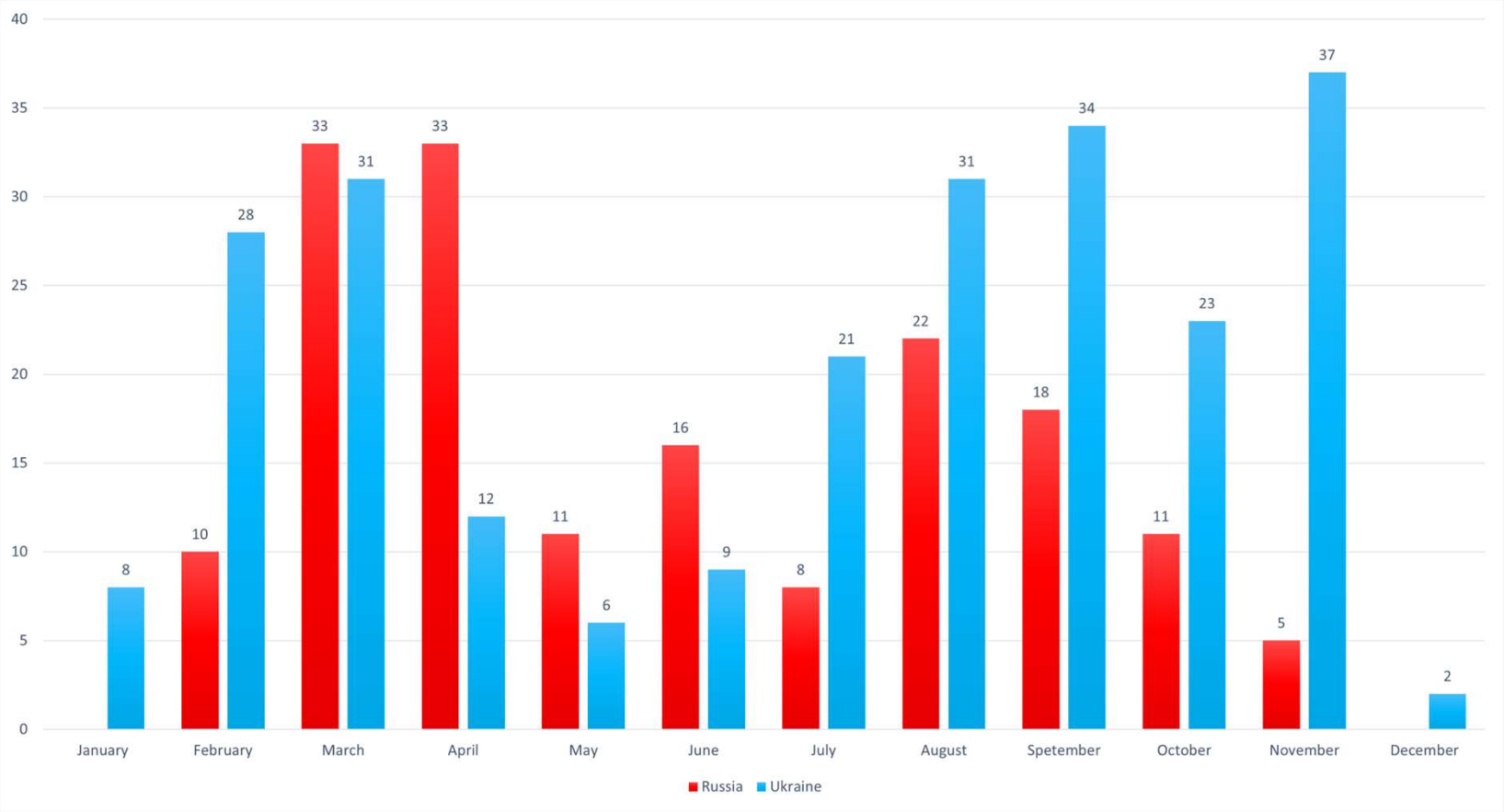
Threat Actors (Ukraine)

Allegiance to Ukraine			
Name	Type	Country	Attacks
Anonymous	Collective	Unknown	55
IT Army of Ukraine	Nation State	Ukraine	39
NB65	Collective	Unknown	9
Haydamaki	Collective	Ukraine	9
GhostSec	Collective	USA	4
Anonymous-DepaixPorteur	Collective	Unknown	3
GURMO	Nation State	Ukraine	2
RIAEvangelist	Individual	USA	2
The Black Rabbit World	Collective	Unknown	2
StudentCyberArmy	Collective	Ukraine	2
v0g3lSec	Collective	Unknown	2
Cyber Partisans	Collective	Belarus	2
2402team	Collective	Unknown	1
Cyber Palyanitsa	Collective	Ukraine	1
National Republican Army	Collective	Russia	1
AgainstTheWest	Collective	Unknown	1
KelvinSecurity	Cybercriminal	Unknown	1
CaucasNet	Unknown	Unknown	1
Team OneFist	Collective	Ukraine	1
Anonymous-Spid3r	Collective	Unknown	1
Anonymous Liberland-Pwn-Bär Hack Team	Collective	Unknown	1

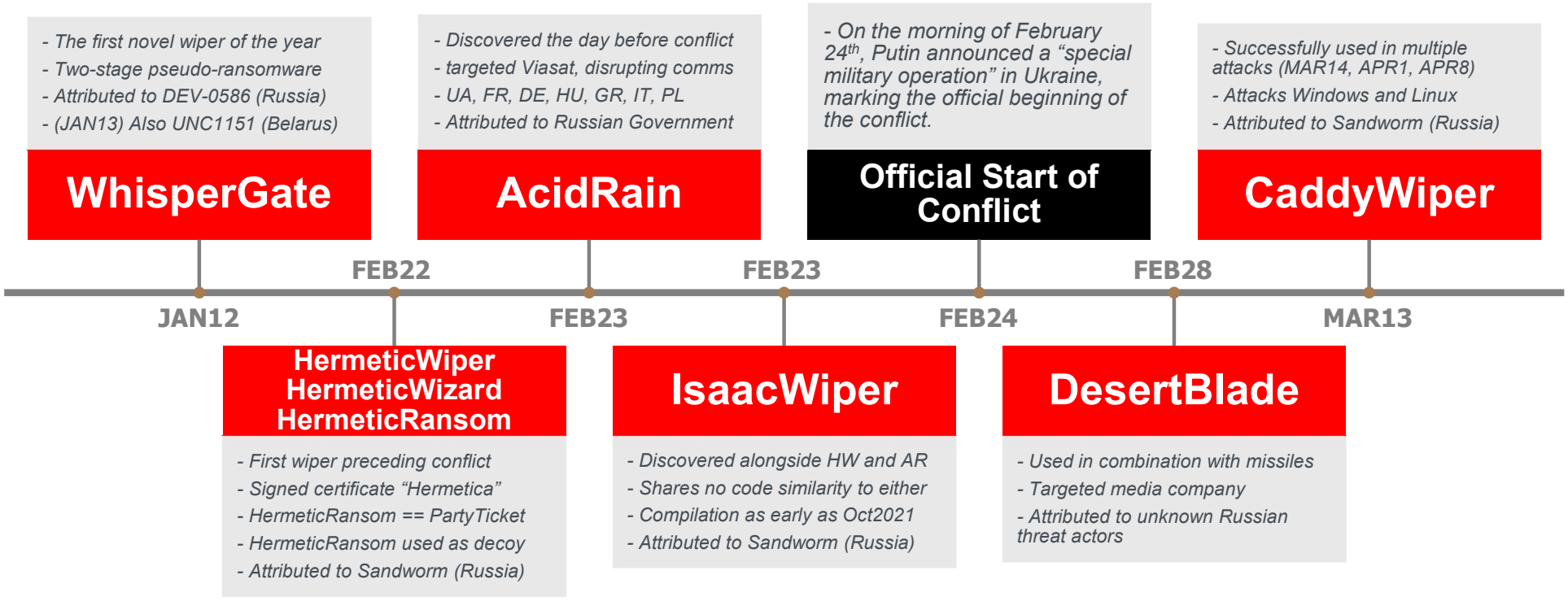
Threat Actors (CyberKnow)


Timeline of various attacks executed in War

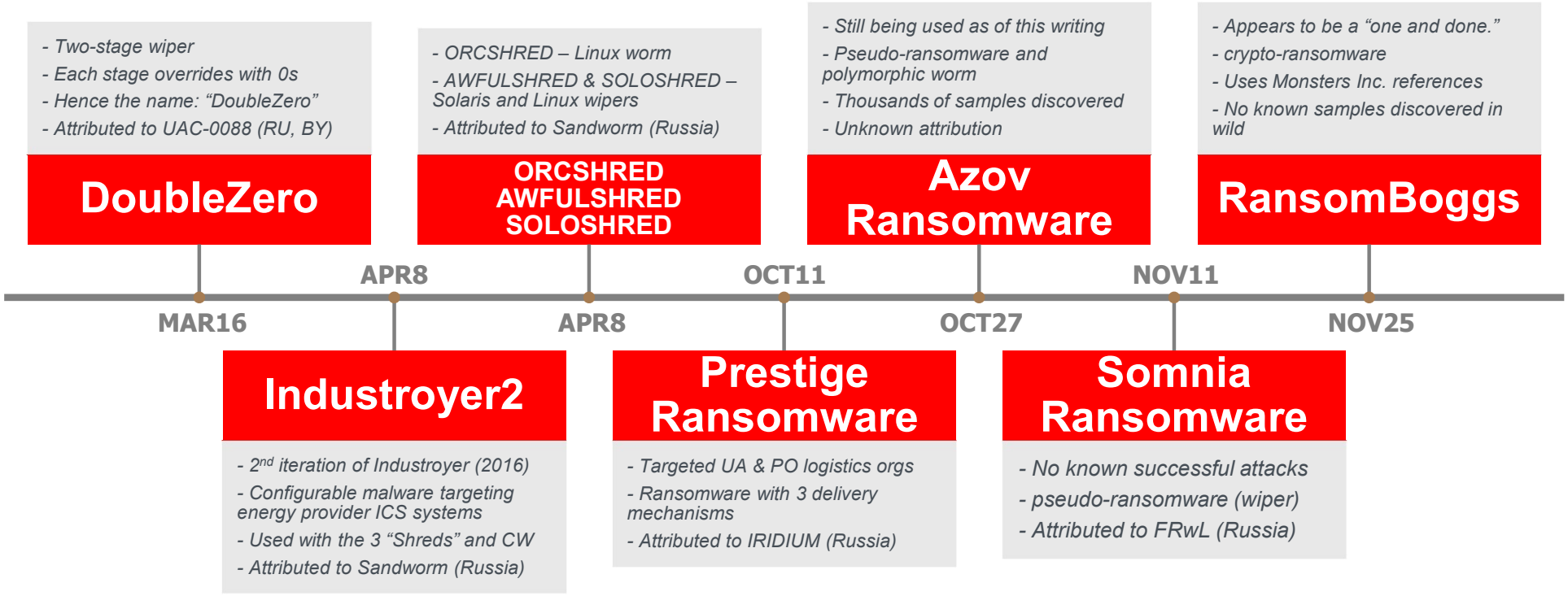
Reported Incidents



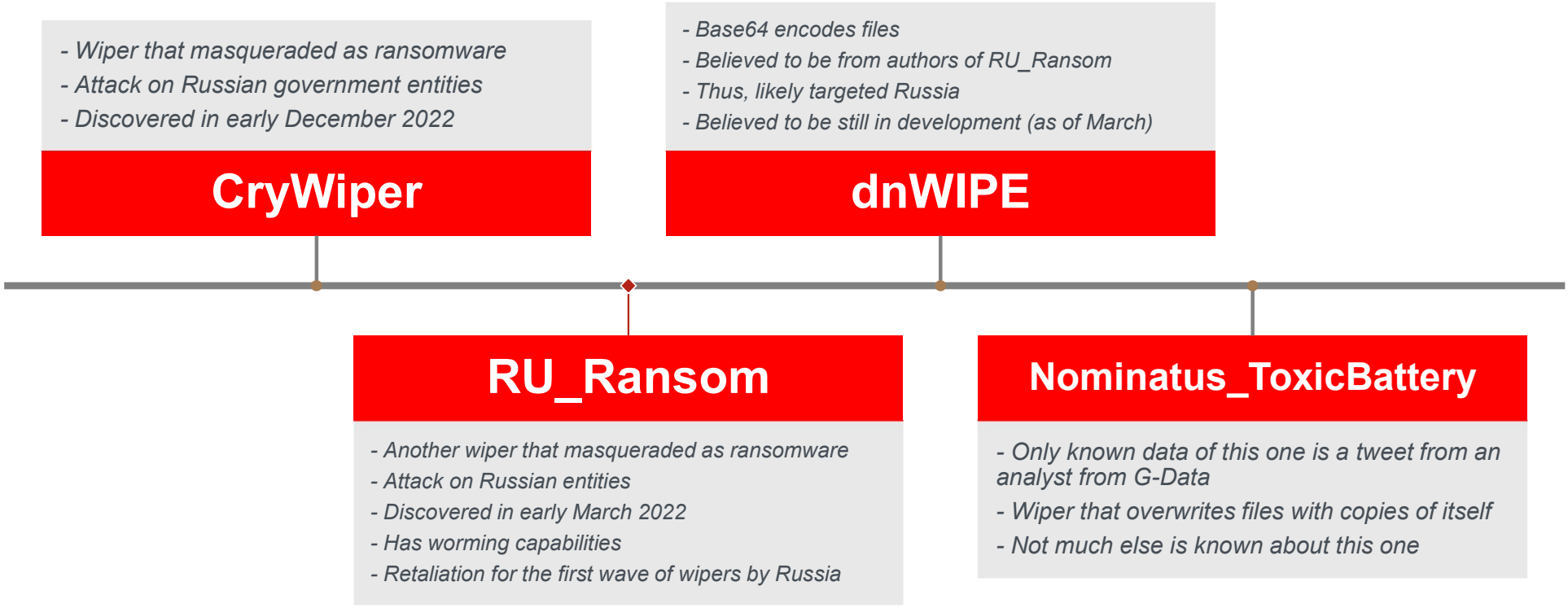
Timeline of Novel Wipers in Ukraine



Timeline of Novel Wipers (cont.)



