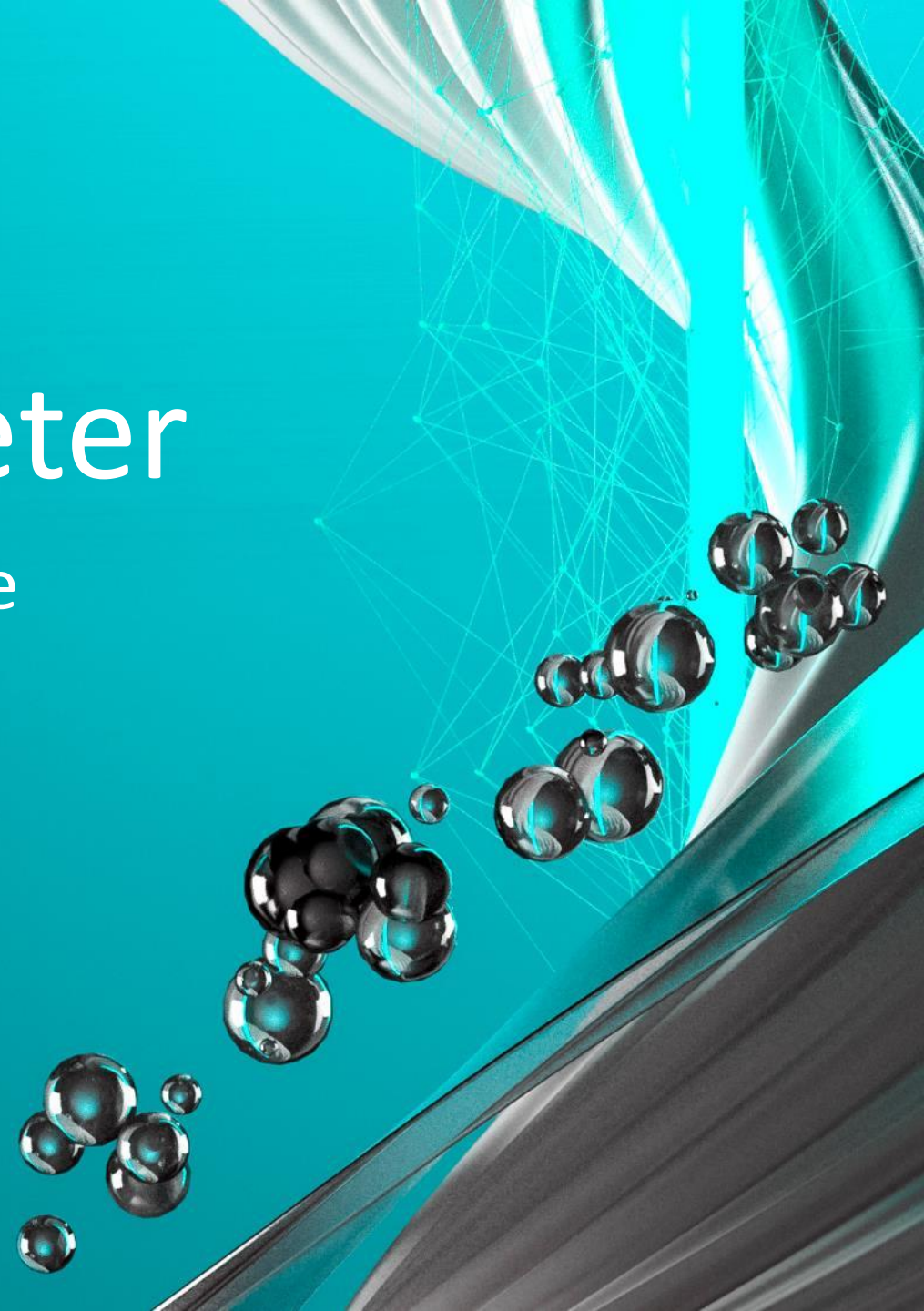


ESET Security Barometer

Aktuelle Bedrohungen und Hintergründe

Thomas Uhlemann
ESET Security Specialist

Thomas.Uhlemann@eset.com





Thomas Uhlemann

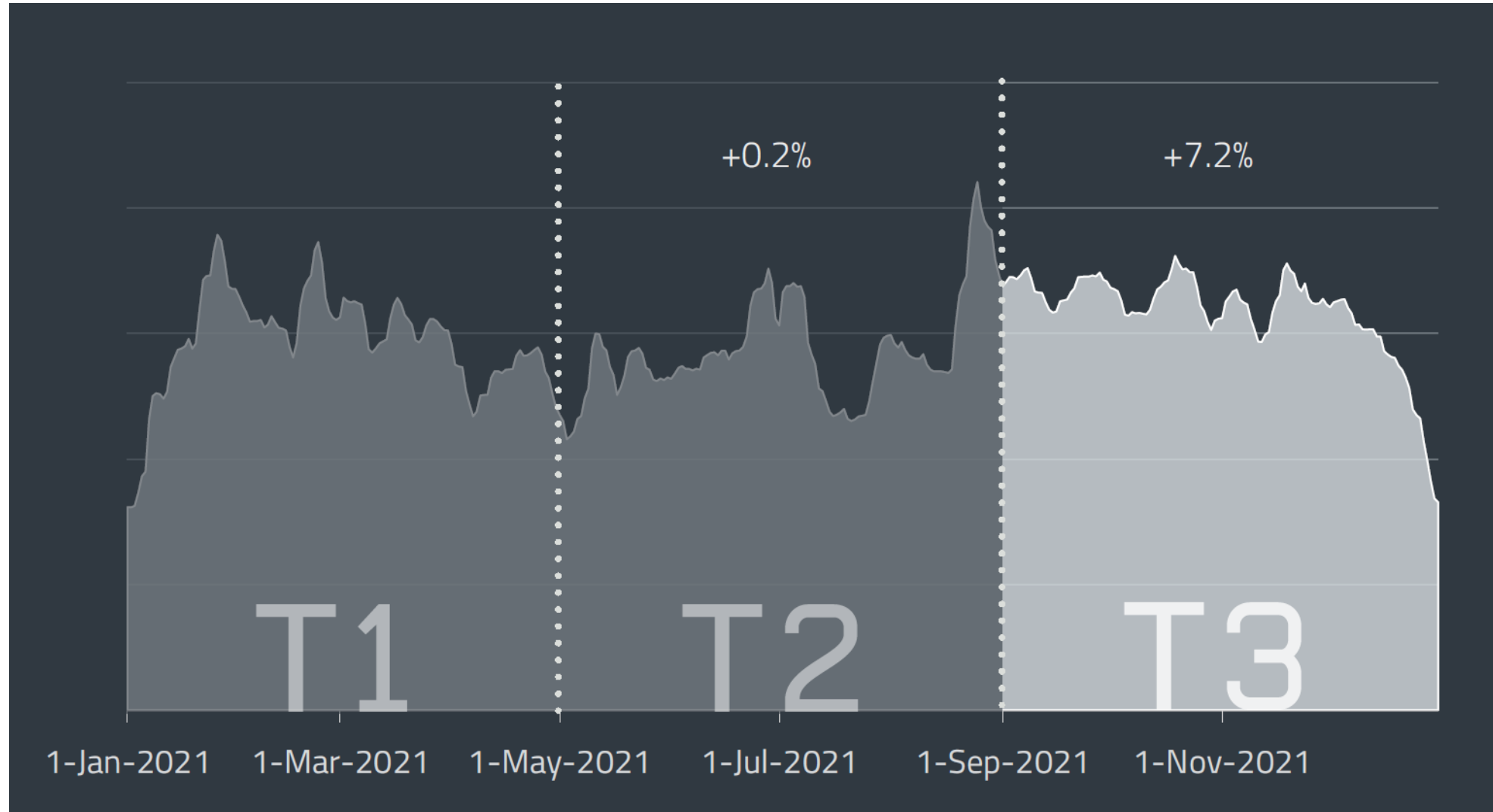
Security Specialist

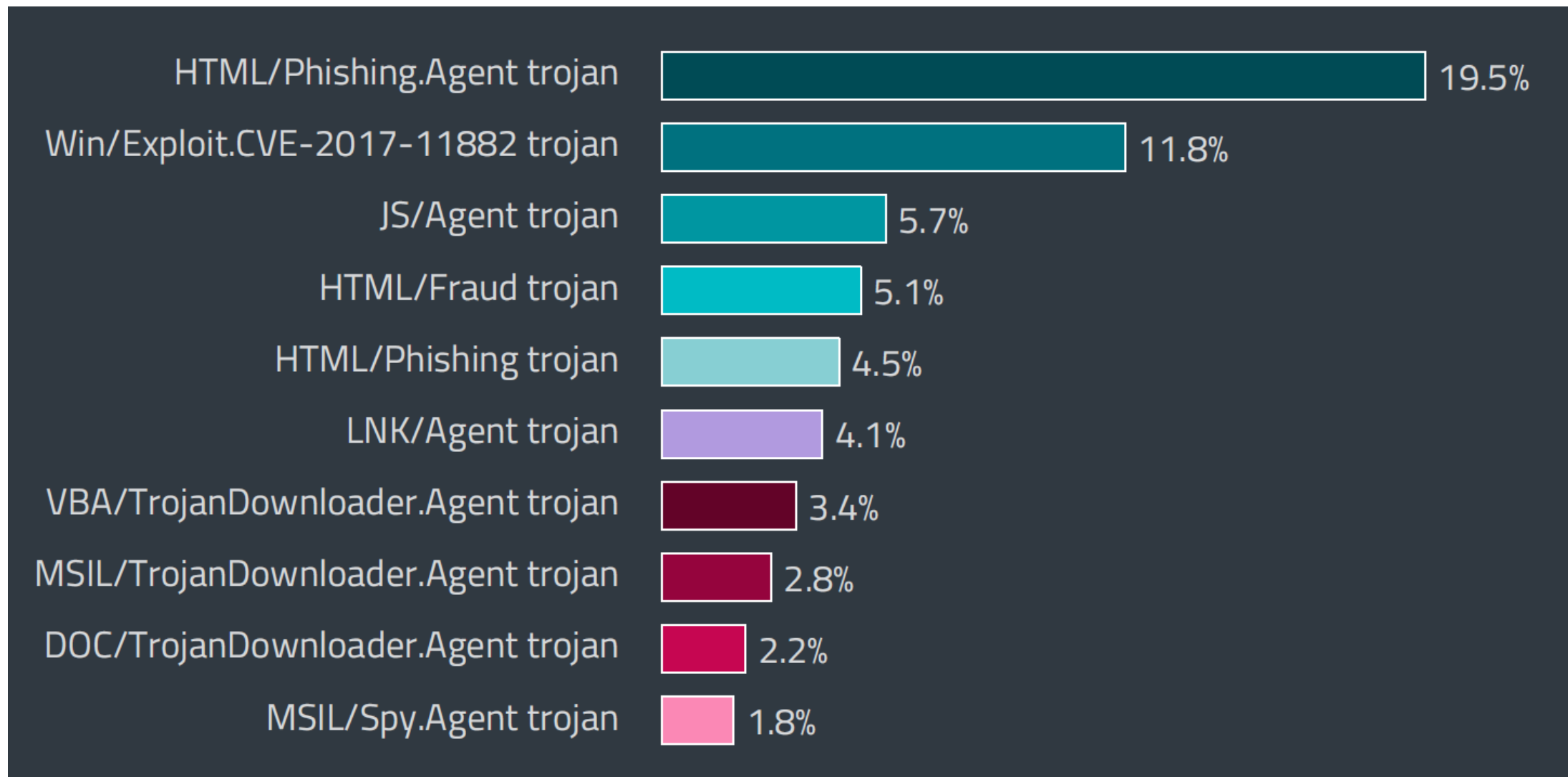
thomas.uhlemann@eset.com

The image features a teal background with a vertical cyan line