Kyberútoky počas vojny?

Toto ESET zachytil pred a počas invázie na Ukrajine

Digital Security
Progress. Protected.

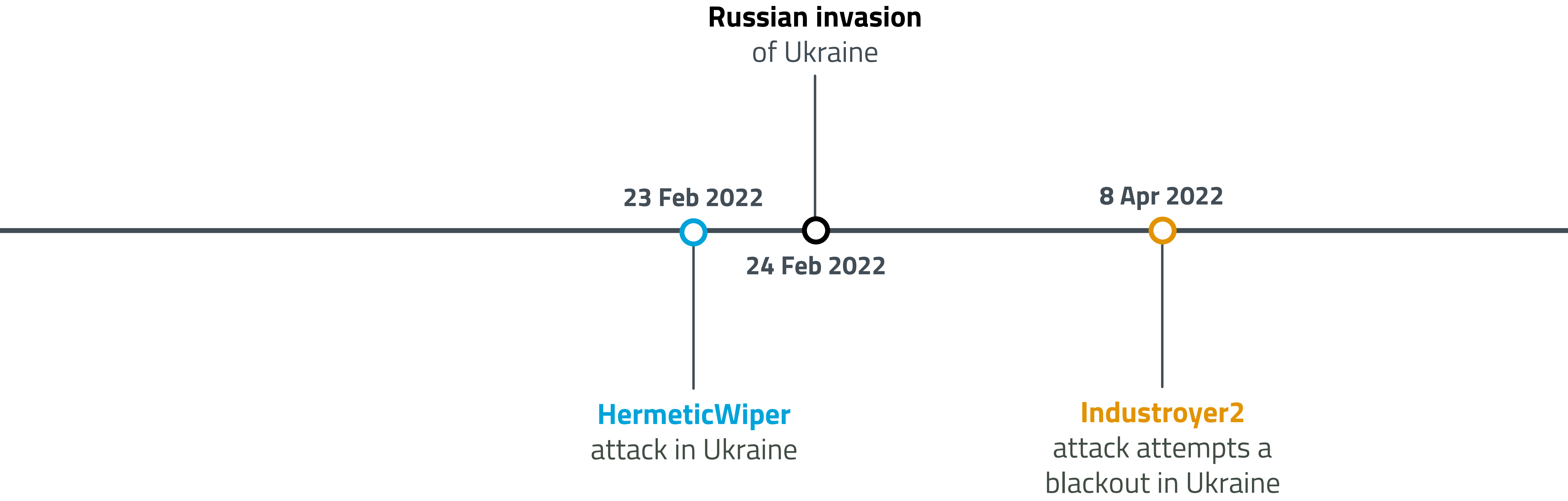
Robert Lipovsky

Principal Threat Intelligence Researcher

🐦@Robert_Lipovsky

Russian invasion
of Ukraine

24 Feb 2022



Russian invasion of Ukraine

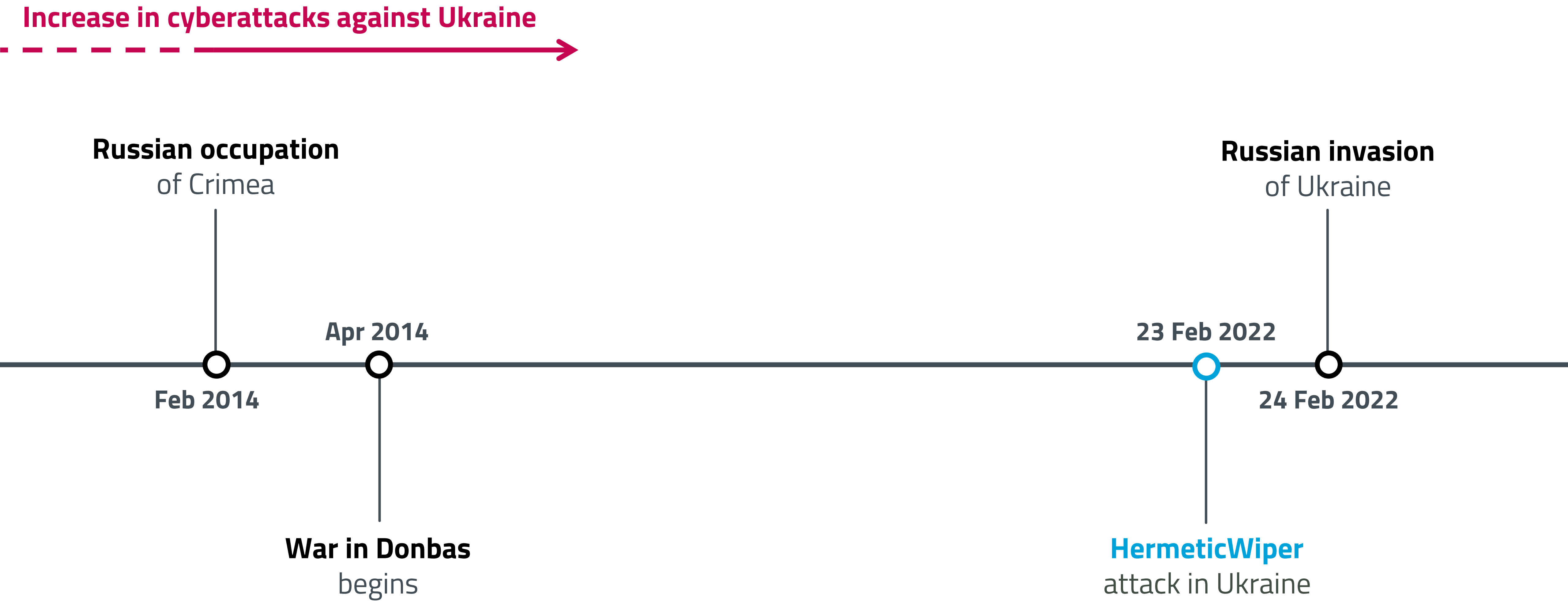
24 Feb 2022

23 Feb 2022

HermeticWiper attack in Ukraine

8 Apr 2022

Industroyer2 attack attempts a blackout in Ukraine



Increase in cyberattacks against Ukraine

Russian occupation of Crimea

Feb 2014

Apr 2014

War in Donbas begins

23 Feb 2022

HermeticWiper attack in Ukraine

24 Feb 2022

Russian invasion of Ukraine

Sandworm

Telebots/Voodoo Bear

Sednit

Fancy Bear/APT28

Lazarus

Operation In(ter)ception
Bluenoroff

The Dukes

Cozy Bear/APT29

Turla

TA428

InvisiMole

Buhtrap

Gamaredon

Sandworm

Telebots/Voodoo Bear

Sednit

Fancy Bear/APT28

Lazarus

Operation In(ter)ception

Bluenoroff

The Dukes

Cozy Bear/APT29

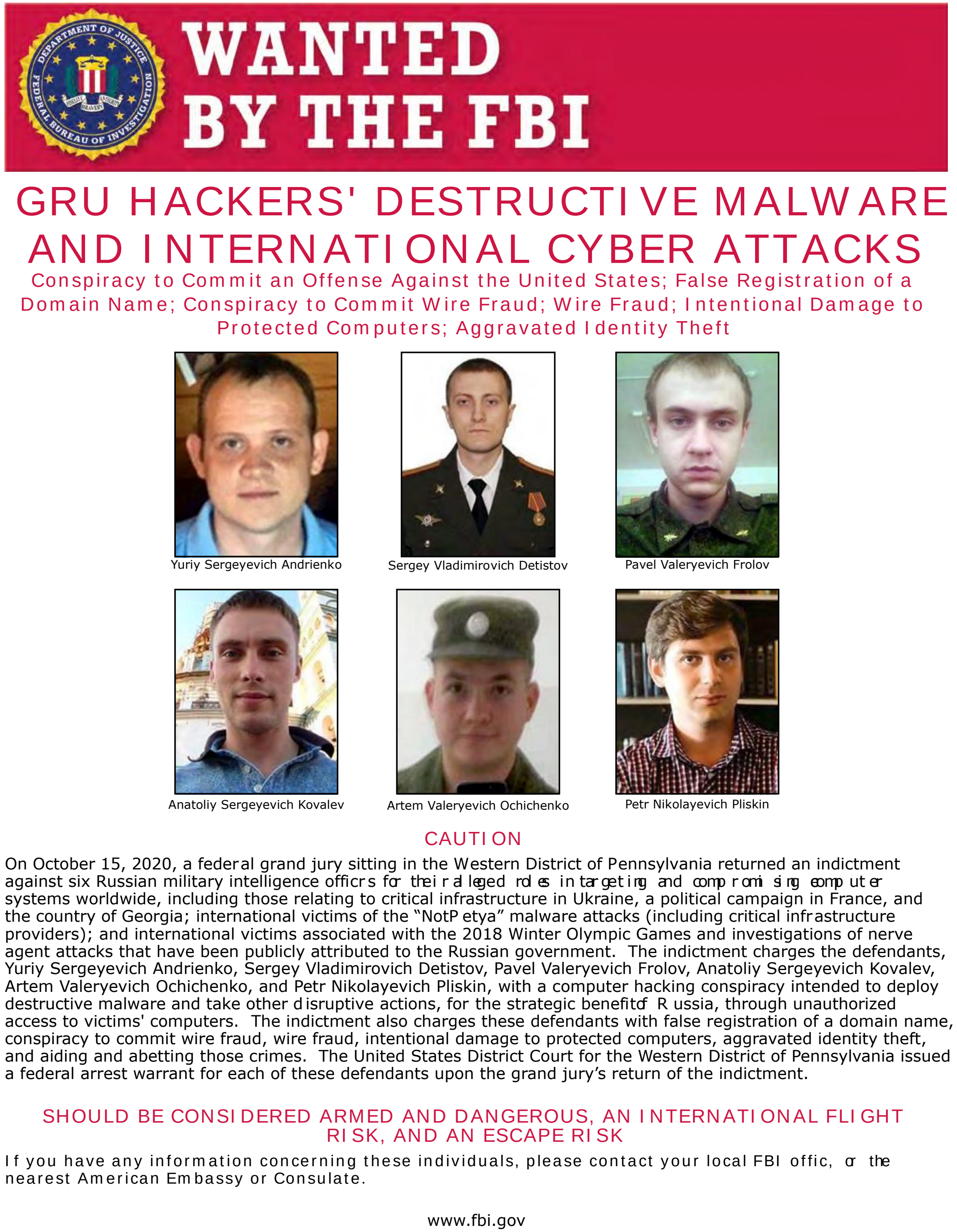
Turla

TA428

InvisiMole

Buhtrap

Gamaredon



WANTED BY THE FBI

GRU HACKERS' DESTRUCTIVE MALWARE AND INTERNATIONAL CYBER ATTACKS

Conspiracy to Commit an Offense Against the United States; False Registration of a Domain Name; Conspiracy to Commit Wire Fraud; Wire Fraud; Intentional Damage to Protected Computers; Aggravated Identity Theft

Yuriy Sergeyevich Andrienko

Sergey Vladimirovich Detistov

Pavel Valeryevich Frolov

Anatoliy Sergeyevich Kovalev

Artem Valeryevich Ochichenko

Petr Nikolayevich Pliskin

CAUTION

On October 15, 2020, a federal grand jury sitting in the Western District of Pennsylvania returned an indictment against six Russian military intelligence officrs for their alleged roles in targeting and compromising computer systems worldwide, including those relating to critical infrastructure in Ukraine, a political campaign in France, and the country of Georgia; international victims of the “NotPetya” malware attacks (including critical infrastructure providers); and international victims associated with the 2018 Winter Olympic Games and investigations of nerve agent attacks that have been publicly attributed to the Russian government. The indictment charges the defendants, Yuriy Sergeyevich Andrienko, Sergey Vladimirovich Detistov, Pavel Valeryevich Frolov, Anatoliy Sergeyevich Kovalev, Artem Valeryevich Ochichenko, and Petr Nikolayevich Pliskin, with a computer hacking conspiracy intended to deploy destructive malware and take other disruptive actions, for the strategic benefitof Russia, through unauthorized access to victims' computers. The indictment also charges these defendants with false registration of a domain name, conspiracy to commit wire fraud, wire fraud, intentional damage to protected computers, aggravated identity theft, and aiding and abetting those crimes. The United States District Court for the Western District of Pennsylvania issued a federal arrest warrant for each of these defendants upon the grand jury’s return of the indictment.

SHOULD BE CONSIDERED ARMED AND DANGEROUS, AN INTERNATIONAL FLIGHT RISK, AND AN ESCAPE RISK

If you have any information concerning these individuals, please contact your local FBI office, or the nearest American Embassy or Consulate.

www.fbi.gov

https://95.143.193.182/**Franceaviatelecom8**/statmach/aorta.php

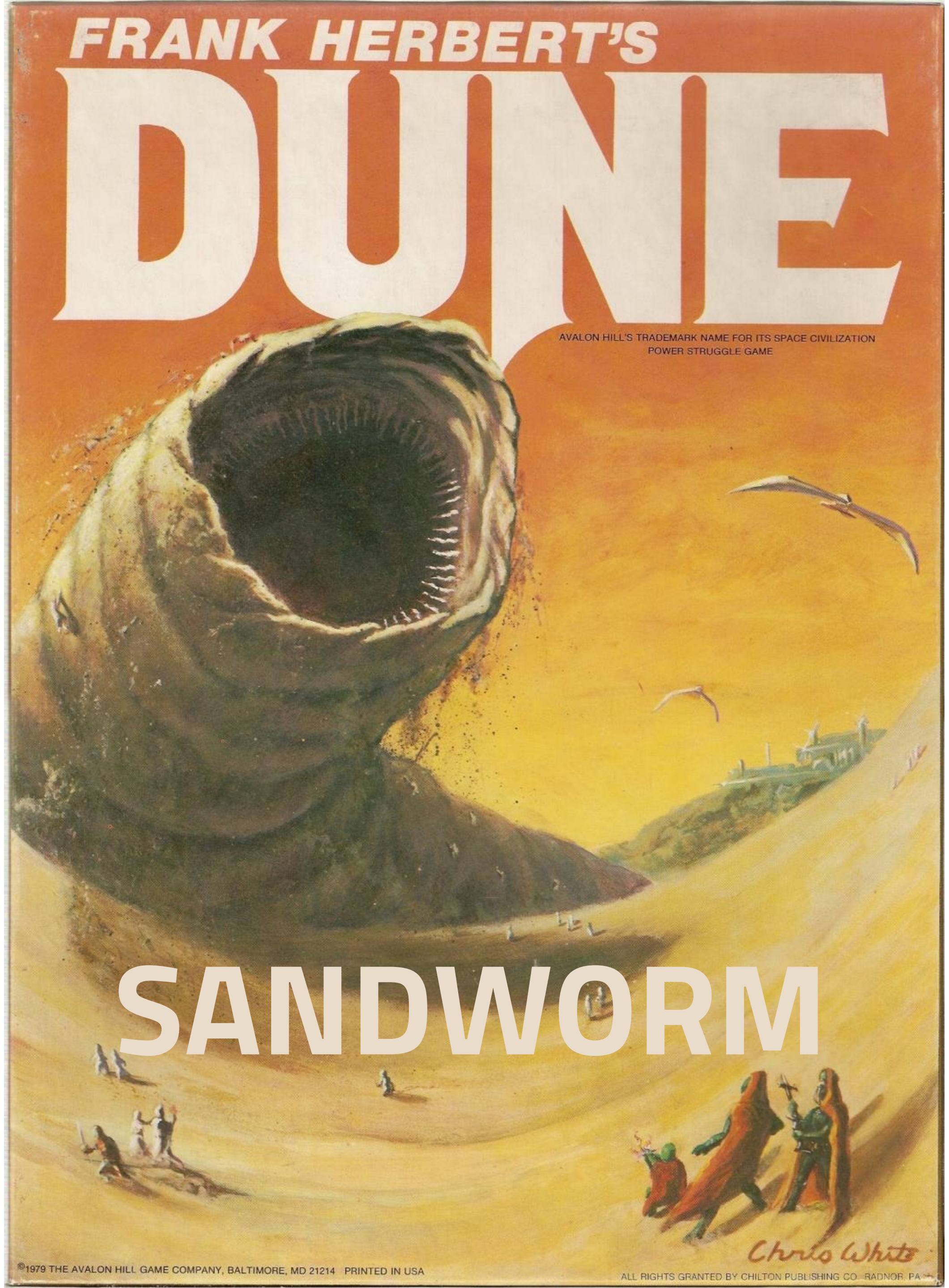
https://5.61.38.31/**epsiloneridani0**/setattr.php

https://144.76.119.48/**arrakis02**/loadvers/paramctrl.php

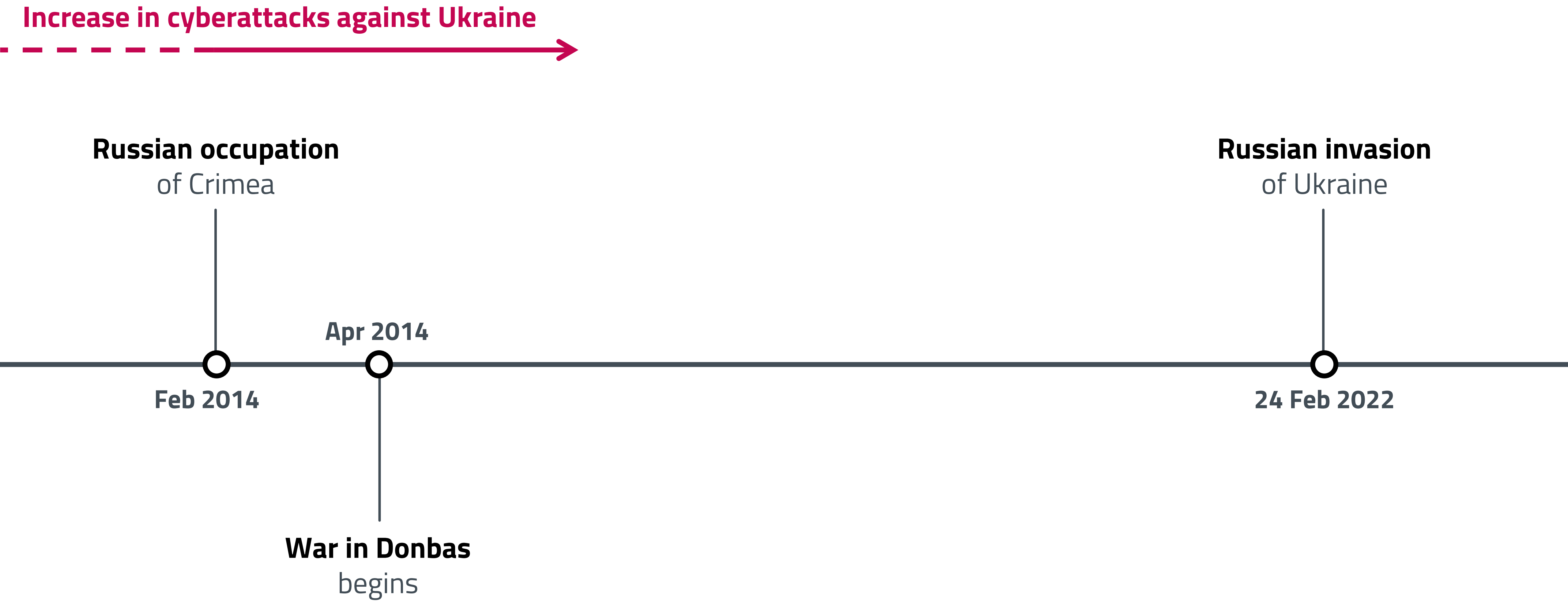
https://78.46.40.239/**SalusaSecundus2**/segments/statinfo.php

https://95.143.193.131/**houseatreides94**/dirconf/check.php

https://46.165.222.6/**BasharoftheSardaukars**/tempreports/vercontrol.php


FRANK HERBERT'S
DUNE
AVALON HILL'S TRADEMARK NAME FOR ITS SPACE CIVILIZATION POWER STRUGGLE GAME
Chris White
©1979 THE AVALON HILL GAME COMPANY, BALTIMORE, MD 21214 PRINTED IN USA
ALL RIGHTS GRANTED BY CHILTON PUBLISHING CO. RADNOR, PA