Timeline of Novel Wipers (Honorable Mentions)




Technical Analysis (ISSACWiper)

ISAACWiper

- Also known as LasainWiper/Lasainraw by Microsoft (I don't know why)
- The name "ISAACWiper" comes from ESET researchers who discovered the file and initially thought the MW used the ISAAC PRNG
  - It uses another PRNG that will be discussed later ☺
- Discovered the day of the conflict (FEB24, 2022)
- Another iteration of ISAACWiper was discovered a day later
  - Has debug strings
  - This is the sample I am analyzing

Reference: https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/

ISAACWiper Samples

- 13037b749aa4b1eda538fda26d6ac41c8f7b1d02d83f47b0d187dd645154e033
  - 🐞 Sample Collected
- 7bcd4ec18fc4a56db30e0aaebd44e2988f98f7b5d8c14f6689f650b4f11e16c0
  - 🐞 Sample Collected
- abf9adf2c2c21c1e8bd69975dfccb5ca53060d8e1e7271a5e9ef3b56a7e54d9f
  - ✕ No Sample
- afe1f2768e57573757039a40ac40f3c7471bb084599613b3402b1e9958e0d27a
  - ✕ No Sample

ISAACWiper Static Analysis

property	value
md5	6C10466AD7C153E7F949FA3C6600B6AC
sha1	5D009F79383A81622EEFD8B183EFB23FBF96A62F
sha256	7BCD4EC18FC4A56DB30E0AAEBD44E2988F98F7B5D8C14F6689F650B4F11E16C0
md5-without-overlay	wait...
sha1-without-overlay	wait...
sha256-without-overlay	wait...
first-bytes-hex	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00
first-bytes-text	M Z . . . . . @ . . . . .
file-size	224800 (bytes)
size-without-overlay	wait...
entropy	6.613
imphash	A4B162717C197E11B76A4D9BC58EA25D
signature	n/a
entry-point	55 8B EC 83 7D 0C 01 75 05 E8 38 05 00 00 FF 75 10 FF 75 0C FF 75 08 E8 AE FE FF FF 83 C4 0C 5D C2
file-version	n/a
description	n/a
file-type	**dynamic-link-library**
cpu	**32-bit**
subsystem	console
compiler-stamp	0x6218FA37 (Fri Feb 25 16:48:07 2022)
debugger-stamp	0x6218FA37 (Fri Feb 25 16:48:07 2022)
resources-stamp	
exports-stamp	0xFFFFFFFF (Sun Feb 07 07:28:15 2106)
version-stamp	n/a
certificate-stamp	n/a

ISAACWiper Static Analysis (Tools)

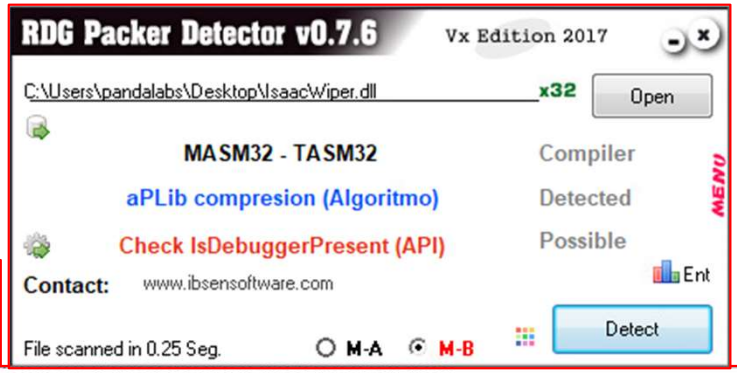
- Tools used:
  - PE Studio
  - Detect it Easy (DiE)
  - RDG Packer Detector
  - Professional PE file Explorer (Puppy)
  - CAPA
  - IDA
  - Hatching Triage (Online Sandbox)
  - Many Microsoft documentation lookups ☺

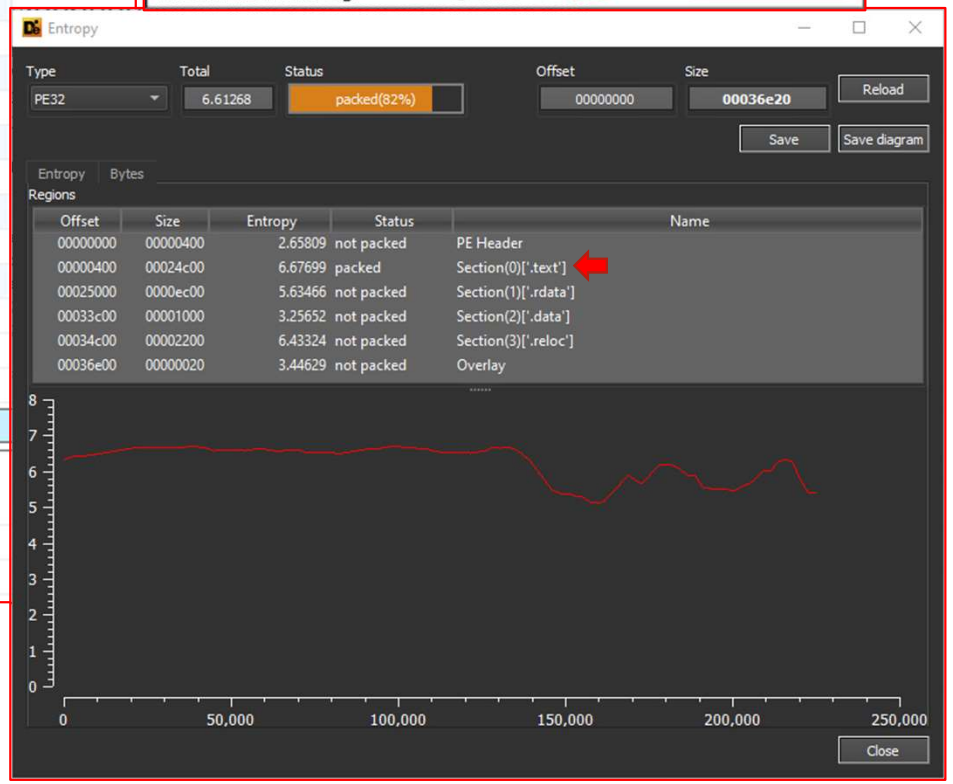
ISAACWiper Static Analysis

Member	Value	Comment
Characteristics	00000000	
TimeDateStamp	FFFFFFFF	Sun, 07 Feb 2106 06:28:15 UTC (-30349 days, -8.27 hours ago)
MajorVersion	0000	
MinorVersion	0000	
Dll Name	00034362	Cleaner.dll
Base	00000001	
NumberOfFunctions	00000001	
NumberOfNames	00000001	
AddressOfFunctions	00034358	
AddressOfNames	0003435C	
AddressOfNameOrdinals	00034360	

Type to filter...

Ordi...	RVA	Name RVA	Name	Forwarded to
0001	000087C0	0003436E	_Start@4	





ISAACWiper Static Analysis (Libraries)

Libraries

library (2)	blacklist (0)	type (1)	imports (89)	description
kernel32.dll	-	implicit	88	Windows NT BASE API Client DLL
user32.dll	-	implicit	1	Multi-User Windows USER API Client DLL

Execution

name (89)	group (10)	type (1)
GetEnvironmentStringsW	execution	implicit
GetExitCodeThread	execution	implicit
CreateThread	execution	implicit
TlsAlloc	execution	implicit
TlsGetValue	execution	implicit
TlsSetValue	execution	implicit
TlsFree	execution	implicit
GetStartupInfoW	execution	implicit
GetCurrentProcess	execution	implicit
ExitProcess	execution	implicit
GetCommandLineA	execution	implicit
GetCommandLineW	execution	implicit
FreeEnvironmentStringsW	execution	implicit

File

FindFirstFileW	file	implicit
FindNextFileW	file	implicit
SetFileAttributesW	file	implicit
GetTempFileNameW	file	implicit
MoveFileW	file	implicit
FindFirstFileExW	file	implicit
CreateFileW	file	implicit
CreateDirectoryW	file	implicit
GetFileSizeEx	file	implicit
WriteFile	file	implicit
FindClose	file	implicit
SetEndOfFile	file	implicit
GetSystemTimeAsFileTime	file	implicit
FlushFileBuffers	file	implicit
SetFilePointerEx	file	implicit
GetFileType	file	implicit
ReadFile	file	implicit

ISAACWiper Static Analysis (Libraries)

Synchronization

WaitForMultipleObjects	synchronization	implicit
WaitForSingleObject	synchronization	implicit
EnterCriticalSection	synchronization	implicit
LeaveCriticalSection	synchronization	implicit
DeleteCriticalSection	synchronization	implicit
InitializeCriticalSectionA...	synchronization	implicit
InitializeSListHead	synchronization	implicit
InterlockedFlushSList	synchronization	implicit

System-Information

GetWindowsDirectoryW	system-information	implicit
GetTickCount	system-information	implicit
QueryPerformanceCount...	system-information	implicit
IsDebuggerPresent	system-information	implicit
IsProcessorFeaturePresent	system-information	implicit
EnumSystemLocalesW	system-information	implicit

Storage

GetDiskFreeSpaceExW	storage	implicit
GetLogicalDrives	storage	implicit

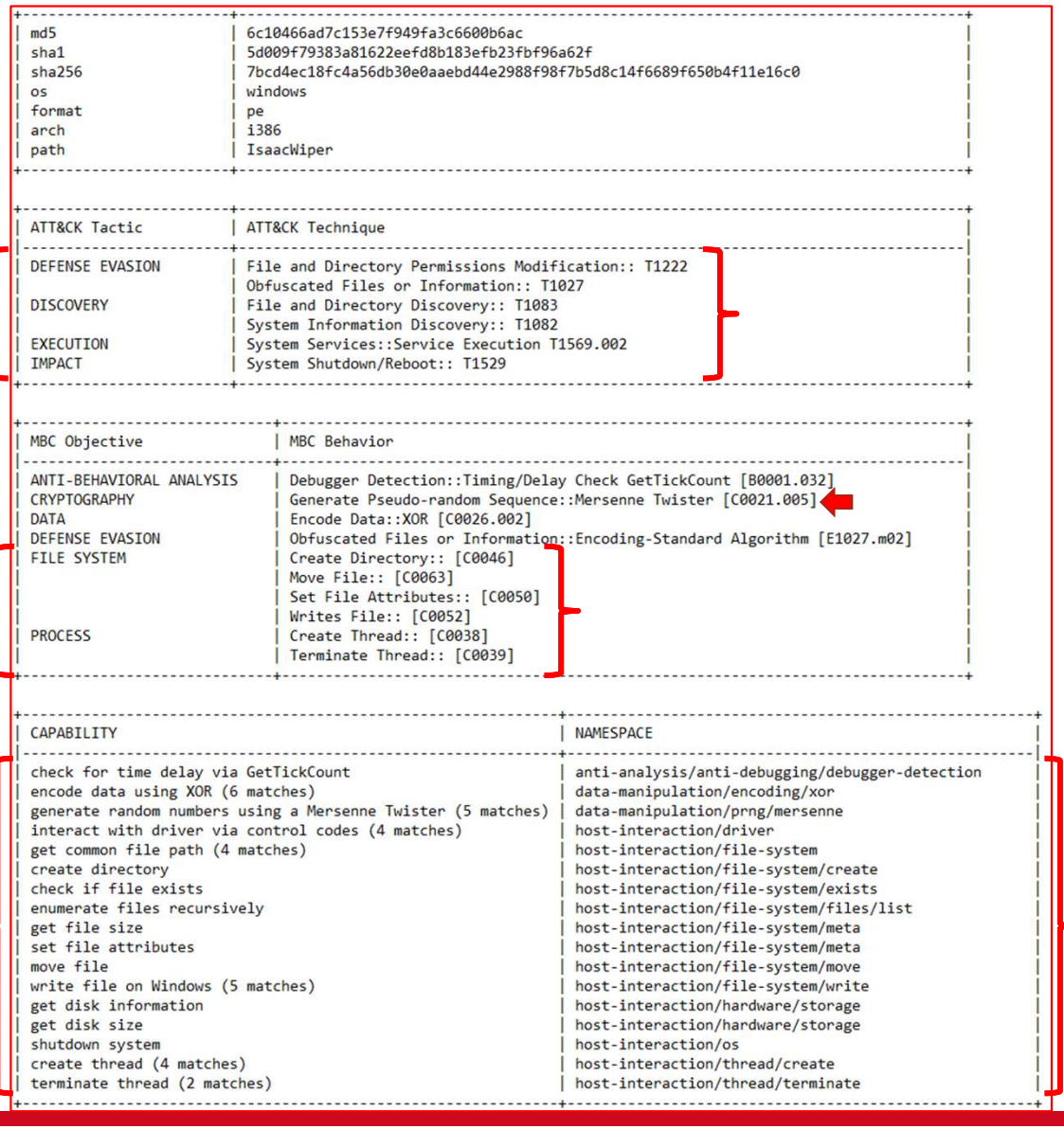
ISAACWiper Static Analysis (Strings)

x	file	-	C:\ProgramData\log.txt

hint (47)	group (11)	value (1969)
x	-	\\.\
utility	-	start erasing physical drives...
utility	-	start erasing system physical drive...
utility	-	start erasing system logical drive

