




Ondrej Kubovič

Security Awareness Specialist

 @OndrashMachula



PARTNERSKÁ
ONLINE KONFERENCIA

Najnovšie trendy a hrozby u nás a v našom susedstve

**Russian invasion
of Ukraine**

23 Feb 2022

24 Feb 2022

HermeticWiper
attack in Ukraine

Increase in cyberattacks against Ukraine



**Russian occupation
of Crimea**



Feb 2014

Apr 2014



**War in Donbas
begins**



**Russian invasion
of Ukraine**



24 Feb 2022

23 Feb 2022



**HermeticWiper
attack in 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



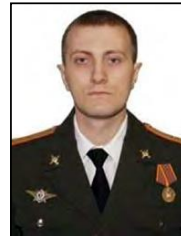
WANTED BY THE FBI

GRU HACKERS' DESTRUCTIVE MALWARE AND INTERNATIONAL CYBER ATTACKS

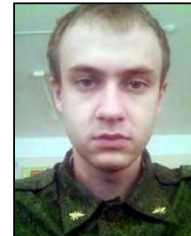
Conspiracy to Commit an Offense Against the United States; False Registration of a Domain Name; Conspiracy to Commit Wire Fraud; Wire Fraud; Intentional Damage to Protected Computers; Aggravated Identity Theft



Yuriy Sergeevich Andrienko



Sergey Vladimirovich Detistov



Pavel Valeryevich Frolov



Anatoliy Sergeevich 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 Sergeevich Andrienko, Sergey Vladimirovich Detistov, Pavel Valeryevich Frolov, Anatoliy Sergeevich 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.

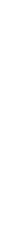
SHOULD BE CONSIDERED ARMED AND DANGEROUS, AN INTERNATIONAL FLIGHT RISK, AND AN ESCAPE RISK

