What's driving cybersecurity?

Tony Anscombe

Chief Security Evangelist

Tony Anscombe

Chief Security Evangelist

tony.anscombe@eset.com

@TonyAtESET

https://www.linkedin.com/in/tonyanscombe/

Digital Security
Progress. Protected.

More than 90% of successful cyber-attacks start with a phishing email.

SHIELDS UP

https://www.cisa.gov/shields-up

businesswire
A BERKSHIRE HATHAWAY COMPANY

Funding the ransomware industry

A record 71% of organizations were impacted by successful ransomware attacks last year, according to the 2022 CDR, up from 55% in 2017. Of those that were victimized, nearly two-thirds (63%) paid the requested ransom, up from 39% in 2017.

https://www.businesswire.com/news/home/20220404005094/en/Nearly-Two-thirds-of-Ransomware-Victims-Paid-Ransoms-Last-Year-Finds-%E2%80%9C2022-Cyberthreat-Defense-Report%E2%80%9D

Cybercrime: Big Business

2025 - US$10.5 Trillion

2020 - US$6 Trillion

2018 - US$1.5 Trillion

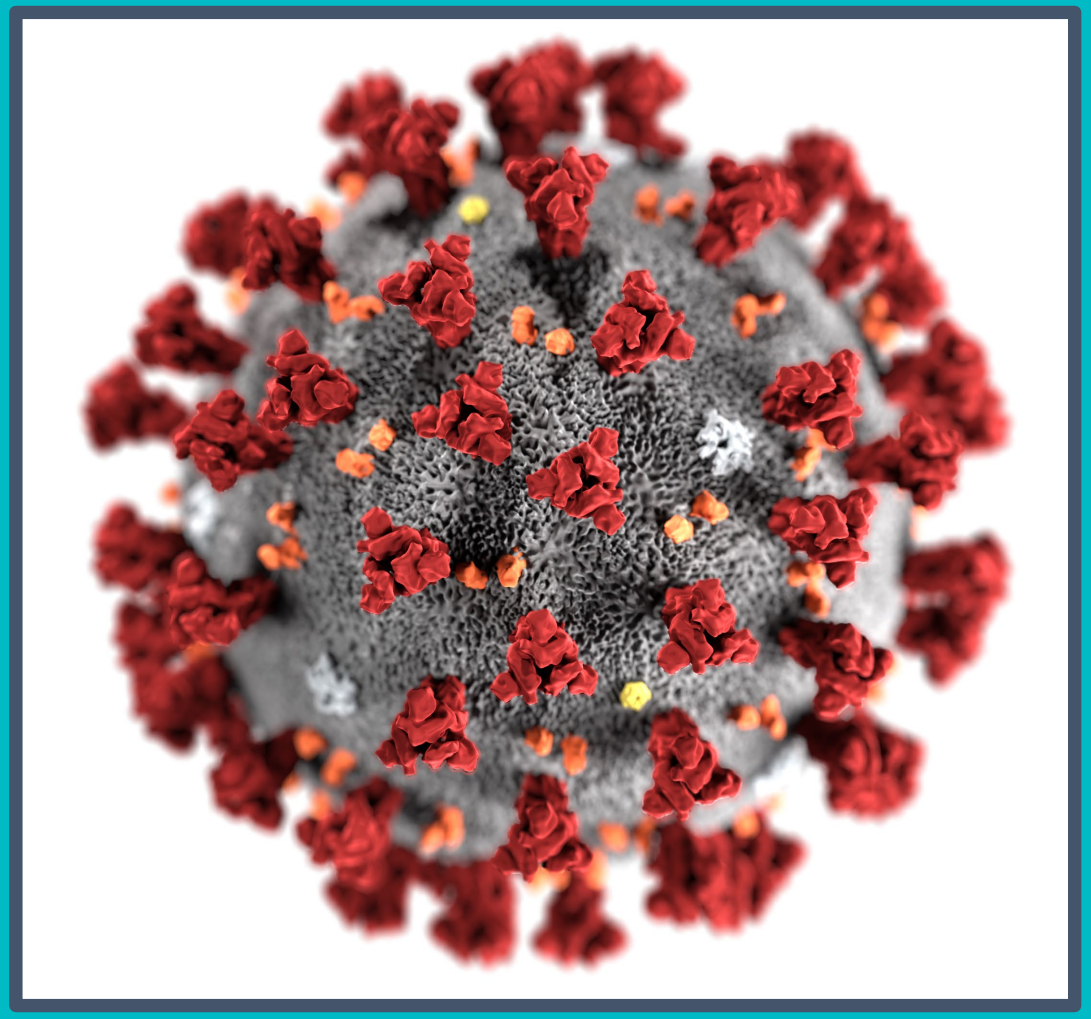
70% of SMEs say investment in IT security has not kept pace with the changes to operational models

"I launch cyberattacks because that's where the money is."