SANDWORM



Increase in cyberattacks against Ukraine

Russian occupation of Crimea

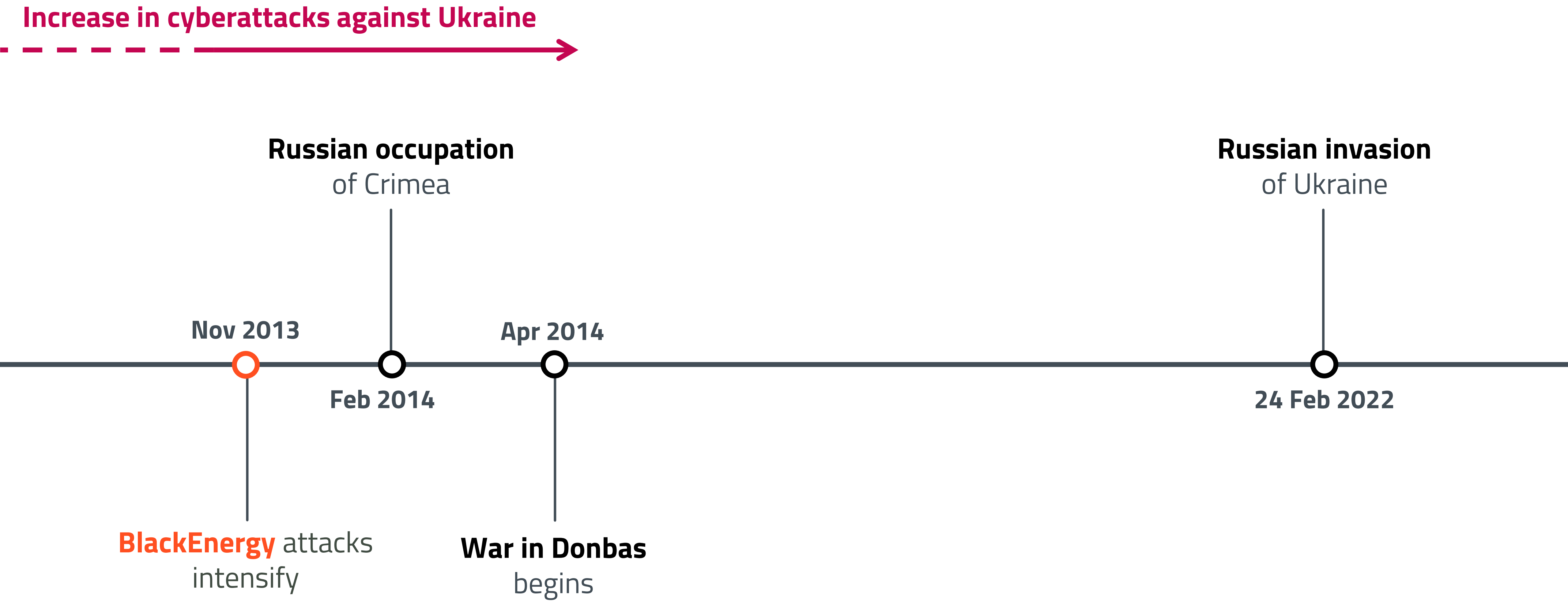
Feb 2014

Apr 2014

War in Donbas begins

Russian invasion of Ukraine

24 Feb 2022



Increase in cyberattacks against Ukraine

Nov 2013

BlackEnergy attacks intensify

Feb 2014

Russian occupation of Crimea

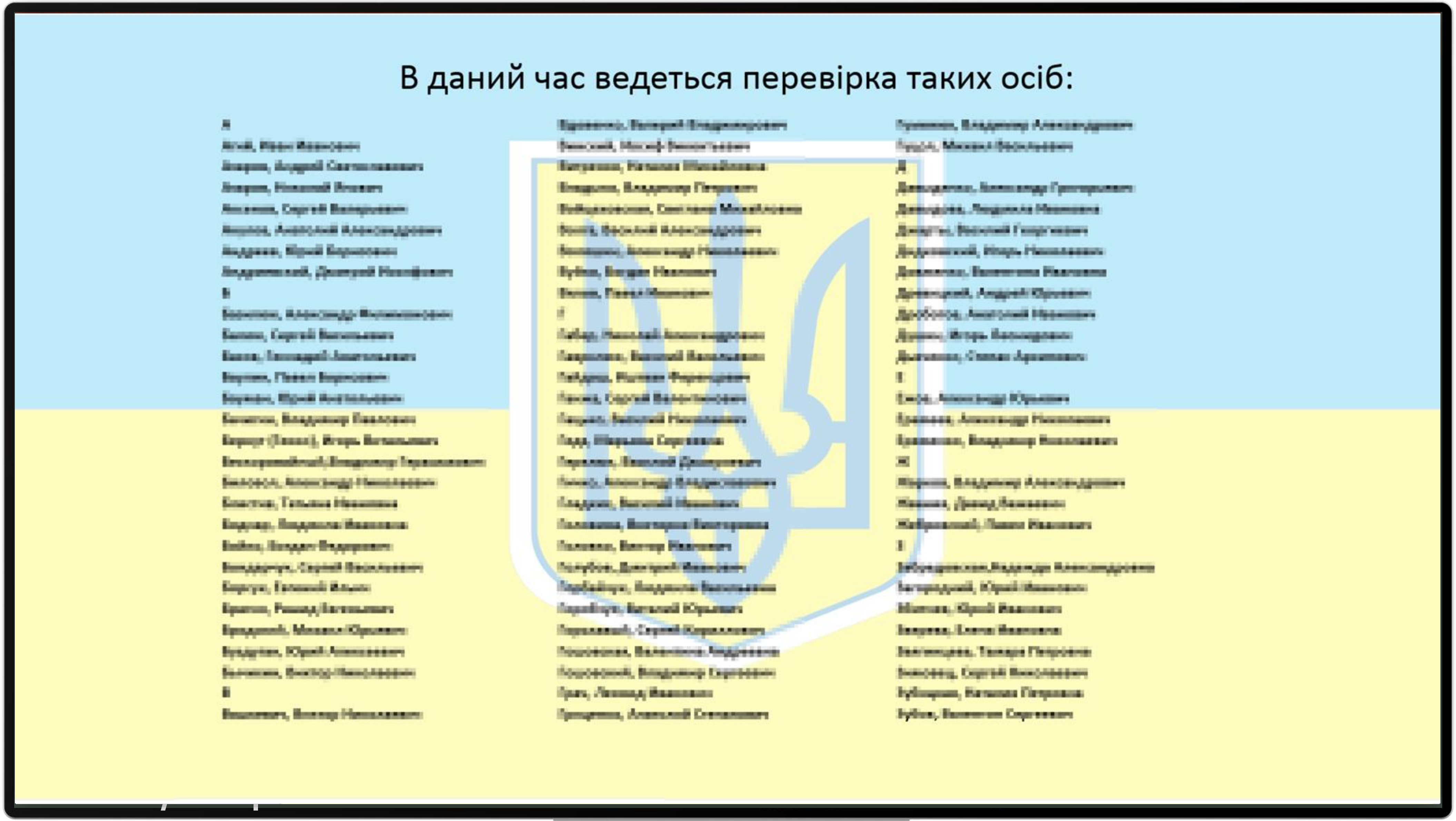
Apr 2014

War in Donbas begins

24 Feb 2022

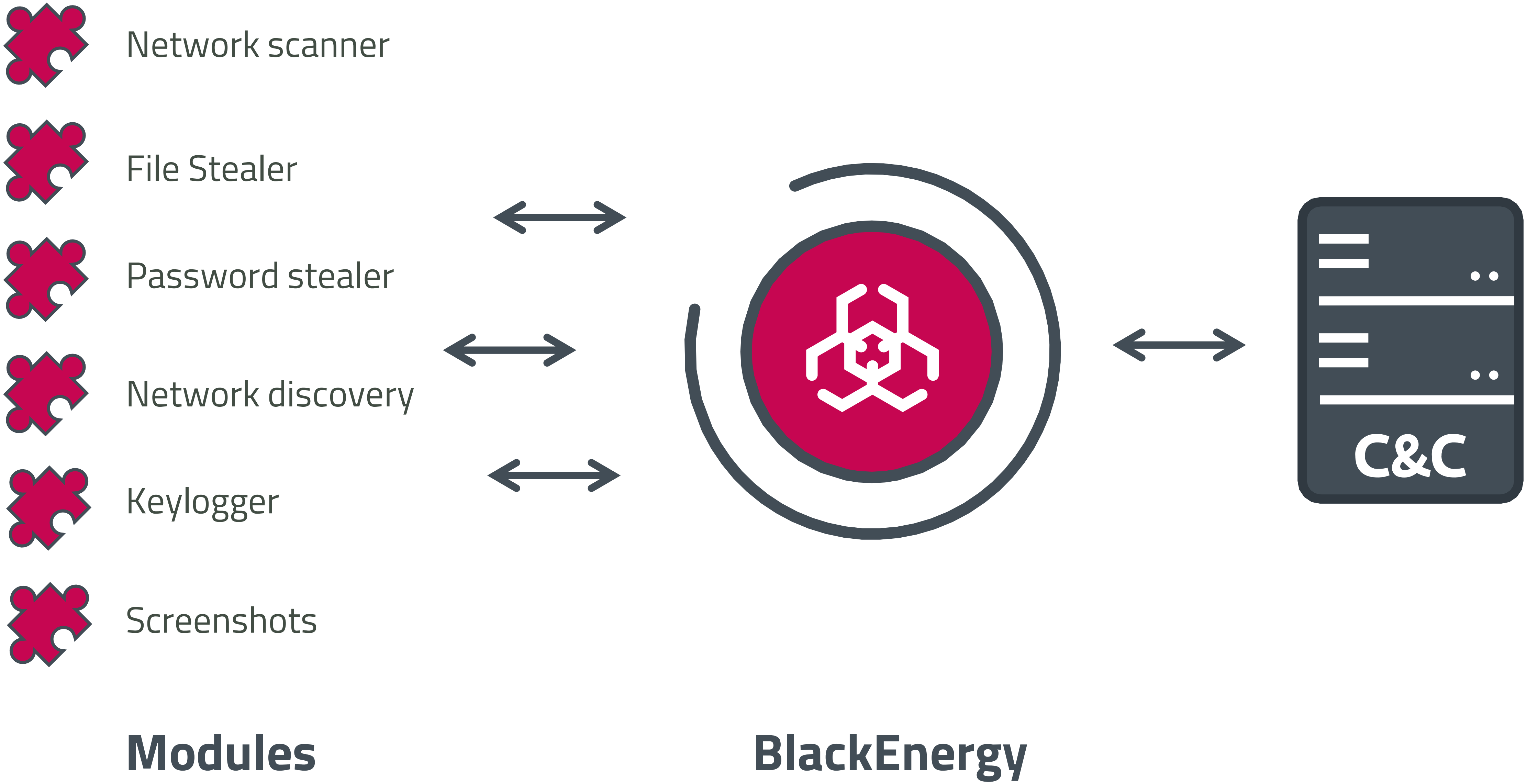
Russian invasion of Ukraine

BlackEnergy pre-blackout (2014)



В даний час ведеться перевірка таких осіб:

[illegible]



