TLDCON 2023

Threat landscape

Vladimir Kuskov

Head of Anti-Malware Research

kaspersky

400 000

New malicious objects detected by Kaspersky every day (2022)

General statistics – Kaspersky Security Network – main numbers (2023 H1)

1,667,005,508

attacks blocked launched from online resources around the globe

462,210,159

malicious and potentially unwanted URLs detected

185,168

users were protected from attempts to steal money from online bank accounts with malware

110,229

customers protected from ransomware attacks

79,485,155

malicious and potentially unwanted objects detected

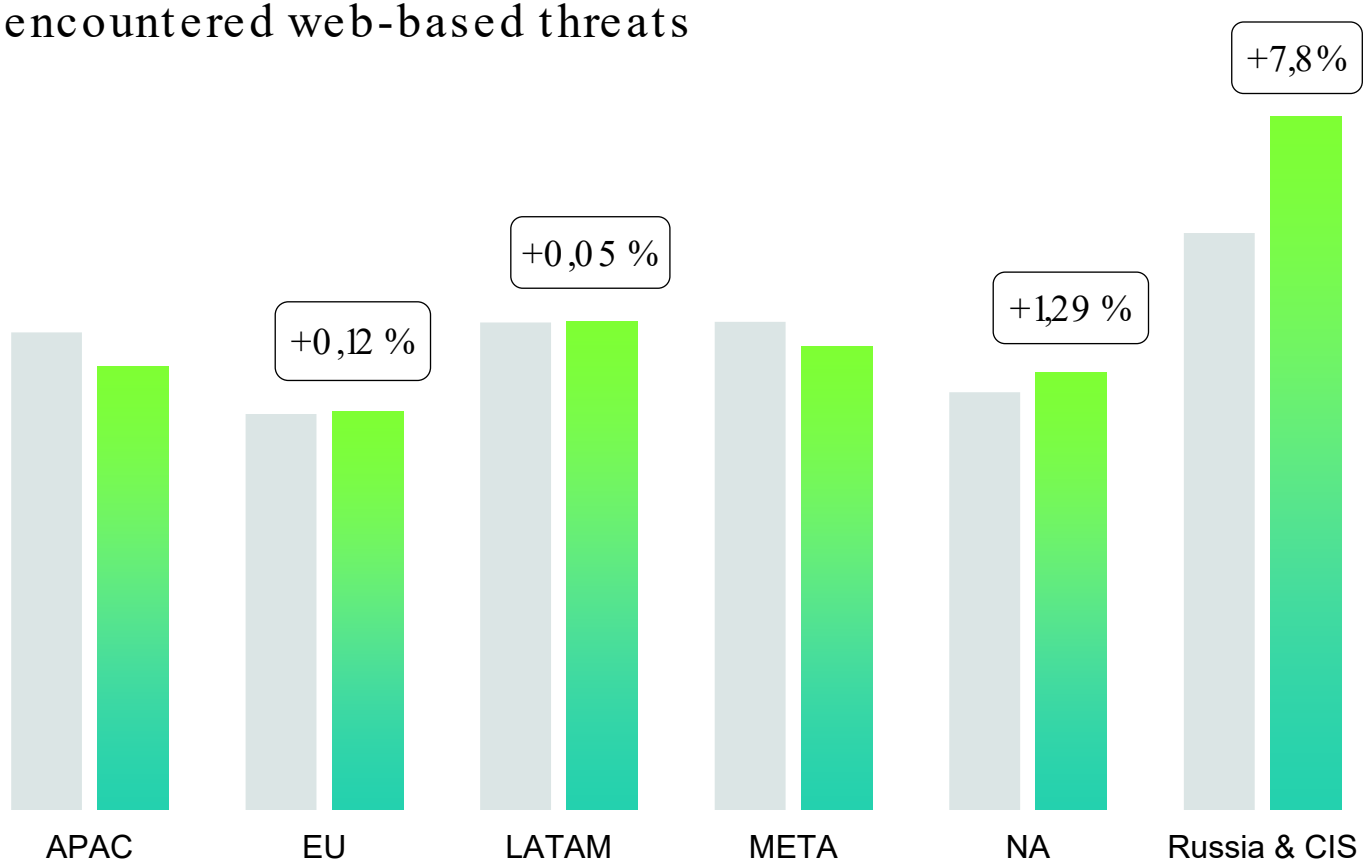
The data is based on detection notifications of Kaspersky products received from users who consented to providing statistical data

Relative attack rate (attacked users / all users)

2023 H1

2022

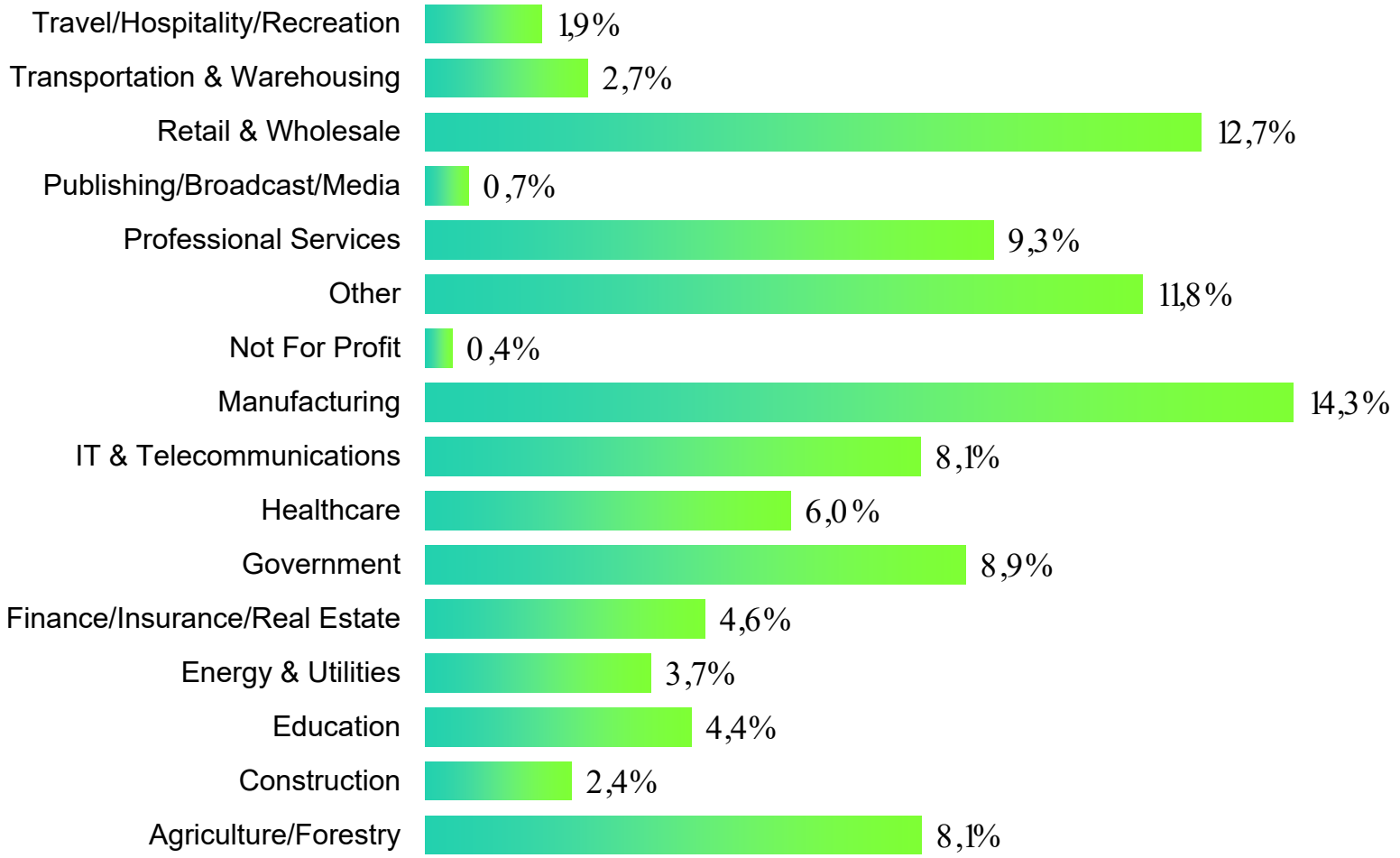
Regions by % of Kaspersky customers encountered web-based threats



The data is based on detection notifications of Kaspersky products received from users who consented to providing statistical data.