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

Increase in cyberattacks against Ukraine



**Russian occupation
of Crimea**



Feb 2014

Apr 2014



**War in Donbas
begins**

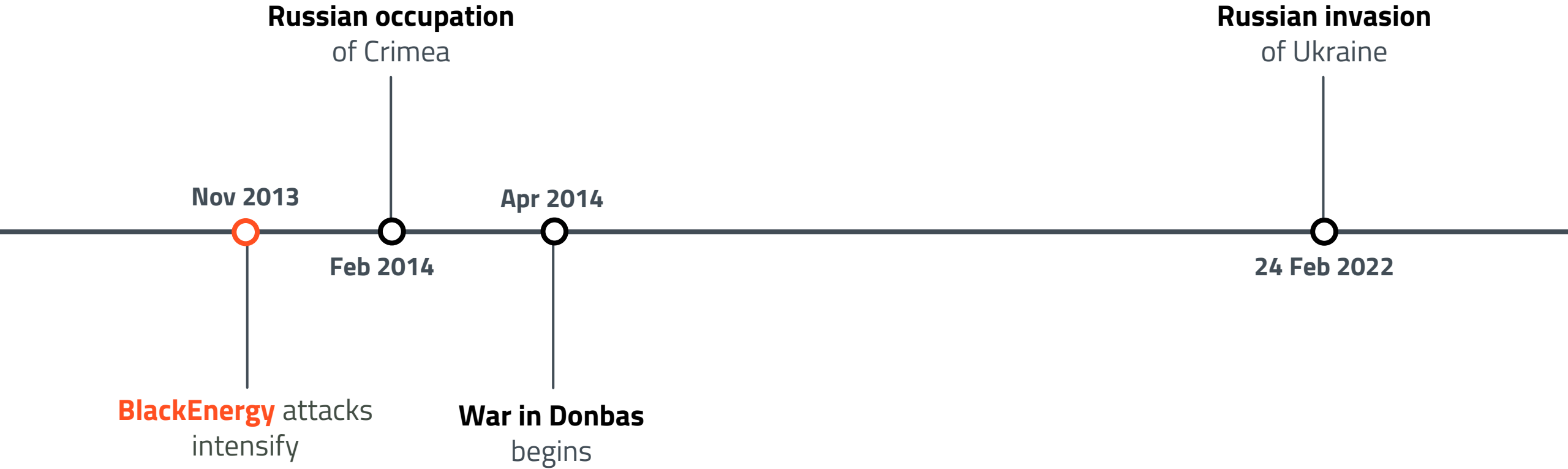


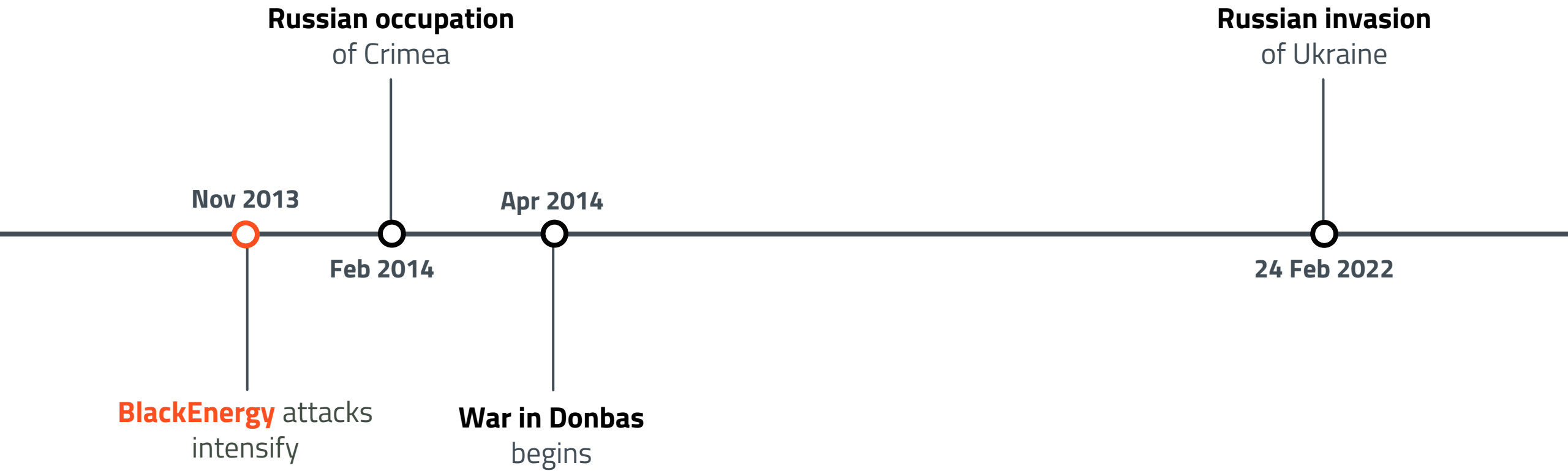
**Russian invasion
of Ukraine**

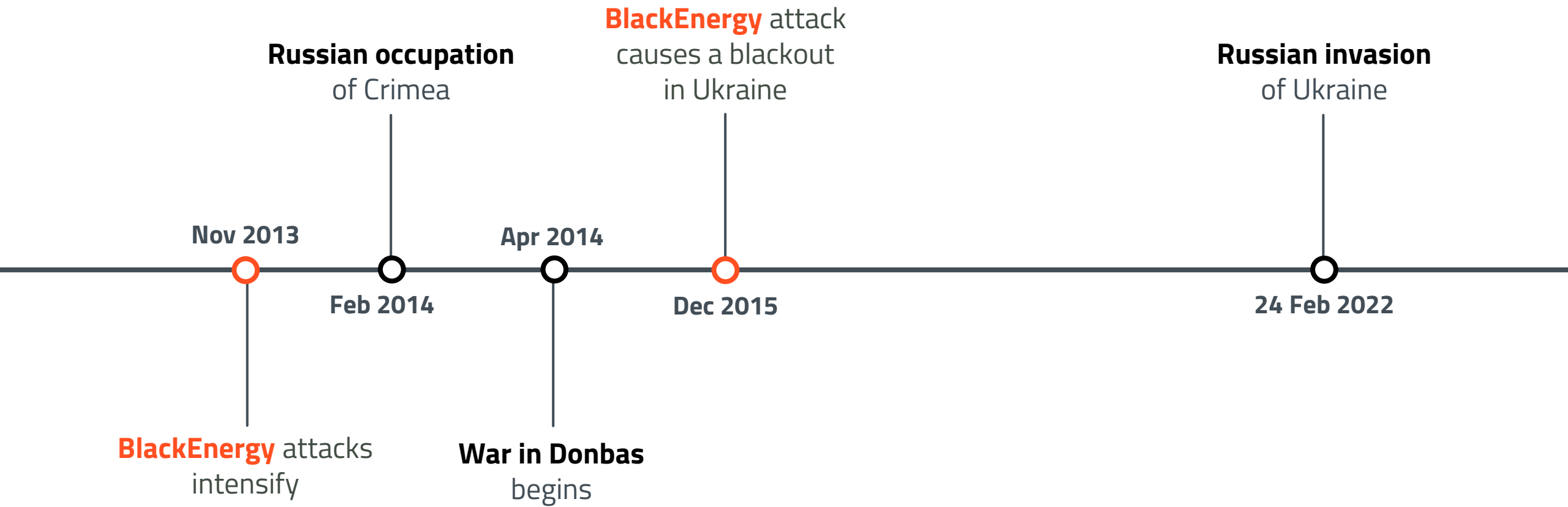


24 Feb 2022

