
SECURITY
DAYS
AKO VOJNA NA UKRAJINE
ZMENILA KYBERNETICKÉ HROZBY
Pohľad do ESET telemetrie
Digital Security
Progress. Protected.
&
SME KONFERENCIE

Thread

ESET Research ✓
@ESETresearch

Breaking. #ESETResearch discovered a new data wiper malware used in Ukraine today. ESET telemetry shows that it was installed on hundreds of machines in the country. This follows the DDoS attacks against several Ukrainian websites earlier today 1/n

9:25 PM · Feb 23, 2022

2,102 Retweets **344** Quotes **3,410** Likes **235** Bookmarks

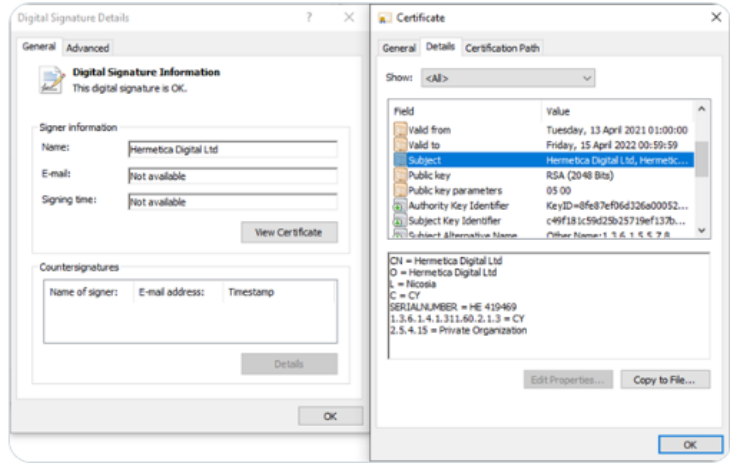
Tweet your reply

Reply

ESET Research ✓ @ESETresearch · Feb 23, 2022
We observed the first sample today around 14h52 UTC / 16h52 local time. The PE compilation timestamp of one of the sample is 2021-12-28, suggesting that the attack might have been in preparation for almost two months. 2/n

7 141 415

ESET Research ✓ @ESETresearch · Feb 23, 2022
The Wiper binary is signed using a code signing certificate issued to Hermetica Digital Ltd 3/n



Search Twitter

Relevant people

ESET Research ✓
@ESETre... Follows you
Following
Security research and breaking news straight from ESET Research Labs.

Trends for you

Politics · Trending
Putin
112K Tweets

Trending
HIMARS
5,278 Tweets

Trending
Kherson
11.4K Tweets

Trending
Belarus
7,123 Tweets

Politics · Trending
Ukrainian
110K Tweets

Trending
#ArtificialIntelligence
14.6K Tweets

Trending
Moldova
6,035 Tweets

Trending in Slovakia
#Crypto
1.97M Tweets

Trending
#CyberAttack
2,165 Tweets

Ondrej Kubovic

14 Jan 2022

WhisperGate

Read more | ESET
Read more | Microsoft

23 Feb 2022

HermeticWiper
HermeticRansom

Read more | ESET

24 Feb 2022

AcidRain

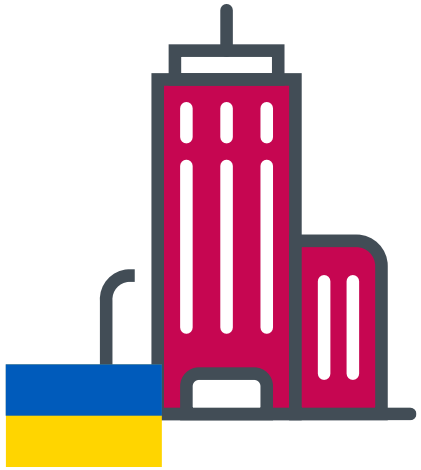
Read more | SentinelOne

24 Feb 2022

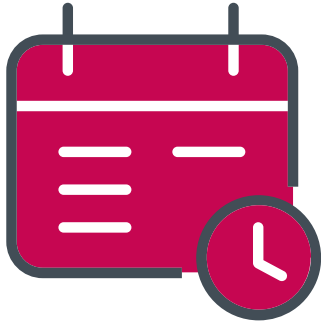
IsaacWiper

HermeticWiper: Dopady

Stovky
napadnutých systémov



5+
organizácií



Dec 28, 2021
compilation timestamp*

Hermetic kampaň

HermeticWiper

HermeticWizard

HermeticRansom

14 Jan 2022

WhisperGate

Read more | ESET
Read more | Microsoft

23 Feb 2022

HermeticWiper
HermeticRansom

Read more | ESET

24 Feb 2022

AcidRain

Read more | SentinelOne

24 Feb 2022

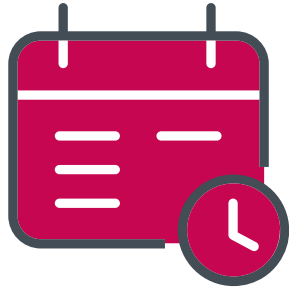
IsaacWiper


~ 10 Mar 2022
HermeticWiper
Read more | Microsoft
14 Mar 2022
CaddyWiper
Read more | ESET
~ 17 Mar 2022
DoubleZero
Read more | CERT-UA
~ 17 Mar 2022
DesertBlade

CaddyWiper

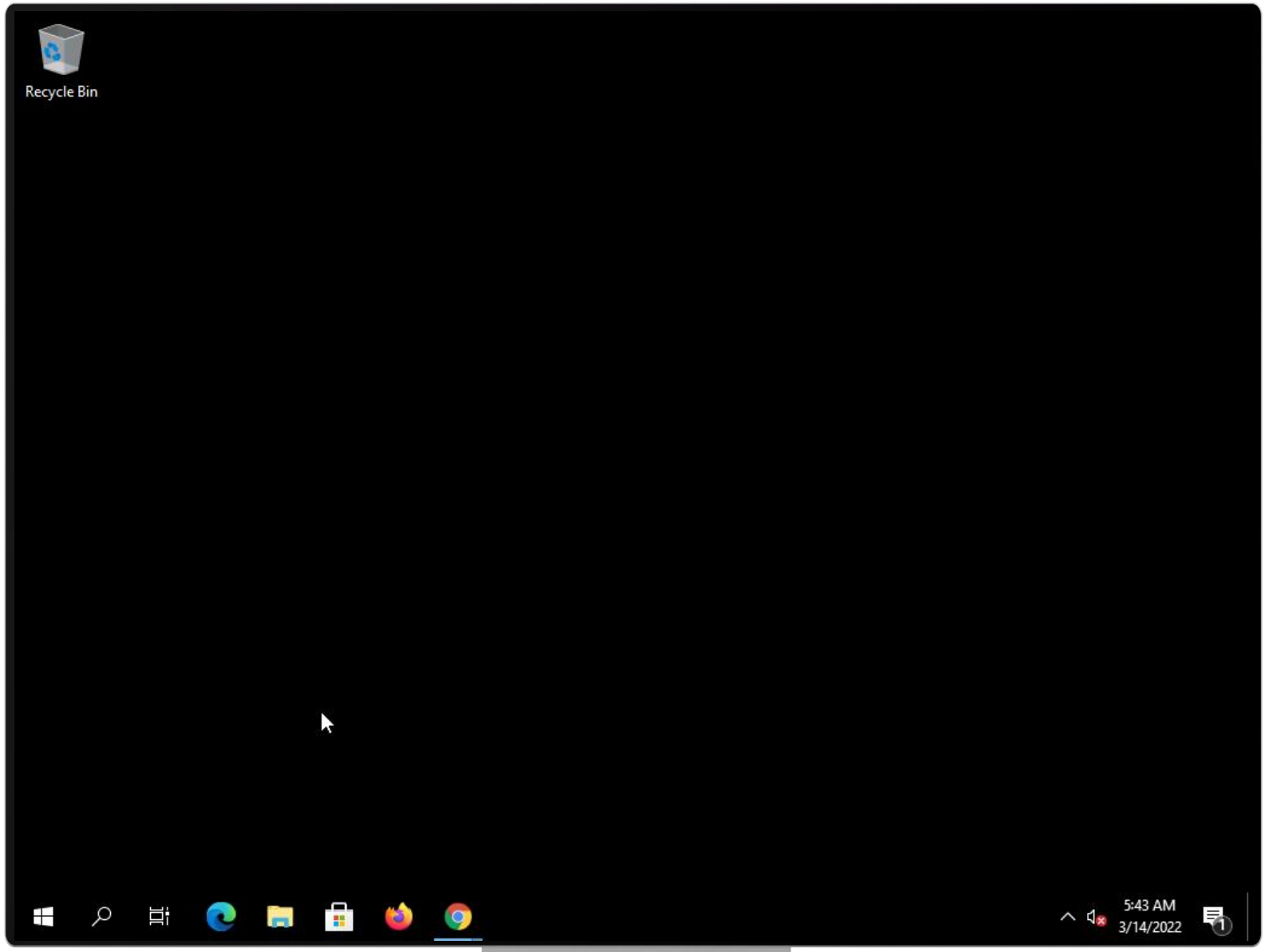
Desiatky systémov

Finančný sektor



Skompilované a použité 14. Mar, 2022

CaddyWiper v akcii



Zdroj: VirusTotal

~ 10 Mar 2022

HermeticWiper

Read more | Microsoft

14 Mar 2022

CaddyWiper

Read more | ESET

~ 17 Mar 2022

DoubleZero

Read more | CERT-UA

~ 17 Mar 2022

DesertBlade

1 Apr 2022

ArguePatch
CaddyWiper

Read more | ESET

8 Apr 2022

ArguePatch
CaddyWiper
ORCSHRED, SOLOSHRED, AWFULSHRED

(Industroyer 2 incident)