running down the center. On either side of the line, there is a trail of reflective, metallic spheres that appear to be moving or falling, creating a sense of motion and depth. The spheres are arranged in a curved path, with some appearing larger and more prominent than others.

MALWARE

Anzahl Malware-Erkennungen in 2021

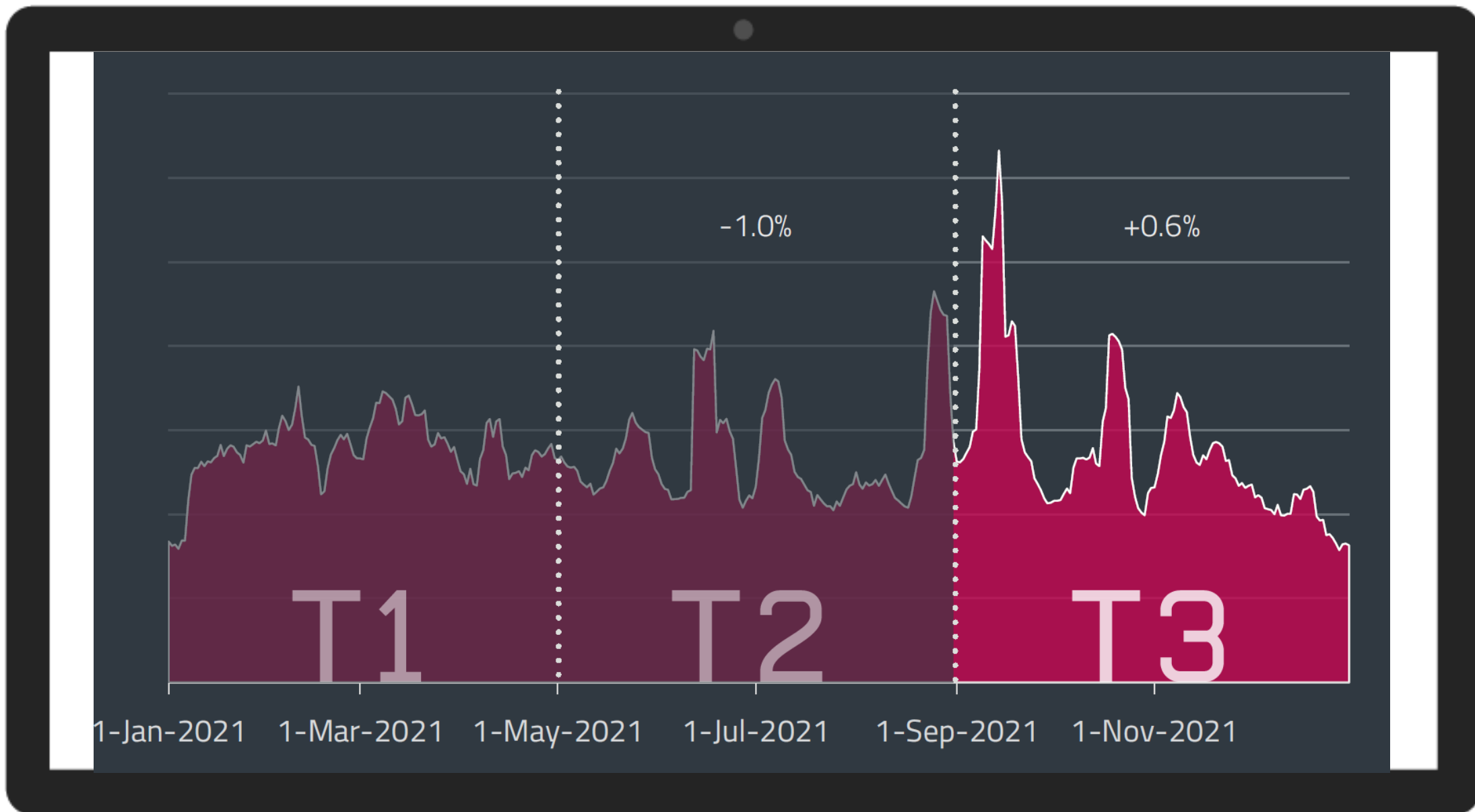




Top 10 Malware-Erkennungen in T3 2021 (Anteil in % an allen Erkennungen)

The image features a teal background with a vertical cyan line running through the center. A curved path of reflective spheres, resembling a DNA helix or a molecular structure, is visible on both the top and bottom halves of the image. The spheres are dark with bright highlights, giving them a three-dimensional appearance.

