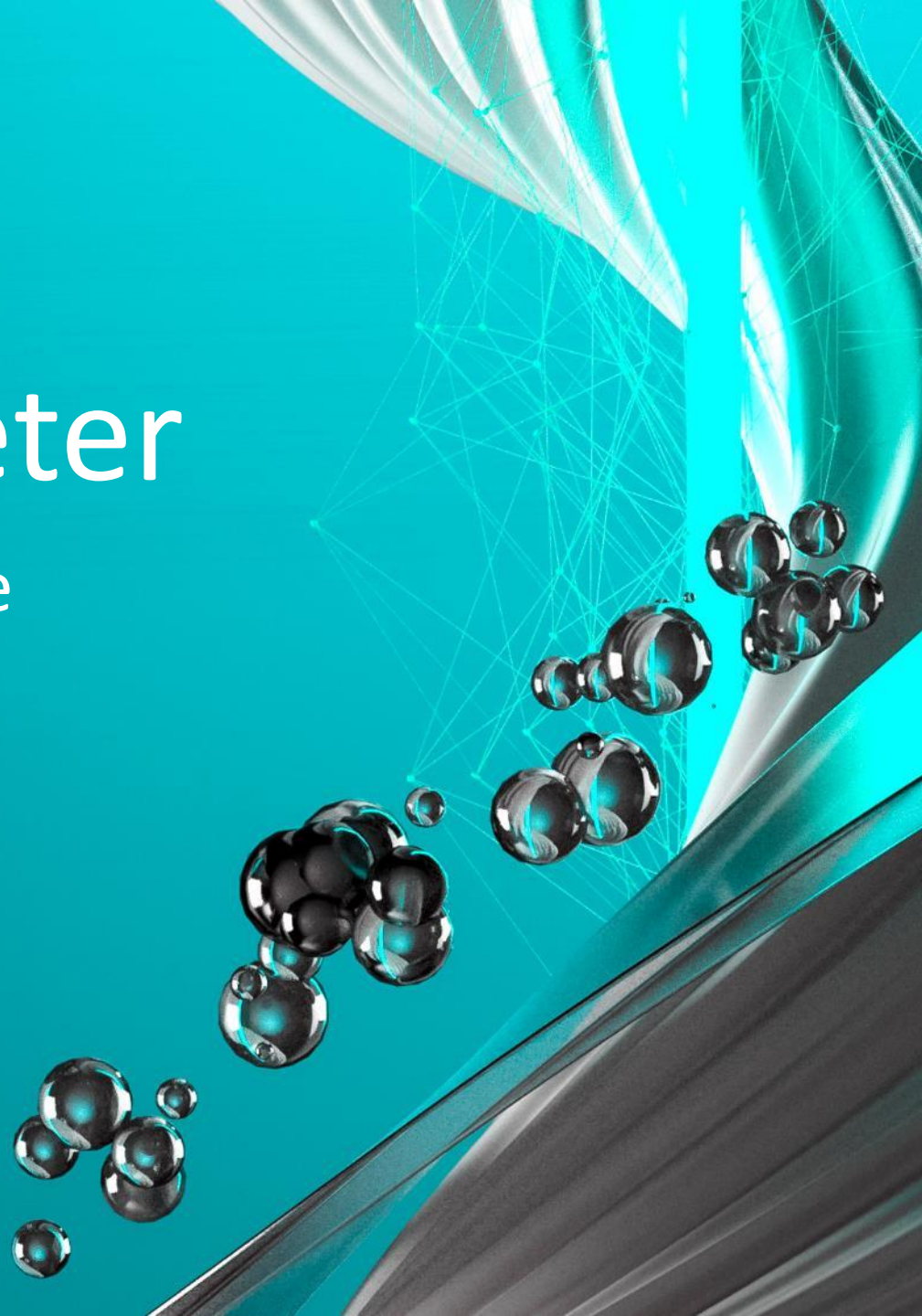
ESET Security Barometer

Aktuelle Bedrohungen und Hintergründe

Thomas Uhlemann
ESET Security Specialist

Thomas.Uhlemann@eset.com

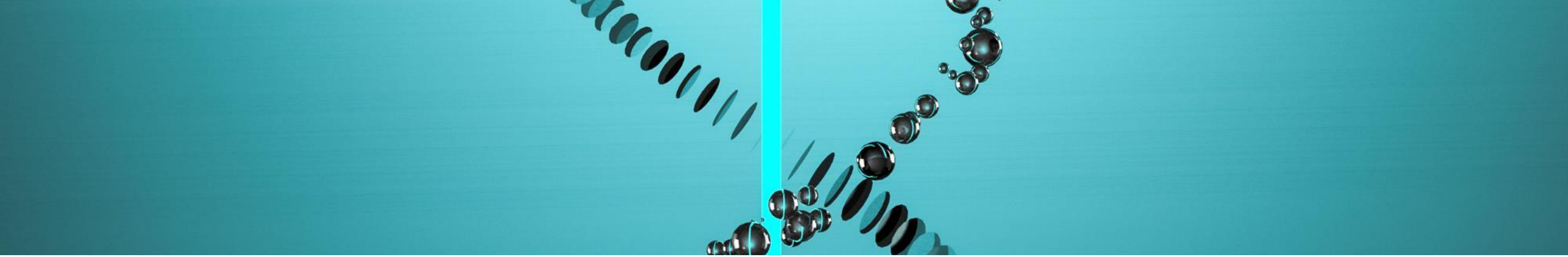


