

In the Line of Fire

Lernen Sie Ihre neuen Gegner frühzeitig kennen.

Thorsten Urbanski, Head of Communication DACH
Leiter der TeleTrust Arbeitsgruppe IT Security made in EU



Digital Security
Progress. Protected.

Wer wir sind:

- **Nummer Eins** EU Cybersecurity Hersteller im Business-Segment
- **1Milliarde+** Internetnutzer werden weltweit durch ESET-Technologien geschützt.
- **400K+** Unternehmenskunden
- **110M** Millionen Anwender



Globale Ausrichtung

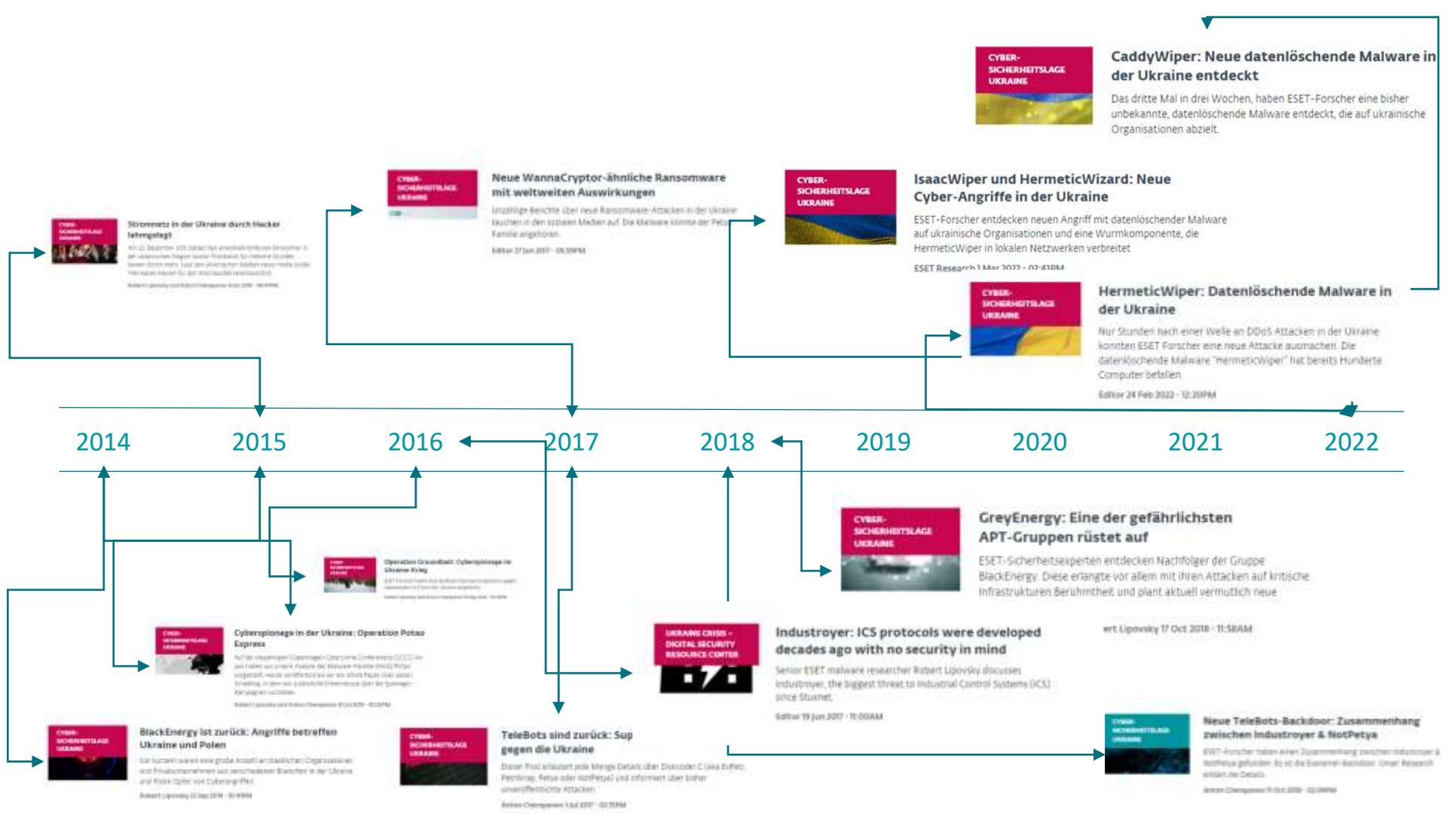
- **In 202 Ländern weltweit vertreten**
- **13 Global R&D Centres**
- **Offices in 23 Ländern**
- **100 % Made in EU**
- **30 Jahre ESET Technologie**



UKRAINE: CHRONOLOGIE



Digital Security
Progress. Protected.