Read more | ESET
Read more | CERT-UA

~ 16 May 2022

ArguePatch
CaddyWiper

Read more | ESET

gov.ua
State Sites of Ukraine

The team operates in within State Service of Special Communication and Information Protection of Ukraine

CERT-UA
Computer Emergency Response Team of Ukraine

People with visual impairment

About CERT-UA | News | Recommendations | Contact Us | Contacts | Search | Українською |

Main | News | Кібератака групи Sandworm (UAC-0082) ...

Cyber attack of the Sandworm group (UAC-0082) on energy facilities of Ukraine using malware INDUSTROYER2 and CADDYWIPER (CERT-UA#4435)

12.04.2022

ШПЗ

Загальна інформація

Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA вжито невідкладних заходів з реагування на інцидент інформаційної безпеки, пов'язаний з цільовою

By topic «ШПЗ»

12.05.2022

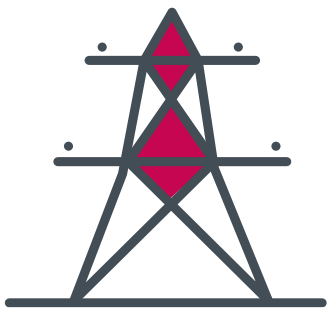
Russia's most aggressive cyberattack team attempted a third blackout in Ukraine, years after its historic cyberattacks on the Ukrainian power grid in 2015 and 2016, still the only confirmed blackouts known to have been caused by hackers.

ESET and CERT-UA say the malware was planted on target systems within a regional Ukrainian energy firm on Friday. CERT-UA says that the attack was successfully detected in progress and stopped before any actual blackout could be triggered. But an earlier, private advisory from CERT-UA last week, first reported by *MIT Technology Review* today, stated that power had been temporarily switched off to nine electrical substations.

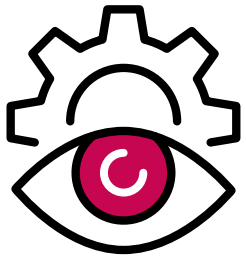
Both CERT-UA and ESET declined to name the affected utility. But more than 2 million people live in the area it serves, according to Farid Safarov, Ukraine's deputy minister of energy.

"The hack attempt did not affect the provision of electricity at the power company. It was promptly detected and mitigated," says Viktor Zhora, a senior official at Ukraine's cybersecurity agency, known as the State Services for Special Communication and Information Protection (SSSCIP). “But the intended disruption was huge.” Asked about the earlier report that seemed to describe an attack that was at least partially successful, Zhora described it as a "preliminary report" and stood by his and CERT-UA's most recent public statements.

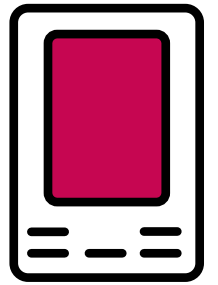
CIELE INDUSTROYER-U...



Odstávka elektriny

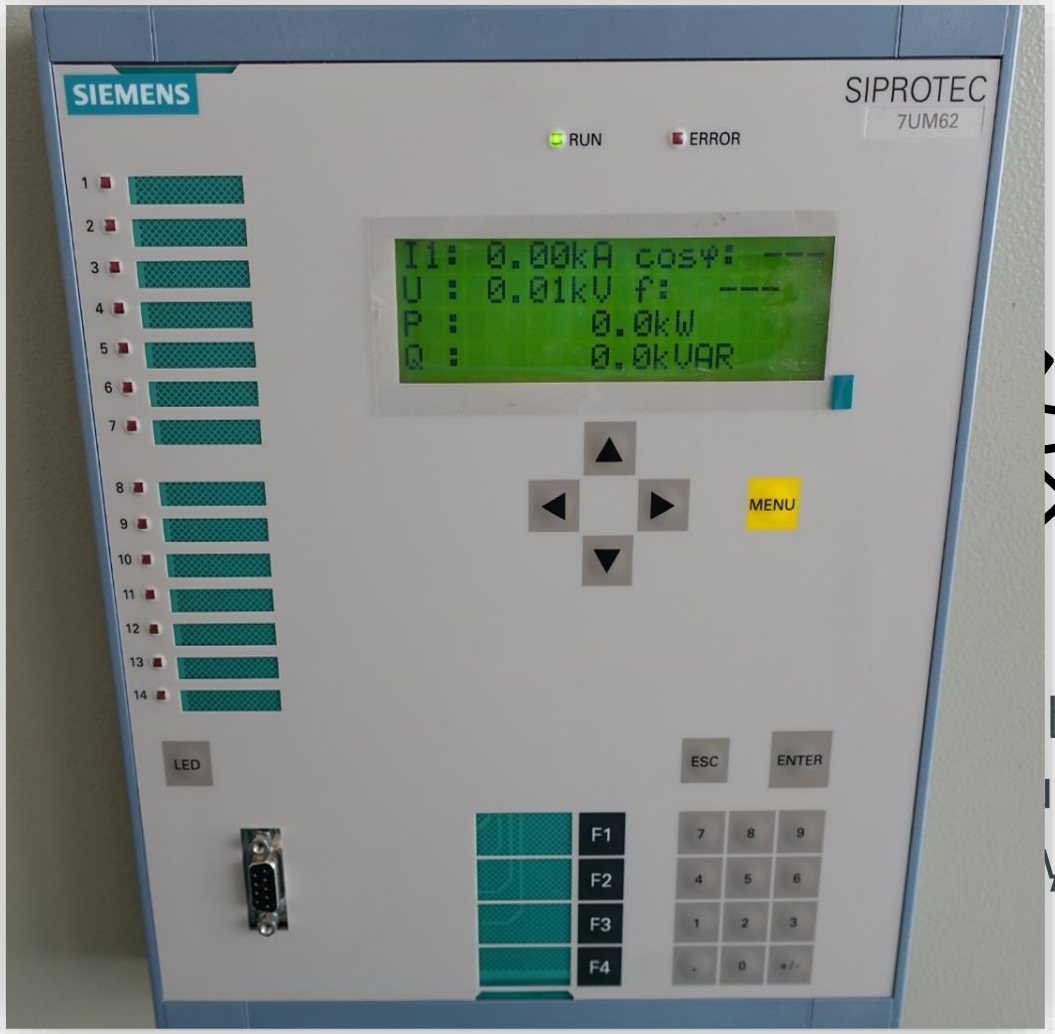


Operátori bez prehľadu a kontroly

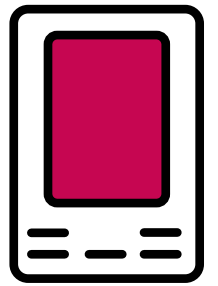


Vypnutie ochrán

CIELE INDUSTROYER-U...



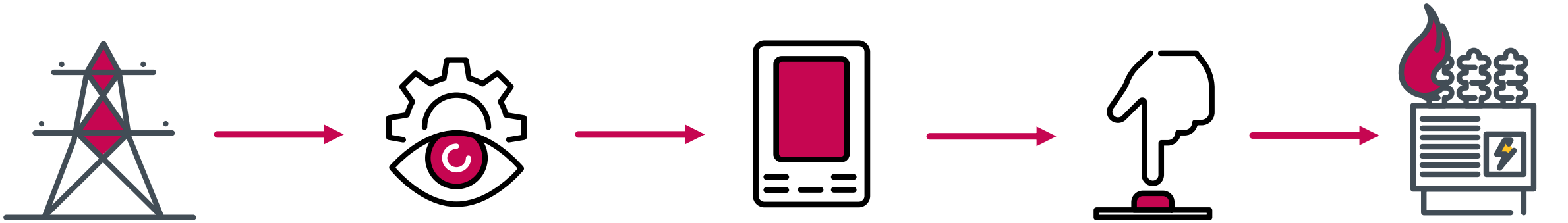
bez
ı a
y



Vypnutie
ochrán

eset Digital Security
Progress. Protected.