ENJOY SAFER TECHNOLOGY™

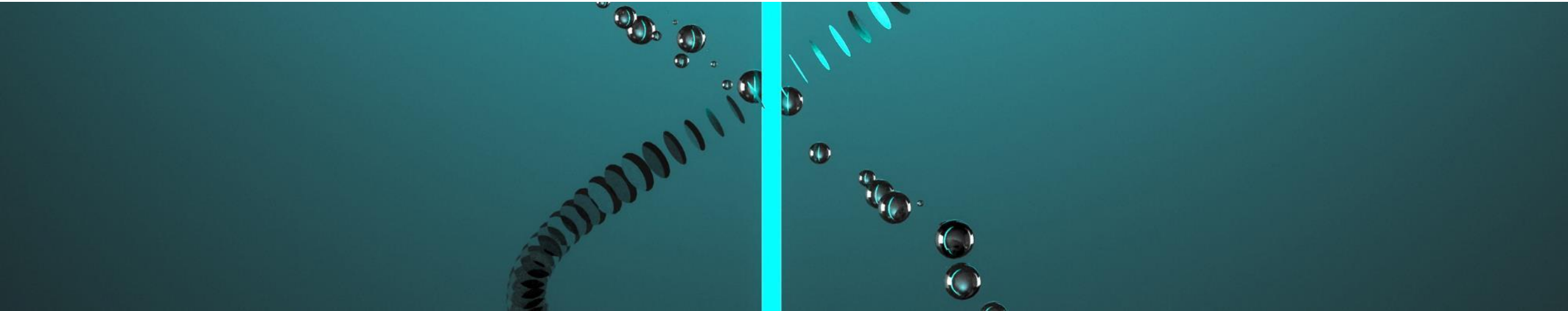
Thomas Uhlemann

Security Specialist

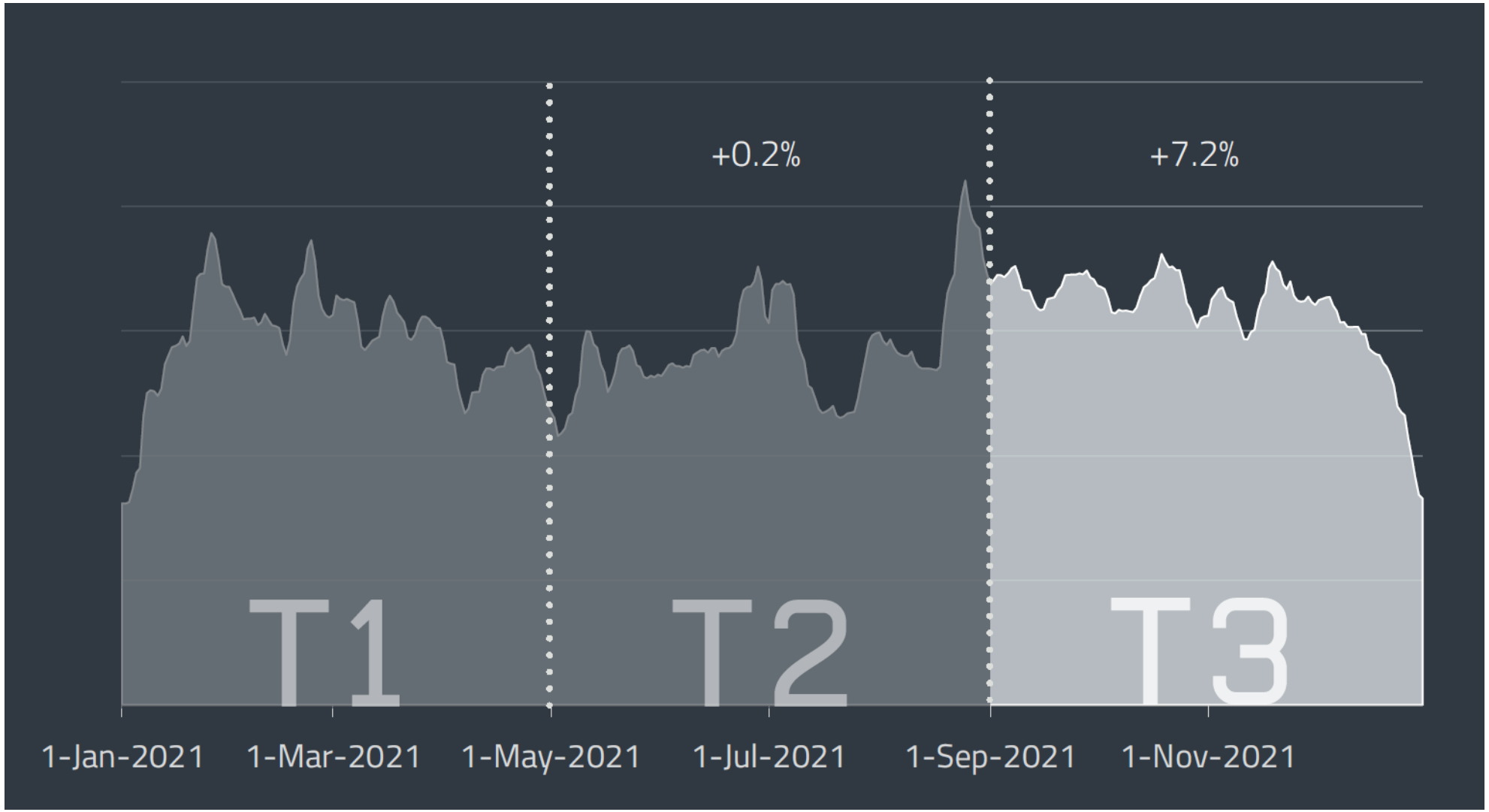
thomas.uhlemann@eset.com



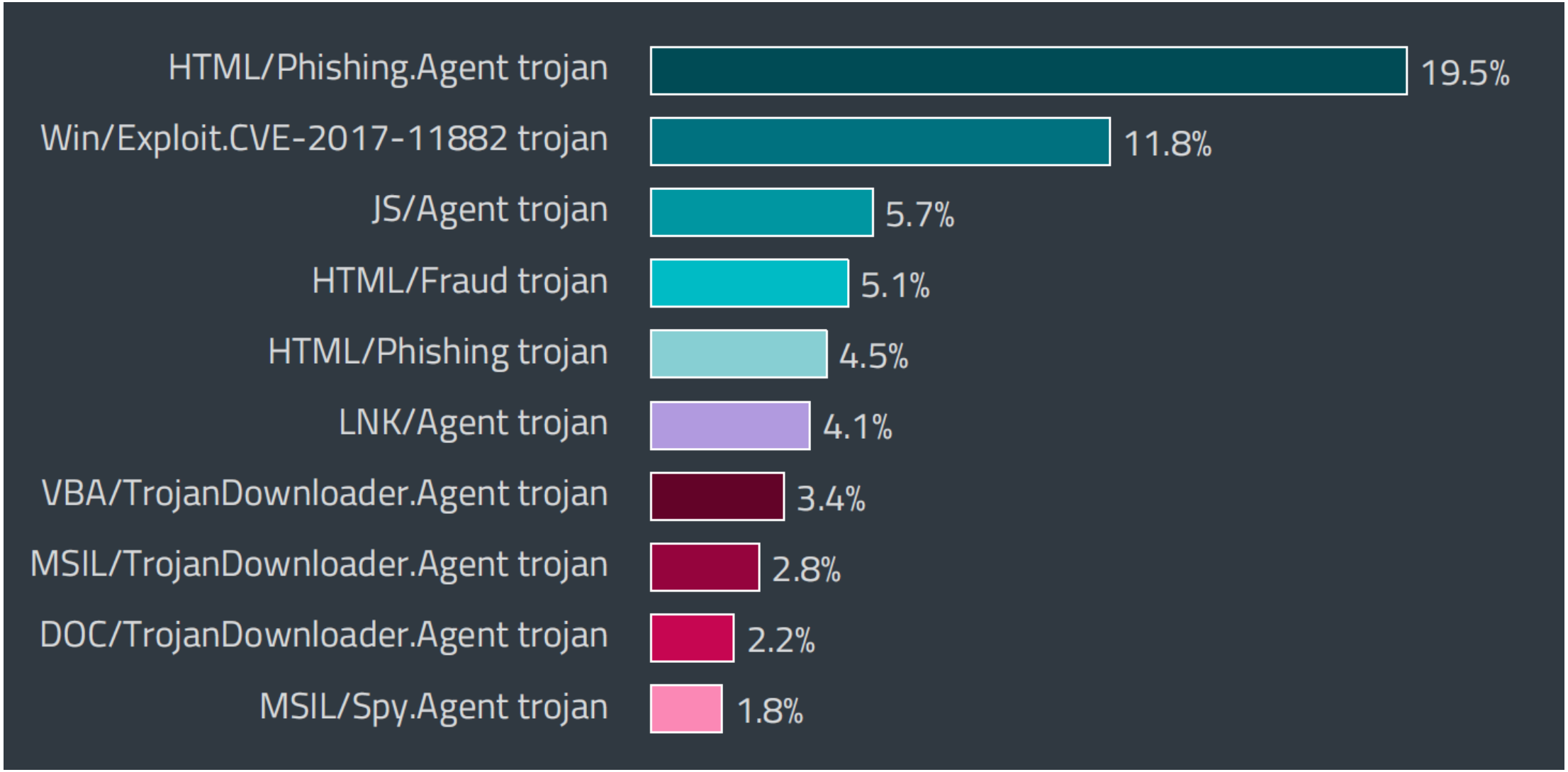