2014 2015 2016 2017 2018 2019 2020 2021 2022



Stuxnet in der Ukraine durch Lehrgang
 Am 2. September 2010 haben fünf ukrainische Unternehmen in der Ukraine einen Angriff durch Stuxnet, die Wurmware, erlitten. Dieser Wurm wird den ukrainischen Behörden zugewiesen. Der Wurm wurde für den Stuxnet-Infestationsprozess entwickelt.
 Editor 12. Sep 2010 - 09:30PM



Neue WannaCryptor-ähnliche Ransomware mit weltweiten Auswirkungen
 Unzählige Berichte über neue Ransomware-Angriffe in der Ukraine tauchen in den sozialen Medien auf. Die Malware könnte der Petya-Familie angehören.
 Editor 27 Jun 2017 - 05:30PM



IsaacWiper und HermeticWizard: Neue Cyber-Angriffe in der Ukraine
 ESET-Forscher entdecken neuen Angriff mit datenlöschender Malware auf ukrainische Organisationen und eine Wurmkomponente, die HermeticWiper in lokalen Netzwerken verbreitet.
 ESET Research 1 Mar 2022 - 07:45AM



HermeticWiper: Datenlöschende Malware in der Ukraine
 Nur Stunden nach einer Welle an DDoS-Angriffen in der Ukraine konnten ESET-Forscher eine neue Attacke ausmachen. Die datenlöschende Malware "hermeticWiper" hat bereits Hunderte Computer befallen.
 Editor 24 Feb 2022 - 12:20PM



Cyberespionage in der Ukraine: Operation Potemkin Express
 Auf der diesjährigen Commonwealth Cyber Centre Conference (CCC) im Juli haben wir unsere Analyse der Ukraine-Phase von BlackEnergy vorgestellt. Heute wird berichtet, wie ein solches Phänomen durch Operation Potemkin Express als gefährliche Operation über die Grenzen hinweg hinweggeführt wird.
 Editor 10 Sep 2016 - 02:00PM



Operation GravelBall: Cyberespionage in der Ukraine-Krieg
 Ein russischer Cyberangriff auf die ukrainische Regierung ist im Zusammenhang mit der Operation GravelBall bekannt.
 Editor 10 Sep 2016 - 02:00PM



Industroyer: ICS protocols were developed decades ago with no security in mind
 Senior ESET malware researcher Robert Lipovsky discusses Industroyer, the biggest threat to industrial control systems (ICS) since Stuxnet.
 Editor 19 Jun 2017 - 11:00AM



GreyEnergy: Eine der gefährlichsten APT-Gruppen rüstet auf
 ESET-Sicherheitsexperten entdecken Nachfolger der Gruppe BlackEnergy. Diese erlangte vor allem mit ihren Angriffen auf kritische Infrastrukturen Berühmtheit und plant aktuell vermutlich neue.
 Editor 17 Oct 2018 - 11:58AM



BlackEnergy ist zurück: Angriffe betreffen Ukraine und Polen
 In der Ukraine wurde eine große Anzahl an staatlichen Organisationen und Privatunternehmen aus verschiedenen Branchen in der Ukraine und Polen Opfer von Cyberangriffen.
 Editor 12 Sep 2015 - 10:45AM



TeleBots sind zurück: Sup gegen die Ukraine
 Dieser Post erläutert jede Menge Details über DiskoBot, C Uka, Eufot, PetWiper, Beta und NotPetya und informiert über bisher unbekannteste Details.
 Editor 09 Sep 2017 - 03:30PM



Neue TeleBots-Backdoor: Zusammenhang zwischen Industroyer & NotPetya
 ESET-Forscher haben einen Zusammenhang zwischen Industroyer & NotPetya gefunden. Es ist die Stuxnet-Backdoor. Unser Research enthält die Details.
 Editor 09 Sep 2017 - 03:30PM



CaddyWiper: Neue datenlöschende Malware in der Ukraine entdeckt
 Das dritte Mal in drei Wochen, haben ESET-Forscher eine bisher unbekannte, datenlöschende Malware entdeckt, die auf ukrainische Organisationen abzielt.

