
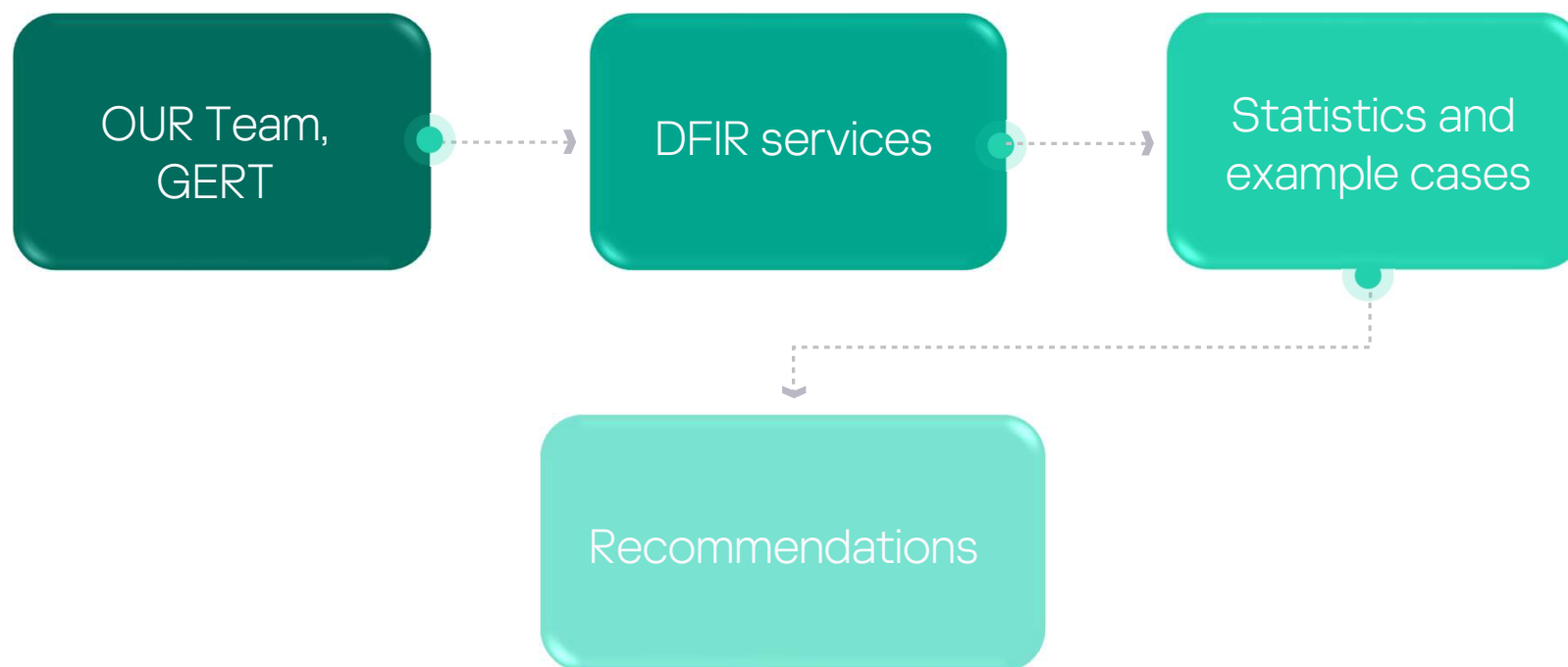


Analyzing the nature of cyber incidents in 2022



kaspersky

Ayman Shaaban
Digital Forensics and Incident
Response Manager



Kaspersky Global Emergency Response Team, **GERT**

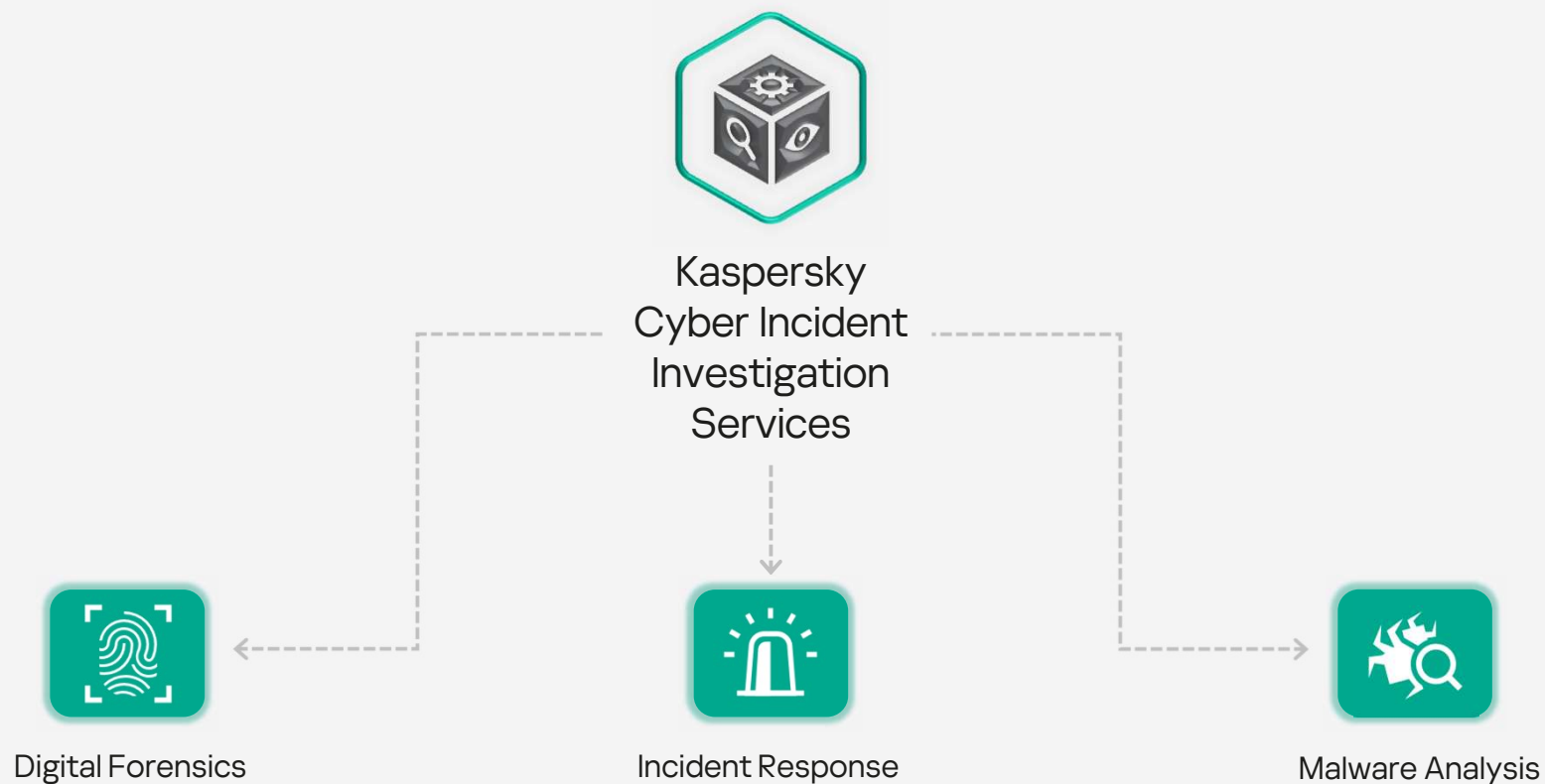
3



We speak English,
