2025年
勒索软件流行态势报告

RANSOMWARE THREAT REARCH REPORT 2025

360数字安全 360安全大模型

360安全能力中心反病毒部

2026年1月

前　言

本报告以三六零数字安全集团能力中心反病毒部（CCTGA勒索软件防范应对工作组成员）在2025年全年监测、分析与处置的勒索软件事件为基础，结合国内外与勒索软件研究相关的一线数据与安全数据进行全面梳理、研判与汇总而成。报告聚焦国内勒索软件的发展动态，同时融入国际热点事件与形势的分析判断，旨在评估2025年勒索软件传播与演化趋势，并深入探讨未来可能的发展方向，以协助个人、企业和政府机构更有效地制定安全规划，降低遭受勒索攻击的风险。

360反病毒部是三六零数字安全集团的核心能力支持部门，由一批常年奋战在网络安全一线的攻防对抗专家组成。该部门负责监测、防御、处置流行病毒木马以及研究新安全威胁。维护360高级威胁主动防御系统、360反勒索服务等基础安全服务，并提供横向渗透防护、网络入侵防护、Web服务保护、挖矿木马防护等多项保护功能，保护政企单位与广大网民的网络安全。

摘　要

- 2025年，360反勒索服务平台共处理2179起勒索软件攻击求助案例。从反馈情况来看，国内勒索软件整体的攻击态势与往年类似，安全形势依然严峻。

- 勒索软件攻击的目标仍然集中于企事业单位，虽然中小企业依然是遭受攻击的主要群体，但规模较大的政企单位受到攻击的情况同样不容忽视。

- 2025年度国内最为流行的勒索软件家族相比去年变化较大，前三家为Weaxor、LockBit和Wmansvcs，我们对这三家勒索软件的处置量占总量的58.4%以上。

- 由于当前勒索软件已基本形成了较为成熟稳定的产业链，其传播手段趋于稳定。2025年，勒索软件的传播依然是以远程桌面和漏洞利用两种手段为主，仅这两种传播途径就占到了总量的近八成。其中利用漏洞传播是去年Mallox家族的传统手段，虽然本年度该家族已不再流行，但Weaxor作为该家族的重塑版本，则很好地继承了这一传统。

- 勒索软件的核心加密算法延续了往年的思路，在保证加密强度的前提下，尽可能提升加密效率。Curve25519、ChaCha20等高效算法已渐成主流，而2025年新兴的The Gentlemen勒索软件，则采用了X25519配合XChaCha20算法，进一步提升了加密的效率与强度。

- 2025年，双重勒索和多重勒索模式在赎金要求方面有所回落。与去年动辄过千万美元的赎金金额有所区别，今年多家勒索软件的勒索金额降至百万美元量级，即使BlackCat对美国环球健康服务公司这类巨头企业的勒索金额也仅为2200万美元。此外，2025年度国内最为流行的Weaxor勒索软件，更是将原本3万元人民币的勒索金额降低至1.2万元左右。

- 服务业、制造业和建筑业是2025年受到双重/多重勒索攻击的主要行业。目前已公开的被勒索企业中，美国企业依然以超过半数的占比位居榜首，我国亦有企业上榜，占比约1.46%。

- 2025年，广东、北京和浙江三省/市排在国内勒索软件攻击态势严重程度的前三位。受攻击的系统类型变化不大，桌面操作系统仍然位居首位，但Windows 10系统正逐步被Windows11取代。

- 制造业、互联网及软件、服务业是2025年国内勒索软件攻击的主要目标，教育、医疗行业也受到了较多的攻击，分列第五和第六位，这也应引起重视。

- 在攻击IP来源方面，美国成为勒索攻击IP的第一大来源地，其后则多为欧洲国家，而新加坡和我国香港地区因为存在大量被黑客租用的服务器机房，也榜上有名。此外，勒索软件作者所采用的沟通邮箱依然以匿名邮箱为主。

- 在与勒索软件对抗的安全技术发展方面，我们认为，未来将朝着AI技术应用、专业化与系统化攻防对抗等方向进一步演进。同时，360也推出了多款创新工具，持续走在与勒索软件对抗的安全技术前沿，推动行业在防护能力和应对策略上不断提升。

目录 | CONTENTS

第一章

勒索软件攻击形势

勒索软件攻击形势

2025年，勒索软件依然是全球范围内风险等级最高、影响面最广的网络安全威胁之一，其在国内的整体传播态势总体延续了2024年以来的相对平稳状态。无论是新出现的勒索软件家族，还是长期活跃的传统勒索软件团伙，其攻击活动依然频繁，且对个人用户、企业及政府机构持续构成现实威胁，但未观察到某单一勒索软件家族在短时间内引发大规模、爆发式传播的情况。这一相对稳定的态势，一方面，得益于全球主流安全厂商在反勒索技术、防护体系和应急响应能力上的持续投入与协同对抗；另一方面，也与个人用户及政企单位对勒索软件这一高危恶意软件类型的认知不断加深、防范意识和基础防护能力显著提升密切相关。

虽然整体数据平稳，但勒索软件的攻势依然不减。攻击方式也有显著变化。针对个人、中小企业以传统勒索攻击为主，头部勒索家族如Makop、Phobos均属于此类情况。赎金金额方面，没有显著变化，仍以2000美元～5000美元为主。针对大中型企业的勒索攻击，已转为窃密、加密双重勒索形式为主，而赎金金额多了“一单一价”的模式。在技术演进方面，主流勒索家族的攻击、加密、运营技术逐步趋同，一个单位频繁遭受多家勒索软件攻击的案例时有发生。**部分新兴家族，在勒索软件创建时，存在疏漏**。360反勒索专家，利用这一特点，成功完成了7款勒索软件的解密。

通过对2025年勒索软件样本的深入分析，以及相关攻击案例的溯源研究可以发现，虽然勒索软件的整体技术框架并没有发生根本变化，但在具体攻击方式和实施细节上，各个家族仍在不断优化和升级。为了提高入侵效率和成功率，越来越多的勒索团伙开始把软件漏洞和 Web 漏洞作为主要突破口，而不再单纯依赖RDP暴破等传统手段。针对大中型企业的边界设备漏洞攻击成为常态，内网横移重点打击AD域控、VMware ESXI、IT管控平台等集

控设备。在勒索病毒免杀对抗方面，这类攻击家族表现并不积极，攻击者一般在获取足够权限后，通过管控方式来关闭设备的安全功能。

值得关注的是，随着人工智能技术的快速发展和普及，勒索软件正在变得更加“聪明”和高效。在AI的帮助下，这类攻击的更新速度明显加快，操作门槛不断降低，使得更多攻击者能够轻易发起复杂的网络攻击。可以预见，未来人工智能驱动的勒索攻击将逐渐成为常态，成为网络空间中不容忽视的重要安全风险。与此同时，人工智能也正在成为网络安全防护的重要力量。越来越多的安全厂商将AI技术引入安全产品和服务中，在威胁发现、异常行为识别和自动化处置等方面显著提升了防御能力。展望未来，那些能够成熟、高效地运用人工智能技术的组织，将在应对勒索软件及其他网络威胁的长期对抗中占据明显优势。可以说，人工智能已经成为当前乃至未来一段时期内，网络攻防博弈中最关键的因素之一。

2025年，360反勒索服务共处理了**2179例**勒索攻击求助，发现84个新勒索家族，其中多重勒索家族40个约占一半。新增支持8款勒索病毒的解密，其中7款为全球独家解密。协助2271位用户，完成486万份文件的解密，挽回损失超4700万元。2025年，360防黑加固共保护近216万台设备免遭入侵，拦截各类弱口令入侵共计超过12亿次。

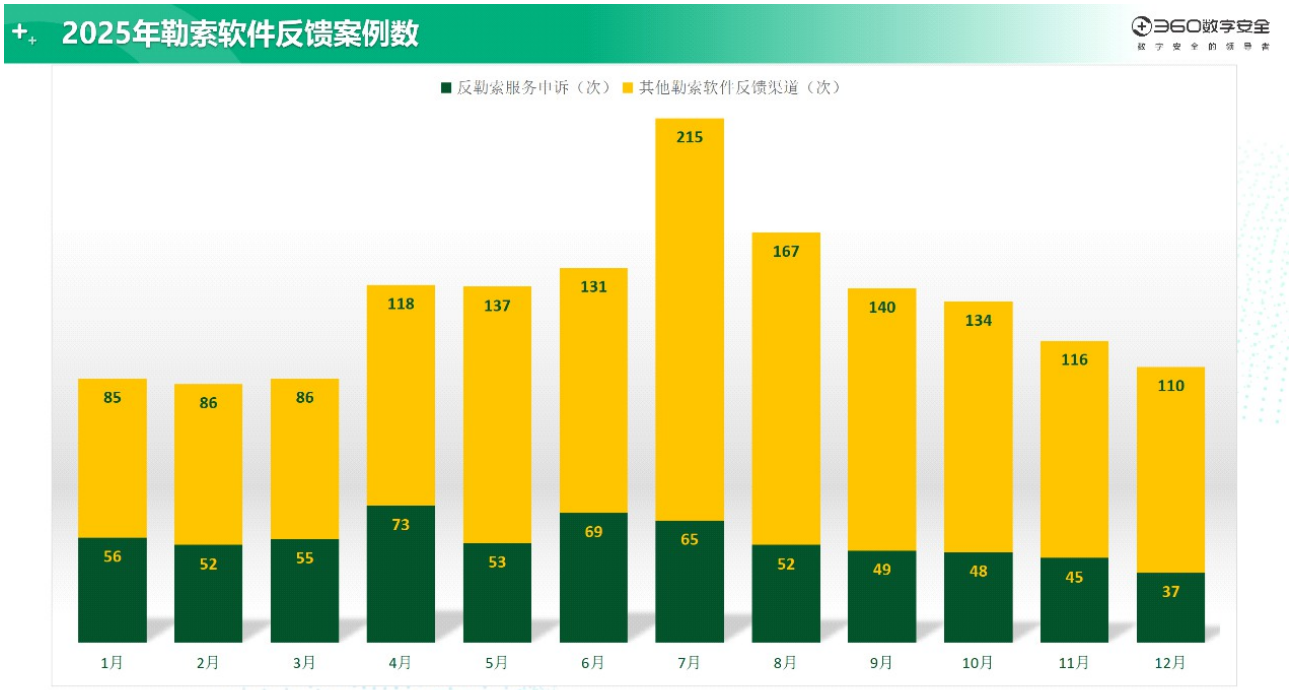
2025年，360反勒索预警服务基于360全网安全大数据视野，监测勒索攻击的多个环节，在勒索攻击的准备阶段，以及病毒初始投递阶段，对监管、企业用户提供勒索预警订阅服务，争取在勒索的前期阶段，进行阻断，避免造成受害单位的进一步损失。2025年共计捕获勒索攻击事件线索5858起，涉及受害单位1639家，确认勒索病毒家族62个，攻击IP来源地涉及境外52个国家或地区，输出勒索攻击事件线索674起，覆盖全国多个地区。

本章将对2025年全年，360反勒索服务检测到的勒索软件相关事件与数据进行分析解读。

勒索软件概况

2025年全年，360反勒索服务平台、360解密大师两个主要渠道，一共接收并处理了**2179位**遭遇勒索软件攻击的受害者求助。其中来自企业用户的求助占比较高，与个人受害者相比，组织单位受到攻击后所影响的设备数量较多、勒索金额较大，造成的损失程度也更为严重。勒索软件对企业的影响正在进一步加深，社会整体面临的勒索软件威胁依旧严峻。

下图给出了2025年各月通过360安全卫士反勒索服务和360解密大师渠道，提交申请并最终确认感染勒索软件的有效求助量情况。

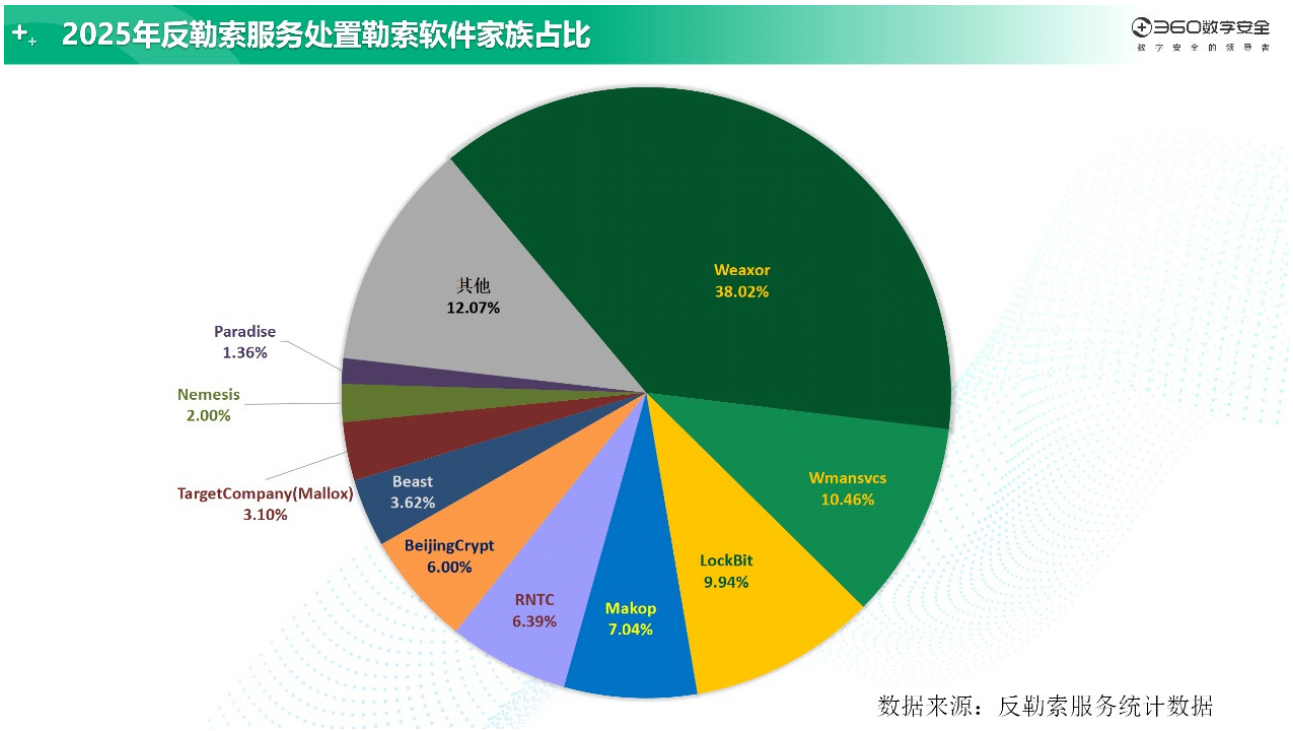


数据来源：反勒索服务统计数据

2025年反馈量的增长波动主要受Wmansvcs家族与Weaxor家族影响。前者频繁发起暴破攻击，造成大量未使用360终端安全产品的设备中招。后者长期无差别发起Web漏洞利用攻击，且攻击过程中加入了大量与安全软件的攻防对抗，造成大量未使用360终端安全产品的用户中招，也使其成为2025年排行第一的勒索家族。

（一）
勒索家族分布

下图给出的是根据360反勒索服务和360解密大师数据所计算出的2025年勒索软件家族流行占比分布图。



其中，PC端系统中Weaxor、LockBit和Wmansvcs这三大勒索软件家族的受害者占比最多，都属于老牌勒索家族及衍生家族。TOP10家族中值得注意的有下面几点：Weaxor最早出现于2024年10月，是TargetCompany（Mallox）勒索家族的重塑版本。

除了使用高度相似的代码外，也沿用了原有的这三个典型投毒渠道。2025年这个家族依靠Web漏洞利用成为断崖式领先的勒索家族，并在攻击过程中积极利用大量存在漏洞的驱动程序远程注入系统进程，与安全软件做内核对抗，进一步保障了勒索攻击的成功率。

1、Wmansvcs最早出现于2025年6月，是基于phobos勒索家族的衍生版本。此家族只在国内传播，未发现任何境外传播案例。传播方式为远程桌面登录后手动投毒，加密器执行后可选择加密SMB共享设备。自2025年6月开始在国内传播以来，该家族从未试图与360进行过任何对抗行为，甚至连攻击IP都没有进行过更换。受害者主要为中小企业以及申请了固定IP的个人用户。这从侧面说明，没有有效终端防护的用户数量庞大，足以支撑黑灰产牟利。

2、LockBit作为历史悠久的全球知名勒索家族，在2025年恢复了LockBit5.0版本的多重勒索站点。在传统的传播模式基础上，引入了第三方黑产团伙的参与，如银狐木马团伙与其背后的电信诈骗团伙。除了年底的LockBit5.0版的复兴外，全年传播的版本主要集中在LockBit3与其泄露代码的构建版本。

3、Beast家族自2022年出现以来，拥有众多变种与衍生家族。2025年该家族对国内目标保持了较高的攻击效率，且由于其跨平台的攻击特性，360同样捕获了大量Linux、Exsi、Nas等平台版本的变种。由于相关平台存在漏洞难以被管理员及时修复，且多数设备没有安装防护产品，形成了安全隐患，因此需对此类跨平台家族保持高度警惕。

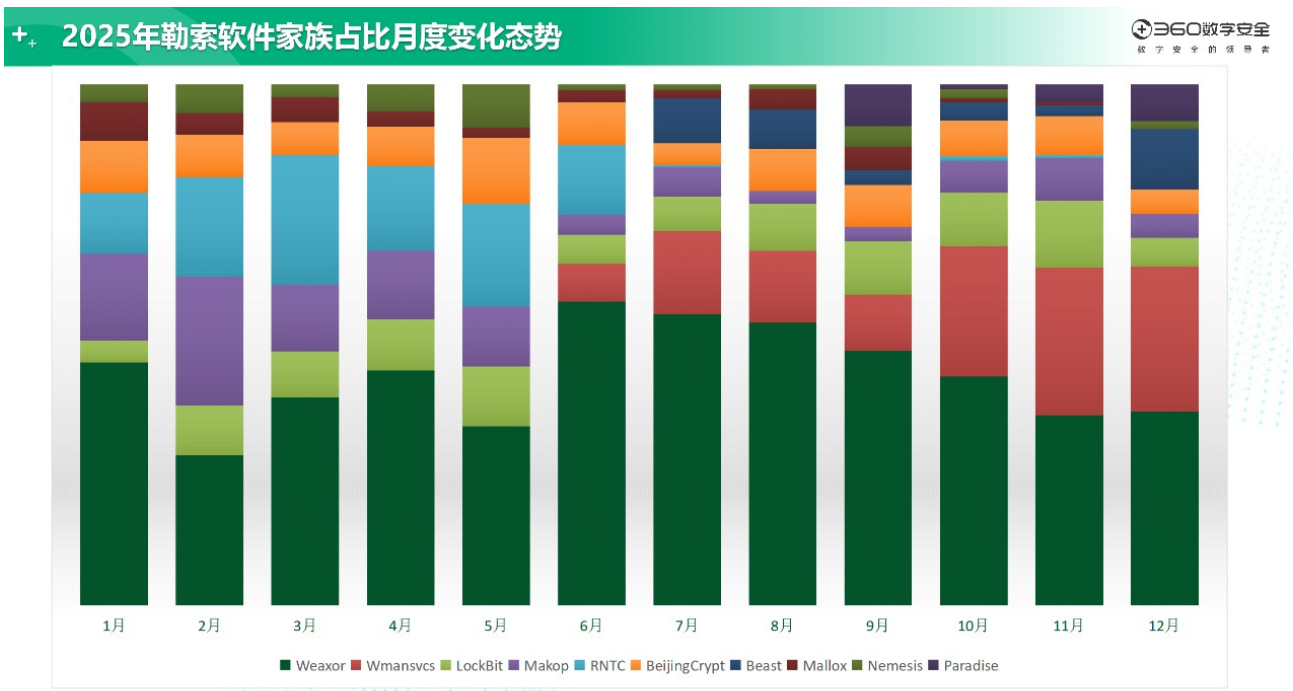
4、Phobos作为曾经排名靠前的勒索软件家族之一，在2025年被缉拿落网归案。360解密大师第一时间提供了对该家族的加密支持。然而，2025年基于该家族的衍生版本Wmansvcs，在国内传播非常广泛，同源并在全球范围内传播的Makop家族也保持着很高的排名。这证明其在传播和加密技术方面相对成熟稳定，因而不断被后来者模仿与借鉴。

（二）

主流勒索软件趋势

我们汇总了2025年各月勒索软件家族的月度感染量TOP10数据，发现通过Web漏洞传播的Weaxor家族成为攻击效率最高的方式，全年霸榜Top1的位置。6月后新增的Wmansvcs家族接棒老牌勒索软件phobos家族，成为传统弱口令登录攻击方式的典型家族。总体而言，从2025年的传播量上看，弱口令攻击仍排行第一，但漏洞利用的传播量已经非常接近此类传统攻击。

- Weaxor家族广泛使用各类Web漏洞进行无差别持续攻击，呈现出稳定且高效的攻击效果。在Web漏洞修复这方面，无论是漏洞所属厂商还是相关客户都存在较为严重的滞后性，为勒索攻击在内的各类攻击提供了周期性大面积爆发的土壤。
- LockBit家族持续发力，并在年底携新版LockBit5.0强势回归。新版本在原有非常多样的攻击方式基础上，引入了电信诈骗强相关的木马团伙进行投毒。对勒索受害者同时造成电诈被骗、信息泄露、数据被加密并勒索的多重伤害。
- Wmansvcs勒索家族继承了phobos勒索家族的攻击方式，只在国内通过远程桌面暴破登录进行传播。 其不与360拦截进行对抗的佛系操作，从侧面印证大量未安装可靠防护软件的存量设备，可为黑灰产提供充足的活动空间和收益来源。



数据来源：反勒索服务统计数据

（三）
加密方式分布

我们对2025年仍在活跃传播且具有代表性的勒索软件家族进行了深入分析，并统计了各家族所采用的编程语言、加密算法及非对称密钥生成方式。部分勒索软件家族曾对其代码进行重构，或针对不同操作系统平台使用了不同的编程语言，因此在编程语言方面，某些家族可能出现多种编程语言的使用。为了加密文件，这些家族采用了多种技术手段，包括但不限于RSA、Curve25519、AES、xChaCha20、Salsa20等算法。以下是各家族采用的具体情况：

家族名称	编译语言	加密算法	非对称密钥生成
Weaxor	C++	Curve25519+AES128/ChaCha20	内置Curve25519公钥
Wmansvcs	Rust	RSA1024+AES256	内置RSA-1024公钥
LockBit5.0	C++	RSA1024+XChaCha20	内置RSA-1024公钥
Beast	Golang, Delphi, C	Curve25519+ChaCha20	内置Curve25519公钥
BeijingCrypt	C++	RSA1024+AES256	内置RSA-1024公钥
Makop	C++	RSA1024+AES256	内置RSA-1024公钥
MedusaLocker	C++	RSA2048+AES256	内置RSA-2048公钥
Loki	C#	RSA2048+AES256	内置RSA-2048公钥
The Gentlemen	Golang	X25519+XChaCha20	动态生成加密
Kalxat	C#	RSA+ChaCha20	动态生成加密
Kann	C++	RSA4096+AES256	内置RSA-4096公钥
FreeFix	EPL	RSA2048	内置RSA-2048公钥
Montelli	C++	RC4	内置RC4密钥
Mallox	C# C#	Curve25519+AES128/ChaCha20	内置Curve25519公钥
BlackMatter	C++	RSA1024+Salsa20	内置RSA-1024公钥

VanHelsing	C++	Curve25519+ChaCha20	动态生成加密
Cephalus	Golang	AES-CTR	内置AES-CTR密钥 +生成假的AES密钥
Nightspire	Golang C++	RSA+AES256	内置RSA公钥
BaqiyatLock	C++	RSA4096+AES256	内置RSA-4096公钥
ShinyHunters	C++ C++	RSA2048+ChaCha20	内置RSA2048公钥
Cuba	C++	RSA1024+ChaCha20	内置RSA-1024公钥
RansomEXX	Rust	RSA4096+AES256	内置RSA-4096公钥
Buran	Delphi	RSA2048/512+AES256	内置RSA公钥
phobos	C++, Delphi C++	RSA1024+AES256	内置RSA-1024公钥
TellYouThePass	C# C#	RSA2048+AES256	内置RSA-2048公钥
Black Basta	C++	RSA4096+ChaCha20	内置RSA-4096公钥
Play	C/C++ Golang, Rust	RSA+AES	内置RSA公钥
Qilin.B	Rust	RSA4096+AES256	内置RSA-4096公钥
Medusa	C/C++	RAS2048+AES256	内置RSA-2048公钥
Trigona	Delphi	RSA4096+AES256	内置RSA-4096公钥
Money Message	C++ C++	ECDH+ChaCha20	ECDH生成密钥对
Cactus	C/C++ -	RSA4096+AES256	内置RSA-4096公钥
Rhysida	Golang, C++	RSA4096+ChaCha20	内置RSA-4096公钥
Hunters International	Rust C# Golang, C++	RSA4096+ChaCha20	内置RSA-4096公钥
DoNex	C/C++	RAS4096+ChaCha20	内置RSA-4096公钥
EMBARGO	Rust	Curve25519+ChaCha20	内置Curve25519公钥
Cicada3301	Rust	RSA+ChaCha20	内置RSA公钥
Eldorado	Golang	RSA+ChaCha20	内置RSA公钥

▲ 2025年代表性勒索软件家族编写语言及算法实现方案

通过对 2025 年勒索软件样本的技术分析可以看出，当前主流勒索软件家族在核心加密设计上仍延续了高度一致的技术路线：以对称加密算法完成大规模文件数据加密，辅以非对称或椭圆曲线算法，完成密钥保护的多级加密方案。这一模式已成为勒索软件领域的事实标准，其目的在于在保证加密强度的同时，兼顾整体加密效率。

从样本分布来看，RSA系列算法依然在非对称加密阶段占据主导地位，其中RSA-2048与RSA-4096 被大量采用，RSA-1024虽然在部分家族中仍有使用，但整体呈现出逐步弱化的趋势。与此同时，Curve25519 / X25519等椭圆曲线算法在 2025年的勒索软件中明显增多，已被多个新老家族采用，并在部分样本中完全替代传统 RSA方案。这一变化反映出勒索软件开发者正主动引入计算效率更高、实现更简洁且具备同等级安全性的现代椭圆曲线密码体系，以缩短密钥交换阶段的执行时间并降低运行痕迹。