MALWARE



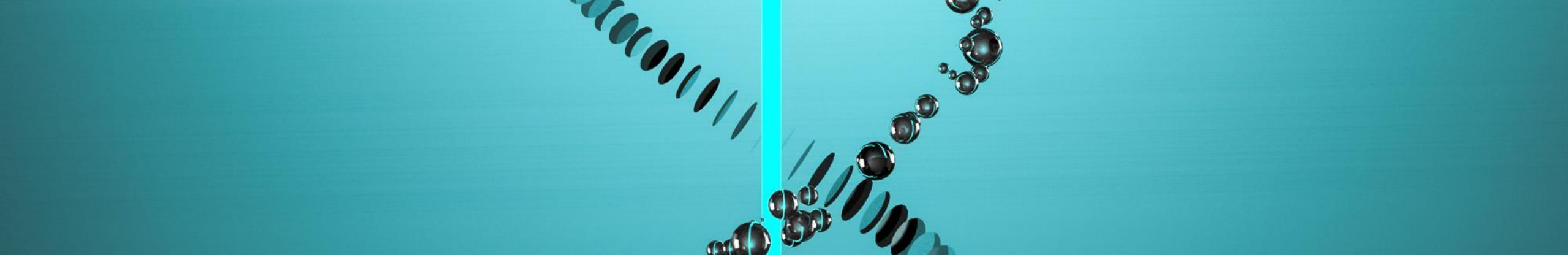
Anzahl Malware-Erkennungen in 2021



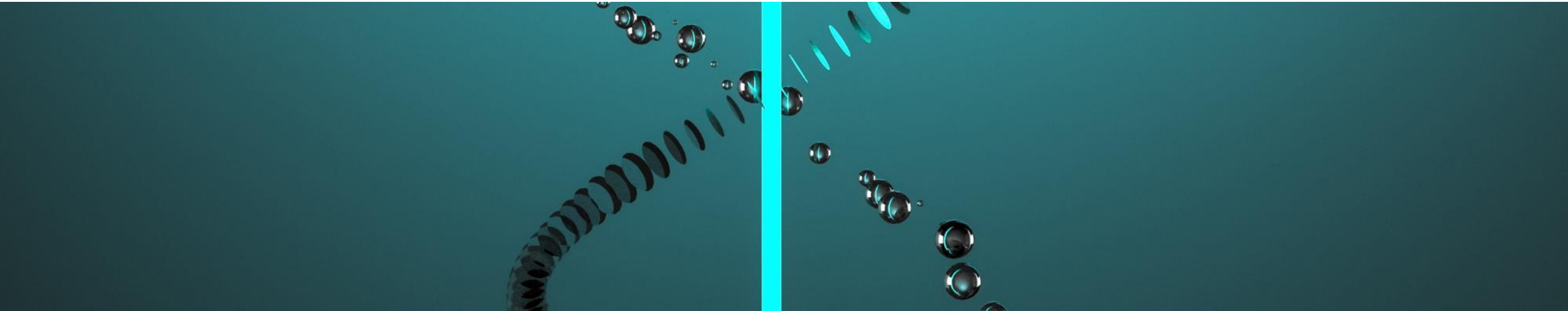
Gesamtzahl erkannter Bedrohungen, Trend in 2021, 7-Tage-Mittel