Arabic, German,
Italian, Russian,
Spanish and French
languages

Incident Response Services, Kaspersky GERT

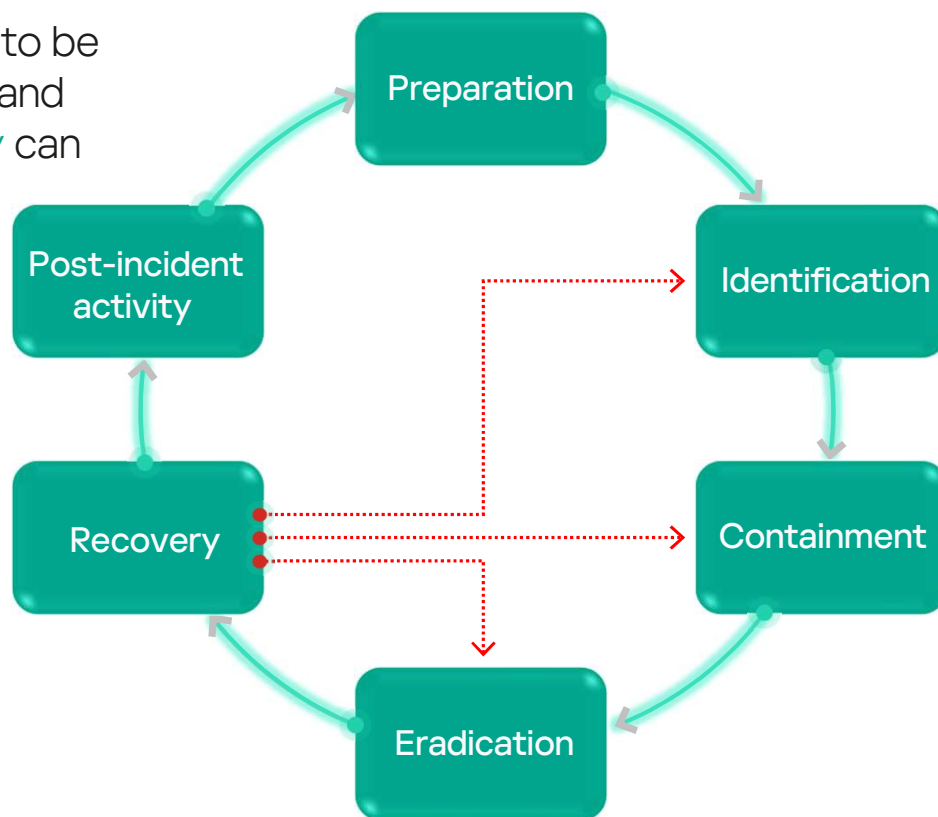
4



Read full report at:

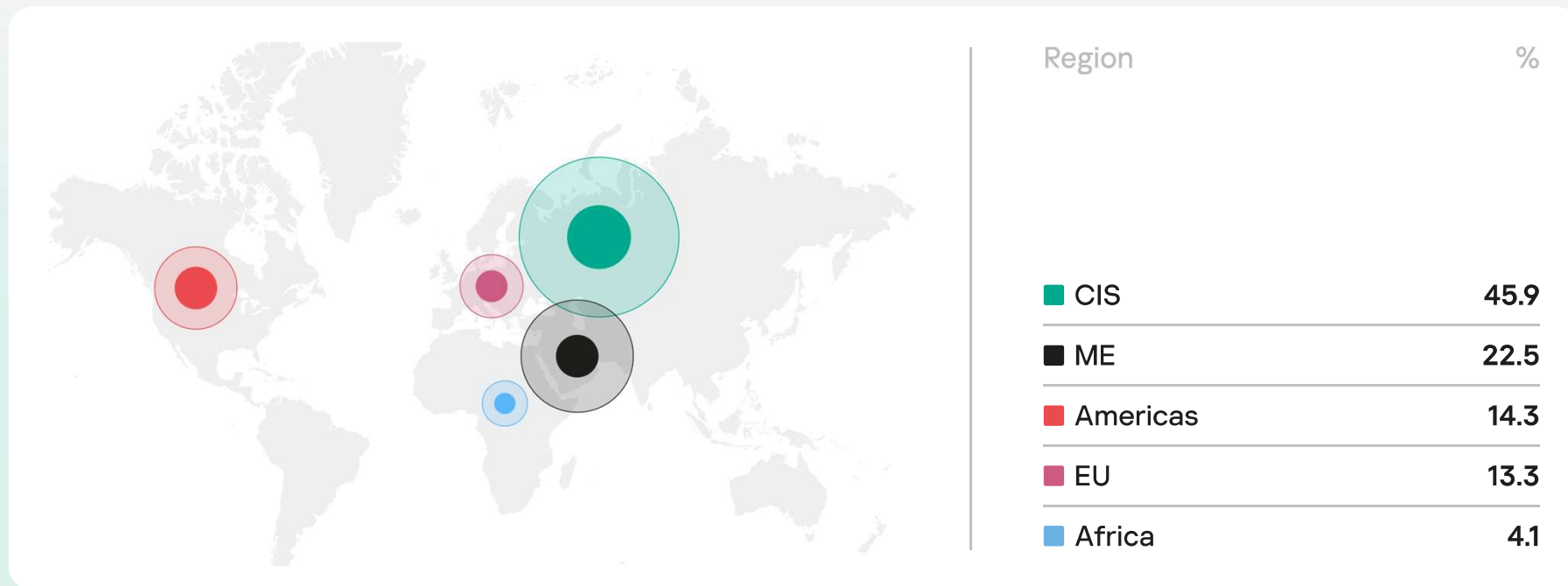
<https://securelist.com/kaspersky-incident-response-report-2022/109680/>