在对称加密算法选择方面，2025年样本中呈现出更加明显的多样化特征。除AES-256仍被广泛使用外，ChaCha20及其变体（如 XChaCha20）已成为最受青睐的替代方案，并在大量家族中与 RSA或Curve25519 组合使用。同时，Salsa20、AES-CTR 等算法亦在部分样本中出现，显示出对高性能流加密算法的持续偏好。相比传统AES，这类算法在无硬件加速或跨平台环境下，具备更稳定的性能优势，尤其适合Go、Rust等新兴开发语言生态。

从密钥管理方式来看，多数家族仍倾向于在样本中内置非对称公钥，以降低部署复杂度并确保加密流程稳定；但也有少数家族开始采用动态生成密钥或 ECDH 协商机制，以进一步提升样本的灵活性与反溯源能力。

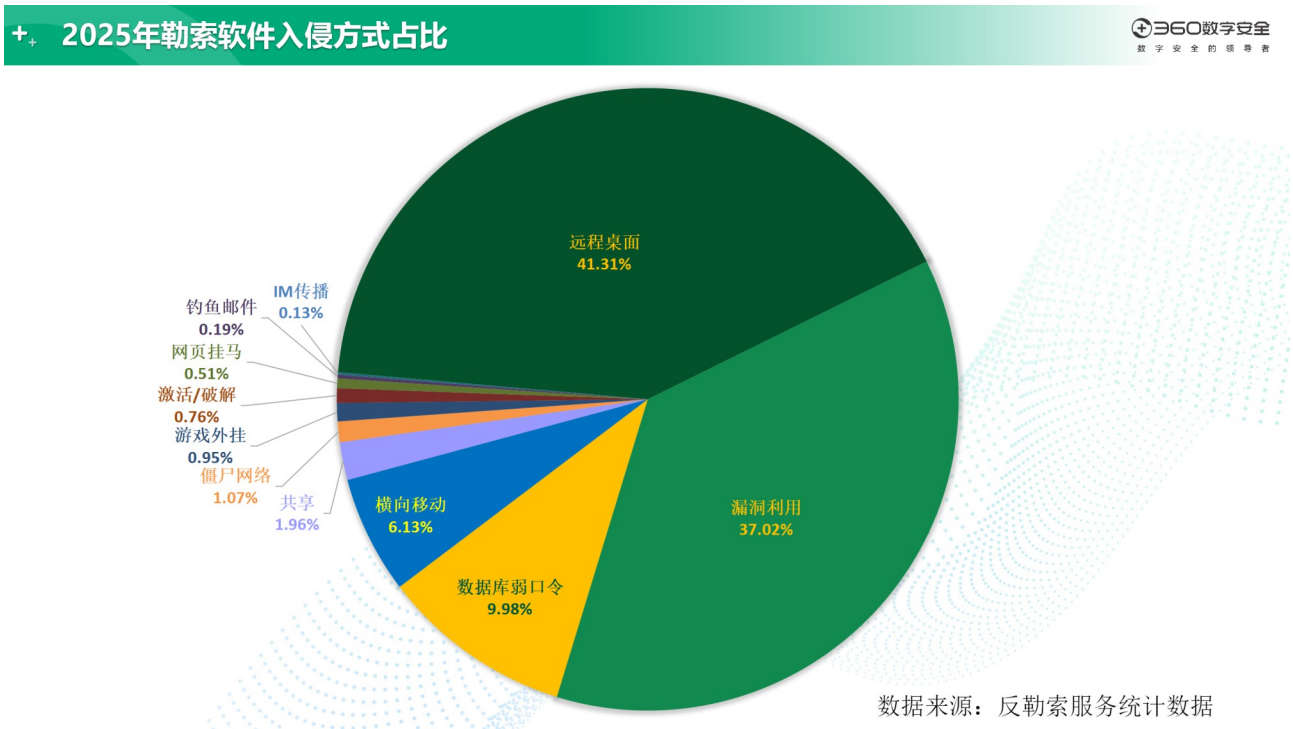
在2025年360独家支持了Freefix家族的解密，该家族利用易语言生态系统中的“.ec”模块文件，构建出了一条从开发者到终端用户的完整攻击链条。与常规的勒索软件传播方式不同，FreeFix采用“源头带毒”策略，将攻击目标直接锁定在了软件开发这一环节上，让开发者在不知情的情况下成为了恶意代码的传播者。

总体而言，2025年勒索软件在加密方案的整体架构上已趋于成熟，主流家族均在多级加密这一既定框架内进行演进。值得关注的是，优化重点正从“加密方案设计”转向“算法实现效率与运行性能”，无论是引入 Curve25519，还是大规模采用 ChaCha20，均体现出勒索软件开发者在提升执行效率、降低异常行为暴露风险方面的持续投入。

二

勒索软件传播方式

下图展示了2025年攻击者在投放勒索软件时所采用的各种入侵方式的占比情况。根据统计可以观察到：远程桌面入侵仍然是导致用户计算机感染勒索软件的主要途径，利用漏洞对目标网络实现入侵的占比持续且稳定，虽然总体占比仍位居第二，但与传统通过远程桌面入侵量的占比已相差无几，说是并列第一也并不为过。



数据来源：反勒索服务统计数据

通过对勒索软件在2025年的具体传播案例进行分析，发现位列前三的传播与入侵方式呈现出当前占比分布情况的主要原因如下：

1、远程桌面入侵

远程桌面入侵依然是国内最频发的勒索攻击手段。此类攻击手段由来已久，有着一套非常成熟的入侵方案和现成工具软件。同时，数量众多的中小型企业，始终未对这类安全隐患

采取有效的防范措施，这也是让远程桌面入侵常年稳居最受攻击者青睐的入侵手段榜首的重要原因。

2、漏洞利用

2025年通过漏洞利用发起的勒索攻击量，已经非常接近远程桌面登录的攻击方式。而在各类应用的漏洞利用中，针对Web应用或嵌入Web组件的各类管理系统的漏洞攻击是所有漏洞利用类攻击中的重灾区。使用这类攻击手段的典型代表是Weaxor家族，而该家族是Mallox家族的品牌重塑版本，其在2025年的攻击态势连续霸榜TOP榜单。

3、数据库弱口令

与远程桌面入侵情形类似，数据库弱口令问题也是中小型企业——甚至一些大型企业中较为广泛存在的安全隐患。不过相对而言，此类入侵方式的效率较低并且对入侵者的“字典规模”有着一定的要求，所以此类攻击的总体占比并不像远程桌面入侵一样高。

令人欣慰的是，随着现在各企业对内的安全培训制度完善，此类隐患也相对容易防范，故此数据库弱口令入侵在2025年的总体占比情况有着较为明显的下降。

三

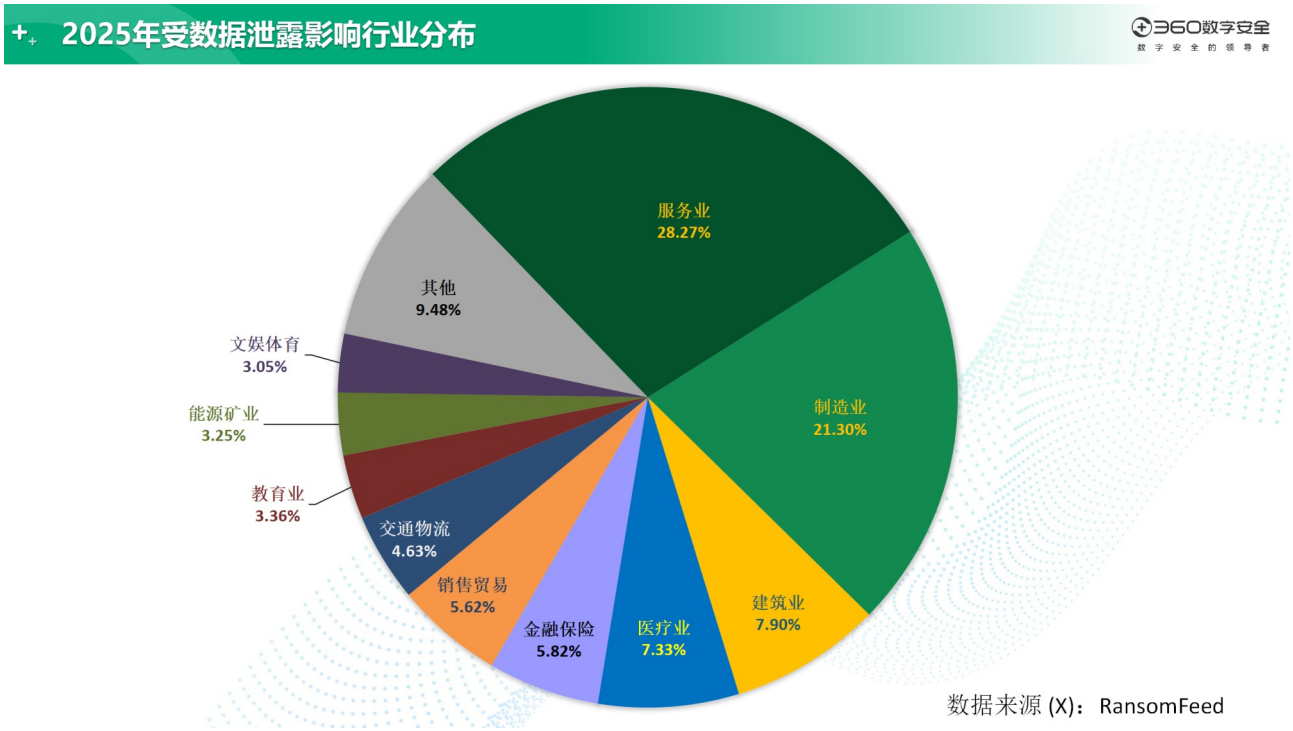
多重勒索与数据泄露

近年来，通过双重勒索或多重勒索模式获利的勒索软件攻击团伙越来越多。2025年360反勒索也第一时间捕获了LockBit5.0版死灰复燃后引入社会工程学攻击渠道的实锤案例，证实了以往安全厂商与监管部门对这个热门家族新增传播方式的猜测。

（一）
行业统计

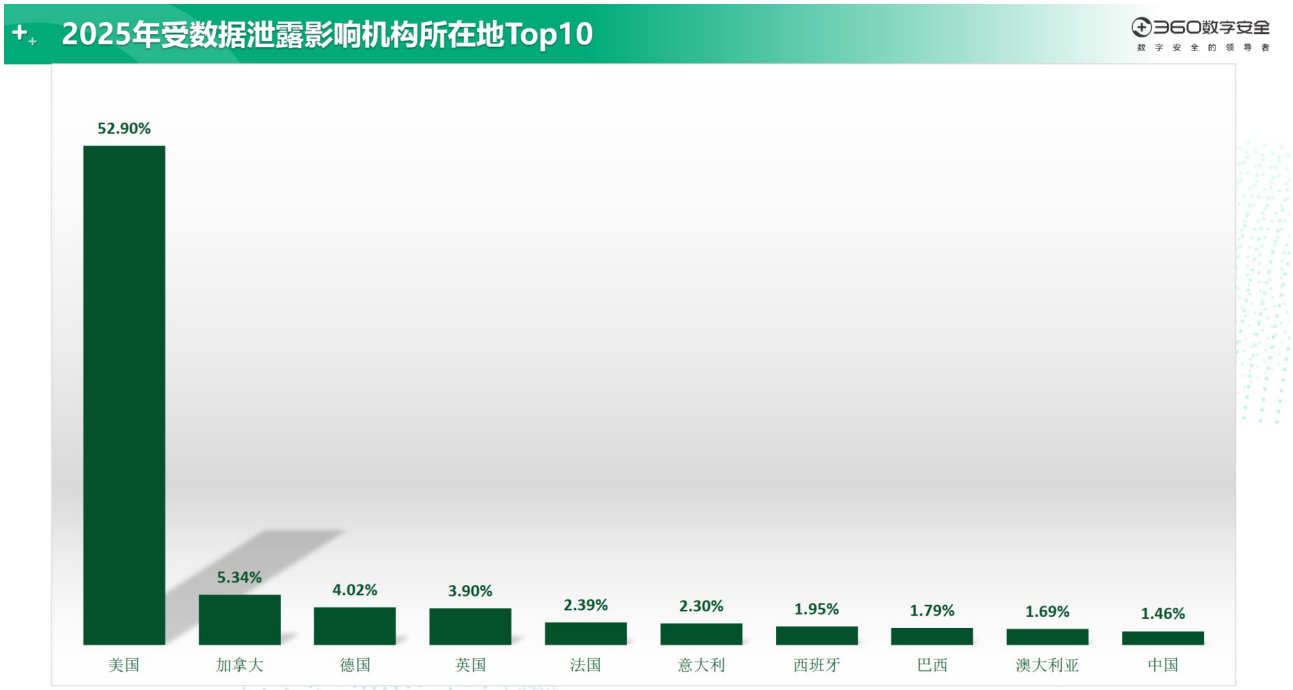
与去年头部行业分布相对平均有明显区别，2025年受数据泄露影响的行业分布较为集中地出现在服务业与制造业两大类。除此之外，建筑业、医疗业、金融保险等行业紧随其后，分列在第三至第五位。推测出现这一变化的主要原因与今年勒索软件的主要攻击目标向中大型企业倾斜有关联。相对而言，服务业与制造业的相关企业中，内部网络中往往拥有较大规模的计算机设备，这也就造成了勒索攻击对这两个行业的攻击更为集中。

此外，教育、能源行业也进入了数据泄露的前十位，而医疗行业更是在前五位。这些敏感行业受到大量勒索攻击而导致数据泄露，也需要相关企事业单位对勒索攻击的防护更加重视。



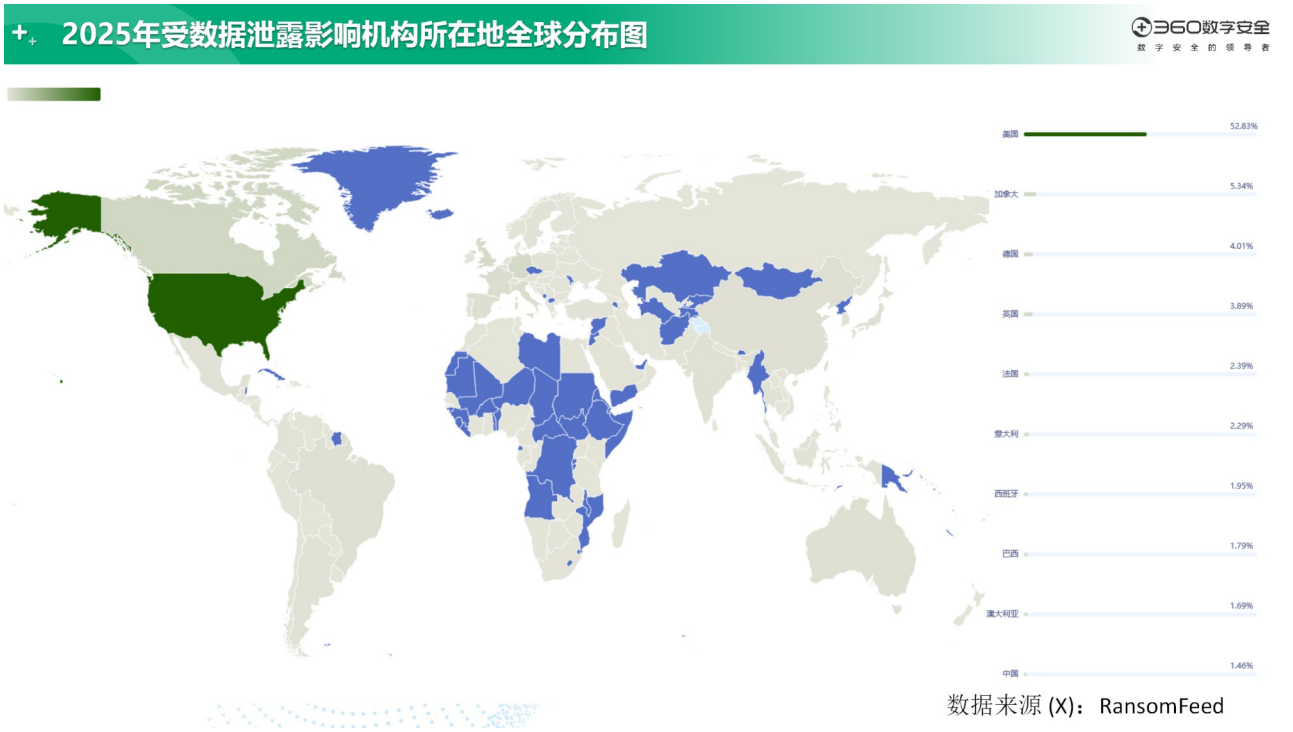
（二）
国家与地区分布

从数据泄露机构所在地分布情况来看，美国机构的占比依然稳居全球首位，相较2024年度有小幅提升，但总体变化不大。美国机构常年位居榜首，一方面是由于美国网络发达且企业众多，同时也与其发达的云服务产业与设备托管业务有关。



数据来源 (X)：RansomFeed

下图为根据全球地区分布数据所绘制的更加直观的地区分布图：

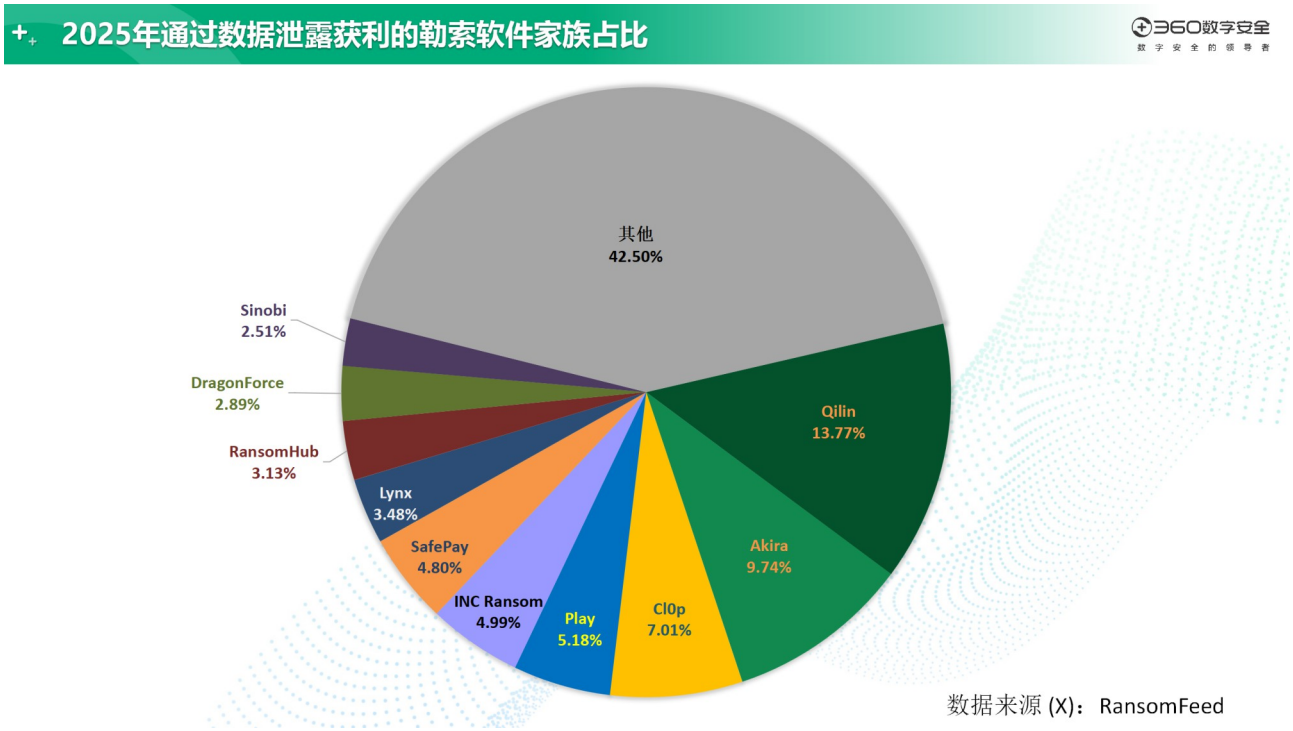


数据来源 (X)：RansomFeed

需要说明的是，以上数据来自各勒索软件的公开数据，各勒索软件家族手中究竟还有多少尚未公开的数据，或是由于已支付赎金等原因不被公开的数据，外界无从知晓也无法进行统计分析。

（三）
家族统计

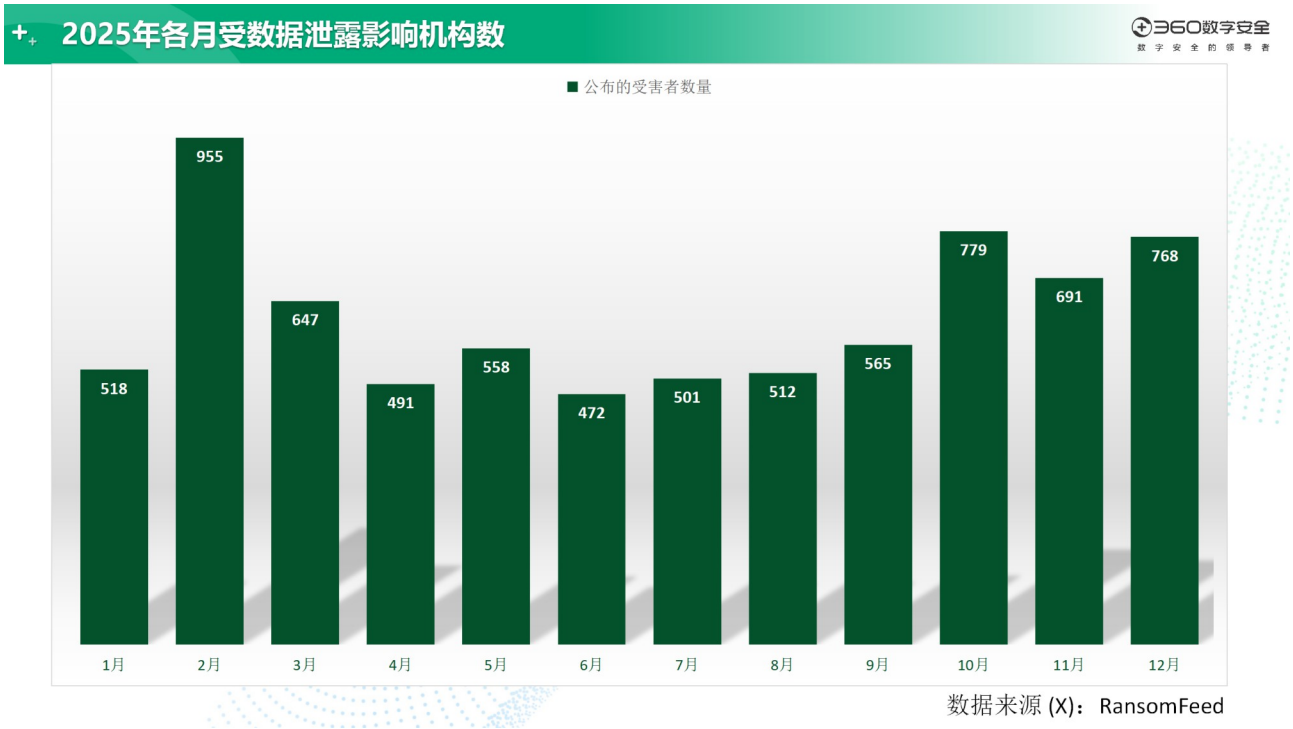
2025年参与双重/多重勒索活动的主要活跃勒索软件家族共计122个。家族总量与2024年相比有显著增加，增幅近三成。这一方面是由于有越来越多的勒索软件家族，加入了多重勒索的队伍中，另一方面也是由于新增勒索软件，往往更倾向于采取这种更为有效的勒索模式所致。具体的占比分布情况如下图所示。



通过对2025年双重/多重勒索软件的占比分布数据进行分析，不难发现Top10中的头部家族占比处于主导地位。而未被列出的“其他”家族占比大幅提升，显示出了较为明显的“长尾”态势，这一点与参与双重/多重勒索活动的主要活跃勒索软件家族数量大幅提升有关。

（四）
逐月统计

从数据泄露的相关统计来看，总体有一定的波动，但并未出现较大规模的爆发现象。



数据来源 (X)：RansomFeed

2025年各月的数据泄露机构数量延续了2024年平稳的态势，但在2月和10月后出现了两个较为明显的峰值。结合目前已公开的勒索事件判断，2月的高峰数据与Clop采用了Palo Alto Network的漏洞入侵手段有关。而年底的一波峰值数据，则主要是受到了Oracle漏洞的影响。

（五）
数据泄露的多重影响：商业、法律与声誉风险

随着数字化和信息化的深入发展，数据已成为企业最核心的资产。然而，信息技术的快速演进也带来了数据泄露事件频发的挑战，对企业产生深远影响。这些影响不仅包括直接的经济损失，还涉及企业声誉、合规要求以及运营连续性等多个层面。在勒索软件和其他网络安全威胁不断增加的背景下，数据泄露已成为全球各行各业亟须重视和应对的重要问题。

近年来，勒索攻击模式不断演变。传统的勒索攻击主要通过加密关键数据索要赎金，而新兴的数据勒索策略则更加复杂，破坏性更强。企业在遭遇数据泄露时，不仅面临数据被加密或外泄问题，还可能同时遭受攻击者的多重威胁与敲诈。这种变化意味着企业需要从多个维度理解数据泄露的潜在风险，并采取综合防护和应对策略，以降低经济、法律和声誉等方面的损失。

声誉风险：品牌形象受损与客户信任危机

声誉风险是数据泄露带来的最直接后果。当企业数据遭到泄露或篡改时，客户和公众对企业的信任度会显著下降。攻击者常通过多种手段加剧信任危机，包括：

- **直接威胁客户**

  攻击者利用被窃取的数据直接联系客户，警告其个人信息可能泄露，甚至要求支付费用以避免进一步信息暴露。此类行为不仅增加受害者心理压力，还削弱客户对企业的信任。

- **操控媒体舆论**

  攻击者可能借助媒体曝光事件，放大舆论压力，甚至将新闻报道链接嵌入赎金页面，迫使企业在公众压力下妥协。

声誉受损会影响客户忠诚度和市场份额，恢复过程可能耗时多年。企业应投入足够资源进行数据保护，同时建立危机公关机制，以便在事件发生时及时管理舆情。

数据竞拍：非法数据交易的经济驱动

随着数据泄露事件增加，非法数据交易市场逐渐成熟。勒索团伙不仅通过赎金获利，还通过数据竞拍获取额外收益，包括：

●数据拍卖

勒索团伙通过黑市网站或平台公开拍卖窃取的数据，包括企业敏感信息、客户资料及内部文件，以高价售卖给其他犯罪分子或竞争对手。

●案例分析

以BlackSuit（又名 Royal）及其关联平台为例，该团伙在2025年通过精密化的竞拍模式实现了利润最大化。执法部门行动中，查封了其暗网泄露及谈判站点，扣押了约109万美元的虚拟货币。