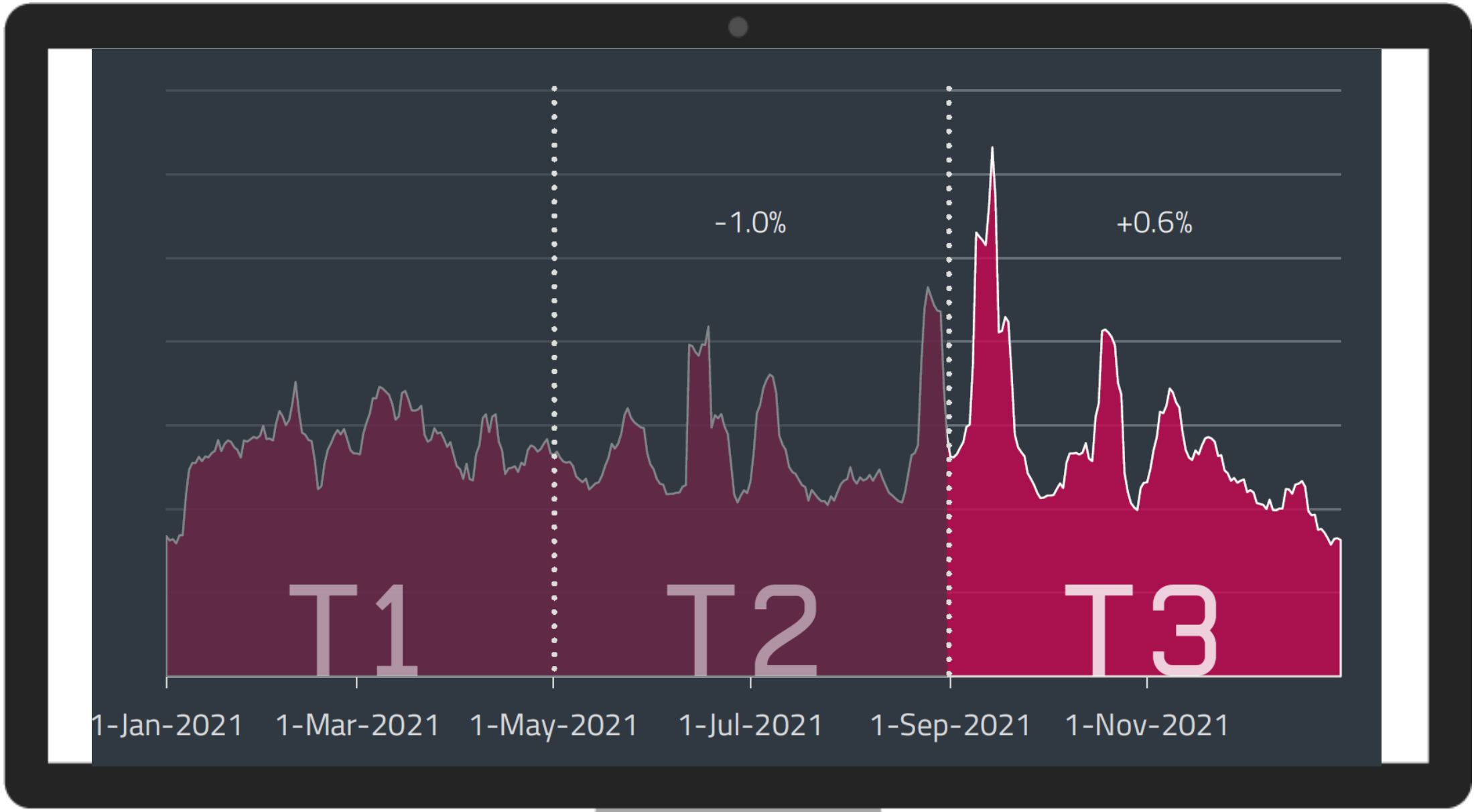


Top 10 Malware-Erkennungen in T3 2021 (Anteil in % an allen Erkennungen)



RANSOMWARE





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

CYBERSECURITY

Reply-Chain-Angriffe

Ikea kär

Mo 29.11.2021 - 14:36
von Pascal Wojnarski

Ikea kämpft gegen
Mail-Kommunikati
Antwortketten geta

Cyberattacke auf IT-Dienstleister der Landeshauptstadt Schwerin

22. November 2021

Update Mo, 22.11.2021, 12:34 Uhr

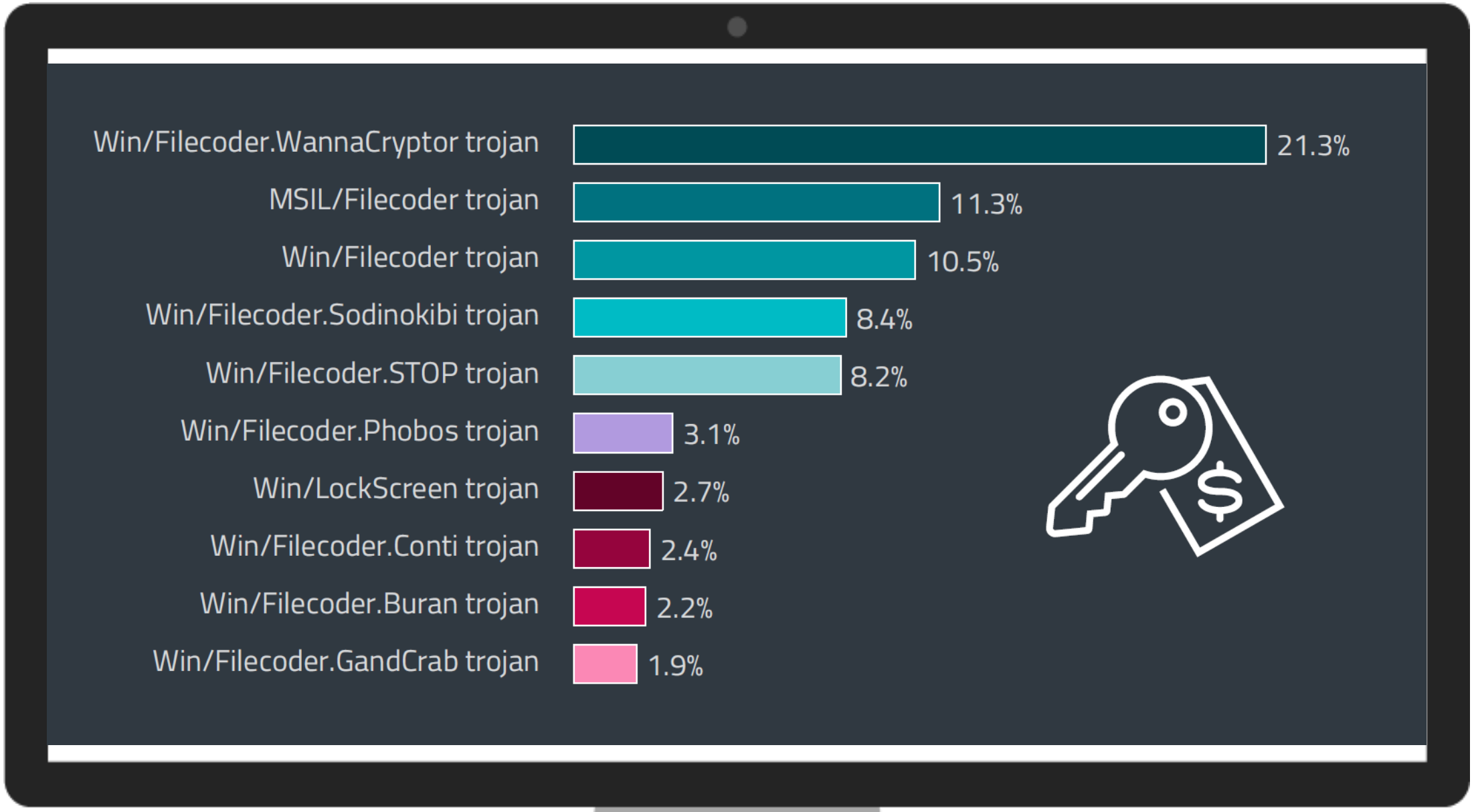
© penofoto/Shutterstock.com

verübt.
hren und vom
l arbeitet mit IT-

Services und

se.

den letzten
len, 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

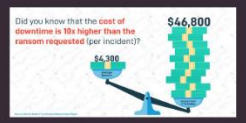
ESET ENJOY SAFER TECHNOLOGY™

Grief list

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.