You need to be prepared and Kaspersky can help



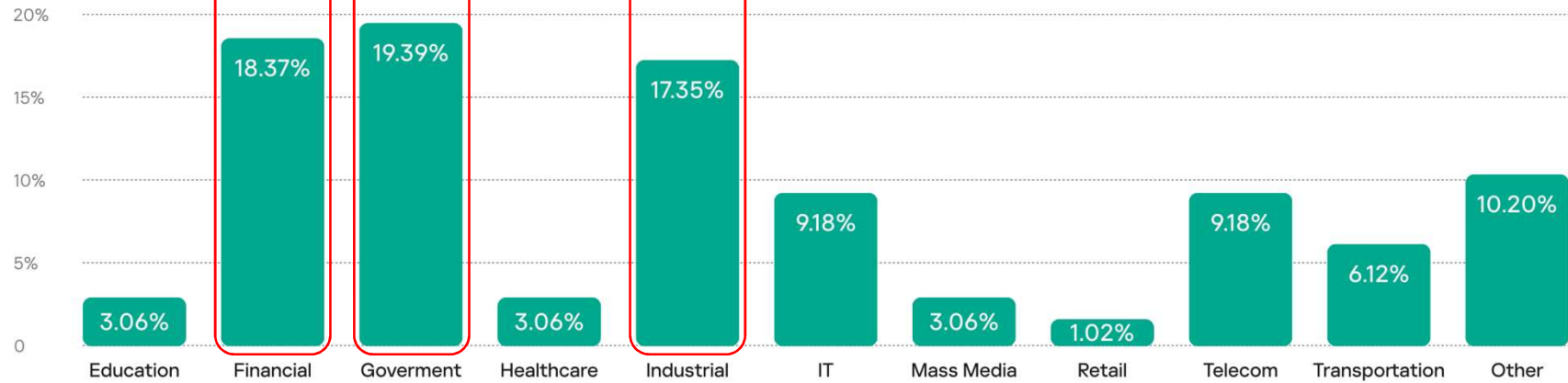
2022 Geography of Incident Responses

6



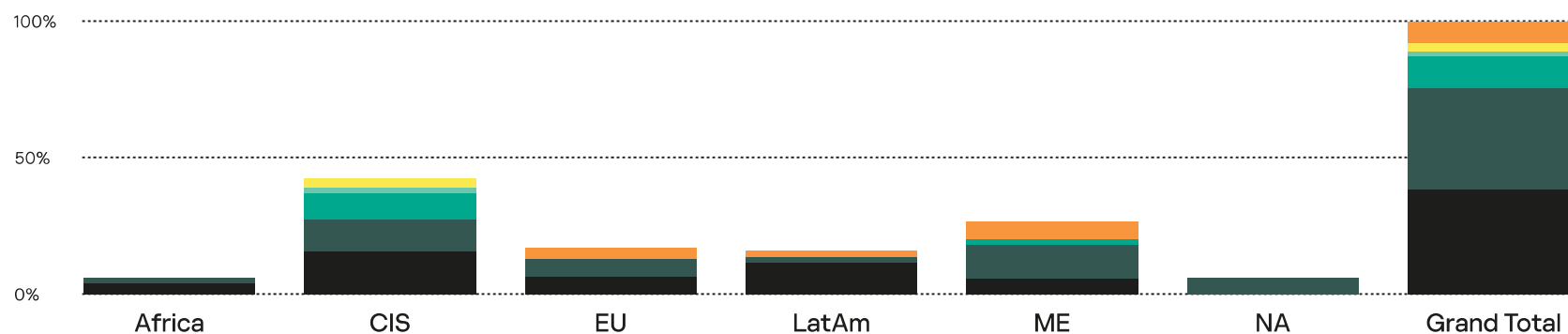
2022 Verticals and Industries

7



2022 Reasons VS Regions

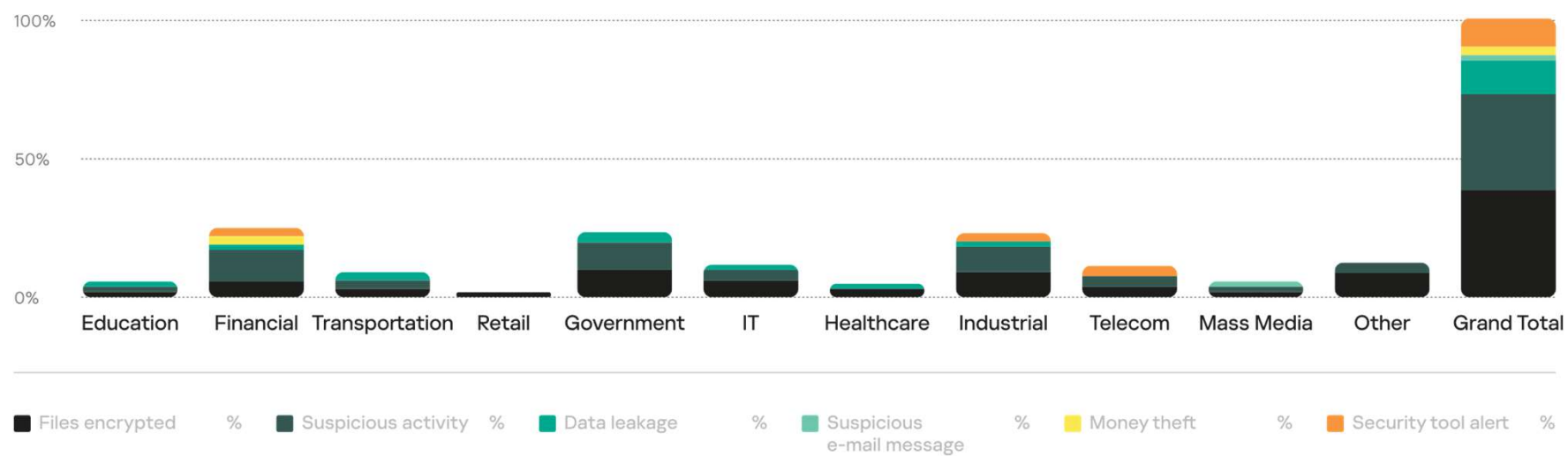
8



Files encrypted	%	Suspicious activity	%	Data leakage	%	Suspicious e-mail message	%	Money theft	%	Security tool alert	%
Africa	3.06	Africa	1.02	Africa	-	Africa	-	Africa	-	Africa	-
CIS	17.35	CIS	16.33	CIS	9.18	CIS	1.02	CIS	2.04	CIS	-
EU	6.12	EU	5.10	EU	-	EU	-	EU	-	EU	2.04
LatAm	11.22	LatAm	1.02	LatAm	-	LatAm	-	LatAm	-	LatAm	1.02
ME	4.08	ME	13.27	ME	1.02	ME	-	ME	-	ME	4.08
NA	-	NA	1.02	NA	-	NA	-	NA	-	NA	-
Grand Total	41.84	Grand Total	37.76	Grand Total	10.20	Grand Total	1.02	Grand Total	2.04	Grand Total	7.14

2022 Reasons VS Industries

9



Sample case _ Ransomware Everywhere (**Hive**)

10

REDLINE/Racoon stealer activity including privileged accounts credentials:

- Atlassian
- Corporate Email
- Corporate services

RDP – Initial access vector (Based on TA)

27/10 RDP Access on behalf of privileged domain account.

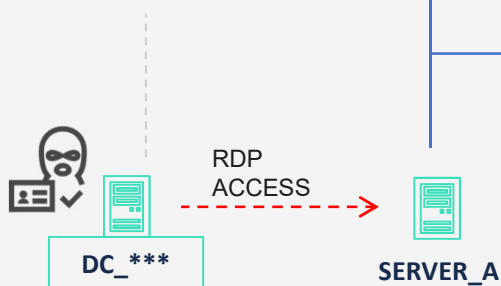
Pack.exe downloaded and executed.

04/11 **Screen connect + LogMeIn** installed

05/11 both payloads (Windows and Linux) arrive to system.

05/11/2022 Ransomware was deployed in the MS Windows infrastructure using a GPO + PSEXec

17/11/2022 A new wave of ransomware spread directed to Linux systems (ESXi). SSH access.