RANSOMWARE



Ransomware Erkennungstrend in T1 2021 & T2 2021, 7-Tage-Mittel

CYBERSECURITY

Reply-Chain-Angriffe

Ikea k

Mo 29.11.2021 - 14:36
von Pascal Wojnarski

Ikea kämpft gegen
Mail-Kommunikati
Antwortketten get



Cyberattacke auf IT-Dienstleister der Landeshauptstadt Schwerin

© 22. November 2021



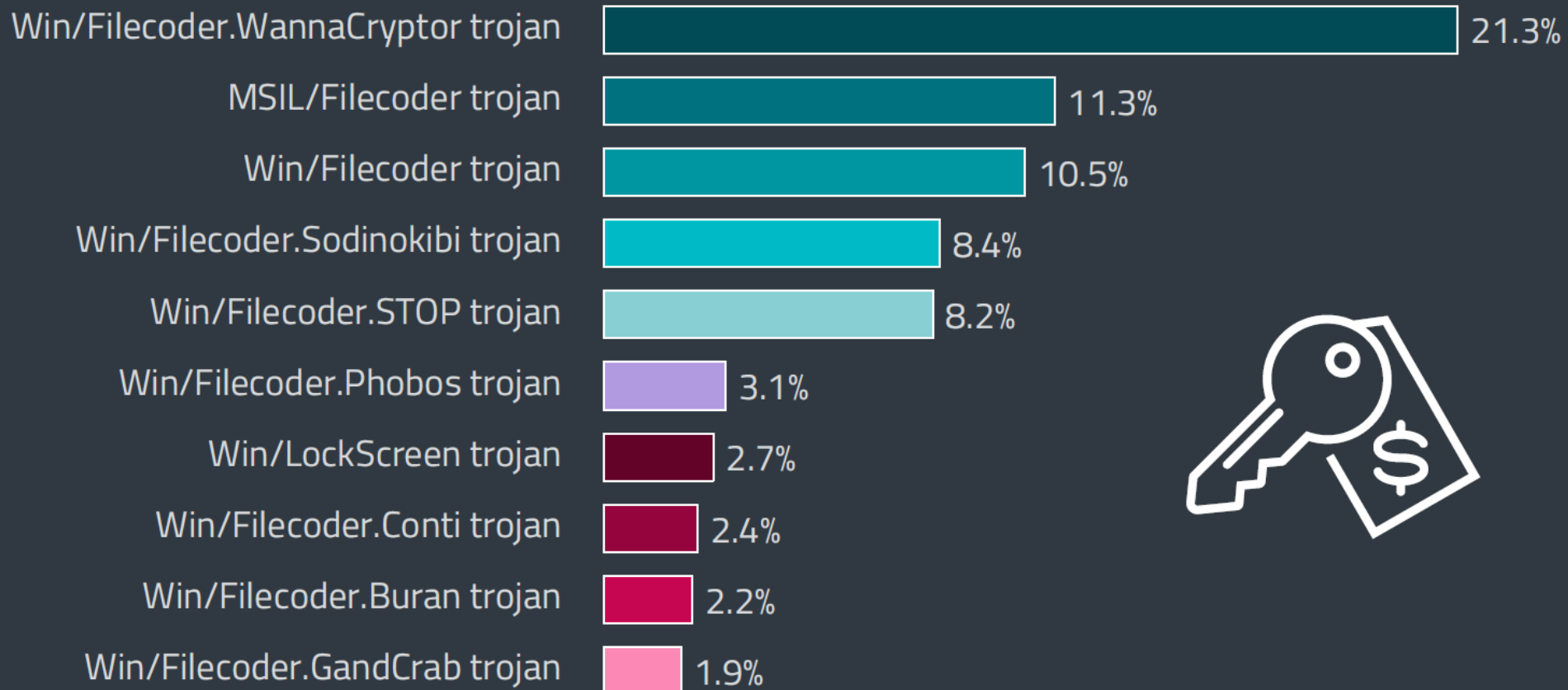
Update Mo, 22.11.2021, 12:34 Uhr

verübt.
hren und vom
l arbeitet mit IT-

Services und

se.

den letzten
ien, dass die
e der



Top 10 Ransomware-Familien in T2 2021 (Anteil in % aller Ransomware Erkennungen)

Beachtenswerte Newcomer

Lorenz

Diavol

DarkRadiation

Beachtenswertes Rebranding

DarkSide -> BlackMatter

DoppelPaymer -> Grief

SynAck -> El_Cometa

FOR ME



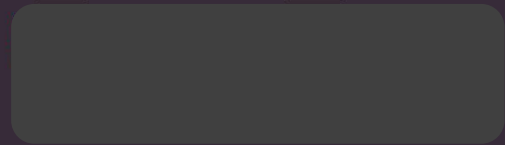
60%



The GDPR at Article 33 requires that, in the event of a personal data breach, data controllers should notify the appropriate supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it.