-	CONOUT$
-	PhysicalDrive
-	getting drives...
-	physical drives:
-	-- system physical drive
-	-- physical drive
-	logical drives:
-	-- system logical drive:
-	-- logical drive:
-	-- FAILED
-	physical drive
-	-- start erasing logical drive
-	system physical drive -- FAILED

ISAACWiper Static Analysis (CAPA)



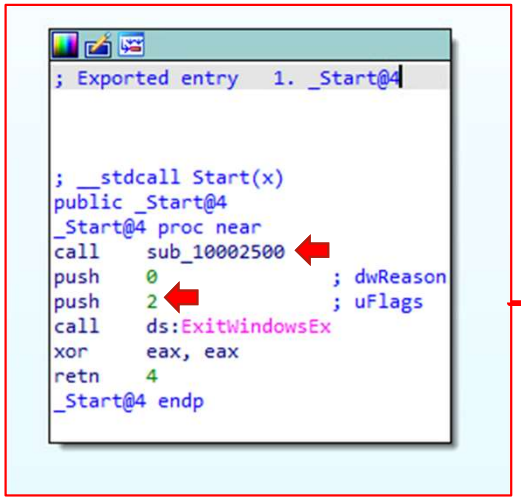
md5	6c10466ad7c153e7f949fa3c6600b6ac
sha1	5d009f79383a81622eefd8b183efb23fbf96a62f
sha256	7bcd4ec18fc4a56db30e0aaebd44e2988f98f7b5d8c14f6689f650b4f11e16c0
os	windows
format	pe
arch	i386
path	IsaacWiper

ATT&CK Tactic	ATT&CK Technique
DEFENSE EVASION	File and Directory Permissions Modification:: T1222
	Obfuscated Files or Information:: T1027
DISCOVERY	File and Directory Discovery:: T1083
	System Information Discovery:: T1082
EXECUTION	System Services::Service Execution T1569.002
IMPACT	System Shutdown/Reboot:: T1529

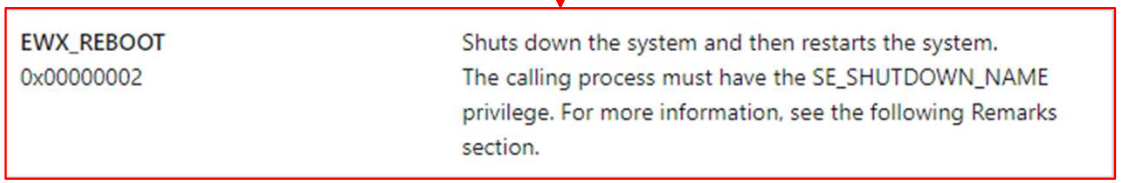
MBC Objective	MBC Behavior
ANTI-BEHAVIORAL ANALYSIS	Debugger Detection::Timing/Delay Check GetTickCount [B0001.032]
CRYPTOGRAPHY	Generate Pseudo-random Sequence::Mersenne Twister [C0021.005]
DATA	Encode Data::XOR [C0026.002]
DEFENSE EVASION	Obfuscated Files or Information::Encoding-Standard Algorithm [E1027.m02]
FILE SYSTEM	Create Directory:: [C0046]
	Move File:: [C0063]
	Set File Attributes:: [C0050]
	Writes File:: [C0052]
PROCESS	Create Thread:: [C0038]
	Terminate Thread:: [C0039]

CAPABILITY	NAMESPACE
check for time delay via GetTickCount	anti-analysis/anti-debugging/debugger-detection
encode data using XOR (6 matches)	data-manipulation/encoding/xor
generate random numbers using a Mersenne Twister (5 matches)	data-manipulation/prng/mersenne
interact with driver via control codes (4 matches)	host-interaction/driver
get common file path (4 matches)	host-interaction/file-system
create directory	host-interaction/file-system/create
check if file exists	host-interaction/file-system/exists
enumerate files recursively	host-interaction/file-system/files/list
get file size	host-interaction/file-system/meta
set file attributes	host-interaction/file-system/meta
move file	host-interaction/file-system/move
write file on Windows (5 matches)	host-interaction/file-system/write
get disk information	host-interaction/hardware/storage
get disk size	host-interaction/hardware/storage
shutdown system	host-interaction/os
create thread (4 matches)	host-interaction/thread/create
terminate thread (2 matches)	host-interaction/thread/terminate

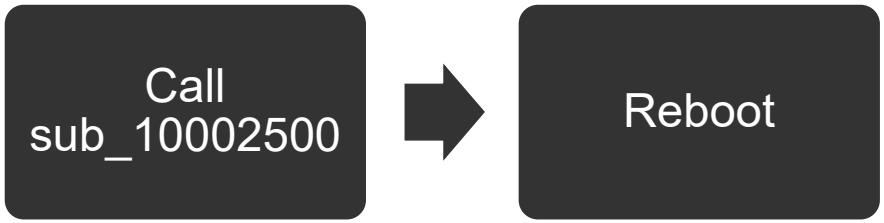
Reversing ISAACWiper (_Start@4)



```
; Exported entry   1. _Start@4


; __stdcall Start(x)
public _Start@4
_Start@4 proc near
call    sub_10002500
push    0                       ; dwReason
push    2                       ; uFlags
call    ds:ExitWindowsEx
xor     eax, eax
retn    4
_Start@4 endp
```

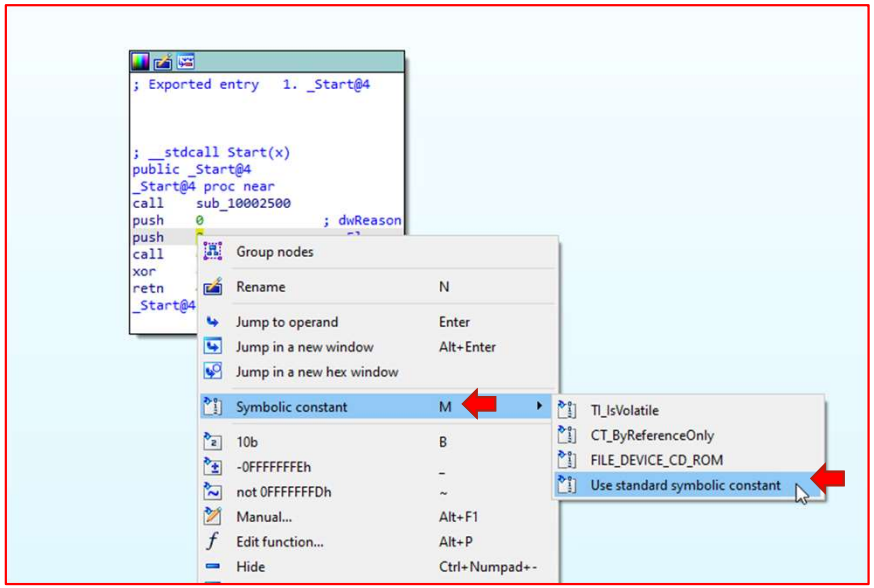


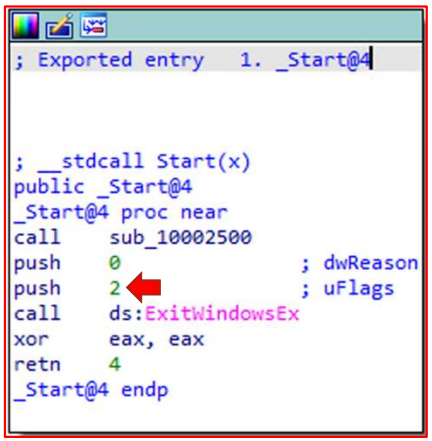
EWX_REBOOT 0x00000002	Shuts down the system and then restarts the system. The calling process must have the SE_SHUTDOWN_NAME privilege. For more information, see the following Remarks section.

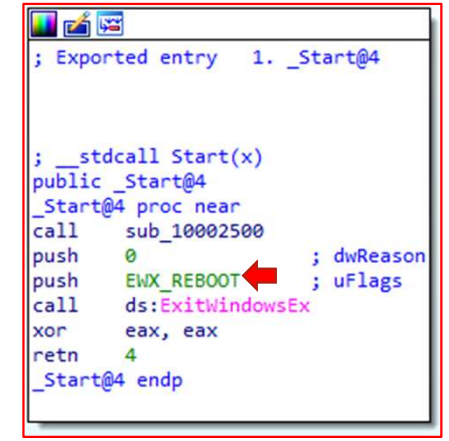


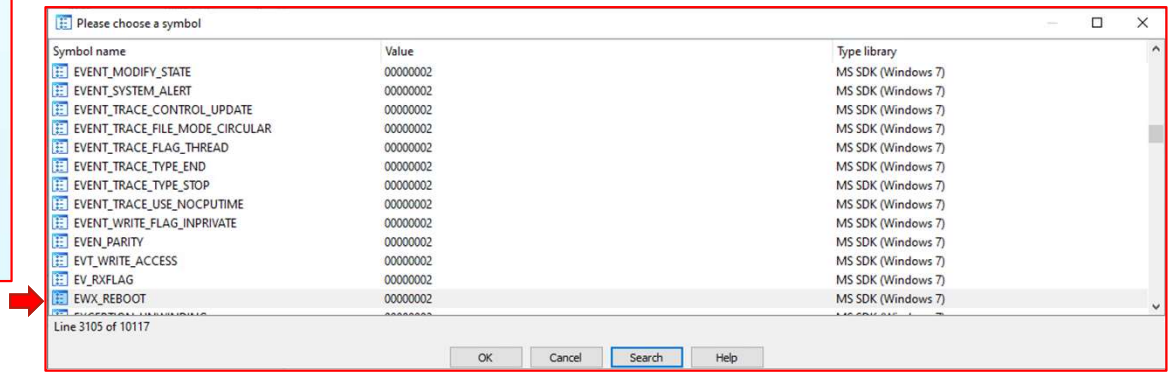
Reference: https://learn.microsoft.com/en-us/windows/win32/api/winuser/nf-winuser-exitwindowsex

Reversing ISAACWiper (Symbolic Constants)







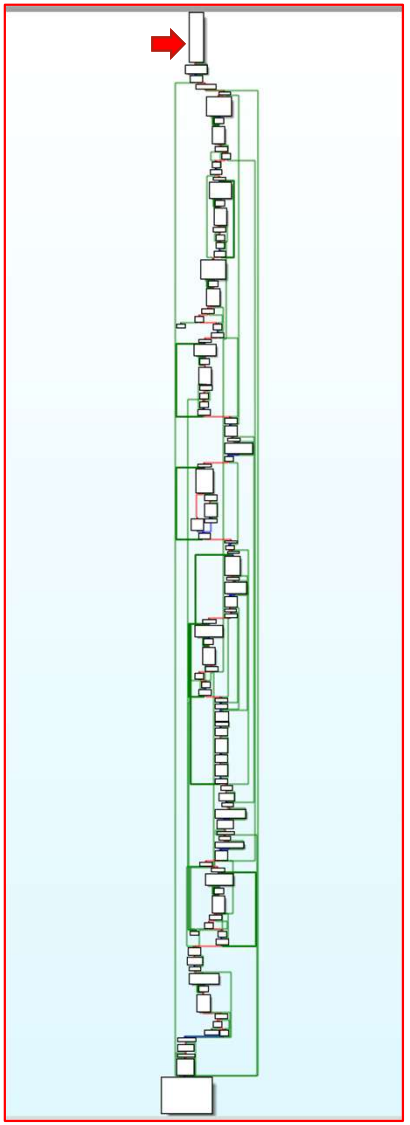


Reversing ISAACWiper (2500)

```
; Exported entry   1. _Start@4


; __stdcall Start(x)
public _Start@4
 Start@4 proc near
call    sub_10002500
push    0               ; dwReason
push    EWX_REBOOT      ; uFlags
call    ds:ExitWindowsEx
xor     eax, eax
retn    4
_Start@4 endp
```