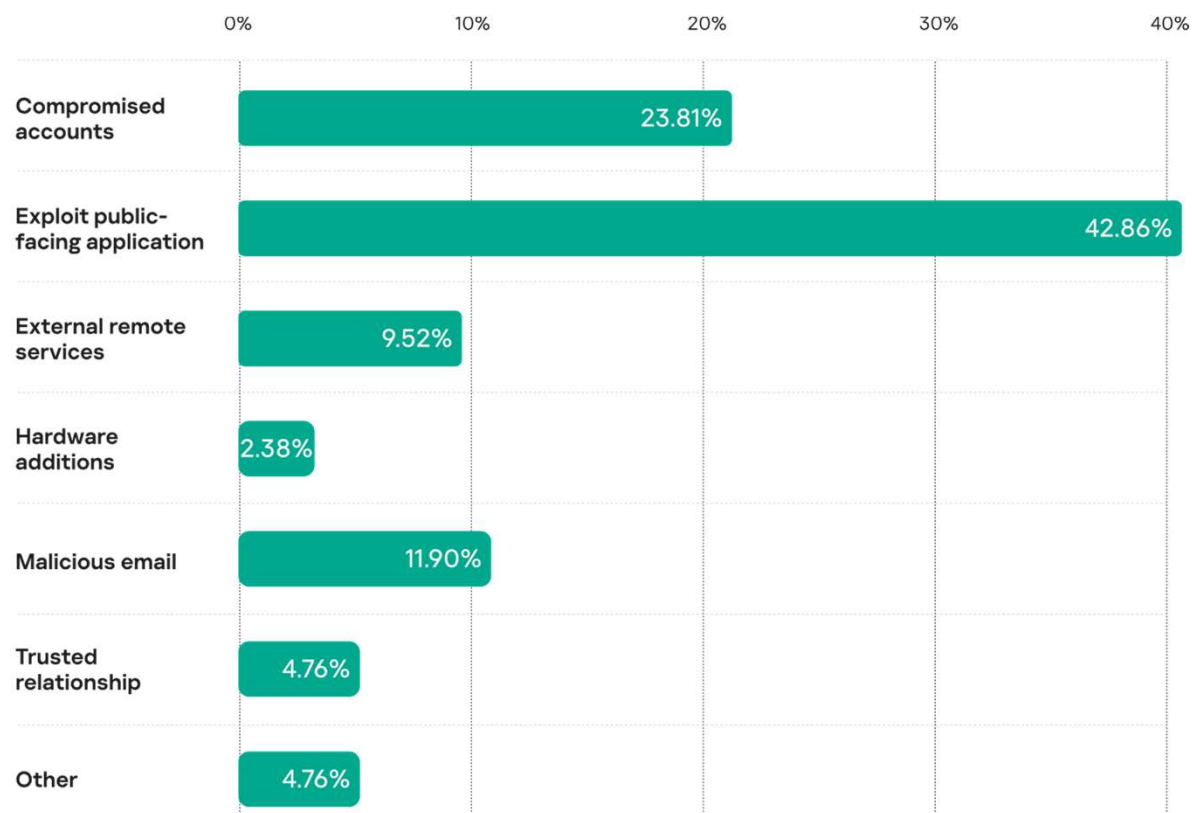


Oct 2022

Nov 2022

Initial Vectors (How Attackers Got In)

11



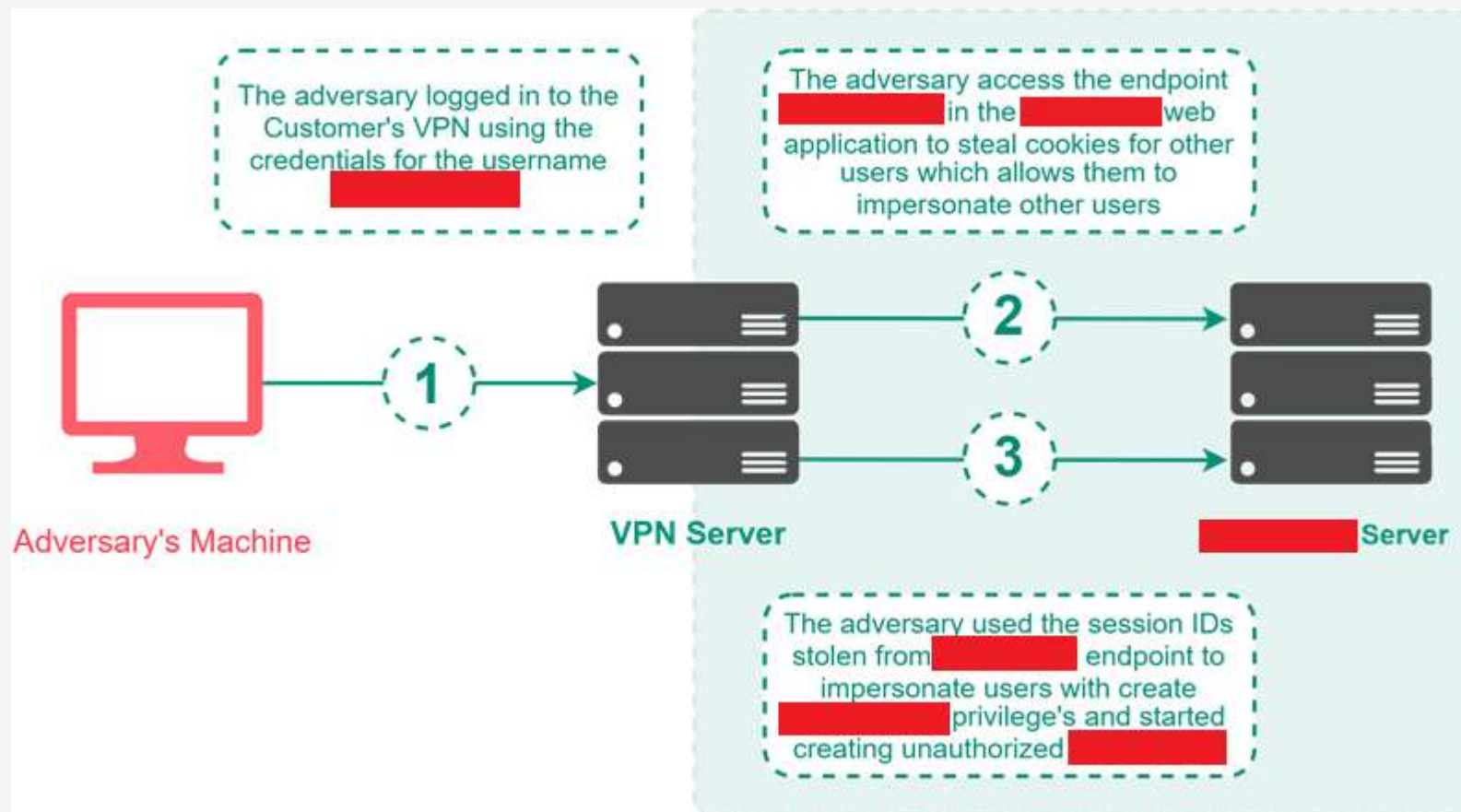
Initial Vectors (How Attackers Got In over the years)

12

	2019		2020		2021		2022	
	Place	%	Place	%	Place	%	Place	%
Exploit Public Facing Apps	1	37%	2	31.5%	1	53.6%	1	42.9%
Compromised accounts	3	13%	1	31.6%	2	17.9%	2	23.8%
Malicious e-mail	2	30%	3	23.7%	3	14.3%	3	11.9%

Sample case (**Insider with valid/compromised accounts**)