CIELE INDUSTROYER-U...V ROKU 2016



Odstávka elektriny

Operátori bez prehľadu a kontroly

Vypnutie ochrán

Manuálna obnova funkcie operátormi

Fyzické poškodenie

1 Apr 2022

ArguePatch
CaddyWiper

Read more | ESET

8 Apr 2022

ArguePatch
CaddyWiper
ORCSHRED, SOLOSHRED, AWFULSHRED

(Industroyer 2 incident)

Read more | ESET
Read more | CERT-UA

~ 16 May 2022

ArguePatch
CaddyWiper

Read more | ESET

~ 5 Oct 2022

HermeticWiper

Read more | ESET

11 Oct 2022

Prestige faux ransomware

Read more | ESET
Read more | Microsoft

11 Oct 2022

NikoWiper

Read more | ESET

~ 11 Nov 2022

Somnia faux ransomware

Prestige faux ransomware

Napadnuté stovky systémov

Logistické spoločnosti

Ukrajina a Poľsko

~ 5 Oct 2022

HermeticWiper

Read more | ESET

11 Oct 2022

Prestige faux ransomware

Read more | ESET
Read more | Microsoft

11 Oct 2022

NikoWiper

Read more | ESET

~ 11 Nov 2022

Somnia faux ransomware

11 Oct 2022 **Prestige faux ransomware**
Read more | ESET
Read more | Microsoft

11 Oct 2022 **NikoWiper**
Read more | ESET

~ 11 Nov 2022 **Somnia faux ransomware**
Read more | CERT-UA

21 Nov 2022 **RansomBoggs faux ransomware**
Read more | ESET

12 Jan 2023 **SDelete**

~ 17 Jan 2023 **CaddyWiper**
ZeroWipe
SDelete
AWFULSHRED
BidSwipe
Read more | CERT-UA

25 Jan 2023 **SwiftSlicer**
Read more | ESET

~20 Wiperov

zanalyzovaných

Desiatky

ochránených inštitúcií

Viac ako tisíc

ochránených zariadení

A year of wiper attacks in Ukraine

ESET Research has compiled a timeline of cyberattacks that used wiper malware and have occurred since Russia's invasion of Ukraine in 2022

(e):r ESET Research

24 Feb 2023 - 11:30AM

(eset):research;podcast

ESET Research Podcast: A year of fighting rockets, soldiers, and wipers in Ukraine

ESET experts share their insights on the cyber-elements of the first year of the war in Ukraine and how a growing number of destructive malware variants tried to rip through critical Ukrainian systems

(e):r ESET Research

30 Mar 2023 - 11:30AM

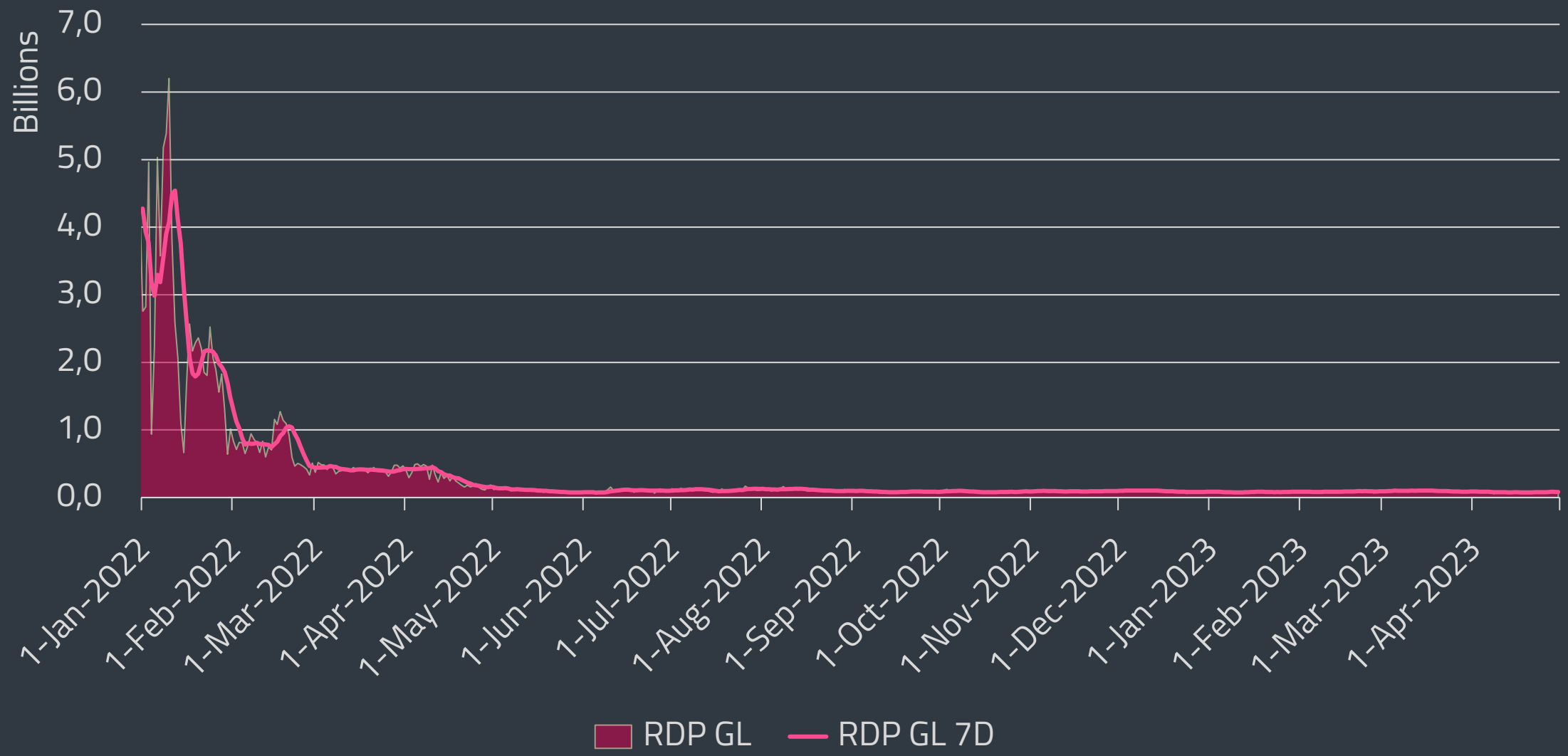
THREAT REPORT T3 2022

WeLiveSecurity.com
@ESETresearch
ESET GitHub

Digital Security
Progress. Protected.