这些现象显示出非法数据交易市场的繁荣，企业不仅面临赎金的威胁，还可能因数据被公开交易而遭受更大的商业损失。因此，企业在网络安全建设中，必须加强对敏感数据的保护，减少数据泄露的可能性，并对数据的流向进行有效监控。

合规压力：法律法规的严格要求

随着全球范围内网络安全法规的不断完善，企业在遭遇数据泄露事件时，必须面对更加严格的法律和合规压力。许多国家和地区对数据泄露事件的报告要求已经变得愈加严格，企业如果未能及时报告，可能会面临严厉的罚款和法律后果。

●隐瞒事件的后果

许多企业在遭遇勒索软件攻击或数据泄露时，可能会选择隐瞒事件，试图通过支付赎金解决问题，而不向公众或监管机构报告。这种做法虽然可能暂时缓解企业的压力，

但一旦被揭露，企业将面临更为严峻的法律制裁。例如，韩国最大移动运营商 SK 电信公司（SK Telecom Co.）2025年8月收到了 1348 亿韩元的罚单。韩国个人信息保护委员会（Personal Information Protection Commission，简称 PIPC）对 SK 电信作出处罚，理由是该公司未能履行用户数据保护义务，且未及时上报数据泄露事件。韩国媒体及公众也对此多有不满。

企业在面临数据泄露时，必须严格遵守相关法律法规，确保及时向监管机构报告事件，并配合相关调查。通过加强合规性，企业可以避免不必要的罚款，同时提升公众和监管机构对企业的信任度。

业务中断：运营能力的系统性受损

数据泄露事件不仅会导致企业声誉受损，还会对企业的正常运营产生严重影响。在数据被加密或备份失效的情况下，企业的关键业务系统可能无法及时恢复，进而影响日常运营和服务交付。特别是在一些关键行业，数据泄露可能导致灾难性的后果。

●医疗行业

2025年5月 Kettering Health 全线停摆事件：2025年5月20日，美国俄亥俄州医疗系统 Kettering Health 遭遇大规模勒索软件攻击，导致其旗下 14家医院的IT系统全线崩溃。此次攻击迫使该医疗系统不得不取消所有非紧急住院和门诊手术，禁用患者门户网站（MyChart），并导致急诊室（ER）被迫采取“救护车分流”措施，将急救患者转运至其他医疗机构。

●工业和制造行业

2025年Nucor钢铁公司生产停滞事件：2025年5月，北美最大的钢铁生产商Nucor Corporation遭到网络攻击，导致其在美国、墨西哥和加拿大的多处生产设施被迫停工。由于关键运营系统受到威胁，公司不得不采取紧急离线措施。此类针对重工业基础设施的攻击，不仅造成了数百万美元的直接产值损失，更对下游建筑与汽车供应链产生了连锁震荡。

因此，企业必须采取有效的业务连续性管理措施，确保关键数据和系统能够在数据泄露或攻击事件发生后尽快恢复，以减少对运营的影响。

经济损失：直接与间接成本的双重压力

勒索攻击的直接后果是企业需支付赎金，但其经济损失远不止于此。企业还需要承担由于数据泄露导致的业务中断、数据恢复、法律诉讼等一系列间接费用。企业的财务状况可能因此受到严重影响。

法律责任：隐私泄露引发的巨额赔偿

数据泄露事件不仅涉及企业的合规问题，还可能引发客户和员工的集体诉讼，导致企业面临巨额赔偿。在一些情况下，客户会对企业未能有效保护个人数据提出诉讼，要求赔偿因数据泄露而产生的经济损失。

●典型案例

Cencora（美源伯根）2.87亿元赔偿案（2025 年 8 月）：2025年8月，美国医药巨头Cencora（原名美源伯根）同意支付2.87亿元人民币（约 4000 万美元），以和解一项针对2024年大规模数据泄露的集体诉讼。该事件涉及27家制药公司、超过143万名患者的敏感健康记录。原告指控公司在发现系统漏洞后，未能及时采取防护措施，导致患者面临长期的个人隐私暴露风险。

四
勒索软件家族更替

（一）
每月新增传统勒索情况

360安全智能体监控到，每月都不断有新的勒索软件出现。以下是2025年每月新出现的传统勒索软件(仅通过加密文件对受害者进行勒索)的部分记录信息，共计46款：

2025年各月新增传统勒索软件家族

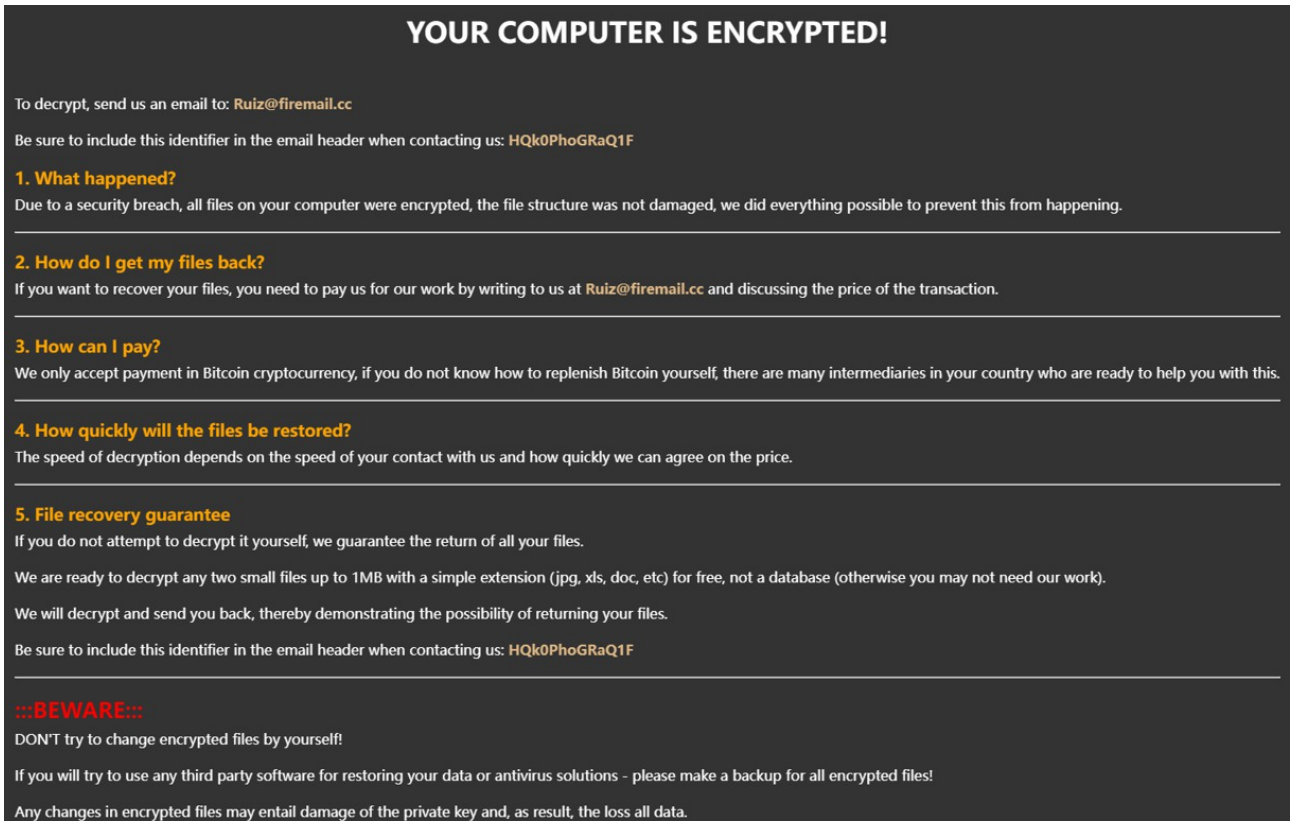
月份	新增传统勒索软件
2025年1月	Contacto、Codefinger、D0glun
2025年2月	CipherLocker、Vgod、LCRYX、Adver
2025年3月	MoroccanDragons、AptLock、Mamona
2025年4月	Asasin、Maximsru、CrypteVex、NanoCrypt、Jeffery
2025年5月	Bert、Kalxat、Lyrix、PowerLocker、YE1337、Mammon
2025年6月	Wmansvcs、UraLocker、SafeLocker、VerdaCrypt、DireWolf
2025年7月	Darkness、Walocker、Mino、SpiderPery、Xentari、Nebula、Cephalus、Pear、Charon
2025年9月	SnowSoul、HybridPetya、Monrans
2025年10月	Monkey、ThunderKitty、BrawLocker
2025年11月	QuickLock、Kazu、BlackHeolas
2025年12月	MiddCrypto、Marabu

▲ 2025年各月新增传统勒索软件家族

针对以上新增勒索软件家族，我们对其中几个典型家族进行具体介绍：

Wmansvcs

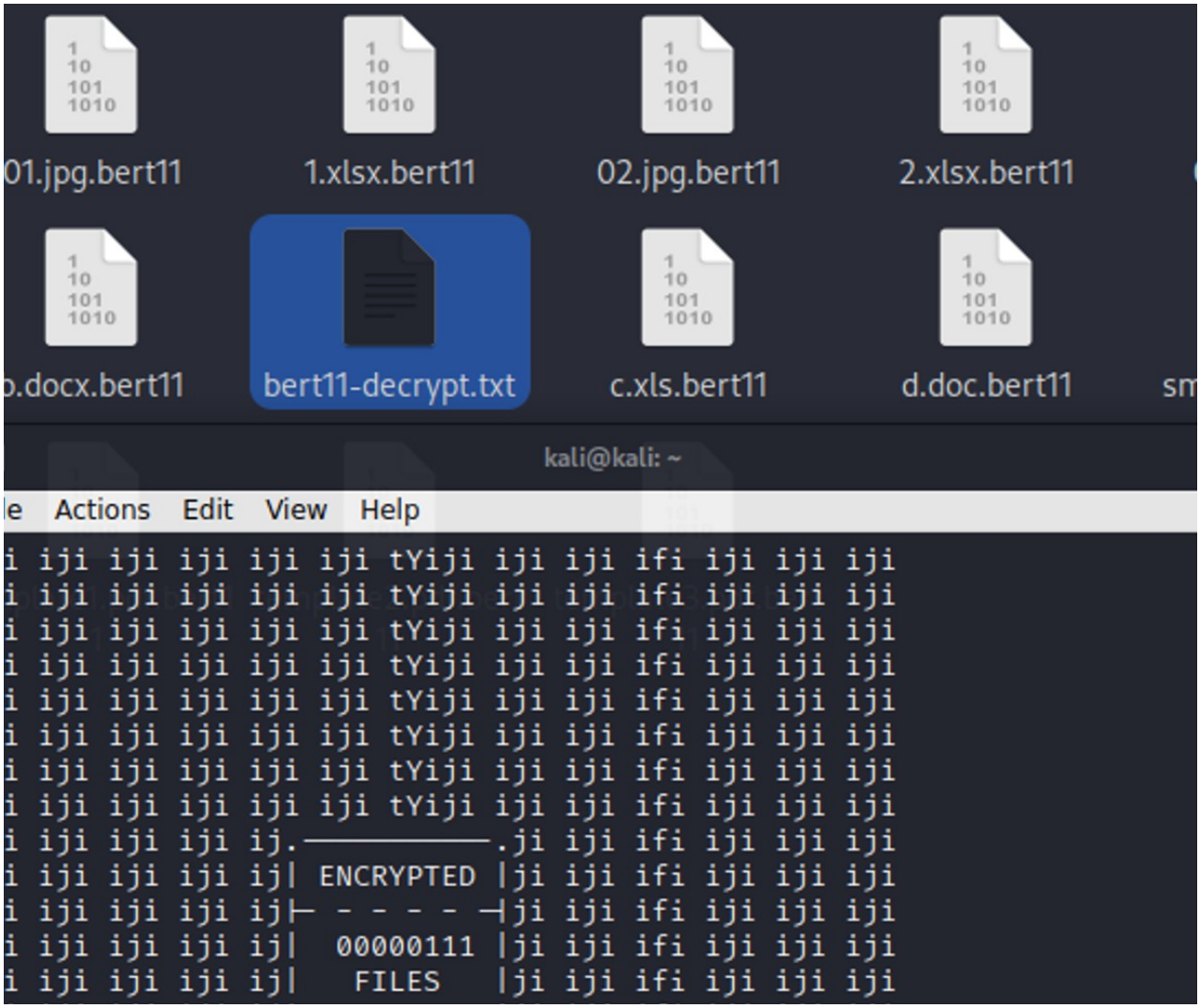
Wmansvcs是phobos家族的衍生版本，2025年6月出现后持续活跃并成为国内勒索量Top2的家族。相关勒索团伙通过某个全年均未改变过的攻击IP进行远程桌面登录投毒与横向渗透，并只攻击国内用户。这个家族在2025年有两个后缀分支的版本，分别是.peng与.wman。值得注意的是，在我们接到的受害者求助中，其设备中招前均未使用360终端安全产品进行防护，这表明，当下黑产团伙无需考虑绕过安全防护软件即可获利。



Bert

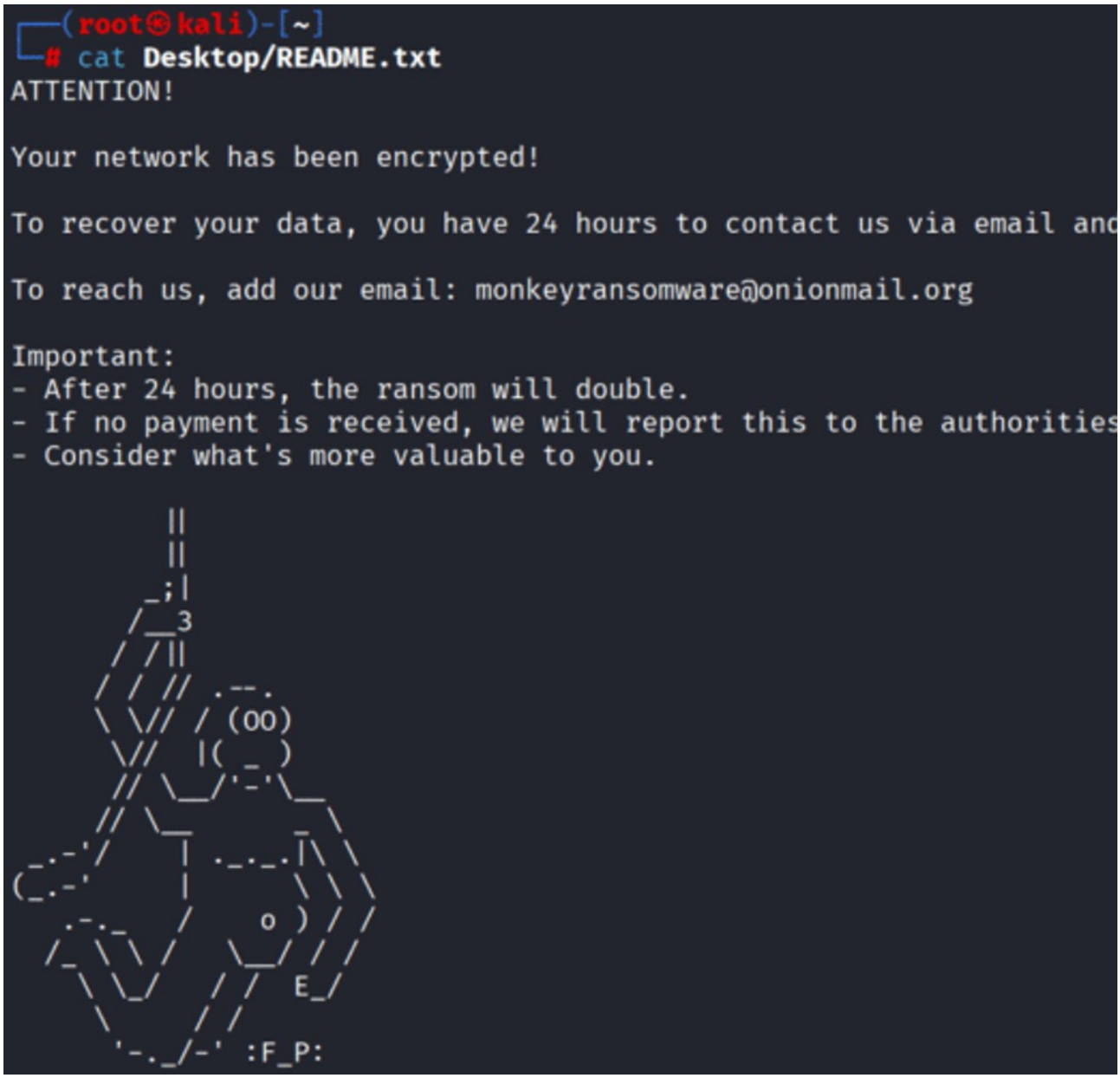
Bert勒索家族在2025年5月出现，攻击Windows与Linux平台。此家族采用Linux原生的ELF文件格式构建恶意 payload，这表明其开发者专门针对Linux系统的底层架构进行了优化。ELF文件是Linux系统中可执行文件、共享库和目标文件的标准格式，这意味着

Bert勒索软件能够直接在Linux环境中运行，无需依赖兼容性层或仿真工具，从而提升了攻击的隐蔽性和执行效率。该勒索家族的出现，与近年来Linux系统在关键基础设施中的普及密切相关。Bert勒索软件试图通过加密关键业务系统和数据来实现勒索收益最大化。



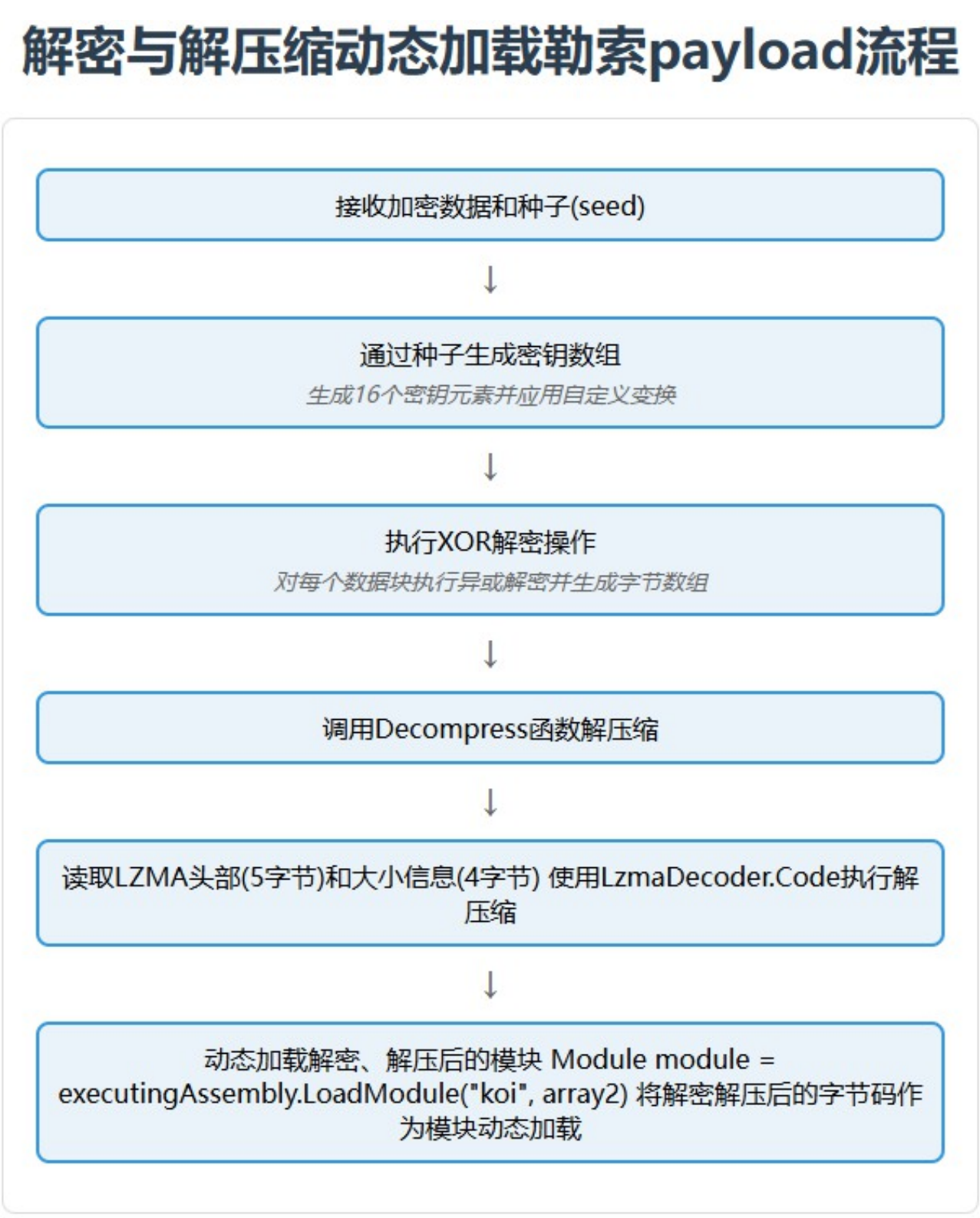
Monkey

Monkey勒索家族出现于2025年10月，攻击Windows与Linux平台。该家族具有明显的AI生成痕迹，尤其是在其Linux版本的样本中，存在删除Windows卷影副本的代码。这种代码实现方式显示出与传统人工编写恶意代码不同的特征，暗示了攻击者可能利用AI技术来辅助开发勒索软件，以提高攻击效率和隐蔽性。AI技术的引入可能使得该勒索软件在代码生成、漏洞利用等方面具有更强的适应性和创新性，给安全防护带来了新的挑战。



Kalxat

Kalxat勒索家族在2025年5月出现并仅在国内传播。该新型勒索软件展现出精密的攻击架构，其采用模块化设计，将勒索信内容、加密文件扩展名、RSA公钥等核心参数封装于独立配置文件，支持攻击者针对不同目标快速生成定制化变种，同时通过动态调整加密策略实现差异化攻击——对数据库等关键数据实施全量加密，对非核心文件采用部分加密以提升攻击效率。



SnowSoul

SnowSoul勒索家族在2025年9月出现并仅在国内传播。该家族采用对称加密与非对称加密相结合的混合方案来加密受害者文件，具有传播快、干扰面广、对生产业务影响显著等

特点。360反勒索服务对其进行了解密支持，但由于作者并未落网，其后续的变种版本需根据具体的变种文件分析算法后，重新评估解密方案。

（二）
每月新增双重、多重勒索情况

另经统计发现，2025年各月也时常出现新的勒索软件加入双重/多重勒索模式的行列中。仅360安全智能体监控到的此类双重/多重勒索软件家族，在本年度就共计新增40个。近年来还出现了具体家族名及出现时间分布如下：

2025年每月新增多重勒索软件

月份	新增双重/多重勒索软件家族	勒索模式
2025年1月	GD LockerSec	加密文件, 数据泄露
2025年2月	RunSomeWares	加密文件, 数据泄露
2025年3月	Crazyhunter	加密文件, 数据泄露
	Babuk2	加密文件, 数据泄露
	Nightspire	加密文件, 数据泄露
	Ralord	加密文件, 数据泄露
	VanHelsing	加密文件, 数据泄露
	Skira	加密文件, 数据泄露
2025年4月	Devman	加密文件, 数据泄露
	Gunra	加密文件, 数据泄露
	Silent	加密文件, 数据泄露
	Nova	加密文件, 数据泄露
2025年5月	J	加密文件, 数据泄露
	Datacarry	加密文件, 数据泄露
	DireWolf	加密文件, 数据泄露
	Worldleaks	加密文件, 数据泄露
2025年6月	WarLock	加密文件, 数据泄露
	Kawalocker	加密文件, 数据泄露
	TeamXXX	加密文件, 数据泄露
2025年7月	BaqiyatLock	加密文件, 数据泄露
	Satanlockv2	加密文件, 数据泄露

月份	新增双重/多重勒索软件家族	勒索模式
2025年8月	Desolator	加密文件, 数据泄露
2025年9月	The Gentlemen	加密文件, 数据泄露
	Coinbase Cartel	加密文件, 数据泄露
	Miga	加密文件, 数据泄露
	Arachna	加密文件, 数据泄露
	WhiteLock	加密文件, 数据泄露
2025年10月	Tengu	加密文件, 数据泄露
	Kyber	加密文件, 数据泄露
	Genesis	加密文件, 数据泄露
	Brotherhood	加密文件, 数据泄露
	Radiant	加密文件, 数据泄露
	Nasirsecurity	加密文件, 数据泄露
2025年11月	Tridentlocker	加密文件, 数据泄露
2025年12月	MintEye	加密文件, 数据泄露
	MS13-089	加密文件, 数据泄露
	Sicari	加密文件, 数据泄露
	Osiris	加密文件, 数据泄露
	Dark Shinigamis	加密文件, 数据泄露