Attacks by industries

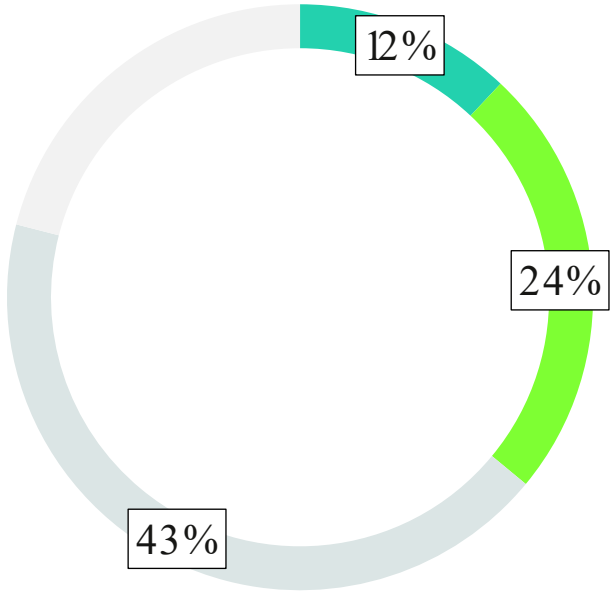
2023 H1



The data is based on detection notifications of Kaspersky products received from users who consented to providing statistical data.

IR statistics (2022)

Most popular attack vectors



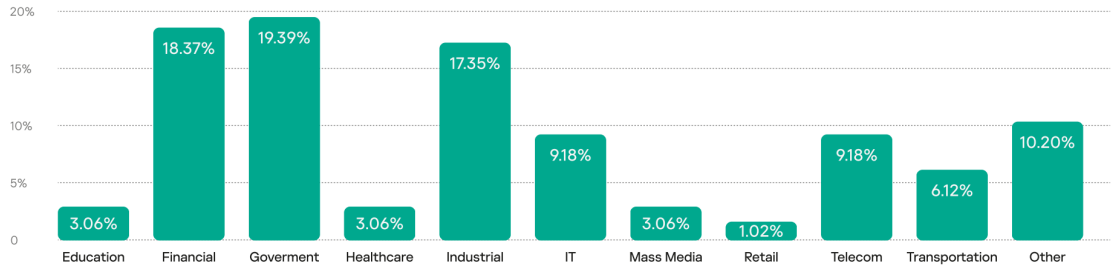
Exploit Public Facing Apps

Compromised Accounts

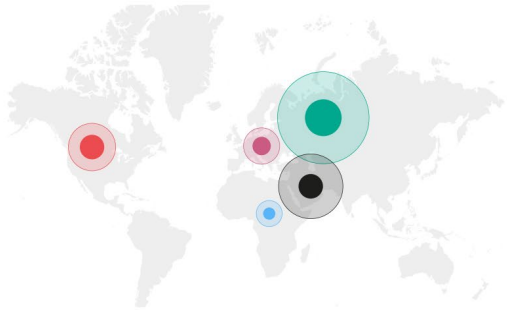
Malicious email

Other

Verticals and industries by IR cases



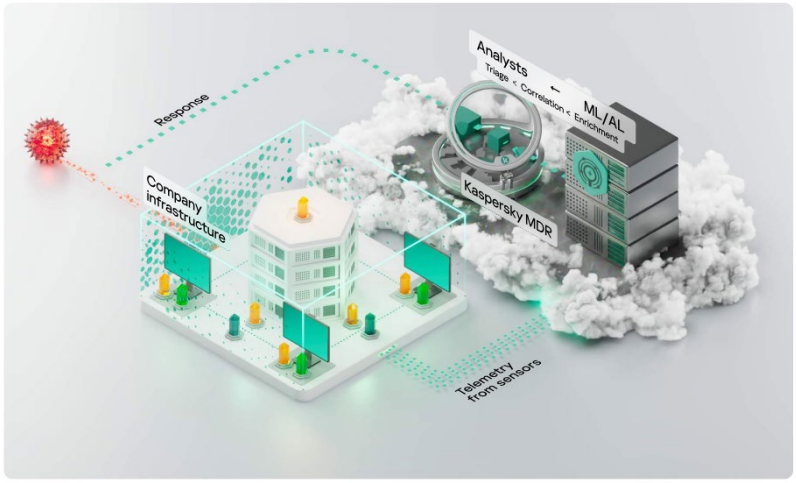
Geography of IR cases



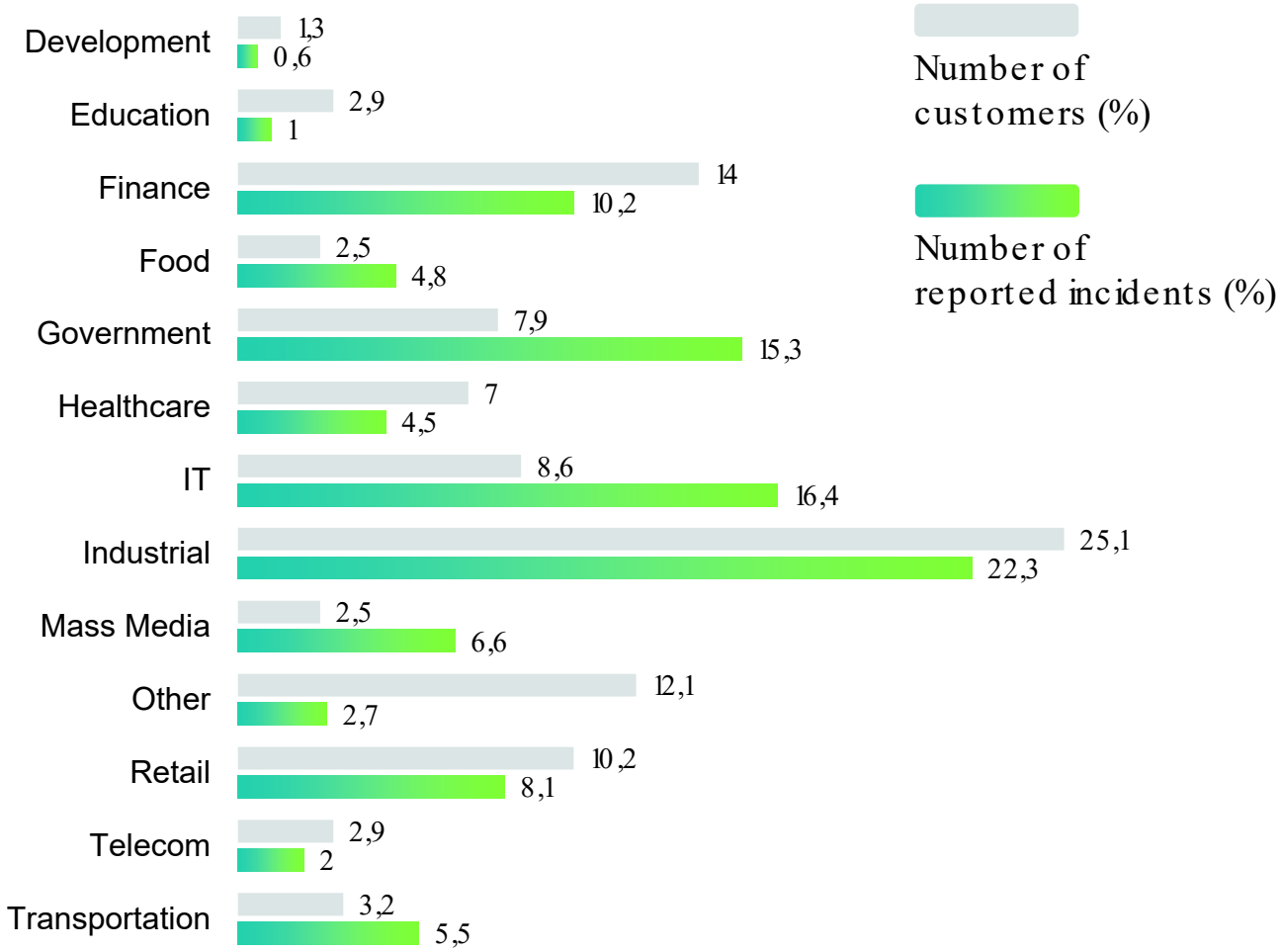
Region	%
CIS	45.9
ME	22.5
Americas	14.3
EU	13.3
Africa	4.1