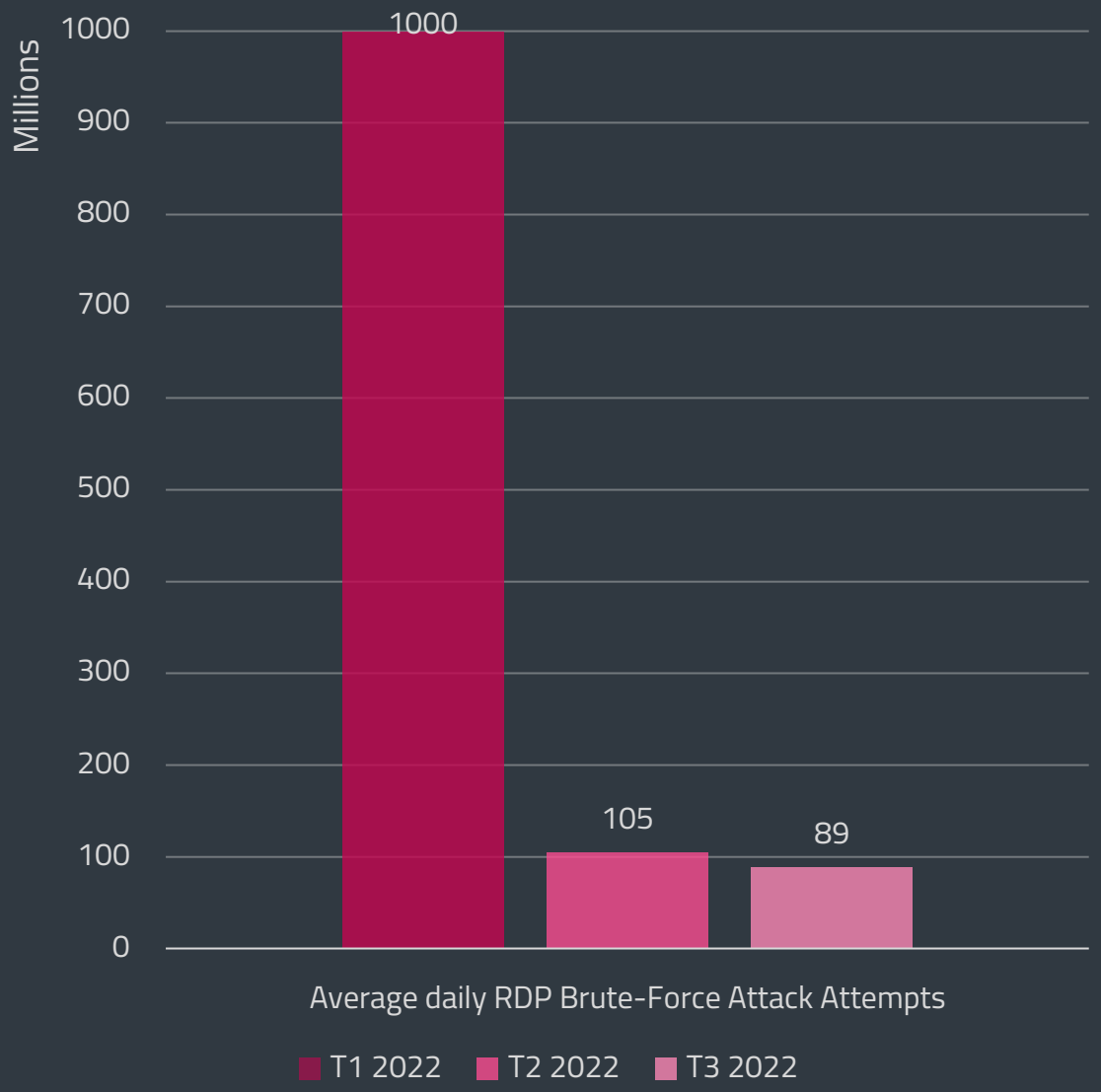
CONTENTS

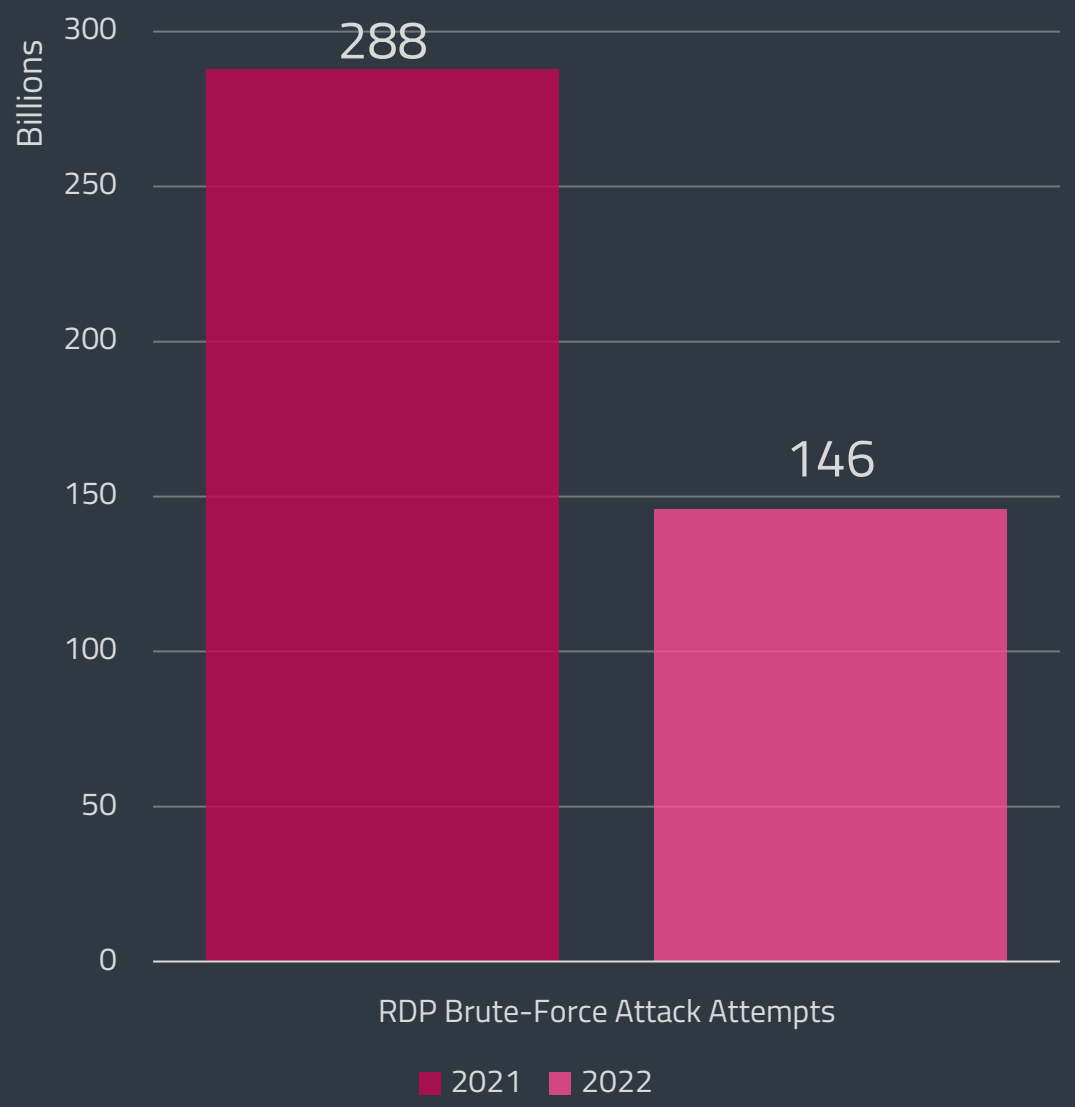
Globálne RDP útoky klesli o viac ako 90%



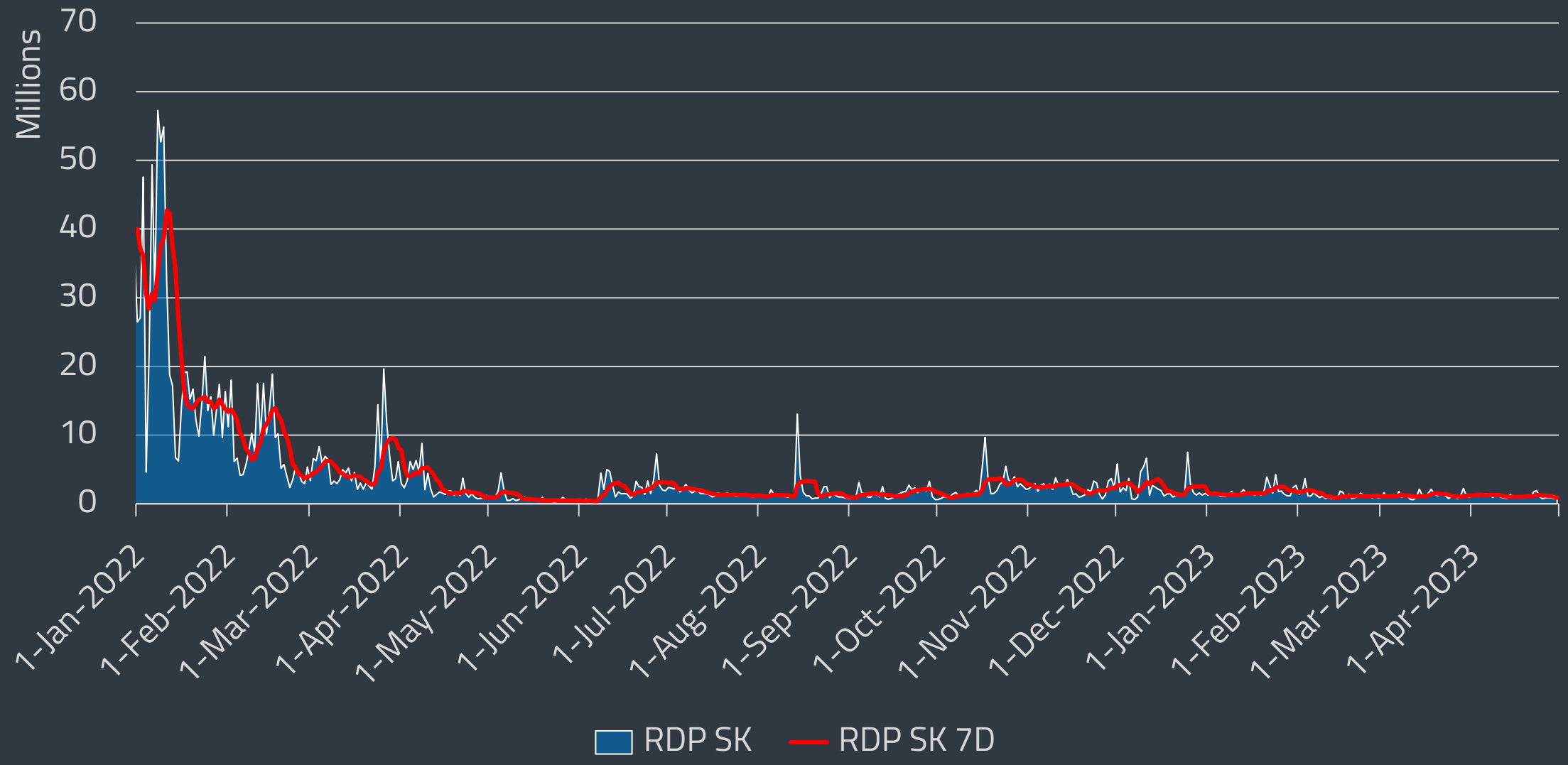
Trends pokusov o pripojenie cez RDP v roku 2022-2023, sedemdňový kĺzavý priemer