Increase in cyberattacks against Ukraine

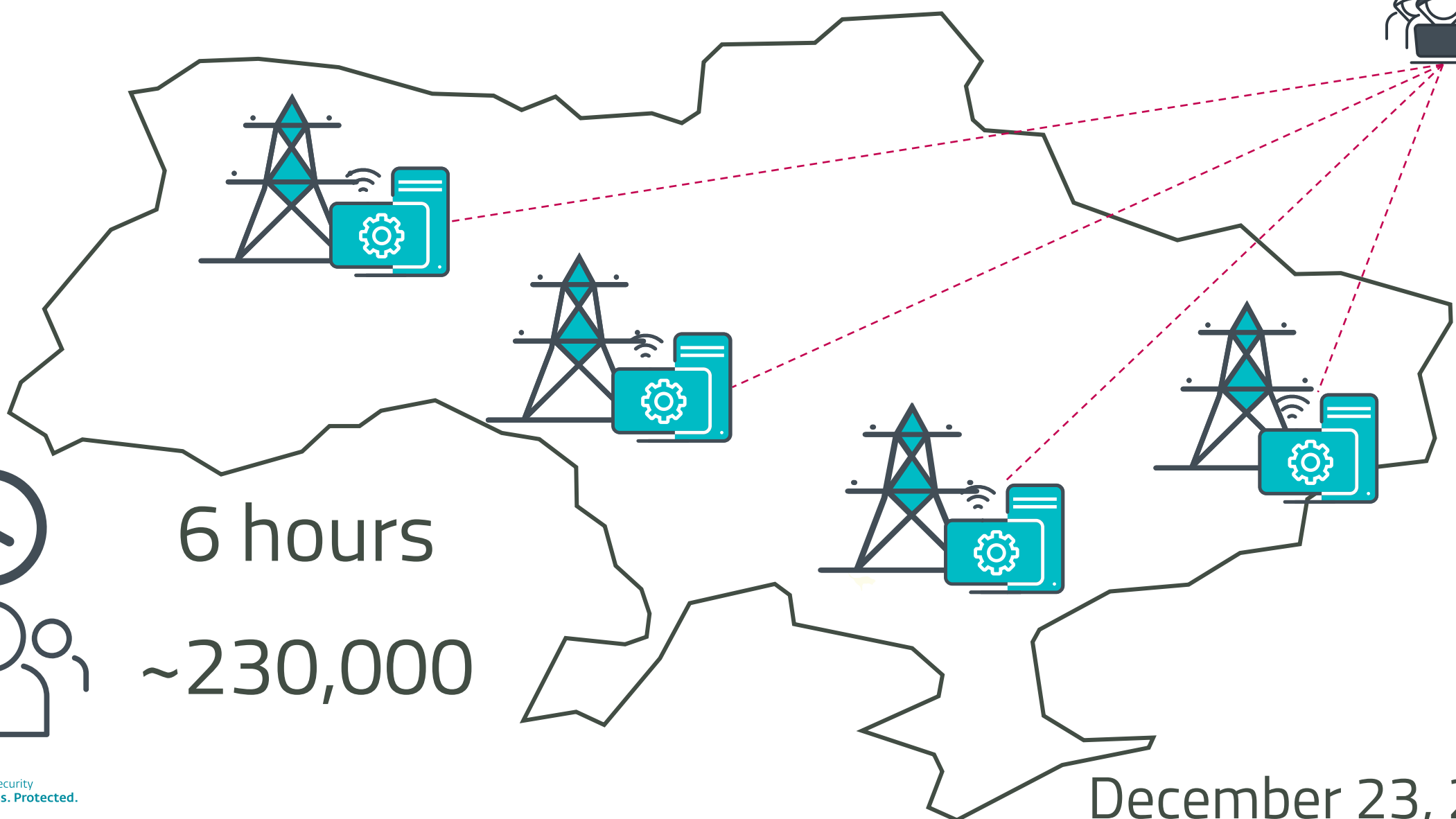






First malware-induced blackout

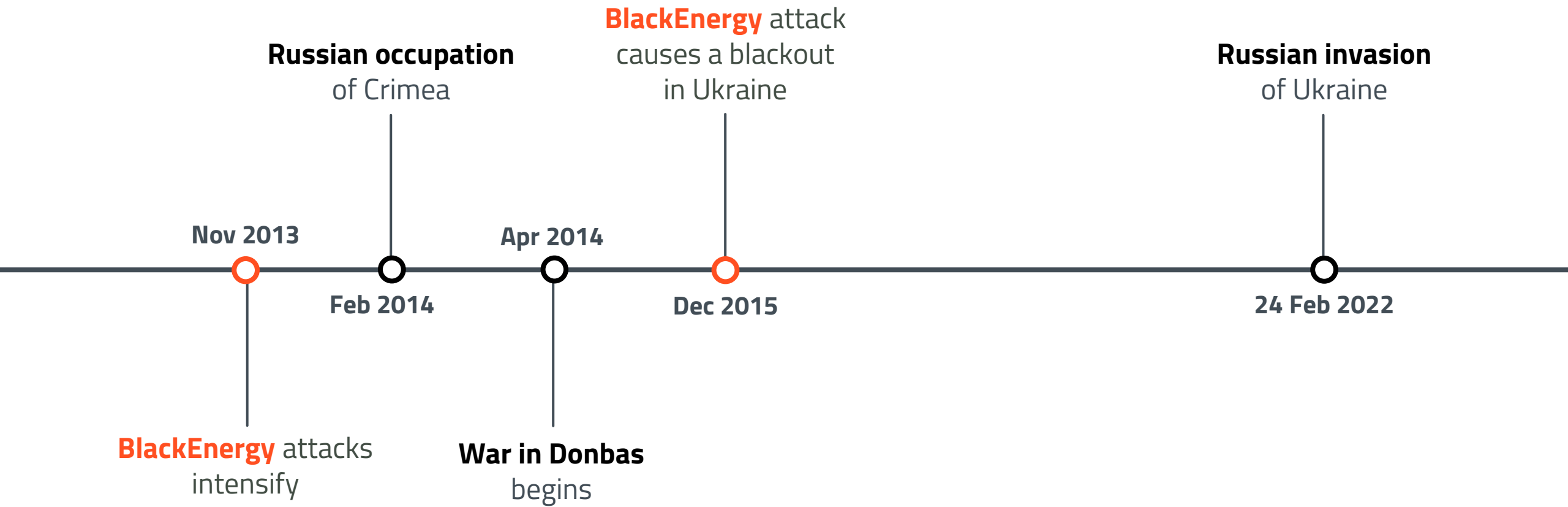
BlackEnergy

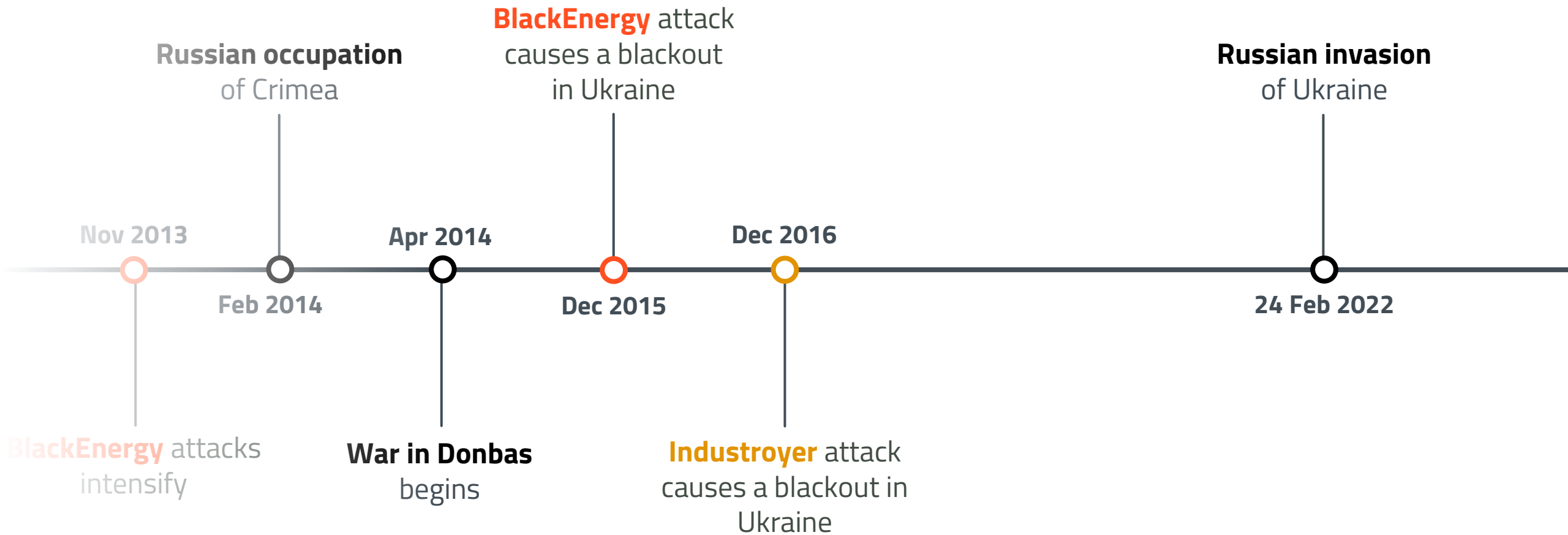


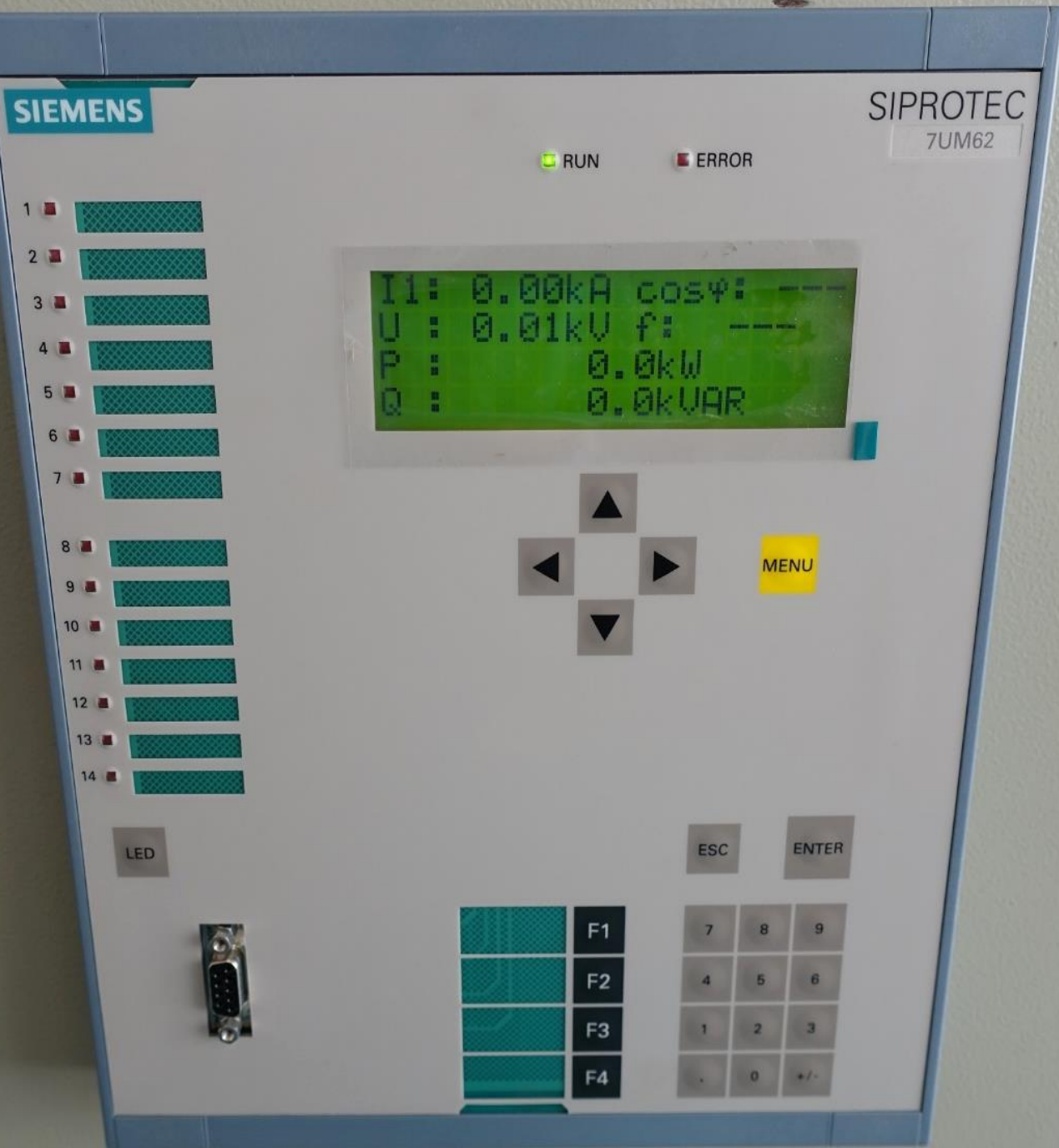
6 hours

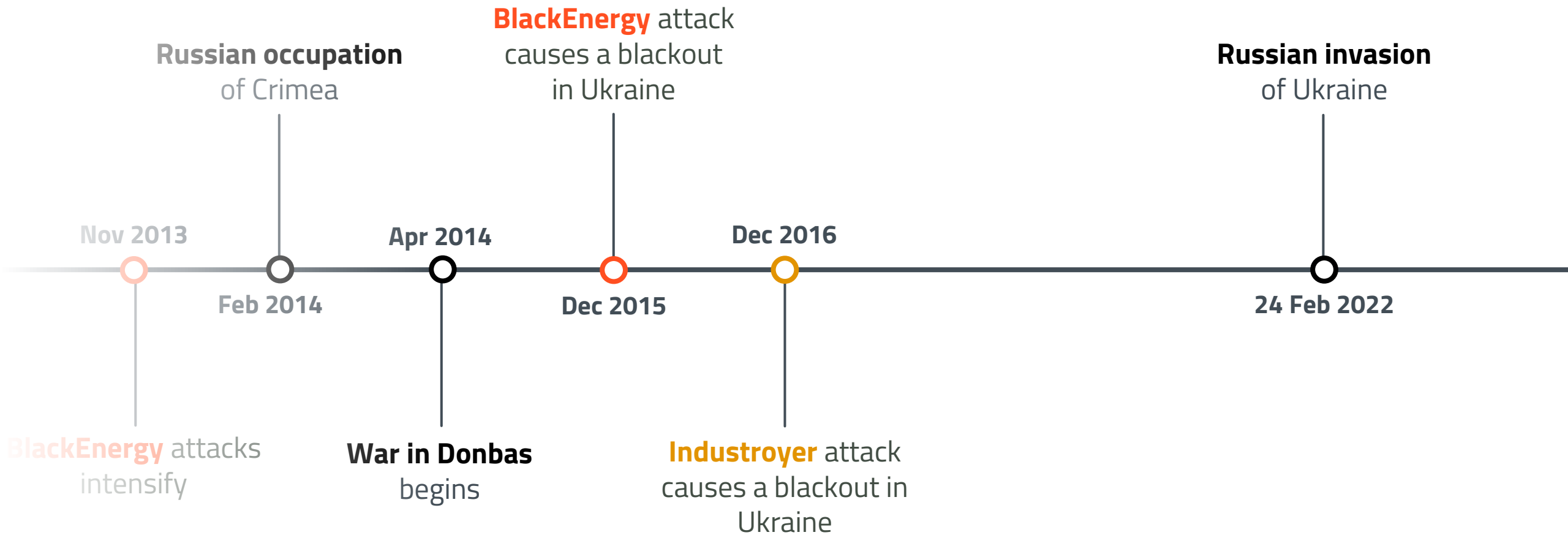


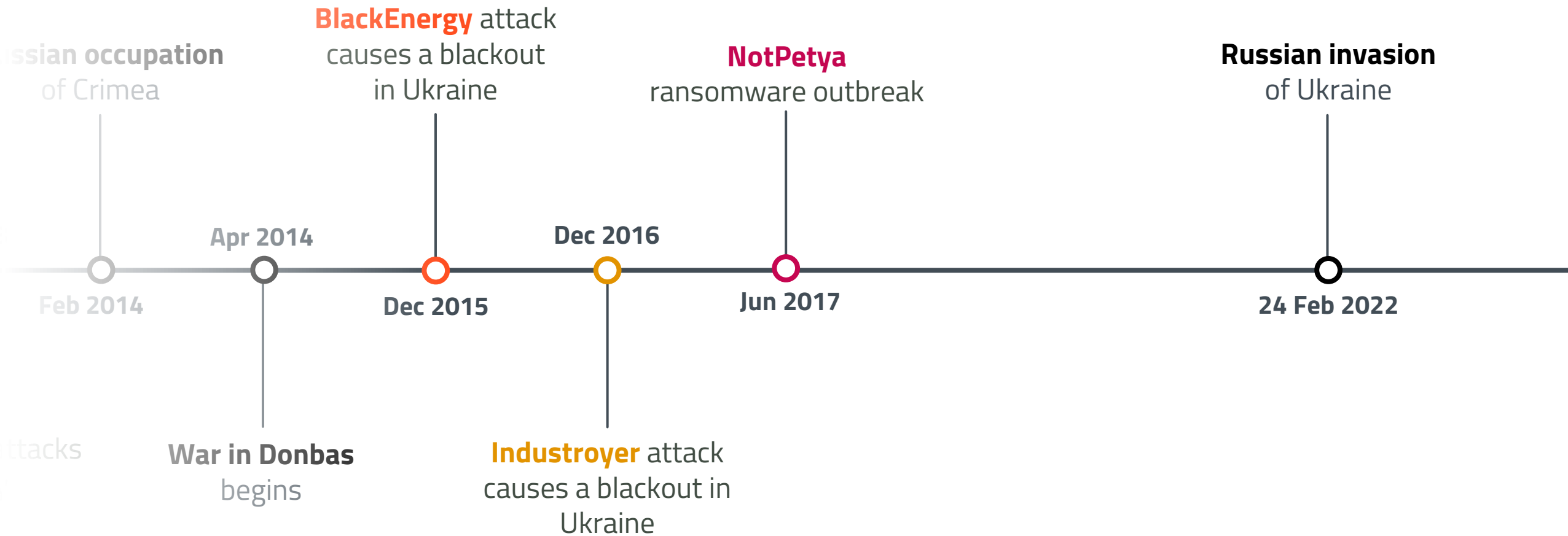
~230,000

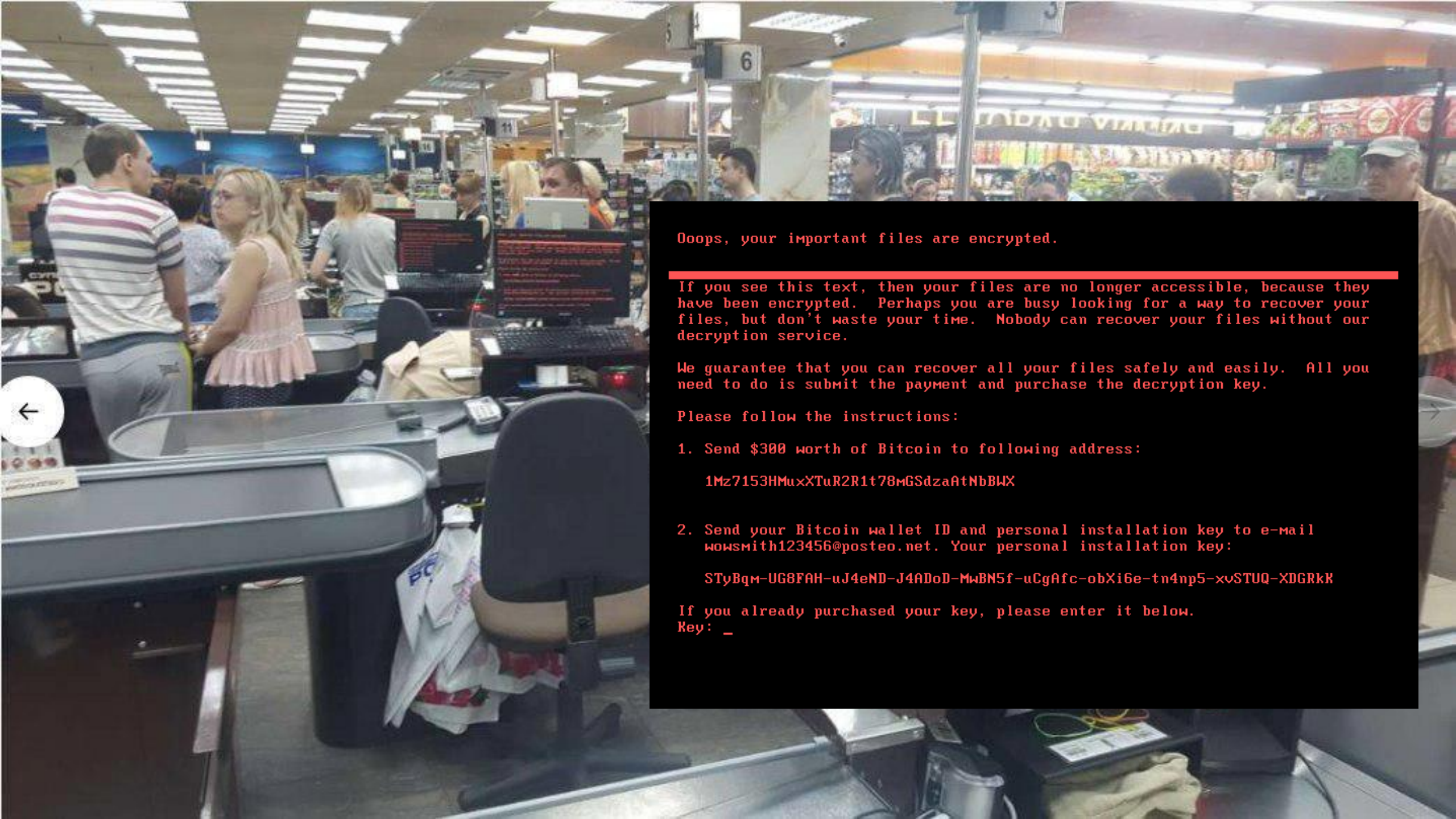