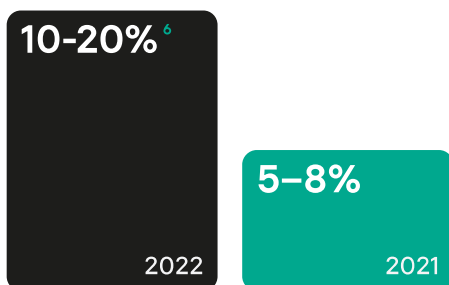
13



Distribution and frequency of tools used in incident cases

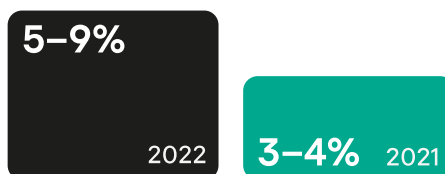
Frequent

⁶ Each tool was identified in 10-20% of incident cases



Cobalt Strike
PowerShell
Mimikatz
PsExec

Average



Advanced_IP_Scanner
ProcDump
Bitlocker
ProcessHacker

Rare

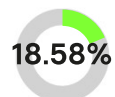


WebBrowserPassView.exe
Fast_Reverse_Proxy_FRP
AnyDesk
DiskCryptor
SMBExec

Tools Used in Attacks

15

Execution



PowerShell PsExec
SmbExec

Defense evasion



ProcessHacker PCHunter
PowerTool

Credential access



Mimikatz PowerTool
ProcDump

Discovery



Advanced IP Scanner
wmic nbtscan

Lateral Movement



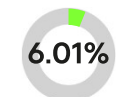
Cobalt Strike Impacket
Empire_Powershell
PowerSploit