The data is based on Incident Response cases by Kaspersky Global Emergency Response Team in 2022

Kaspersky Managed Detection and Response statistics (2022)



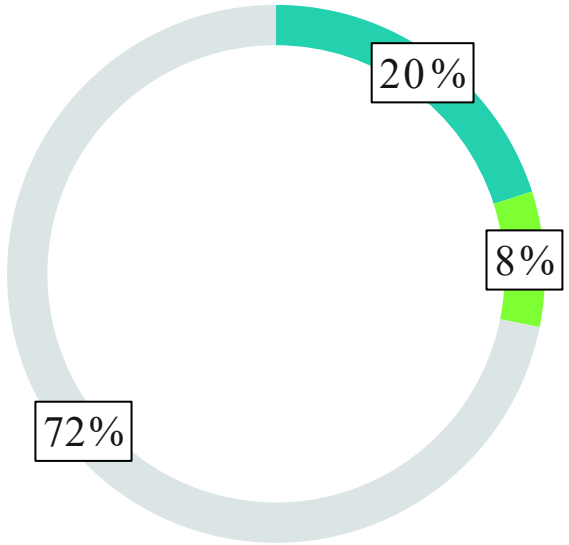
Key regions



The data is based on incidents reported to customers of Kaspersky Management Detection and Response service in 2022

Kaspersky Managed Detection and Response statistics (2022)

Reported incidents by severity

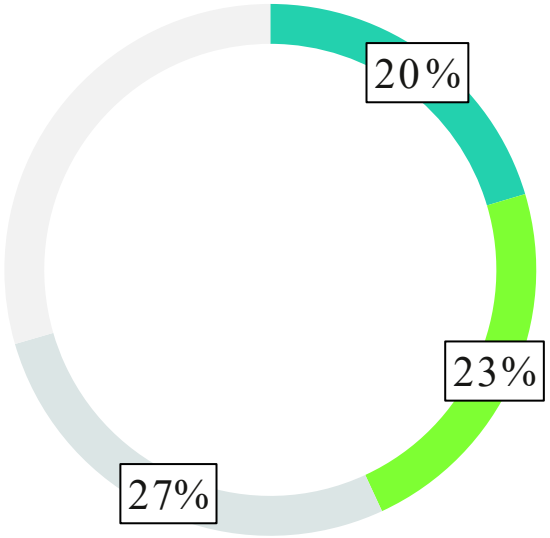


Low

High

Medium

Most used techniques



Account Manipulation

Valid Accounts

Exploitation of Remote Services

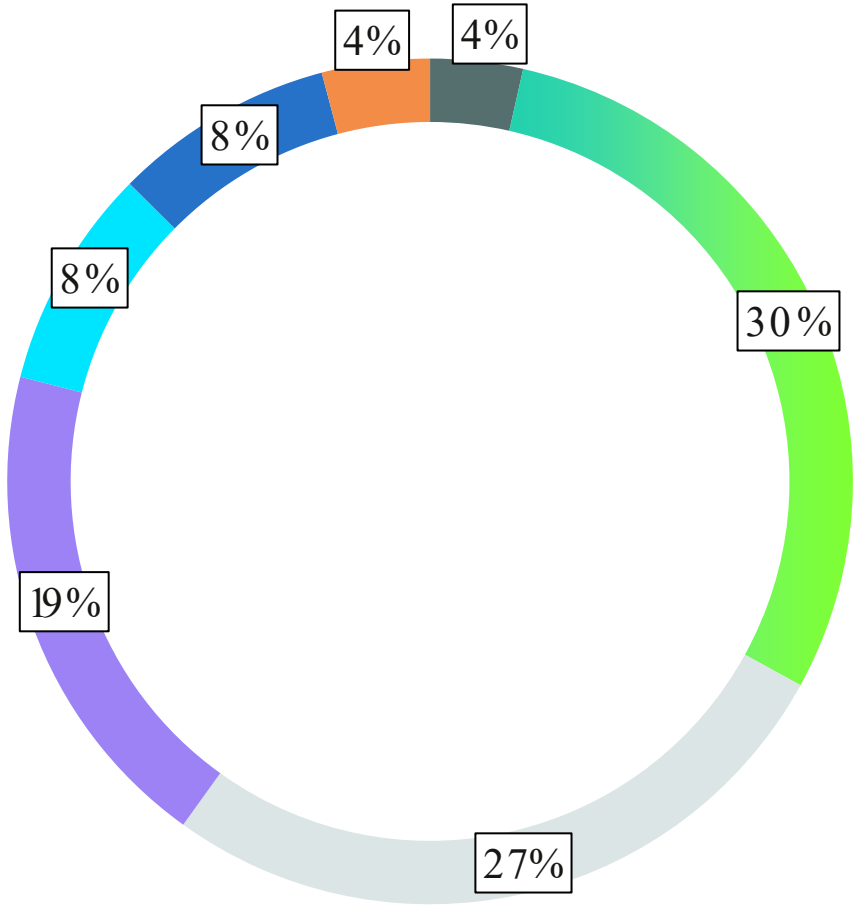
Other

The data is based on incidents reported to customers of Kaspersky Management Detection and Response service in 2022

Kaspersky Managed Detection and Response statistics (2022)

High severity incident root causes

- APTs
- APT traces
- Insider
- Malware
- Critical vulnerabilities
- Red Teaming
- Social engineering



The data is based on incidents reported to customers of Kaspersky Management Detection and Response service in 2022

Phishing & spam – main numbers (2023 H1)

41.69% of all emails around the world and **41.49%** of all emails in the Russian segment of the internet were spam

31,064,405
malicious email attachments blocked

312,195,337
attempts to follow phishing links blocked

2,366,406
attempts to follow phishing links were associated with Telegram account hijacking