Network scanner

File Stealer

Password stealer

Network discovery

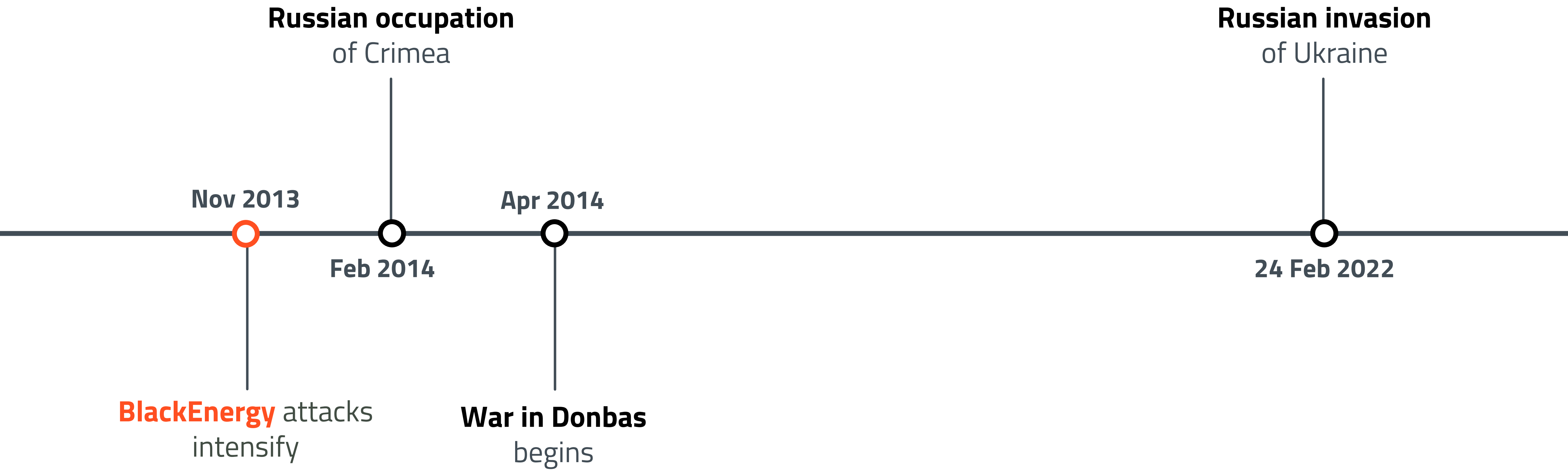
Keylogger

Screenshots

Modules

BlackEnergy

C&C



Nov 2013

BlackEnergy attacks intensify

Feb 2014

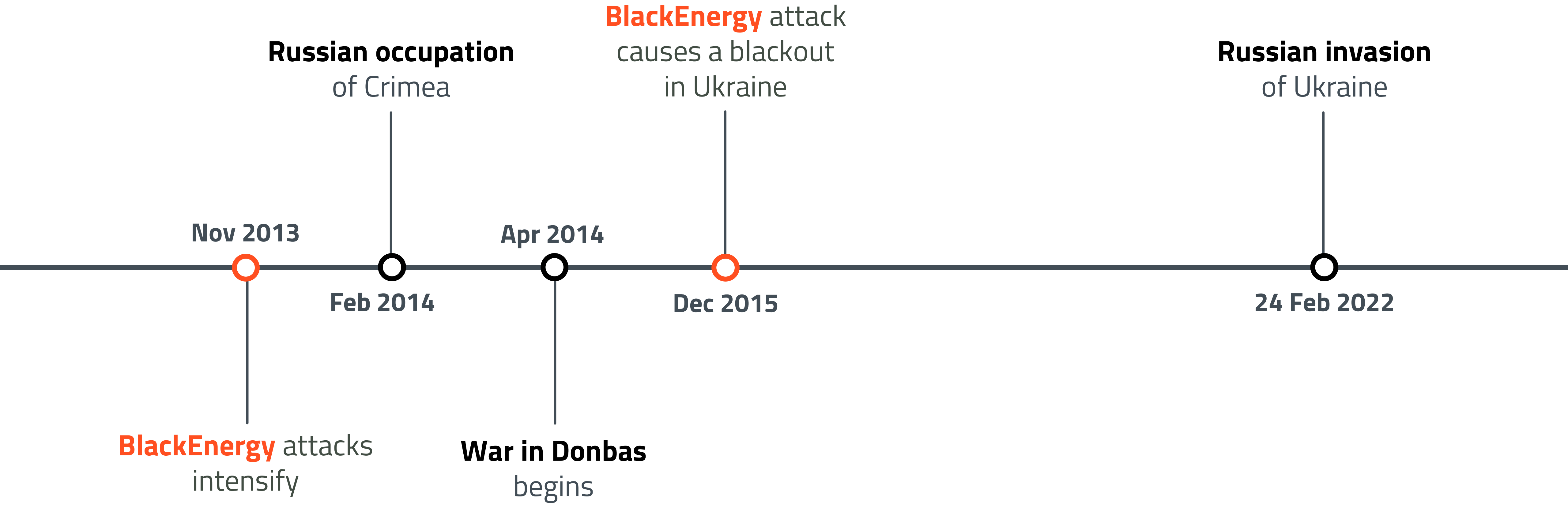
Russian occupation of Crimea

Apr 2014

War in Donbas begins

24 Feb 2022

Russian invasion of Ukraine



Nov 2013
BlackEnergy attacks intensify

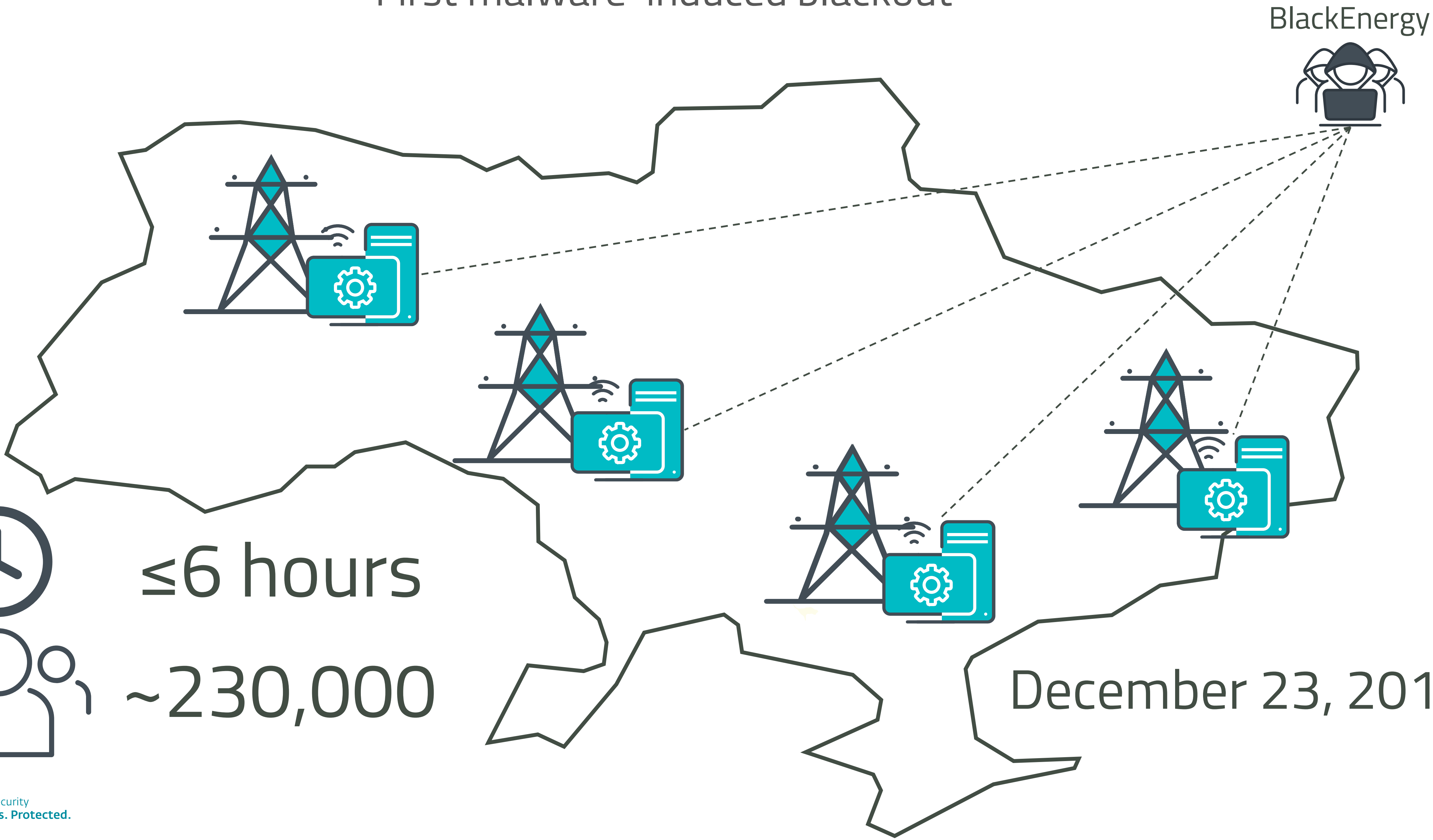
Feb 2014
Russian occupation of Crimea

Apr 2014
War in Donbas begins

Dec 2015
BlackEnergy attack causes a blackout in Ukraine

24 Feb 2022
Russian invasion of Ukraine

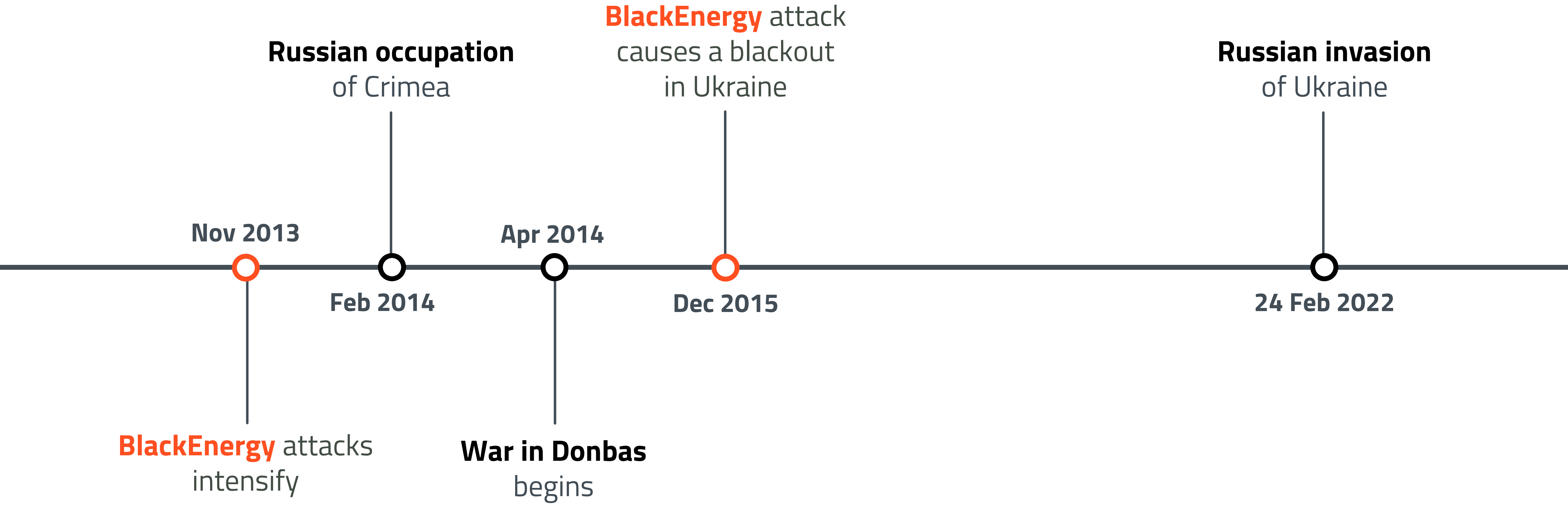
First malware-induced blackout



≤6 hours

~230,000

December 23, 2015



Nov 2013

BlackEnergy attacks intensify

Feb 2014

Russian occupation of Crimea

Apr 2014

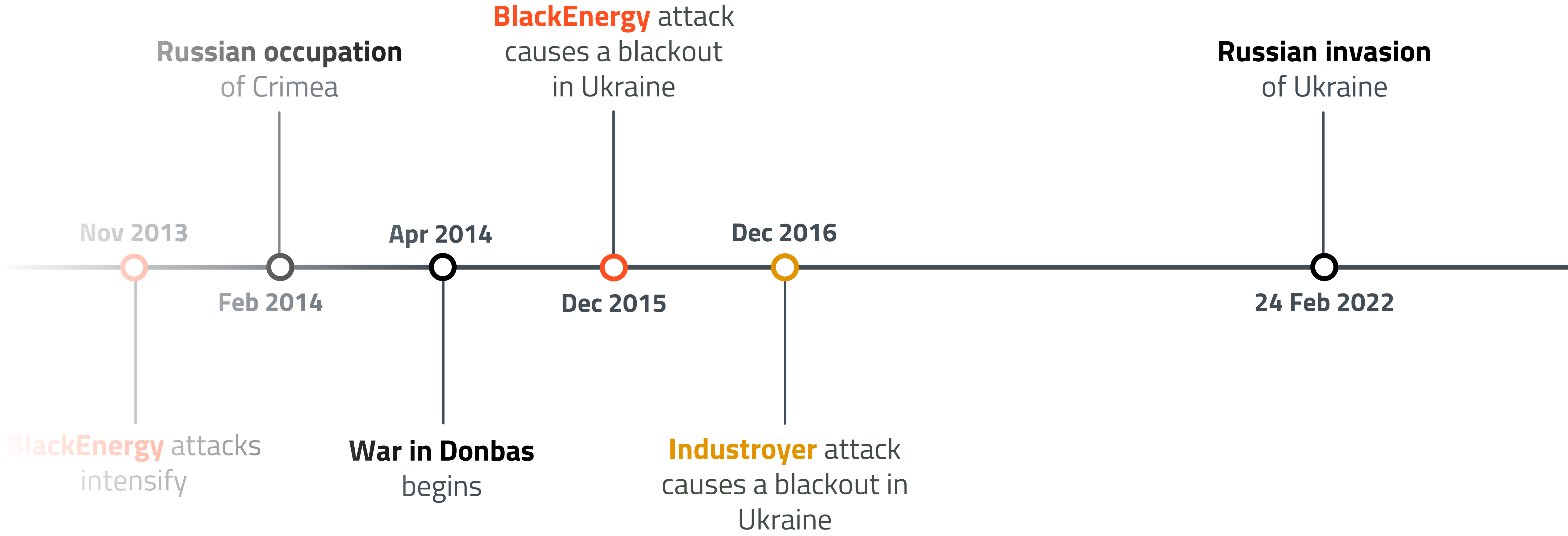
War in Donbas begins

Dec 2015

BlackEnergy attack causes a blackout in Ukraine

24 Feb 2022

Russian invasion of Ukraine



Nov 2013

BlackEnergy attacks intensify

Feb 2014

Russian occupation of Crimea

Apr 2014

War in Donbas begins

Dec 2015

BlackEnergy attack causes a blackout in Ukraine

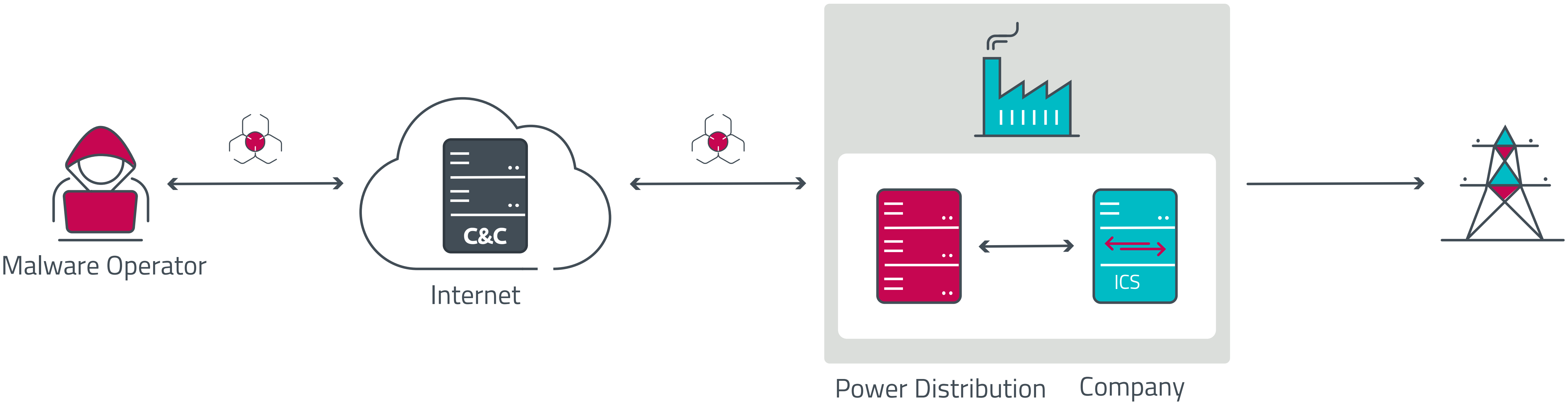
Dec 2016

Industroyer attack causes a blackout in Ukraine

24 Feb 2022

Russian invasion of Ukraine

Industroyer compromise



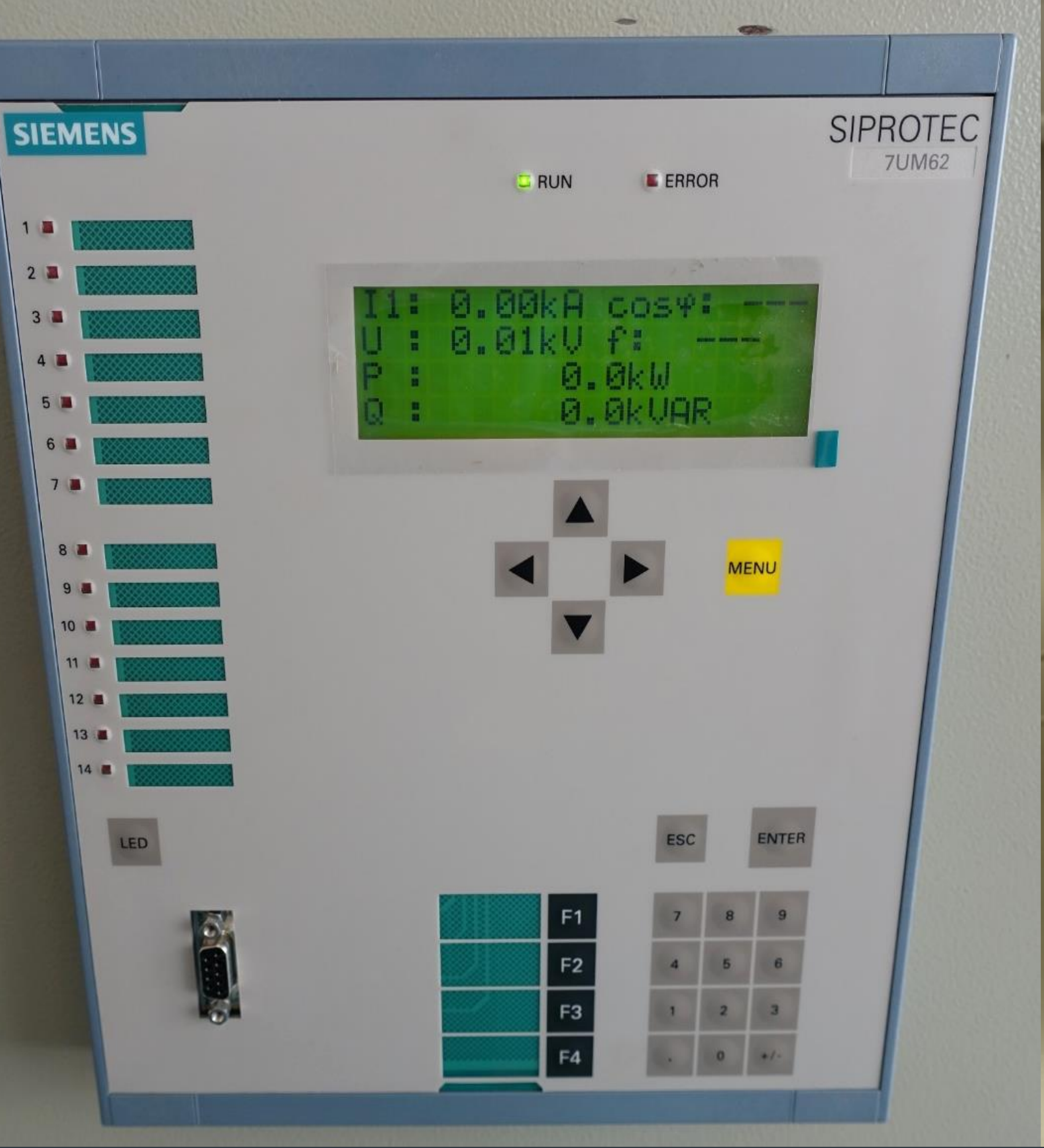
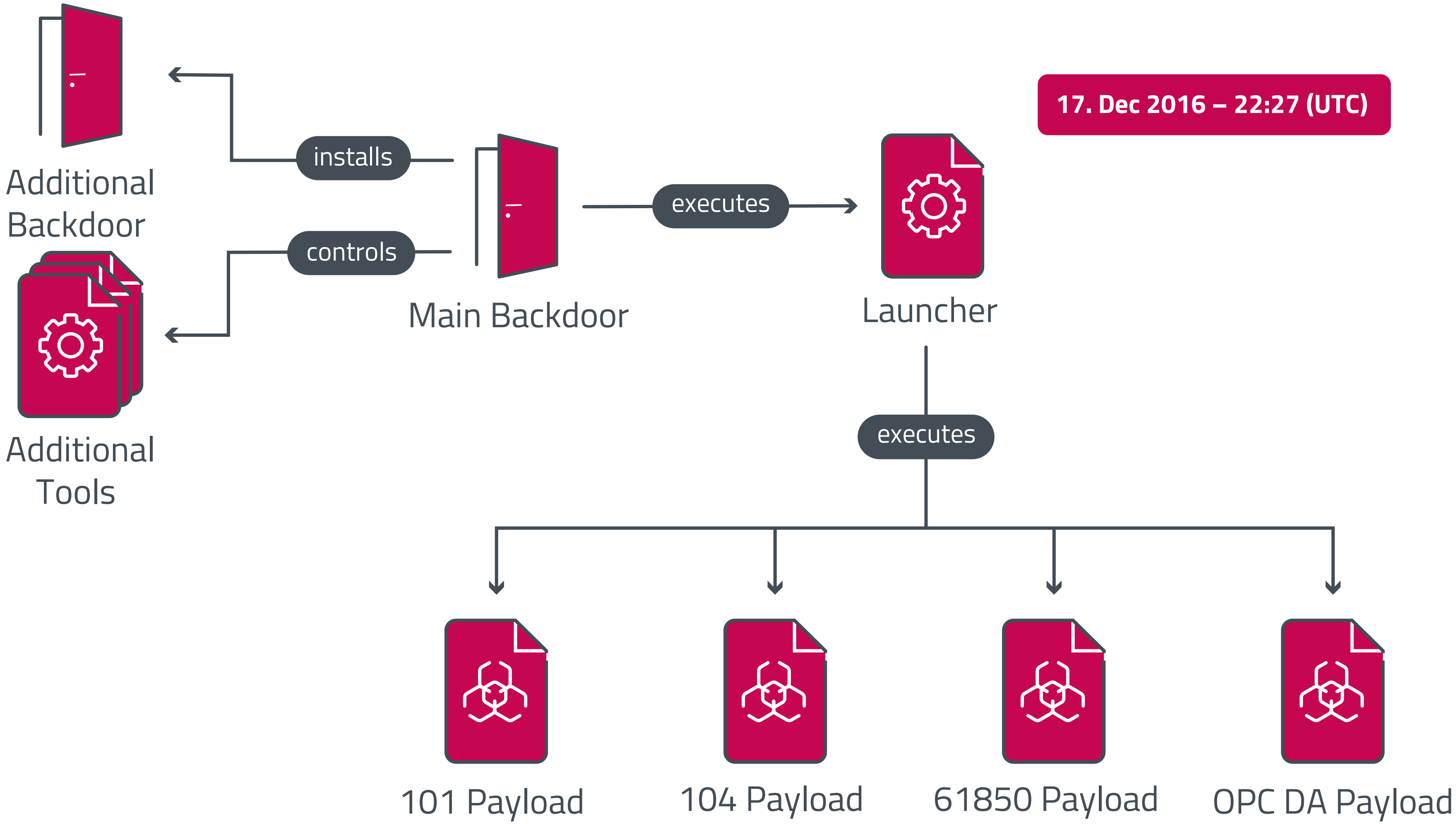
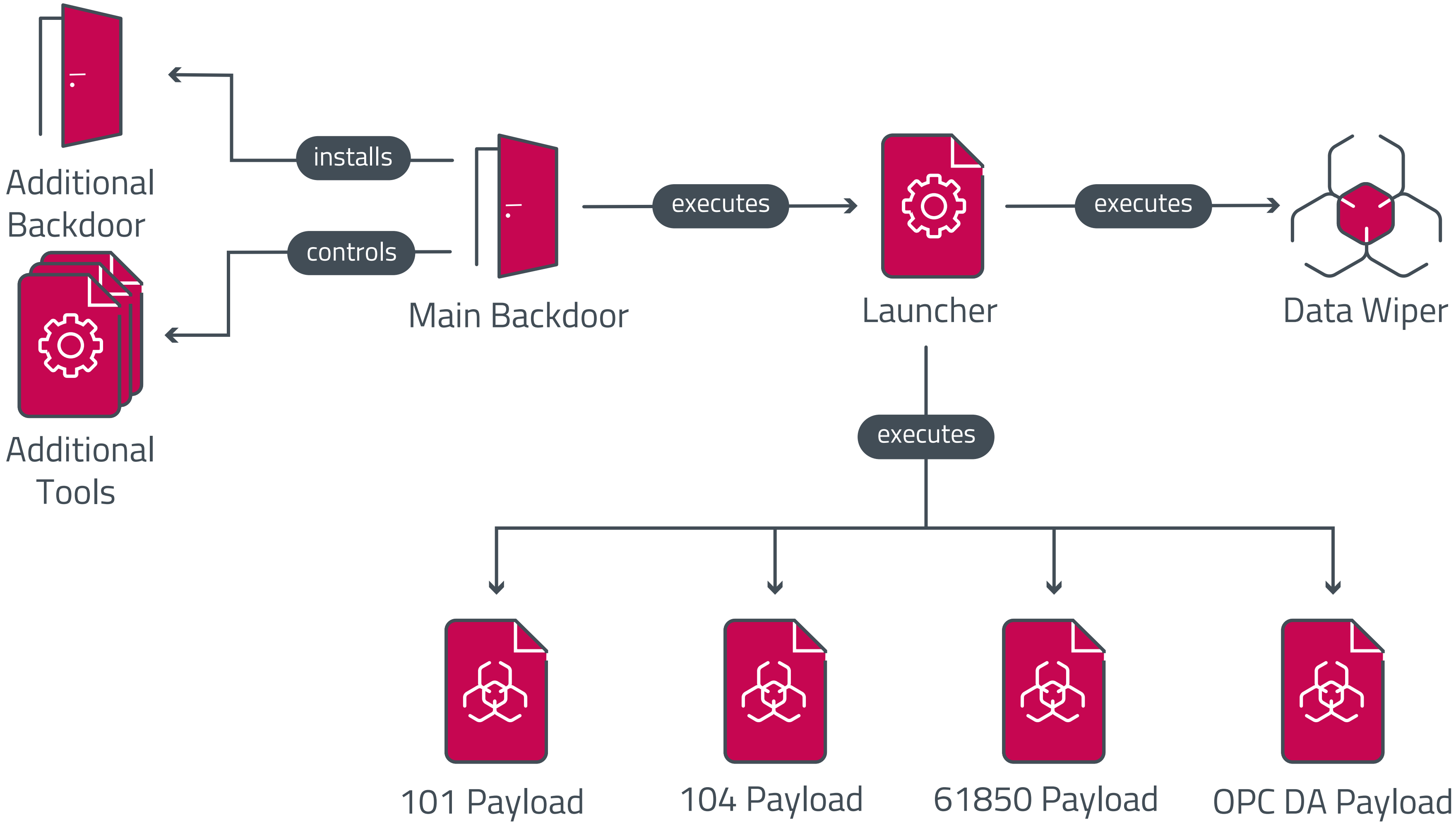