Collection



winrar 7zip

Command and Control



RDP AnyDesk

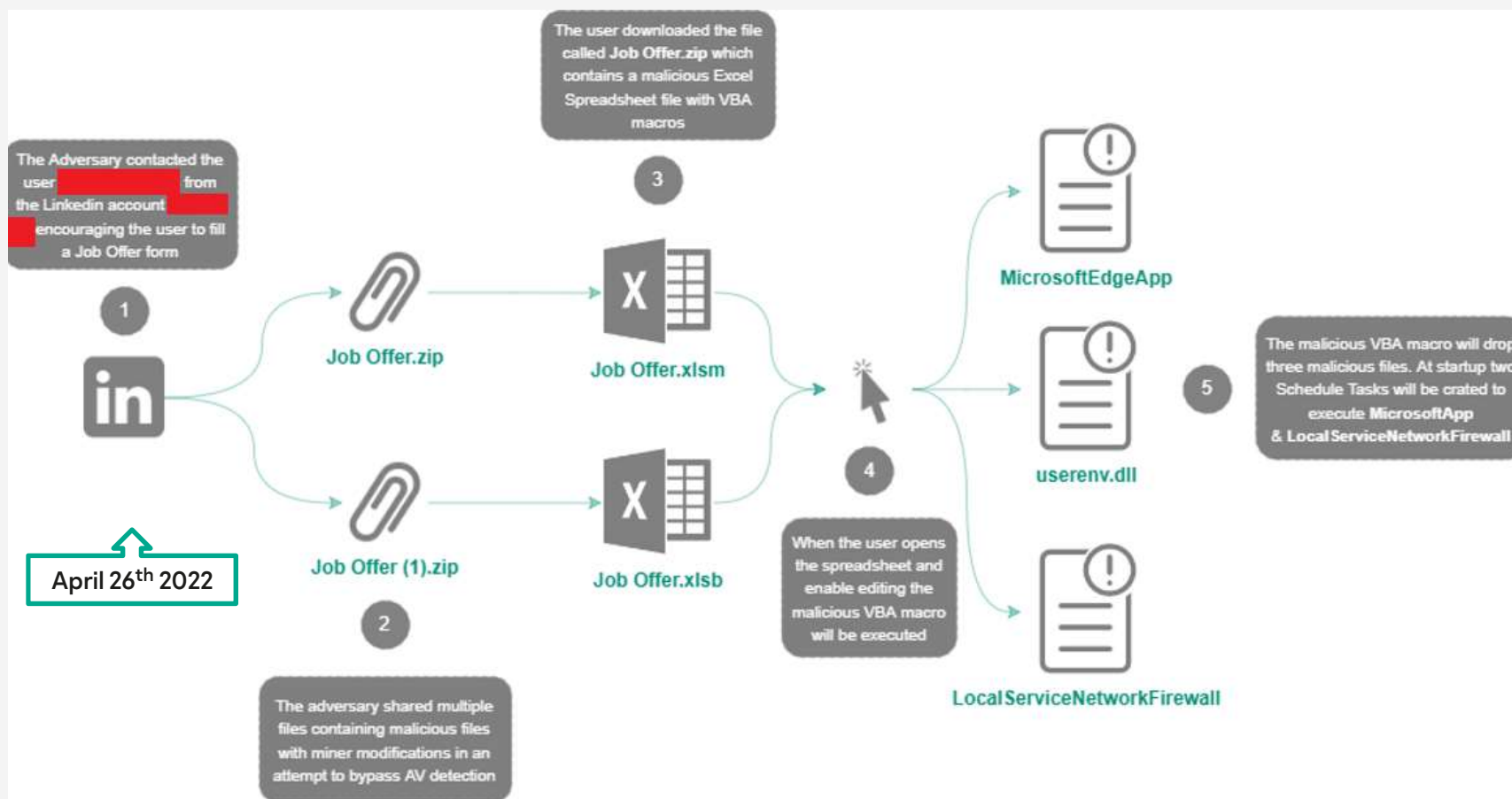
Impact



DiskCryptor BitLocker

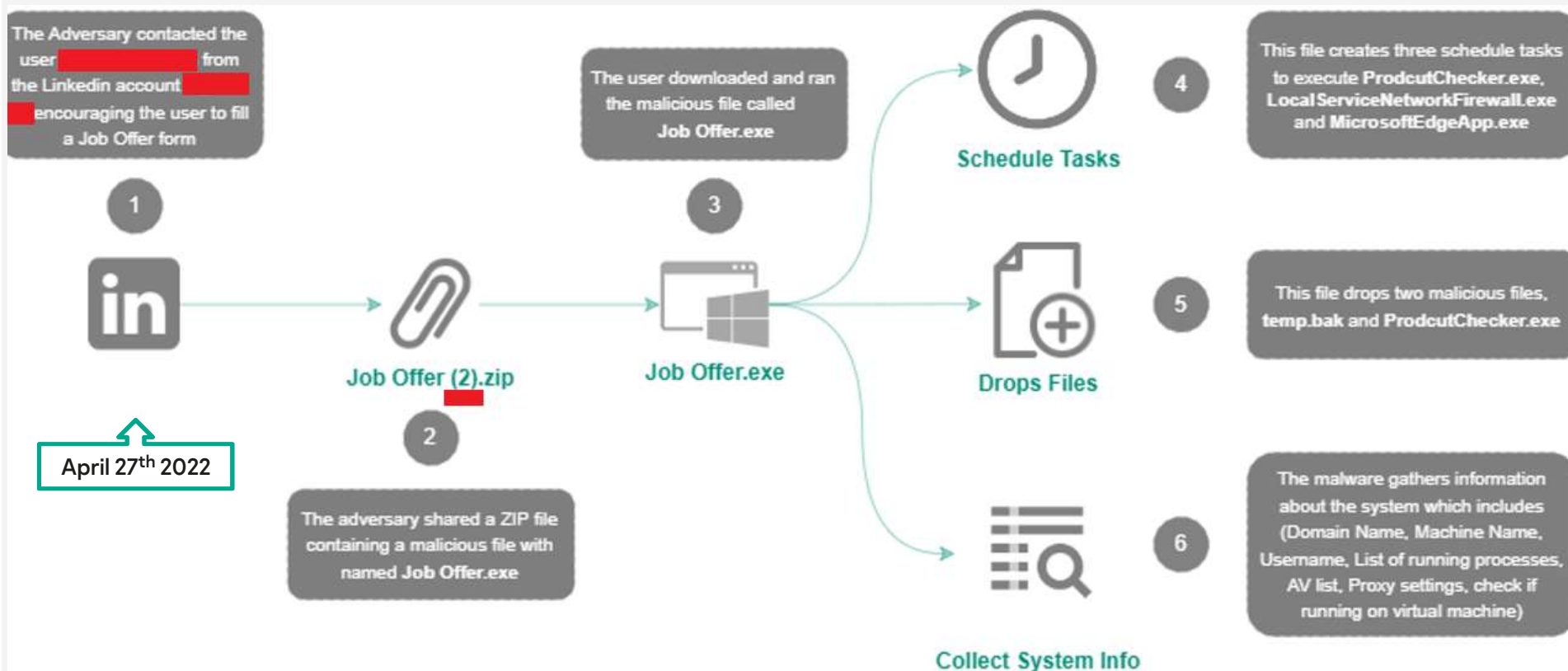
Sample case (PowerShell after social engineering and Spearphishing)

16



Sample case (PowerShell after social engineering and Spearphishing)

17



Rush

Hours and days

Attack amount



Average attack duration



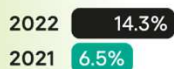
Representative impact

Ransomware



Average

Weeks



Ransomware and money theft



Long lasting

Month and longer



Data leakage and ransomware



Initial Attack Vector and Incident Response Duration

19

Initial attack vector (rated by frequency in cases)

🔄 Bruteforce

🔗 Exploitation of public-facing applications

📧 Spear phishing link

🔗 Exploitation of public-facing applications

⚡ Drive-by compromise

🔄 Bruteforce

💾 Replication through removable media

📧 Spear phishing links

🔗 Exploitation of public-facing applications

📧 Spear phishing attachment

🔄 Bruteforce

⚡ Drive-by compromise

👤 Insider

Incident response duration (time spent investigating)

Attacks that lasted
up to a week

2022	60.2 hours
2021	29.4 hours

Attacks that lasted
up to a month

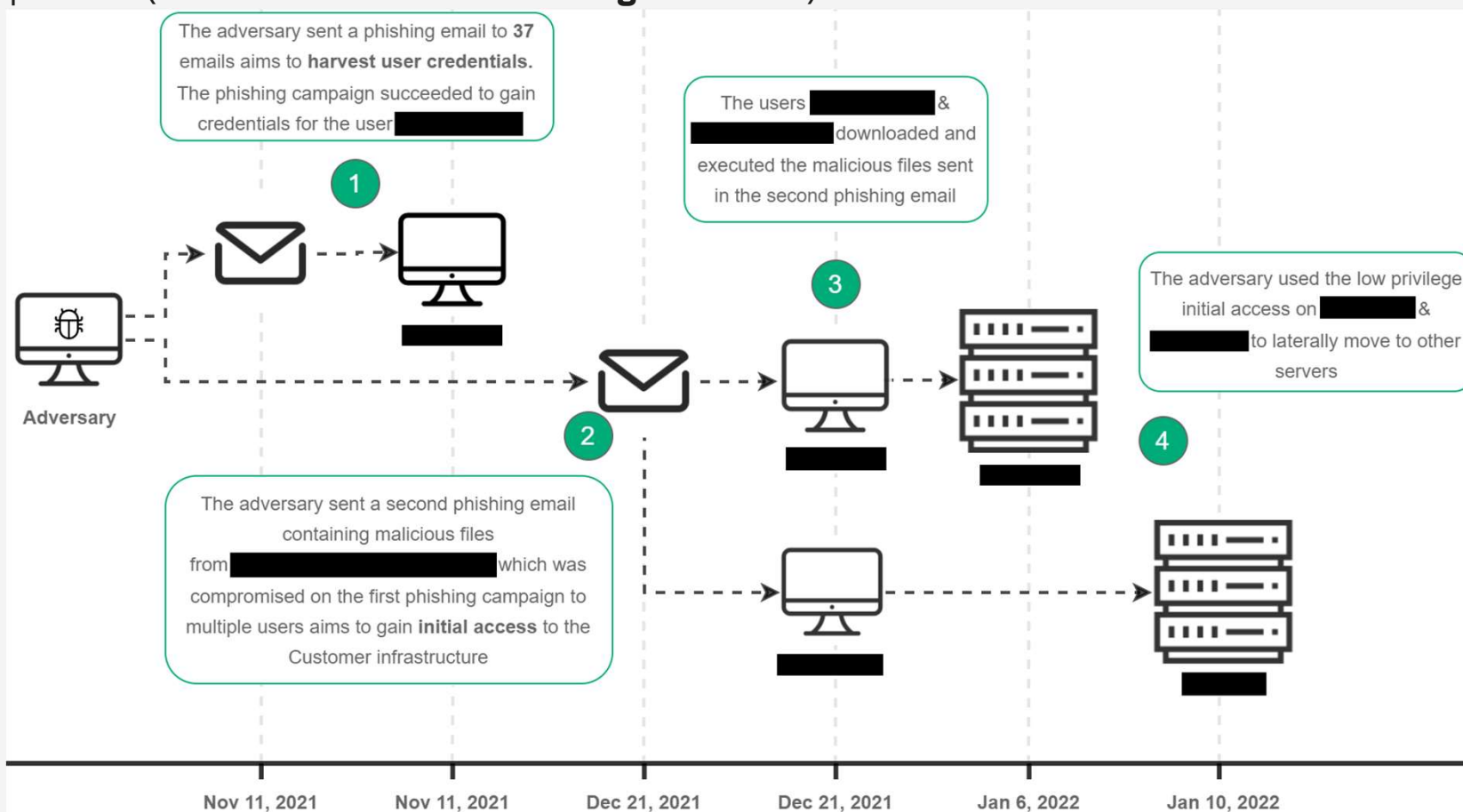
2022	67.1 hours
2021	48.3 hours

Attacks that lasted
more than a month

2022	47.8 hours
2021	60.13 hours




Sample case (**Attack Duration and investigation time**)