Medziročne sa RDP útoky prepadli o polovicu



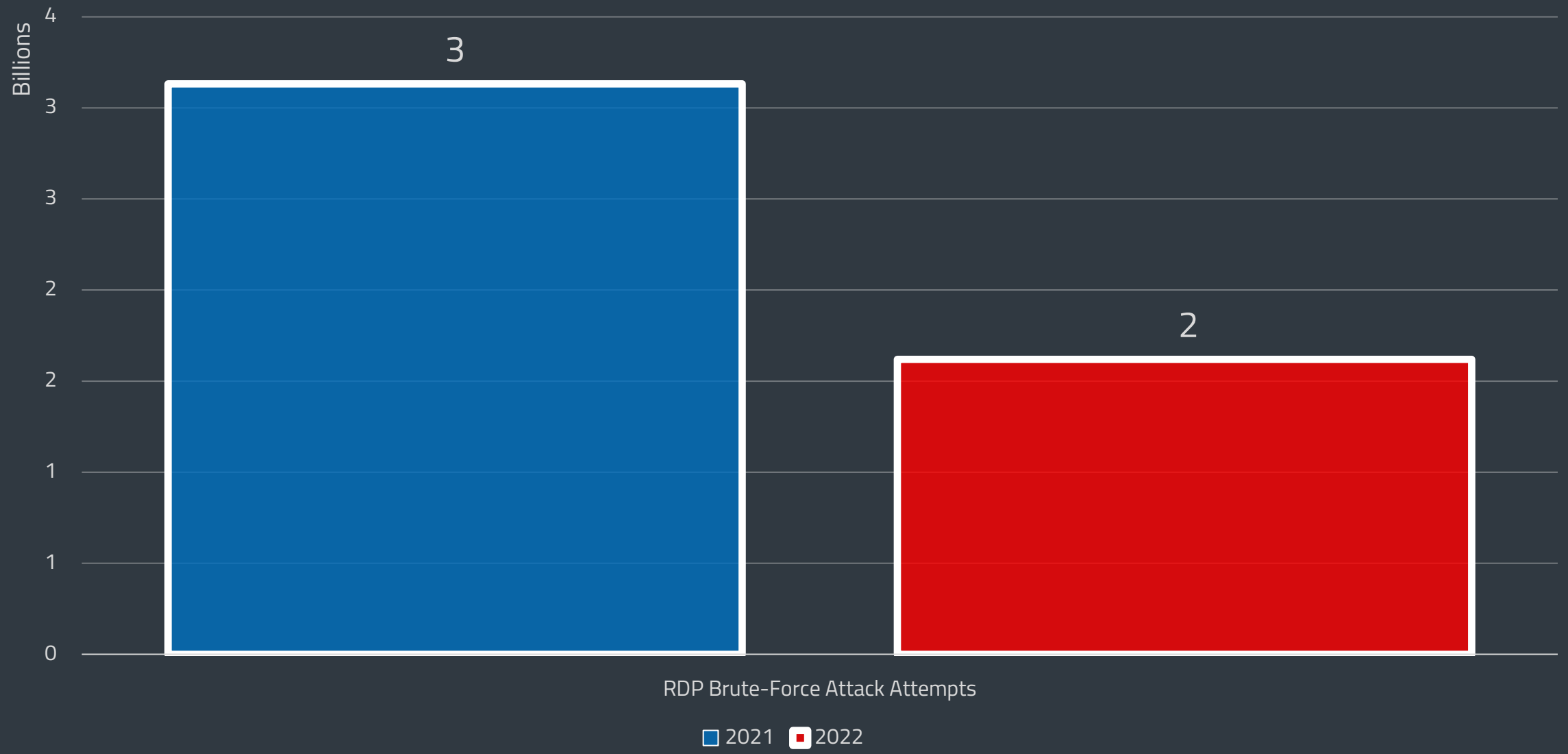


RDP útoky na Slovensku klesli o 84%, následne však rástli



Trends pokusov o pripojenie cez RDP v roku 2022-2023, sedemdňový kĺzavý priemer

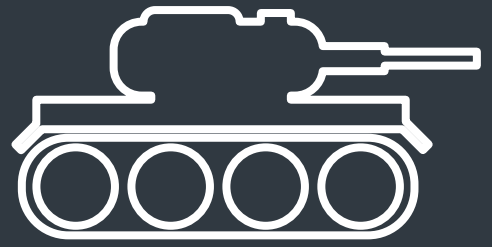
Na Slovensku bol pokles o niečo pomalší