Griefs in progress:_ Complete Griefs:_



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

Beachtenswerte Enden/Verhaftungen

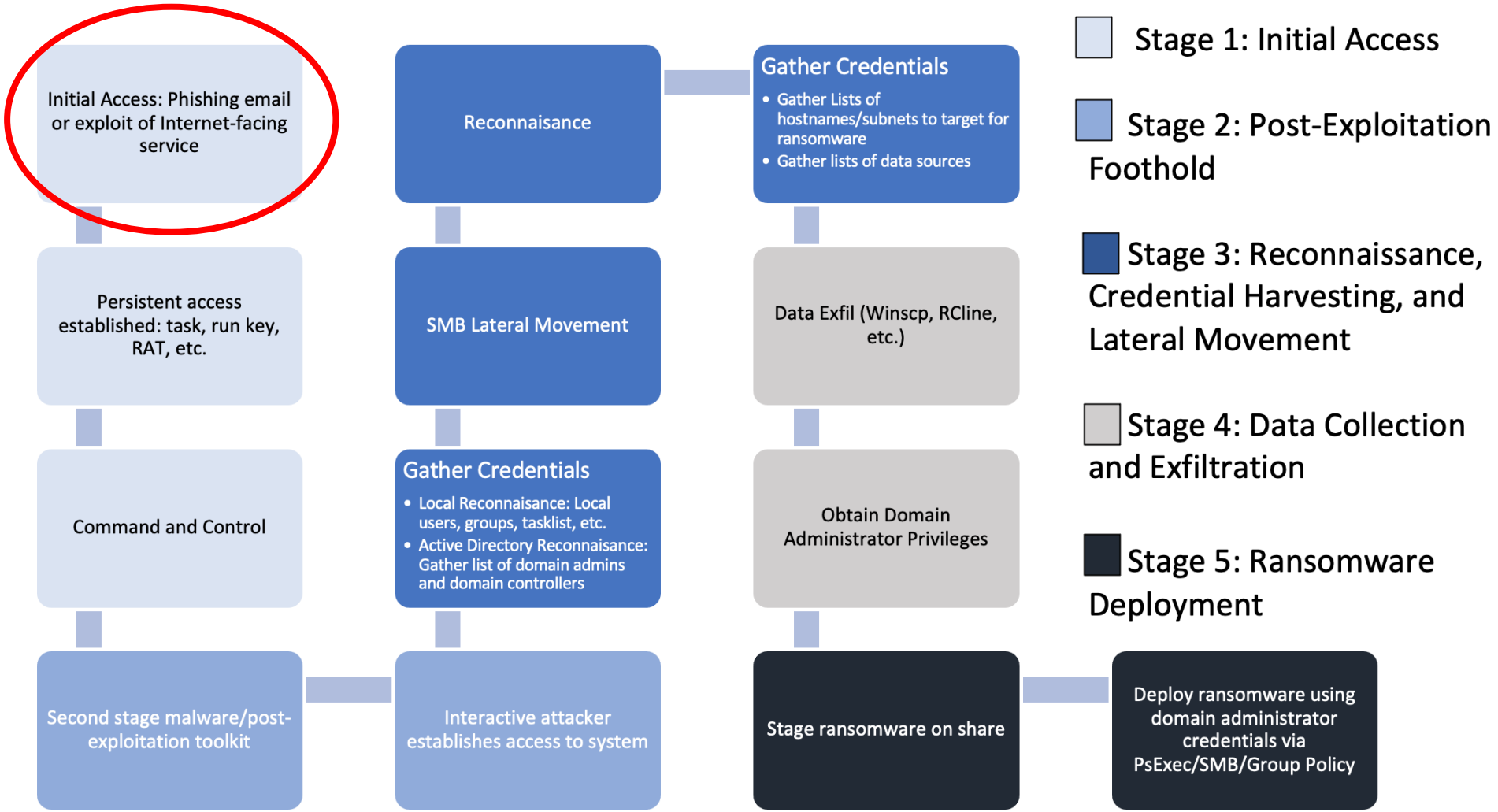
Avaddon
(Ende + Entschlüsselungskeys)

Ragnarok
(Ende + Entschlüsselungskeys)

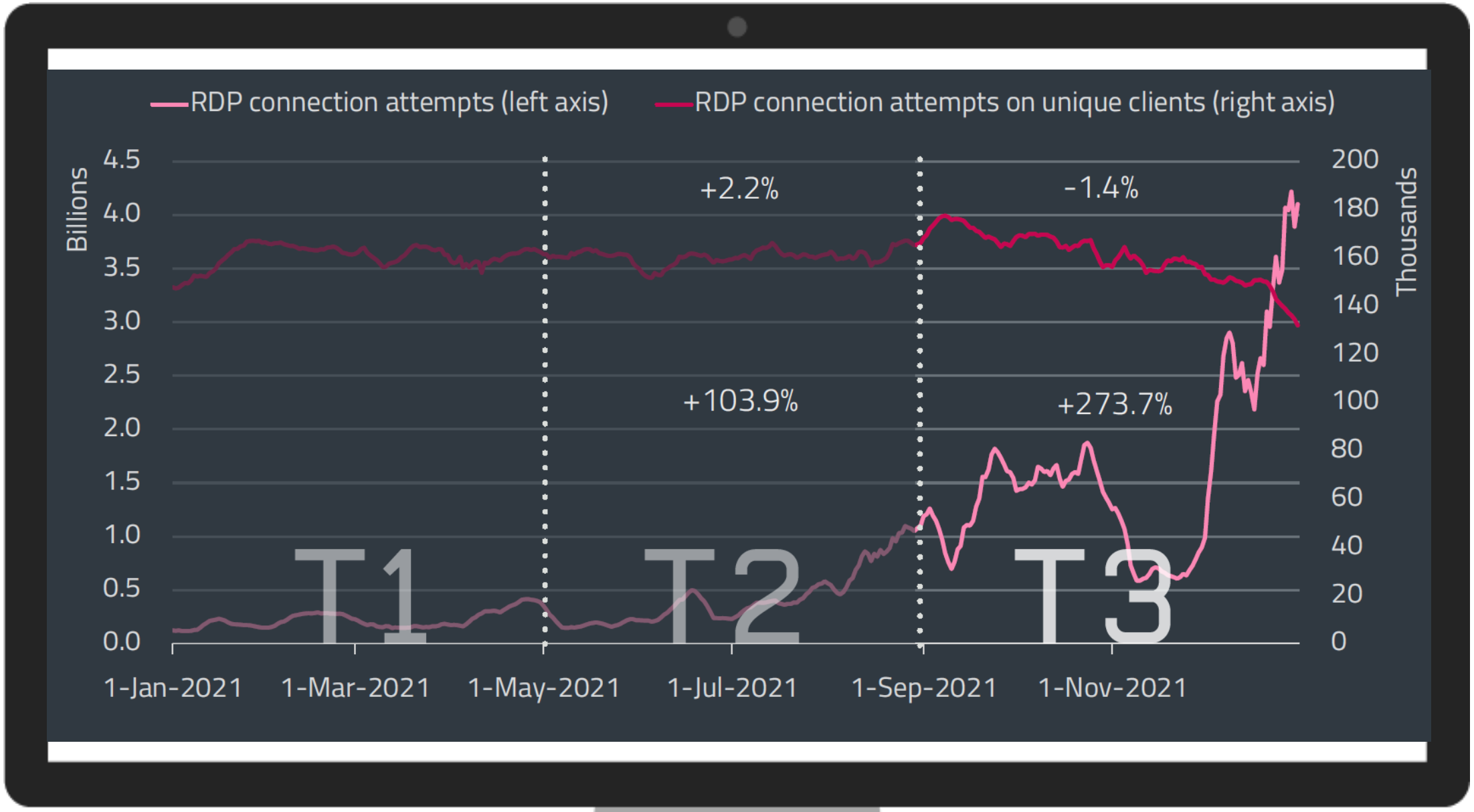
ClOp
(Verhaftung)