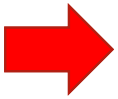


```
sub_10002500 proc near

var_2B30= dword ptr -2B30h
var_2B20= dword ptr -2B20h
var_2B1C= dword ptr -2B1Ch
var_2B18= dword ptr -2B18h
ExitCode= dword ptr -2B14h
var_2B10= dword ptr -2B10h
var_2B04= dword ptr -2B04h
var_2B00= dword ptr -2B00h
var_2AF8= byte ptr -2AF8h
var_2AAC= dword ptr -2AACh
var_2A98= dword ptr -2A98h
Parameter= byte ptr -2A50h
var_2A40= byte ptr -2A40h
var_2A2C= dword ptr -2A2Ch
var_2A20= dword ptr -2A20h
var_2A1C= dword ptr -2A1Ch
var_2A10= byte ptr -2A10h
var_29E8= dword ptr -29E8h
var_29E4= byte ptr -29E4h
var_29B0= dword ptr -29B0h
var_29AC= dword ptr -29ACh
var_29A8= byte ptr -29A8h
var_2980= dword ptr -2980h
var_2940= byte ptr -2940h
var_1F18= dword ptr -1F18h
Handles= dword ptr -1F10h
var_1F0C= byte ptr -1F0Ch
var_1EA8= dword ptr -1EA8h
var_1EA0= byte ptr -1EA0h
var_1820= dword ptr -1820h
var_1818= dword ptr -1818h
nCount= dword ptr -17B0h
var_17A8= byte ptr -17A8h
var_1128= dword ptr -1128h
var_1120= byte ptr -1120h
var_AA0= dword ptr -0AA0h
var_A98= byte ptr -0A98h
var_8= dword ptr -8

push    ebp
mov     ebp, esp
and     esp, 0FFFFFFF8h
mov     eax, 2B34h
call    __alloca_probe
push    ebx
push    esi
push    edi
sub     esp, 10h
lea     ecx, [esp+2B50h+var_2B10]
call    sub_10004A80
cmp     [esp+2B40h+var_2AAC], 0
mov     [esp+2B40h+var_8], 0
mov     [esp+2B40h+var_1128], 0
jz      short loc_1000255F
```



Reversing ISAACWiper (4A80)

```
push    ebp
mov     ebp, esp
and     esp, 0FFFFFFF8h
mov     eax, 2B34h
call    __alloca_probe
push    ebx
push    esi
push    edi
sub     esp, 10h
lea     ecx, [esp+2B50h+var_2B10]
call    sub_10004A80
cmp     [esp+2B40h+var_2AAC], 0
mov     [esp+2B40h+var_8], 0
mov     [esp+2B40h+var_1128], 0
jz      short loc_1000255F
```



```
 93  this[12] = 0;
 94  this[16] = 0;
 95  this[7] = 0;
 96  this[11] = 0;
 97  this[15] = 0;
 98  this[22] = v18;
 99  v19 = dword_10036C48;
100  this[25] = 0;
101  this[23] = v19;
102  this[20] = 0;
103  v20 = sub_10009159(L"C:\\ProgramData\\log.txt", 2, 64);
104  v21 = (int)v30;
105  v29 = v20;
106  if ( v20 )
107  {
108    v10[72] = 1;
109    *((_DWORD *)v10 + 11) = v10 + 36;
110    *((_DWORD *)v10 + 4) = v10 + 8;
111    v10[62] = 0;
112    *((_DWORD *)v10 + 8) = v10 + 24;
```

This PC › Windows (C:) › ProgramData ›

Search ProgramData

Name	Date modified	Type
Adobe	11/11/2022 1:45 PM	File folder
Microsoft	11/11/2022 1:47 PM	File folder
Microsoft OneDrive	11/11/2022 1:36 PM	File folder
Mozilla	11/11/2022 1:50 PM	File folder
Oracle	11/11/2022 1:46 PM	File folder
Package Cache	11/11/2022 1:41 PM	File folder
Packages	11/11/2022 1:37 PM	File folder
regid.1991-06.com.microsoft	11/11/2022 1:46 PM	File folder
SoftwareDistribution	12/7/2019 9:14 AM	File folder
ssh	5/11/2020 5:43 AM	File folder
USOPrivate	11/11/2022 9:33 PM	File folder
USOShared	12/7/2019 9:14 AM	File folder
WindowsHolographicDevices	12/7/2019 9:54 AM	File folder
log.txt	1/5/2023 4:53 AM	Text Document

Reversing ISAACWiper (2500 DBG Strings)

```
86  sub_10004A80(v56, v48, v49, v50, v53);
87  v82 = 0;
88  v78 = 0;
89  if ( v59 )
90  {
91    v0 = sub_10006FC0(int)v57, L"getting drives...");
92    v1 = sub_100071D0(v0);
93    sub_100071D0(v1);
94  }
95  if ( (unsigned __int8)sub_10007240(v65, v81) && (unsigned __int8)sub_100074F0((LPCWSTR)Parameter) )
96  {
97    if ( v59 )
98    {
99      v2 = sub_10006FC0(int)v57, L"physical drives:");
100     sub_100071D0(v2);
101     sub_10006FC0(int)v57, L"-- system physical drive ");
102     v3 = sub_10004D90(v66);
103     sub_10006FC0(v3, L": ");
104     sub_10005F70(v65, wcslen((const unsigned __int16 *)v65));
105     v4 = sub_100085D0(0);
106     sub_100071D0(v4);
107     v5 = 0;
108     if ( v82 )
109     {
110       v6 = v81;
111       do
112       {
113         sub_10006FC0(int)v57, L"-- physical drive ");
114         v7 = sub_10004D90(*((_DWORD *)v6 + 10));
115         sub_10006FC0(v7, L": ");
116         sub_10005F70(v6, wcslen((const unsigned __int16 *)v6));
117         v8 = sub_100085D0(0);
118         sub_100071D0(v8);
119         ++v5;
120         v6 += 104;
121       }
122       while ( v5 < v82 );
123     }
124     sub_100071D0((int)v57);
125     v9 = sub_10006FC0(int)v57, L"logical drives:");
126     sub_100071D0(v9);
127     sub_10006FC0(int)v57, L"-- system logical drive: ");
128     sub_10005F70(Parameter, wcslen((const unsigned __int16 *)Parameter));
129     v10 = sub_100085D0(0);
130     sub_100071D0(v10);
131     v11 = 0;
132     if ( v78 )
133     {
134       v12 = (const unsigned __int16 *)&v77;
135       do
136       {
137         sub_10006FC0(int)v57, L"-- logical drive: ");
138         sub_10005F70(v12, wcslen(v12));
139         v13 = sub_100085D0(0);
```

Create log.txt

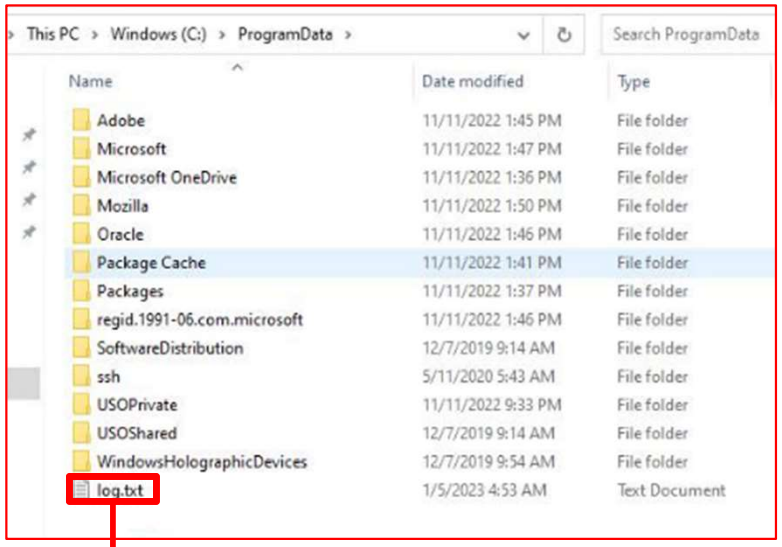
```
v74 = 0;
nCount = 0;
if ( v82 )
{
  if ( v59 )
  {
    v17 = sub_10006FC0(int)v57, L"start erasing physical drives...");
    v18 = sub_100071D0(v17);
    sub_100071D0(v18);
    v14 = v82;
    v15 = v72;
    v16 = v70;
  }
```

Reversing ISAACWiper (2500 DBG Strings 2)

```
if ( v59 )
{
  v35 = sub_10006FC0((int)v57, L"start erasing system physical drive...");
  v36 = sub_100071D0(v35);
  sub_100071D0(v36);
}
v37 = sub_10003310(v67, v68);
if ( v37 != v67 || v38 != v68 )
{
  if ( v59 )
  {
    v39 = sub_10006FC0((int)v57, L"system physical drive -- FAILED");
    sub_100071D0(v39);
  }
  v80 = 0;
  sub_10007680(v66);
  if ( v59 )
  {
    v40 = 0;
    if ( v74 )
    {
      v41 = (const unsigned __int16 *)v73;
      do
      {
        sub_10006FC0((int)v57, L"-- start erasing logical drive ");
        sub_10005F70(v41, wcslen(v41));
        v42 = sub_100085D0(0);
        sub_100071D0(v42);
        ++v40;
        v41 += 32;
      }
      while ( v40 < v74 );
    }
  }
  sub_100076F0(v73, v79);
  if ( nCount )
  {
    WaitForMultipleObjects(nCount, v75, 1, 0xFFFFFFFF);
    sub_100077F0(v73);
  }
  if ( v59 )
  {
    sub_10006FC0((int)v57, L"start erasing system logical drive ");
    sub_10005F70(Parameter, wcslen((const unsigned __int16 *)Parameter));
    v43 = sub_100085D0(0);
    sub_100071D0(v43);
  }
```

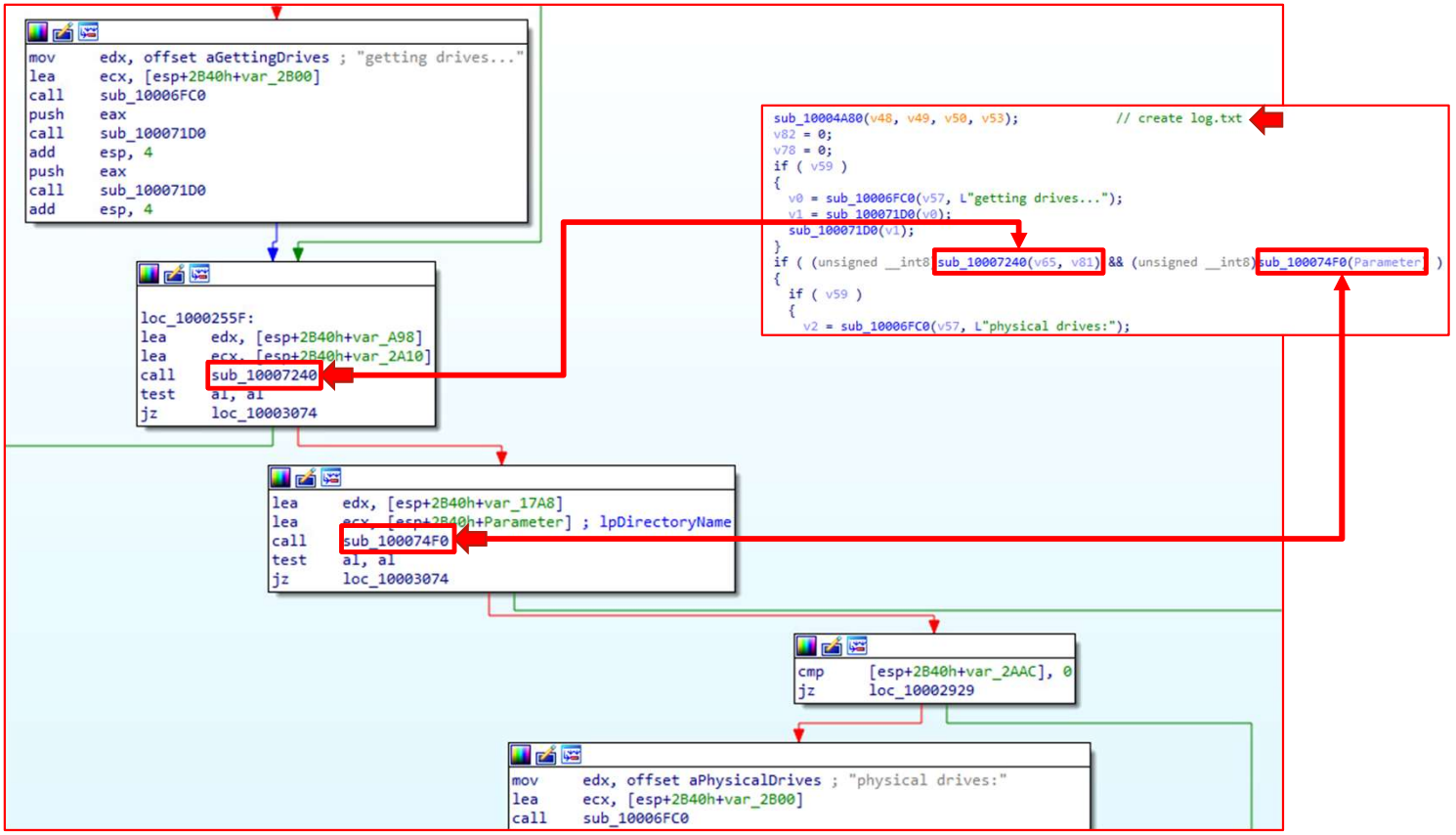
```
if ( !v26 )
{
  if ( v59 )
  {
    sub_10006FC0((int)v57, L"physical drive ");
    v27 = sub_10004D90(*(_DWORD *)&v69[104 * v23 + 40]);
    v28 = sub_10006FC0(v27, L"-- FAILED");
    sub_100071D0(v28);
  }
  v80 = 0;
  sub_10007680(*(_DWORD *)&v69[104 * v23 + 40]);
  if ( v80 )
  {
    if ( v59 )
    {
      v29 = 0;
      if ( v74 )
      {
        v30 = (const unsigned __int16 *)v73;
        do
        {
          ExitCode = sub_10006FC0((int)v57, L"-- start erasing logical drive ");
          sub_10005F70(v30, wcslen(v30));
          v31 = sub_100085D0(0);
          sub_100071D0(v31);
          ++v29;
          v30 += 32;
```