Možné dôvody pre klesajúci trend

Menej práce na diaľku

Lepšie bezpečnostné povedomie

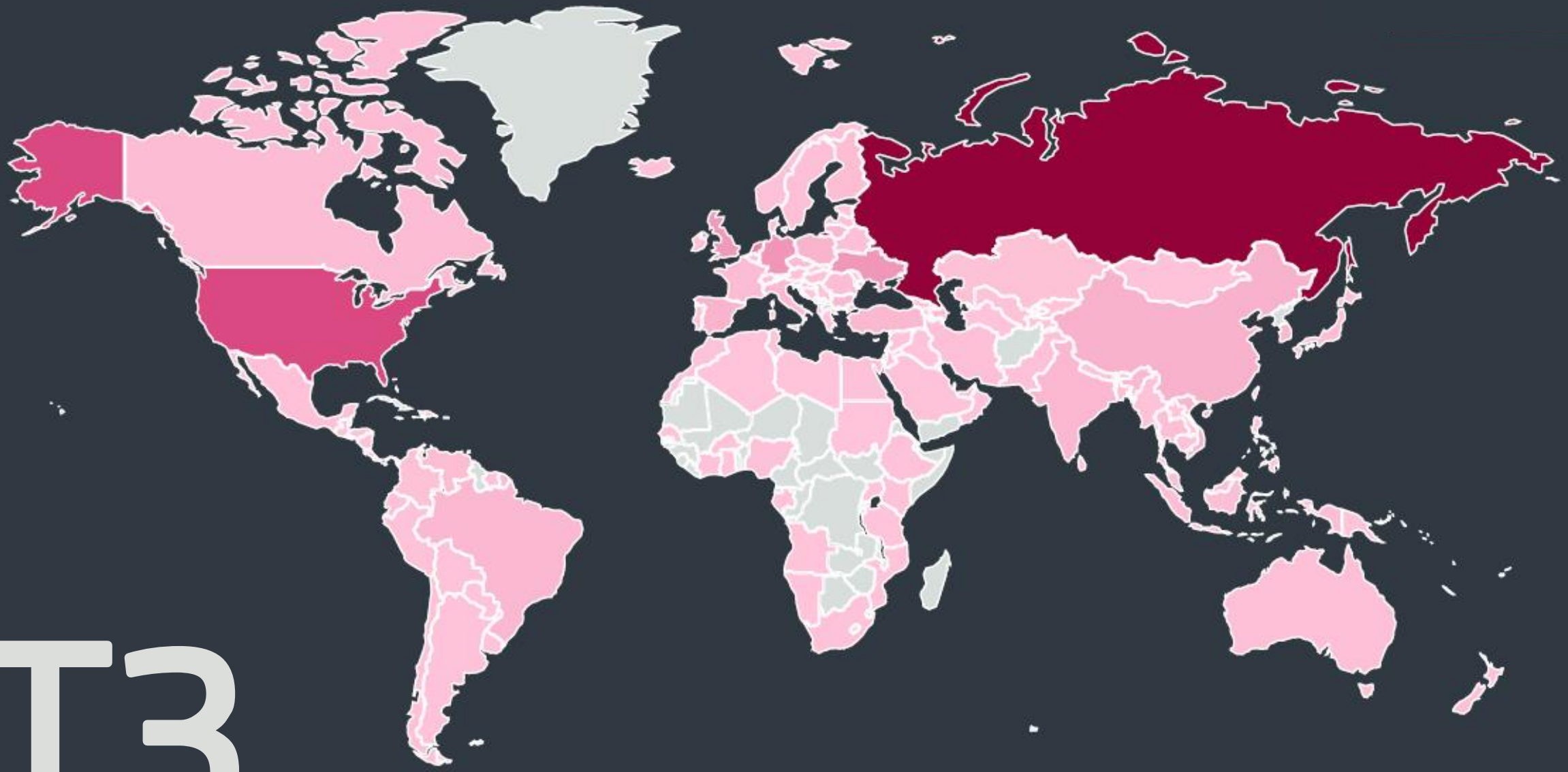


Vojna na Ukrajine

Brute-force lockout vo Win11

Útočiace IP adresy (RDP)

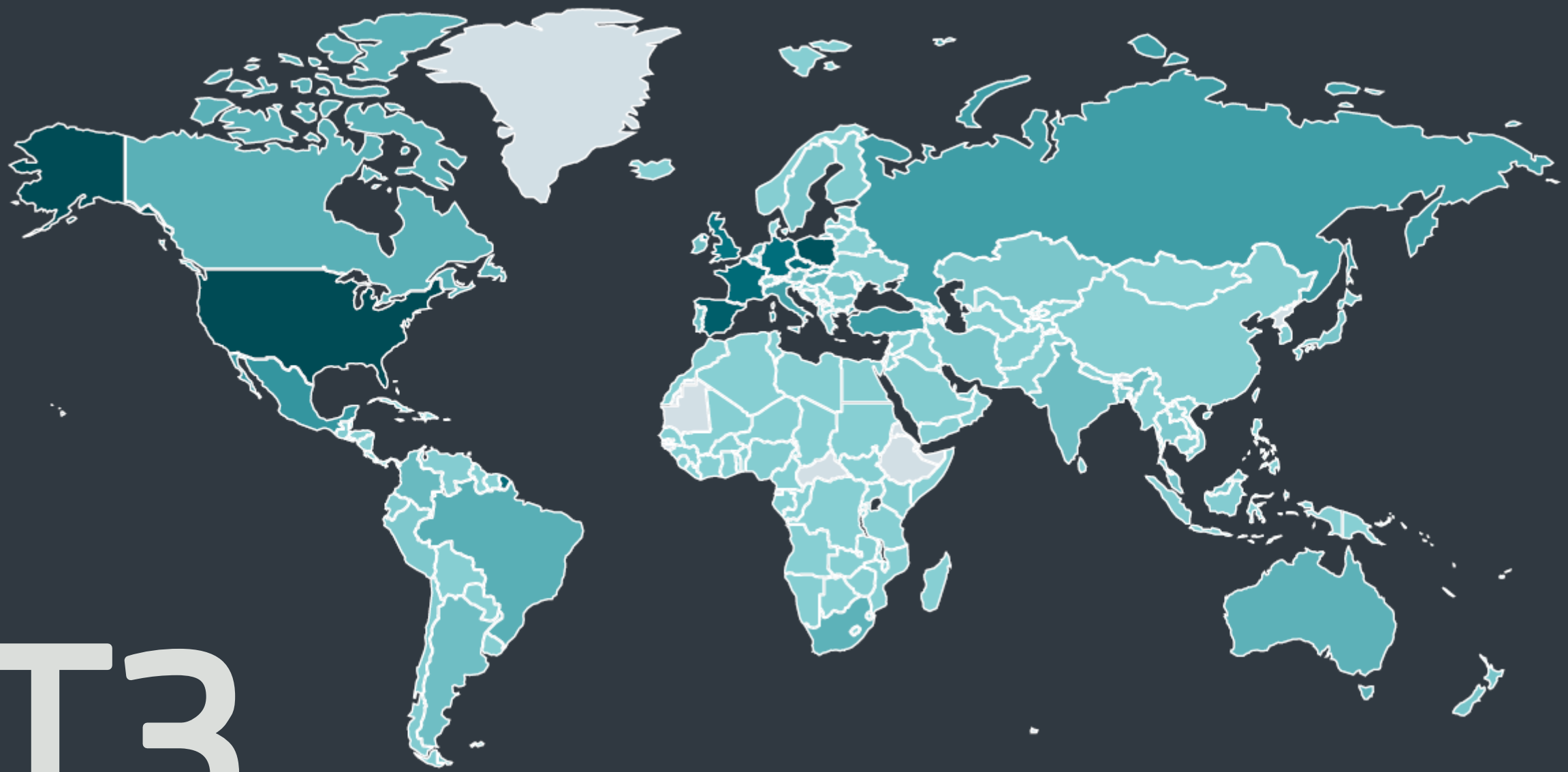
0.0% 31.5%



T3

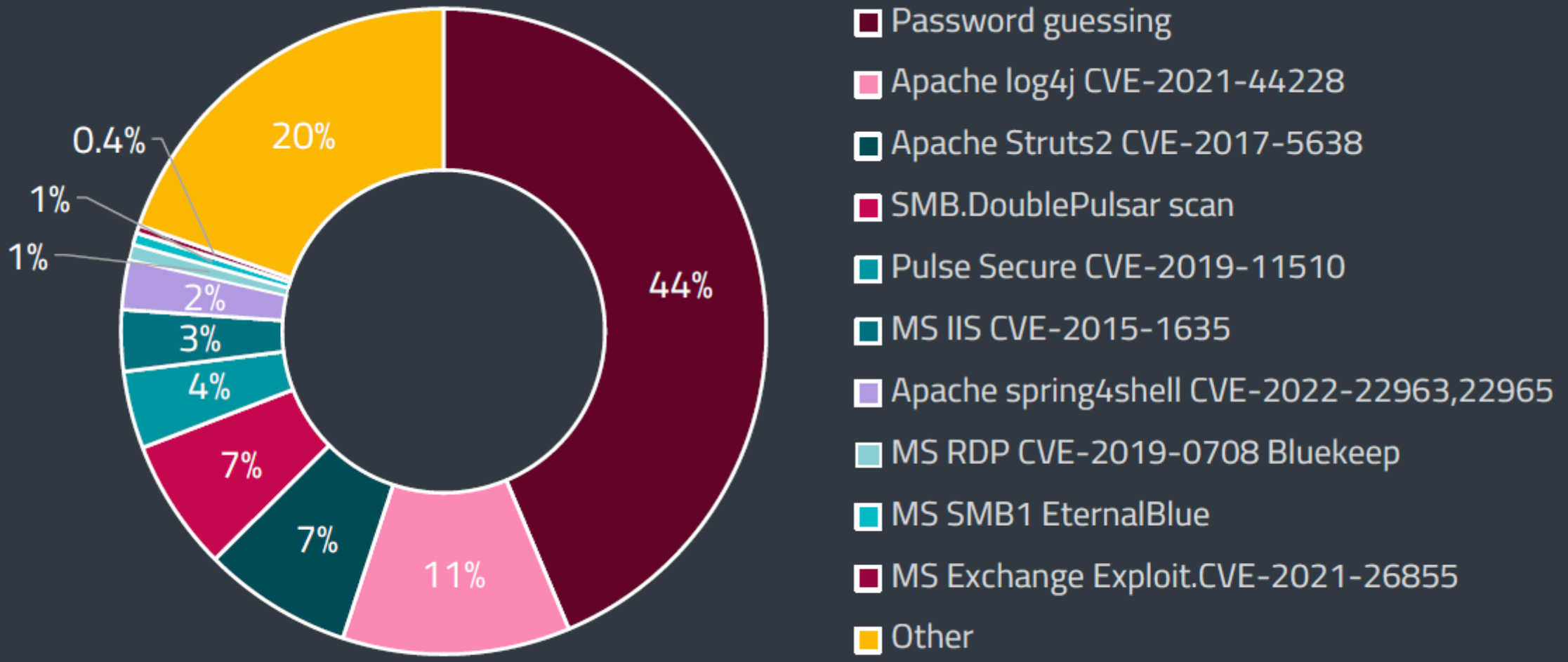
Cieľové IP adresy (RDP)