UKRAINE: 2015

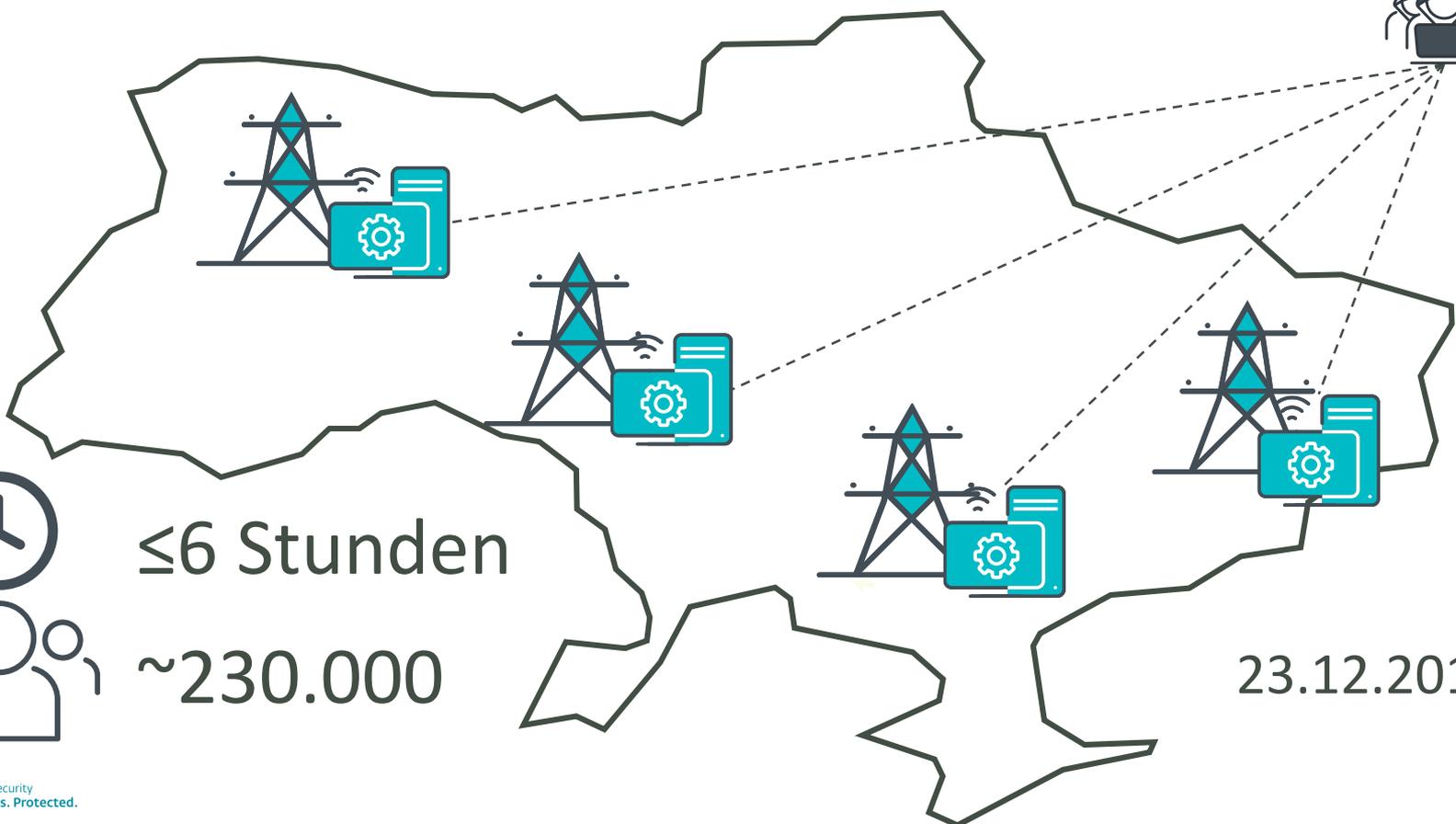


Digital Security
Progress. Protected.

BlackEnergy

ERSTER STROMAUSFALL DURCH MALWARE

BlackEnergy



≤6 Stunden



~230.000

23.12.2015



Netzwerk Scanner



File Stealer



Password Stealer



Network Discovery

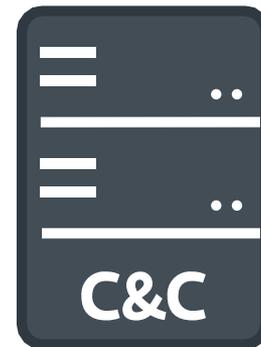


Keylogger



Screenshots

Module



BlackEnergy

GAMECHANGER 2016



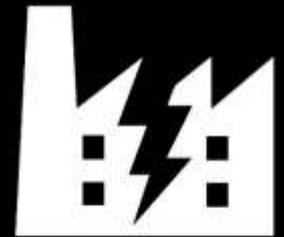
Digital Security
Progress. Protected.



17. Dezember 2016

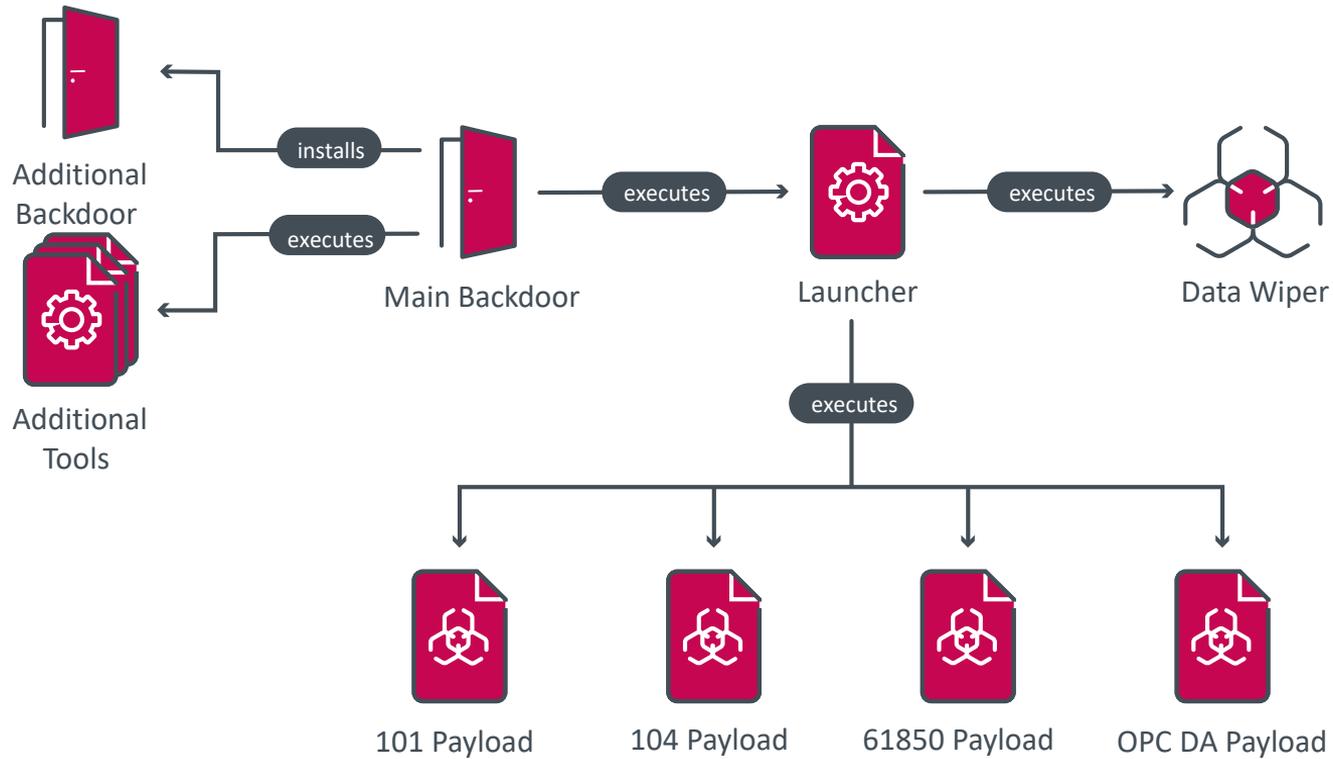
Angriffsziel:
KRITIS; Stromversorgung
in Kiew

Auswirkungen:
Blackout



INDUSTROYER

Industroyer Architektur



**WAS IST SO
BESONDERS AN
INDUSTROYER?**



2022: WIPER-MALWARE



Digital Security
Progress. Protected.