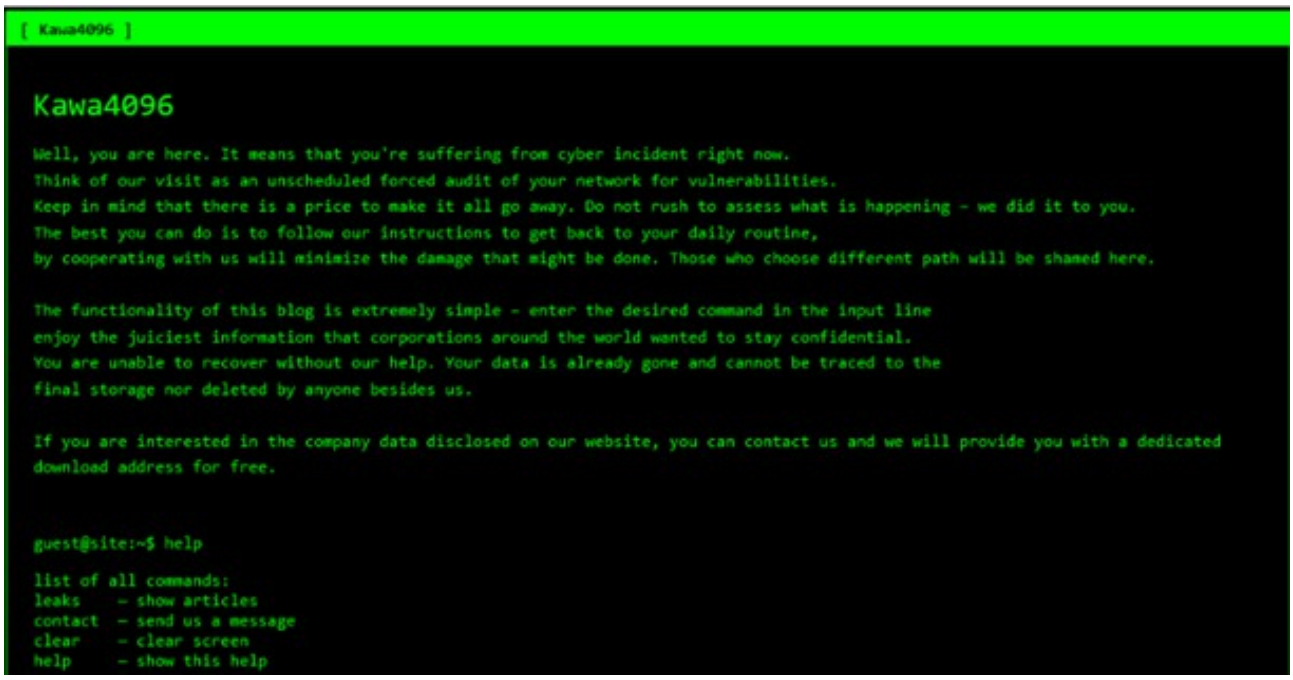
▲2025年各月新增双重/多重勒索软件家族

针对以上新增双重/多重勒索软件家族，我们对其中几个典型家族进行具体的说明：

KawaLocker

KawaLocker勒索家族，也被称为KAWA4096，是一个于2025年6月首次出现的新型勒索软件。该家族在发展早期就获得了较高的关注度，其部分特征与其他勒索软件变种存在相似之处，例如，其数据泄露网站设计与Akira勒索软件的泄露网站相似，而勒索信则与Qilin勒索软件几乎相同。

KawaLocker勒索家族在攻击过程中，会通过远程桌面协议访问受害者的设备。登录后采用多种手段识别和致盲受害设备上的安全工具，包括部署kill.exe与HRSword。HRSword旨在监控各种系统组件，能让攻击者获得对整个系统的可见性与结束任意进程。

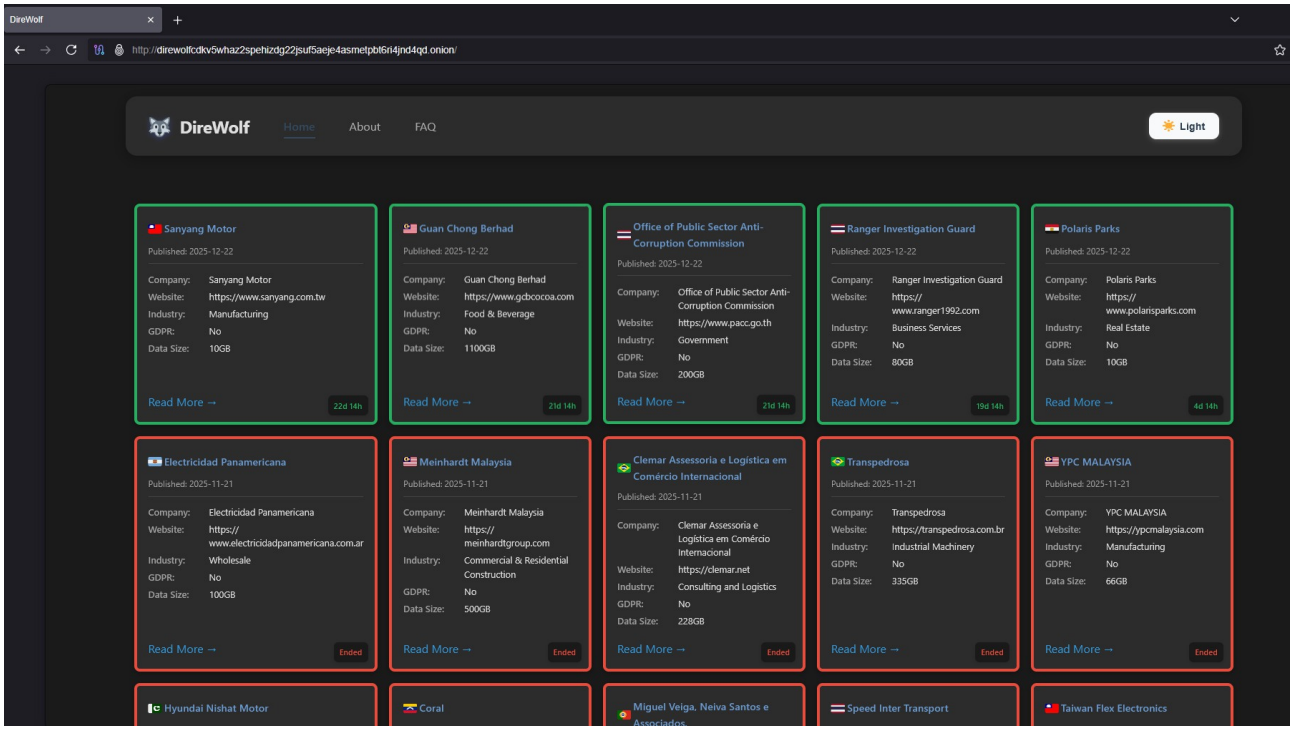


▲ KawaLocker家族发布页

DireWolf

DireWolf是一个于2025年5月出现的勒索软件组织，采用双重勒索模型，主要针对制造业和科技行业，活动范围覆盖全球多个国家。其中亚太地区为核心目标，包括美国、泰国、台湾、新加坡、印度等地区。该组织以其高度专业化的攻击策略和技术成熟度著称，被认为是继LockBit和Conti等老牌勒索家族后崛起的新兴威胁。

DireWolf采用Golang编写，具有跨平台特性。结合Curve25519密钥交换和ChaCha20流加密算法，加密强度高，且每个文件生成随机会话密钥。

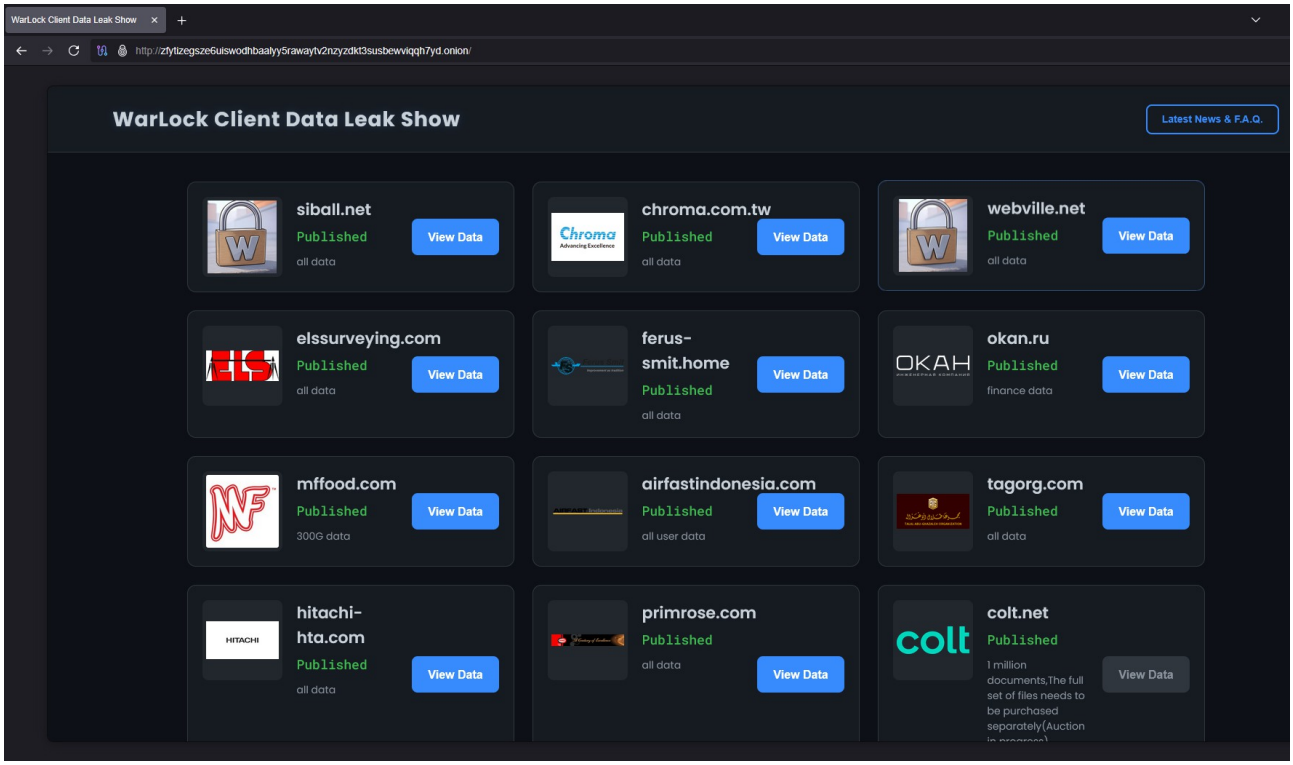


▲以上为DireWolf家族的发布页

WarLock

WarLock勒索家族是一个具有较高威胁性的勒索软件，基于泄露的LockBit 3.0构建器定制的衍生版本。该家族主要通过攻击企业级网络，加密受害者数据以勒索赎金，采用了勒索软件即服务（RaaS）模式，并且在攻击过程中展现出了复杂的战术、技术和流程，对全球多个行业的组织造成了严重影响。

WarLock勒索家族的主要初始访问途径是利用Microsoft SharePoint服务器的多个高危漏洞，形成所谓的ToolShell组合攻击，其中包括CVE-2025-49704、CVE-2025-49706、CVE-2025-53770和CVE-2025-53771等。攻击者通过向SharePoint服务器的ToolPane端点发送恶意POST请求，绕过身份验证并实现远程代码执行，进而部署ASPX webshell，以获取对服务器的初始控制权。在成功利用漏洞后，攻击者会通过web



▲ 以上为WarLock家族的官方页面

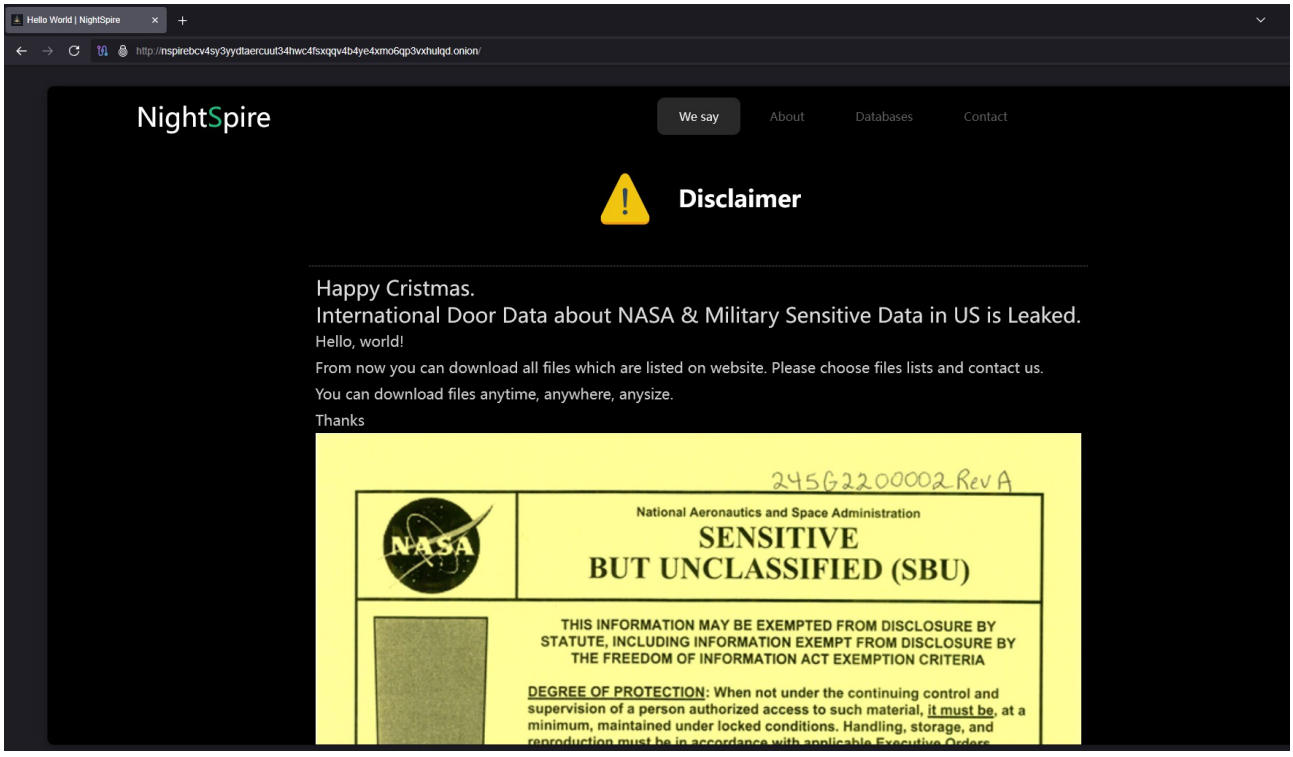
Nightspire

Nightspire勒索家族最早出现于2025年3月，有高度可能性是Rbfs勒索团伙的变种或品牌重塑。从多方面证据来看，两团伙存在密切关联：首先，它们共享操作员，且已知受害者重叠；其次，随着Nightspire的出现，Rbfs勒索团伙在网上的相关引用已停止；再者，

Nightspire的泄露网站显示，至少有两名受害者此前曾被Rbfs勒索团伙声称攻击过。该家族有两名已知附属机构xdragon128和cuteliyuan，他们早在2025年3月就曾在线推广Rbfs勒索软件。2025年3月2日，xdragon128在BreachForums 2上宣传Rbfs勒索软件攻击的受害者；几天后的3月6日，cuteliyuan分享了一个Telegram链接以展示该团伙的受害者，但该频道已不再活跃。

Nightspire是一个以经济利益为驱动的团伙，采用机会主义策略，针对所有行业发起攻击。其主要目的是从目标中窃取敏感信息，通过勒索或将受害者数据出售给第三方来获利。该团伙在窃取数据后，还会部署有效载荷对数据进行加密。Nightspire在2025年已对受害者数据进行加密，这表明该团伙已从仅进行数据勒索的运营模式转变为更传统的双重勒索模式。

Nightspire利用了CVE-2024-55591，这是一个FortiOS零日漏洞，允许未授权的攻击者在不提供有效凭证的情况下，获得对Fortigate防火墙设备的超级管理员访问权限。该团伙设有一个名为“We say”的“点名羞辱”页面，专门针对不付款的受害者。该页面上的内容包括受害者的公司名称、关于可用被盗数据的公告，在某些情况下还包括免费下载链接。



▲以上为Nightspire家族的“We say”页面

BaqiyatLock

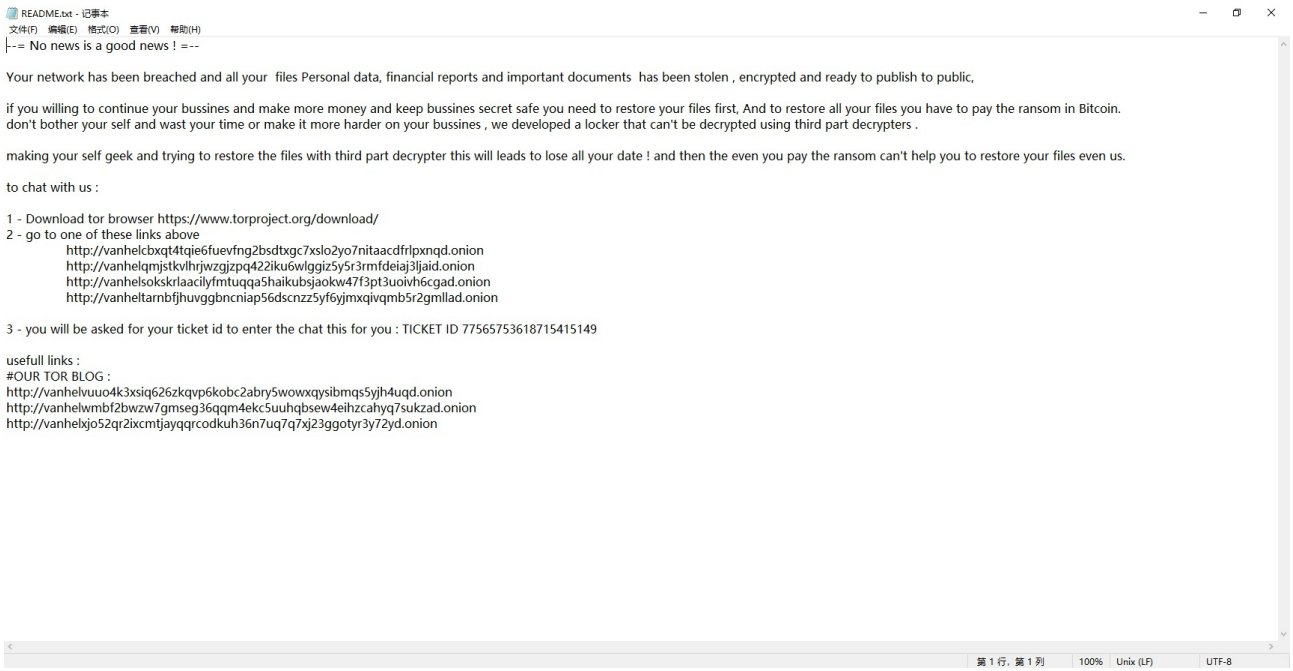
BaqiyatLock勒索家族(又称BQTLock),最早出现于2025年7月，采用勒索软件即服务（RaaS）模式运营。该家族与据称是亲巴勒斯坦黑客组织Liwaa Mohammed的领导人“ZerodayX”相关联，ZerodayX还与沙特游戏数据泄露事件有关。

BaqiyatLock主要通过恶意ZIP档案进行分发，该档案包含名为Update.exe的文件，负责加密本地所有类型的文件，附加自定义扩展名，并放置带有说明的勒索通知。攻击者还可能利用服务漏洞、钓鱼活动、软件漏洞和供应链攻击等方式获取初始访问权限。这个黑客组织的负责人在社交媒体上较为活跃，在积极推广的同时还经常与安全分析人员互相嘲讽，算是一个比较有意思的插曲。

▲ 以上为BaqiyatLock家族修改的桌面壁纸

VanHelsing

VanHelsing勒索软件组织最早出现于2025年3月，采用勒索软件即服务（RaaS）模式运作。其已经展示了快速的增长和致命的潜力，知名的合作方可以免费加入，而新合作方必须支付5000美元的押金才能获得该计划的访问权限。在受害者支付赎金的两笔区块链确认之后，合作方将获得80%的收入，其余20%支付给RaaS运营商。合作方提供了一个易于使用的控制面板来管理攻击，并且有一个跨平台的加密工具VanHelsing，它针对包括“Windows、Linux、BSD、ARM和VMware ESXi系统”在内的各种系统。由于该家族代码实现层面存在缺陷，导致部分加密场景即使有准确的解密工具也会无法解密。值得注意的是，该组织的源码很快就被完整泄露，进而导致后续此家族的活跃度降低。


README.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

--= No news is a good news ! =--

Your network has been breached and all your files Personal data, financial reports and important documents has been stolen , encrypted and ready to publish to public,

if you willing to continue your bussines and make more money and keep bussines secret safe you need to restore your files first, And to restore all your files you have to pay the ransom in Bitcoin.
don't bother your self and wast your time or make it more harder on your bussines , we developed a locker that can't be decrypted using third part decrypters .

making your self geek and trying to restore the files with third part decrypter this will leads to lose all your date ! and then the even you pay the ransom can't help you to restore your files even us.

to chat with us :

1 - Download tor browser https://www.torproject.org/download/
2 - go to one of these links above
http://vanhelcbxqt4tqie6fuevfng2bsdtxgc7xslo2yo7nitaacdfrlpxnqd.onion
http://vanhelqmjstkvlhrjwzgjzpq422iku6wlggiz5y5r3rmfdeiaj3ljaid.onion
http://vanhelsokskrlaacilyfmtuqqa5haikubsjaokw47f3pt3uoivh6cgad.onion
http://vanheltarnbfjhuvggbncniap56dscnzz5yf6yjmxqivqmb5r2gmllad.onion

3 - you will be asked for your ticket id to enter the chat this for you : TICKET ID 77565753618715415149

usefull links :
#OUR TOR BLOG :
http://vanhelvuuo4k3xsiq626zkqvp6kobc2abry5wowxqysibmqs5yjh4uqd.onion
http://vanhelwmbf2bwzw7gmseg36qqm4ekc5uuhqbsew4eihzcahyq7sukzad.onion
http://vanhelxjo52qr2ixcmtjayqqrcodkuh36n7uq7q7xj23ggotyr3y72yd.onion

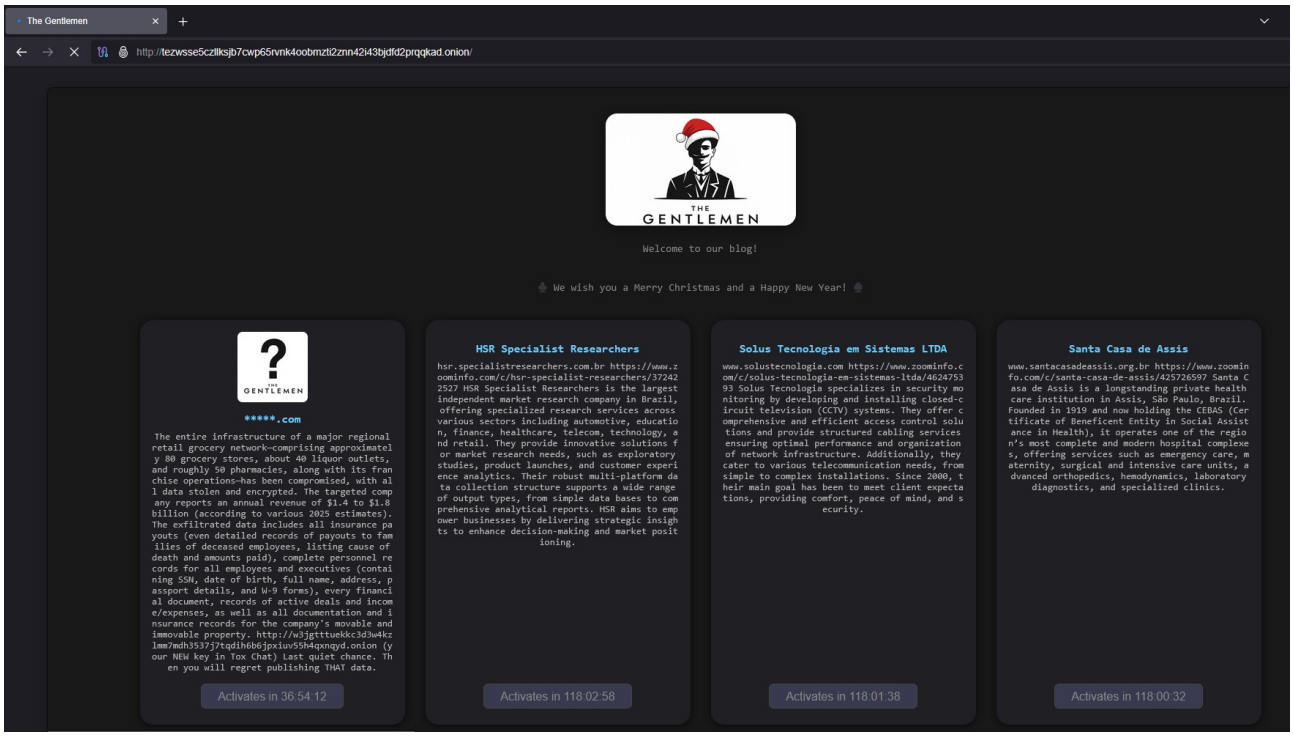
第 1 行，第 1 列 100% Unix (LF) UTF-8

▲ 以上为VanHelsing家族勒索信

The Gentlemen

The Gentlemen勒索家族是2025年新出现的高度活跃威胁组织，首次被发现于2025年7月，其快速扩张使其成为年度最受关注的勒索团伙之一。该组织名称疑似借鉴盖·里奇电影《绅士们》，并采用专业品牌形象，包括暗网泄漏站点和定制化勒索信。支持平台包括Windows、Linux、VMware ESXI、UNIX、NAS。

The Gentlemen勒索软件采用Go语言开发，通过强制密码参数限制执行环境，防止在分析环境中运行。命令行参数支持定制化加密目标、速度和模式。结合X25519密钥交换和XChaCha20流密码算法，为每个文件生成唯一密钥和随机数。对小于1MB的文件进行全加密，大于1MB的文件则采用分段加密以平衡效率。攻击时会利用合法驱动ThrottleStop.sys的CVE-2025-7771漏洞执行BYOVD攻击，终止EDR防护进程。Windows下通过组策略操纵实现域内传播。在Linux系统中，通过system-level autostart实现持久化，并支持从普通用户权限提升至root权限。

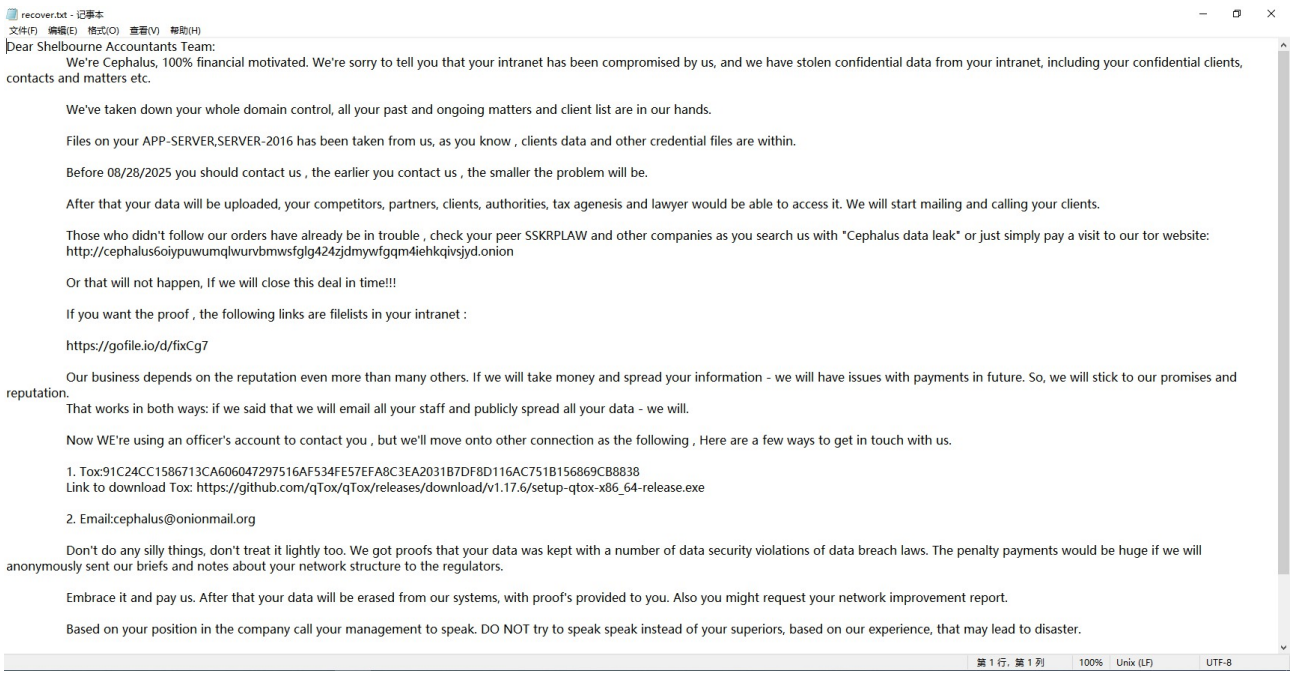


▲ 以上为The Gentlemen家族的发布页

Cephalus

Cephalus勒索家族于2025年6月首次被发现，名称来源于希腊神话中手持“无虚发之矛”的人物Cephalus，象征其对攻击成功率的自信。该家族为纯金融动机的勒索组织，采用数据窃取+文件加密的双重勒索策略。其恶意代码使用Go语言开发，具有较强的反分析和环境适配能力。

Cephalus主要通过暴力破解或购买未启用多因素认证的RDP凭证，利用远程桌面协议直接登录目标系统。入侵后使用MEGA云存储平台进行数据窃取，涉及财务记录、法律文件、客户数据等敏感信息。通过伪装合法SentinelOne安全软件的SentinelBrowserNativeHost.exe实现DLL侧加载，加载恶意SentinelAgentCore.dll后，进一步执行data.bin中的勒索代码。该白利用手法利用安全软件白名单特性规避检测。


recover.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

Dear Shelbourne Accountants Team:

We're Cephalus, 100% financial motivated. We're sorry to tell you that your intranet has been compromised by us, and we have stolen confidential data from your intranet, including your confidential clients, contacts and matters etc.