20



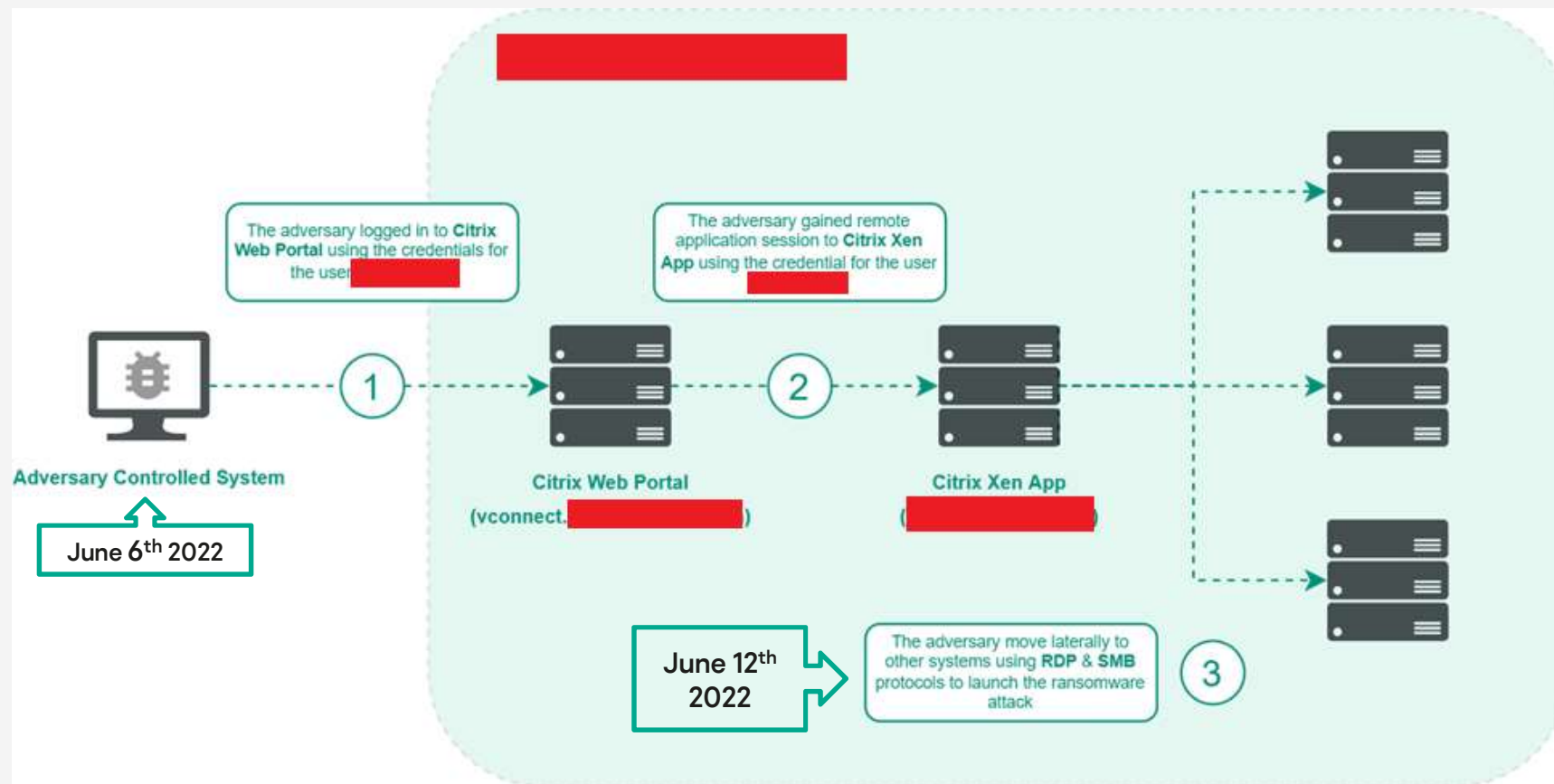
Attack Durations VS Initial Vectors (**Ransomware**)

21

Initial attack vector	Attack duration					Grand total
	Hours	Days	Weeks	Months	Years	
Compromised accounts	9.52%	2.38%	4.76%	7.14%	0.00%	23.81% 
Exploitation of public-facing applications	4.76%	14.29%	9.52%	11.90%	2.38%	42.86% 
External remote services	2.38%	4.76%	2.38%	0.00%	0.00%	9.52%
Malicious email	2.38%	2.38%	2.38%	4.76%	0.00%	11.90% 
Trusted relationships	0.00%	2.38%	0.00%	2.38%	0.00%	4.76%
Hardware additions	2.38%	0.00%	0.00%	0.00%	0.00%	2.38%
Other	2.38%	2.38%	0.00%	0.00%	0.00%	4.76%
Grand total	23.81%	28.57%	19.05%	26.19%	2.38%	100.00%

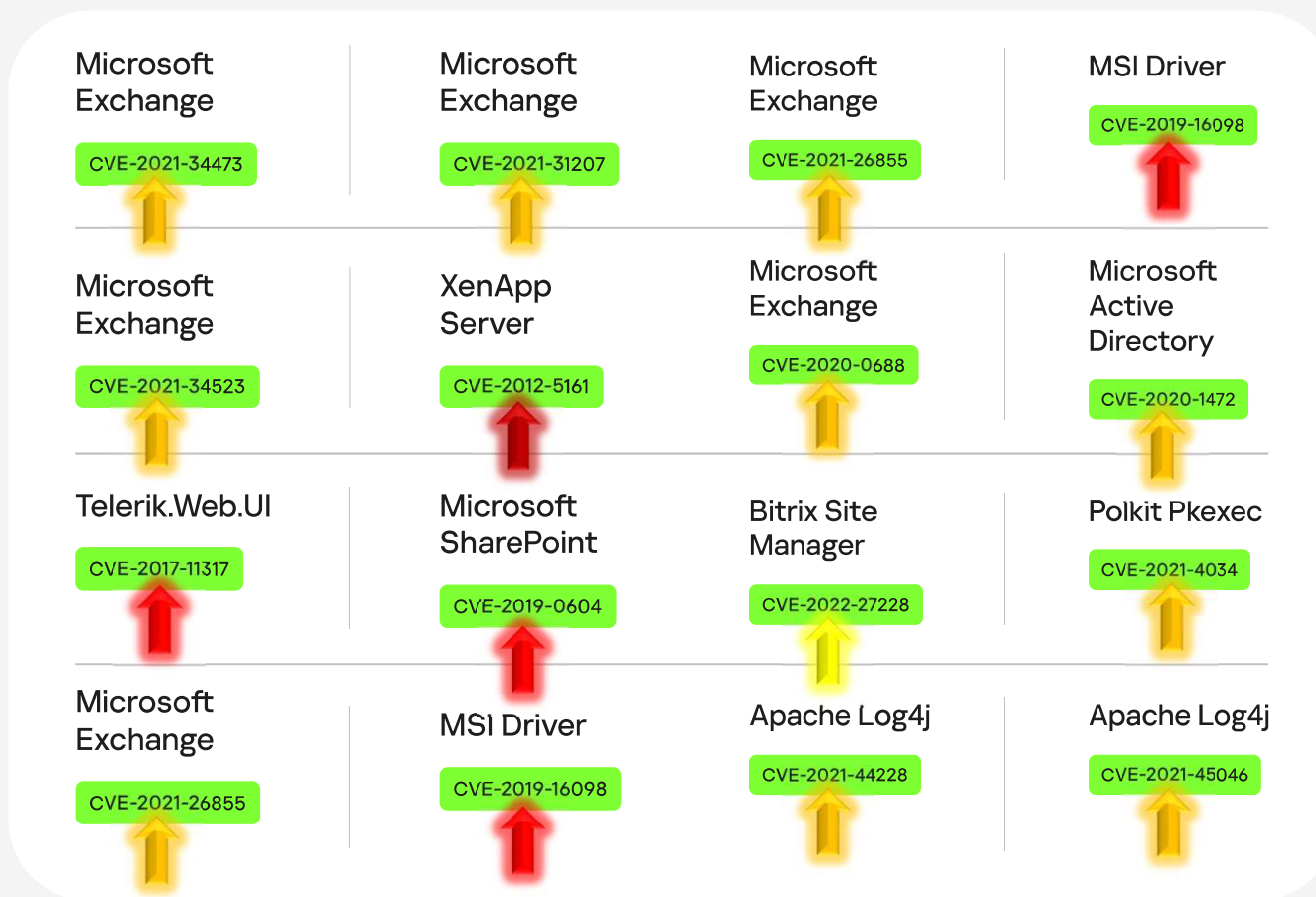
Sample case (**Ransomware**)