HermeticWiper-Kampagne



HermeticWiper



HermeticWizard



HermeticRansom

HermeticWiper



>100

Systeme



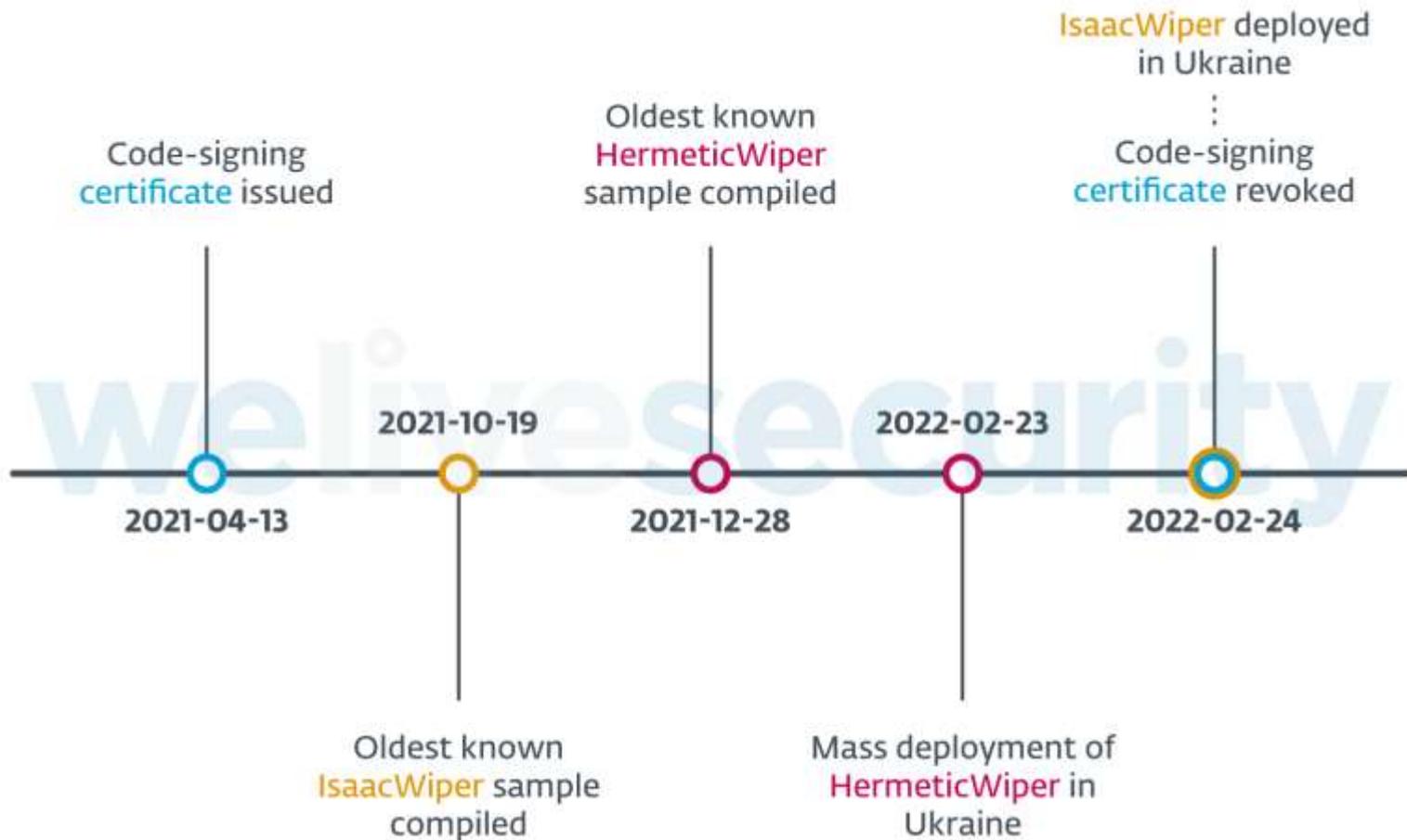
5+

Organisationen



28. Dez. 2021

Compilation Timestamp



STAATLICHE AKTEURE!



Digital Security
Progress. Protected.