Oops, your important files are encrypted.

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

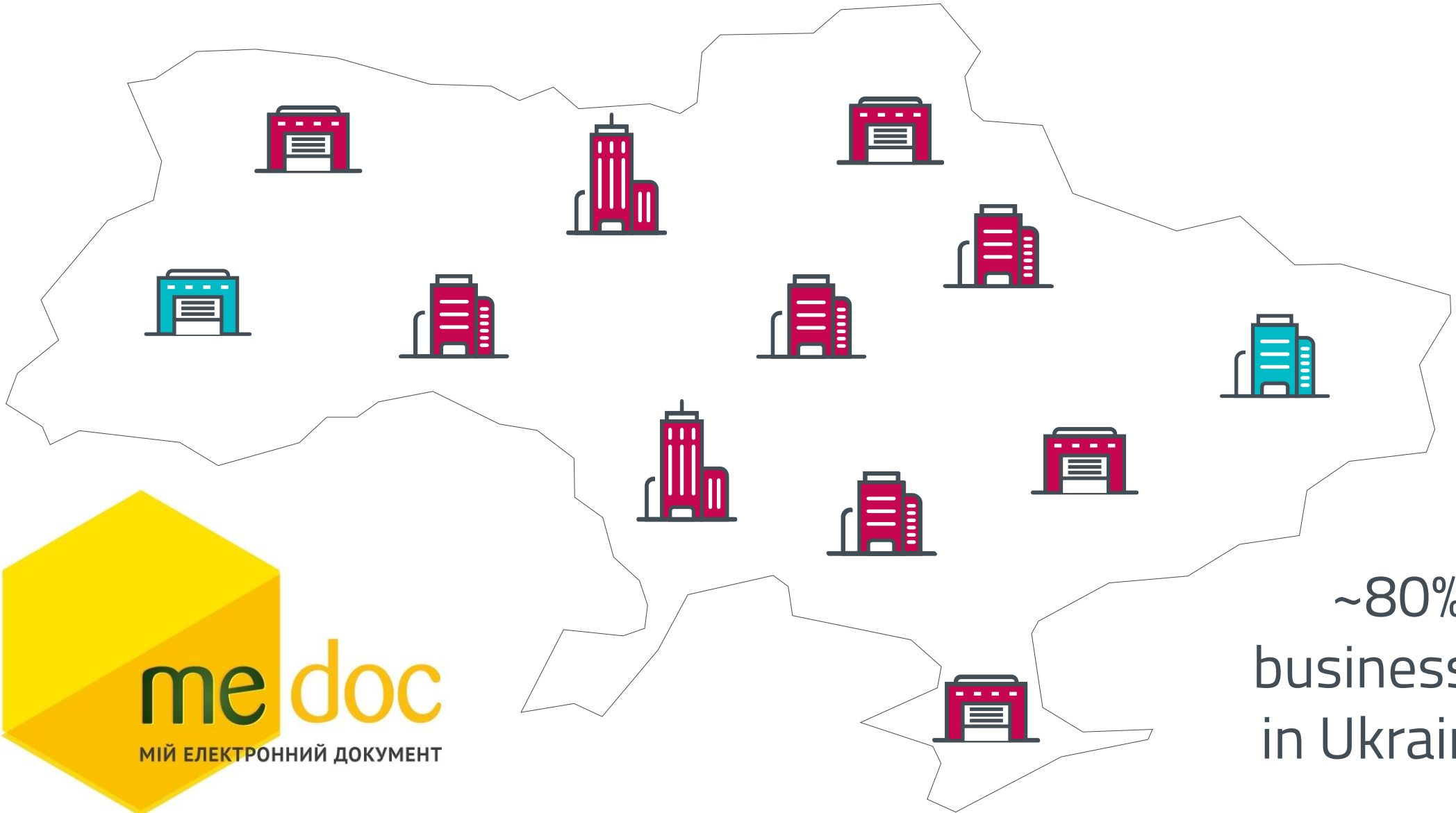
2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:

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

If you already purchased your key, please enter it below.

Key: _

NotPetya initial vector...