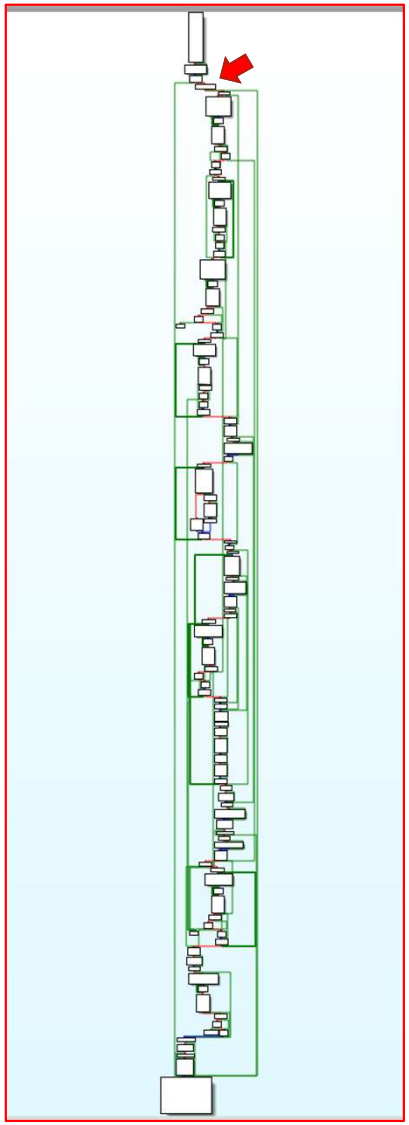
Reversing ISAACWiper (log.txt)




```
getting drives...

physical drives:
-- system physical drive 0: PhysicalDrive0

logical drives:
-- system logical drive: C:
-- logical drive: D:

start erasing system physical drive...

system physical drive -- FAILED
start erasing system logical drive C:
```

Reversing ISAACWiper (7240-74F0 Conditionals)





Reversing ISAACWiper (7240)

Get the list of physical drives (0-n)

```
push    ebp
mov     ebp, esp
sub     esp, 34h
push    ebx
push    esi
push    edi
mov     edi, edx
mov     ebx, ecx
push    1Ah
push    offset aPhysicaldrive ; "PhysicalDrive"
mov     edx, 22h ; '"'
mov     [ebp+var_14], edi
mov     [ebp+var_28], ebx
call    sub_100087F0
```

```
*((_BYTE *)lpDirectoryName + 40) = v3;
*(_DWORD *)(lpDirectoryName + 1) = 58;
*((_DWORD *)lpDirectoryName + 2) = 2;
v6 = sub_100087F0(L"\\\\.\\", 8) >> 1;
*((_DWORD *)lpDirectoryName + 8) = v6;
```

```
v12 = CreateFileW(v30, 0x80000000, 3u, 0, 3u, 0, 0);
if ( v12 == (HANDLE)-1 )
  return 0;
BytesReturned = 0;
v13 = DeviceIoControl(v12, 0x2D1080u, 0, 0, OutBuffer, 0xCu, &BytesReturned, 0);
v14 = v13;
if ( v13 )
{
  v15 = 0;
  if ( OutBuffer[0] == 7 )
    v15 = OutBuffer[1];
  v39 = v15;
}
CloseHandle(v12);
```

dwIoControlCode

```
v12 = CreateFileW((LPCWSTR)v30, GENERIC_READ, 3u, 0, 3u, 0, 0);
if ( v12 == (HANDLE)-1 )
  return 0;
BytesReturned = 0;
v13 = DeviceIoControl(v12, IOCTL_STORAGE_GET_DEVICE_NUMBER, 0, 0, OutBuffer, 0xCu, &BytesReturned, 0);
v14 = v13;
if ( v13 )
{
  v15 = 0;
  if ( OutBuffer[0] == FILE_DEVICE_DISK )
    v15 = OutBuffer[1];
  v39 = v15;
}
CloseHandle(v12);
```

Reference: https://learn.microsoft.com/en-us/windows-hardware/drivers/kernel/specifying-device-types
Reference: https://learn.microsoft.com/en-us/windows-hardware/drivers/ddi/wdm/ns-wdm-_device_object
Reference: https://learn.microsoft.com/en-us/windows-hardware/drivers/ddi/ntddstor/ni-ntddstor-ioctl_storage_get_device_number

Reversing ISAACWiper (7240: DeviceIoControl)

Remarks

To retrieve a handle to the device, you must call the CreateFile function with either the name of a device or the name of the driver associated with a device. To specify a device name, use the following format:

\\.*DeviceName*

DeviceIoControl can accept a handle to a specific device. For example, to open a handle to the logical drive A: with CreateFile, specify \\.\a:. Alternatively, you can use the names \\.\PhysicalDrive0, \\.\PhysicalDrive1, and so on, to open handles to the physical drives on a system.

Reference: https://learn.microsoft.com/en-us/windows/win32/api/ioapiset/nf-ioapiset-deviceiocontrol

Reversing ISAACWiper (7240 cont.)

```
push    0               ; lpTotalNumberOfFreeBytes
lea     eax, [ebp+OutBuffer]
push    eax             ; lpTotalNumberOfBytes
lea     eax, [ebp+FreeBytesAvailableToCaller]
push    eax             ; lpFreeBytesAvailableToCaller
push    esi             ; lpDirectoryName
call    ds:GetDiskFreeSpaceExW
cmp     eax, 1
jnz     short loc_1000128C
```

GetDiskFreeSpaceExW function (fileapi.h)

Article • 07/27/2022 • 2 minutes to read

Feedback

In this article

- Syntax
- Parameters
- Return value
- Remarks
- Requirements
- See also

Retrieves information about the amount of space that is available on a disk volume, which is the total amount of space, the total amount of free space, and the total amount of free space available to the user that is associated with the calling thread.

Reference: https://learn.microsoft.com/en-us/windows/win32/api/fileapi/nf-fileapi-getdiskfreespaceexw

Reversing ISAACWiper (74F0)

Get partition of physical drive (n)

```
FileW = CreateFileW((LPCWSTR)(a2 + 44), GENERIC_READ, 3u, 0, 3u, 0, 0);
if ( FileW == (HANDLE)-1 )
  return 0;
BytesReturned = 0;
v11 = DeviceIoControl(FileW, IOCTL_DISK_GET_DRIVE_GEOMETRY_EX, 0, 0, OutBuffer, 0x28u, &BytesReturned, 0);
v12 = v11;
if ( v11 )
{
  *(_DWORD *)(a2 + 96) = v15;
  *(_DWORD *)(a2 + 100) = v16;
}
CloseHandle(FileW);
return v12;
```

IOCTL_DISK_GET_DRIVE_GEOMETRY_EX IOCTL (winioctl.h)

Article • 05/18/2021 • 2 minutes to read

Feedback

In this article

Requirements

See also

Retrieves extended information about the physical disk's geometry: type, number of cylinders, tracks per cylinder, sectors per track, bytes per sector, and size.

To perform this operation, call the DeviceIoControl function with the following parameters.

C++ Copy

```
BOOL DeviceIoControl(
  (HANDLE) hDevice,                // handle to device
  IOCTL_DISK_GET_DRIVE_GEOMETRY_EX, // dwIoControlCode
  NULL,                            // lpInBuffer
  0,                               // nInBufferSize
  (LPVOID) lpOutBuffer,            // output buffer
  (DWORD) nOutBufferSize,          // size of output buffer
  (LPDWORD) lpBytesReturned,       // number of bytes returned
  (LPOVERLAPPED) lpOverlapped      // OVERLAPPED structure
);
```

Reference: https://learn.microsoft.com/en-us/windows/win32/api/winioctl/ni-winioctl-ioctl_disk_get_drive_geometry_ex

ISAACWiper Wiping Operations (3310)

```
FileW = CreateFileW(v1, GENERIC_WRITE|GENERIC_READ, 3u, 0, 3u, 0, 0);
hFile = FileW;
if ( FileW == (HANDLE)-1 )
  return v24;
BytesReturned = 0;
v3 = DeviceIoControl(FileW, FSCTL_LOCK_VOLUME, 0, 0, 0, 0, &BytesReturned, 0);
```

FSCTL_LOCK_VOLUME IOCTL (winioctl.h)

Article • 05/18/2021 • 2 minutes to read

Feedback

In this article

Remarks

Requirements

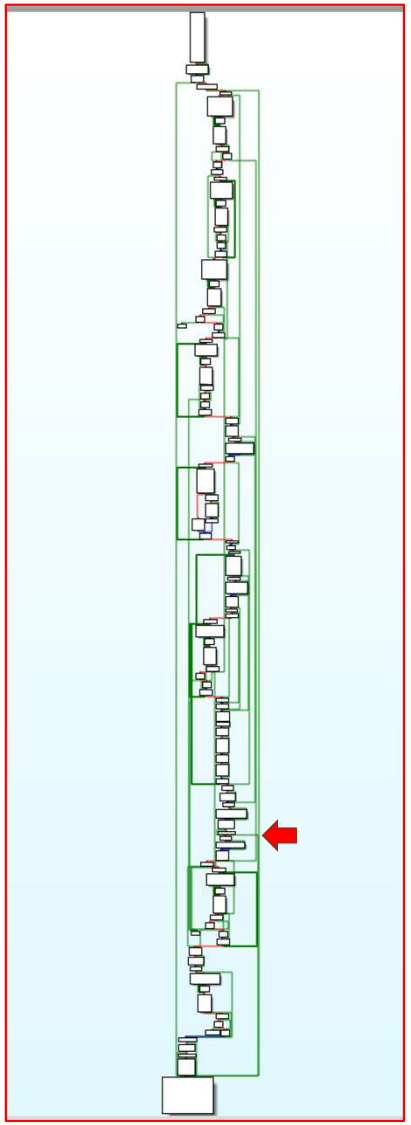
See also

Locks a volume if it is not in use. A locked volume can be accessed only through handles to the file object (*hDevice*) that locks the volume. For more information, see the Remarks section.

To perform this operation, call the DeviceIoControl function with the following parameters.

C++ Copy

```
BOOL DeviceIoControl(
  (HANDLE) hVolume,           // handle to a volume
  (DWORD) FSCTL_LOCK_VOLUME,  // dwIoControlCode
  NULL,                       // lpInBuffer
  0,                          // nInBufferSize
  NULL,                       // lpOutBuffer
  0,                          // nOutBufferSize
  (LPDWORD) lpBytesReturned,  // number of bytes returned
  NULL                        // OVERLAPPED structure
);
```



Reference: https://learn.microsoft.com/en-us/windows/win32/api/winioctl/ni-winioctl-fsctl_lock_volume

ISAACWiper Wiping Operations (3310 cont.)

```
v17 = 0;
v16[0] = GetTickCount();
for ( i = 1; i < 0x270; ++i )
  v16[i] = i + 1812433253 * (*(_DWORD *)&Buffer[4 * i + 65532] ^ (*(_DWORD *)&Buffer[4 * i + 65532] >> 30));
v10 = 624;                              // Degree of recurrence
v11 = Buffer;
v17 = 624;
do
{
  if ( v10 == 624 )
  {
    sub_10005AC0(v16);                  // Generate Random Seed
    v10 = v17;
  }
  v12 = v16[v10++];
  v17 = v10;
  v13 = ((((v12 >> 11) ^ v12) & 0xFF3A58AD) << 7) ^ (v12 >> 11) ^ v12;
  *(_DWORD *)v11 = ((v13 & 0xFFFFDF8C) << 15) ^ v13 ^ ((((v13 & 0xFFFFDF8C) << 15) ^ v13) >> 18);
  v11 += 4;
}
while ( v11 < (char *)v16 );
```

```
y = rand->mt[rand->index++];
y ^= (y >> 11);
y ^= (y << 7) & TEMPERING_MASK_B;
y ^= (y << 15) & TEMPERING_MASK_C;
y ^= (y >> 18);
return y;
```

Python “twist” implementation

A Mersenne Twister operates by maintaining a giant array of state, the initial state of which is our random seed. This array feeds each element through a series of operations to produce a new pseudo-random number. After exhausting the entire state array, the array is regenerated (“twisted”). To discuss these operations further, we must define a set of constants used in these operations. These constants correspond to MT19937[2], which is what the Python implementation corresponds to.