SIEMENS
SIPROTEC
7UM62
RUN
ERROR
I1: 0.00kA cosφ: ---
U : 0.01kV f: ---
P : 0.0kW
Q : 0.0kVAR
1
2
3
4
5
6
7
8
9
10
11
12
13
14
MENU
LED
ESC
ENTER
F1
F2
F3
F4
7 8 9
4 5 6
1 2 3
. 0 +/-

ABB
RED
Ready
Start
Trip
S/S Väs
LINE
RED67
1. DIFF PROT T
2. IMP PROT TR
3. CURRENT PR
4. VOLT'PROT T
5. BFP TRIP
6. REMOTE TRIP
7. GENERAL STAR
8. PROT START L1
9. PROT START L2
10. PROT START L3
11. AR CLOSE CB
12. SUPERV. ALARM
13. COM FAIL
14. COM OK
15. LDL BLOCK
O: Open
I: Close
C: Cancel/Clear
E: Enter/Select/Execute
L/R: Local/Remote/Off
/RED670
Control
Measurements
Events
Disturbance records
Settings
Diagnostics
Test
Reset
Authorization
Language
2014-05-09 20:49:48
SuperUser
I
E
Menu
Help
C
Reset
L
R

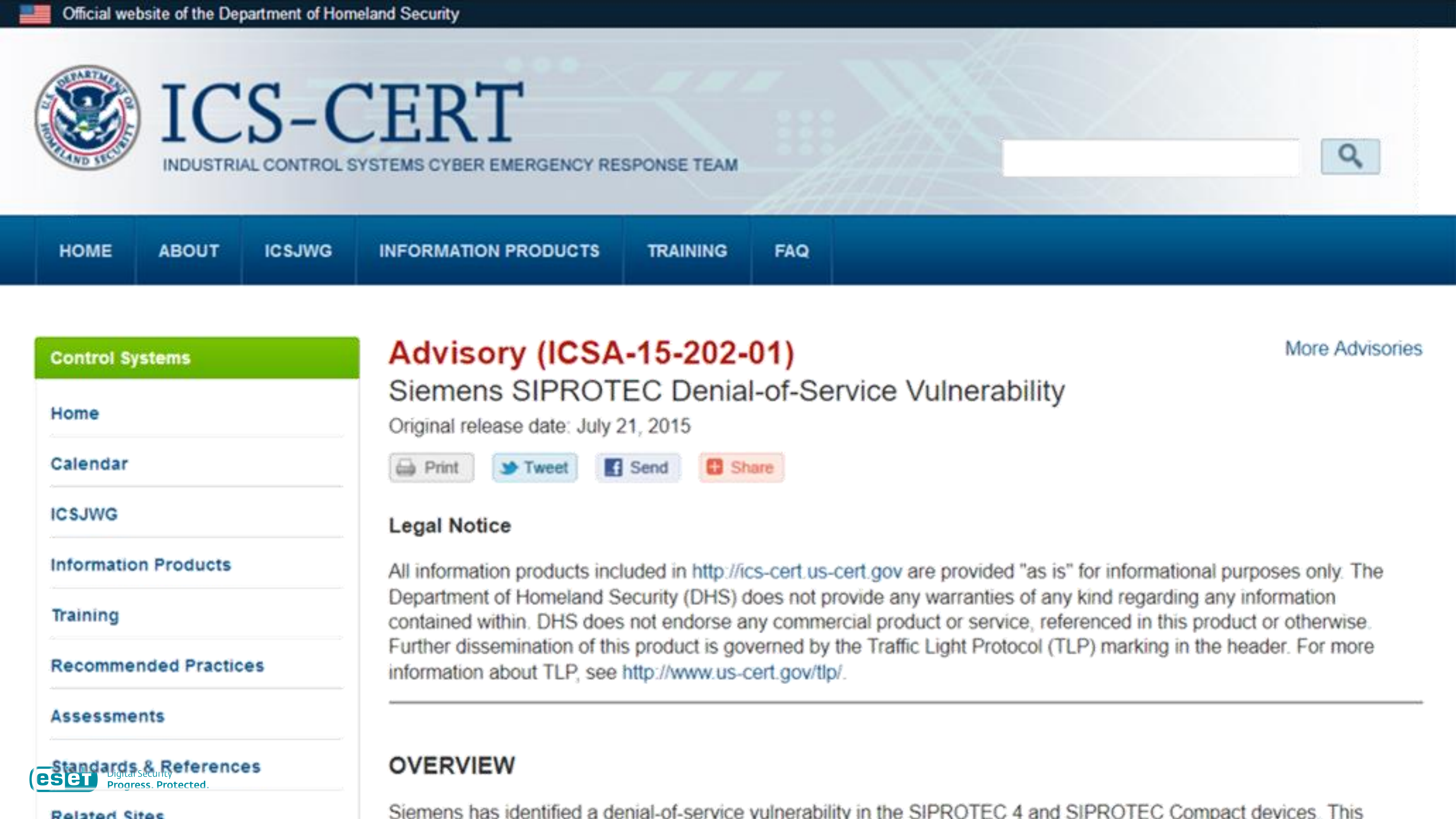
Industroyer architecture



Industroyer architecture



Digital Security
Progress. Protected.



Advisory (ICSA-15-202-01)

Siemens SIPROTEC Denial-of-Service Vulnerability

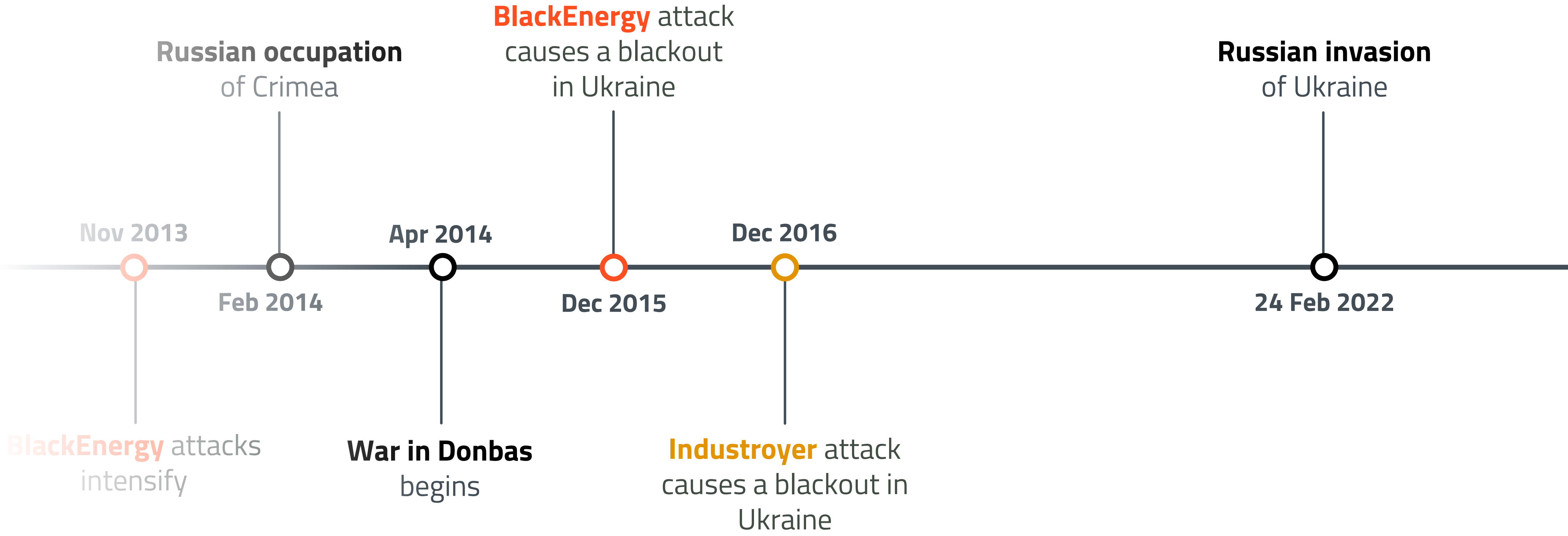
Original release date: July 21, 2015

Legal Notice

All information products included in http://ics-cert.us-cert.gov are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see http://www.us-cert.gov/tlp/.

OVERVIEW

Siemens has identified a denial-of-service vulnerability in the SIPROTEC 4 and SIPROTEC Compact devices. This



Nov 2013

BlackEnergy attacks intensify

Feb 2014

Russian occupation of Crimea

Apr 2014

War in Donbas begins

Dec 2015

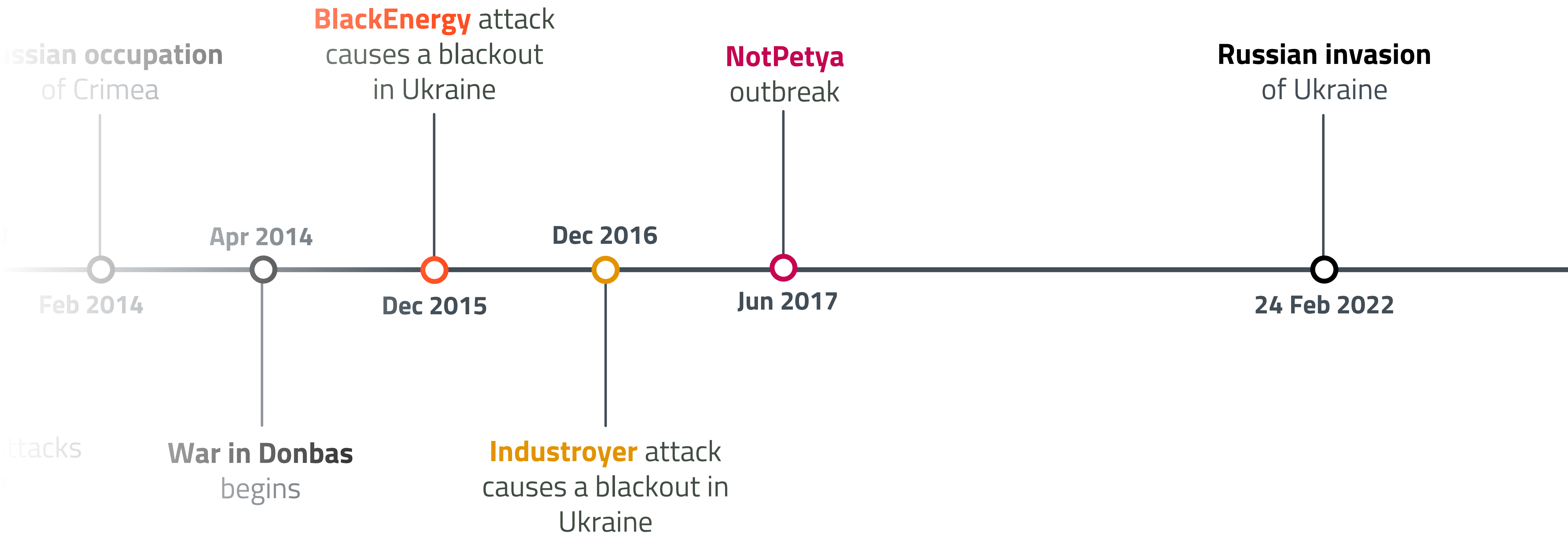
BlackEnergy attack causes a blackout in Ukraine

Dec 2016

Industroyer attack causes a blackout in Ukraine

24 Feb 2022

Russian invasion of Ukraine



ssian occupation of Crimea

Feb 2014

ttacks

Apr 2014

War in Donbas begins

BlackEnergy attack causes a blackout in Ukraine

Dec 2015

Dec 2016

Industroyer attack causes a blackout in Ukraine

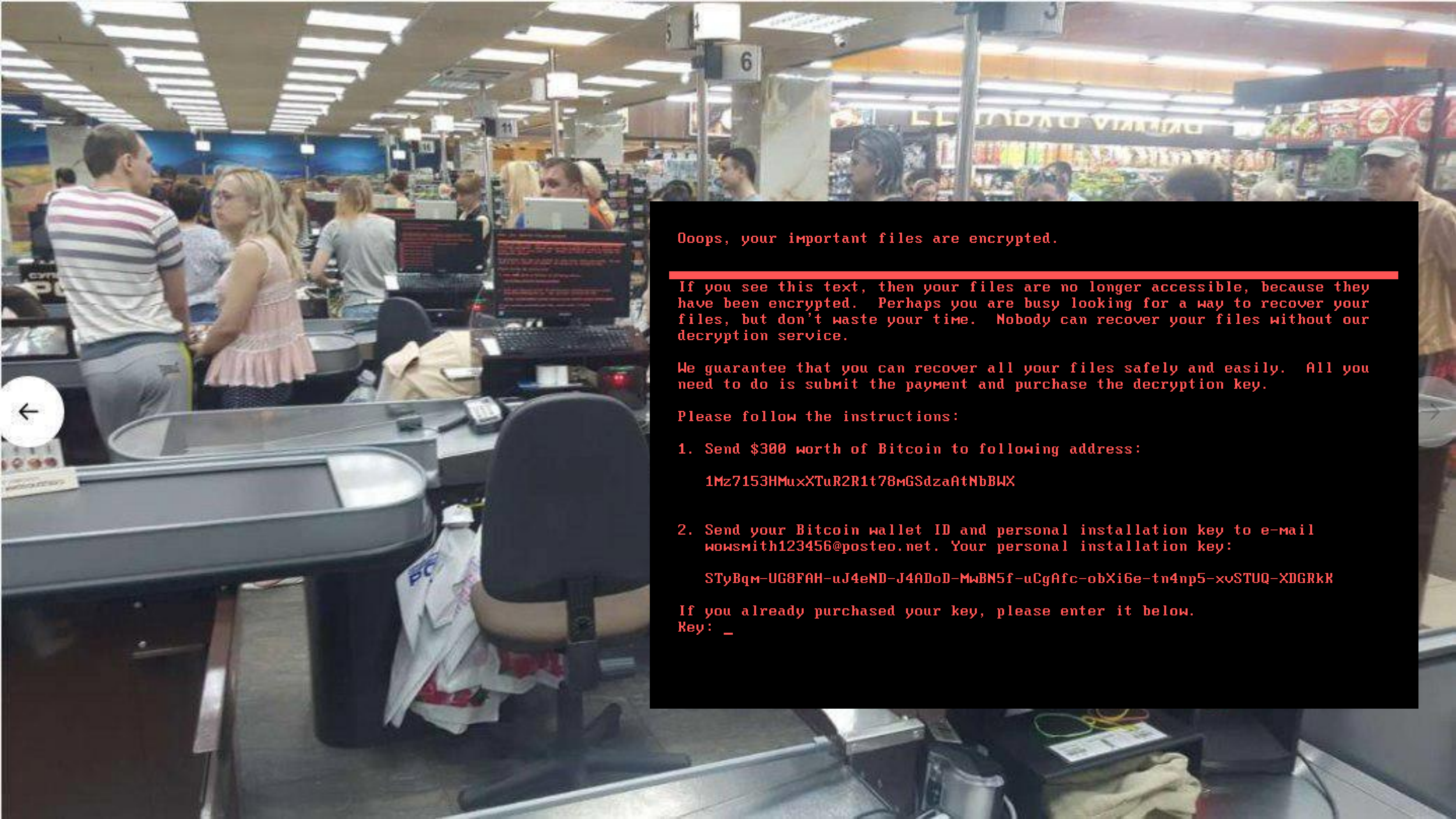
NotPetya outbreak

Jun 2017

Russian invasion of Ukraine

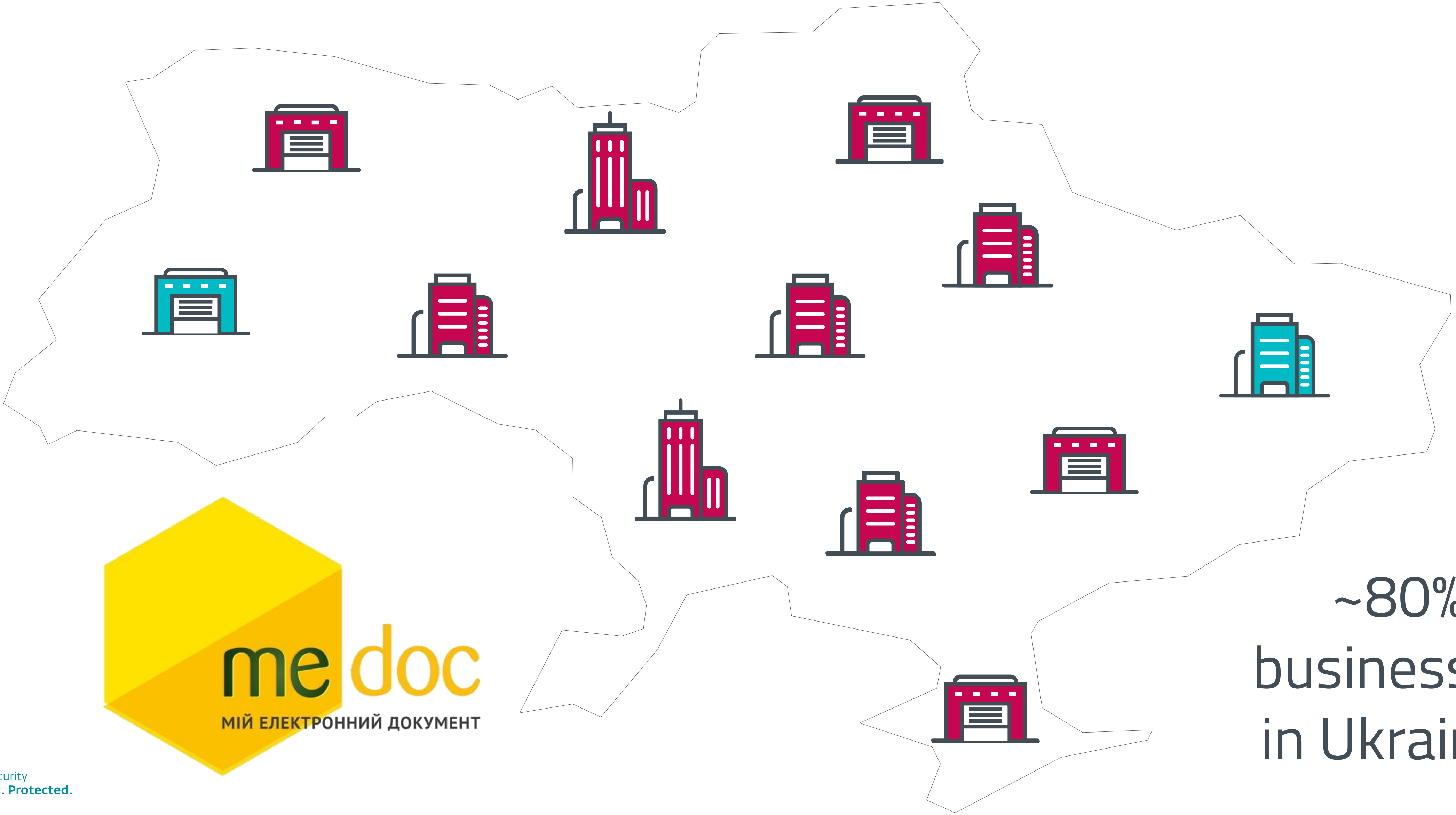
24 Feb 2022

Digital Security
Progress. Protected.



```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted.  Perhaps you are busy looking for a way to recover your
files, but don't waste your time.  Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily.  All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX


2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:

   STyBqm-UG8FAH-uJ4eND-J4ADoD-MwBN5f-uCgAfc-obXi6e-tn4np5-xvSTUQ-XDGRkK

If you already purchased your key, please enter it below.
Key: _
```