We've taken down your whole domain control, all your past and ongoing matters and client list are in our hands.

Files on your APP-SERVER,SERVER-2016 has been taken from us, as you know , clients data and other credential files are within.

Before 08/28/2025 you should contact us , the earlier you contact us , the smaller the problem will be.

After that your data will be uploaded, your competitors, partners, clients, authorities, tax agenesis and lawyer would be able to access it. We will start mailing and calling your clients.

Those who didn't follow our orders have already be in trouble , check your peer SSKRPLAW and other companies as you search us with "Cephalus data leak" or just simply pay a visit to our tor website:
http://cephalus6oiypuwumqlwurvbmwsfglg424zjdmywfgqm4iehkqivsjyd.onion

Or that will not happen, If we will close this deal in time!!!

If you want the proof , the following links are filelists in your intranet :

https://gofile.io/d/fixCg7

Our business depends on the reputation even more than many others. If we will take money and spread your information - we will have issues with payments in future. So, we will stick to our promises and reputation.
That works in both ways: if we said that we will email all your staff and publicly spread all your data - we will.

Now WE're using an officer's account to contact you , but we'll move onto other connection as the following , Here are a few ways to get in touch with us.

1. Tox:91C24CC1586713CA606047297516AF534FE57EFA8C3EA2031B7DF8D116AC751B156869CB8838
Link to download Tox: https://github.com/qTox/qTox/releases/download/v1.17.6/setup-qtox-x86_64-release.exe

2. Email:cephalus@onionmail.org

Don't do any silly things, don't treat it lightly too. We got proofs that your data was kept with a number of data security violations of data breach laws. The penalty payments would be huge if we will anonymously sent our briefs and notes about your network structure to the regulators.

Embrace it and pay us. After that your data will be erased from our systems, with proof's provided to you. Also you might request your network improvement report.

Based on your position in the company call your management to speak. DO NOT try to speak speak instead of your superiors, based on our experience, that may lead to disaster.

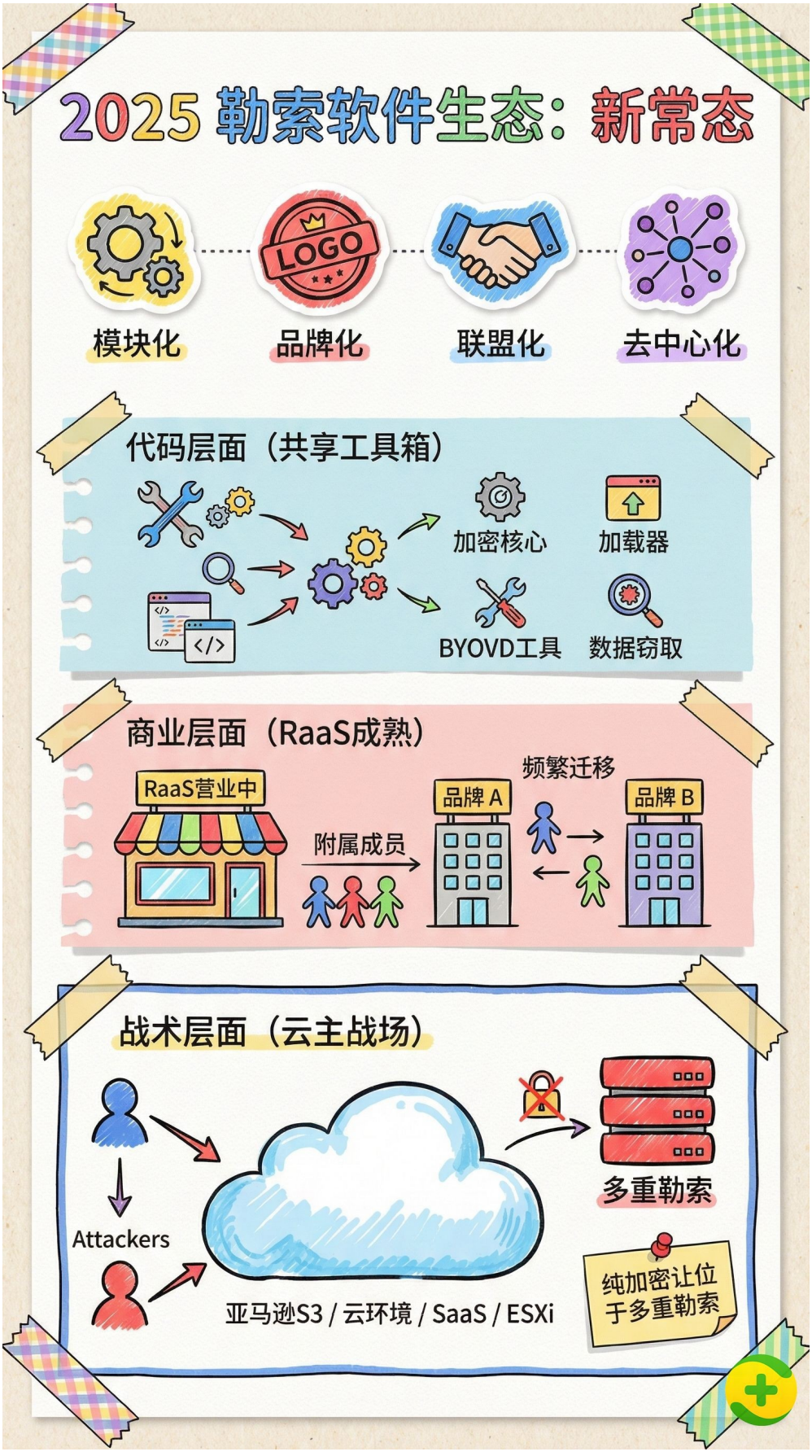
第 1 行，第 1 列 100% Unix (LF) UTF-8

▲ 以上为Cephalus家族的勒索信

（三）
家族衍生关系

2025年的勒索软件生态呈现出高度“模块化、品牌化、联盟化、去中心化”的特征。表现在以下几个方面：

- **代码层面**：大量家族共享或直接复用同一加密核心、加载器、BYOVD漏洞利用工具、数据窃取工具、渗透框架、穿透代理等。
- **商业层面**：RaaS模式全面成熟，家族更像“品牌”，其成员与附属团伙频繁迁移。
- **战术层面**：纯加密让位于多重勒索，亚马逊S3/各类云环境/SaaS/ESXi成为主战场。
- **演进逻辑**：不是线性的新老更替，而是在全球监管压力与同行“黑吃黑”的现实中不断分支、复活、重塑以及联盟合并。


2025 勒索软件生态：新常态
LOGO
模块化
品牌化
联盟化
去中心化
代码层面（共享工具箱）
加密核心
加载器
BYOVD工具
数据窃取
商业层面（RaaS成熟）
RaaS营业中
附属成员
品牌 A
频繁迁移
品牌 B
战术层面（云主战场）
Attackers
亚马逊S3 / 云环境 / SaaS / ESXi
多重勒索
纯加密让位于多重勒索

核心加密代码的衍生关系

Ryuk/Conti系列的衍生与重组，conti被制裁与打击之后，分散为多个勒索家族，衍生出一系列勒索家族，他们使用相同的攻击链路，如：RDP、VPN、ESXi、Confluence等。使用相似的赎金谈判与泄露站点结构,主要有下面一些：

- Black Basta家族，其战术、代码、人员高度继承自Conti勒索家族。
- Hunters International家族，重点攻击Oracle/ESXi/SaaS目标。
- Akira家族，使用相似横向与凭证滥用战术。
- Interlock、Lynx 、Play家族，部分战术继承。

Conti是人员迁移演进的一类代表。

Babuk系列，LockBit/Alphv/Babuk均源自Babuk代码泄露，且后续分支出现多次泄露。

其主要分支：

●Babuk/Babuk2/Babuk-Ba/Babuk2S家族

●LockBit虽独立进化，但大量吸收了大量Babuk家族成员。

●Alphv/BlackCat家族，采用了很多激进的社工方式进行勒索。

2025年的一些表现：

LockBit5.0品牌回归与基础设施重建，360独家确认引入社会工程学方式定向钓鱼投毒。

LockBit3.0泄露代码的衍生家族数量庞大，在国内有持续的受害反馈。

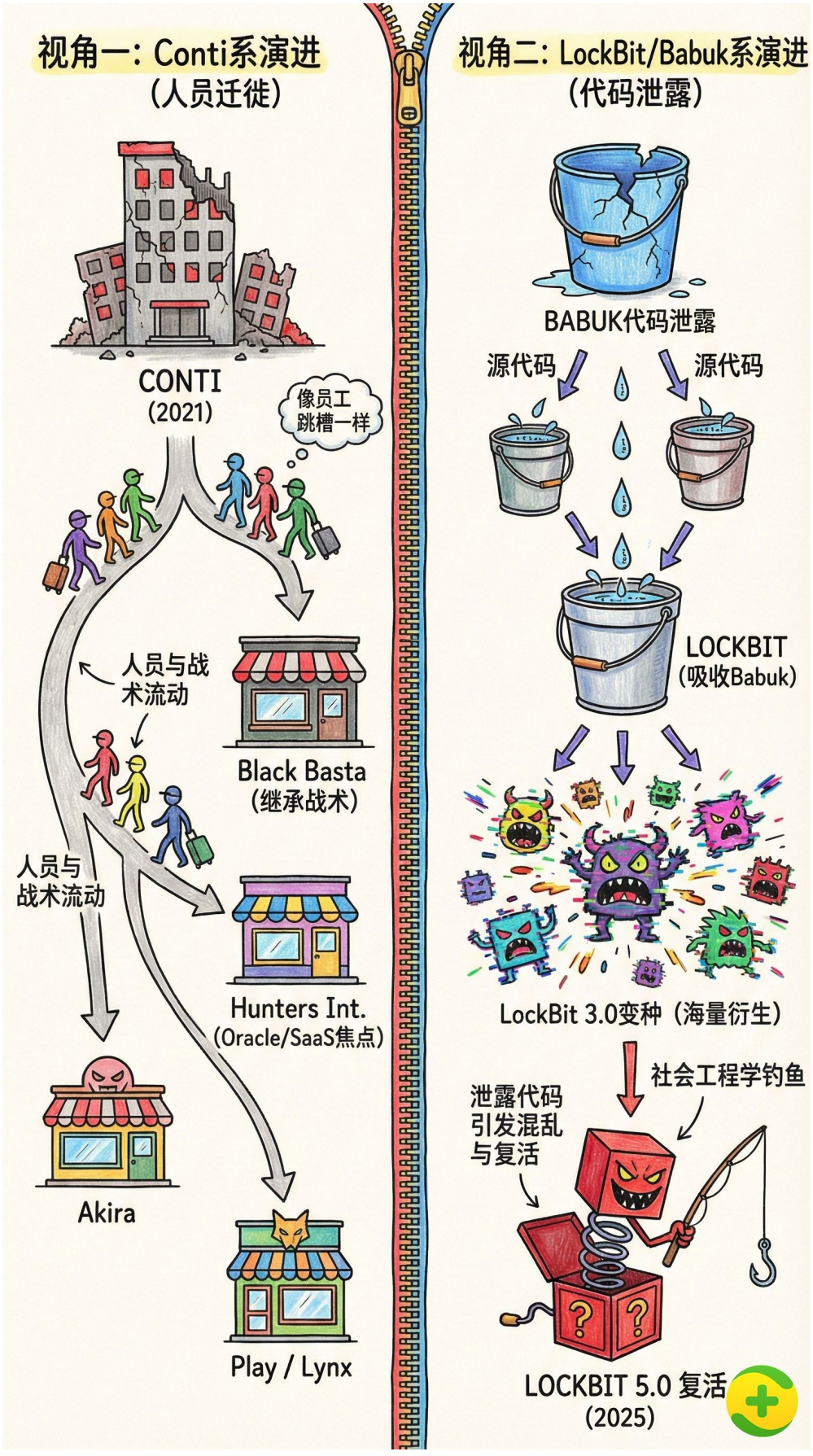
LockBit系是代码泄露类的演进代表。

RansomHub家族起源自2024年后，与ShadowSyndicate合作形成了勒索联盟，吸收BlackCat、LockBit、Conti勒索家族的前附属成员，其技术特征包括：使用Python/Go/Rust多语言；利用Skuld/StealC数据窃取；擅长EDRKillShifter/BYOVD漏洞利用；使用亚马逊S3加密。其衍生与关联：

●Codefinger亚马逊S3定向攻击

●GD LockerSec新的数据泄漏站点

RansomHub是联盟化的演进代表。

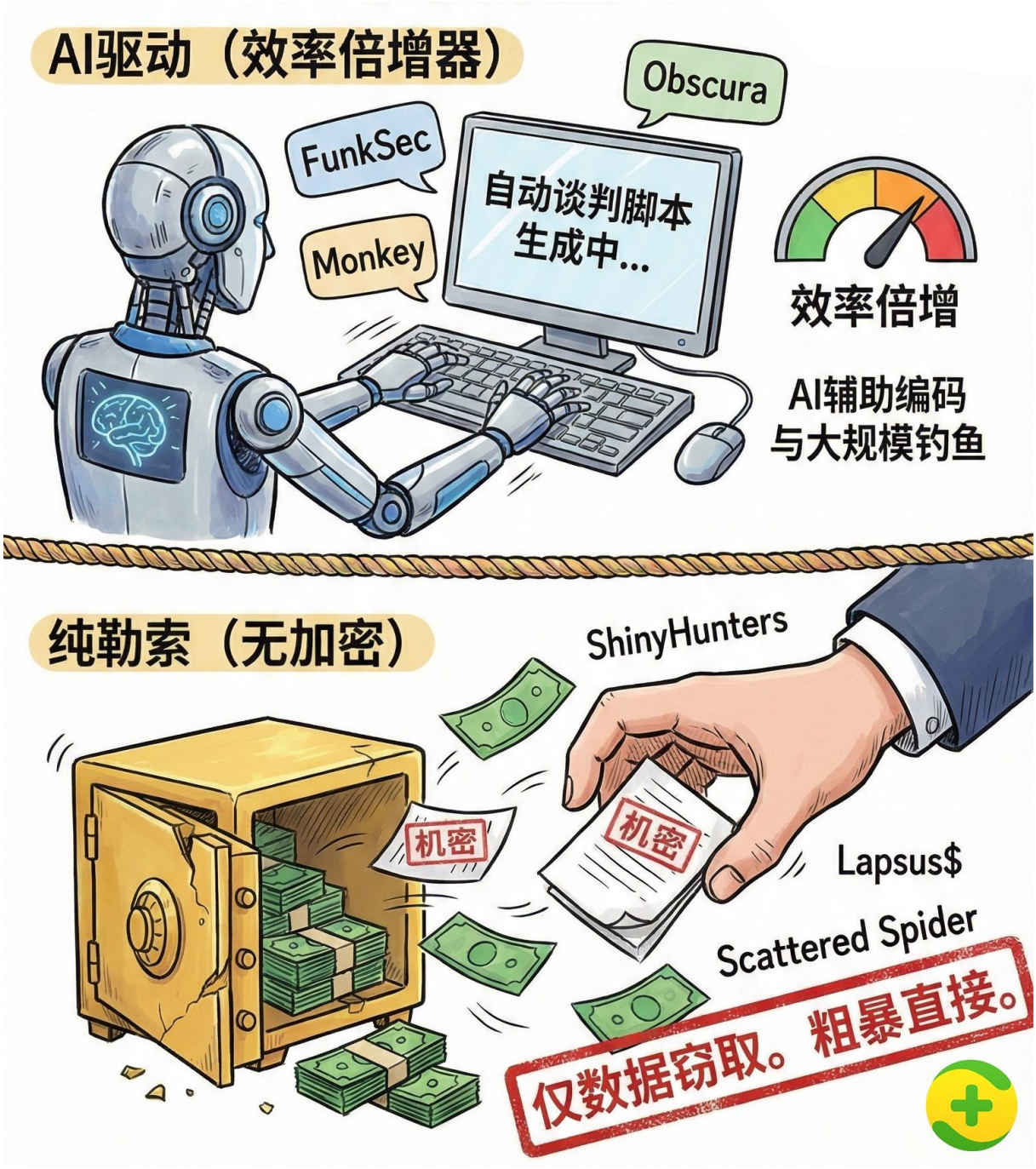

视角一：Conti系演进
（人员迁徙）
CONTI
(2021)
像员工
跳槽一样
人员与战
术流动
Black Basta
（继承战术）
人员与
战术流动
Hunters Int.
(Oracle/SaaS焦点)
Akira
Play / Lynx
视角二：LockBit/Babuk系演进
（代码泄露）
BABUK代码泄露
源代码
源代码
LOCKBIT
（吸收Babuk）
LockBit 3.0变种（海量衍生）
社会工程学钓鱼
泄露代码
引发混乱
与复活
LOCKBIT 5.0 复活
(2025)

Ai自动化驱动的家族：

FunkSec家族由AI辅助开发、运营。此类还包括Monkey、FunkLocker、Obscura家族。此类家族使用LLM辅助代码生成、创建自动谈判脚本并利用大规模钓鱼传播。AI介入尚处在初始阶段，属于效率倍增器的范畴。

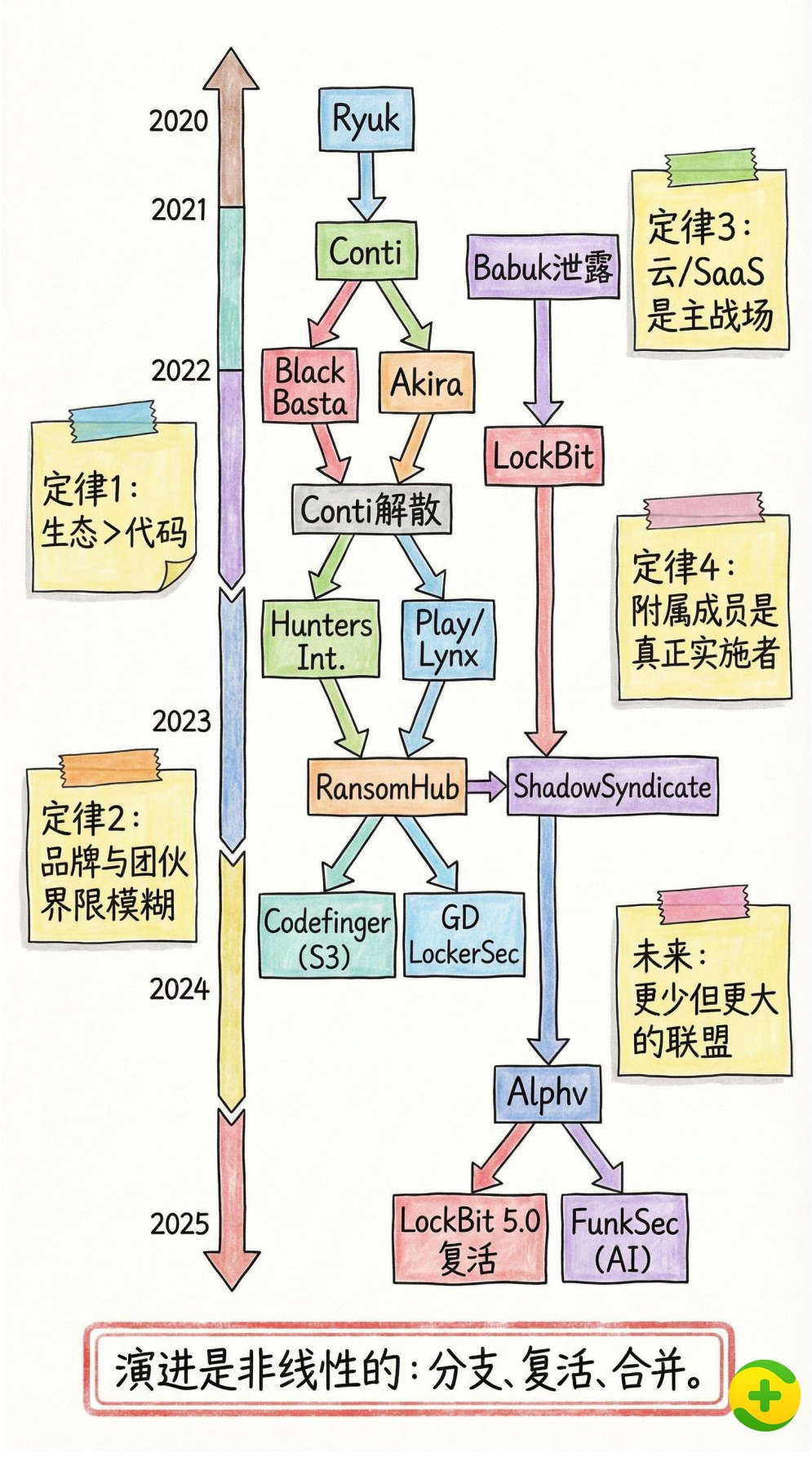
无加密或轻加密纯勒索路线的代表家族：

ShinyHunters、Scattered Spider、Lapsus$联盟，进行数据窃取无需部署加密器。相关家族是勒索获利更加粗暴与直接的典型。



2025 年勒索软件“演化规律”可以总结为以下几点：

- 生态是维系勒索家族的重要纽带，而非代码
- 品牌、团伙、开发者界限模糊，勒索家族交流广泛
- 云环境、ESXi、SaaS服务成为勒索攻击主战场
- 未来，将是越来越多的勒索联盟，而非独立的勒索家族


2020
2021
2022
2023
2024
2025
Ryuk
Conti
Babuk泄露
Black Basta
Akira
LockBit
Conti解散
Hunters Int.
Play/ Lynx
RansomHub
ShadowSyndicate
Codefinger (S3)
GD LockerSec
Alphv
LockBit 5.0 复活
FunkSec (AI)
定律1：生态>代码
定律2：品牌与团伙界限模糊
定律3：云/SaaS是主战场
定律4：附属成员是真正实施者
未来：更少但更大的联盟
演进是非线性的：分支、复活、合并。

第二章

勒索软件受害者分析

勒索软件受害者分析

我们根据2025年，360反勒索服务问卷调查结果，汇总了本年度勒索软件受害人群数据画像。在受攻击地域分布方面并没有显著变化，数字经济发达地区以及人口密集地区依然是受攻击的主要区域。而受感染的操作系统、所属行业则受年度流行的勒索软件家族影响，有着较为明显的变化。