Constant	Value	Notes
w	32	Word size in bits
n	624	Degree of recurrence
r	31	Lower bits of bitmask
m	397	Offset to generate next state
a	0x9908b0df	Bottom row of twist transformation matrix
b	0x9d2c5680	Tempering bitmask
c	0xefc60000	Tempering bitmask
s	7	Tempering bit shift
t	15	Tempering bit shift
u	11	Tempering bit shift
l	18	Tempering bit shift

The process for generating a random numbers from the state array is as follows:

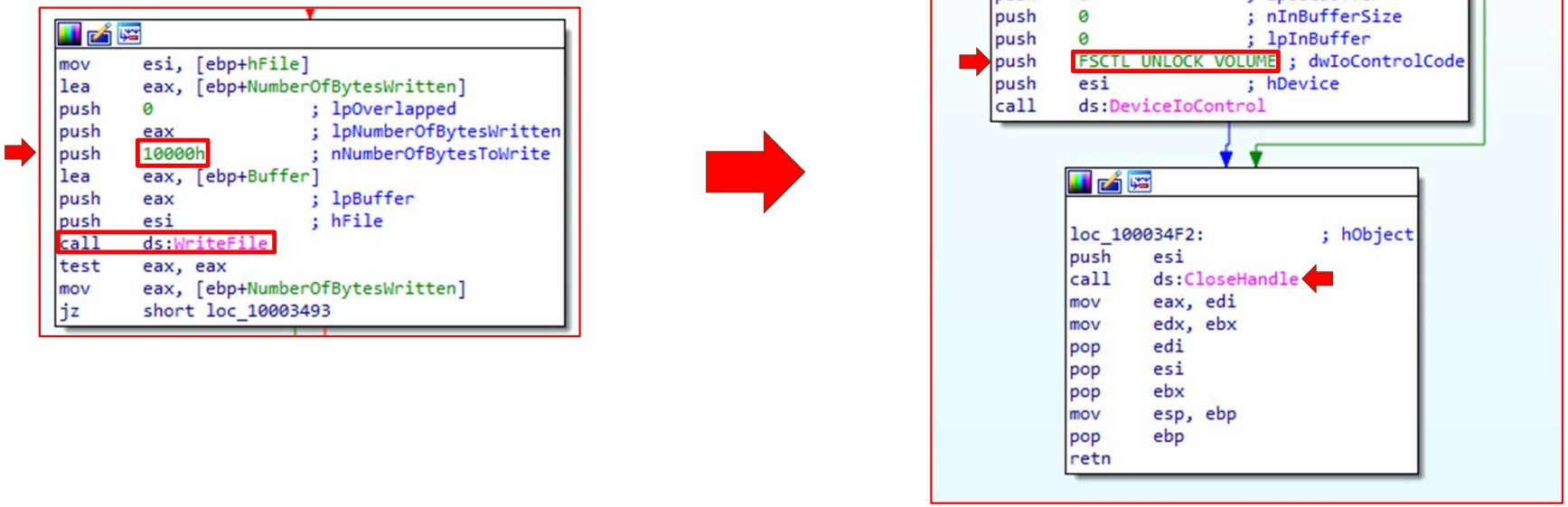
1. `y = x[i]`
2. `y = y ^ (y >> u)`
3. `y = y ^ ((y << s) & b)`
4. `y = y ^ ((y << t) & c)`
5. `y = y ^ (y >> l)`
6. Increment `i`
7. `return y`

Pseudocode “twist” implementation

Reference: https://blog.ollien.com/posts/reverse-mersenne-twister/

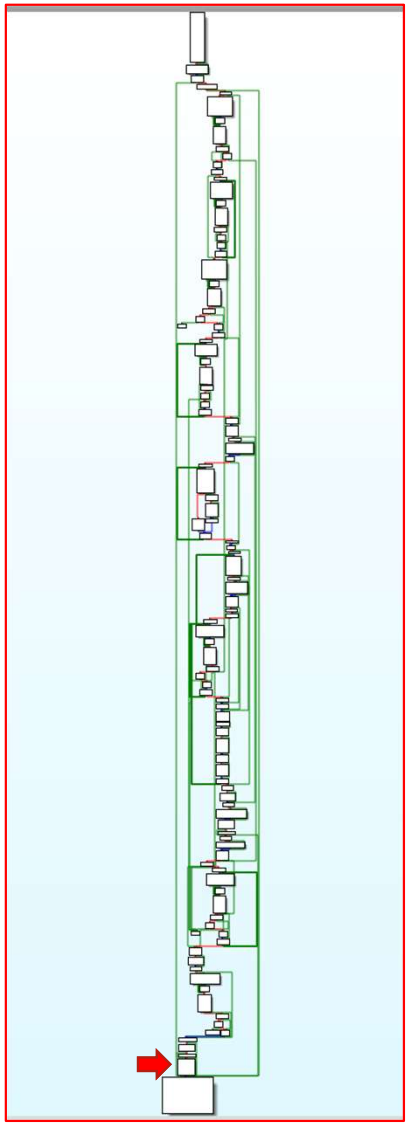
Reference: https://github.com/python/cpython/blob/main/Modules/_randommodule.c#L25

ISAACWiper Wiping Operations (3310 cont.)



ISAACWiper Wiping Operations (2500 cont.)

```
loc_1000303B:           ; lpThreadId
push    0
push    0               ; dwCreationFlags
lea     eax, [esp+2B48h+Parameter]
push    eax             ; lpParameter
push    offset sub_100039F0 ; lpStartAddress
push    0               ; dwStackSize
push    0               ; lpThreadAttributes
call    ds:CreateThread
lea     ecx, [esp+2B40h+Parameter]
mov     esi, eax
call    sub_10003700
push    0FFFFFFFFh      ; dwMilliseconds
push    esi             ; hHandle
call    ds:WaitForSingleObject
push    esi             ; hObject
call    ds:CloseHandle
```



ISAACWiper Wiping Operations (39F0)

Mersenne Twister Algorithm

```
TickCount = GetTickCount();
GetTempFileNameW((LPCWSTR)PathName, L"Tmd", TickCount, (LPWSTR)PathName);
CreateDirectoryW((LPCWSTR)PathName, 0);
SetFileAttributesW((LPCWSTR)PathName, FILE_ATTRIBUTE_HIDDEN);
for ( i = PathName; *i; ++i )
  ;
sub_100087F0(0x208u, (char *)TempFileName, (char *)PathName, 2 * (i - PathName) + 2);
v3 = GetTickCount();
GetTempFileNameW(TempFileName, L"Tmf", v3, TempFileName);
FileW = CreateFileW(TempFileName, GENERIC_WRITE|GENERIC_READ, 3u, 0, 2u, 0, 0);
hFile = FileW;
if ( FileW != (HANDLE)-1 )
{
  v5 = *((_DWORD *)lpThreadParameter + 14);
  v6 = *((_DWORD *)lpThreadParameter + 15);
  NumberOfBytesWritten = 0;
  while ( v6 || v5 >= 0x10000 )
  {
    v18 = 0;
    v17[0] = GetTickCount();
    for ( j = 1; j < 0x270; ++j )
      v17[j] = j
             + 1812433253 * (*(_DWORD *)&TempFileName[2 * j + 258] ^ (*(_DWORD *)&TempFileName[2 * j + 258] >> 30));
    v8 = 624;
    v9 = Buffer;
    v18 = 624;
    do
    {
      if ( v8 == 624 )
      {
        sub_10005AC0(v17);
        v8 = v18;
      }
      v10 = v17[v8++];
      v18 = v8;
      v11 = ((((v10 >> 11) ^ v10) & 0xFF3A58AD) << 7) ^ (v10 >> 11) ^ v10;
      *(_DWORD *)v9 = ((v11 & 0xFFFFDF8C) << 15) ^ v11 ^ ((((v11 & 0xFFFFDF8C) << 15) ^ v11) >> 18);
      v9 += 4;
    }
    while ( v9 < &vars0 );
    FileW = hFile;
    if ( !WriteFile(hFile, Buffer, 0x10000u, &NumberOfBytesWritten, 0) || NumberOfBytesWritten != 0x10000 )
      goto LABEL_20;
```

ISAACWiper Wiping Operations (GetTempFileNameW)

```
GetTempFileNameW(PathName, L"Tmf", TickCount, PathName);
```

C++ Copy

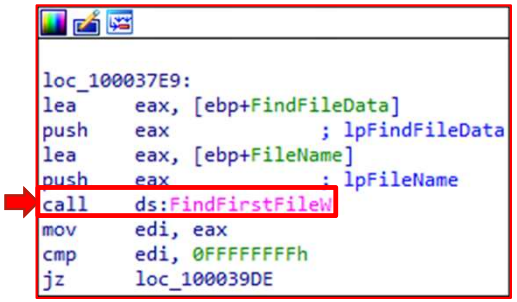
```
UINT GetTempFileNameA(
  [in]  LPCSTR lpPathName,
  [in]  LPCSTR lpPrefixString,
  [in]  UINT   uUnique,
  [out] LPSTR  lpTempFileName
);
```

GetTempFileNameW(“.”, ”Tmf”, TickCount, “.”)

File Write	process: rundll32.exe	path: C:\Tmd7B11.tmp	op: OpenModify	status: 0×00000000	
File Create	process: rundll32.exe	path: C:\Tmd7B11.tmp\Tmf7B30.tmp	op: CreateModify	status: 0×00000000	

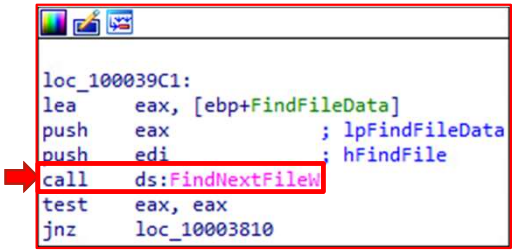
Reference: https://learn.microsoft.com/en-us/windows/win32/api/fileapi/nf-fileapi-gettempfilenamea

ISAACWiper Wiping Operations (3700)



```
loc_100037E9:
lea     eax, [ebp+FindFileData]
push    eax             ; lpFindFileData
lea     eax, [ebp+FileName]
push    eax             ; lpFileName
call    ds:FindFirstFileW
mov     edi, eax
cmp     edi, 0FFFFFFFFh
jz      loc_100039DE
```

```
if ( !(unsigned __int8)sub_10003560(FileName) )
{
  PathName[sub_100087F0(0x20Au, (char *)PathName, (char *)FileName, v25) >> 1] = 0;
  TickCount = GetTickCount();
  GetTempFileNameW(PathName, L"Tmf", TickCount, PathName);
  MoveFileW(FileName, PathName);
  sub_10003560(PathName);
}
```



```
loc_100039C1:
lea     eax, [ebp+FindFileData]
push    eax             ; lpFindFileData
push    edi             ; hFindFile
call    ds:FindNextFileW
test    eax, eax
jnz     loc_10003810
```

Sub_10003560

```
FileW = CreateFileW(this, GENERIC_WRITE|GENERIC_READ, 3u, 0, OPEN_EXISTING, 0, 0);
hFile = FileW;
if ( FileW != (HANDLE)-1 )
{
  GetFileSizeEx(FileW, &FileSize);
  HighPart = FileSize.HighPart;
  LowPart = FileSize.LowPart;
  v5 = sub_10025980(FileSize.LowPart, FileSize.HighPart, 0x10000, 0);
  NumberOfBytesWritten = 0;
  nNumberOfBytesToWrite = v5;
  v6 = LowPart < v5;
  for ( i = LowPart - v5; ; i -= 0x10000 )
  {
    HighPart -= v6;
    if ( !(HighPart | i) )
      break;
    v17 = 0;
    v16[0] = GetTickCount();
    for ( j = 1; j < 0x270; ++j )
      v16[j] = j + 1812433253 * (*(_DWORD *)&Buffer[4 * j + 65532] ^ (*(_DWORD *)&Buffer[4 * j + 65532] >> 30));
    v9 = 624;
    v10 = Buffer;
    v17 = 624;
    do
    {
      if ( v9 == 624 )
      {
        sub_10005AC0(v16);
        v9 = v17;
      }
      v11 = v16[v9++];
      v17 = v9;
      v12 = ((((v11 >> 11) ^ v11) & 0xFF3A58AD) << 7) ^ (v11 >> 11) ^ v11;
      *(_DWORD *)v10 = ((v12 & 0xFFFFDF8C) << 15) ^ v12 ^ ((((v12 & 0xFFFFDF8C) << 15) ^ v12) >> 18);
      v10 += 4;
    }
    while ( v10 < (char *)v16 );
    FileW = hFile;
    if ( !WriteFile(hFile, Buffer, 0x10000u, &NumberOfBytesWritten, 0) || NumberOfBytesWritten != 0x10000 )
```