Grievances in progress: 0

Complete Grievances: 0



2018 VARONIS GLOBAL DATA RISK REPORT

Grief came to:



[Redacted]

Dodge Ram Dealership

URL

[Redacted]

READ MORE

Views: 6669 | Published: 2021-07-08 19:22:50 | Updated: 2021-07-28 20:38:51



[Redacted] County, Alabama

URL

[Redacted]

READ MORE

Views: 35187 | Published: 2021-05-27 20:41:14 | Updated: 2021-07-28 20:10:57

Data co

- Bankin
- Details
- Contra
- Interna
- Custom
- Custom

PU

Beachtenswerte Enden/Verhaftungen

Avaddon

(Ende + Entschlüsselungsskeys)

Ragnarok

(Ende + Entschlüsselungsskeys)

CIOp

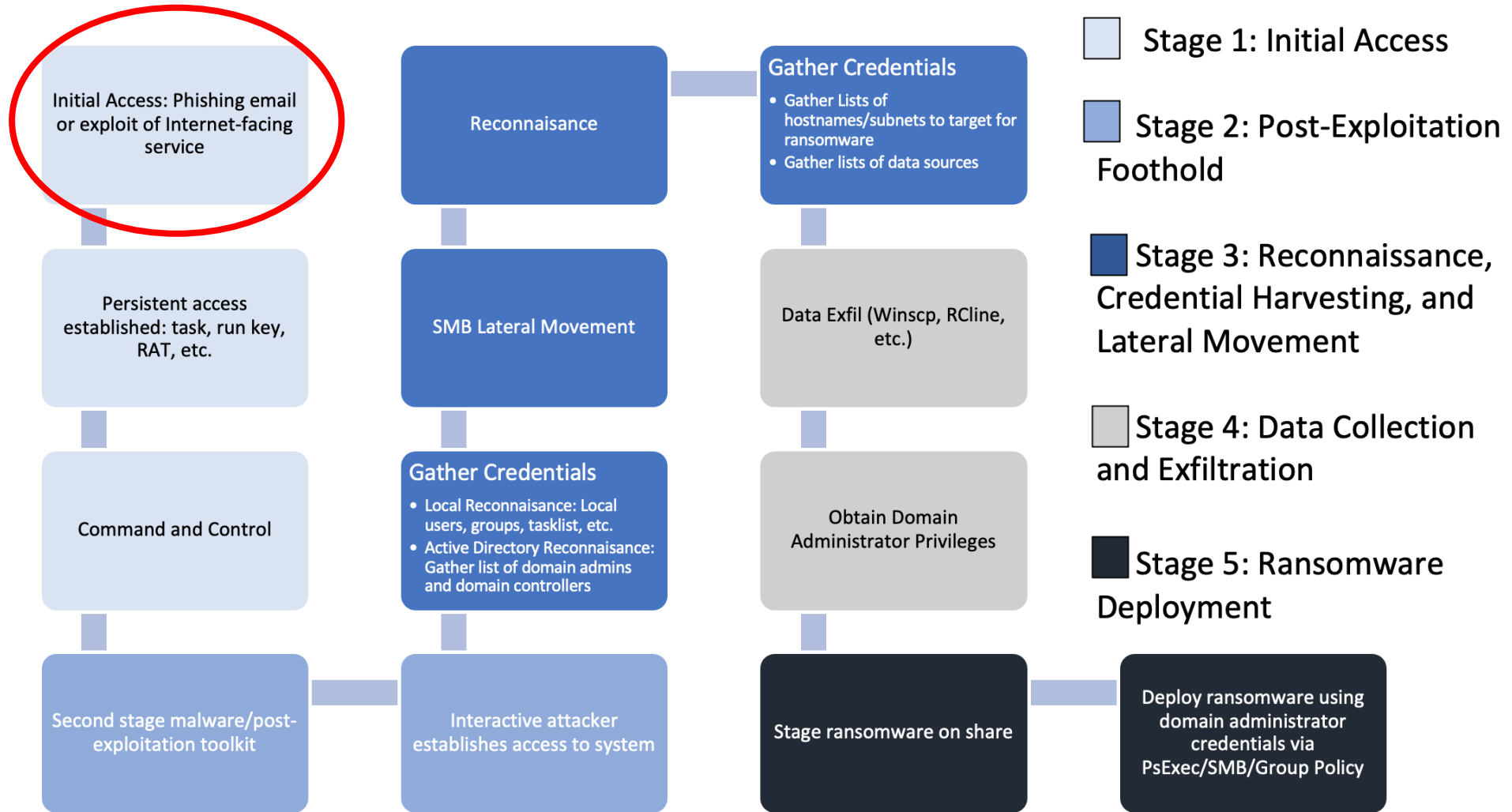
(Verhaftung)