Qlocker
(Ende)

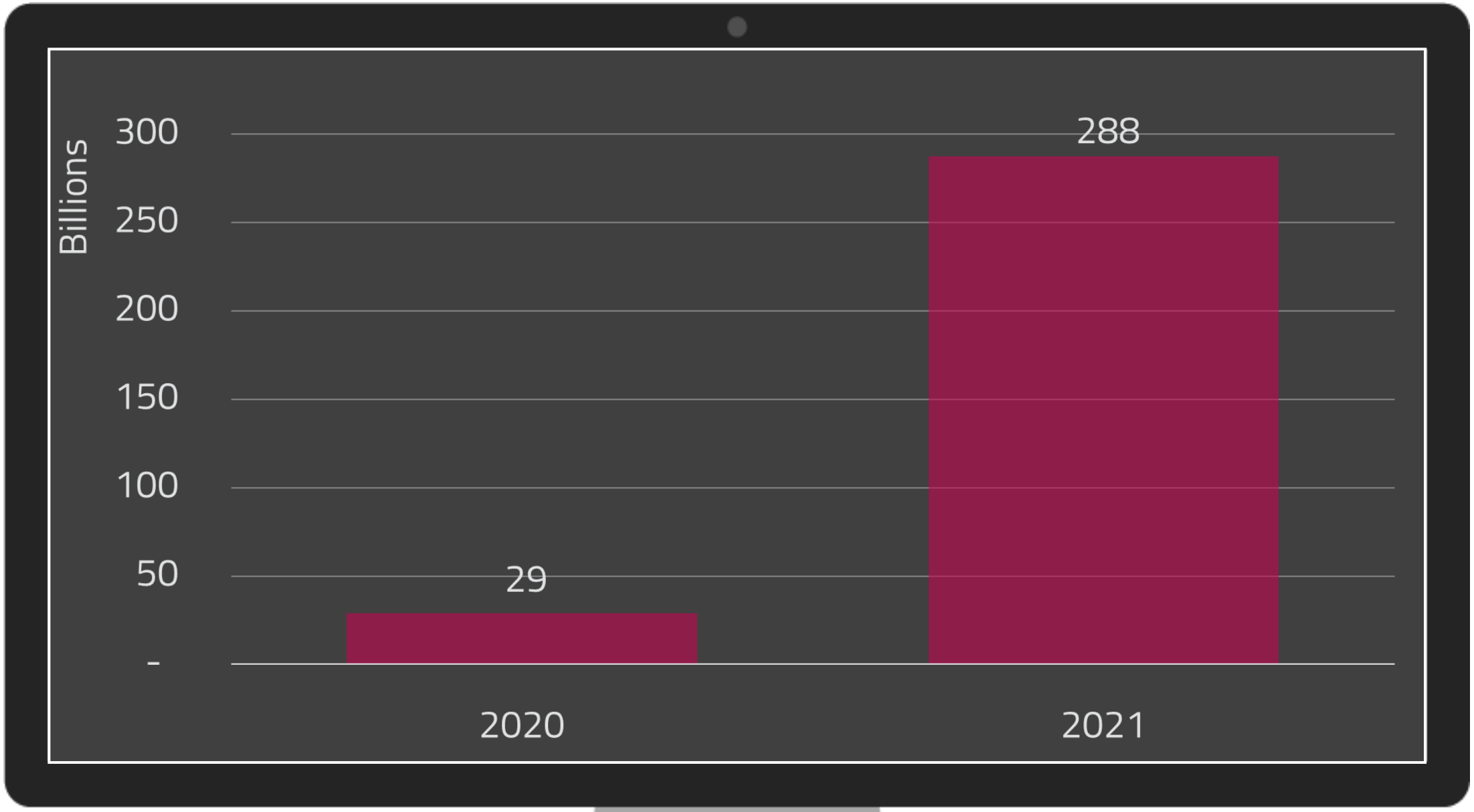
Babuk
(Ende + veröffentlichter Quellcode)