NotPetya’s initial vector



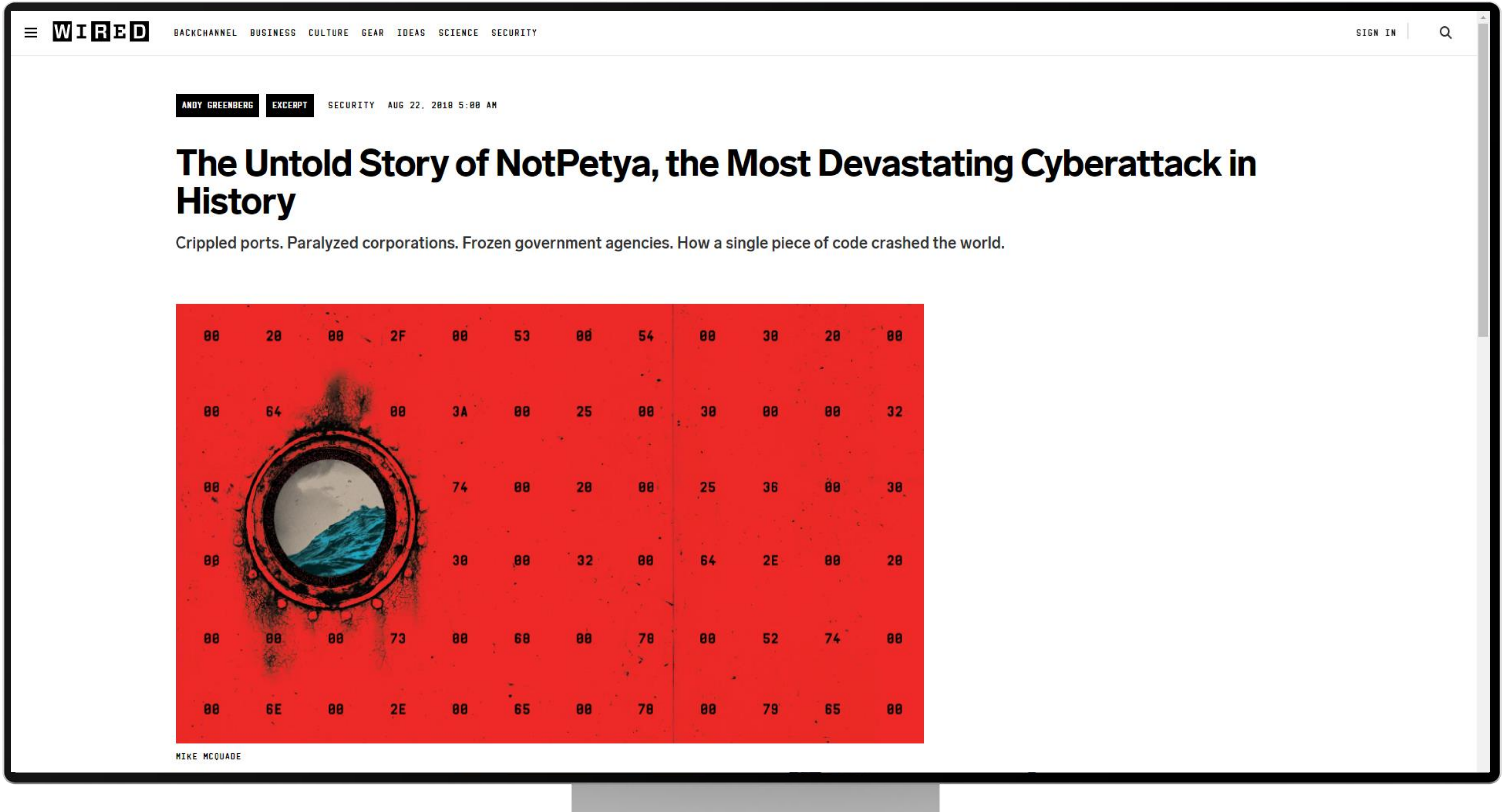
me doc

МІЙ ЕЛЕКТРОННИЙ ДОКУМЕНТ

~80% businesses in Ukraine*

...and worldwide compromise

Impact of NotPetya



WIRED
BACKCHANNEL
BUSINESS
CULTURE
GEAR
IDEAS
SCIENCE
SECURITY
SIGN IN

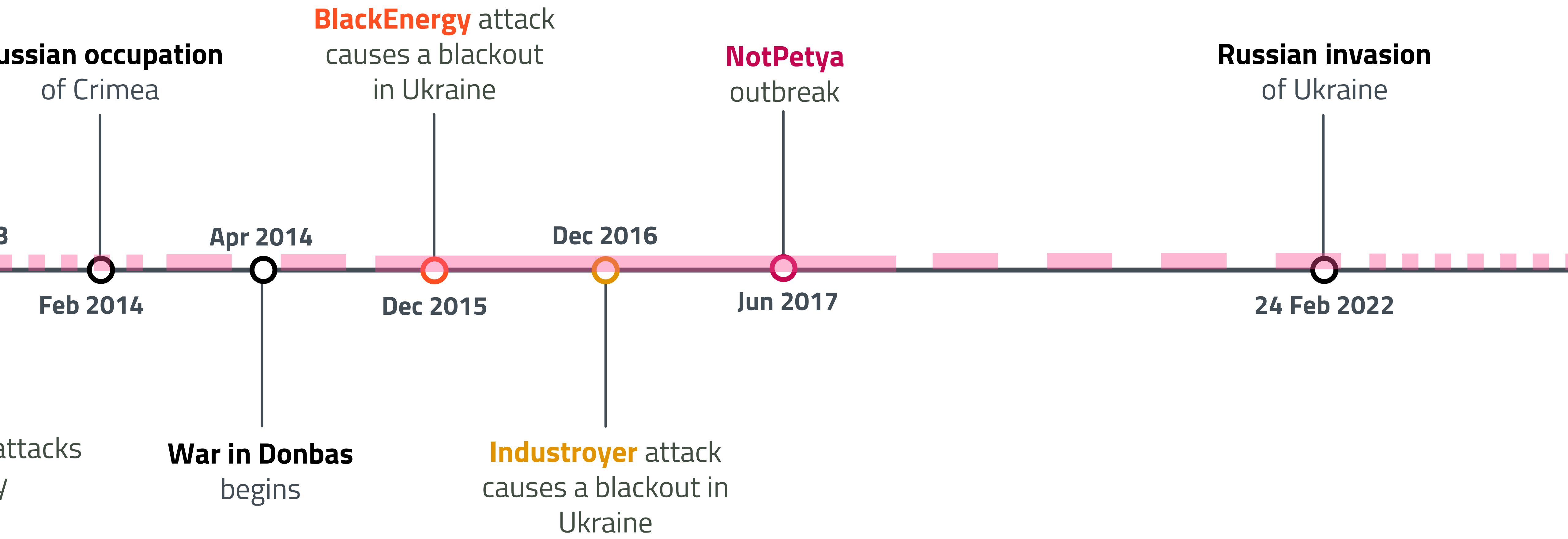
ANDY GREENBERG EXCERPT SECURITY AUG 22, 2018 5:00 AM

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.

00 20 00 2F 00 53 00 54 00 30 20 00
00 64 00 3A 00 25 00 30 00 00 32
00 74 00 20 00 25 36 00 30
00 30 00 32 00 64 2E 00 20
00 00 00 73 00 68 00 70 00 52 74 00
00 6E 00 2E 00 65 00 78 00 79 65 00

MIKE MCQUADE



3

ussian occupation of Crimea

Feb 2014

attacks

/

Apr 2014

War in Donbas begins

BlackEnergy attack causes a blackout in Ukraine

Dec 2015

Dec 2016

Industroyer attack causes a blackout in Ukraine

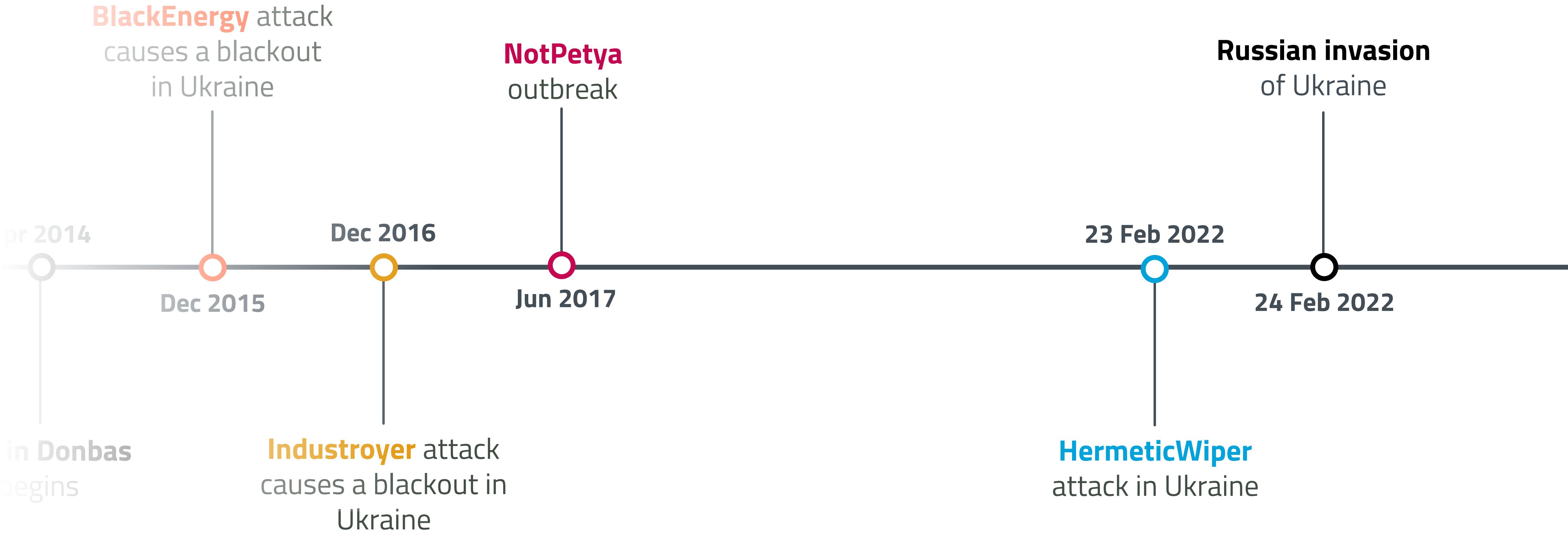
NotPetya outbreak

Jun 2017

Russian invasion of Ukraine

24 Feb 2022

Digital Security
Progress. Protected.



pr 2014

in Donbas
egins

Dec 2015

BlackEnergy attack
causes a blackout
in Ukraine

Dec 2016

Industroyer attack
causes a blackout in
Ukraine

Jun 2017

NotPetya
outbreak

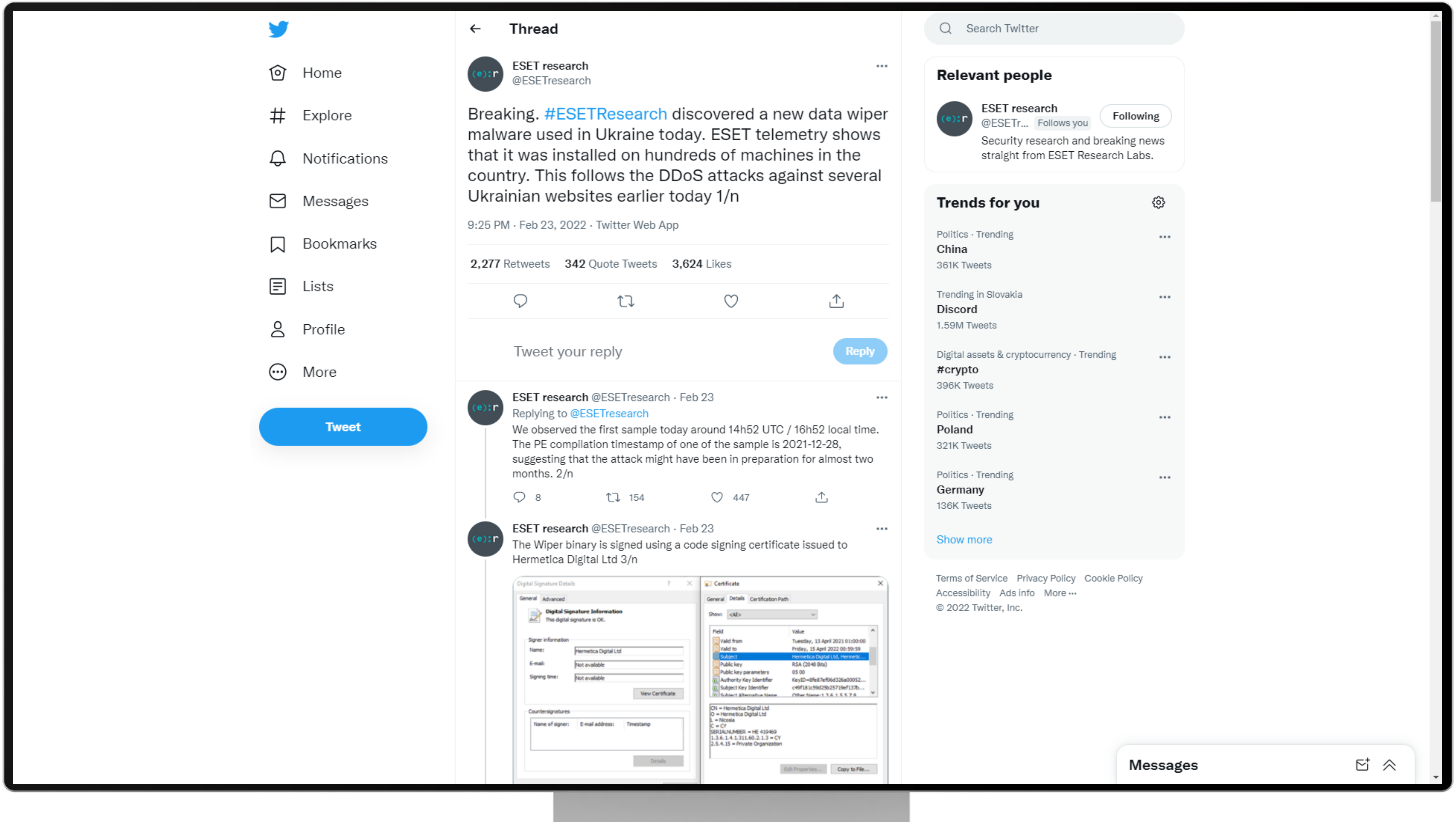
23 Feb 2022

HermeticWiper
attack in Ukraine

24 Feb 2022

Russian invasion
of Ukraine

HermeticWiper



ESET research
@ESETresearch

Security research and breaking news straight from ESET Research Labs.

Breaking. #ESETResearch discovered a new data wiper malware used in Ukraine today. ESET telemetry shows that it was installed on hundreds of machines in the country. This follows the DDoS attacks against several Ukrainian websites earlier today 1/n

9:25 PM · Feb 23, 2022 · Twitter Web App

2,277 Retweets 342 Quote Tweets 3,624 Likes

ESET research @ESETresearch · Feb 23
Replying to @ESETresearch
We observed the first sample today around 14h52 UTC / 16h52 local time. The PE compilation timestamp of one of the sample is 2021-12-28, suggesting that the attack might have been in preparation for almost two months. 2/n

8 154 447

ESET research @ESETresearch · Feb 23
The Wiper binary is signed using a code signing certificate issued to Hermetica Digital Ltd 3/n

Digital Signature Details

General Advanced

Digital Signature Information
This digital signature is OK.

Signer information
Name: Hermetica Digital Ltd
E-mail: Not available
Signing time: Not available

View Certificate

Countersignatures

Name of signer:	E-mail address:	Timestamp

Details

Certificate

General Details Certification Path

Show: <All>

Field	Value
Valid from	Tuesday, 13 April 2021 01:00:00
Valid to	Friday, 15 April 2022 00:59:59
Subject	Hermetica Digital Ltd, Hermetic...
Public key	RSA (2048 Bits)
Public key parameters	05 00
Authority Key Identifier	KeyID=8fe87ef06d326a00052...
Subject Key Identifier	c49f181c59d25b25719ef137b...
Subject Alternative Name	Other Name:1.3.6.1.5.5.7.8

```
CN = Hermetica Digital Ltd
O = Hermetica Digital Ltd
L = Nicosia
C = CY
SERIALNUMBER = HE 419469
1.3.6.1.4.1.311.60.2.1.3 = CY
2.5.4.15 = Private Organization
```

Edit Properties... Copy to File...

HermeticWiper: Impact

100s

systems

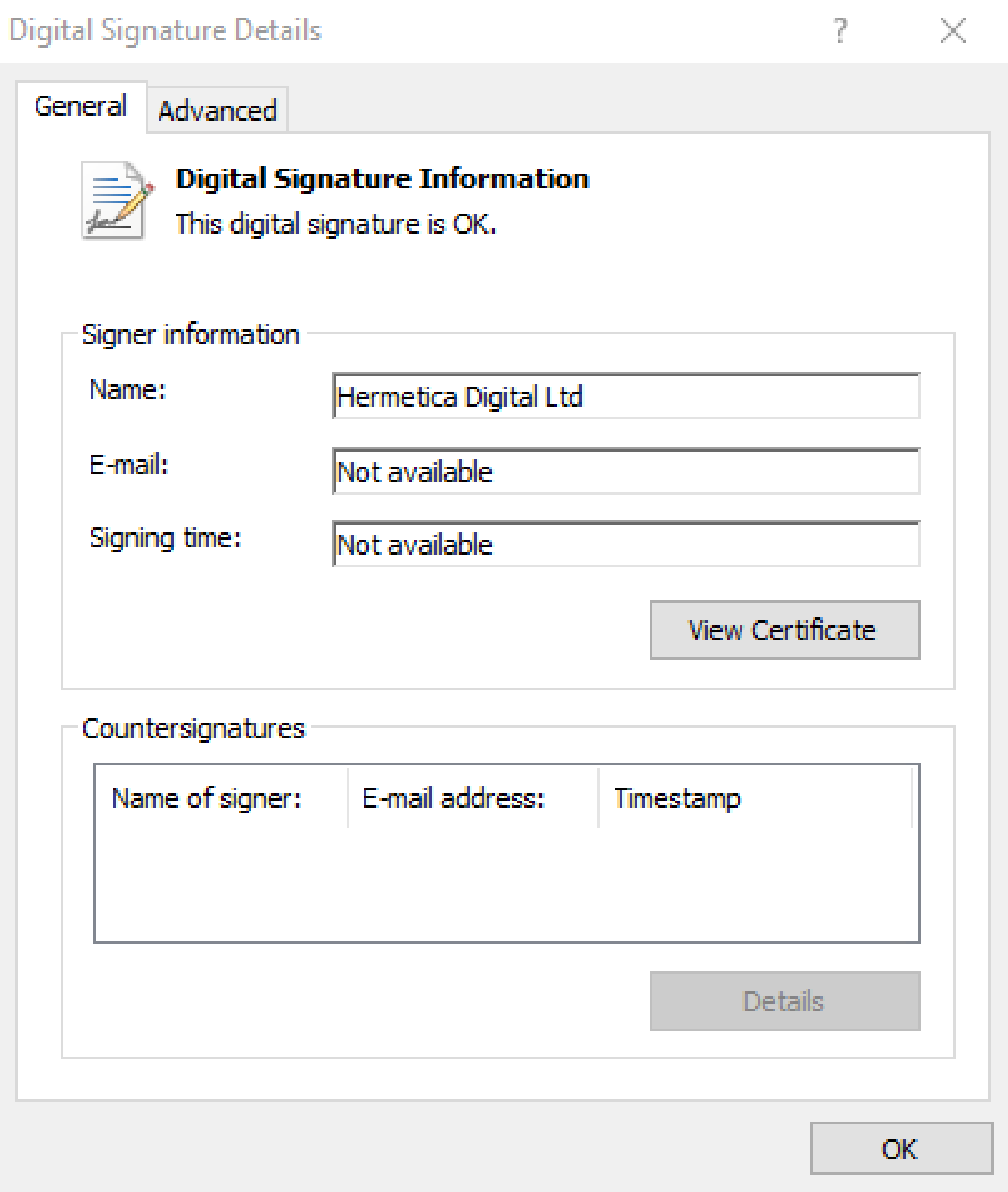
5+

organizations

Dec 28, 2021

compilation timestamp*

Why Hermetic*?