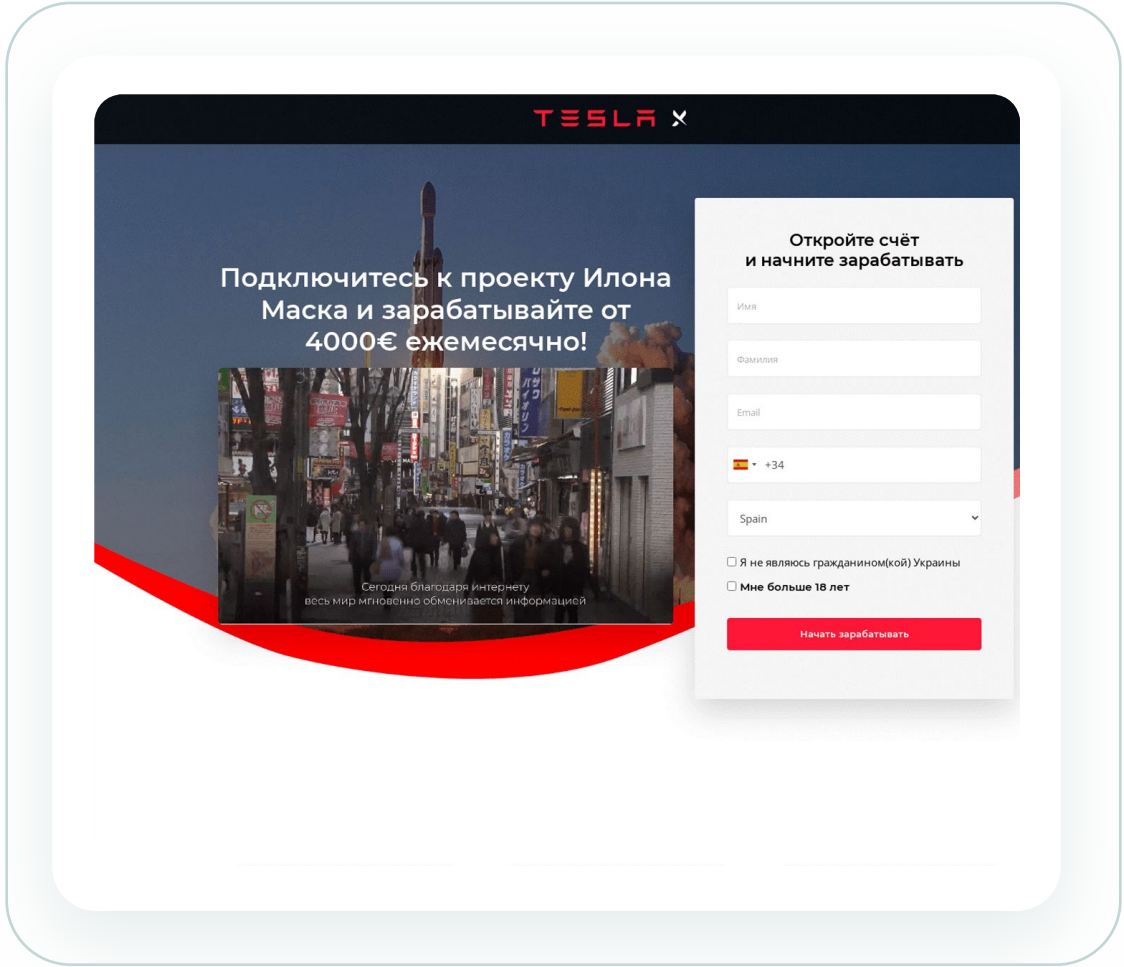
The data is based on detection notifications of Kaspersky products received from users who consented to providing statistical data.

Phishing – examples – fake investments

Elon Musk's name is often used by scammers in RU segment

This scam attack lures victims with the fake investment site in Russian

Obviously, once victim "tops up the account" money will go to the scammers

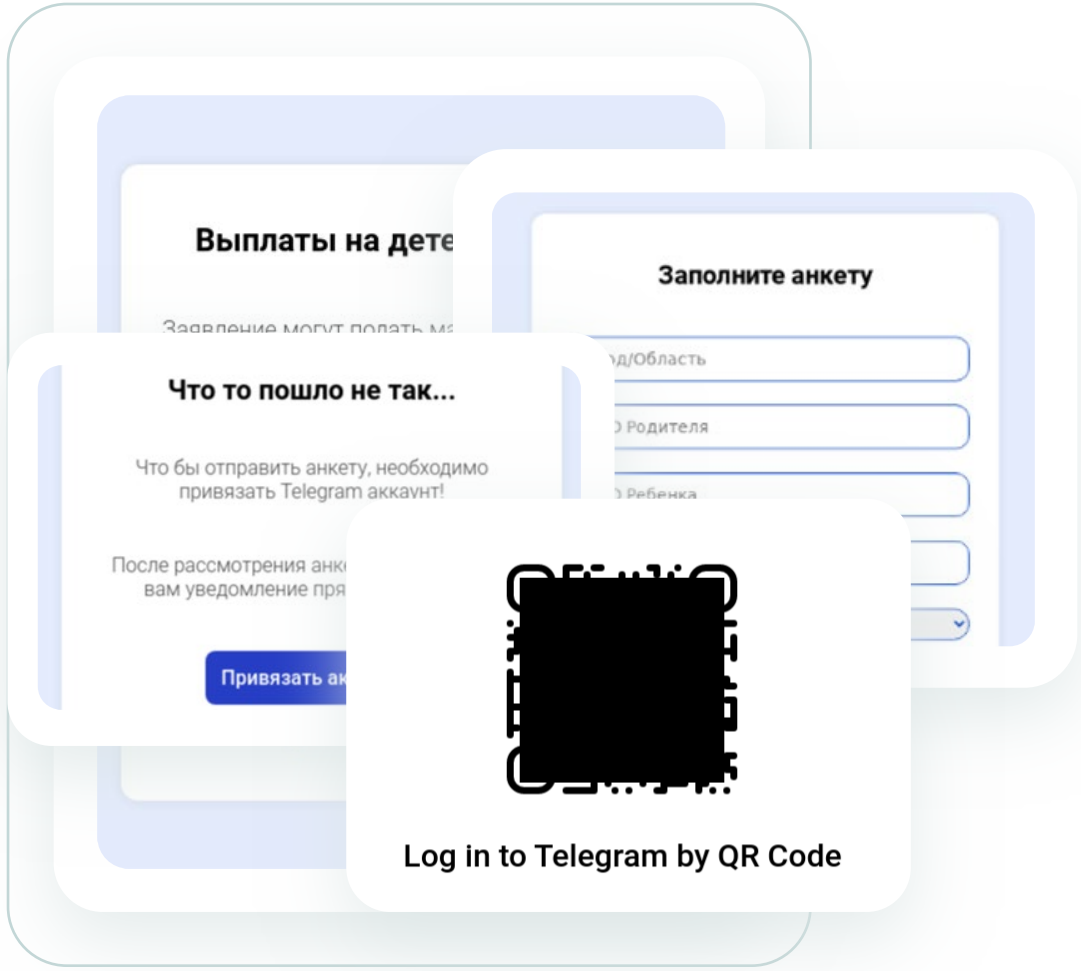


Phishing – examples – fake form to take over victim's Telegram account

Fake form to receive a payment for children under 18

It imitates an error and lures victim to scan the provided QR code with his Telegram app