"I launch cyberattacks because that's my job."

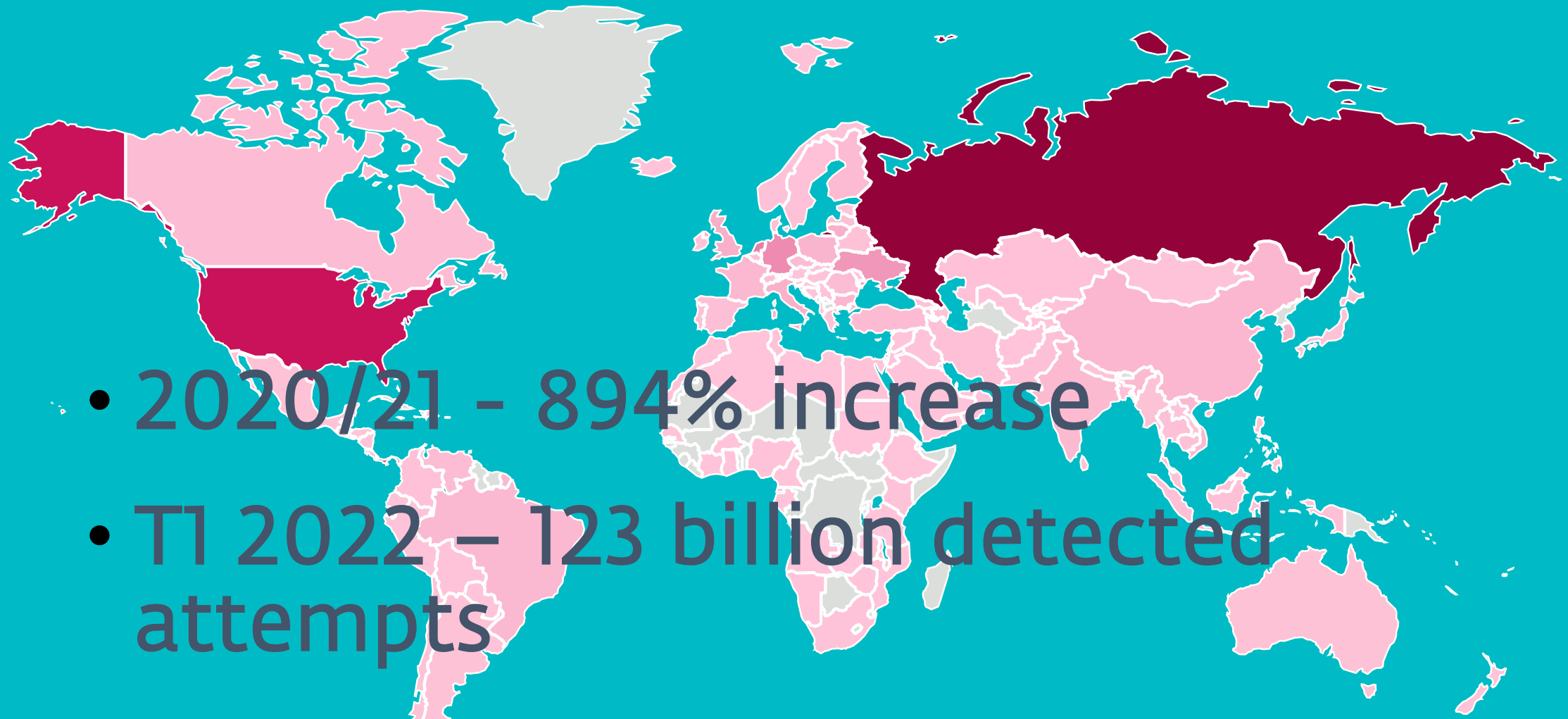
"I launch cyberattacks because that's what my government tells me to do."