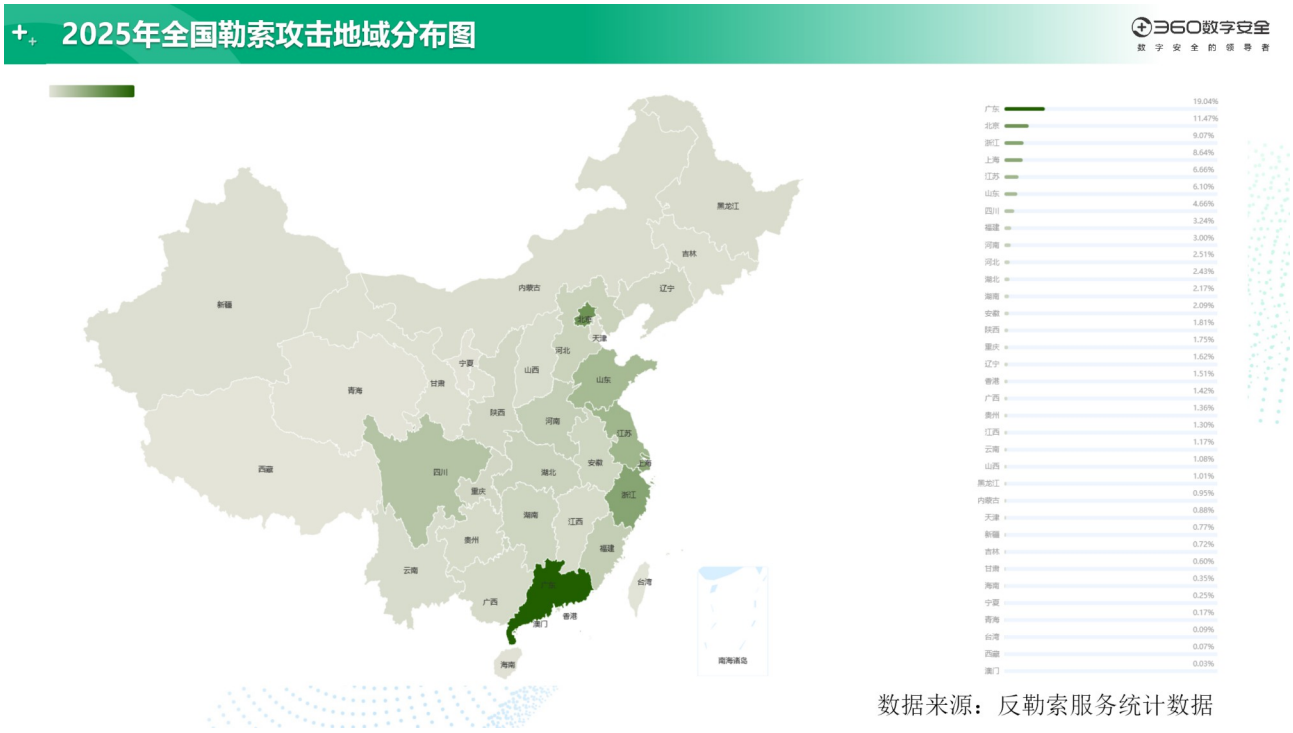
一

受害者所在地域分布

以下是对2025年攻击系统所属地域采样制作的分布图，总体分布态势变化并不明显。以北上广、江浙沪为代表的数字经济发达区域，受勒索软件影响显著高于其他区域。

数据来源：反勒索服务统计数据

下面使用地图更直观地展示这一结果：



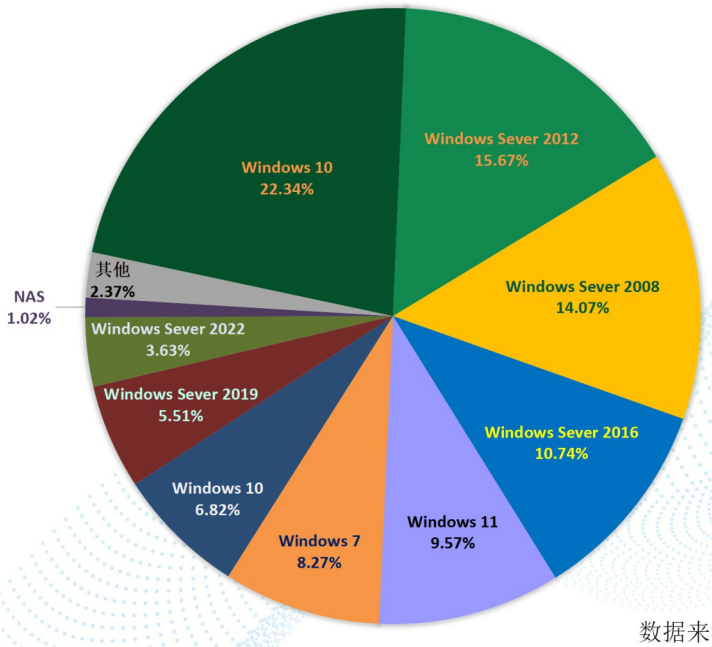
数据来源：反勒索服务统计数据

二

受攻击系统分布

对2025年受攻击的操作系统数据进行统计，位居前三的系统为Windows 10、Windows Server 2012和Windows Server 2008。其中，Windows 10系统的占比虽然依旧位居第一，但相较2024年有明显回落。出现这一现象主要是Windows10已经进入生命末期，更多地被Windows 11替代；但另一方面，本年度针对中大型政企单位的攻击占比升高，也导致了Server系统的占比略有升高，这也是Windows 10这类桌面终端系统占比下降的原因之一。

2025年受勒索软件影响操作系统占比

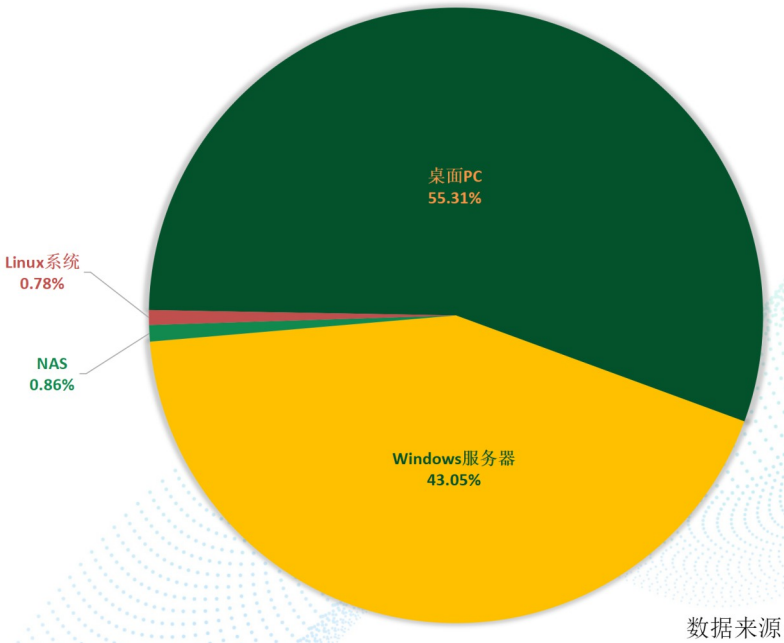


数据来源：反勒索服务统计数据

从操作系统类型的角度看，随着Windows 10的占比回落，桌面PC的占比也同样回落到了55.31%。而针对Linux及NAS系统的攻击量则依然稳定存在但占比不高。

本年度桌面PC占比的回落也再次提醒广大政企机构，尤其是部分中大规模的相关单位应更加关注数字安全的保护。与我们此前的研判相符，勒索软件在2025年针对服务器的攻击发力迅猛，针对政企目标的攻击渐成勒索软件的发展趋势。

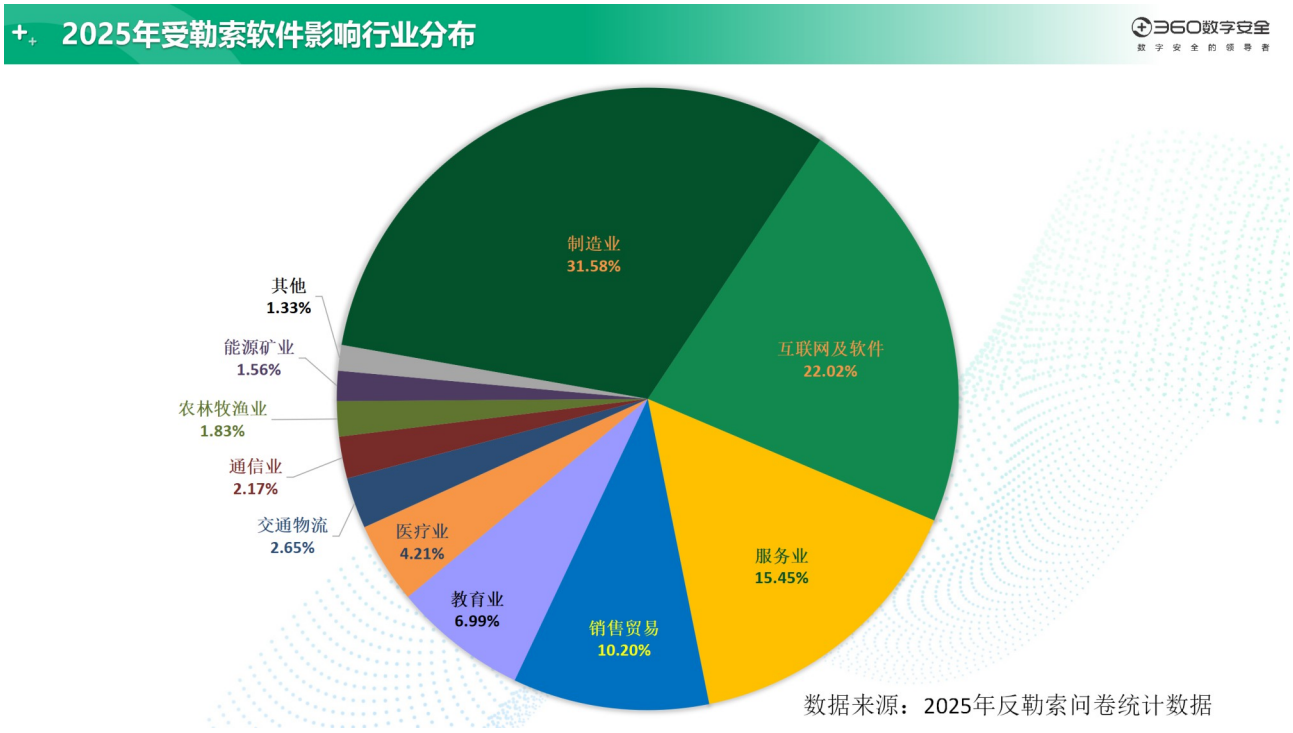
2025年受勒索软件影响操作系统类型占比



数据来源：反勒索服务统计数据

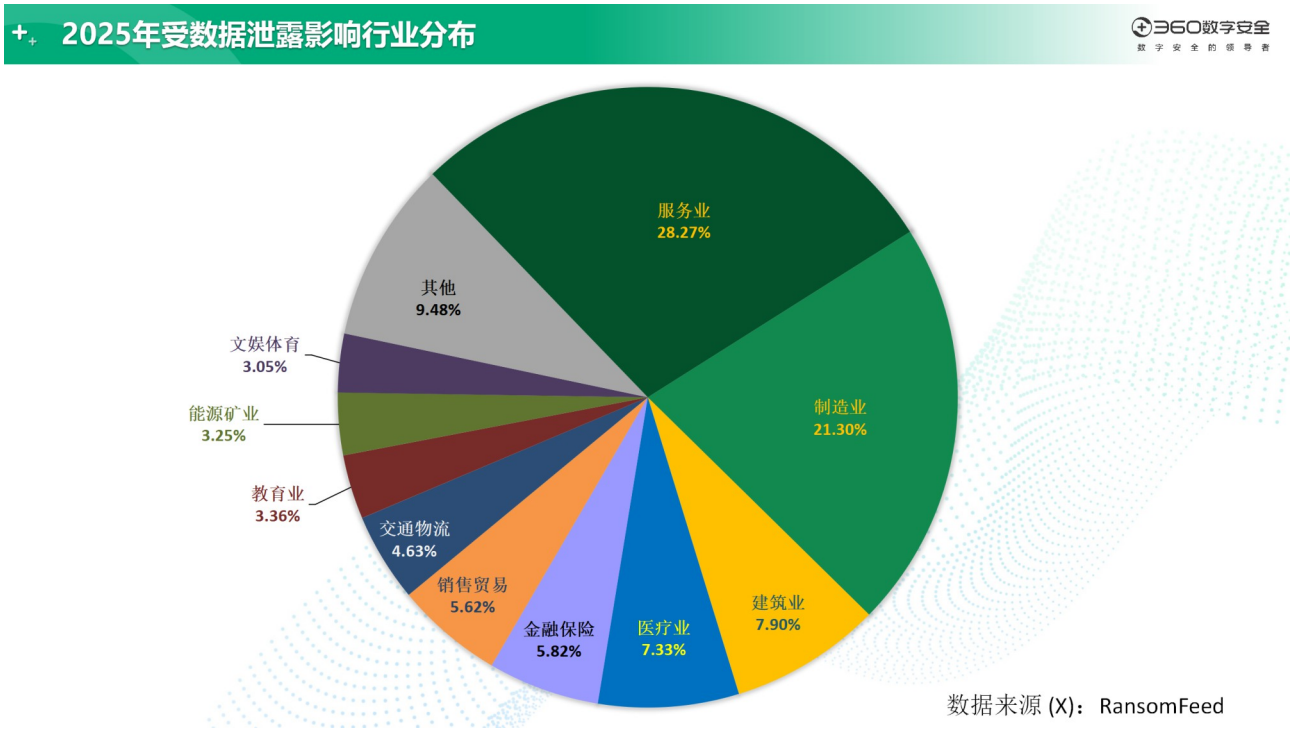
三
受害者所属行业

对来自反勒索服务申诉的受害者行业进行分析，发现制造业、互联网及软件服务、服务业三个大类位居受害者行业前三。此外，颇为敏感的医疗行业也榜上有名。虽然排名先后有所变化，但头部行业并没有较为本质的区别。主要还是集中在对互联网数据或数字自动化依赖程度较高的行业领域，这类行业信息化程度更高，有更多被勒索攻击的暴露面。同时，此类企业的数据资产价值较高，支付的意愿更高，这些特点往往也意味着攻击者有更大可能性从其手中攫取更大的利益。



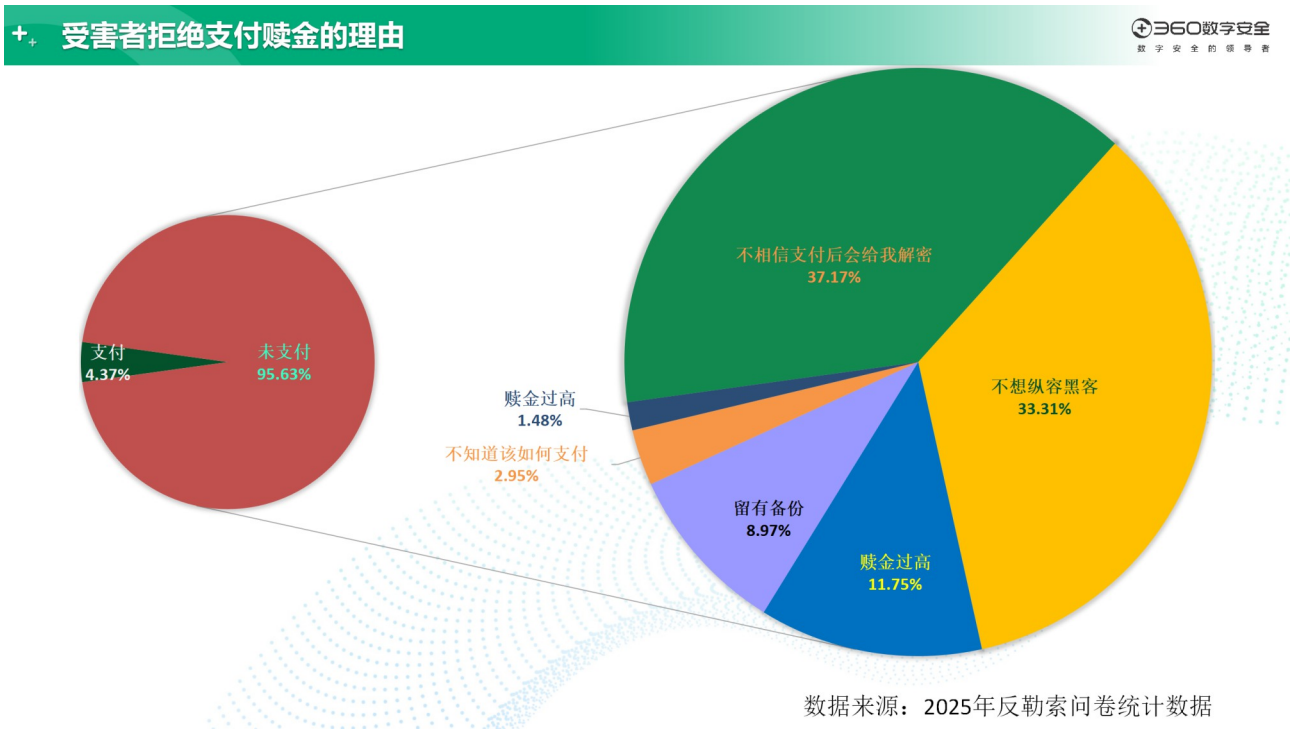
数据来源：2025年反勒索问卷统计数据

当前，双重/多重勒索已成为中大型企业的主流勒索手段，其中服务贸易、制造业、医疗、金融行业常年位居双重勒索前列。



四
受害者支付赎金情况

2025年，受害者支付勒索赎金的情况依然没有显著变化。与往年相似，大多数受害者并不会支付勒索赎金。不支付的理由则依然是不信任或不纵容的态度。此外，越来越高的勒索赎金也让部分受害者望而却步。而“留有备份”这一选项的进一步提升，也显示出用户数据安全的认知和行动的进一步提升。

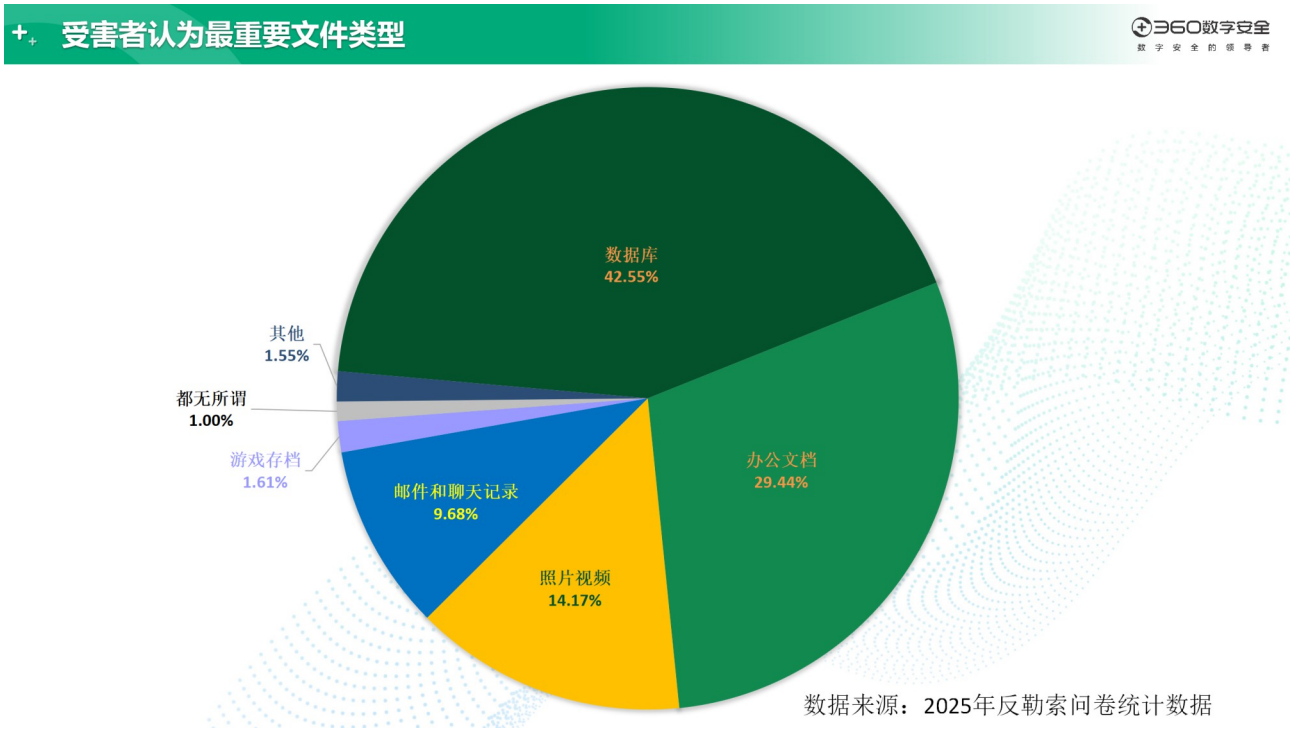


数据来源：2025年反勒索问卷统计数据

支付赎金的占比虽然依旧很低，但相较2024年还是有小幅上涨。经分析，这与勒索软件进一步地侧重于针对政企单位的攻击有着密切关系。尤其是中大型企业在受到攻击后，往往会权衡利弊，选择更为稳妥及快速的解决方案来尽可能地降低损失。而普通人看似高昂的勒索赎金在中大型企业可能面临的巨大损失面前，通常就显得并没有那么不可接受了。

五
对受害者影响最大的文件类型

基于2025年的问卷数据统计分析，数据库和办公文档两类依然分列受害者最重要的被加密数据类型，排名前两位。不过与2024年度略有区别的是，两者的排名先后产生了对调。且数据库类型文件的领先幅度颇为明显，分析推测这与各类政企单位受到的攻击量上升有关，此类组织内往往有更多的数据是存储在数据库当中，也有更多的专业软件通过数据库进行各类数据的存储与调用。

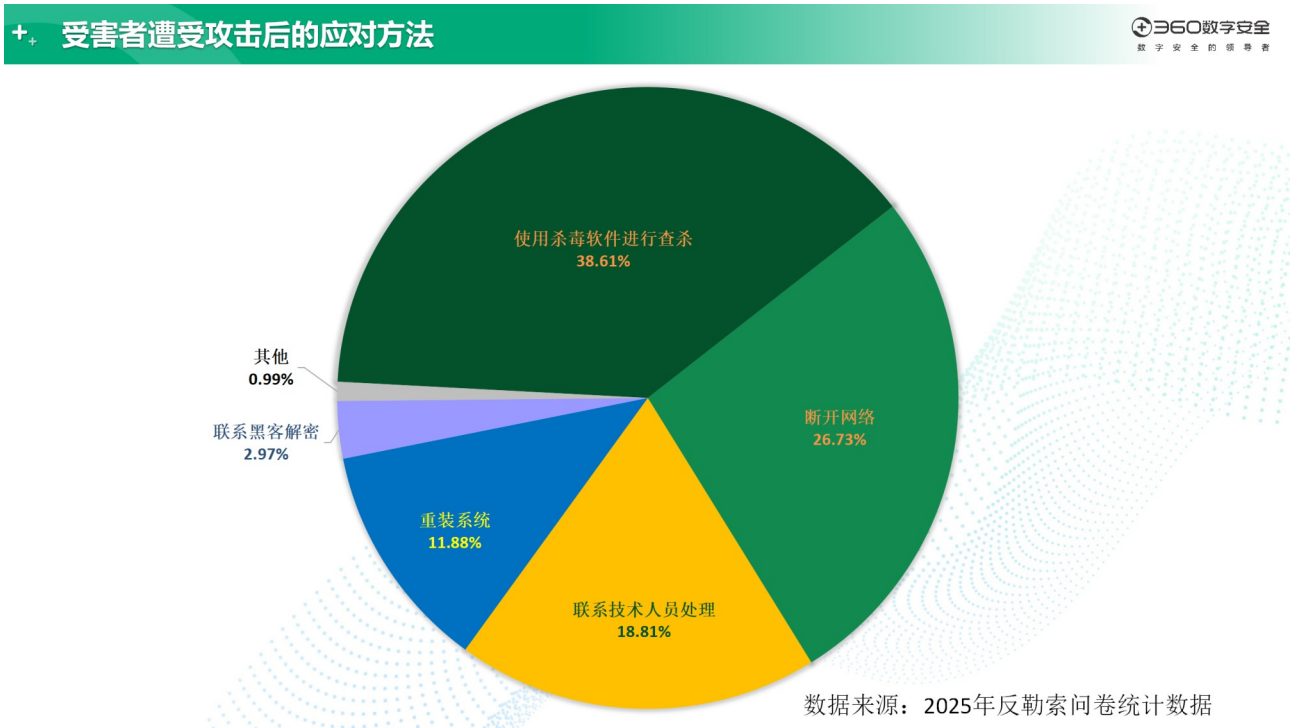


数据来源：2025年反勒索问卷统计数据

六
受害者遭受攻击后的应对方式

同样的，我们对2025年勒索受害者在受到攻击后的应对方式进行的问卷调查统计结果，与2024年的占比分布也几乎完全一样：利用安全软件查杀、断开网络、求助于技术人员以及重装系统都是被官方采用的主流应对手段。

不过与去年略有区别的是，断开网络的操作占比有着显著提升，而及时断开网络也正是在单位组织内受到攻击后的当务之急。该操作作为受到攻击后的第一选项，显然是政企单位的标准化处置流程。这一点也意味着随着相关法规的健全和对网络安全的重视，越来越多的机构和个人对此类问题的处置策略愈发趋向专业化和理性化。

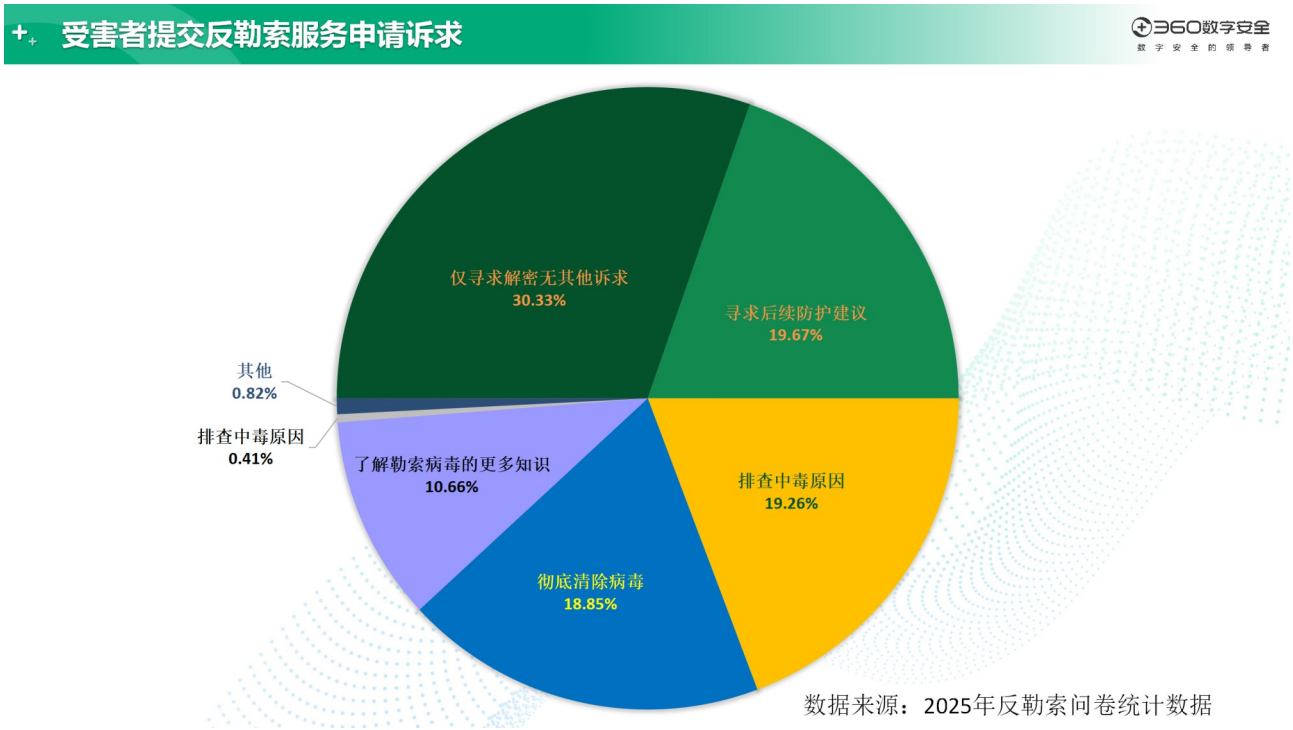


数据来源：2025年反勒索问卷统计数据

七
受害者提交反勒索服务申请诉求

根据问卷反馈的统计数据来看，提交调查问卷的受害者的主要诉求依然是为了能够恢复被加密的数据。寻求防护建议、排查中毒原因的占比分列其后。整体占比分布与往年几乎完全一致。