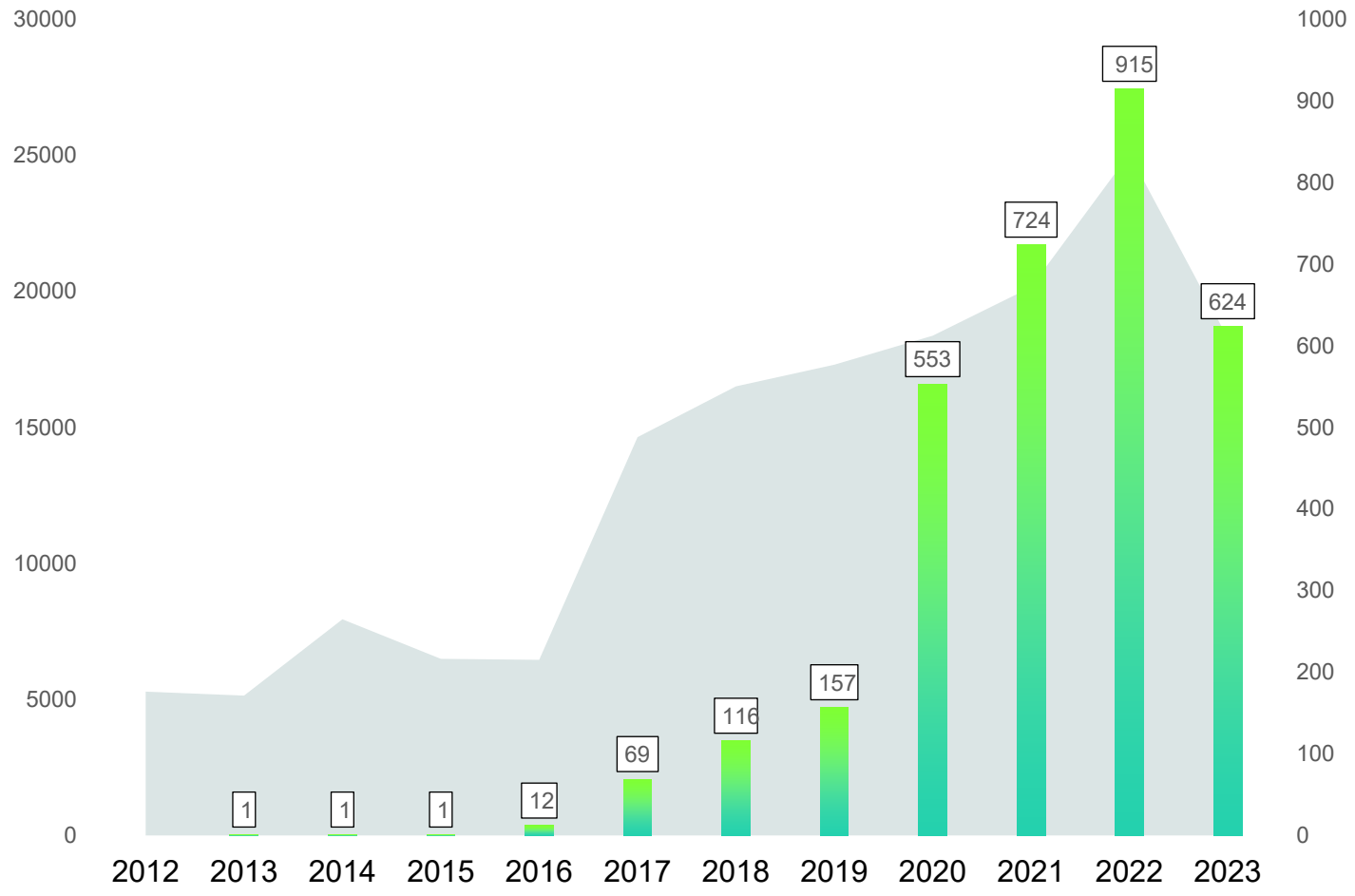
If victim does that, his/her Telegram account will be taken over



Vulnerabilities

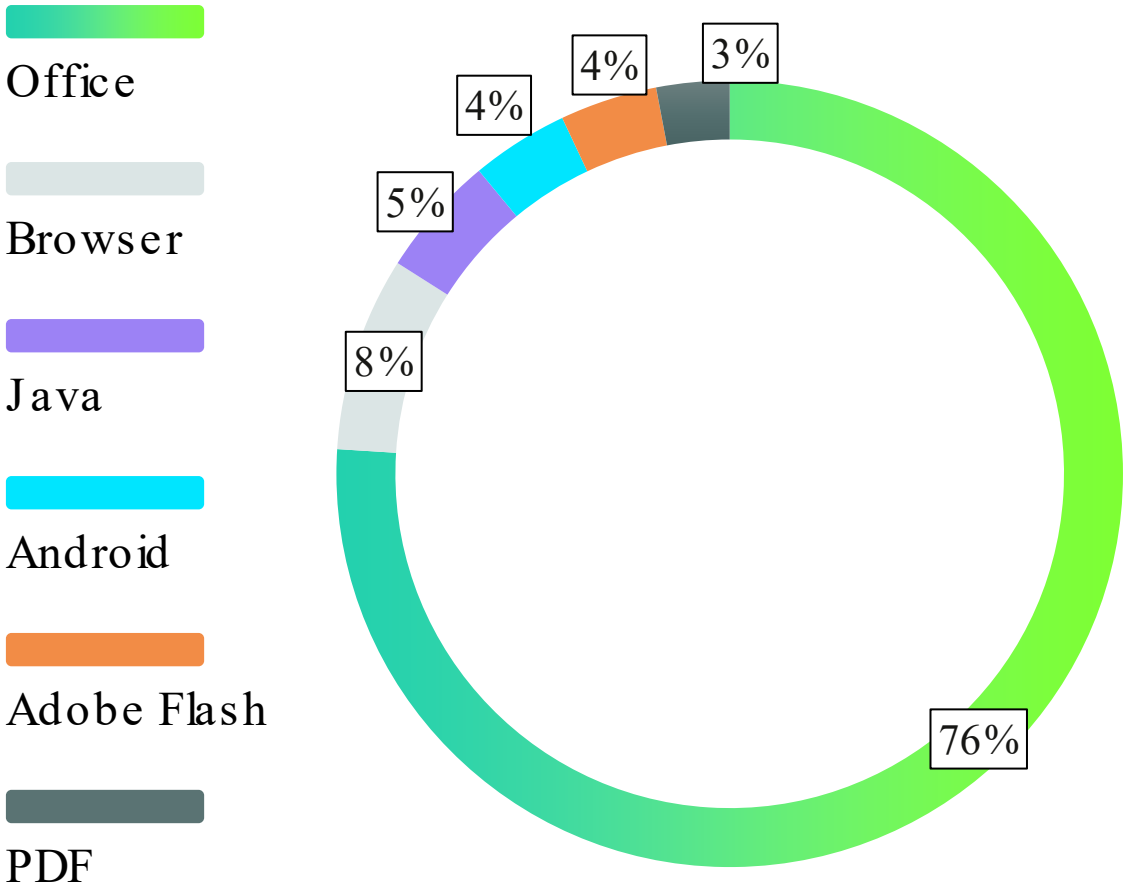
CVEs

Critical CVE



The chart is based on the data is from cve.mitre.org

Vulnerabilities – Q2 2023 – most exploited software



Most actively exploited vulnerabilities (on EP):

CVE-2017-11882 CVE-2018-0802

RCE in MS Office Equation Editor

CVE-2017-0199

RCE in MS Office Word/WordPad

CVE-2017-8570

RCE in MS Office, exploited via specifically crafted HTA script

The data is based on detection notifications of Kaspersky products received from users who consented to providing statistical data.

Most actively exploited vulnerabilities (on EP):

CVE-2017-11882 CVE-2018-0802

RCE in MS Office Equation Editor

CVE-2017-0199

RCE in MS Office Word/WordPad

CVE-2017-8570

RCE in MS Office, exploited via specifically crafted HTA script

Notable new vulnerabilities:

CVE-2023-34362 CVE-2023-35036 CVE-2023-35708

a group of CVEs in MoveIT Transfer software, actively used by Clop ransomware gang; almost 1000 organizations affected