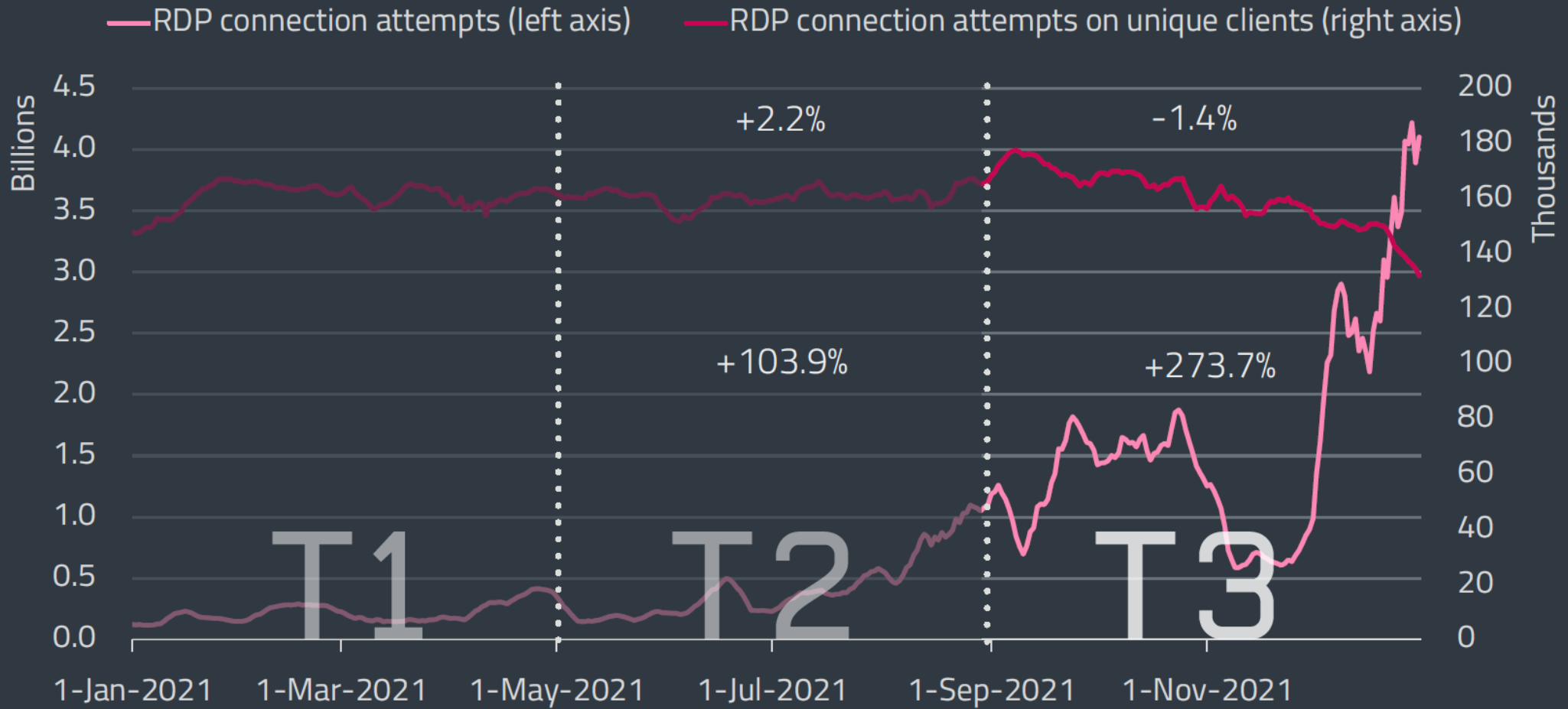
Qlocker

(Ende)