Digital Signature Information

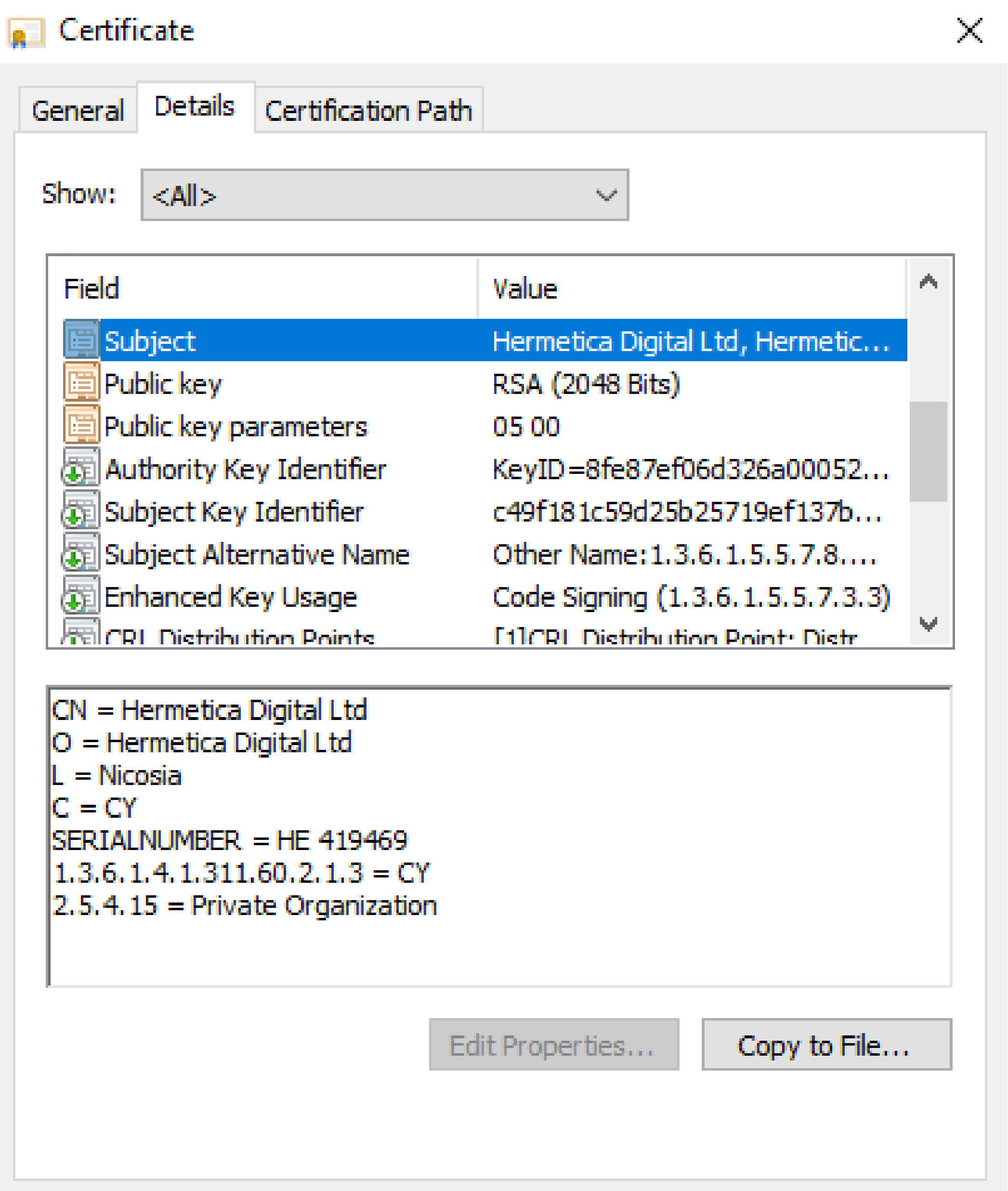
This digital signature is OK.

Signer information

Name:	Hermetica Digital Ltd
E-mail:	Not available
Signing time:	Not available

Countersignatures

Name of signer:	E-mail address:	Timestamp



Show: <All>

Field	Value
Subject	Hermetica Digital Ltd, Hermetic...
Public key	RSA (2048 Bits)
Public key parameters	05 00
Authority Key Identifier	KeyID=8fe87ef06d326a00052...
Subject Key Identifier	c49f181c59d25b25719ef137b...
Subject Alternative Name	Other Name:1.3.6.1.5.5.7.8....
Enhanced Key Usage	Code Signing (1.3.6.1.5.5.7.3.3)
CRL Distribution Points	[1]CRL Distribution Point: Distr

CN = Hermetica Digital Ltd
O = Hermetica Digital Ltd
L = Nicosia
C = CY
SERIALNUMBER = HE 419469
1.3.6.1.4.1.311.60.2.1.3 = CY
2.5.4.15 = Private Organization

Hermetic campaign

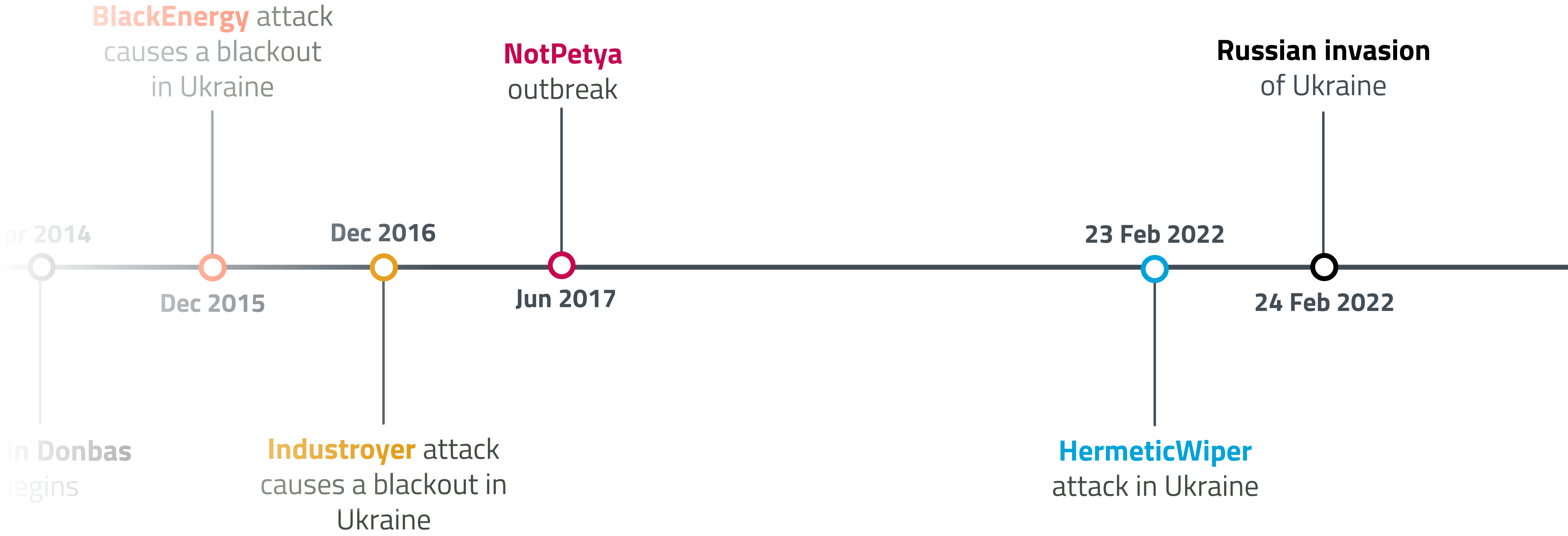
HermeticWiper

HermeticWizard

HermeticRansom

HermeticRansom

- _/C_/projects/403for**Biden**/**wHiteHousE**.baggageGatherings
- _/C_/projects/403for**Biden**/**wHiteHousE**.lookUp
- _/C_/projects/403for**Biden**/**wHiteHousE**.primaryElectionProcess
- _/C_/projects/403for**Biden**/**wHiteHousE**.GoodOffice1



pr 2014

in Donbas
egins

Dec 2015

BlackEnergy attack
causes a blackout
in Ukraine

Dec 2016

Industroyer attack
causes a blackout in
Ukraine

Jun 2017

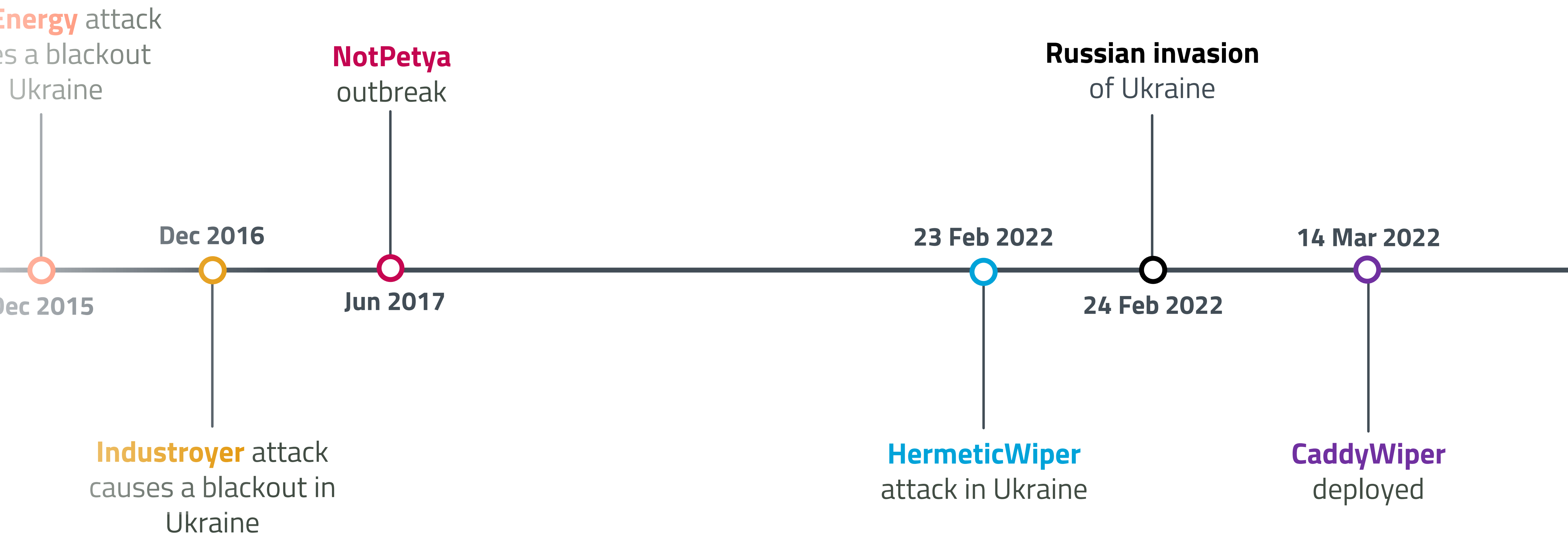
NotPetya
outbreak

23 Feb 2022

HermeticWiper
attack in Ukraine

24 Feb 2022

Russian invasion
of Ukraine



nergy attack
es a blackout
Ukraine

ec 2015

Dec 2016

Industroyer attack
causes a blackout in
Ukraine

NotPetya
outbreak

Jun 2017

23 Feb 2022

HermeticWiper
attack in Ukraine

Russian invasion
of Ukraine

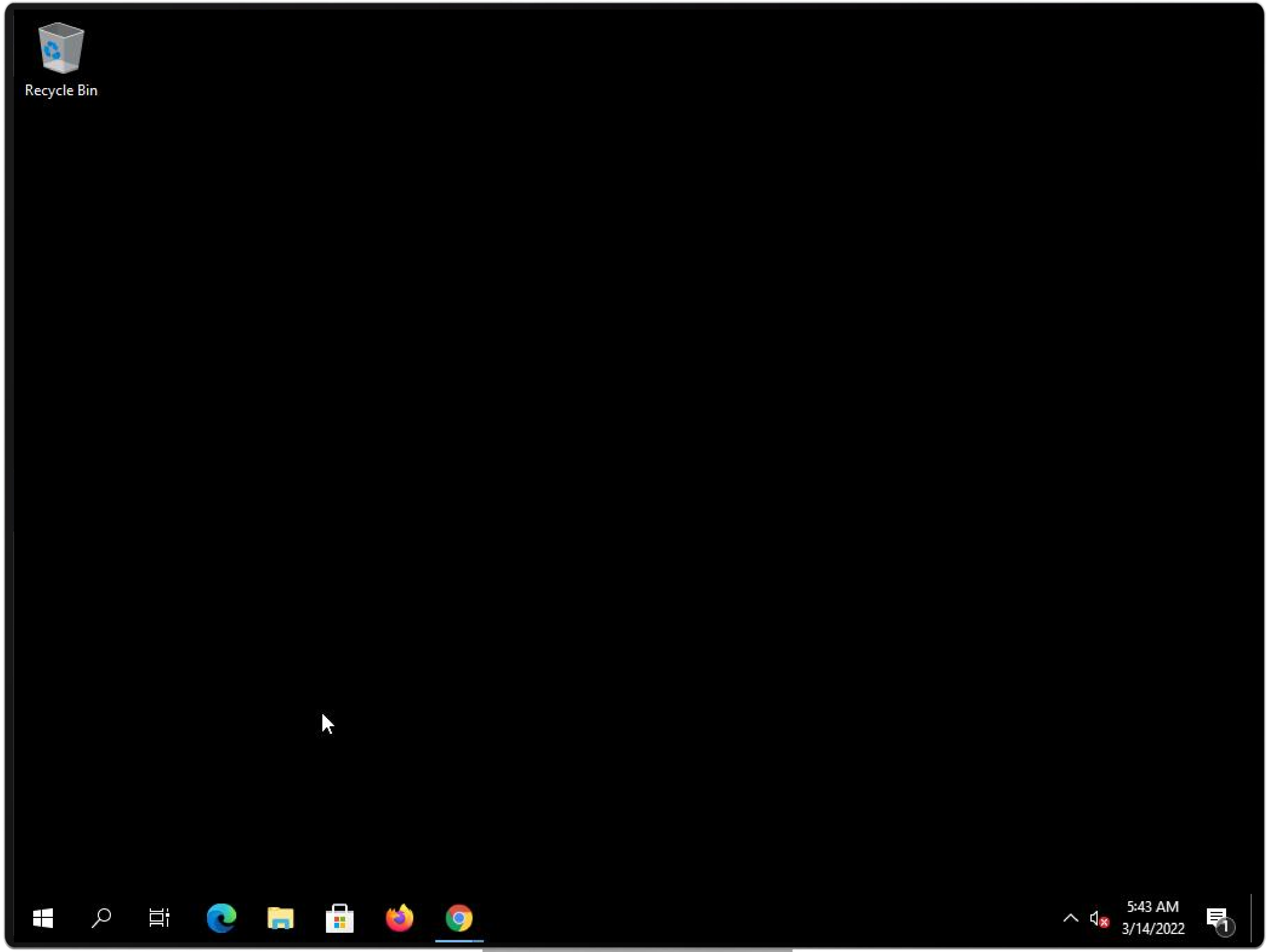
24 Feb 2022

14 Mar 2022

CaddyWiper
deployed

Digital Security
Progress. Protected.