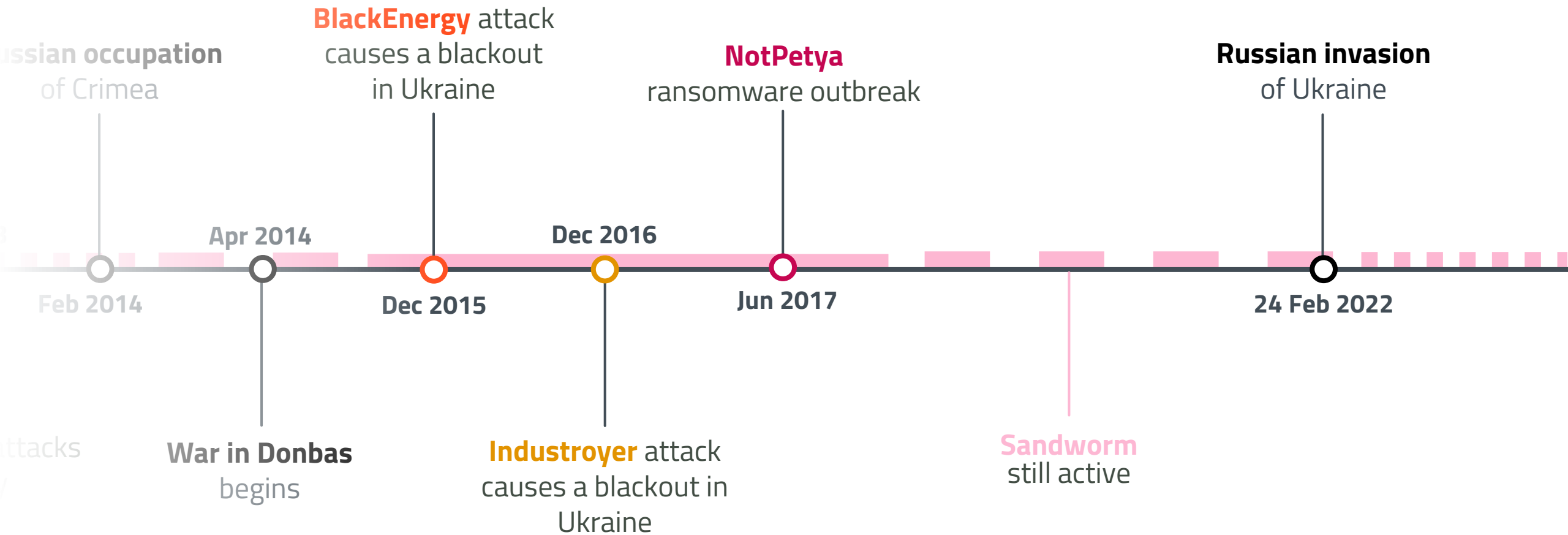


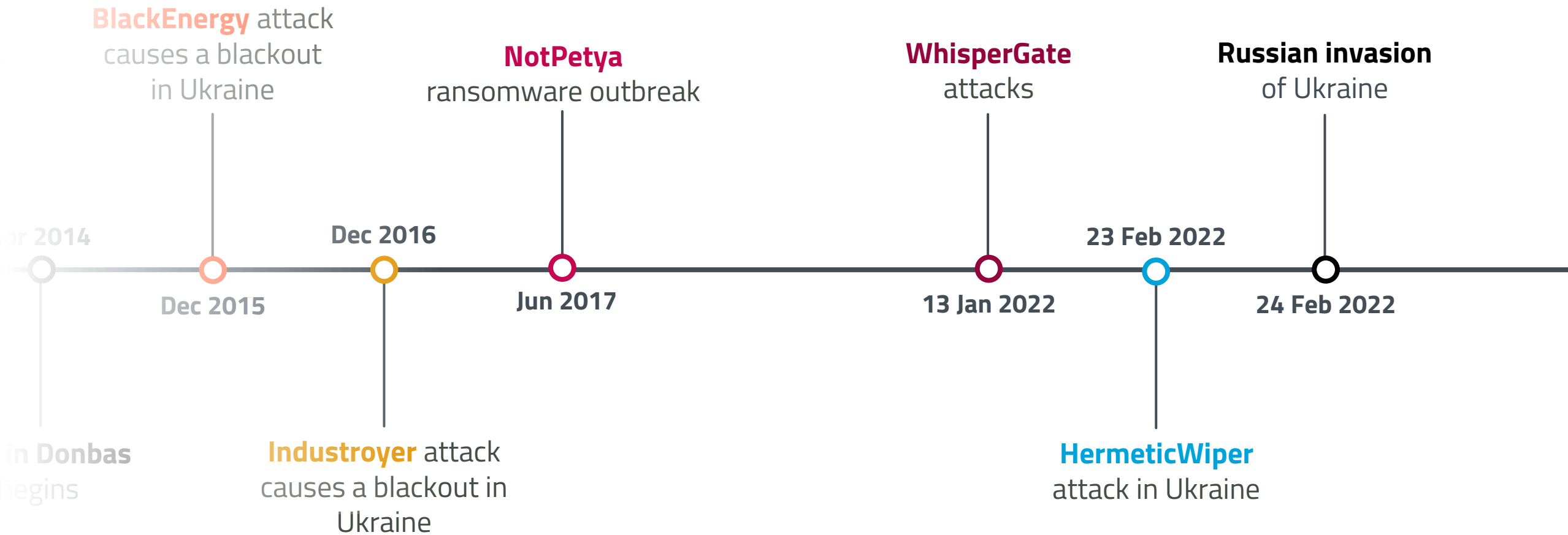
~80%
businesses
in Ukraine*



...and worldwide compromise







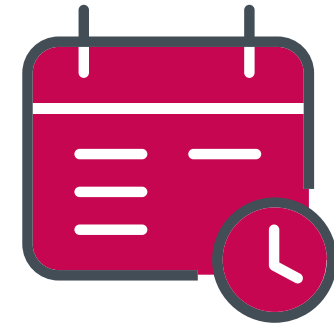
HermeticWiper



100s
systems



5+
organizations



Dec 28, 2021
compilation timestamp

Hermetic campaign



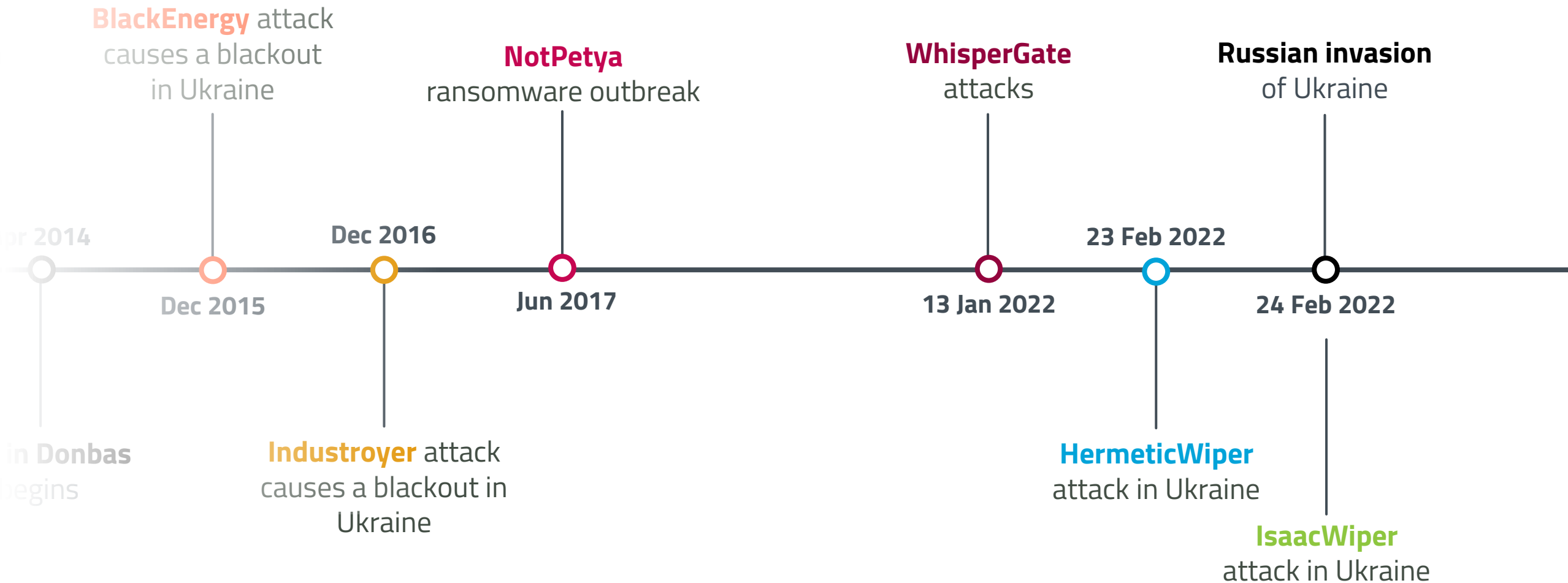
HermeticWiper



HermeticWizard



HermeticRansom



BlackEnergy attack
causes a blackout
in Ukraine

Dec 2015

Dec 2016

Industroyer attack
causes a blackout in
Ukraine

NotPetya
ransomware outbreak