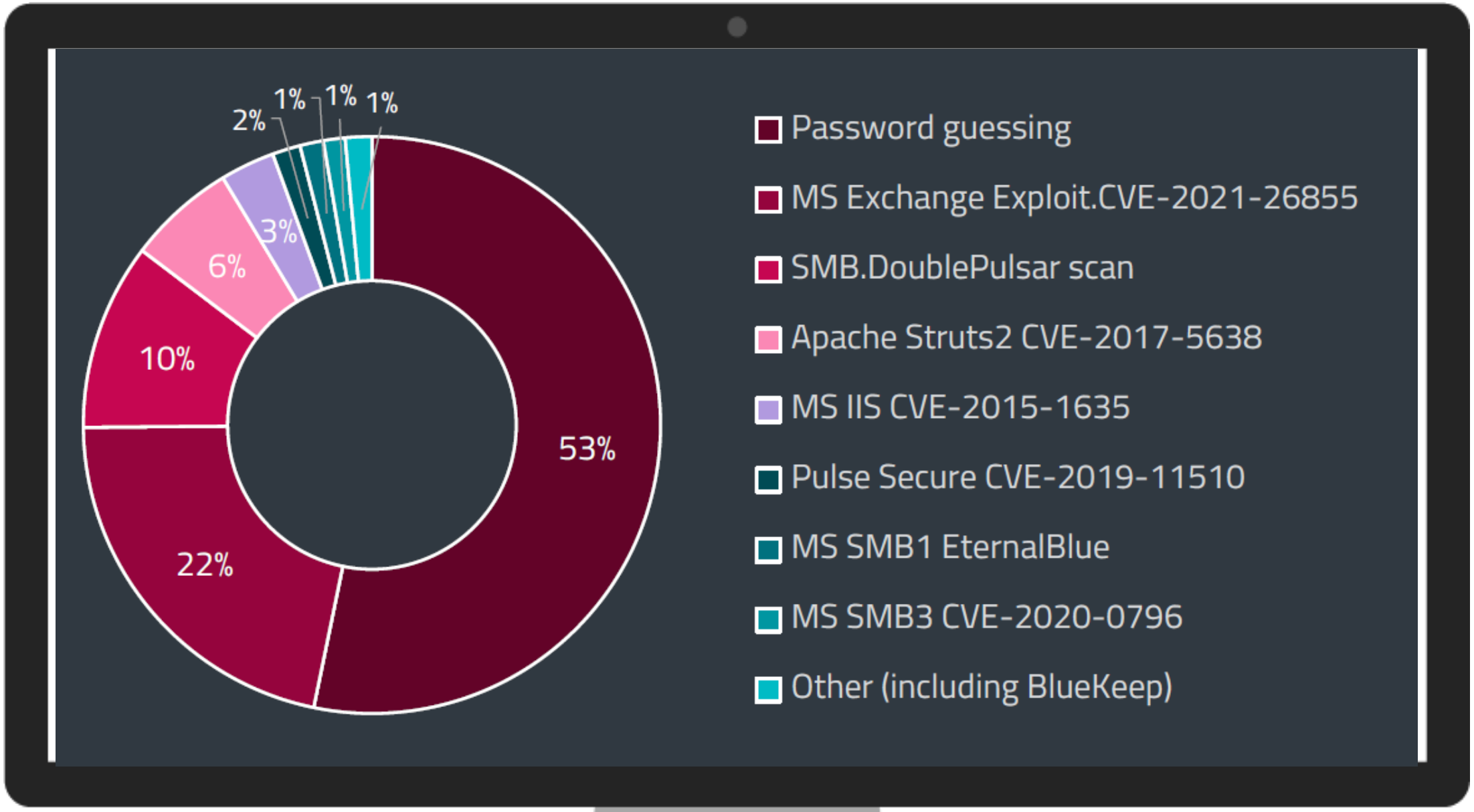
Quelle: IBM X-Force



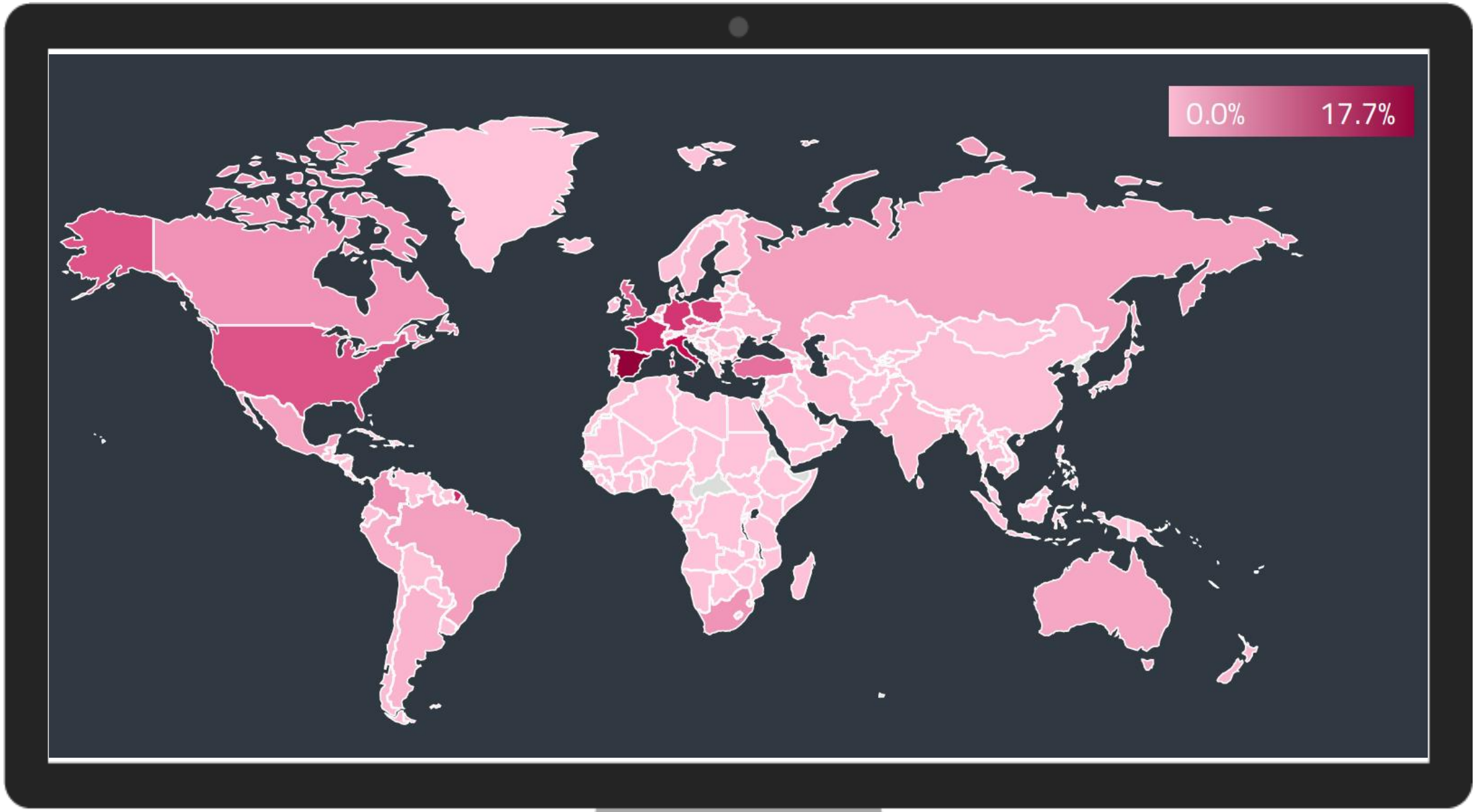
Trends RDP Verbindungsversuche gesamt und auf einzelne Clients in 2021, 7-Tage-Mittel



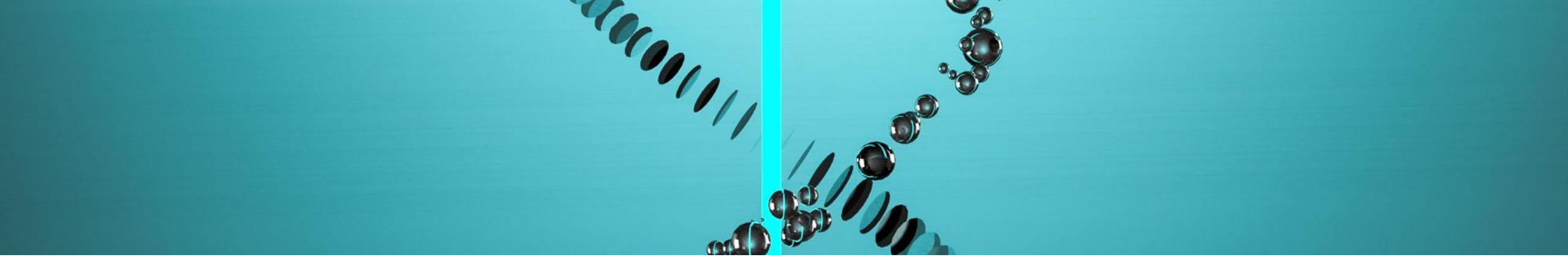
Trends versuchter RDP-Brute-Force-Attacken YoY