22



Exploits in Incidents

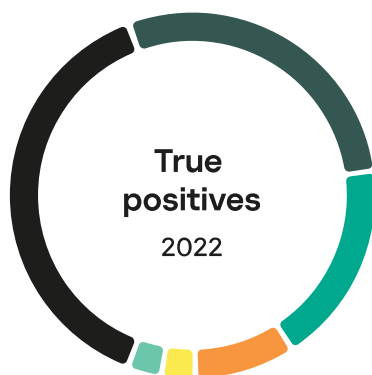
23



False Positives Were There

24

23.5% of all incident response requests were for false alarms



Incidents

%

■ Files encrypted	40.00
■ Suspicious activity	30.00
■ Data leakage	17.50
■ Security tool alert	7.50
■ Money theft	2.50
■ Suspicious e-mail message	2.50



Suspicious activity

%

■ Suspicious endpoint activity	43.50
■ Suspicious file	30.40
■ Suspicious network activity	13.00
■ Security tool alert	13.00

Recommendations (Initial Attack Vectors)

25

Exploitation of public-facing applications



Compromised accounts



Malicious email



Recommendations

- Implement a robust password policy and multifactor authentication
- Remove management ports from public access
- Establish a zero-tolerance policy for patch management or compensation measures for public-facing applications
- Ensure that employees maintain a high level of security awareness

Recommendations (Attack Tools and Detection)

26

Cobalt Strike

2022 6.0%
2021 9.7%

Mimikatz

2022 9.8%
2021 9.7%

PowerShell

2022 4.4%
2021 8.6%

PsExec

2022 10.4%
2021 10.8%

Other

2022 15.3%
2021 0.9%

Recommendations

- Implement rules for detection of pervasive tools used by adversaries
- Employ a security toolstack with EDR-like telemetry
- Constantly test reaction times of security operations with offensive exercises
- Eliminate usage of similar tools by internal teams (IT)

Recommendations (Reducing Impact)

27

Data leakage

2022 18.4%

2021 16%

Active Directory compromised

2022 17.3%

2021 11.1%

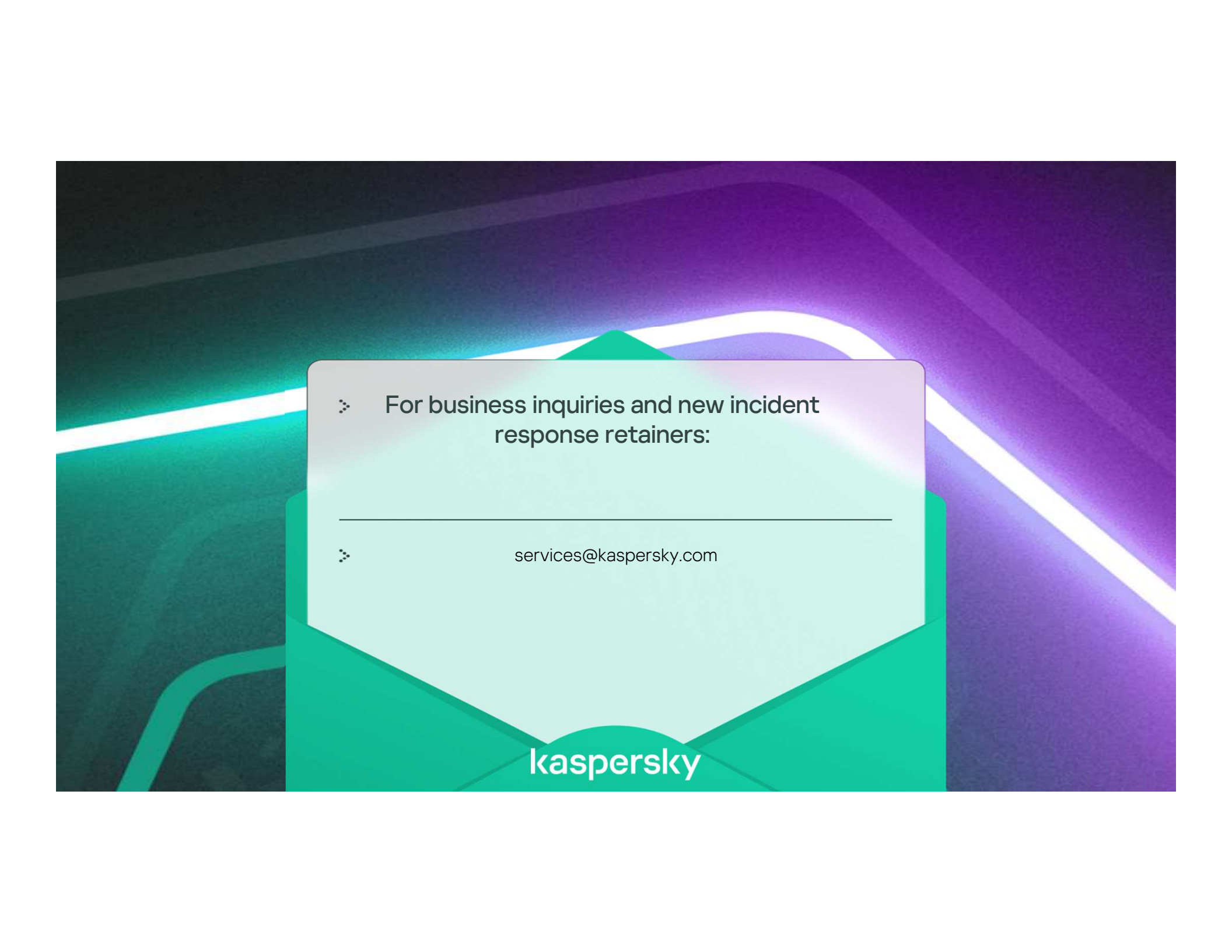
Files encrypted

2022 39.8%

2021 51.9%

Recommendations

- Back up your data
- Work with an Incident Response Retainer partner to address incidents with fast SLA
- Implement strict security programs for applications with PII
- Continuously train your incident response team to maintain their expertise and stay up to speed with the changing threat landscape



➤ For business inquiries and new incident response retainers:

➤ services@kaspersky.com

kaspersky

Questions

Ayman Shaaban
DFIR Manager, GERT

kaspersky