Energetic Bear

The Dukes

Cozy Bear/APT29

Sandworm

Telebots
/Voodoo Bear

Turla

InvisiMole

Sednit

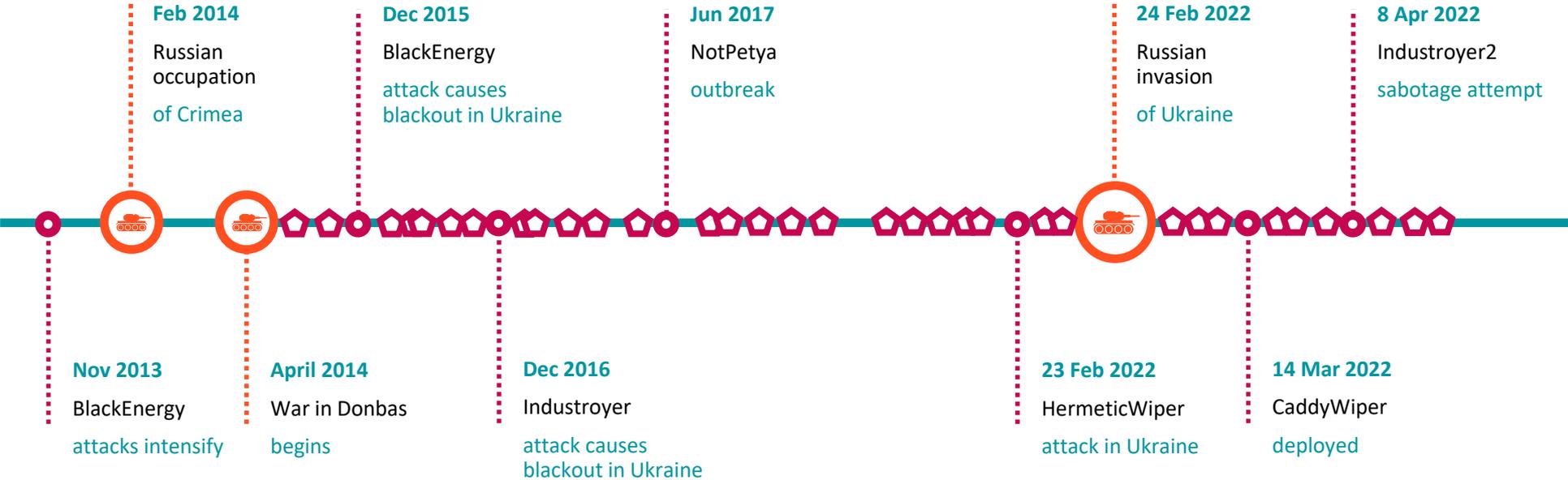
Fancy
Bear/APT28

Gamaredon

Buhtrap



Gamaredon (FSB)



Buhtrap

InvisiMole

Energetic Bear

The Dukes

Sandworm

Telebots
/Voodoo Bear

Cozy Bear/APT29

Turla

Gamaredon



FSB



SVR



GRU

Sednit
Fancy
Bear/APT28

RELEVANZ FÜR DEUTSCHLAND STATUS UND RÜCKBLICK



Digital Security
Progress. Protected.

MÖGLICHE AUSWIRKUNGEN

- Bei einer weiteren Eskalation des Konflikts könnten andere Länder stärker als zuvor in den Fokus staatlich motivierter Cyberangriffe geraten.
- Es ist nicht auszuschließen, dass Computersysteme kleinerer Versorgungsunternehmen, z.B. lokale Energieversorger bereits erfolgreich infiltriert wurden.



Presse

Zahl der IT-Störungen Kritischer Infrastrukturen

Inneres und Heimat/Antwort - 12.10.2022 (hib 532/2022)

Berlin: (hib/STO) Dem Bundesamt für Sicherheit in der Informationstechnik (BSI) sind laut Bundesregierung seit dem Beginn des russischen Angriffskrieges gegen die Ukraine am 24. Februar dieses Jahres bis zum 9. September insgesamt 253 IT-Störungen Kritischer Infrastrukturen gemeldet worden. Neben Cyber-Angriffen zählen dazu auch Ausfälle von Hard- und Software oder IT-Störungen allgemeiner Art, wie aus der Antwort der Bundesregierung ([D 20/3262](#)) auf eine Kleine Anfrage der CDU/CSU-Fraktion ([D 20/3308](#)) weiter hervorgeht. Danach ist das BSI gemäß Paragraf 8b des BSI-Gesetzes die zentrale Meldestelle für Betreiber Kritischer Infrastrukturen in Angelegenheiten der Sicherheit in der Informationstechnik.

253 IT-Störungen

Herausgeber

Deutscher Bundestag, Parlamentsnachrichten

Verantwortlich: Christian Zentner (V.i.S.d.P.)

Redaktion: Lisa Brüßler, Claudia Heine, Alexander Heinrich, Nina Jeglinski, Claus Peter Kosfeld, Hans-Jürgen Leersch, Johanna Metz, Elena Müller, Sören Christian Reimer, Sandra Schmid, Michael Schmidt, Helmut Stoltenberg, Alexander Weinleib

> Herausgeber "heute im bundestag" (hib)

Abonnement

> Newsletter abonnieren

> RSS-Dienste



KOLLATERALSCHÄDEN?!?

NOTPETYA RANSOMWARE



Digital Security
Progress. Protected.