0.0% 11.1%



T3

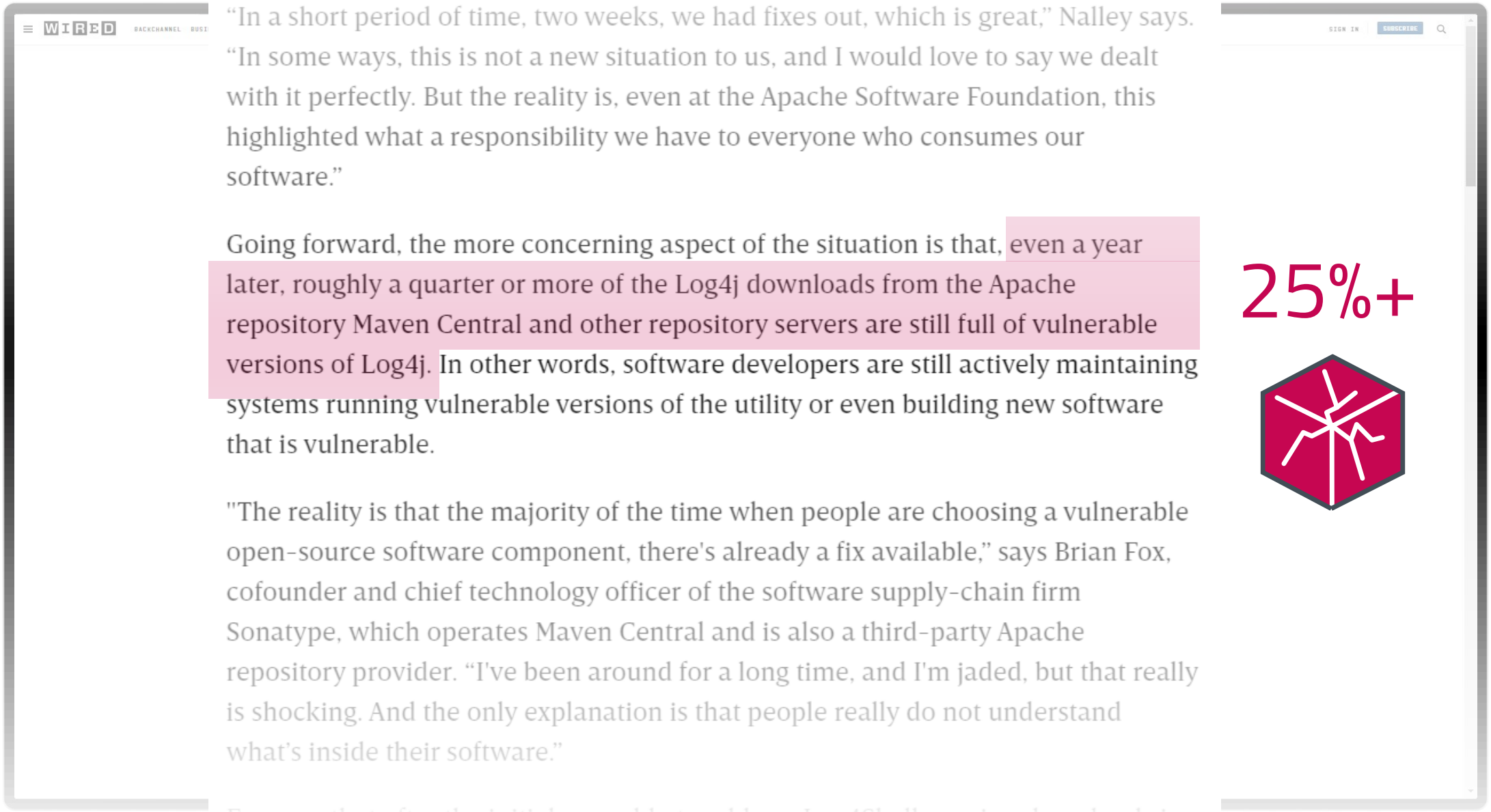
Log4Shell je stále druhým najčastejšie zneužívaným útočným vektorom



T3

Externé sieťové vektory prieniku podľa unikátnych klientov v T3 2022

projects to catch bugs before they ship in code and respond to incidents when necessary.



“In a short period of time, two weeks, we had fixes out, which is great,” Nalley says. “In some ways, this is not a new situation to us, and I would love to say we dealt with it perfectly. But the reality is, even at the Apache Software Foundation, this highlighted what a responsibility we have to everyone who consumes our software.”

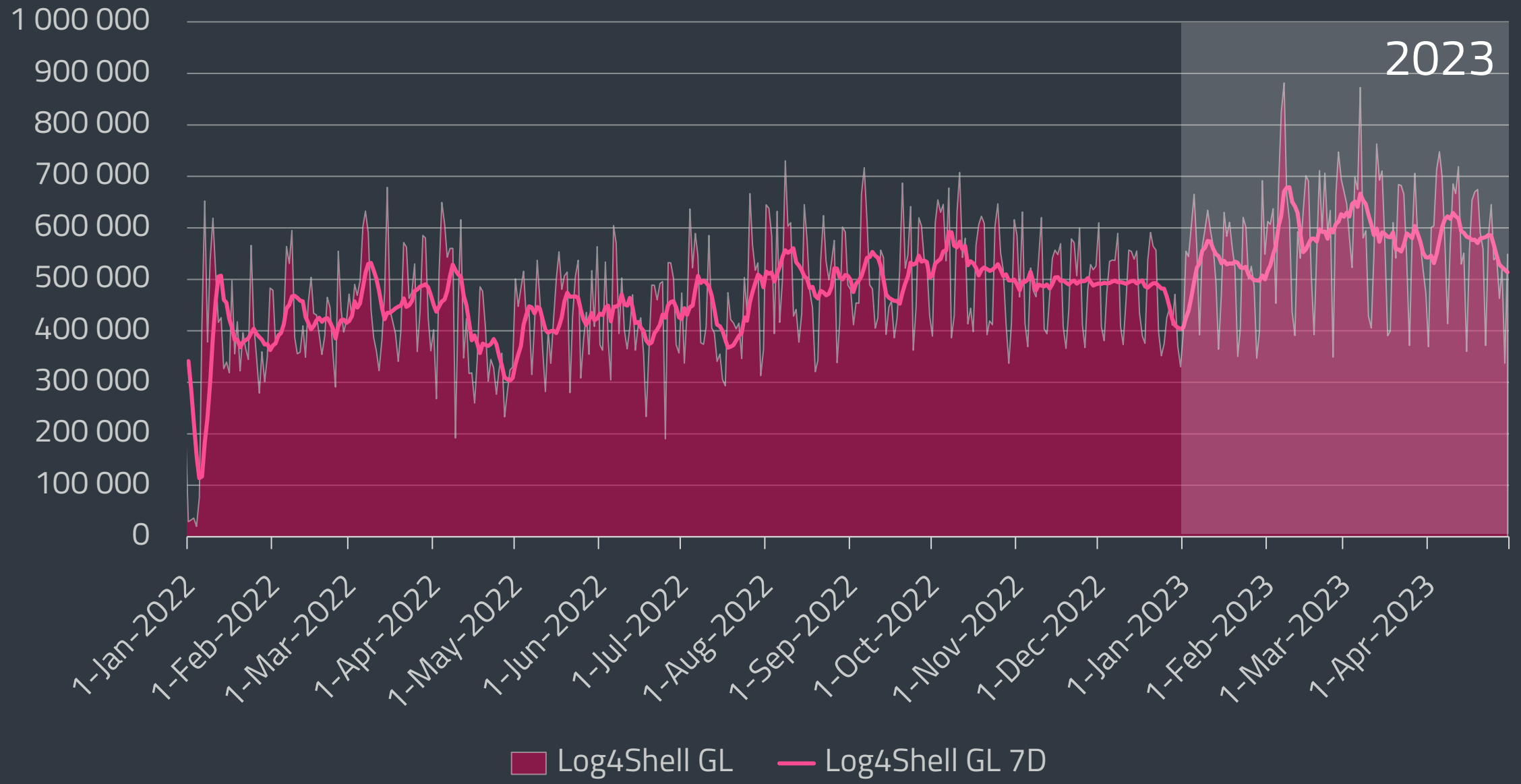
Going forward, the more concerning aspect of the situation is that, even a year later, roughly a quarter or more of the Log4j downloads from the Apache repository Maven Central and other repository servers are still full of vulnerable versions of Log4j. In other words, software developers are still actively maintaining systems running vulnerable versions of the utility or even building new software that is vulnerable.