Jun 2017

WhisperGate
attacks

13 Jan 2022

23 Feb 2022

HermeticWiper
attack in Ukraine

Russian invasion
of Ukraine

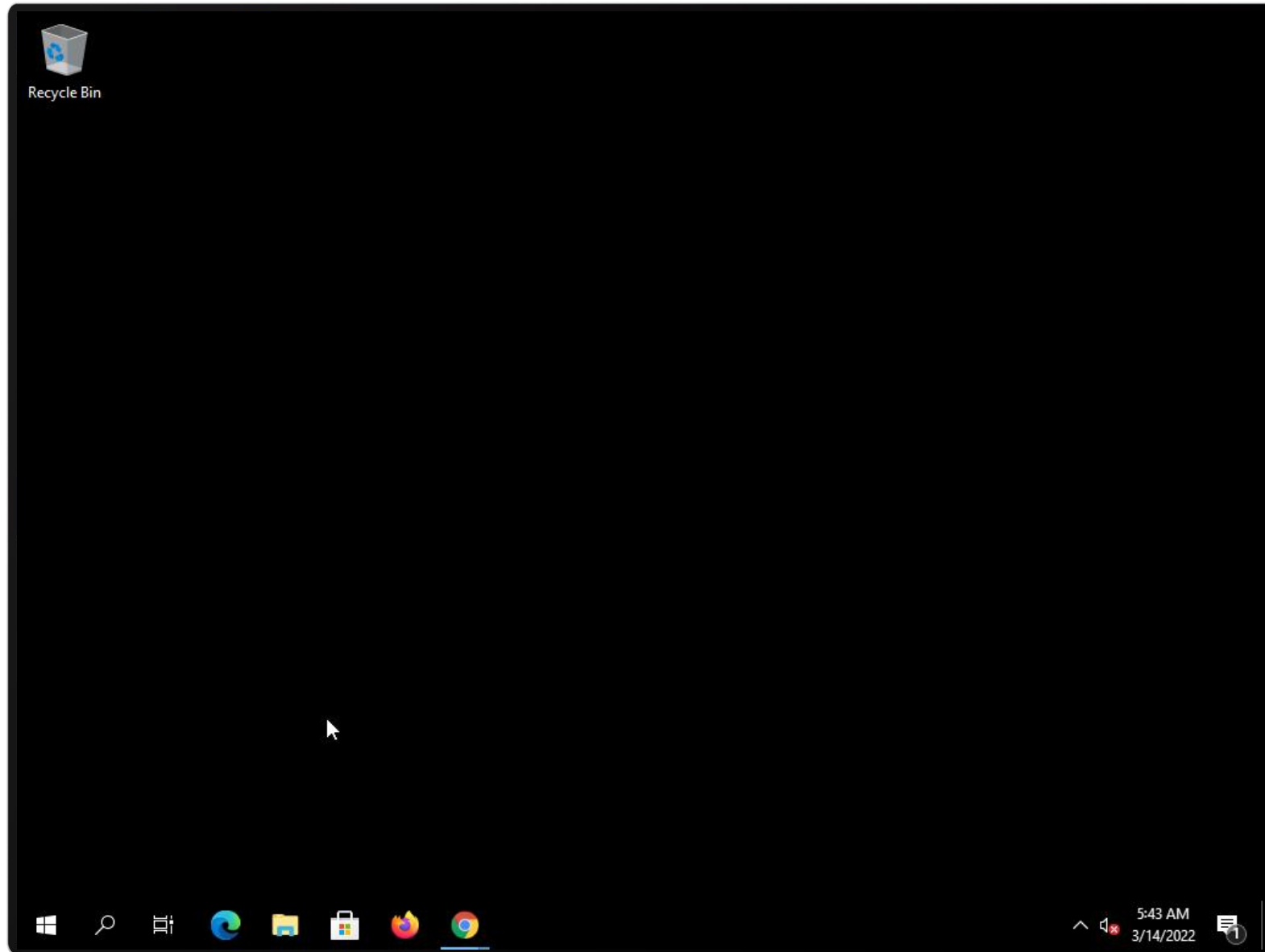
24 Feb 2022

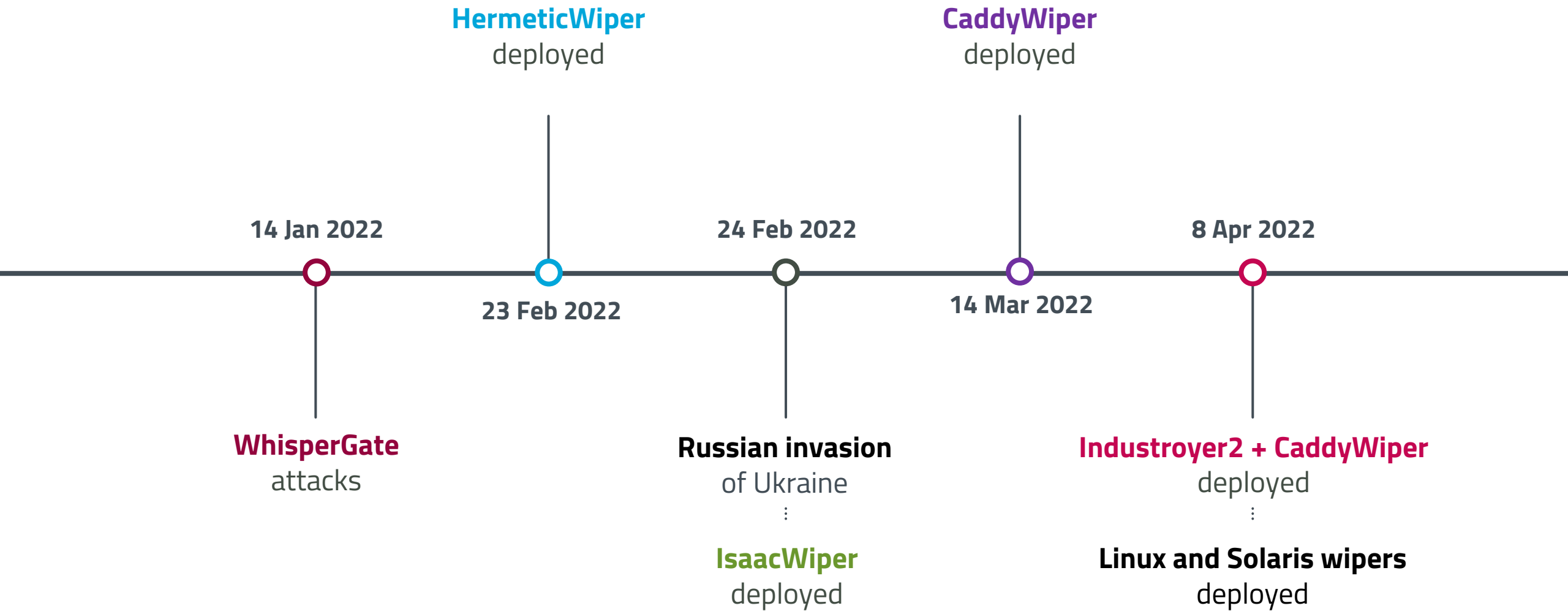
IsaacWiper
attack in Ukraine

14 Mar 2022

CaddyWiper
attack in Ukraine

...and a third one: CaddyWiper





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.

Source: [MIT Technology Review](#), [CERT-UA](#), [ESET](#), [Ukrainian Energy](#), [Ukrainian Cybersecurity Agency](#), [Ukrainian Ministry of Energy](#)