Feb 2014

Russian occupation of Crimea

Dec 2015

BlackEnergy attack causes blackout in Ukraine

Jun 2017

NotPetya outbreak

24 Feb 2022

Russian invasion of Ukraine

2013

Energy attacks intensify

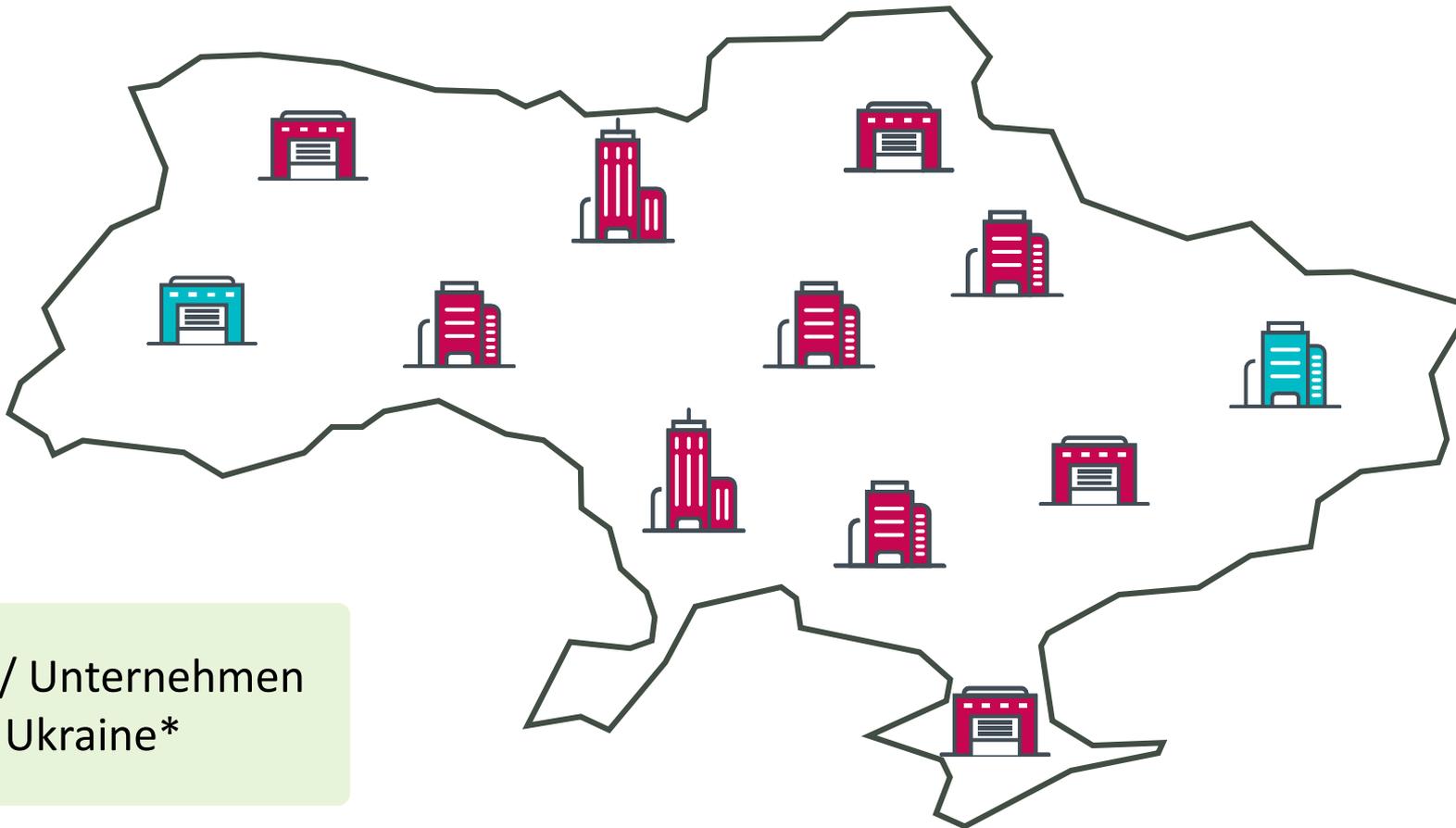
April 2014

War in Donbas begins

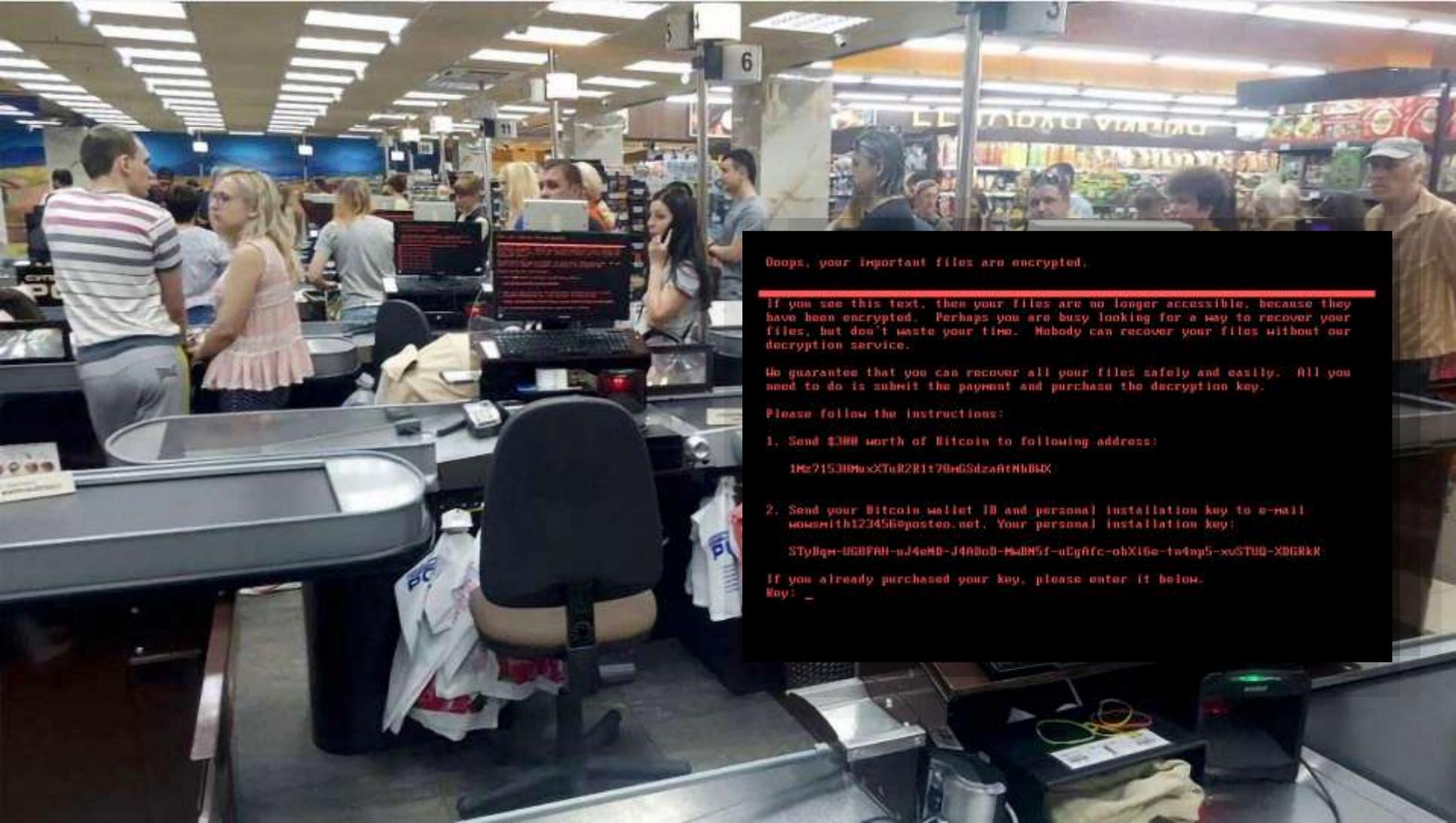
Dec 2016

Industroyer attack causes blackout in Ukraine

NotPetya's initial vector



~80% / Unternehmen
in der Ukraine*



Boops, 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.

No 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:

1Mz7153BMuxXTuR2R1t70n6SdzafNnB04X

2. Send your Bitcoin wallet ID and personal installation key to e-mail mossmith123456@posteo.net. Your personal installation key:

STyIqe-466F8H-uJ4eMB-J466o0-M46M5f-uCp0c-obX16e-tw4p5-xcSTUD-XDGkkk

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

Key: _

SCHADEN DURCH NOTPETYA

10 Milliarden USD



*„Weniger als **10 Prozent** vom IT-Budget wird für IT-Sicherheit investiert.“*

BMWi Deutschland

ZERO-TRUST-SECURITY



Digital Security
Progress. Protected.

NIEDRIGES LEVEL

- AV-Level
- kein Monitoring

-
- Keine Policy
 - Unmanaged
 - Small Office / HO

GRUNDSCHUTZ BASIS

- Endpoint-Schutz
 - Phishing / Spam
 - Firewall
-
- Device / Web
 - Managed
 - Small Office / SMB

► Erste Stufe zu Zero-Trust ◀

GRUNDSCHUTZ PLUS

- Verschlüsselung
 - Authentifizierung
 - Cloud-Sandbox
-
- Adaptiv
 - Automatisiert
 - Small Office ► SMB

INNENANSICHT / EDR

- Incident Detection
 - Threat Monitoring
 - Isolation (IoC)
-
- Evolutionär
 - + Forensik
 - SMB ► Enterprise

AUSSENSICHT / TI

- Frühwarnsystem
 - Datafeeds
 - Malware
 - Botnets
 - Domains
-
- Präventiv
 - + SIEM / SOC
 - Enterprise / KRITIS

INNENANSICHT



Digital Security
Progress. Protected.

ESETs Endpoint Lösungen

Jede einzelne Schicht unserer Endpoint-Lösung liefert Daten an den ESET INSPECT.

Eine umfassende EDR Lösung
zur Abwehr von Gefahren