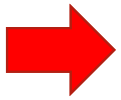
ISAACWiper Execution

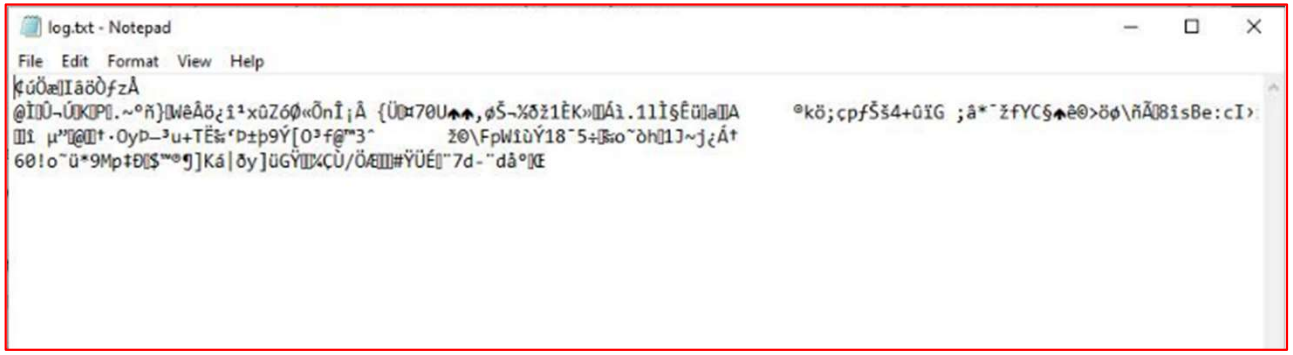
File Create	process: rundll32.exe	path: C:\ProgramData\log.txt	op: CreateModify	status: 0×00000000
File Read	process: rundll32.exe	path: \??\PhysicalDrive0	op: OpenRead	status: 0×00000000
File Read	process: rundll32.exe	path: \??\PhysicalDrive1	op: OpenRead	status: 0xC0000034
File Read	process: rundll32.exe	path: \??\C:	op: OpenRead	status: 0×00000000
File Read	process: rundll32.exe	path: \??\PhysicalDrive0	op: OpenRead	status: 0×00000000
File Read	process: rundll32.exe	path: \??\C:	op: OpenRead	status: 0×00000000
File Read	process: rundll32.exe	path: \??\D:	op: OpenRead	status: 0×00000000
File Write	process: rundll32.exe	path: \??\PhysicalDrive0	op: OpenModify	status: 0×00000000
File Write	process: rundll32.exe	path: \??\C:	op: OpenModify	status: 0×00000000
File Read	process: rundll32.exe	path: \??\C:\	op: Unknown	status: 0×00000000

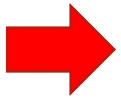
File Read	process: rundll32.exe	path: C:\Tmd7B11.tmp	op: Unknown	status: 0×00000000
File Write	process: rundll32.exe	path: C:\Tmd7B11.tmp	op: OpenModify	status: 0×00000000
File Create	process: rundll32.exe	path: C:\Tmd7B11.tmp\Tmf7B30.tmp	op: CreateModify	status: 0×00000000

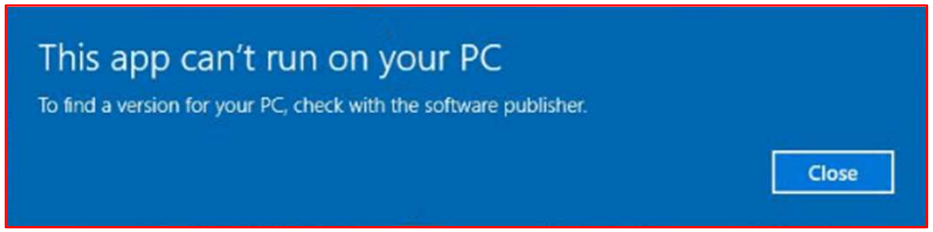
ISAACWiper Execution cont.

```
getting drives...

physical drives:
-- system physical drive 0: PhysicalDrive0

logical drives:
-- system logical drive: C:
-- logical drive: D:

start erasing system physical drive...

system physical drive -- FAILED
start erasing system logical drive C:
```

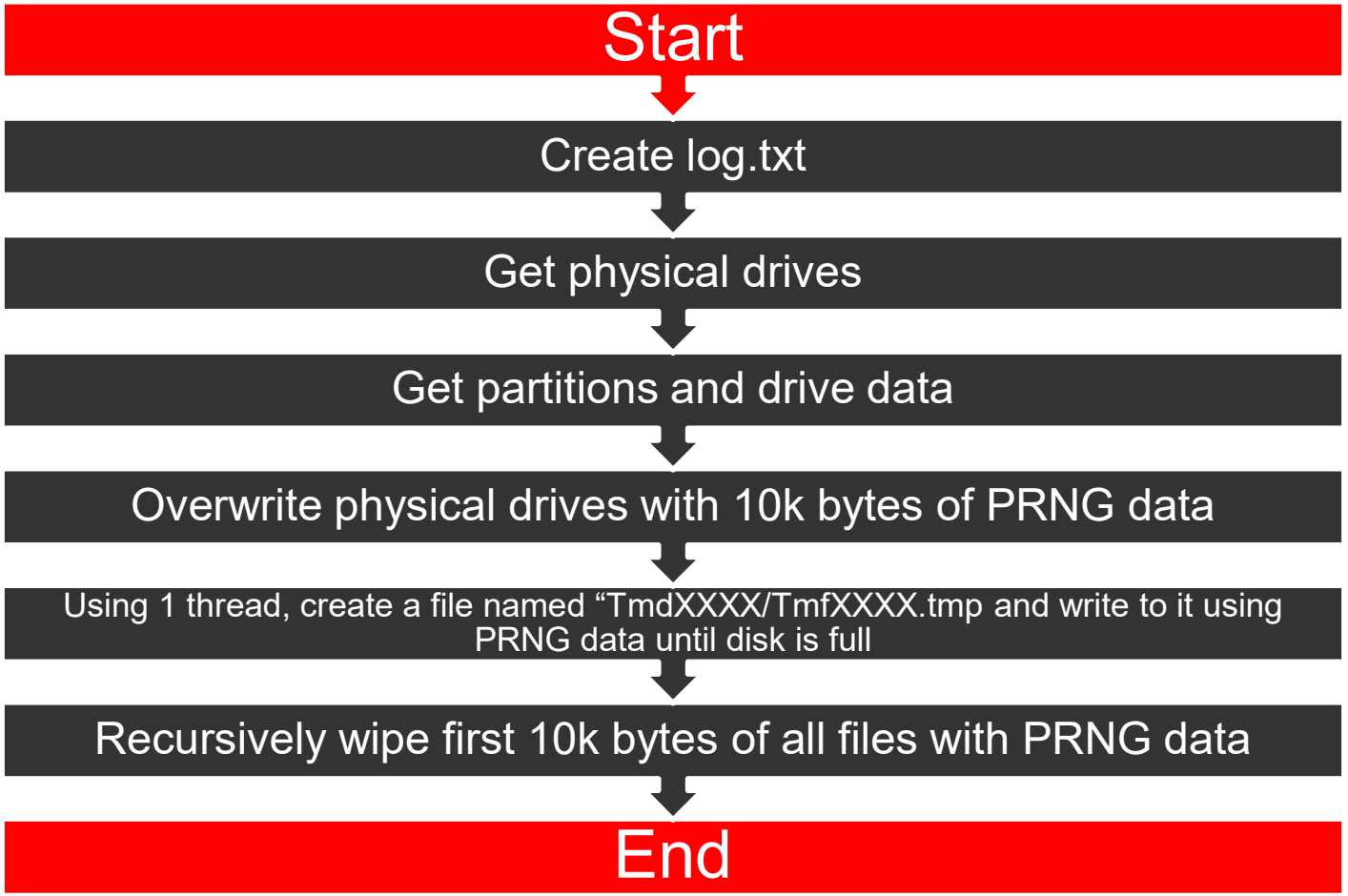








ISAACWiper Recap



ISAACWiper?

More like…

MersenneTwisterWiper

YARA Signature (ISAACWiper)

```
rule isaacwiper_wg {

    meta:
        author = "Ryan Estes"
        date = "2023-01-07"
        category = "Wiper"
        wiper = "ISAACWiper"
        description = "YARA rule for ISAACWiper, created for WatchGuard Wipers presentation."

        hash0 = 13037b749aa4b1eda538fda26d6ac41c8f7b1d02d83f47b0d187dd645154e033
        hash1 = 7bcd4ec18fc4a56db30e0aaebd44e2988f98f7b5d8c14f6689f650b4f11e16c0
        hash2 = abf9adf2c2c21c1e8bd69975dfccb5ca53060d8ele7271a5e9ef3b56a7e54d9f
        hash3 = afe1f2768e57573757039a40ac40f3c7471bb084599613b3402b1e9958e0d27a

    strings:
        $s0 = "_Start@4"
        $s1 = "Tmd"
        $s2 = "Tmf"
        $s3 = "\\.\"
        $s4 = "PhysicalDrive"

        $dbg0 = "cleaner.dll"
        $dbg1 = "C:\Programata\log.txt"
        $dbg2 = "start erasing physical drives..."
        $dbg3 = "start erasing system physical drive..."
        $dbg4 = "start erasing system logical drive"
        $dbg5 = "getting drives..."
        $dbg6 = "physical drives:"
        $dbg7 = "-- system physical drive"
        $dbg8 = "-- physical drive"
        $dbg9 = "logical drives:"
        $dbg10 = "-- system logical drive:"
        $dbg11 = "-- logical drive:"
        $dbg12 = "-- FAILED"
        $dbg13 = "physical drive"
        $dbg14 = "-- start erasing logical drive"
        $dbg15 = "system physical drive -- FAILED"

    rule has_strings:
    {
        condition:
            (all of ($s*))
    }
    rule has_dbg:
    {
        condition:
            (all of ($dbg*))
    }

    rule is_pe:
    {
        condition:
            pe.is_pe
    }

    rule is_dll:
    {
        condition:
            pe.characteristics & pe.DLL
    }

    rule has_export:
    {
        condition:
            pe.exports("_Start@4")
    }

    condition:
        (has_strings or has_dbg) and (is_pe or is_dll) and (has_export)
}
```

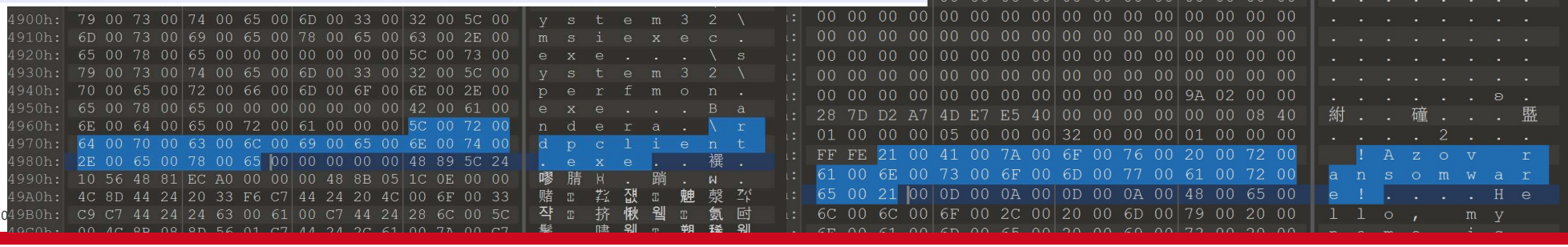

Technical Analysis (Azov Ransomware)

Azov Ransomware

- TBD

YARA Signature (Azov)

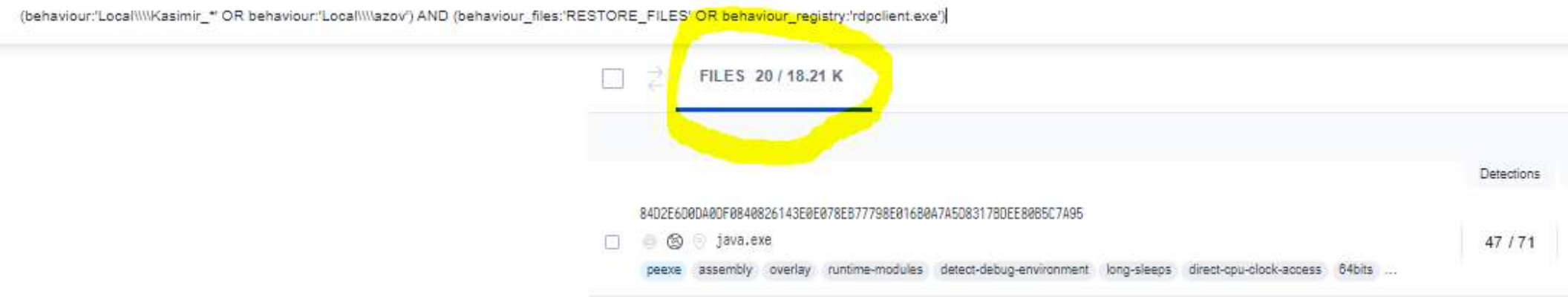
```
rule win64_azov_ransomware {

    meta:
        author = "Ashu Sharma"
        date = "4-1-2023"
        version = "1"
        description = "Detects Win64/AzovRansomware which is fake ransomware and backdoor dropper with wiper fuctionality."
        hash = "650f0d694c0928d88aeeed649cf629fc8a7bec604563bca716b1688227e0cc7e"


    /* Note
     * The strings used in this rule have been extracted from the decryptor of malicious code and the strings extracted from static file
     */

    strings:
        $decryptor = { 48 C7 C1 ?? ?? ?? ?? 41 B9 13 5C 01 00 41 BA ?? ?? ?? ?? 48 FF C9 8A 40 ?? 44 30 CA 88 40 8 41 81 EA ?? ?? ?? ?? 45
            //  48:C7C1 E03F0000                | mov rcx,3FE0                          | counter Variable
            //  41:B9 135C0100                  | mov r9d,15C13                         | key
            //  41:BA 00928192                  | mov r10d,92819200                     | seed initialization
            //  48:FFC9                         | dec rcx                               |
            //  8A1408                          | mov dl,byte ptr ds:[rax+rcx]          |
            //  44:30CA                         | xor dl,r9b                            | decrption operation
            //  881408                          | mov byte ptr ds:[rax+rcx],dl          | copying code in byte array
            //  41:81EA E26F0200                | sub r10d,26FE2                        |
            //  45:01D1                         | add r9d,r10d                          | r9d:EntryPoint
            //  41:81C1 E26F0200                | add r9d,26FE2                         | r9d:EntryPoint
            //  41:81C2 E26F0200                | add r10d,26FE2                        |
            //  41:D1C1                         | rol r9d,1                             | r9d:EntryPoint

        $Paternl = {21 00 41 00 7A 00 6F 00 76 00 20 00 72 00 61 00 6E 00 73 00 6F 00 6D 00 77 00 61 00 72 00 65 00 21}
        // "Azov ransomware!" in Unicode

        $Patern2 = {5C 00 72 00 64 00 70 00 63 00 6C 00 69 00 65 00 6E 00 74 00 2E 00 65 00 78 00 65}
        // "\rdpclient.exe" in unicode


    condition:
        uint16(0) == 0x5a4d and pe.is_64bit() and $code and any of ($Patern*)
}
```



VirusTotal Query (Azov)

- VirusTotal query – Azov-related samples

(behaviour:'Local\\\\Kasimir_*'
OR behaviour:'Local\\\\azov')
AND
(behaviour_files:'RESTORE_FILES'
OR behaviour_registry:'rdpclient.exe')




Postmortem and Recommendations

Consequences

- Most strategically impactful cyber operation in wartime history.
- Ability to paralyze Ukrainian decision-making and critical infrastructure
- Signs of coordination between Russian kinetic and cyber operations
- Cyber operations intended to disrupt, destroy, or manipulate data or systems.