CaddyWiper



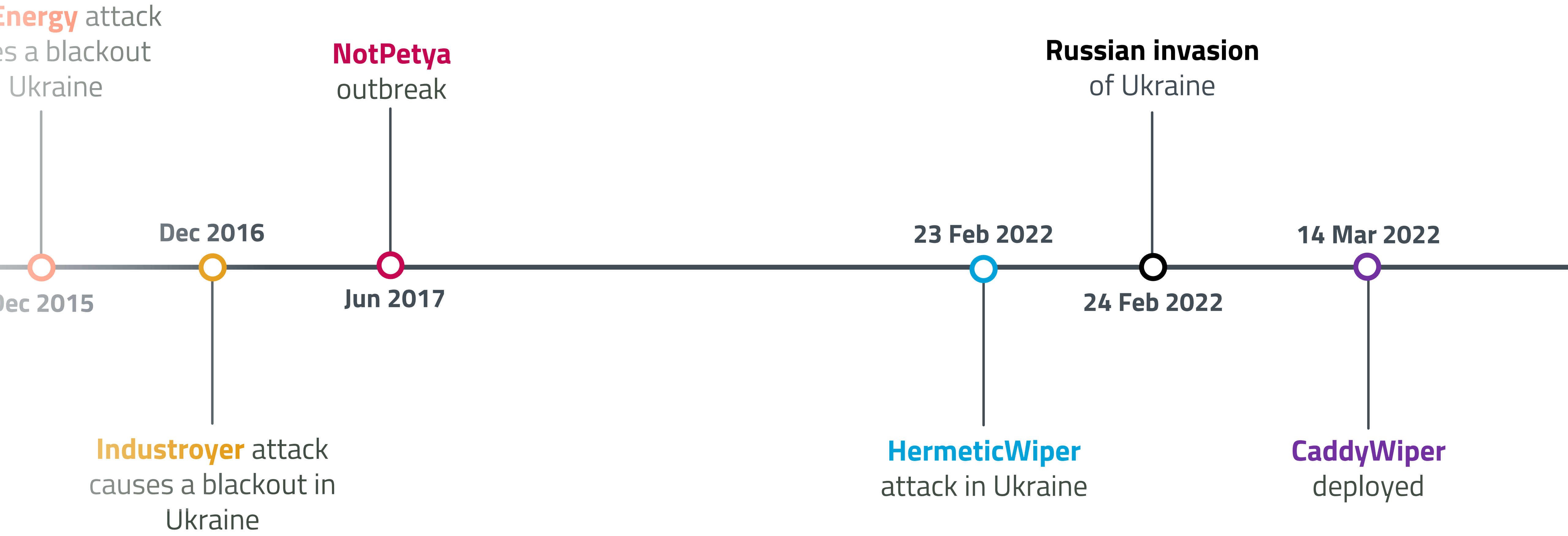
Source: VirusTotal

CaddyWiper

Dozens of systems

Targeted financial sector

Compiled & deployed Mar 14, 2022



Energy attack
es a blackout
Ukraine

ec 2015

Dec 2016

Industroyer attack
causes a blackout in
Ukraine

NotPetya
outbreak

Jun 2017

23 Feb 2022

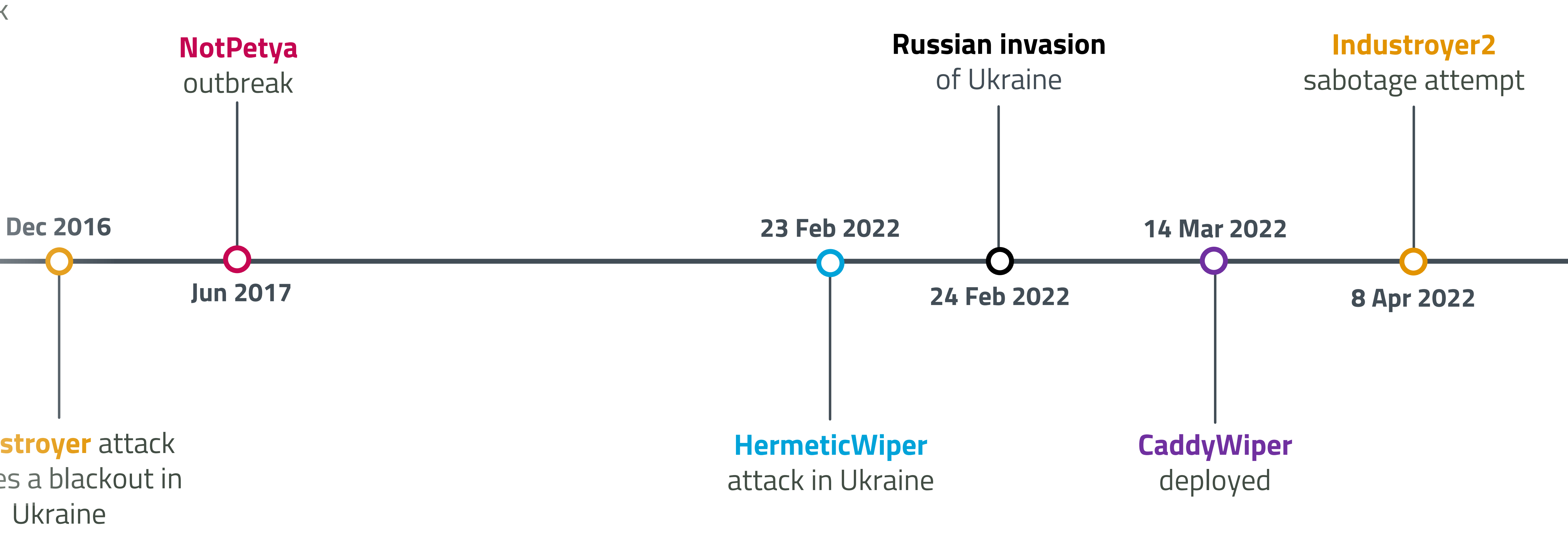
HermeticWiper
attack in Ukraine

Russian invasion
of Ukraine

24 Feb 2022

14 Mar 2022

CaddyWiper
deployed



k

Dec 2016

stroyer attack
es a blackout in
Ukraine

NotPetya
outbreak

Jun 2017

23 Feb 2022

HermeticWiper
attack in Ukraine

Russian invasion
of Ukraine

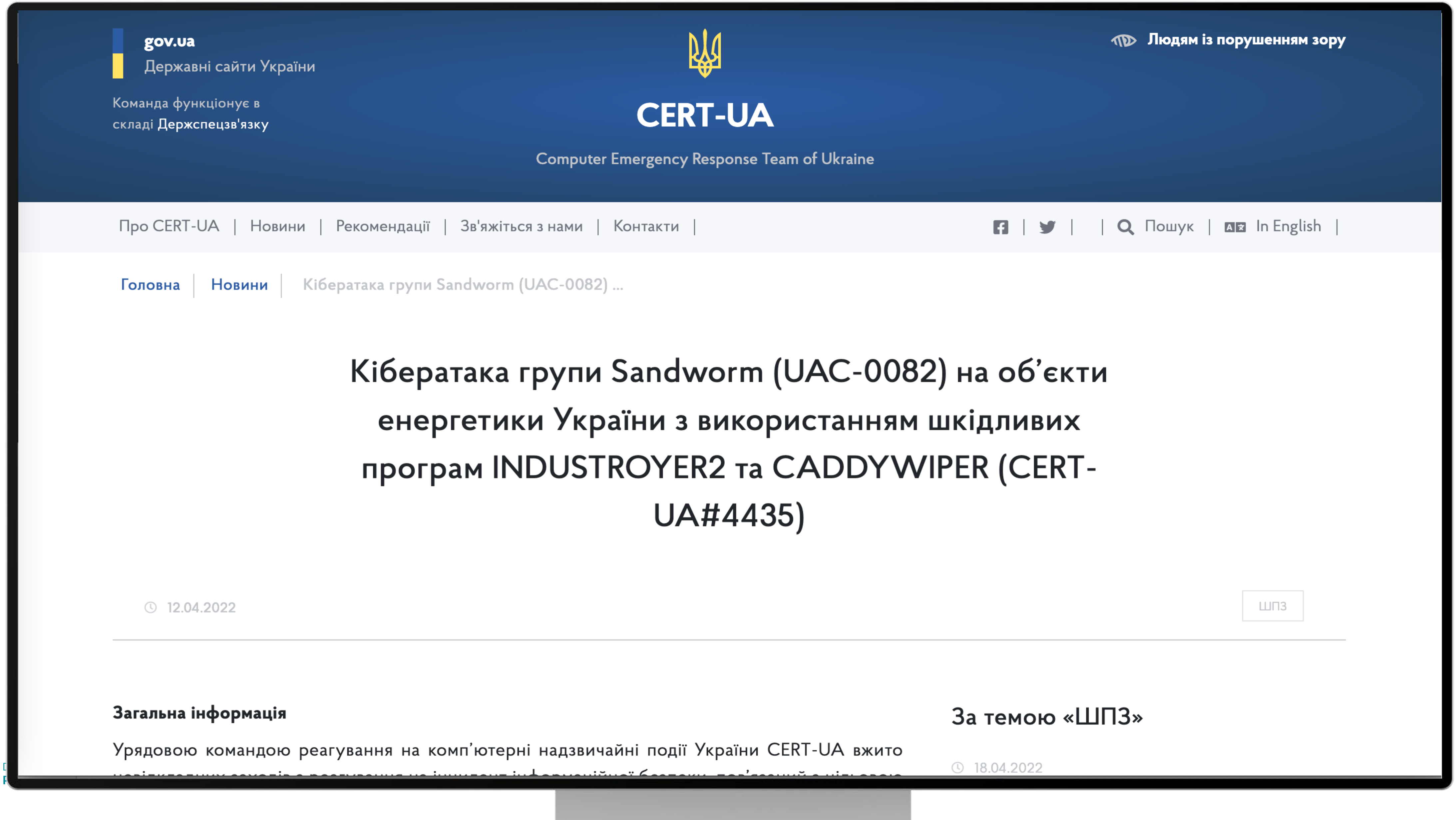
24 Feb 2022

14 Mar 2022

CaddyWiper
deployed

Industroyer2
sabotage attempt

8 Apr 2022


gov.ua
Державні сайти України
Команда функціонує в складі Держспецзв'язку
Людям із порушенням зору
CERT-UA
Computer Emergency Response Team of Ukraine
Про CERT-UA | Новини | Рекомендації | Зв'яжіться з нами | Контакти |
| Пошук | In English |
Головна | Новини | Кібератака групи Sandworm (UAC-0082) ...

Кібератака групи Sandworm (UAC-0082) на об’єкти енергетики України з використанням шкідливих програм INDUSTROYER2 та CADDYWIPER (CERT-UA#4435)

12.04.2022

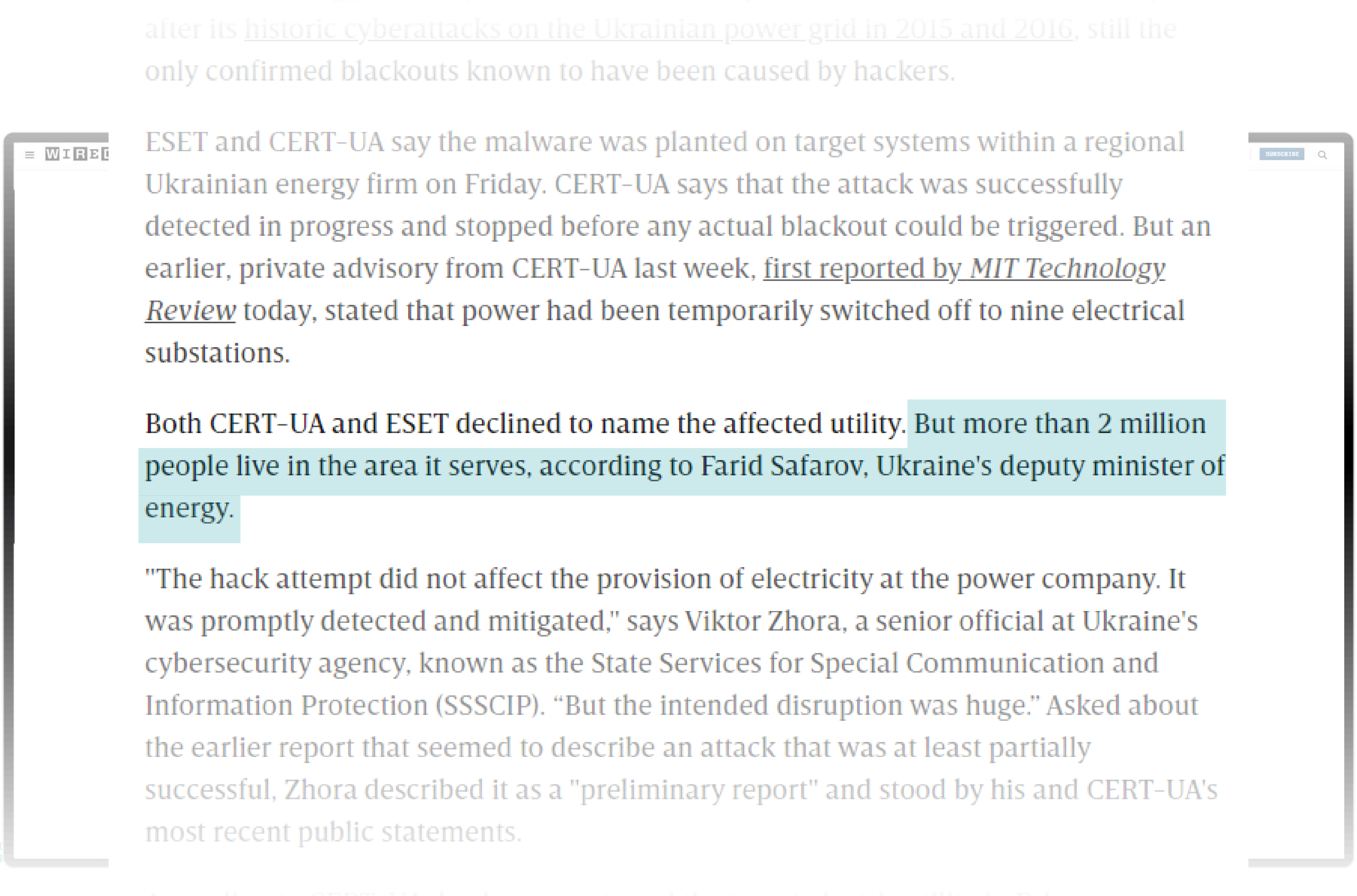
ШПЗ

Загальна інформація

Урядовою командою реагування на комп’ютерні надзвичайні події України CERT-UA вжито

За темою «ШПЗ»

18.04.2022



after its historic cyberattacks on the Ukrainian power grid in 2015 and 2016, still the only confirmed blackouts known to have been caused by hackers.

ESET and CERT-UA say the malware was planted on target systems within a regional Ukrainian energy firm on Friday. CERT-UA says that the attack was successfully detected in progress and stopped before any actual blackout could be triggered. But an earlier, private advisory from CERT-UA last week, first reported by *MIT Technology Review* today, stated that power had been temporarily switched off to nine electrical substations.

Both CERT-UA and ESET declined to name the affected utility. But more than 2 million people live in the area it serves, according to Farid Safarov, Ukraine's deputy minister of energy.

"The hack attempt did not affect the provision of electricity at the power company. It was promptly detected and mitigated," says Viktor Zhora, a senior official at Ukraine's cybersecurity agency, known as the State Services for Special Communication and Information Protection (SSSCIP). "But the intended disruption was huge." Asked about the earlier report that seemed to describe an attack that was at least partially successful, Zhora described it as a "preliminary report" and stood by his and CERT-UA's most recent public statements.