für Ihr Netzwerk ,
inklusive Maßnahmen
zur Vorbeugung, Erkennung
und Beseitigung.

ESET INSPECT

Hochentwickeltes EDR-Tool, mit dem Sie in Echtzeit große Datenmengen analysieren und so jede Gefahr frühzeitig erkennen.

Innenansicht / EDR

Alarm details

Filecoder behaviour (2060 [1])

SOURCE	Filecoder behaviour (2060 [1])
CATEGORY	Filecoder
RECORDED	11 minutes ago - Mar 7, 2024, 4:07:08 PM
SEVERITY	0

ESET UserGrid®

SERVATION	●
SEVERALITY	●
FIRST SEEN	116 years ago

CATEGORY Filecoder

DESCRIPTION File with a duplicate extension created on top of a unique file extension (such as .jpg.doc), has been created, that may indicate activity of ransomware encrypting files.

MAJOR CAUSES Generated by ransomware when encrypting files.

MINOR CAUSES Sometimes used by legitimate programs to "test" before renaming a file. Usually used only on one or few files.

RECOMMENDED ACTIONS Check the count of files with changed extension and content of such changed files. Are they encrypted? Is there any reason for adding a duplicate extension? Scan the ransomware program by AV. If not detected then submit the analysis. Consider investigating files that did not suffer of damage. Shares on network may be affected. Investigate how the program reached your company and how was it used installed.

ALARM TYPE File was detected

SOURCE NAME Filecoder behaviour (2060 [1])

explor.exe

SIGNATURE TYPE
SIGNER NAME
ARCH ON	Executable
FIRST SEEN	116 years ago - Mar 6, 2024, 2:02:02 PM
LAST DETECTED	11 minutes ago - Mar 7, 2024, 4:07:08 PM

findyppd-328

PARENT GROUP	Private Department
LAST CONNECTED	116 years ago - Mar 7, 2024, 3:02:02 PM
LAST EVENT	116 years ago - Mar 7, 2024, 3:02:02 PM
AGENT VERSION	1.2.345
OS	Windows 7



Organisationen müssen heute umfassend über die Vorgänge in Ihrem Netzwerk informiert sein, um **Angriffe von außen**, **Fehlverhalten von Mitarbeitern** und **unerwünschte Anwendungen** umgehend zu identifizieren.