WIRED

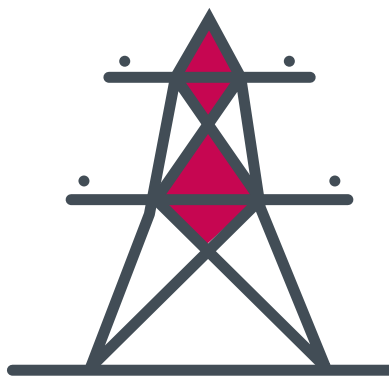
SUBSCRIBE

eSet

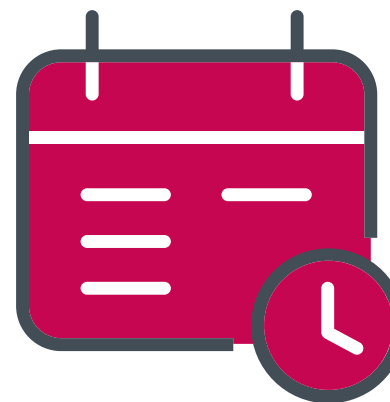
Industroyer2



Code similarity
w/ Industroyer



Targeted
energy sector

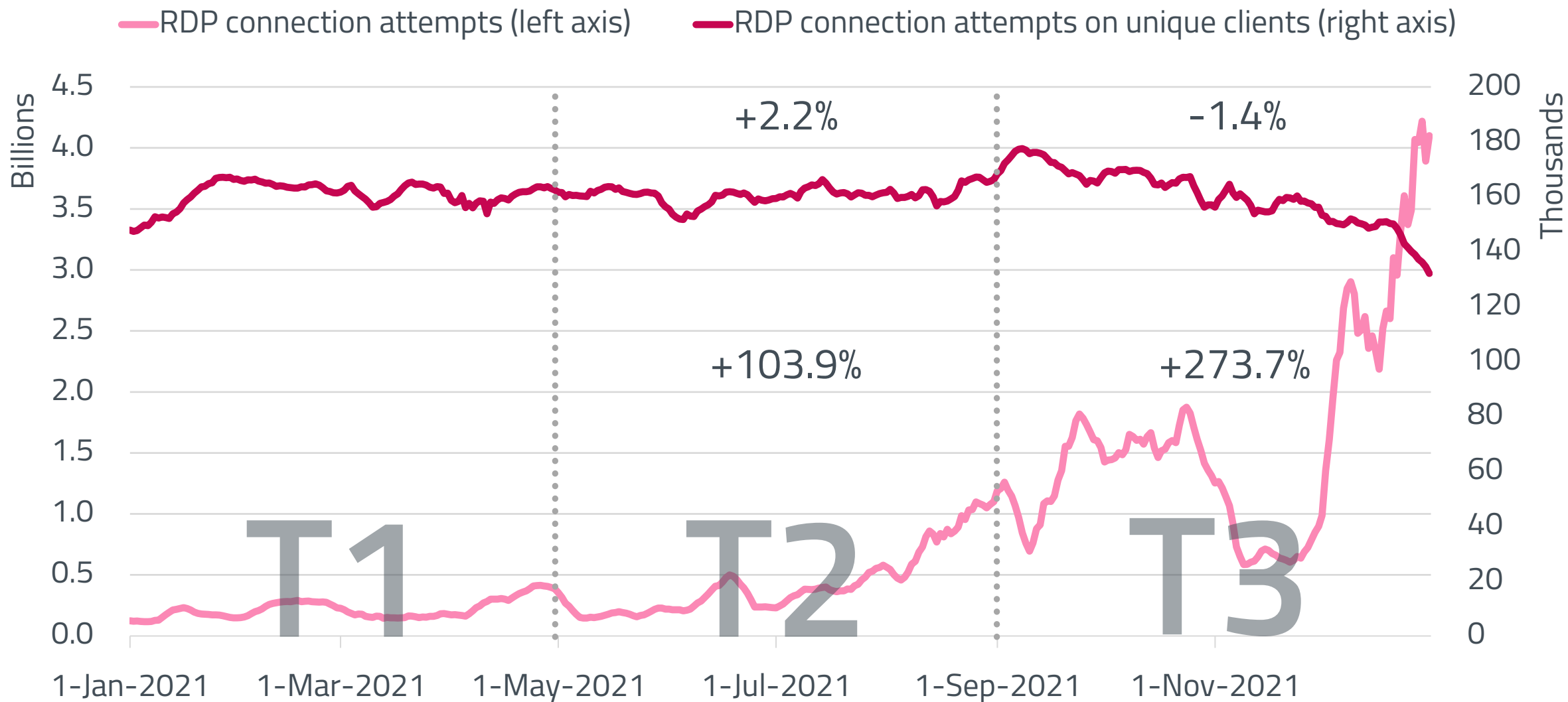


Comp. timestamp
Mar 23, 2022



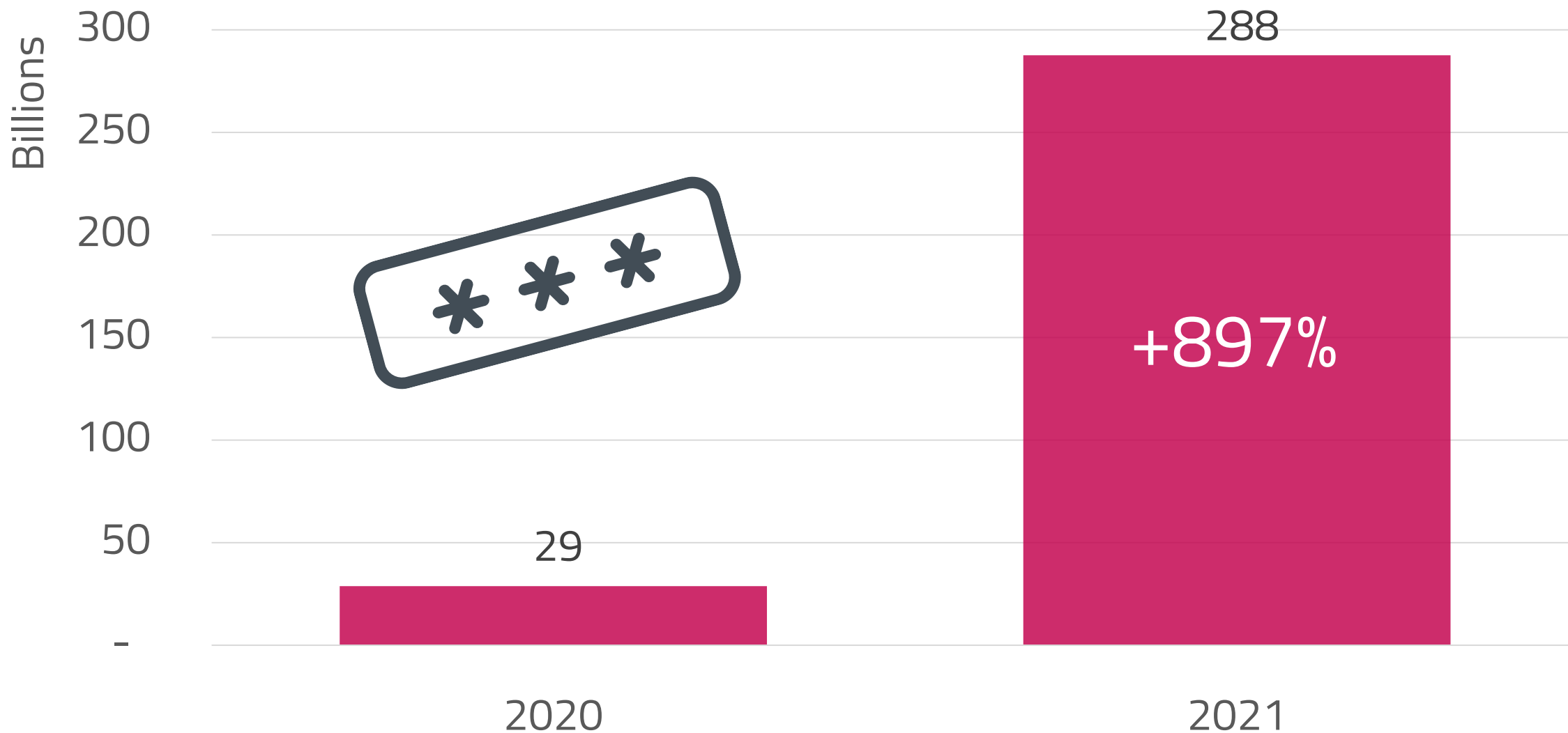
2021/2022 Trends

2021 Trends: Increase of RDP brute-force attacks



Trends of RDP connection attempts and unique clients in 2021, seven-day moving average

2021 Trends: Increase of RDP brute-force attacks





HiveLeaks

\$240,000,000

MediaMarkt

Founded in 2016 and headquartered in Zurich, Switzerland, MediaMarktSaturn Retail Group is a retail company for consumer electronics