The Threat



Remote desktop protocol

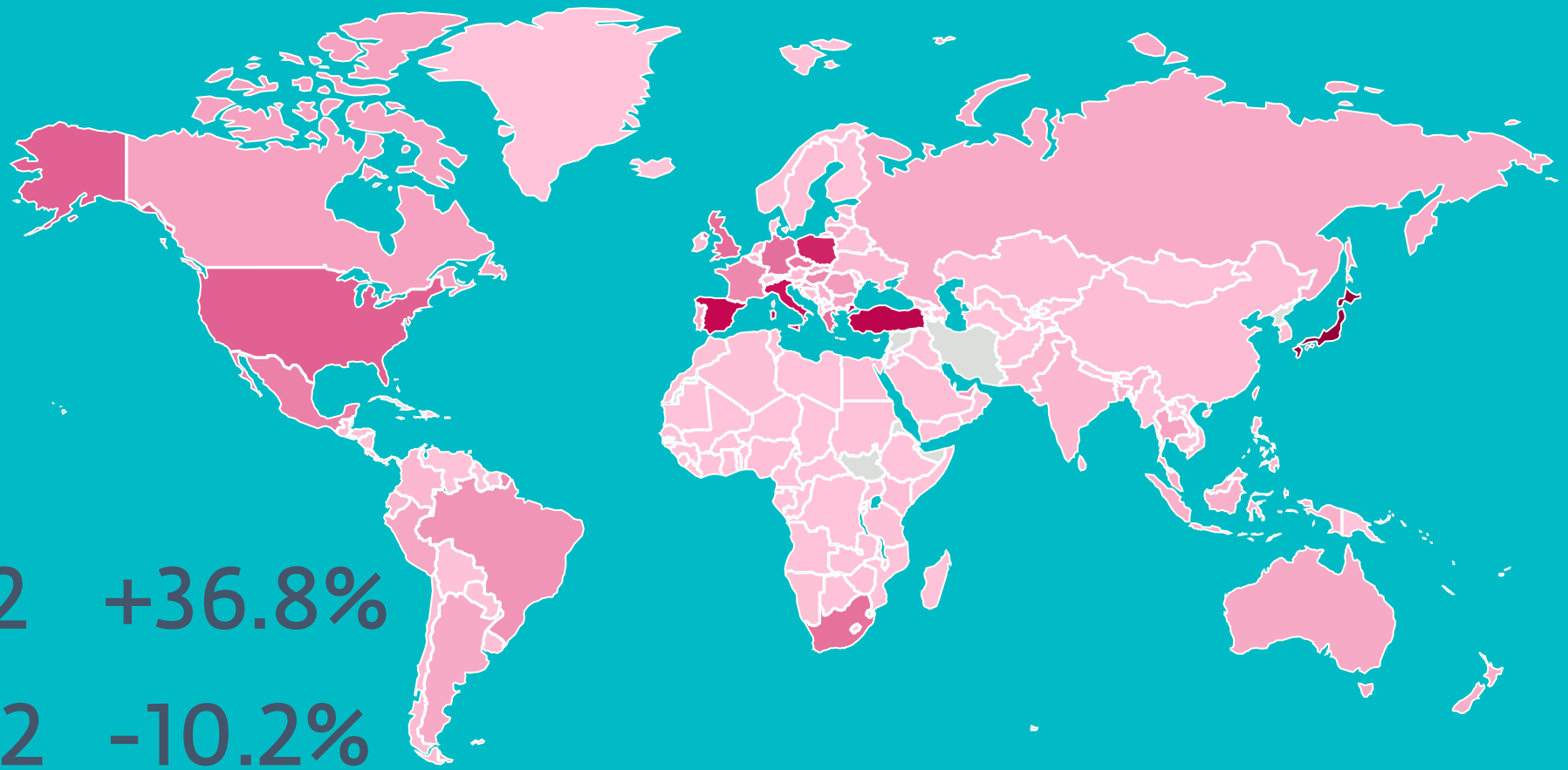
RDP – The source & quantity



- 2020/21 - 894% increase
- T1 2022 – 123 billion detected attempts
- T2 2022 – 13 billion detected