25%+

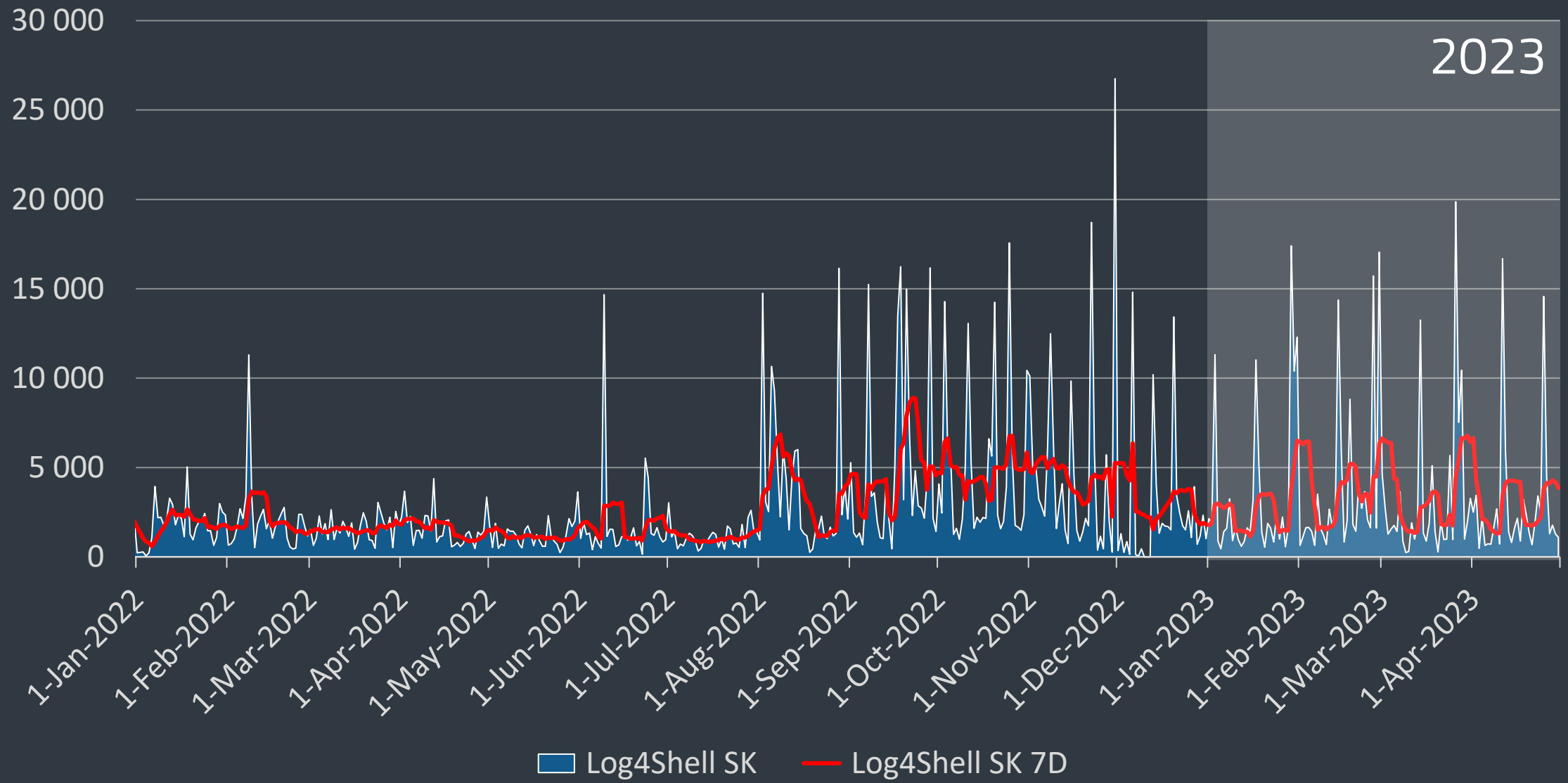
"The reality is that the majority of the time when people are choosing a vulnerable open-source software component, there's already a fix available,” says Brian Fox, cofounder and chief technology officer of the software supply-chain firm Sonatype, which operates Maven Central and is also a third-party Apache repository provider. “I've been around for a long time, and I'm jaded, but that really is shocking. And the only explanation is that people really do not understand what's inside their software.”

Fox says that after the initial scramble to address Log4Shell, version downloads in

Pokusy o zneužitie zraniteľnosti Log4Shell (globálne)



Pokusy o zneužitie zraniteľnosti Log4Shell (Slovensko)



welivesecurity BY ESET

In English

Menu

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

Research

Expert content, for researchers by researchers

Research

A lookback under the TA410 umbrella: Its cyberespionage TTPs and activity

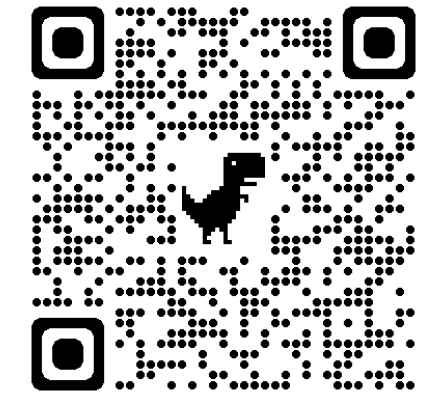
ESET researchers reveal a detailed profile of TA410: we believe this cyberespionage umbrella group consists of three different teams using different toolsets, including a new version of the FlowCloud espionage backdoor discovered by ESET.

Alexandre Côté Cyr and Matthieu Faou 27 Apr 2022 - 03:00PM

When "secure" isn't secure at all: High-impact UEFI vulnerabilities discovered in Lenovo consumer laptops

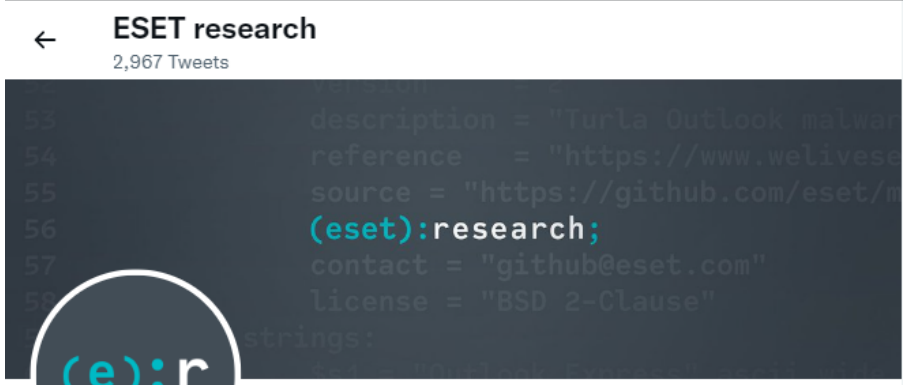
ESET researchers discover multiple vulnerabilities in various Lenovo laptop models that allow an attacker with admin privileges to expose

Follow us



ESET research

2,967 Tweets



(e):r

Following

ESET research

@ESETresearch Follows you

Security research and breaking news straight from ESET Research Labs.

welivesecurity.com/research/ Joined July 2009

31 Following **26K** Followers

Followed by Daniela Skripkova, Jen Easterly, and 132 others you follow

Tweets | Tweets & replies | Media | Likes

ESET research @ESETresearch · May 25

#ESETresearch's very own @HrckaVladislav is going to present „Under the hood of Wslink's multilayered virtual machine" at @reconmtl! He will describe the features of the advanced VM u
explain the semiautomated approach to ove

1 9

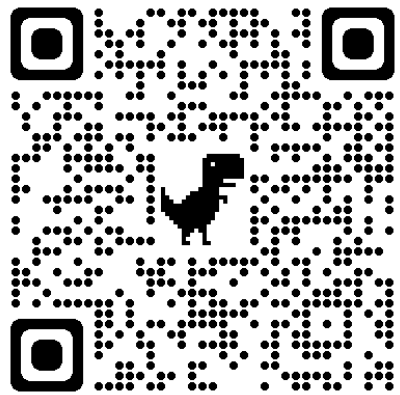
ESET research @ESETresearch · May 25

He will provide insights into the process of r
of undocumented VM and describe the app
protection,extending existing deobfuscatio
execution to determine the meaning of the

1

ESET research @ESETresearch · May 25

@HrckaVladislav will explain step-by-step h
without any previous knowledge, deobfusc



SECURITY DAYS

Ďakujem za pozornosť!

Digital Security
Progress. Protected.

&

SME KONFERENCIE