The Cost of Cyberwarfare

- Ukrainian President Volodymyr Zelensky accused Russia of 'energy terrorism' and said that about 4.5 million Ukrainian consumers were temporarily disconnected from the power supply.
- Also referred to the water shortages.
- includes a hack, which the White House blamed on the Kremlin, that disrupted satellite internet communications in Ukraine on the eve of Russia's invasion.
- In 2017, NotPetya wiped computer systems at companies across Ukraine before spreading around the world; The incident cost the global economy billions of dollars by disrupting shipping giant Maersk and other multinational firms.
- Groups are currently working on some high-complexity attacks that we will observe later on.

Recommendations for users & organizations

- ✓ Know what your critical assets are and what software is running on them.
- ✓ Keep your software up to date. Prioritize patching critical and high vulnerabilities that allow remote code execution.
- ✓ Enforce Multifactor Authentication (MFA) to the greatest extent possible.
- ✓ Require the use of a password manager to generate strong and unique passwords for each separate account.
- ✓ Backup all the essential files on the cloud and external drives and regularly maintain them.
- ✓ Train your employees to recognize phishing emails, suspicious websites, infected links or other abnormalities to prevent successful compromise of email accounts.

Sample Hashes (SHA256)

AcidRain:
9b4dfaca873961174ba935fddaf696145afe7bbf5734509f95feb54f3584fd9a

Azov Ransomware:
b102ed1018de0b7faea37ca86f27ba3025c0c70f28417ac3e9ef09d32617f801
650f0d694c0928d88aeeed649cf629fc8a7bec604563bca716b1688227e0cc7e

CaddyWiper:
a294620543334a721a2ae8eaaf9680a0786f4b9a216d75b55cfd28f39e9430ea
7f76e7a9e784b90463a67ad40b1acf68c6e706fe489f82058ae608dbc203f832

CryWiper:
bdf8b53d73ca1ed1b649b32a61608b2cf952397ef3d5fc2e6e9f41ad98c40110

DesertBlade:
a196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92
dcbbae5a1c61dbbbb7dcd6dc5dd1eb1169f5329958d38b58c3fd9384081c9b78

dnWipe:
610ec163e7b34abd5587616db8dac7e34b1aef68d0260510854d6b3912fb0008

DoubleZero:
3b2e708eaa4744c76a633391cf2c983f4a098b46436525619e5ea44e105355fe
30b3cbe8817ed75d8221059e4be35d5624bd6b5dc921d4991a7adc4c3eb5de4a

HermeticWiper:
5a300f72e221a228e3a36a043bef878b570529a7abc15559513ea07ae280bb48
2d29f9ca1d9089ba0399661bb34ba2fd8aba117f04678cd71856d5894aa7150b
a259e9b0acf375a8bef8dbc27a8a1996ee02a56889cba07ef58c49185ab033ec
1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591
2c10b2ec0b995b88c27d141d6f7b14d6b8177c52818687e4ff8e6ecf53adf5bf
3c557727953a8f6b4788984464fb77741b821991acbf5e746aebdd02615b1767
0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da
06086c1da4590dcc7f1e10a6be3431e1166286a9e7761f2de9de79d7fda9c397
b6f2e008967c5527337448d768f2332d14b92de22a1279fd4d91000bb3d4a0fd
fd7eacc2f87aceac865b0aa97a50503d44b799f27737e009f91f3c281233c17d
b01e0c6ac0b8bcde145ab7b68cf246deea9402fa7ea3aede7105f7051fe240c1
e5f3ef69a534260e899a36cec459440dc572388defd8f1d98760d31c700f42d5
23ef301ddba39bb00f0819d2061c9c14d17dc30f780a945920a51bc3ba0198a4
2c7732da3dcfc82f60f063f2ec9fa09f9d38d5cfbe80c850ded44de43bdb666d
8c614cf476f871274aa06153224e8f7354bf5e23e6853358591bf35a381fb75b
96b77284744f8761c4f2558388e0aee2140618b484ff53fa8b222b340d2a9c84

IsaacWiper:
13037b749aa4b1eda538fda26d6ac41c8f7b1d02d83f47b0d187dd645154e033
7bcd4ec18fc4a56db30e0aaebd44e2988f98f7b5d8c14f6689f650b4f11e16c0
abf9adf2c2c21c1e8bd69975dfccb5ca53060d8e1e7271a5e9ef3b56a7e54d9f
afe1f2768e57573757039a40ac40f3c7471bb084599613b3402b1e9958e0d27a

PartyTicket Ransomware:
4dc13bb83a16d4ff9865a51b3e4d24112327c526c1392e14d56f20d6f4eaf382

Nominatus_ToxicBattery:
45e433d6fd0710d2905f21fda25c02fccab9eef43732384f0f0ea65ee464b936

Prestige Ransomware:
5dd1ca0d471dee41eb3ea0b6ea117810f228354fc3b7b47400a812573d40d91d
5fc44c7342b84f50f24758e39c8848b2f0991e8817ef5465844f5f2ff6085a57
6cff0bbd62efe99f381e5cc0c4182b0fb7a9a34e4be9ce68ee6b0d0ea3eee39c

RansomBoggs:
78dcf144e82e947c20f152a8a57376b43e7aac3fee4bf1d18d22d4c14b25e56f
a490d03e780a6b664da65e20afa7845c6f79af60b6a496ff113bf9e9034e77d0

RU_Ransom:
107da216ad99b7c0171745fe7f826e51b27b1812d435b55c3ddb801e23137d8f
1f36898228197ee30c7b0ec0e48e804caa6edec33e3a91eeaf7aa2c5bbb9c6e0
610ec163e7b34abd5587616db8dac7e34b1aef68d0260510854d6b3912fb0008
696b6b9f43e53387f7cef14c5da9b6c02b6bf4095849885d36479f8996e7e473
8f2ea18ed82085574888a03547a020b7009e05ae0ecbf4e9e0b8fe8502059aae
979f9d1e019d9172af73428a1b3cbdff8aec8fdbe0f67cba48971a36f5001da9

Somnia Ransomware:
100c5e4d5b7e468f1f16b22c05b2ff1cfaa02eafa07447c7d83e2983e42647f0
ac5e68c15f5094cc6efb8d25e1b2eb13d1b38b104f31e1c76ce472537d715e08
156965227cbeeb0e387cb83adb93ccb3225f598136a43f7f60974591c12fafcf
e449c28e658bafb7e32c89b07ddee36cadeddfc77f17dd1be801b134a6857aa9

WhisperGate:
a196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92
44ffe353e01d6b894dc7ebe686791aa87fc9c7fd88535acc274f61c2cf74f5b8
dcbbae5a1c61dbbbb7dcd6dc5dd1eb1169f5329958d38b58c3fd9384081c9b78

Industroyer2:
d69665f56ddef7ad4e71971f06432e59f1510a7194386e5f0e8926aea7b88e00

AwfulShred:
bcdf0bd8142a4828c61e775686c9892d89893ed0f5093bdc70bde3e48d04ab99

OrcShred:
NONE

SoloShred:
NONE

Open for Q&A

Ashu.Sharma@watchguard.com
Ryan.Estes@watchguard.com

Thank you!

References

1. https://arstechnica.com/information-technology/2022/12/never-before-seen-malware-is-nuking-data-in-russias-courts-and-mayors-offices/
2. https://avertium.com/blog/hermeticwizard-hermeticransom-isaacwiper-target-ukraine
3. https://bitdefender.com/blog/hotforsecurity/russian-courts-attacked-by-crywiper-malware-that-poses-as-ransomware/
4. https://bleepingcomputer.com/news/security/ukraine-says-russian-hacktivists-use-new-somnia-ransomware/
5. https://blog.checkpoint.com/2022/12/12/from-disruption-to-destruction-azov-ransomware-presents-a-new-shift-towards-destructive-wipers/
6. https://blog.ollien.com/posts/reverse-mersenne-twister/
7. https://blogs.vmware.com/security/2022/04/ruransom-a-retaliatory-wiper.html
8. https://cert.gov.ua/article/2724253
9. https://cert.gov.ua/article/38088
10. https://cert.gov.ua/article/39518
11. https://cisa.gov/uscert/ncas/analysis-reports/ar22-115b
12. https://crowdstrike.com/blog/how-to-decrypt-the-partyticket-ransomware-targeting-ukraine/
13. https://crowdstrike.com/blog/technical-analysis-of-whispergate-malware/
14. https://crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-1/
15. https://crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-2/
16. https://crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-3/
17. https://crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-4/
18. https://csis.org/analysis/cyber-war-and-ukraine
19. https://cyberconflicts.cyberpeaceinstitute.org/threats
20. https://cyberconflicts.cyberpeaceinstitute.org/threats/attack-details
21. https://cyberpeaceinstitute.org/ukraine-timeline-of-cyberattacks/
22. https://cyfirma.com/outofband/prestige-ransomware-analysis/
23. https://esentire.com/blog/esentire-threat-intelligence-malware-analysis-caddywiper
24. https://europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf
25. https://fortinet.com/blog/threat-research/the-increasing-wiper-malware-threat
26. https://github.com/eset/malware-ioc/tree/master/ua_wipers
27. https://github.com/python/cpython/blob/main/Modules/_randommodule.c#L25
28. https://i.blackhat.com/USA-22/Wednesday/US-22-Cherepanov-Industroyer2-Sandworms-Cyberwarfare-Targets-Ukraines-Power-Grid-Again.pdf

References

29. https://iisf.ie/wiper-malware
30. https://inquest.net/blog/2022/04/07/ukraine-cyberwar-overview
31. https://learn.microsoft.com/en-us/windows-hardware/drivers/ddi/ntddstor/ni-ntddstor-ioctl_storage_get_device_number
32. https://learn.microsoft.com/en-us/windows-hardware/drivers/ddi/wdm/ns-wdm-_device_object
33. https://learn.microsoft.com/en-us/windows-hardware/drivers/kernel/specifying-device-types
34. https://learn.microsoft.com/en-us/windows/win32/api/fileapi/nf-fileapi-getdiskfreespaceexw
35. https://learn.microsoft.com/en-us/windows/win32/api/ioapiset/nf-ioapiset-deviceiocontrol
36. https://learn.microsoft.com/en-us/windows/win32/api/winioctl/ni-winioctl-fsctl_lock_volume
37. https://learn.microsoft.com/en-us/windows/win32/api/winioctl/ni-winioctl-ioctl_disk_get_drive_geometry_ex
38. https://learn.microsoft.com/en-us/windows/win32/api/winuser/nf-winuser-exitwindowsex
39. https://microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland/
40. https://msrc-blog.microsoft.com/2022/02/28/analysis-resources-cyber-threat-activity-ukraine/
41. https://politico.com/news/2022/12/07/estonia-ukraine-cybersecurity-russian-hackers-00072925
42. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd
43. https://research.checkpoint.com/2022/pulling-the-curtains-on-azov-ransomware-not-a-skidsware-but-polymorphic-wiper/
44. https://sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/
45. https://sentinelone.com/labs/hermetic-wiper-ukraine-under-attack/
46. https://splunk.com/en_us/blog/security/threat-update-doublezero-destructor.html
47. https://techtarget.com/searchsecurity/news/252528410/Check-Point-classifies-Azov-as-wiper-not-ransomware
48. https://trellix.com/en-us/about/newsroom/stories/research/wipermania-an-all-you-can-wipe-buffet.html
49. https://trendmicro.com/en_us/research/22/c/cyberattacks-are-prominent-in-the-russia-ukraine-conflict.html
50. https://trendmicro.com/en_us/research/22/c/new-ruransom-wiper-targets-russia.html
51. https://trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war/
52. https://twitter.com/struppigel/status/1501473254787198977
53. https://unit42.paloaltonetworks.com/doublezero-net-wiper/
54. https://welivesecurity.com/2022/02/24/hermeticwiper-new-data-wiping-malware-hits-ukraine/
55. https://welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/
56. https://welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/
57. https://zscaler.com/blogs/security-research/technical-analysis-partyticket-ransomware