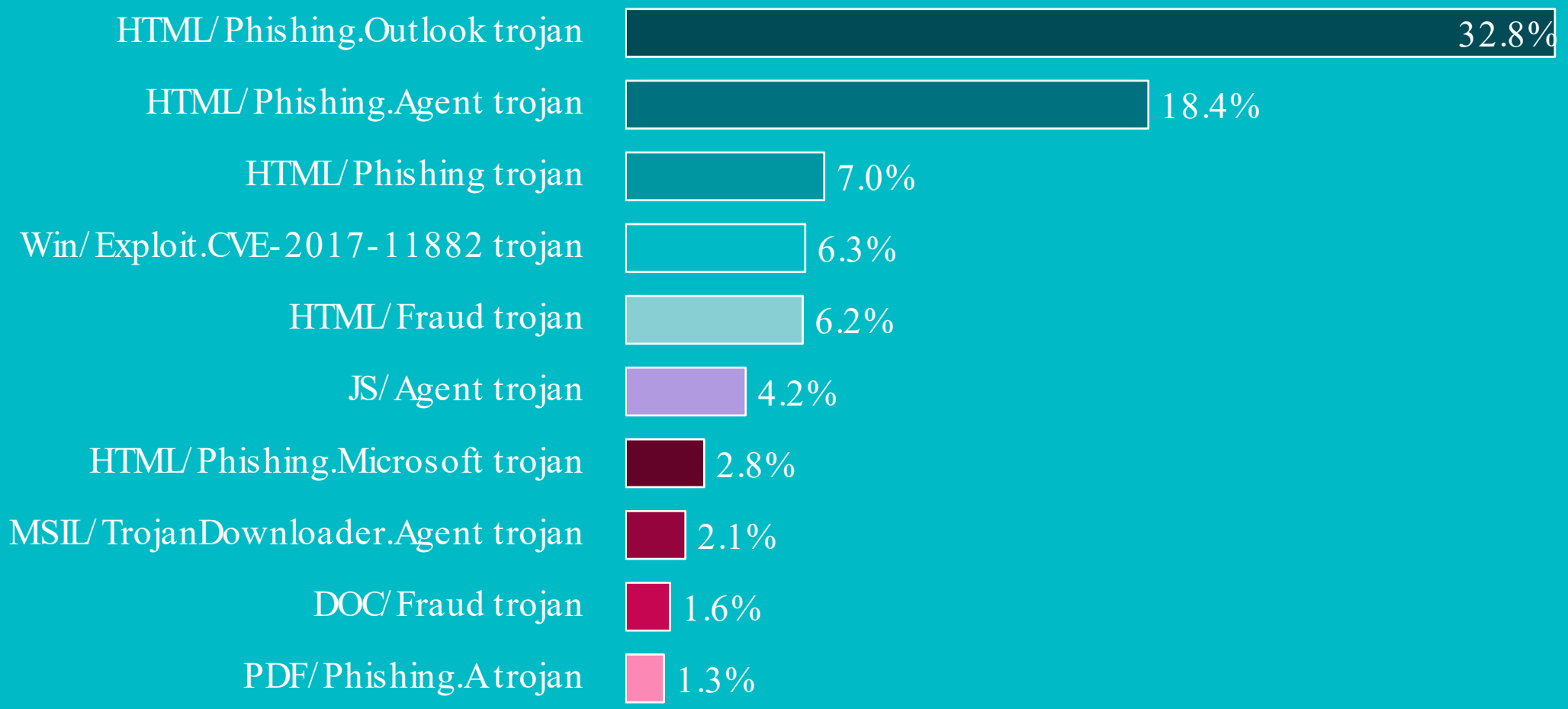
77% of SMEs will continue to use RDP despite security risks