Externe Angriffsvektoren für Netzwerke, gemeldet von einzelnen Clients in T2 2021

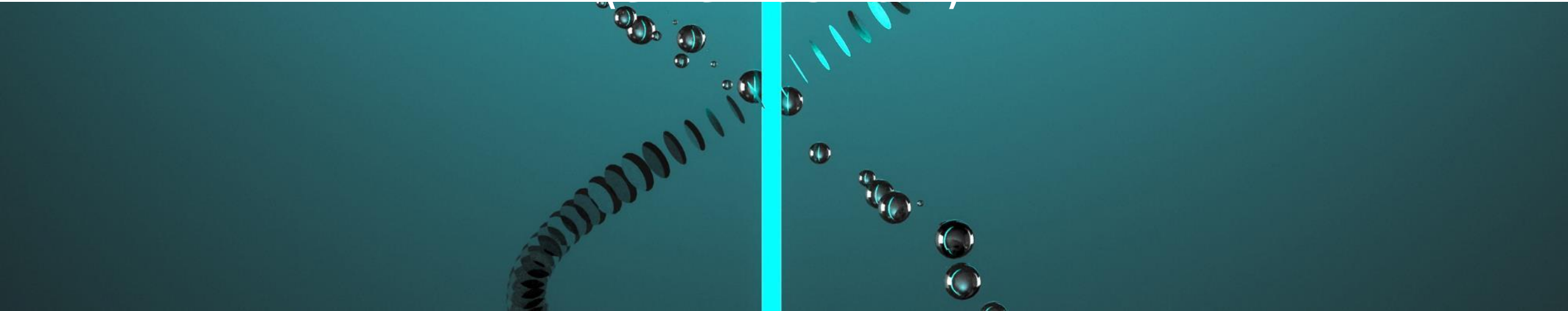


Hauptsächlich per RDP attackierte Länder in 2021



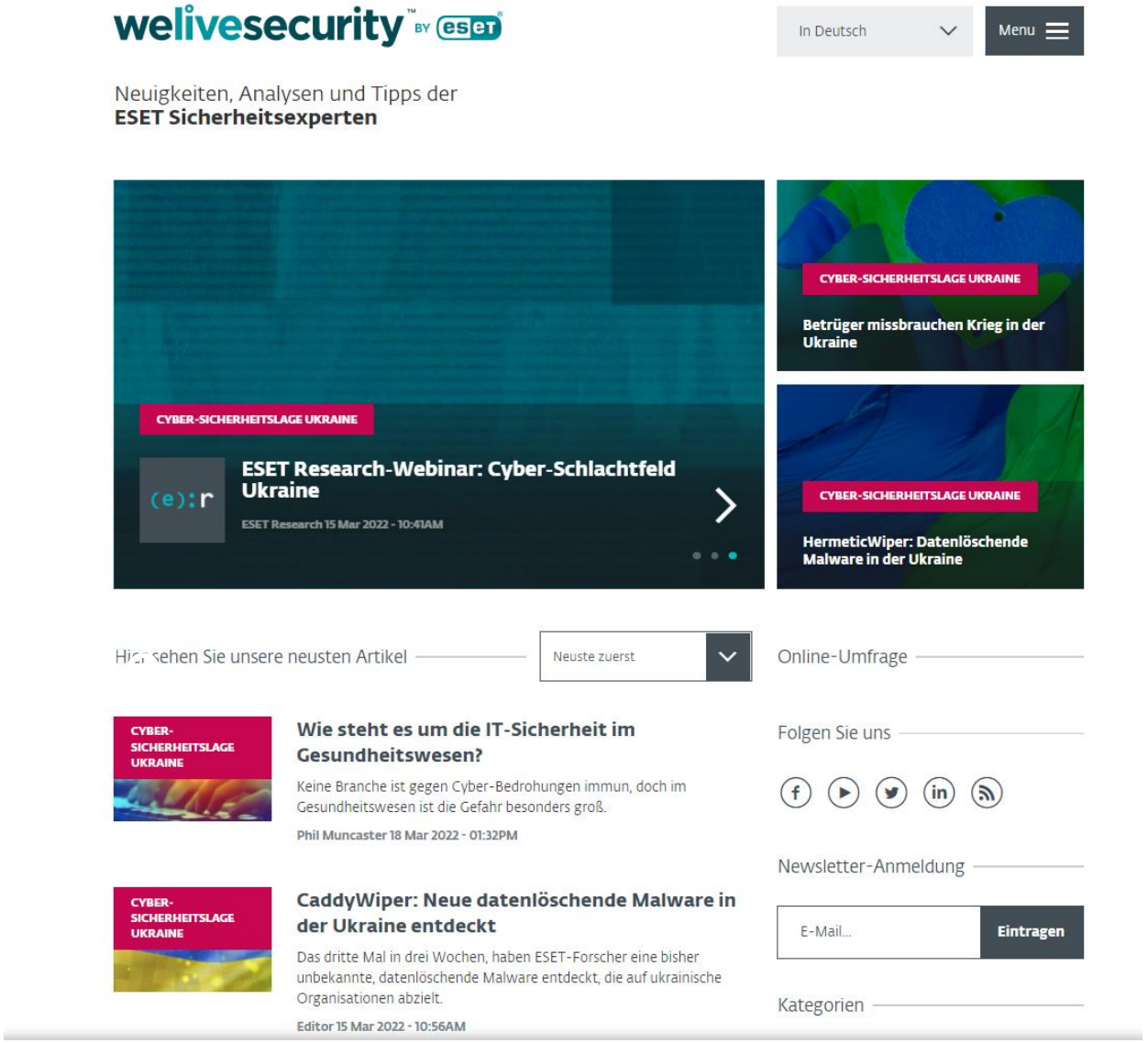
WAS TUN?

(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
- …



www.WeLiveSecurity.de

eset Digital Security
Progress. Protected.

Fragen?

Ich könnte Antworten für Sie haben! ;)

CYBERSECURITY EXPERTS ON YOUR SIDE

Thomas Uhlemann

Security Specialist

thomas.uhlemann@eset.com