与我们提供反勒索服务的初衷相同，不仅是为广大受害用户提供数据恢复帮助，也是希望能在沟通中尽可能提供安全相关的建议及溯源排查，帮助受害用户增强安全防范意识，以及更为彻底地解决潜在的安全隐患。



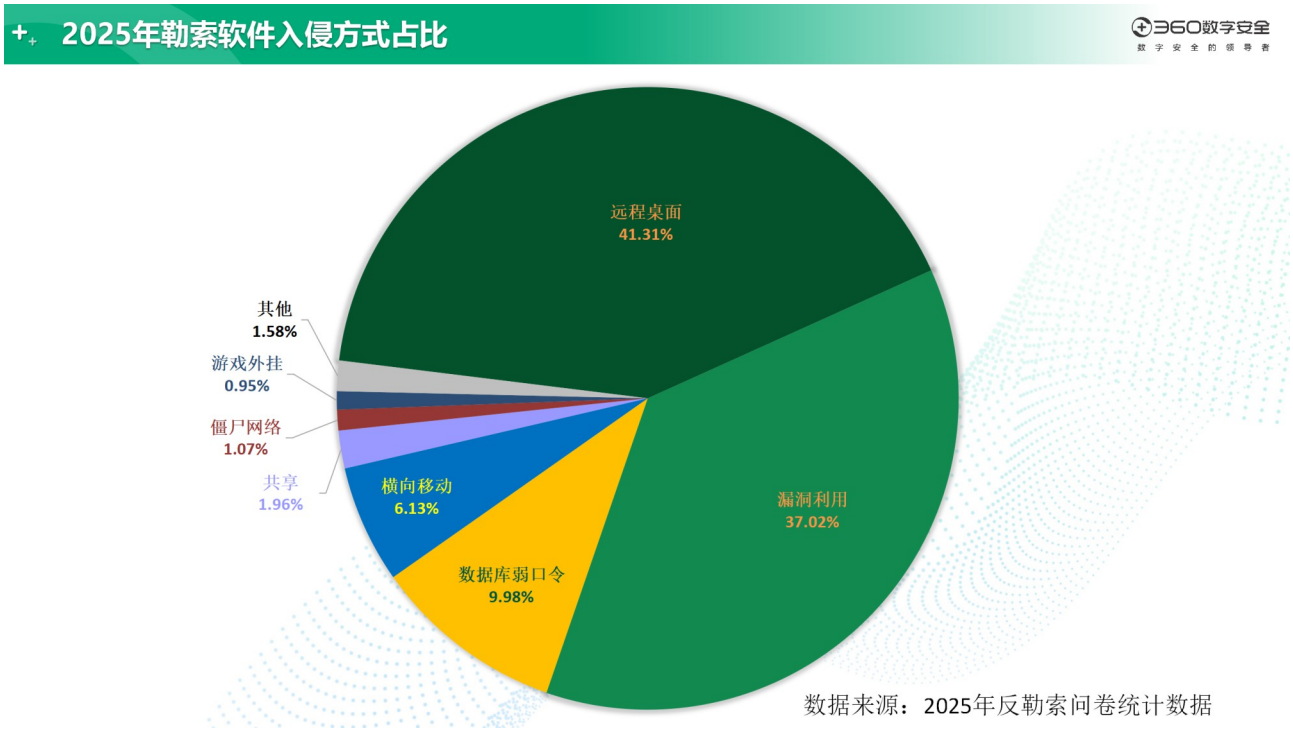
数据来源：2025年反勒索问卷统计数据

第三章

勒索软件攻击者分析

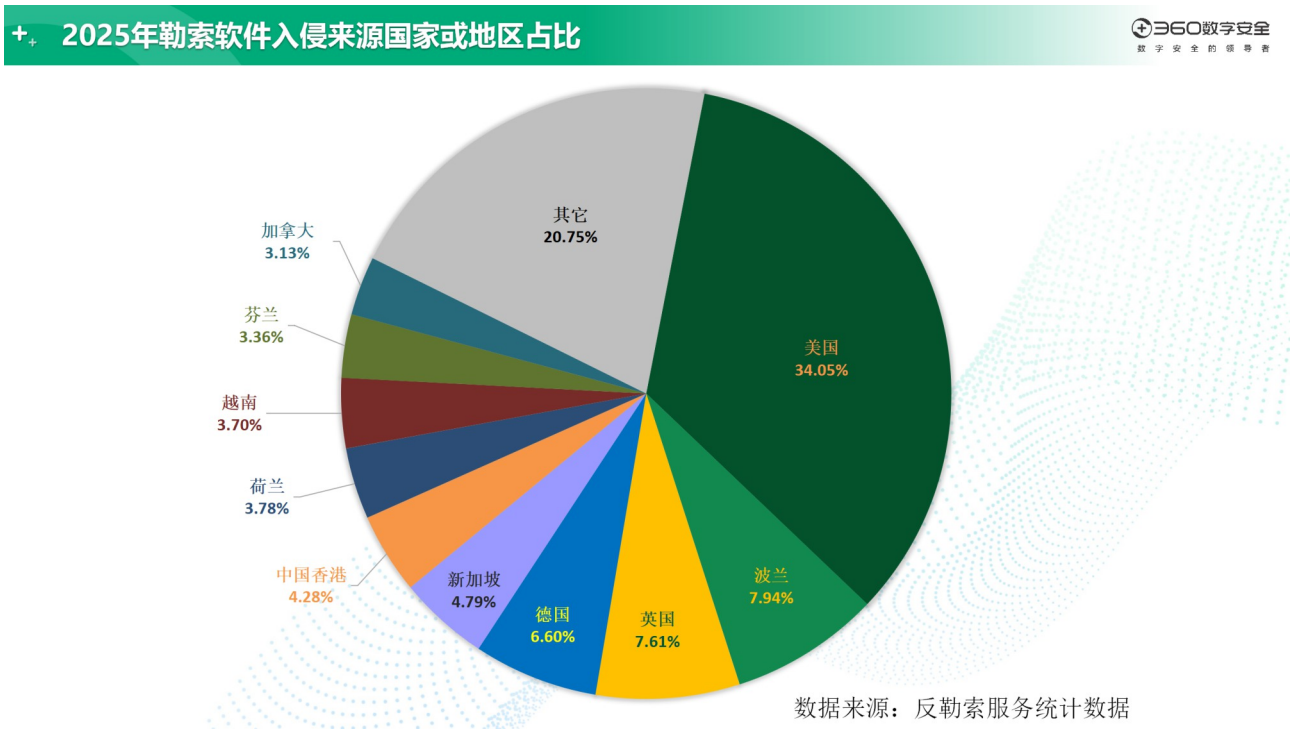
勒索软件攻击形势

分析2025年的勒索软件攻击数据，发现远程桌面入侵和漏洞利用两种方式的占比提升至了前两位。提升较为明显的是漏洞利用的方式，几乎所有主流勒索家族，均通过这两类攻击方式来进行入侵。



黑客使用IP

对2025年勒索软件入侵IP的归属地进行分析，发现来自美国的攻击有着非常显著的提升，推测这与当前的国际局势不无关系。而波兰、英国、德国等欧洲国家因较为发达的互联网基础设施以及颇为庞大的高技术人群，始终是攻击来源的“重灾区”。而新加坡和我国香港地区，则主要是因为运营者大量的托管服务器也被众多攻击者租赁，用作发起网络攻击的代理或跳板设备。



数据来源：反勒索服务统计数据

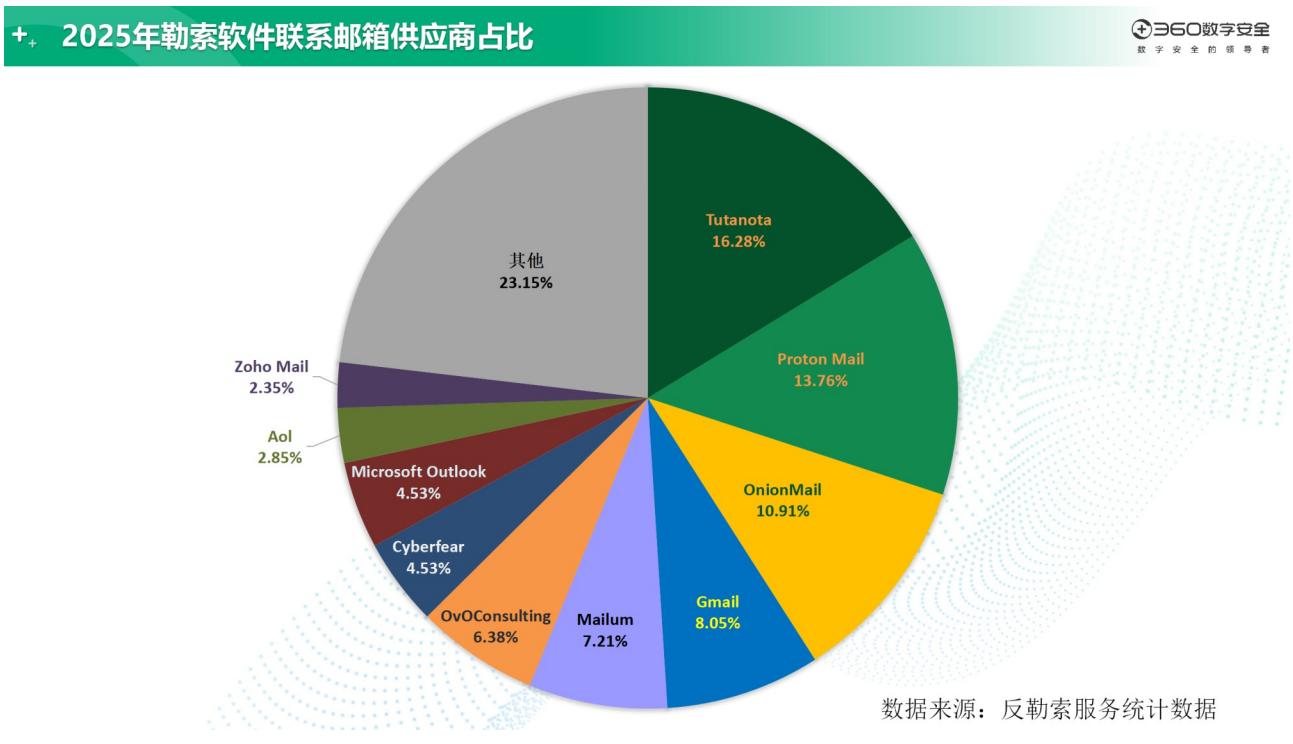
二

勒索联系邮箱的供应商分布

2025年，勒索软件主流的联系方式依然以各类匿名通信软件及邮箱为主。而匿名通信软件则主要采取各类E2EE（端到端加密）或区块链技术对通信双方进行隐藏，便于攻击者隐藏自身行踪，同时保证对话的私密性。

而电子邮件作为传统的赎金谈判渠道，依旧是勒索软件攻击者的首选通信方式。为了确保受害者能够顺利联系到他们，攻击者往往会提供两个以上电子邮件地址，并定期更换以避免被追踪。以采用RaaS运营模式的家族为代表，部分勒索软件家族可能会出现同一家族的不同传播者，使用不同的电子邮件地址进行通信。这种做法导致我们能够监测到的活跃邮件地址数量，相较于其他通信方式要多得多。

通过对2025年收集到的黑客邮箱进行数据分析，发现Tutanota跃升至最受勒索软件作者欢迎的邮箱运营商，而Proton则下降至第二位。不过两者占比依旧维持在高位，总体来说与往年占比波动并不算非常大。针对TOP10邮件服务商提供的邮箱属性进行研究发现，其中匿名邮箱占到了总量的69.43%，相较于去年略有回落，但依然占到了近七成。



数据来源：反勒索服务统计数据

三
攻击手段

本节将介绍一些最为常见的勒索攻击手段，帮助读者更好地理解勒索软件攻击。对下面一些攻击手段做好防御，可以避免绝大多数的勒索攻击事件。

（一）
口令破解攻击

口令破解类攻击是网络攻击中最为基础、同时也是历史最为悠久的攻击手段之一，在国内勒索软件传播链条中长期扮演着重要角色。尽管目前业界已部署多种技术与管理手段用于缓解口令脆弱性问题，但“弱口令”现象依然普遍存在，持续成为企业与个人用户面临的突出安全隐患。该问题成因复杂，既涉及技术层面，也与管理制度和使用习惯密切相关，并在不同规模、不同行业的组织中均有不同程度体现。

需要特别澄清的是，“弱口令”并不等同于“简单密码”。在实际攻击场景中，即便表面上看似复杂的口令，也可能因其可预测性或重复使用而被视为弱口令。常见的弱口令情形包括：使用过于简单的数字或字符组合、采用高频出现的口令字典词汇（如“888888”“qwerty”等）、在口令中直接或间接包含个人身份信息（如姓名、生日、工号等）。

此外，实际环境中还存在一些更为隐蔽、却同样高风险的弱口令类型，往往容易被忽视，例如:

●产品内置的默认账户和默认密码：这些密码通常未经过修改，攻击者可以通过简单的

扫描工具获取。

- 统一运维账户的默认口令：许多企业使用默认的统一运维密码，这为攻击者提供了方便的突破口。
- 失窃的口令：在发生网络攻击后，未及时更换的旧账户密码可能已经泄露，成为攻击者的突破点。
- 信息泄露：管理员在维护日志中记录了后台账户信息，在代码仓库中上传了私钥等也可能导致密码泄露。

在勒索软件攻击事件中，常见的弱口令问题通常出现在以下几类环境中：

- 远程桌面服务（RDP）
- 数据库服务
- NAS设备

这些环境的共同特点是，它们通常会将认证接口暴露到公网。攻击者只要掌握相关账户和密码信息，就可以直接登录到这些设备，从而成为进一步攻击内网的入口。如果攻击者能够控制一个高权限账户，那么就能够在内网中自由行动，进一步窃取数据和控制其他设备。

对于密码管理，用户和企业在实践中常常遇到诸多困难。虽然大家都已熟知一些密码安全的基本措施，比如定期更新密码、不使用简单密码、避免密码重用等，但在实际操作中，这些措施的落实常常存在挑战。以下是一些建议，旨在加强对密码的管理：

- 避免在单一设备上存储大量密码或登录凭据

  不要低估攻击者对设备信息的挖掘能力，黑客在攻击过程中通常首先会寻找设备中存储的账户凭据信息。

- 加强账户验证策略

  可以通过设置IP白名单、限制密码验证尝试次数等简单有效的手段，缓解暴力破解攻击的风险。另外，对于一些老旧系统，缺乏足够的安全防护，容易遭受口令暴力破解

攻击的系统应当避免使用。

●启用多因素认证（MFA）

如果条件允许，务必启用多因素认证（MFA）。MFA可以显著增加口令破解的难度，是一种简单而有效的防护措施，能够有效减少由于口令泄漏带来的风险。

●使用密码管理工具和单点登录（SSO）

尽管一些人可能认为单点登录（SSO）会增加系统风险，但实际上，当企业使用多个系统时，维护多个认证系统和口令信息会带来很大的管理负担。尤其是让员工记住多个复杂的密码并定期更新，这在实际操作中非常困难。使用SSO能够将认证过程集中化，提高可操作性，同时可以结合MFA进一步增强认证的安全性。

此外，密码管理工具能够帮助员工生成强密码，减少设置“弱口令”的可能性，并且可以避免将明文密码存储在不安全的位置。

（二）
漏洞利用攻击

漏洞问题在全球范围内的勒索软件攻击活动中始终占据关键地位，既常作为攻击链条中的初始入侵入口，也频繁在内网横向移动和权限提升阶段被加以利用。随着信息系统架构和业务环境的不断复杂化，漏洞的产生在客观上几乎不可避免，其类型也呈现出多样化特征，涵盖硬件漏洞、操作系统漏洞、应用软件漏洞以及第三方组件漏洞等多个层面。

在实际勒索软件攻击案例中，应用软件漏洞的利用尤为突出，攻击目标通常集中在暴露面较大的关键系统，包括Web服务类应用（如 OA、ERP 等业务系统）、域控制器相关服务，以及位于网络边界的关键基础设施（如 VPN 服务器等）。

从漏洞修补状态的角度来看，漏洞通常可划分为“0day漏洞”（厂商尚未发布修复补丁）与“nday 漏洞”（厂商已发布补丁但尚未被及时修复）。综合过去一年的攻击样本与事件分析结果可以发现，在勒索软件攻击活动中，被利用频率最高的仍然是 nday 漏洞，这反映出补丁管理滞后和资产安全基线薄弱，依然是当前勒索攻击得以成功实施的重要现实原因之一。漏洞的复杂性和多样性往往让管理者不知从何入手，因此我们从不同的视角帮助读者更好地理解漏洞攻击问题。

黑客视角

黑客在发起攻击时从来不是“徒手作战”，而是依托各类成熟的攻击工具与技术手段，有计划、有步骤地实现攻击目标。攻击的第一阶段通常是侦察，攻击者会利用自动化扫描工具对潜在目标进行大规模探测，以识别对外暴露的服务、端口以及可能存在的安全漏洞。扫描对象既可能覆盖整个网段、数据中心或云平台资源池，也可能基于前期情报收集结果，对特定目标服务器实施定向扫描。此类扫描活动通常通过租用的云服务器、被控制的“肉鸡”，或借助第三方开放平台完成。

由于上述扫描行为具备持续性和高度自动化特征，互联网中暴露的公共服务几乎都会在短时间内被发现并纳入攻击者视野。因此，运维与安全管理人员不应心存侥幸，误以为自身部署的对外服务“规模较小”或“关注度不高”而能够规避攻击。

在攻击工具的准备阶段，并非所有攻击者都具备独立挖掘漏洞或编写完整利用代码的能力。现实中，大量攻击行为依赖成熟的漏洞利用工具集（Exploit Kits，EK）。此类工具集通常集成了多个现成的漏洞利用模块，尤其是厂商已发布补丁、但尚未被大范围修复的 nday（亦称 1-day）漏洞。攻击者无需自行开发攻击代码，仅需更换或定制攻击载荷（Payload），即可快速发起攻击。针对补丁部署滞后的设备与系统，一旦漏洞影响范围广、利用权限高且相关产品部署量大，攻击往往会在极短时间内进入高频、高成功率阶段。

在实际勒索软件攻击中，攻击时机的选择同样具有明显策略性。攻击者通常倾向于在非工作时间实施攻击，尤其是周五晚间或节假日前夕，以充分利用运维与安全响应能力相对薄

弱的时间窗口，完成横向移动、权限扩展和恶意程序投递等关键步骤。相关攻击流程高度自动化，个别环节可能辅以半自动化人工操作，这使得单一攻击团伙在短时间内即可对数千乃至上万台服务器发起攻击。

因此，管理人员需要充分认识到，在当前高度自动化和规模化的攻击环境下，只要对外暴露网络服务，就不可避免地处于攻击者的持续扫描与尝试之中。唯有建立完善的安全防护体系、及时修补漏洞并加强持续监测，才能有效降低勒索软件等大规模攻击带来的现实风险。

软件供应商视角

从整体情况来看，主流操作系统供应商普遍高度重视产品安全，在系统设计与发布阶段即经过较为充分的安全测试，并在漏洞披露后能够相对及时地发布安全补丁。在实际运行环境中，只要用户保持良好的补丁更新习惯，通常可以有效规避因操作系统层面漏洞被利用而引发的勒索软件风险。

相较之下，第三方软件供应商在漏洞应对能力和安全治理意识方面存在较为明显的差异。一部分厂商能够积极对待漏洞问题，配合安全研究人员进行分析并及时发布修复补丁；但也有部分厂商对漏洞披露持回避态度，将漏洞视为负面信息，不愿公开说明，甚至淡化其安全影响。此外，仍有厂商错误地将漏洞利用与网络攻击问题完全归因于安全厂商或攻击者，未能从产品安全责任的角度正视自身问题，对漏洞修复工作投入不足，补丁发布不及时。

在部分场景下，厂商对盗版用户或未续费用户不提供安全补丁支持，进一步加剧了安全风险的外溢效应，使相关系统长期暴露在已知漏洞威胁之下，成为勒索软件等攻击活动的高风险目标。

与此同时，供应链安全问题也成为软件厂商普遍面临的现实挑战。现代信息系统往往依赖大量开源或商业第三方组件，一旦某个供应链组件被披露存在安全漏洞，若厂商未能及时

完成版本更新或兼容适配，相关风险便可能在整个生态中迅速扩散。例如， NodeJS的CVE-2025-55182基础组件漏洞，就同时影响了大量业务系统，一些知名软件供应商在当天就提供了漏洞修复，但任由大量中小软件厂商，未对包含漏洞的组件进行更新处理。

安全公司视角

在系统安全维护过程中，安全厂商同样面临诸多现实挑战。对于操作系统层面的漏洞，通常可以通过官方补丁进行直接修复；但在第三方应用场景下，受限于软件版权、版本差异以及技术实现的多样性，安全厂商难以针对每一款应用程序提供定制化、原生级别的补丁支持。

在此背景下，安全厂商通常采用热修复（Hotfix）以及通用型漏洞缓解技术，为相关系统提供一定程度的防护能力。这类技术手段主要包括输入校验增强、内存行为监控、异常行为分析以及攻击特征拦截等，用于在漏洞被触发或利用过程中进行阻断与告警。

但需要注意的是，上述防护机制并非对所有漏洞场景均具备完全覆盖能力，其主要作用在于缓解部分常见、通用类型漏洞的风险，为暂时无法打补丁或尚无官方补丁的运行环境提供过渡性防护。因此，这类措施应被视为补丁管理的补充手段，而非替代方案。用户在有条件更新补丁的情况下，应该尽快通过补丁来解决问题。

用户视角

从用户视角出发，本节内容旨在引导读者形成清晰共识：在当前的网络环境下，不应心存侥幸，任何对外开放的服务都可能成为攻击者重点关注和持续探测的目标。用户应摒弃“补丁无用论”等错误认知，避免因片面担忧补丁可能带来的性能下降、兼容性或稳定性问题，而忽视其在漏洞防护中的关键作用。

即便在部分场景中，用户因授权、服务费用或其他客观原因暂时无法获取官方补丁，也应主动采取替代性安全措施，如缩小暴露面、强化访问控制、部署安全防护设备或引入专业安全服务，以降低系统长期暴露于已知漏洞风险之下的可能性。

同时，也需要正视部分用户因顾虑补丁可能对业务连续性产生影响而选择延迟或拒绝更新的现象。但必须明确的是，安全补丁仍然是当前防范和修复漏洞最直接、最有效的技术手段之一。将补丁管理纳入日常安全运维流程，建立评估、测试与定期更新机制，应成为各类组织的基础安全实践，而非临时性或被动性的应对措施。

漏洞治理建议

1. **定期更新与补丁管理**：及时更新系统和软件补丁，是解决漏洞问题最可靠的手段。管理员应建立健全的补丁管理机制，确保所有设备和系统都在第一时间获得修复。

2. **安装安全防护软件**：如前文所述，安全软件能够提供多层次的漏洞防御和缓解机制，减少通用漏洞造成的危害。定期更新安全软件，提升防护能力。

3. **减少对外暴露的服务**：尽量减少非必要的对外服务暴露，采用反向代理等技术手段降低服务被探测的可能性，减少潜在攻击面。

漏洞与工具

我们总结了在2025年的勒索攻击活动中经常被使用到的漏洞。其中主要的漏洞基于CVE/CNVD编号的归类汇总如下：

CVE编号	涉及产品/应用/服务/设备	漏洞类型	家族
CVE-2021-23758	畅捷通T+ GetStoreWarehouseByStore	反序列化漏洞	Weaxor
无	用友u8 NCCloudGatewayServlet接口	命令执行漏洞	Weaxor
CVE-2025-1055	K7 Security Anti-Malware	提权漏洞	Weaxor
CVE-2020-12271	Sophos	安全功能绕过漏洞	RagnarLocker
CVE-2024-51324	百度杀毒	提权漏洞	Weaxor, DeadLock
CVE-2025-11371	Gladinet CentreStack	未授权访问漏洞	Clop
CVE-2025-6264	Rapid7 Velociraptor	不当授权漏洞	Babuk, LockBit
CVE-2025-61882	Oracle E-Business Suite	远程代码执行漏洞	Clop
CVE-2025-61884	Oracle E-Business Suite	远程代码执行漏洞	ShinyHunters
CVE-2025-10035	GoAnywhere MFT	远程代码执行漏洞	Clop, Medusa
CVE-2024-7344	Howyar UEFI	代码执行漏洞	HybridPetya
CVE-2025-7771	ThrottleStop	提权漏洞	MedusaLocker
CVE-2025-49704	Microsoft SharePoint	远程代码执行漏洞	WarLock, Mino
CVE-2024-21762	Fortinet	堆缓冲区溢出漏洞	Qilin
CVE-2024-57726	SimpleHelp	权限提升漏洞	DragonForce
CVE-2024-21893	Ivanti	路径遍历漏洞	DragonForce
CVE-2025-29824	Windows 通用日志文件系统驱动程序	权限提升漏洞	RansomEXX, Play
CVE-2025-21418	Windows Kernel	缓冲区溢出漏洞	Babuk
CVE-2025-0285	Paragon Partition Manager	权限提升漏洞	Lazarus, BlackByte, LockBit
CVE-2024-24919	Check Point	任意文件读取漏洞	Nailaolocker
CVE-2022-2294	Chrome	缓冲区溢出漏洞	Medusa
CVE-2022-21999	Windows Print Spooler服务	权限提升漏洞	Medusa