CVE-2023-27350

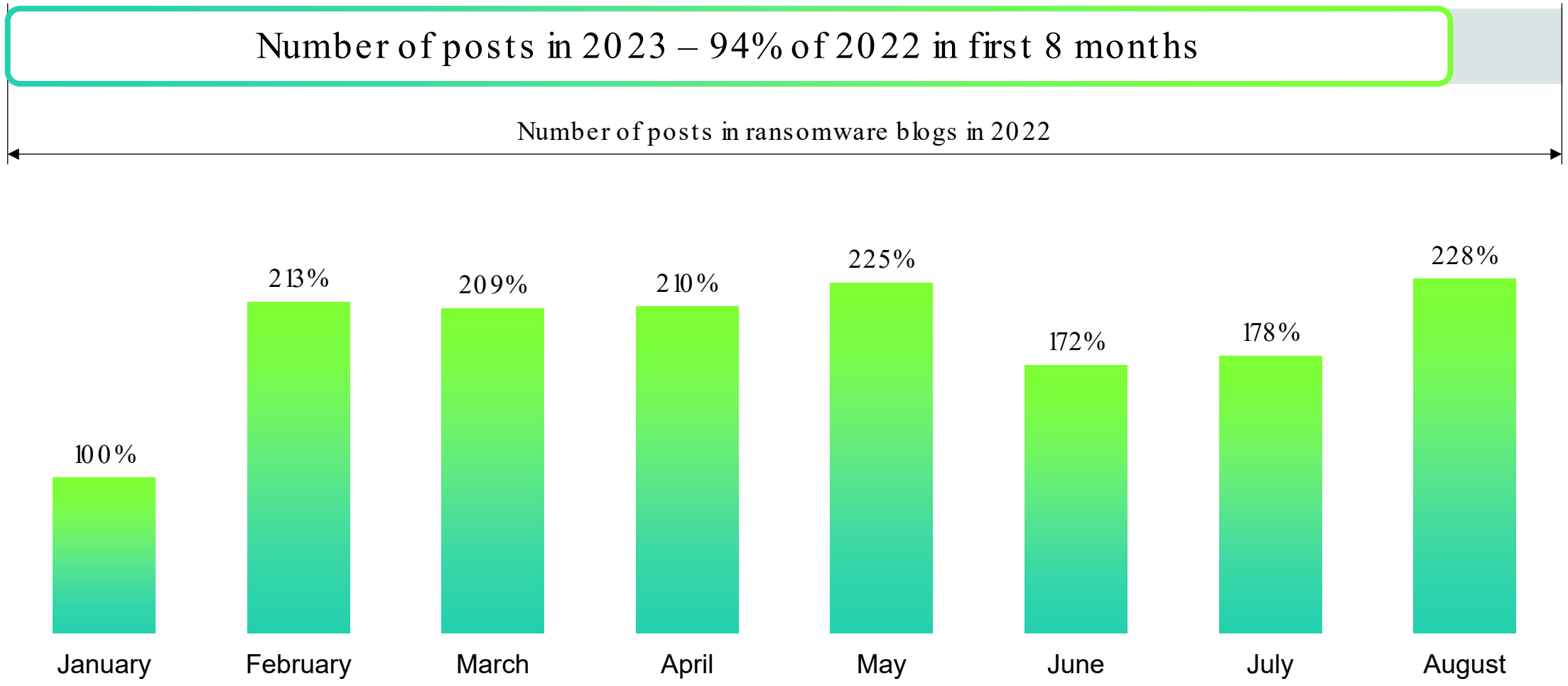
in PaperCut software, actively exploited by Bloody group

CVE-2023-28252 Learn more

Windows vulnerability used in Nokoyawa ransomware attacks. First reported by Kaspersky (Boris Larin).

The data is based on detection notifications of Kaspersky products received from users who consented to providing statistical data.

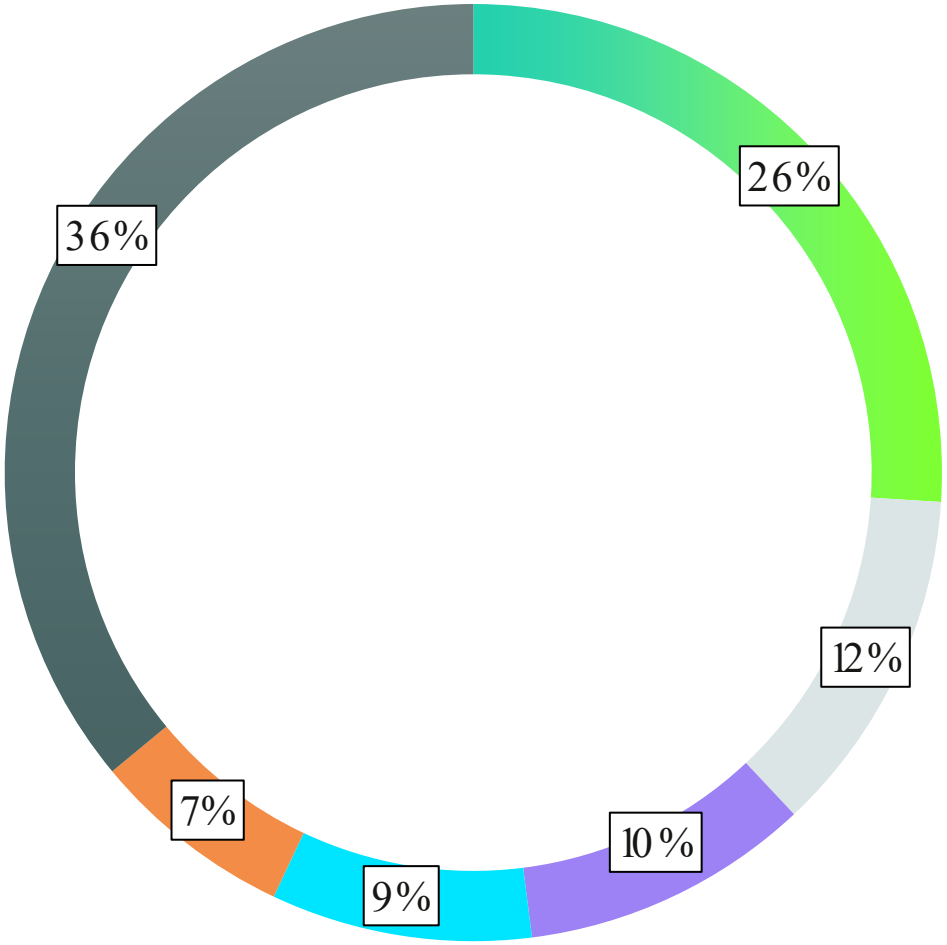
New posts on ransomware blogs (aka data leak sites, DLS) per month, dynamics, 2023 H1



The data is based on detection notifications of Kaspersky products received from users who consented to providing statistical data.

Ransomware – DLS statistics (2023 H1)

The diagram reflects the most prolific extortion gangs, that is, the ones that added the largest numbers of victims to their data leak sites (DLS).



Lockbit
Clop
Vice Society
Black Basta
BlackCat/ ALPHV
Other

Ransomware – initial vectors and tools

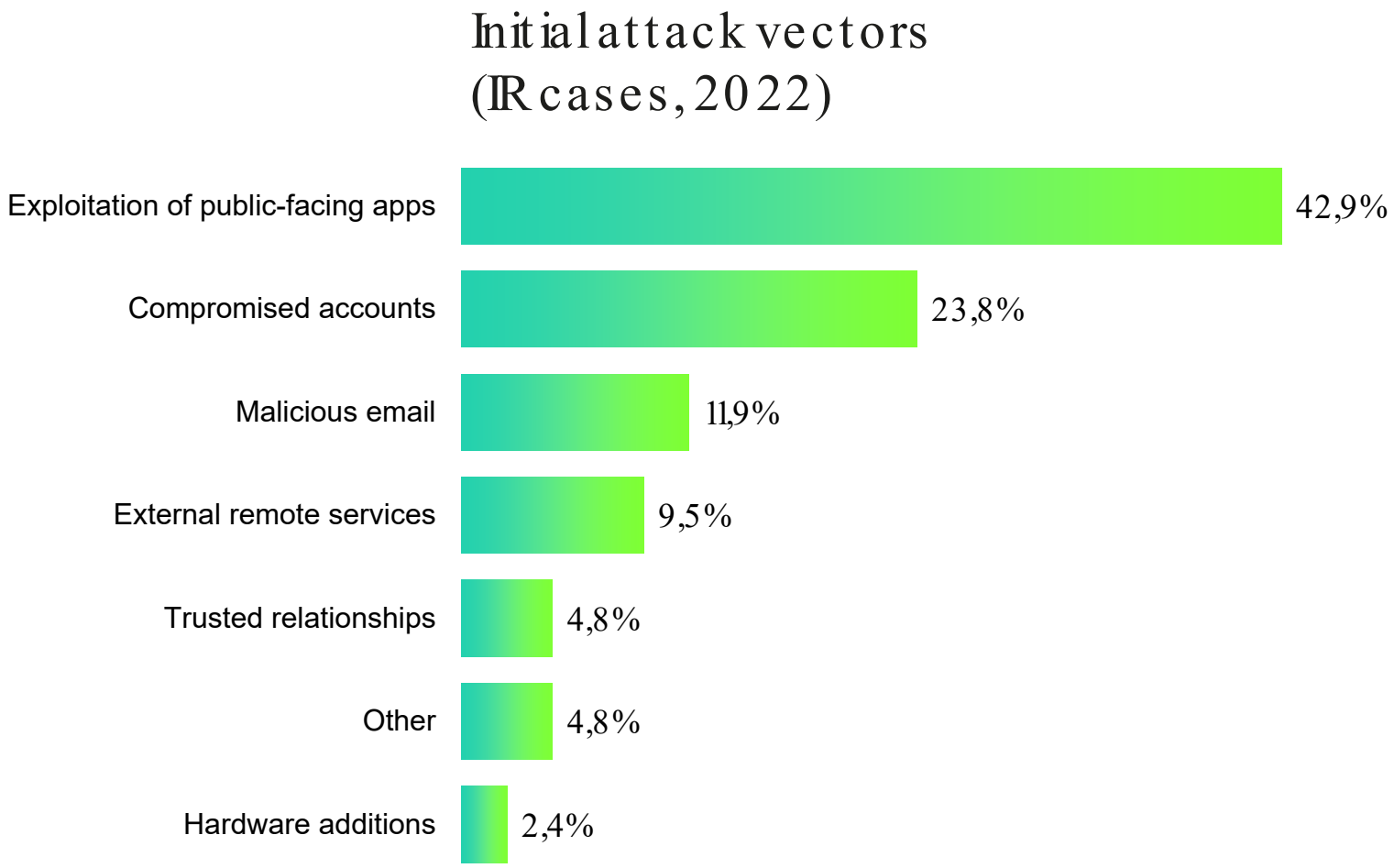
Attackers often use:

PowerShell
to collect data

Mimikatz
to escalate privileges

PsExec
to escalate privileges

Cobalt Strike
frameworks like for all stages of attack



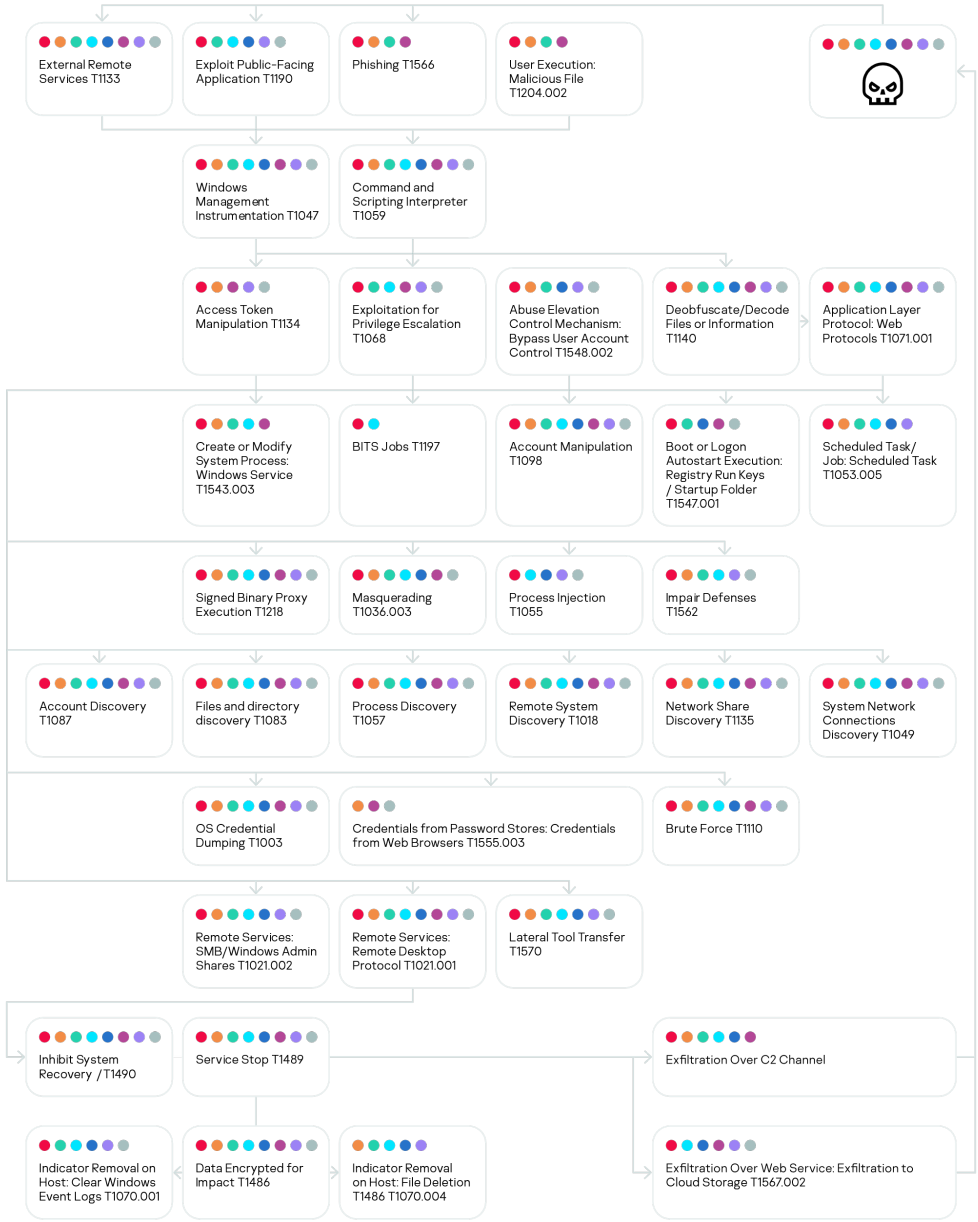
Ransomware – initial vectors and tools

The hateful eight:

Kaspersky's guide to modern ransomware groups' TTPs

Learn more

- Conti/Ryuk
- Clop (TA505)
- Lockbit 2.0
- BlackByte
- Pysa
- Hive
- RagnarLocker
- BlackCat



New cases of supply chain attacks continue to emerge

Not just an infostealer: Gopuram backdoor deployed through 3CX supply chain attack

APT REPORTS 03 APR 2023 4 minute read

GREAT WEBINARS

13 MAY 2021, 1:00PM
GReAT Ideas. Bala
BORIS LARIN, DENIS LEGEZO

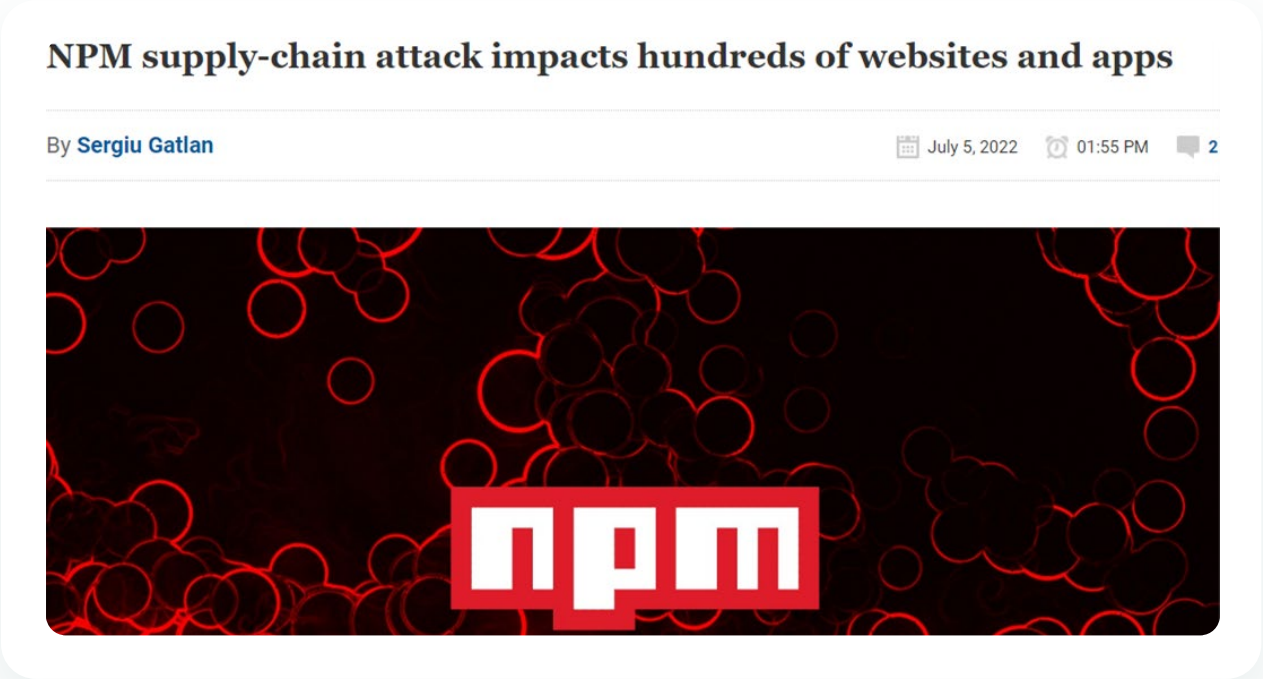
26 FEB 2021, 12:00PM
GReAT Ideas. Gree
JOHN HULTQUIST, BRIAN BARTHO
SUGURU ISHIMARU, VITALY KAML
YUSUKE NIWA, MOTOHIKO SATO