Phishing and spear-phishing attacks



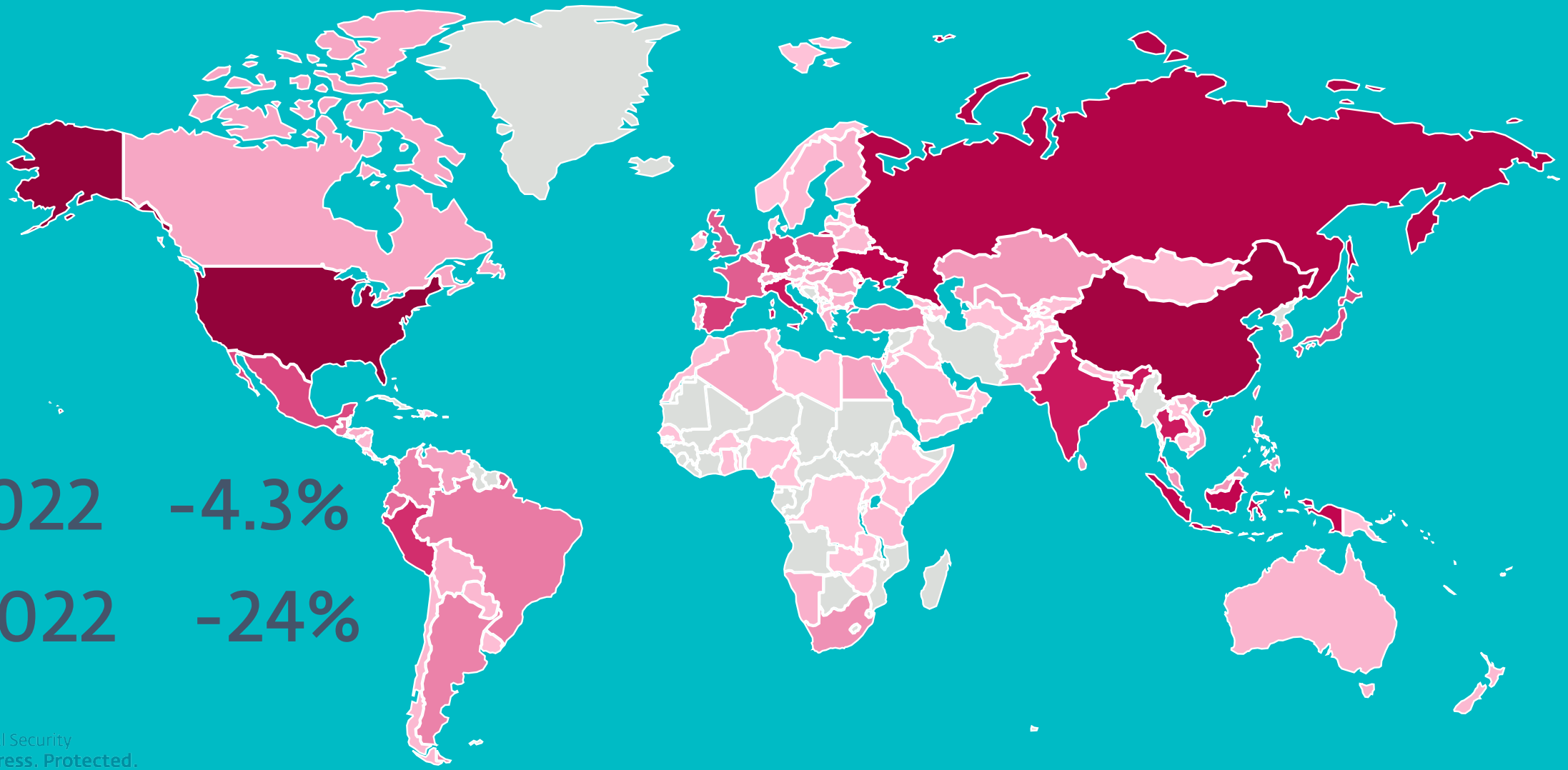
- T1 2022 +36.8%
- T2 2022 -10.2%

New Zealand - Top 10 malware detections