Innenansicht / EDR

Secur|Ty

made in EU

100% Data Protection

AUSSENANSICHT



Digital Security
Progress. Protected.

Frühwarnsystem

Überwacht Ihre Assets im Cyberraum mit Hilfe einer der besten Datengrundlagen weltweit.

ESET Threat Intelligence
liefert globale Daten aus gesicherten Quellen in Echtzeit, schützt Ihre Onlinepräsenzen, Zertifikate und Apps und damit letztlich Ihre Reputation

Datafeeds

110 Mio. Sensoren, Honey-Pots, DarkWeb und Social-Media Daten und eigene Expertenteams sorgen für Qualität.

Außensicht / TI

WAS HEIßT DAS IN
LÖSUNGEN?



Digital Security
Progress. Protected.

Datafeeds + APT-Reports
ESET Threat Intelligence

Endpoint Detection & Response
On-Premises: ESET Inspect*
Cloud: ESET Inspect Cloud*
Managed Detection & Response
ESET Security Services

Cloud-Sandboxing
ESET LiveGuard Advanced
Microsoft 365 Bedrohungsschutz
ESET Cloud Office Security*
Verschlüsselung
ESET Endpoint Encryption*
ESET Full Disk Encryption
Multi-Faktor-Authentifizierung
ESET Secure Authentication*

Schutz von Clients & Mobilgeräten
ESET Endpoint Security
ESET Endpoint Antivirus
Schutz von Fileservern
ESET Server Security
Schutz von Mailservern
ESET Mail Security

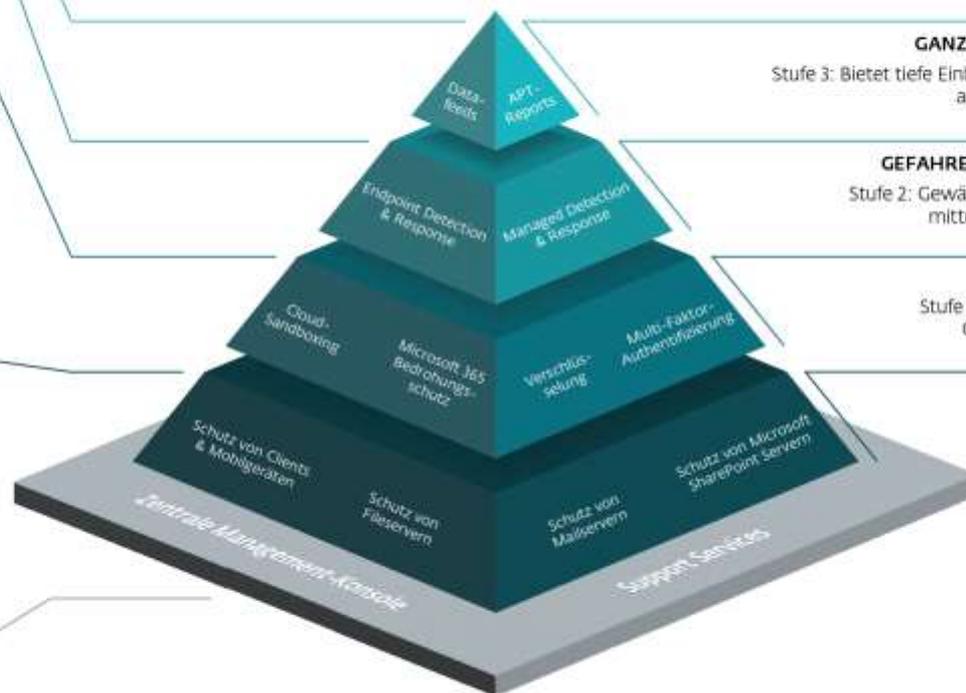
Schutz von Microsoft SharePoint Servern
ESET Security for Microsoft SharePoint Server

Zentrale Management-Konsole
On-Premises: ESET PROTECT
Cloud: ESET PROTECT Cloud

Support Services
Technischer Support **24/7**
ESET Premium Support
ESET Upgrade & Deployment
ESET Healthcheck

EINSATZBEREICH

SCHUTZLEVEL



GANZHEITLICHES LAGEBILD – AUSSENSICHT

Stufe 3: Bietet tiefe Einblicke in die globale Bedrohungslandschaft als Grundlage für einen SOC-/SIEM-Betrieb

GEFAHRENSUCHE UND ABWEHR – INNENSICHT

Stufe 2: Gewährleistet die Wirksamkeit der IT-Sicherheit mittels Anomalie-Erkennung, Schwachstellenanalyse und Incident Management

GRUNDSCHUTZ PLUS

Stufe 1: Empfohlene zusätzliche Absicherung für Cloud-Anwendungen, Daten und Zugänge sowie erweiterter Schutz vor Zero-Days

GRUNDSCHUTZ BASIS

Stufe 0: Mindestabsicherung für Endgeräte und Server



Digital Security
Progress. Protected.

*Verwaltung über separate Management-Konsole

IT-Sicherheit ist Vertrauenssache

25.-27.
Oktober
in Nürnberg



Digital Security
Progress. Protected.



Besuchen Sie ESET
am Stand 7-530



HOME OF IT SECURITY



Digital Security
Progress. Protected.