INCIDENTS

LofyLife: malicious npm packages steal Discord tokens and bank card data

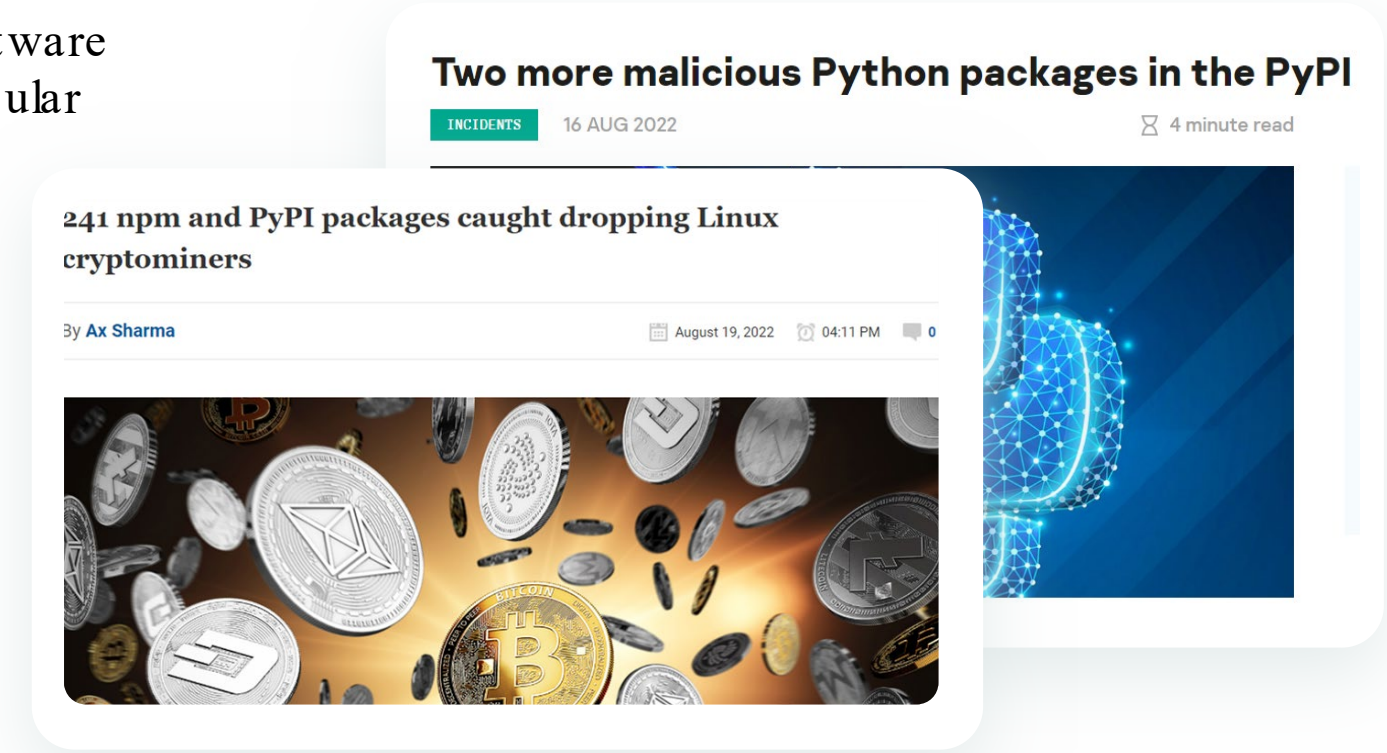
28 JUL 2022 1 minute read

Open source software brings supply chain risks



Vulnerabilities discovered in 35,000+ packages in popular repositories

Malware or potentially dangerous software discovered in 4,500+ packages in popular repositories



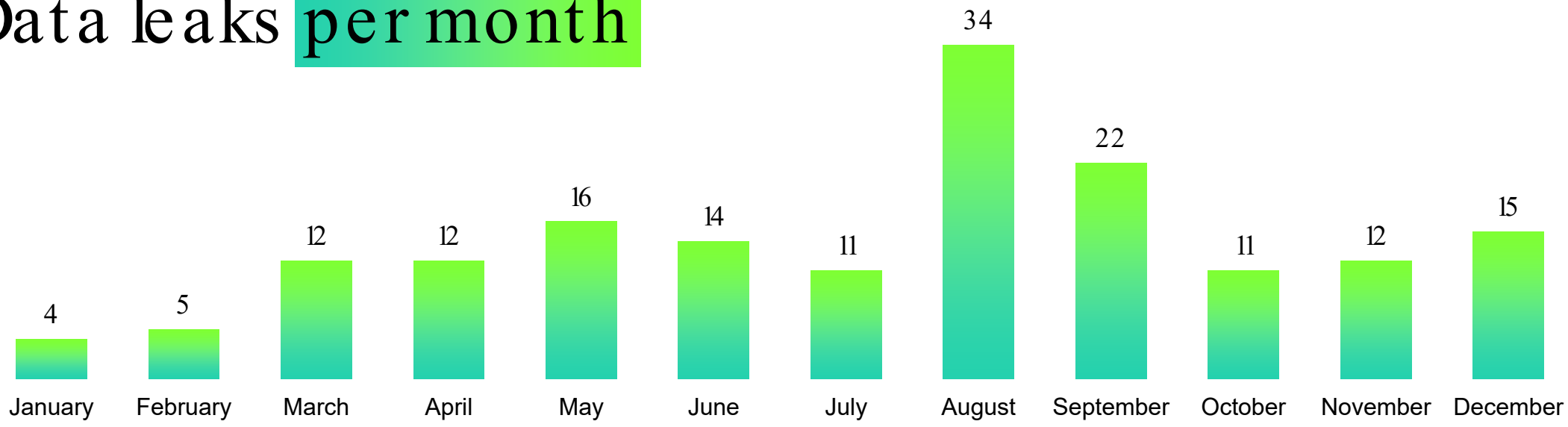
Data leaks – statistics (Russia only, 2022)

168
data leaks detected

2,126,095,255
leaked data rows found

47,663,767
leaked data records with passwords found

Data leaks per month



The data is based on research by Kaspersky Security Services and Kaspersky Digital Footprint Intelligence service

Operation Triangulation

Found by our own SOC with Kaspersky Unified Monitoring and Analysis Platform products

An unknown actor using iOS iMessage exploit since 2019

Disables iOS updates to prevent patching the bug

Memory-resident only. No persistence

Highly sophisticated cyberespionage campaign

Discovery

Detection Tool

Implant

TLDCON 2023

Thank you!

Vladimir
Kuskov

Vladimir.Kuskov@kaspersky.com