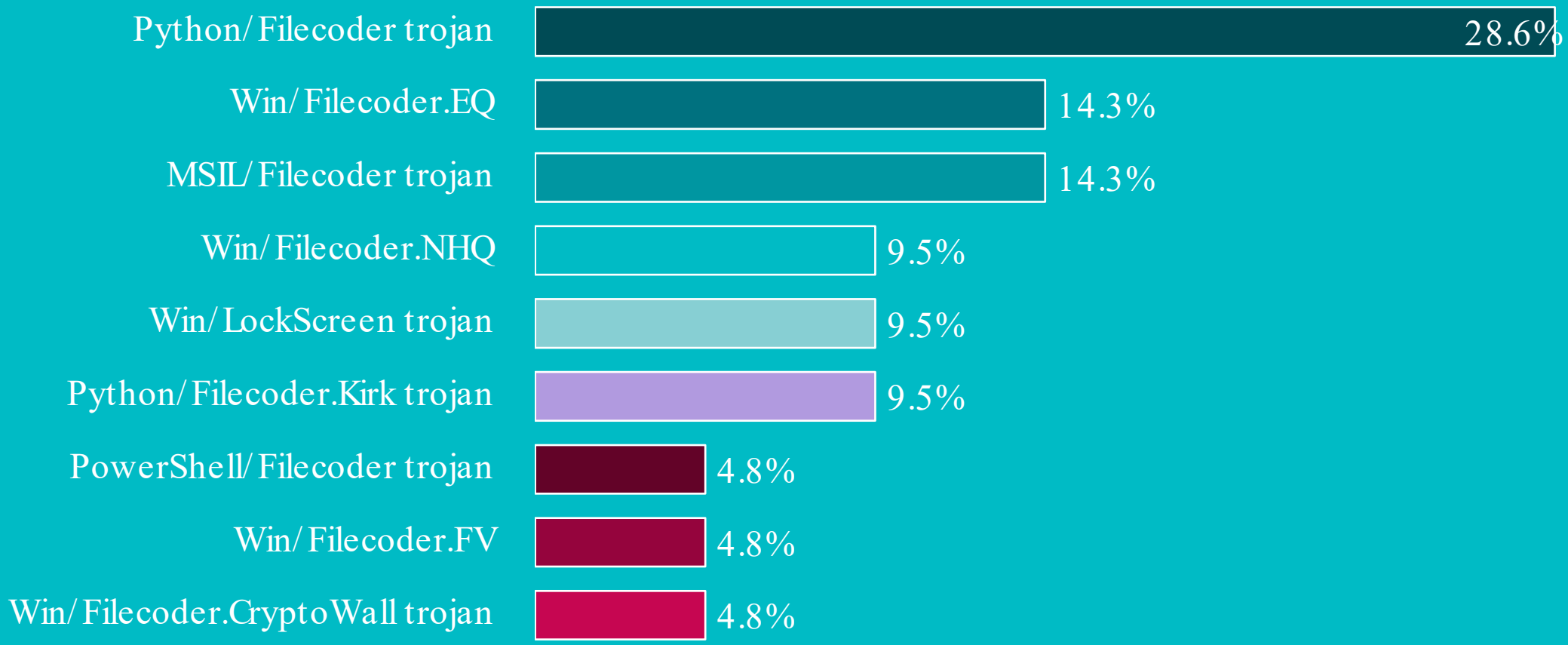

welivesecurity BY ESET
Amazon-themed campaigns of Lazarus in the Netherlands and Belgium