Website

www.mediamarktsaturn.com

Revenue

\$240 000M

Employees

53 000



Encrypted at

8 November 2021

01:47:30



Disclosed at

1 December 2021 · 17:26:00

Share





2021 Trends: Emotet is back from the dead

DARKReading 

Emotet Is Back and More Dangerous Than Before



Emotet, once the world's most dangerous malware, is back

BLEEPINGCOMPUTER

Emotet malware is back and rebuilding its botnet via TrickBot

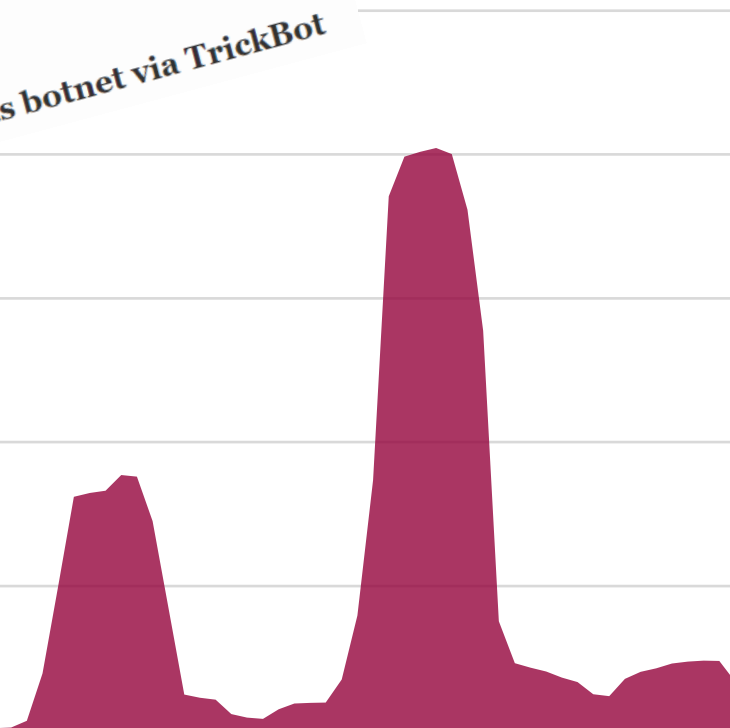
T3

1-Sep-2021

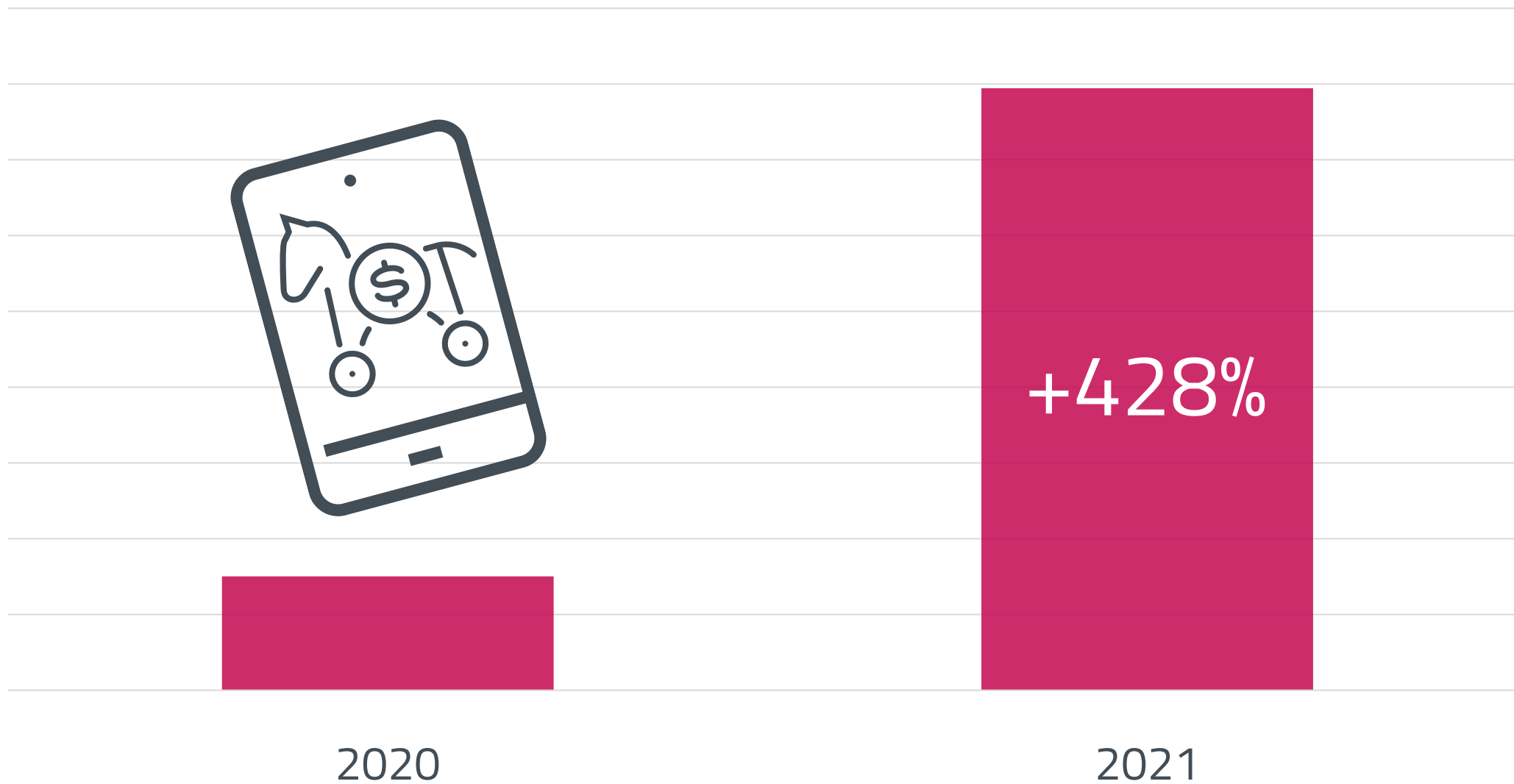
1-Oct-2021

1-Nov-2021

1-Dec-2021



2021 Trends: Extreme growth of Android banking malware

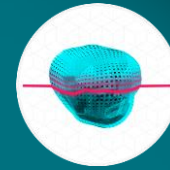




Reputation and Cache



Ransomware Shield



Advanced Memory Scanner



Brute-Force Attack Protection

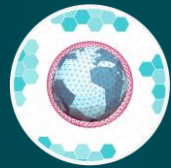


Network Attack Protection



Device Control

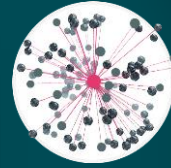
POST EXECUTION



LiveGrid[®] Protection



Secure Browser



Botnet Protection



Exploit Blocker



DNA Detections

PRE-EXECUTION

EXECUTION



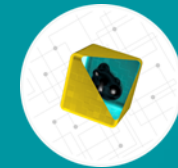
UEFI Scanner



Script Scanner & AMSI



Deep Behavioral Inspection



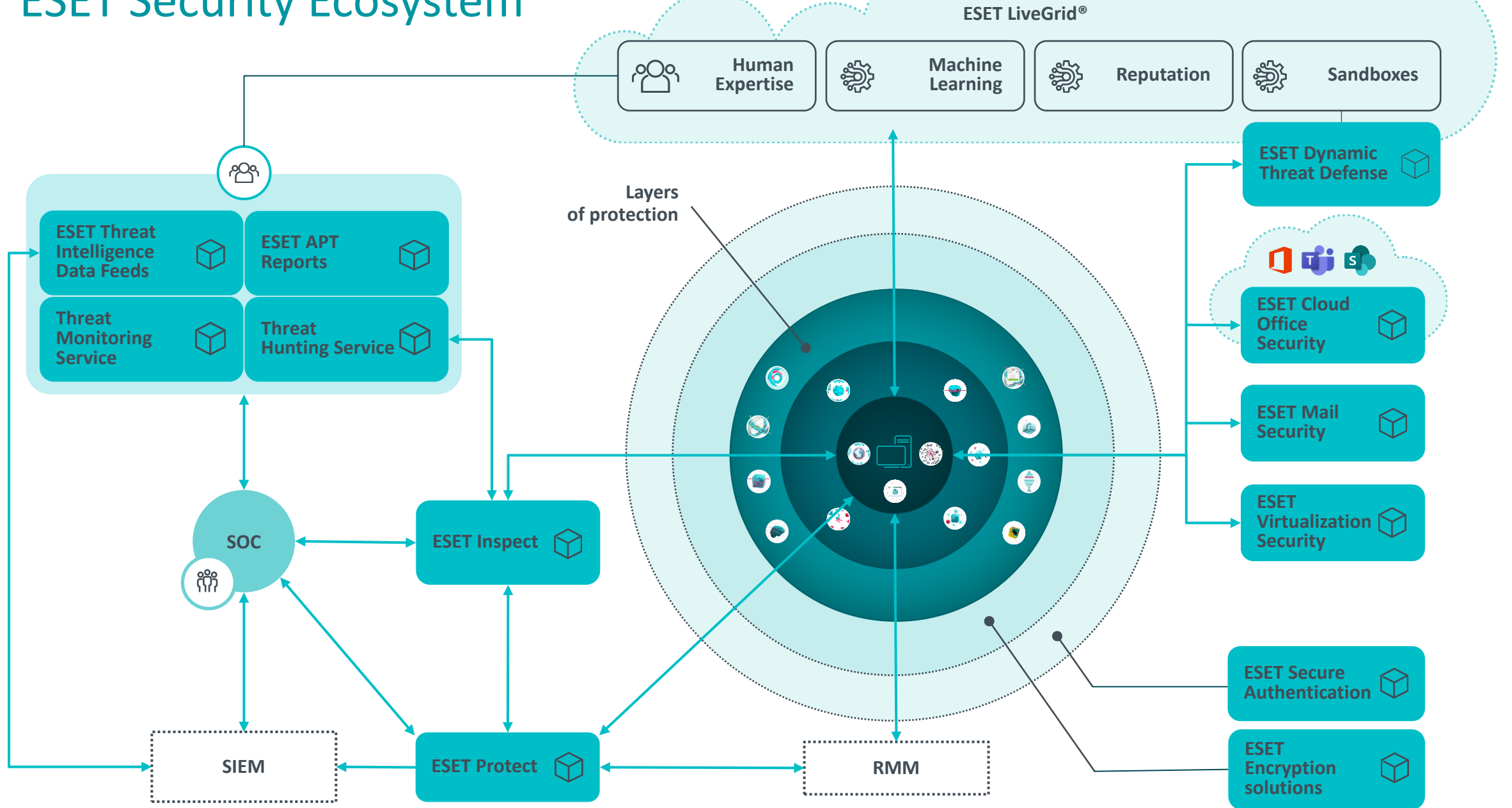
In-Product Sandbox



Advanced Machine Learning



ESET Security Ecosystem





Expert content, for researchers by researchers

Research



Watering hole deploys new macOS malware, DazzleSpy, in Asia

Hong Kong pro-democracy radio station website compromised to serve a Safari exploit that installed cyberespionage malware on site visitors' Macs

Marc-Etienne M. Léveill   and Anton Cherepanov 25 Jan 2022 - 11:30AM



DoNot Go! Do not respawn!

ESET researchers take a deep look into recent attacks carried out by Donot Team throughout 2020 and 2021, targeting government and military entities in several South Asian countries

Facundo Mu  oz and Mat  as Porolli 18 Jan 2022 - 11:30AM

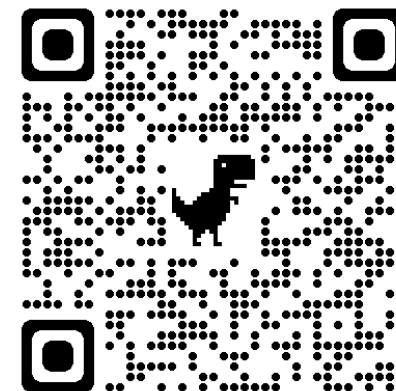
Follow us



Newsletter

Email...

Our experts



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

In English ▼ Menu ☰

Search... 🔍



Research



Watering hole deploys new macOS malware, DazzleSpy, in Asia

Hong Kong pro-democracy radio station website compromised to serve a Safari exploit that installed cyberespionage malware on site visitors' Macs

Marc-Etienne M. Léveill  and Anton Cherepanov 25 Jan 2022 - 11:30AM

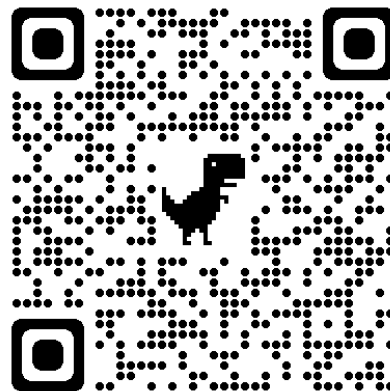


DoNot Go! Do not respawn!

ESET researchers take a deep look into recent attacks carried out by Donot Team throughout 2020 and 2021, targeting government and military entities in several South Asian countries

Facundo Mu oz and Mat as Porolli 18 Jan 2022 - 11:30AM

Follow us



ESET research
2,803 Tweets



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

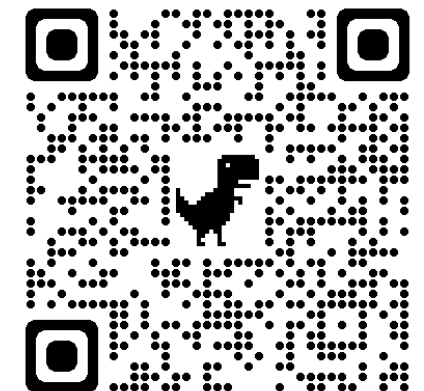
👤 Followed by Daniela Skripkova, Vladislav Hrcka, and 119 others you follow

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...



🗨️ 8

Ďakujem!



OndrashKubovic



OndrashMachula