Industroyer2

Comp. timestamp

Mar 23, 2022

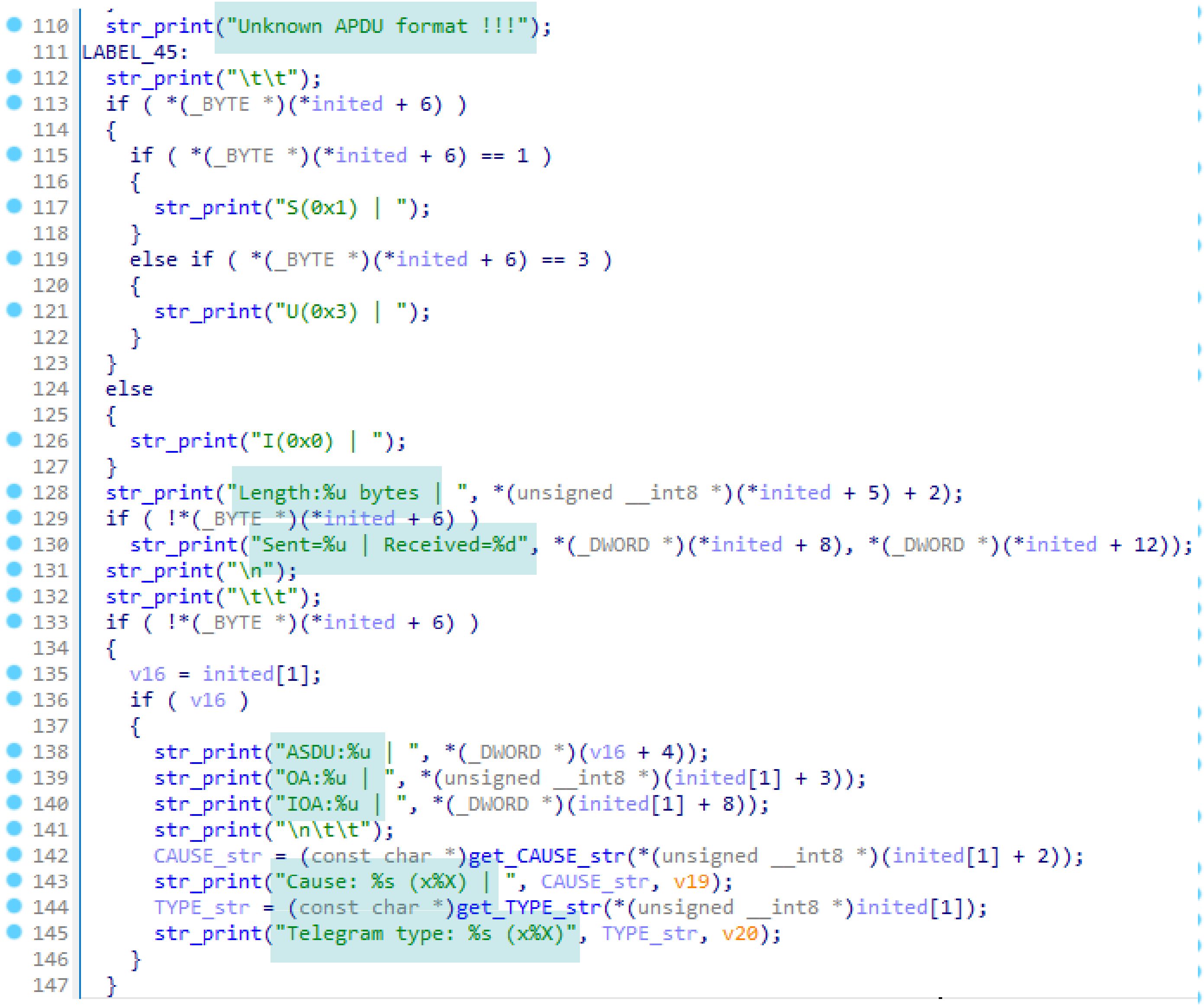
IEC-104 protocol

only

Code similarity

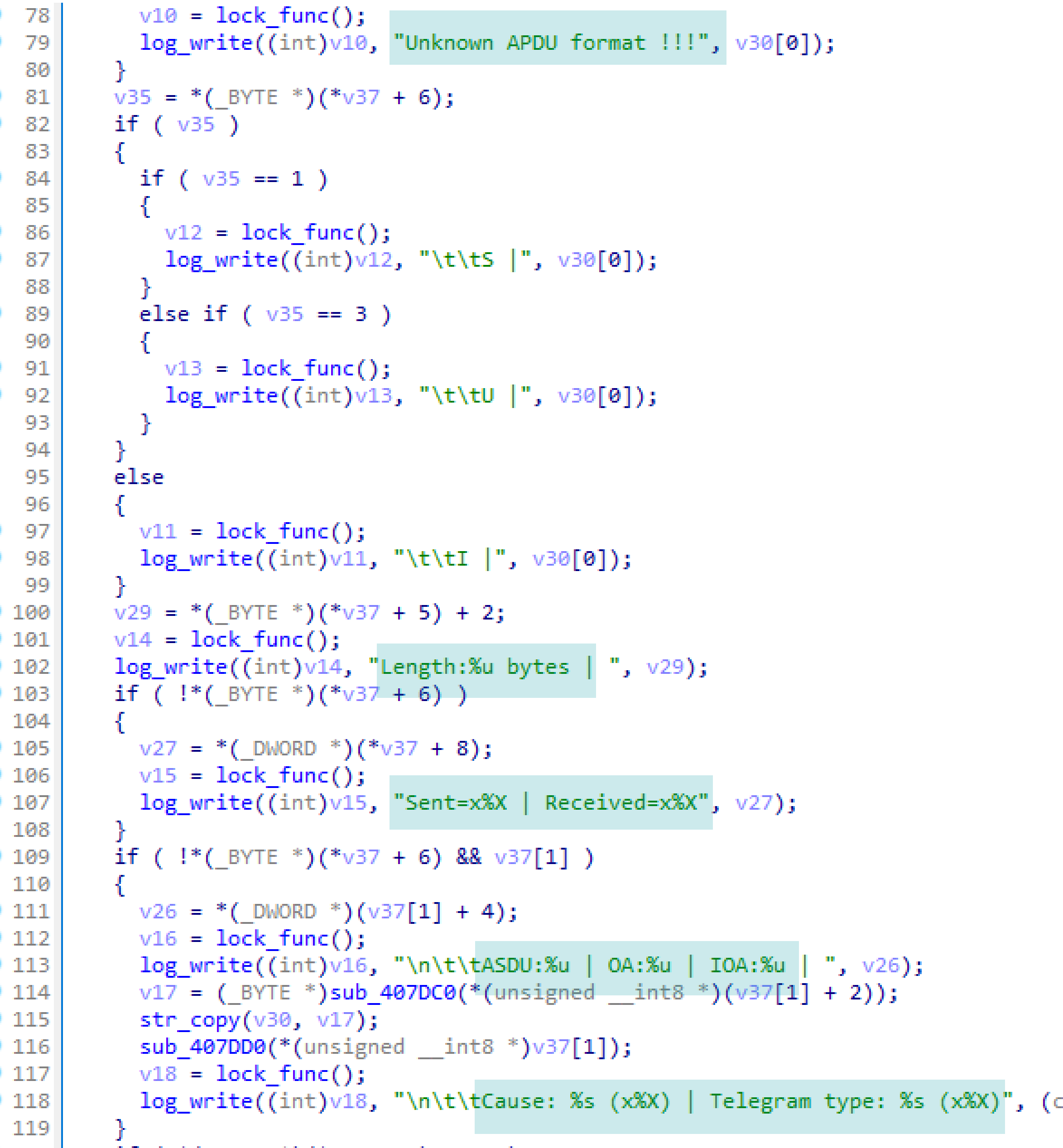
with Industroyer

Industroyer 2016

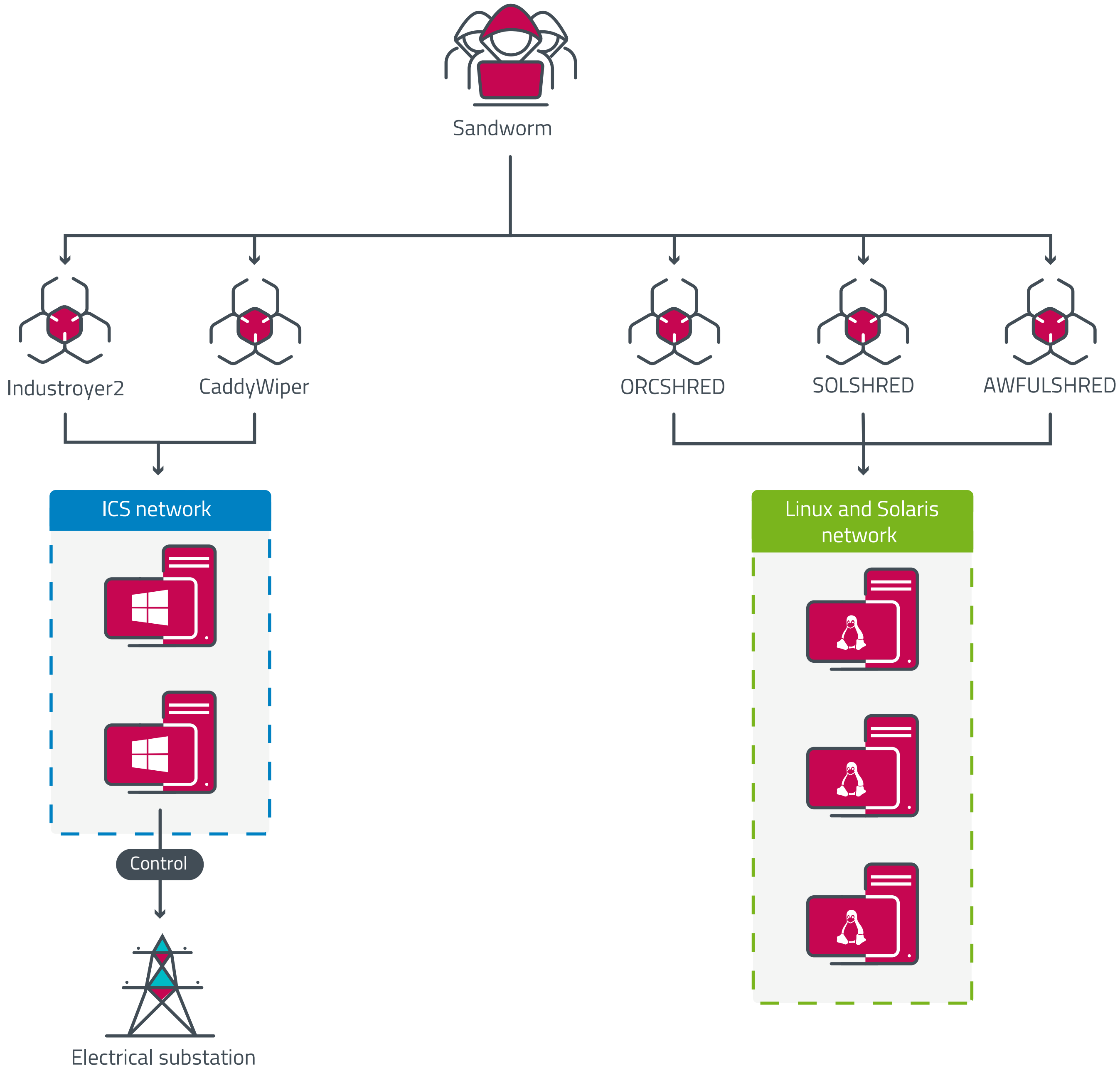


```
  str_print("Unknown APDU format !!!");
LABEL_45:
  str_print("\t\t");
  if ( *(_BYTE *)(*inited + 6) )
  {
    if ( *(_BYTE *)(*inited + 6) == 1 )
    {
      str_print("S(0x1) | ");
    }
    else if ( *(_BYTE *)(*inited + 6) == 3 )
    {
      str_print("U(0x3) | ");
    }
  }
  else
  {
    str_print("I(0x0) | ");
  }
  str_print("Length:%u bytes | ", *(unsigned __int8 *)(*inited + 5) + 2);
  if ( !*(_BYTE *)(*inited + 6) )
    str_print("Sent=%u | Received=%d", *(_DWORD *)(*inited + 8), *(_DWORD *)(*inited + 12));
  str_print("\n");
  str_print("\t\t");
  if ( !*(_BYTE *)(*inited + 6) )
  {
    v16 = inited[1];
    if ( v16 )
    {
      str_print("ASDU:%u | ", *(_DWORD *)(v16 + 4));
      str_print("OA:%u | ", *(unsigned __int8 *)(inited[1] + 3));
      str_print("IOA:%u | ", *(_DWORD *)(inited[1] + 8));
      str_print("\n\t\t");
      CAUSE_str = (const char *)get_CAUSE_str(*(unsigned __int8 *)(inited[1] + 2));
      str_print("Cause: %s (x%X) | ", CAUSE_str, v19);
      TYPE_str = (const char *)get_TYPE_str(*(unsigned __int8 *)inited[1]);
      str_print("Telegram type: %s (x%X)", TYPE_str, v20);
    }
  }
```

Industroyer2 2022



```
  v10 = lock_func();
  log_write((int)v10, "Unknown APDU format !!!", v30[0]);
}
v35 = *(_BYTE *)(*v37 + 6);
if ( v35 )
{
  if ( v35 == 1 )
  {
    v12 = lock_func();
    log_write((int)v12, "\t\tS |", v30[0]);
  }
  else if ( v35 == 3 )
  {
    v13 = lock_func();
    log_write((int)v13, "\t\tU |", v30[0]);
  }
}
else
{
  v11 = lock_func();
  log_write((int)v11, "\t\tI |", v30[0]);
}
v29 = *(_BYTE *)(*v37 + 5) + 2;
v14 = lock_func();
log_write((int)v14, "Length:%u bytes | ", v29);
if ( !*(_BYTE *)(*v37 + 6) )
{
  v27 = *(_DWORD *)(*v37 + 8);
  v15 = lock_func();
  log_write((int)v15, "Sent=x%X | Received=x%X", v27);
}
if ( !*(_BYTE *)(*v37 + 6) && v37[1] )
{
  v26 = *(_DWORD *)(v37[1] + 4);
  v16 = lock_func();
  log_write((int)v16, "\n\t\tASDU:%u | OA:%u | IOA:%u | ", v26);
  v17 = (_BYTE *)sub_407DC0(*(unsigned __int8 *)(v37[1] + 2));
  str_copy(v30, v17);
  sub_407DD0(*(unsigned __int8 *)v37[1]);
  v18 = lock_func();
  log_write((int)v18, "\n\t\tCause: %s (x%X) | Telegram type: %s (x%X)", (c
}
```


Sandworm
Industroyer2
CaddyWiper
ORCSHRED
SOLSHRED
AWFULSHRED
ICS network
Linux and Solaris network
Control
Electrical substation

14:58 UTC: Deployment of CaddyWiper on some Windows machines and of Linux and Solaris destructive malware at the energy provider

15:02 UTC: Sandworm operator creates the scheduled task to launch Industroyer2

16:10 UTC: Scheduled execution of Industroyer2 to cut power in a Ukrainian region

16:20 UTC: Scheduled execution of CaddyWiper on the same machine to erase Industroyer2 traces

2022-04-08

Sandworm

Telebots/Voodoo Bear

Sednit

Fancy Bear/APT28

Lazarus

Operation In(ter)ception
Bluenoroff

The Dukes

Cozy Bear/APT29

Turla

TA428

InvisiMole

Buhtrap

Gamaredon

welivesecurity by eset

Operation Ghost: The Dukes aren’t back – they never left

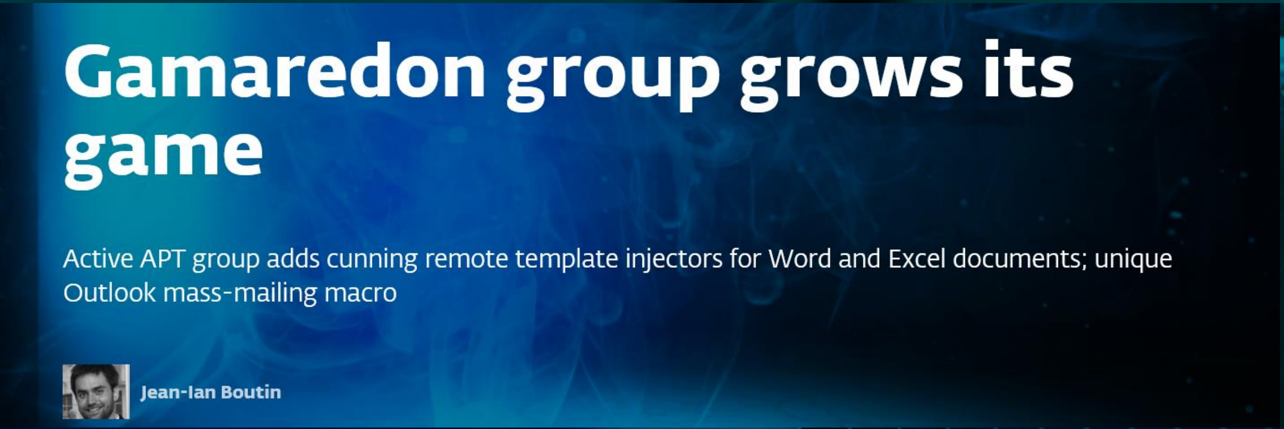
ESET researchers describe recent activity of the infamous espionage group, the Dukes, including three new malware families

(e):r ESET Research

Buhtrap group uses zero-day in latest espionage campaigns

ESET research reveals notorious crime group also conducting espionage campaigns for the past five years

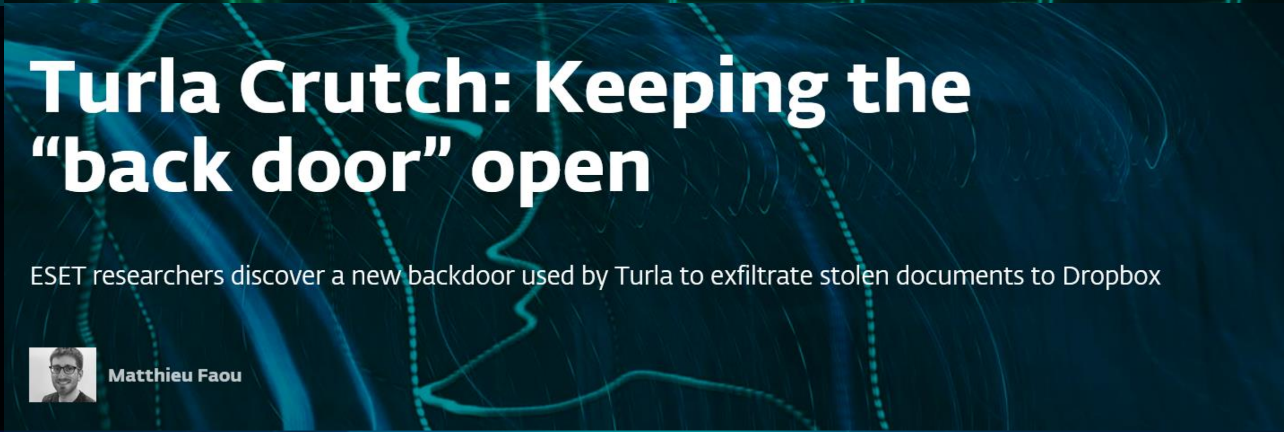
Jean-Ian Boutin



Gamaredon group grows its game

Active APT group adds cunning remote template injectors for Word and Excel documents; unique Outlook mass-mailing macro

Jean-Ian Boutin



Turla Crutch: Keeping the “back door” open

ESET researchers discover a new backdoor used by Turla to exfiltrate stolen documents to Dropbox

Matthieu Faou

Digging up InvisiMole’s hidden arsenal

ESET researchers reveal the modus operandi of the elusive InvisiMole group, including newly discovered ties with the Gamaredon group

Zuzana Hromcová Anton Cherepanov

Operation In(ter)ception: Aerospace and military companies in the crosshairs of cyberspies

ESET researchers uncover targeted attacks against high-profile aerospace and military companies

Dominik Breitenbacher Kaspars Osis

Main objectives of attackers in Ukraine?

Espionage

Data collection

Sabotage

Signaling

Main takeaways

- In the past years, Ukraine has been a cyber-battlefield, facing **many sophisticated attacks**.
- We expect the **APT attacks to continue**
- **Other countries have been targeted as well;** users need to **stay vigilant**
- ESET will continue publishing its findings via **public and private reports** to **improve the defenses of its clients and everyone else**

ESET Threat Intelligence APT reports PREMIUM

TLP: AMBER*

ENJOY SAFER TECHNOLOGY™

THREAT RESEARCH

ACTIVITY SUMMARY

Issue:

AS-2021-0009

1 May – 15 May, 2021

* This report and its contents have been provided for distribution within your organization only.

ESET Threat Intelligence Report

TLP: AMBER*

ENJOY SAFER TECHNOLOGY™

THREAT RESEARCH

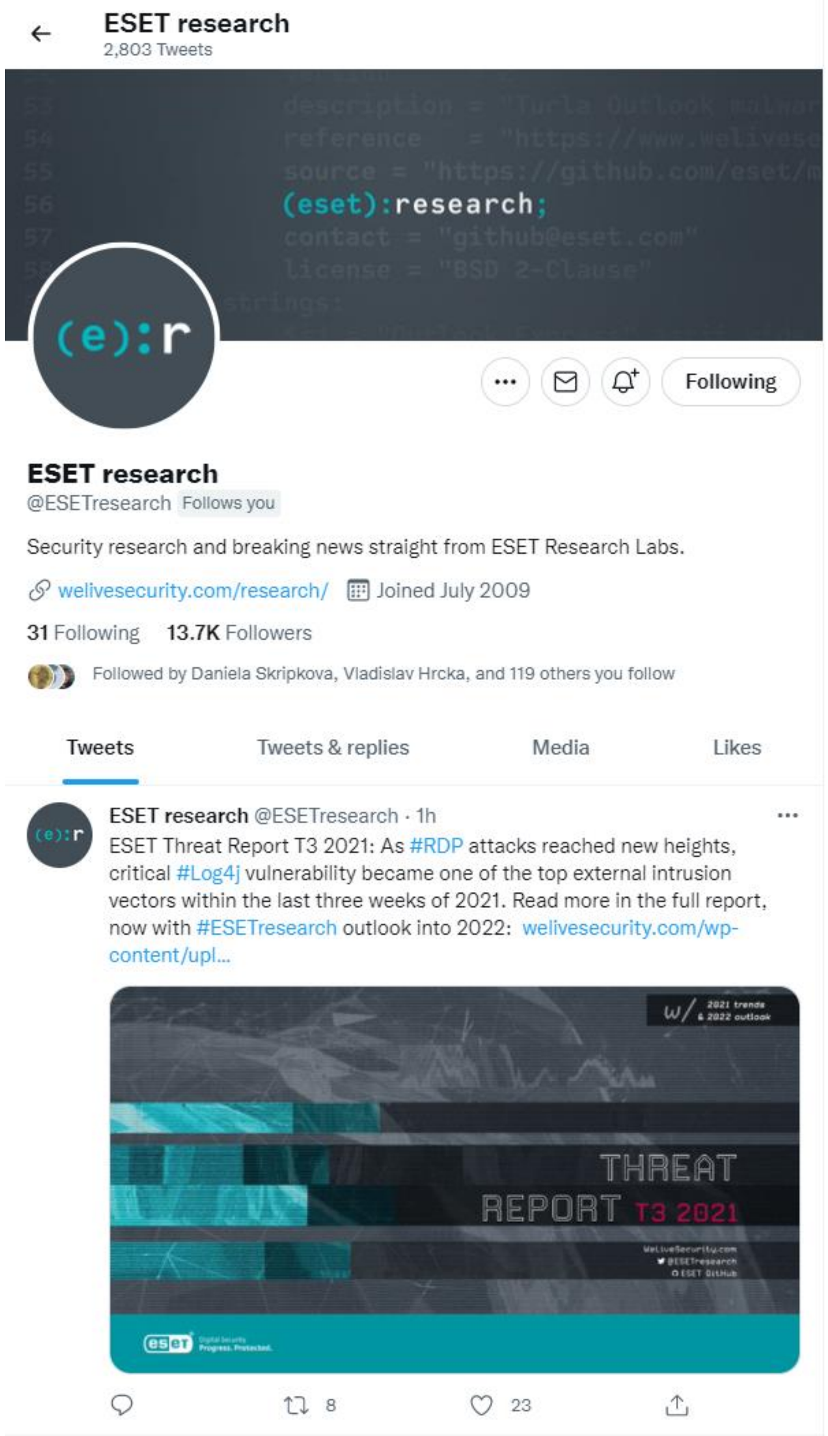
TECHNICAL ANALYSIS NETVULTURE & TURLACHOPPER

Issue:

TA-2021-0002

12 March, 2021

* This report and its contents have been provided for distribution within your organization only



ESET research
2,803 Tweets

description = "Turla Outlook malwar
reference = "https://www.welivese
source = "https://github.com/eset/m
(eset):research;
contact = "github@eset.com"
license = "BSD 2-Clause"
strings:
(e):r

Following

ESET research
@ESETresearch Follows you

Security research and breaking news straight from ESET Research Labs.

welivesecurity.com/research/ Joined July 2009

31 Following 13.7K Followers

Followed by Daniela Skripkova, Vladislav Hrcka, and 119 others you follow

Tweets | Tweets & replies | Media | Likes

ESET research @ESETResearch · 1h

ESET Threat Report T3 2021: As #RDP attacks reached new heights, critical #Log4j vulnerability became one of the top external intrusion vectors within the last three weeks of 2021. Read more in the full report, now with #ESETresearch outlook into 2022: welivesecurity.com/wp-content/upl...

w/ 2021 trends & 2022 outlook
THREAT
REPORT T3 2021
WeLiveSecurity.com
@ESETresearch
ESET GitHub
eset Digital Security Progress. Protected.

8 23

Q&A

🐦@Robert_Lipovsky

📷@Rockouter

🐦@ESETResearch