Ransomware heat map – T2 2022



- T1 2022 -4.3%
- T2 2022 -24%

New Zealand - Top 10 ransomware detections



Cybercrime monetization 2021

JBS

Kaseya

GARMIN

CNA

MediaMarkt

$4.4m $10m $14m $40m $70m $240m

Cybercrime monetization 2022

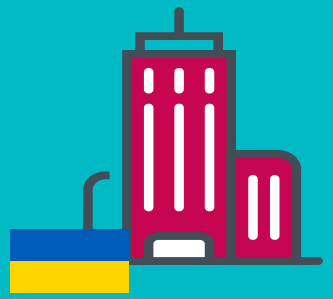
Ransomware business model

Cyberwarfare

Data wipers

100s

systems

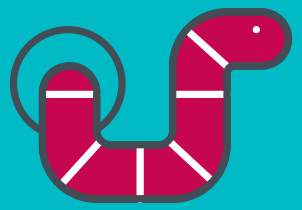


5+

organizations

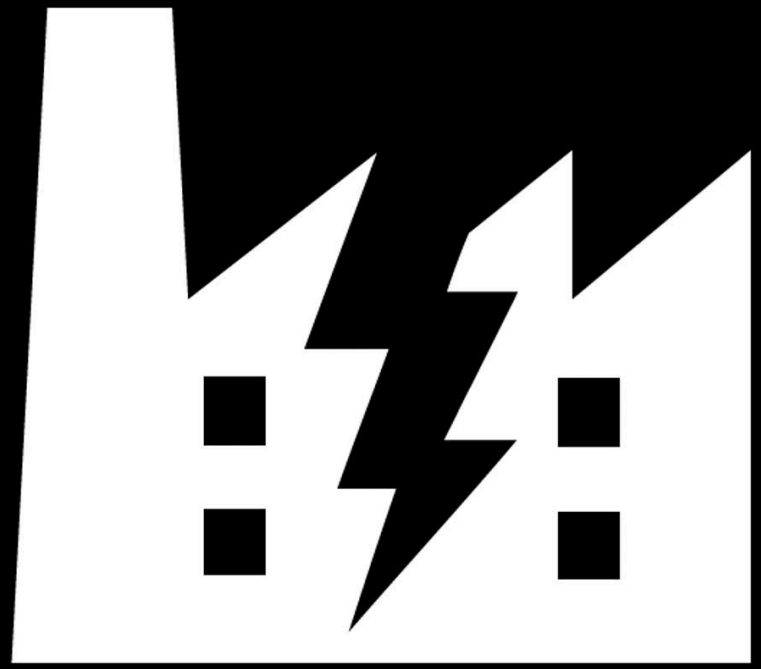
Dec 28, 2021

compilation timestamp*



HermeticWizard

HermeticRansom



INDUSTROYER2

Cyberattacks against Ukraine

ESET

The objectives are different

Espionage

Data collection

Sabotage

Signaling

73% of SMEs say the pandemic and war in Ukraine have driven increased investment in cybersecurity in business

Cyber risk insurance

CYBERSECURITY DIVE

MENU

What cyber insurance companies want from clients

Insurers evaluate how a company leverages technology and what internal standards are in place to manage risk.

Published April 28, 2022

By Sue Poremba

Political & Legislators

- Defense Authorization Act Amendment – Passed the house
- Sanction and Stop Ransomware Act – Introduced
- Ransomware and Financial Stability Act - Introduced
- Bill to require certain entities to disclose to the Secretary of Homeland Security ransom payments, and for other purpose – Introduced
- The Cyber Incident Notification Act (CINA) – Introduced
- The Ransomware Payments Bill (Australia) – Failed
- The Ransom Disclosure Act - Introduced
- The Cyber Incident Notification Act (CINA) – Introduced
- Bill C-26 – An Act Respecting Cyber Security (ARCS) (Canada) - Introduced
- Critical Cyber Systems Protection Act (CCSPA) (Canada) - Introduced
- Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) - Law

Financial Regulators

- Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies
- Requires extensive policies and procedures
- Requires increased disclosures and recordkeeping around cybersecurity practices, risks, and incidents.

Industry Regulators

- 36 hour incident reporting
- Defines cybersecurity incident
- Business impact
- Third-party notification
- April 1, 2022

Whether there is legislation or not reporting cyber-incidents will be required in some way

The business requirement

Cybersecurity	Cyber Resilience
Define procedures or measures to ensure the security of an organization	The capacity to recover or to continue to operate through an incident
Technologies and processes to protect from cybercrime	Technologies and processes designed to allow the business to continue to operate
Reduction in the risk of cyberattacks and against theft and espionage	Prediction and monitoring of risk and how to protect
Work without compromising the operation of systems	Culture shift to embed the needed process as normal
A plan to recover and resume functionality	A plan to operate during, recover and resume business operations

Over half (52%) of SMEs say they are only slightly or not at all confident in their overall cyber resilience over next 12 months

Only 33% of SMEs have conducted a cybersecurity audit the last 12 months

POLONIUM targets Israel with Creepy malware

You never walk alone: The SideWalk backdoor gets a Linux variant

ESET Threat Report T2 2022

IoCs

A comprehensive list of Indicators of Compromise and samples can be found in our GitHub repository.

SHA-1	Filename	ESET detection name	Description
3F4E3C5301752D39DAF97384CCA47564DA1C3314	dnw.exe	PowerShell/Agent.GJ	CreepyDrive
CC820ED9A23084104807941B76A2679243BA357C	Request.exe	PowerShell/Agent.HF	CreepySnail
03A35A0167684E6CCCA641296969972E49B88D60	DropBox.exe	MSIL/Agent.DPT	DeepCreep
4E7DBFF20995E97190536B284D7E5CC65922FD55	Mega.exe	MSIL/Agent.DPT	MegaCreep
994EAD7666A67E33C57A51EF98076D41AABB7FB7	Regestries.exe	MSIL/Tiny.DG	FlipCreep
79DE0AF2F10F8D39A93EED911D4048D87E3C8A1C	WinUpdate.dll	MSIL/Agent.DYU	TechnoCreep

Cyber defenders have a new voice

“Give in to the cybercriminal and you breed more cybercrime.”

Questions?