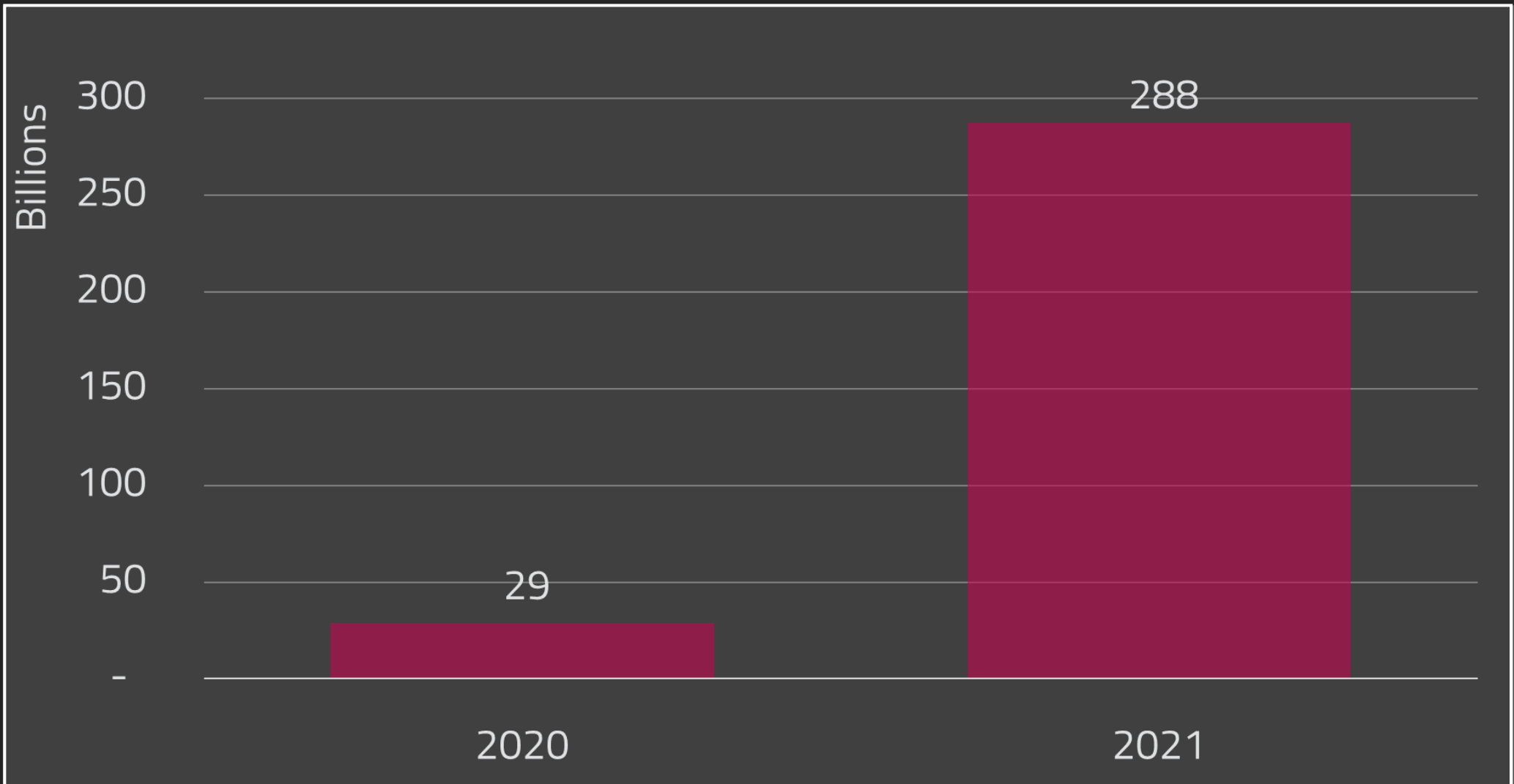
Babuk

(Ende + veröffentlichter Quellcode)

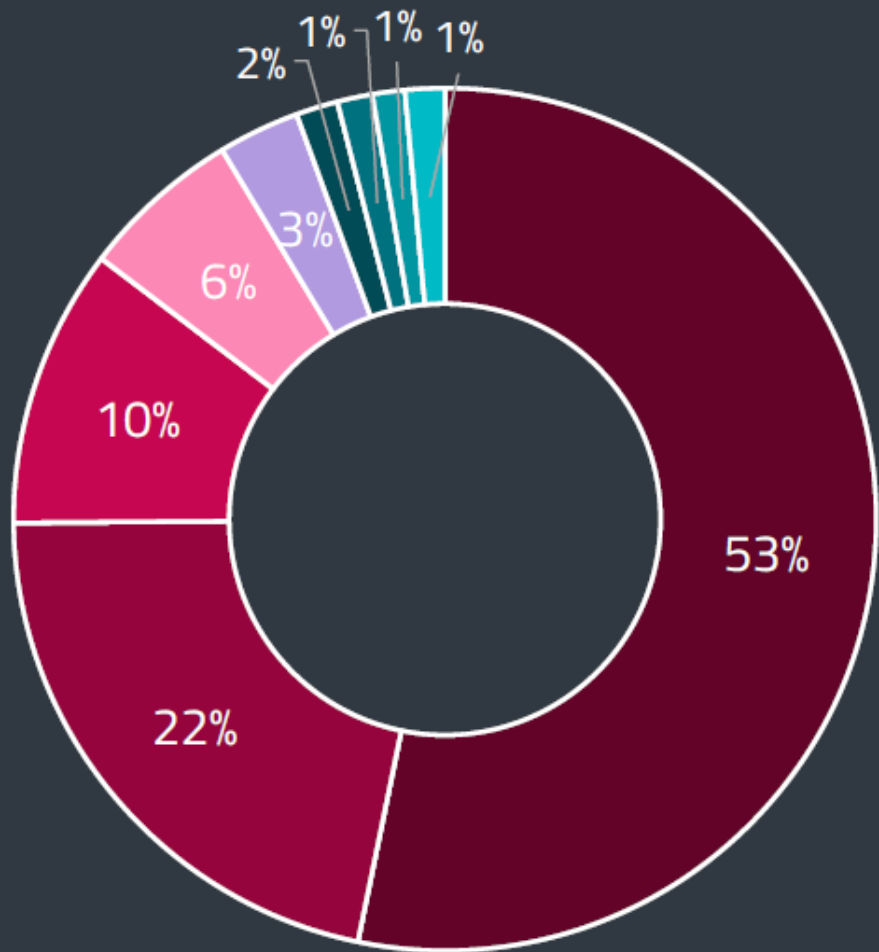




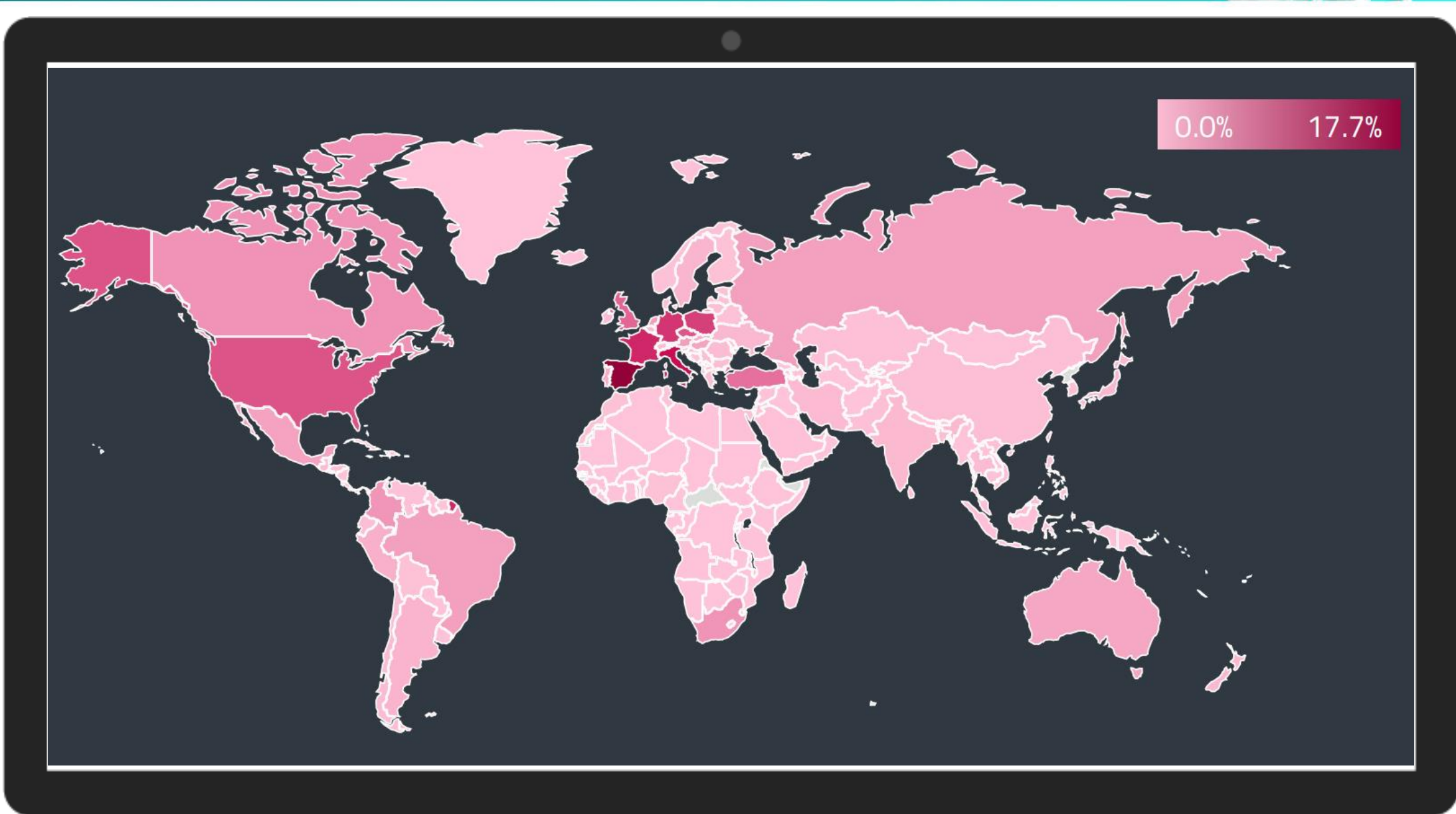
Trends RDP Verbindungsversuche gesamt und auf einzelne Clients in 2021, 7-Tage-Mittel



Trends versuchter RDP-Brute-Force-Attacken YoY



- Password guessing
- MS Exchange Exploit.CVE-2021-26855
- SMB.DoublePulsar scan
- Apache Struts2 CVE-2017-5638
- MS IIS CVE-2015-1635
- Pulse Secure CVE-2019-11510
- MS SMB1 EternalBlue
- MS SMB3 CVE-2020-0796
- Other (including BlueKeep)



Hauptsächlich per RDP attackierte Länder in 2021

The image features a teal background with a vertical cyan line running through the center. A curved path of reflective, metallic spheres starts from the top left and curves towards the bottom right, crossing the cyan line. The spheres are arranged in a sequence that suggests a path or a trajectory.

WAS TUN?

(Auswahl)

- ZERO TRUST – nur so viele Nutzerrechte wie absolut nötig
- IT-Security als Geschäftsgrundlage verstehen
- Klare Pläne:
 - Updates & Patches möglichst zeitnah
 - Dezentrale, inkrementelle Backups – regelmäßig testen
 - Notfallplan ständig aktualisiert und getestet

- 2FA überall wo es möglich ist
- Passwortmanager nutzen mit Masterpassphrase
- Gruppenrichtlinien verhindern das Ausführen von Programmen aus *C:\Users\All Users*
- Mitarbeiter*innen regelmäßig (nach-)schulen
- ...

Neuigkeiten, Analysen und Tipps der
ESET Sicherheitsexperten

CYBER-SICHERHEITSLAGE UKRAINE
ESET Research-Webinar: Cyber-Schlachtfeld Ukraine
ESET Research 15 Mar 2022 - 10:41AM

CYBER-SICHERHEITSLAGE UKRAINE
Betrüger missbrauchen Krieg in der Ukraine

CYBER-SICHERHEITSLAGE UKRAINE
HermeticWiper: Datenlöschende Malware in der Ukraine

Hier sehen Sie unsere neusten Artikel Neuste zuerst ▼

Online-Umfrage



Wie steht es um die IT-Sicherheit im Gesundheitswesen?

Keine Branche ist gegen Cyber-Bedrohungen immun, doch im Gesundheitswesen ist die Gefahr besonders groß.

Phil Muncaster 18 Mar 2022 - 01:32PM

Folgen Sie uns



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.

Editor 15 Mar 2022 - 10:56AM

Newsletter-Anmeldung

E-Mail... Eintragen

Kategorien



Fragen?

Ich könnte Antworten für Sie haben! ;)



Thomas Uhlemann

Security Specialist

thomas.uhlemann@eset.com