CVE编号	涉及产品/应用/服务/设备	漏洞类型	家族
CVE-2022-2295	Chrome	堆损坏	Medusa
CVE-2023-27532	Veeam Backup & Replication	关键功能漏洞身份验证缺失	Akira, Cuba, Noname, ScRansom
CVE-2023-22515	Atlassian Confluence	身份验证漏洞	LockBit, LockBit3.0, LockBit4.0, LockBit Black, Ransomhub
CVE-2022-22954	Vmware Workspace ONE Access, Vmware Identity Manager	远程代码执行漏洞	RAR1
CVE-2022-41080	Microsoft Exchange Server服务	权限提升漏洞	Play, PlayCrypt, Cuba
CVE-2023-24880	Windows SmartScreen	安全功能绕过漏洞	Magniber
CVE-2021-27876	Veritas Backup Exec	代理文件访问漏洞	BlackCat, ALPHV
CVE-2021-27877	Veritas Backup Exec	代理不正确身份验证漏洞	BlackCat, ALPHV
CVE-2021-27878	Veritas Backup Exec	命令执行漏洞	BlackCat, ALPHV
CVE-2023-47246	SysAid	路径遍历漏洞	CL0P, Clop
CVE-2019-1068	Microsoft SQL Server	远程代码执行漏洞	Mallox
CVE-2019-068	Microsoft SQL Server Reporting Services	远程代码执行漏洞	Mallox
CVE-2020-3259	Cisco AnyConnect	信息泄露漏洞	Akira
CVE-2024-1708	ConnectWise ScreenConnect	路径遍历漏洞	LockBit, LockBit3.0, LockBit4.0,LockBit Black, Black Basta, Bl00dy
CVE-2024-1709	ConnectWise ScreenConnect	身份绕过漏洞	Black Basta, LockBit, LockBit3.0, LockBit4.0, LockBit Black, Bl00dy
CVE-2017-10271	WebLogic	远程代码执行漏洞	
CVE-2022-41802	OpenHarmony	内核堆栈溢出漏洞	
CVE-2022-41082	Microsoft Exchange Server服务	远程代码执行漏洞	Play, PlayCrypt
CVE-2023-3467	Citrix	权限提升漏洞	8BASE
CVE-2022-24682	Zimbra Webmail	跨站脚本漏洞	MalasLocker
CVE-2018-13374	FortiADC, Fortinet FortiOS	不当访问控制漏洞	Conti
CVE-2022-27924	Zimbra	Zimbra memcache命令注入	MalasLocker

CVE编号	涉及产品/应用/服务/设备	漏洞类型	家族
CVE-2022-27925	Zimbra	管理目录遍历	MalasLocker
CVE-2022-30333	UnRAR	目录遍历漏洞	MalasLocker
CVE-2022-37042	Zimbra	身份验证漏洞, 远程代码执行漏洞	MalasLocker
CVE-2022-24521	Windows 通用日志文件系统驱动程序	特权提升漏洞	Cuba, Yanluowang
CVE-2022-30190	Microsoft Windows 支持诊断工具(MSDT)	远程代码执行漏洞	Black Basta
CVE-2021-42278	Active Directory 域	特权提升漏洞	Black Basta, Noname, ScRansom
CVE-2021-42287	Active Directory 域	特权提升漏洞	Black Basta, Noname, ScRansom
CVE-2017-5638	Apache Struts	远程代码执行漏洞	Cerber
CVE-2017-0199	Microsoft Office, WordPad	远程代码执行漏洞	Cerber
CVE-2021-22205	GitLab	远程命令执行漏洞	Cerber
CVE-2023-3519	Citrix ADC, Citrix Gateway	远程代码执行漏洞	INC Ransom, Ransomhub
CVE-2024-26169	Windows 错误报告服务特权漏洞提升	特权提升漏洞	Black Basta
CVE-2024-4577	PHP-CGI	参数注入	TellYouThePass
CVE-2022-29499	Mitel VoIP	远程代码执行漏洞	Lorenz
CVE-2023-48788	Fortinet FortiClientEMS	SQL注入漏洞	Medusa, Ransomhub, Akira
CVE-2021-22986	F5 BIG-IP	远程代码执行漏洞	LockBit, LockBit3.0, LockBit4.0, LockBit Black
CVE-2024-37085	VMware ESXI	身份验证漏洞	Black Basta, Akira, BlackByte
CVE-2021-1732	Windows Win32k	权限提升漏洞	BlueSky
CVE-2024-23897	Jenkins	身份验证漏洞	RansomEXX
CVE-2023-38831	WinRAR	代码执行漏洞	Babuk, LockBit, LockBit Black, LockBit3.0
CVE-2023-46747	F5 BIG-IP	身份验证漏洞	Ransomhub
CVE-2023-27997	Fortinet FortiOS	堆缓冲区溢出漏洞	Ransomhub

CVE编号	涉及产品/应用/服务/设备	漏洞类型	家族
CVE-2023-36884	Windows Search	远程代码执行漏洞	Underground
CVE-2020-0787	Windows Background Intelligent Transfer Service (BITS))	权限提升漏洞	Ransomhub
CVE-2022-41352	Zimbra	文件上传漏洞	Rorschach
CVE-2023-24489	Citrix ShareFile	身份验证漏洞	Hunters International
CVE-2024-21338	Windows Kernel	权限提升漏洞	Mallox, Kryptina
CVE-2024-40711	Veeam Backup & Replication	反序列化漏洞	Akira, Fog
CVE-2023-41266	Qlik Sense	身份验证漏洞	Cactus
CVE-2023-41265	Qlik Sense	权限提升漏洞	Cactus
CVE-2020-28188	TerraMaster TOS	远程代码执行漏洞	LVTLocker
CVE-2022-24989	TerraMaster NAS	代码执行漏洞	LVTLocker
CVE-2022-24990	TerraMaster NAS	信息泄露漏洞	LVTLocker
CVE-2019-7192	QNAP	任意文件读取漏洞	eCh0raix
CVE-2019-7194	QNAP	路径遍历漏洞	eCh0raix
CVE-2019-7195	QNAP		eCh0raix
CVE-2018-4878	Adobe Flash Player	代码执行漏洞	Paradise
CVE-2023-38035	Ivanti MobileIron Sentry	身份验证绕过漏洞	Cactus
CVE-2023-48365	Qlik Sense	远程代码执行漏洞	Cactus
CVE-2024-51567	CyberPanel	远程命令执行漏洞	PSAUX
CVE-2024-51568	CyberPanel	身份验证绕过漏洞	PSAUX
CVE-2024-51378	CyberPanel	身份验证绕过漏洞	PSAUX
CVE-2024-40766	SonicWall SonicOS	不当访问控制漏洞	Fog, Akira
CVE-2022-47966	Apache Santuario xmlsec	远程代码执行漏洞	EMBARGO

CVE编号	涉及产品/应用/服务/设备	漏洞类型	家族
CVE-2023-29300	Adobe ColdFusion	代码执行漏洞	EMBARGO
CVE-2023-38203	Adobe ColdFusion	代码执行漏洞	EMBARGO
CVE-2022-42475	FortiOS SSL VPN	代码执行漏洞, 远程命令执行漏洞	Noname, ScRansom
CVE-2017-0290	Microsoft Malware Protection Engine	远程代码执行漏洞	Noname, ScRansom
CVE-2024-42057	Zyxel ATP	命令注入漏洞	Helldown
CVE-2023-20263	Cisco HyperFlex HX	身份验证绕过漏洞	Akira
CVE-2024-27198	JetBrains	身份绕过漏洞	BianLian, Jasmin
CVE-2021-44529	Ivanti	代码执行漏洞	BlackCat
CVE-2021-40347	Postorius	权限提升漏洞	BlackCat
CVE-2019-16098	MSI	BYOVD	BlackByte, BlackByteNT
CVE-2021-21551	Dell	BYOVD	BlackByte, BlackByteNT
CVE-2024-27199	JetBrains	路径遍历漏洞	Jasmin
CVE-2010-2861	Adobe ColdFusion	目录遍历漏洞	Cring
CVE-2009-3960	Adobe ColdFusion	目录遍历漏洞	Cring
CVE-2019-0604	Microsoft SharePoint	远程代码执行漏洞	Cring
CVE-2023-22527	Atlassian Confluence	远程代码执行漏洞	LockBit
CVE-2017-12149	Jboss	反序列化漏洞	Satan
CVE-2010-0738	Jboss	不当访问控制漏洞	Satan
CVE-2017-12615	Apache Tomcat	文件上传漏洞	Satan
CVE-2025-0286	Paragon Partition Manager	身份验证漏洞	Lazarus, BlackByte, LockBit
CVE-2025-0287	Paragon Partition Manager	堆缓冲区溢出漏洞	Lazarus, BlackByte, LockBit
CVE-2025-0288	Paragon Partition Manager	权限提升漏洞	Lazarus, BlackByte, LockBit

CVE编号	涉及产品/应用/服务/设备	漏洞类型	家族
CVE-2025-0289	Paragon Partition Manager	权限提升漏洞	Lazarus, BlackByte, LockBit
CVE-2024-55591	FortiOS, FortiProxy	身份验证漏洞	LockBit, NightSpire
CVE-2024-3806	The Porto theme for WordPress	身份验证漏洞	STORMOUS, Dragon Ransomware, GhostLocker, SiegedSec
CVE-2024-3807	The Porto theme for WordPress	权限提升漏洞	STORMOUS, Dragon Ransomware, GhostLocker, SiegedSec
CVE-2024-3808	The Porto theme for WordPress	远程代码执行漏洞	STORMOUS, Dragon Ransomware, GhostLocker, SiegedSec
CVE-2024-3809	The Porto theme for WordPress	远程代码执行漏洞	STORMOUS, Dragon Ransomware, GhostLocker, SiegedSec
CVE-2022-0073	LiteSpeed	注入漏洞	STORMOUS, Dragon Ransomware, GhostLocker, SiegedSec
CVE-2022-0074	LiteSpeed	权限提升漏洞	STORMOUS, Dragon Ransomware, GhostLocker, SiegedSec
CVE-2023-2359	WordPress	任意文件上传漏洞	STORMOUS, Dragon Ransomware, GhostLocker, SiegedSec
CVE-2023-47784	ThemePunch OHG	任意文件上传漏洞	STORMOUS, Dragon Ransomware, GhostLocker, SiegedSec
CVE-2023-6925	WordPress	任意文件上传漏洞	STORMOUS, Dragon Ransomware, GhostLocker, SiegedSec
CVE-2024-47374	LiteSpeed	注入漏洞	STORMOUS, Dragon Ransomware, GhostLocker, SiegedSec
CVE-2015-2291	BYOVD	特权提升漏洞	Fog
CVE-2023-46805	Ivanti	安全功能绕过漏洞	DragonForce
CVE-2024-21887	Ivanti	安全功能绕过漏洞	DragonForce
CVE-2024-21412	Windows SmartScreen	权限绕过漏洞	DragonForce
CVE-2024-57727	SimpleHelp	路径遍历漏洞	DragonForce
CVE-2024-57728	SimpleHelp	文件上传漏洞	DragonForce
CVE-2025-49706	Microsoft SharePoint	欺骗漏洞	WarLock, Mino
CVE-2025-53770	Microsoft SharePoint	反序列化漏洞	Mino
CVE-2025-53771	Microsoft SharePoint	路径遍历漏洞	Mino
CVE-2024-38475	Apache HTTP Server	会话劫持漏洞	Akira

CVE编号	涉及产品/应用/服务/设备	漏洞类型	家族
CVE-2025-40599	SonicWall SMA	文件上传漏洞	Akira
CVE-2025-40600	SonicWall SonicOS	格式化字符串漏洞	Akira
CVE-2025-52915	K7 Security Anti-Malware	BYOVD	Weaxor
CVE-2020-3580	Cisco ASA	跨站脚本漏洞	Akira
CVE-2025-14611	Gladinet	未经授权的访问漏洞	Clop

（三）
横向渗透攻击

横向渗透攻击是中大型企业内网面临的一项重大安全挑战，尤其在勒索攻击场景中，常常成为攻击者的关键入侵策略之一。在典型的攻击模式下，攻击者首先通过一个受感染的终端或节点入侵，随后利用各种手段在内部网络中扩展，最终可能导致大规模的设备感染，甚至使整个网络瘫痪。

攻击目标：核心资产

在企业网络环境中，域控制服务器（Domain Controller，DC）及各类管理服务器通常是攻击者重点关注和优先攻击的核心目标。一旦此类关键资产被成功入侵，攻击者往往能够迅速获取对内网的集中控制能力，在网络环境中“自由行动”，并以此为跳板持续向其他业务系统和终端设备进行渗透。

此外，企业内网环境中普遍存在软件版本统一、系统配置相似以及口令策略复用等情况，这在一定程度上提升了运维效率，但也在客观上扩大了安全风险。一旦攻击者攻破任意一台具备代表性的设备，相关攻击手法和凭据便可能被快速复制和复用，从而对整个内网环境构成系统性威胁，显著降低勒索软件等攻击活动的实施成本与成功门槛。

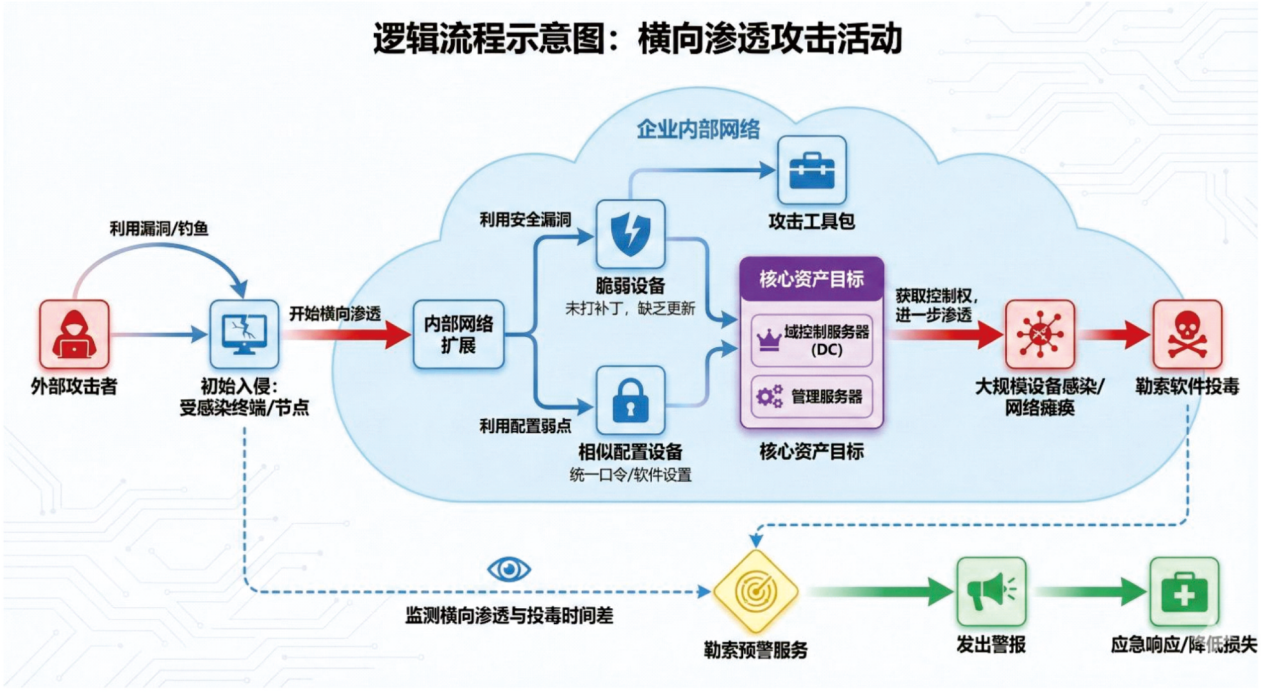
安全漏洞与攻击工具

内网设备的安全性与是否及时应用系统补丁密切相关。许多设备由于缺乏及时更新，变得异常脆弱，成为黑客攻击的首选目标。现代攻击者通常使用集成了多种漏洞利用工具的攻击工具包（如Exploit Kits），针对未打补丁的设备进行攻击，从而快速获得控制权并扩大影响范围。

横向渗透与勒索预警

在我们的勒索预警服务中，横向渗透攻击的检测占据了重要部分。通过监测网络中横向渗透到勒索软件投毒的短暂时间差，我们能够及时发出警报，帮助企业在攻击初期采取应急响应措施，防止攻击蔓延并降低损失。

下图展示了，横向渗透攻击，如何在内网中渗透活动。



▲ 典型横向渗透攻击流程

下面整理了一些勒索家族在横向渗透中常用的攻击工具，包括进程查看器，端口扫描工具，口令提取工具，各种内网渗透工具。黑客通过这些工具大大简化了攻击过程，降低了黑客的攻击门槛。其中有部分工具是通用工具，被几乎所有黑客团伙使用，最为常见的通用工具有如下这些：

●Rootkit工具：PChunter、Process Hacker、Process Explorer

●密钥窃取工具：Mimikatz

●资源收集与数据窃取工具：Everything、NetworkShare

值得一提的是：Everything除了被用来搜集文件外，还被黑客用来批量窃取文件。Everything可被部署为文件服务器，攻击者利用这一特性，在被攻击设备中暗中植入everything作为后门使用。

●远程控制工具：AnyDesk

下面对当前最流行的部分勒索家族，及其使用的工具进行了一些整理：

利用工具

家族	Tool
Wmansvcs	PasswordFox,Mimikatz,PassShow,SoftPerfect Network Scanner,PassView,Dialupass,NetRouteView,VNCPassView,WebBrowserPassView,WirelessKeyView,Geek Uninstaller
Akira	AdaptixC2,Mimikatz,AdFind,LaZagne,MEGAsync,Ngrok,WinRAR,WinSCP,AnyDesk,FileZilla,PowerTool,Rclone,PChunter,MobaXterm,RustDesk,Terminator,Advanced IP Scanner,Radmin,Cloudflare,DWAgent,Cloudflare Tunnel,PowershellKerberos,Veeam-Get-Creds,Cloudflared
Kawalocker	HRSWord,Advanced Port Scanner,PsExec
Interlock	AnyDesk,Cobalt Strike,PSExec,PuTTY,ScreenConnect,SystemBC,WinSCP
LockBit	MEGAsync, CrackMapExec, Mimikatz, PsExec, AnyDesk, GMER, Process Explorer, FileZilla, ScreenConnect, LaZagne, NetworkShare, Cobalt Strike, Exfitrator-22, KPortScan, NetScan, PChunter, PowerTool, Process Hacker, Network Password Recovery, HRSWord, denfendercontrl, Exmatter, Poortry, SplashTop
Mallox	fscan, AnyDesk, powercat, lcx, DefinderControl, Mimikatz, NetScan, Process Hacker, PChunter, Cobalt Strike, Nasp, NetworkShare
BlackByte	Cobalt Strike, AnyDesk, anonymfiles.com, file.io, LoLBins, WinRAR, Exbyte DEWMODE, FlawedGrace, SDBot, Truebot, Cobalt Strike
Everest	ProcDump, NetScan, SoftPerfect Network Scanner, WinRAR, AnyDesk, Cobalt Strike, SplashTop, Atera Agent, TeamViewer
Noname	WinRAR, Spacecolon
ScRansom	WinRAR, Spacecolon
RansomEXX	Cobalt Strike, Mimikatz, Metasploit, Vatet Loader, LaZagne
STORMOUS	GhostPresser

家族	Tool
Vice Society	Cobalt Strike, Mimikatz, PowerShell
BianLian	Rclone, MEGAsync, TeamViewer, Atera Agent, SplashTop, AnyDesk, PuTTY, PDQ Deploy, Ligolo, Chisel, Cobalt Strike, Sliver, LaZagne, Mimikatz, FileZilla, Non-sucking Service Manager, 7-Zip, WinSCP, Azure Storage Explorer, Ngrok
GlobeImposter	Process Hacker, NetScan, PChunter, NetworkShare, Mimikatz
Makop	PChunter, Process Hacker, Process Explorer, NetScan, dfcontrol, netpass, NetworkShare, Everything, Mimikatz, mouselock, Exploit, Advanced Port Scanner, ARestore, PuTTY, PsExec, YDArk, PuffedUp, KPortScan, NLBrute, denfendercontrl, ydayk, GotoHTTP, Nasp, BDcontrol,MASSCAN
Buran	AZORult, Vidar, Rig EK, PChunter, Mimikatz, NetworkShare, Process Hacker, dfcontrol, YDArk Magnitude Exploit Kit, YDArk, Pchunter
phobos	DataBase, DefinderControl, accountrestore, denfendercontrl, netpass, pyark, NetworkShare, Everything, FRP, frpc, KPortScan, Mimikatz, luciroot, NetScan, Nasp, PChunter, YDArk, PuTTY, dfcontrol, GMER, HRSWord, NLBrute, ydayk, WebBrowserPassView, Process Hacker, SmokeLoader, Cobalt Strike, BloodHound, Sharphound, NirSoft, MEGAsync, WinSCP, FTP
Stop	NetworkShare, Advanced Port Scanner, LaZagne
TellYouThePass	certutil, bitsadmin, PowerShell
Loki	Mimikatz, NetworkShare
BeijingCrypt	AnyDesk, PChunter, Everything, Process Hacker, netpass, PEview, KPortScan, Nasp, NetworkShare, HRSWord, GMER, NetScan
MedusaLocker	PChunter, denfendercontrl, Mimikatz, Process Hacker, NetScan, Advanced Port Scanner, HRSWord, PsExec, Bdcontrol
Venus	PChunter, NetworkShare, Process Hacker, Mimikatz, NirSoft, netpass
Black Basta	PsExec, Cobalt Strike, Mimikatz, TeamViewer, AnyConnect, Windows Quick Assist, ScreenConnect, NetSupport Manager, Rclone, bitsadmin, WinSCP, EvilProxy

家族	Tool
RansomHouse	MrAgent, Vatet Loader, Metasploit, Cobalt Strike, Mimikatz, PowerShell, 7zip, MEGAsync
MONTI	AnyDesk, Cobalt Strike, GMER, MEGAsync, Mimikatz, NetScan, PsExec, PuTTY, Veeamp, WinSCP, Action1 PsExec, Mimikatz, Process Hacker, GMER, PowerTool, Cobalt Strike, AdFind, Microsoft NItest, BloodHound, IOBit, Plink, AnyDesk, PowerShell, WinSCP, WinPEAS, SystemBC RAT, WinRAR, Sliver, ConnectWise
BlackBit	NetworkShare, netpass, WebBrowserPassView,NetGUI,WirelessKeyView,RouterPassView,PST Password Recovery,Dialupass,VNCPassView,BulletsPassView,DnsJumper
Qilin	Cobalt Strike, PsExec, SecureShell, YDArk, nmap, Nping,ScreenConnect
Medusa	NetScan, PsExec, put.io, Poortry, ConnectWise
Trigona	HRSWord, Atera Agent, SplashTop, ScreenConnect, AnyDesk, LogMeIn, TeamViewer
Cactus	PAExec, SuperOps, SplashTop, AnyDesk, Chisel, Rclone, PowerShell, SoftPerfect Network Scanner, Plink, ManageEngine UEMS, 7zip, PSnmap, Cobalt Strike
BlackSuit	Sliver, Chisel, Cloudflare, AnyDesk, Atera Agent, MobaXterm, PsExec, Rubeus, ScreenConnect, Cobalt Strike, Mimikatz, WinRAR, WinSCP, Sharphound, SystemBC RAT, AdFind, SysInternals
INC Ransom	PsExec, MEGAsync, WinRAR, LoLBins, AnyDesk, NetScan, 7zip, PuTTY, Advanced IP Scanner, AdFind, restic, Restic
Rhysida	PStools, PuTTY, AnyDesk, NetSupport Manager, PsExec, WinSCP, MEGAsync, SystemBC RAT, SysInternals, Azure Storage Explorer
DragonForce	Cobalt Strike, SystemBC RAT, Mimikatz, SoftPerfect Network Scanner
Mimic	Everything, AnyDesk, Cobalt Strike, WinRAR, 7zip LoLBins, WinPEAS

家族	Tool
Ransomhub	Atera Agent, SplashTop, NetScan, Advanced Port Scanner, ScreenConnect, EDRKillShifter, Poortry, nmap, AngryIPScanner, PsExec, ConnectWise, N-Able, PuTTY, WinSCP, Rclone, Cobalt Strike, Metasploit, bitsadmin, Sliver, CrackMapExec, Amazon AWS S3, SMBExec, Mimikatz, PowerShell, Kerberoast, TDSSKiller, LaZagne
EMBARGO	Impacket, Cobalt Strike, Rclone, AADInternals
Moneyistime	Lightshot, BDcontrol, PowerTool, Pchunter
MorLock	Sliver, AnyDesk, PuTTY, Non-sucking Service Manager, PAExec, XenAllPasswordPro, pretender, localtonet, resocks, SoftPerfect Network Scanner, Godzilla web-shell, PingCastle
Fog	AdaptixC2,PsExec, Advanced Port Scanner, SoftPerfect Network Scanner, SharpShare, Rclone, AnyDesk, nmap, MEGAsync
Helldown	Mimikatz, TeamViewer, HRSWord, Advanced Port Scanner
Ymir	SystemBC RAT, Process Hacker, Advanced IP Scanner, PowerShell

▲ 勒索软件传播中所使用的黑客工具

（四）
共享文件

加密共享文件夹：勒索攻击中的潜在风险

虽然加密共享文件夹本身并非勒索软件直接传播的手段，但根据实际用户反馈和安全事件处理经验，这一问题在企业和个人网络环境中频繁出现，值得特别关注。及时了解风险成因并采取针对性防护措施，可显著降低共享文件夹遭受勒索软件加密的可能性。

在相关事件中，通常并非存储共享文件的服务器或存储设备本身遭到入侵，而是其他具有访问权限的终端或设备被感染，导致攻击者通过已获取的访问权限对共享文件夹内的文件实施加密操作。这种攻击方式强调了横向传播和权限利用的重要性，也提示企业和个人在管理共享资源时，需严格控制访问权限、保持终端安全，并配合备份和监控策略，降低勒索软件造成的潜在损失。

勒索软件如何加密共享文件

当前主流勒索软件普遍具备自动化扫描和枚举网络资源的能力，其扫描范围通常覆盖局域网内的各类共享文件夹和网络存储资源。在攻击过程中，勒索软件会在不需要用户干预的情况下，持续探测可访问的共享路径，并对满足权限条件的文件执行加密操作。对共享文件夹的加密往往属于勒索软件的默认行为之一，一旦具备相应访问权限，加密过程即可自动完成。

与此同时，在实际使用场景中，部分用户为了提升使用便利性，在配置共享文件夹时采用了过于宽松的访问控制策略，例如，为访客账户或低权限用户开放写入权限。这类配置在无意中降低了安全门槛，使得一旦相关终端或账户被勒索软件感染，攻击者即可借助已有的低权限访问能力，对共享文件夹内的大量文件实施加密，从而放大攻击影响范围并造成更为严重的业务损失。

有效防护措施

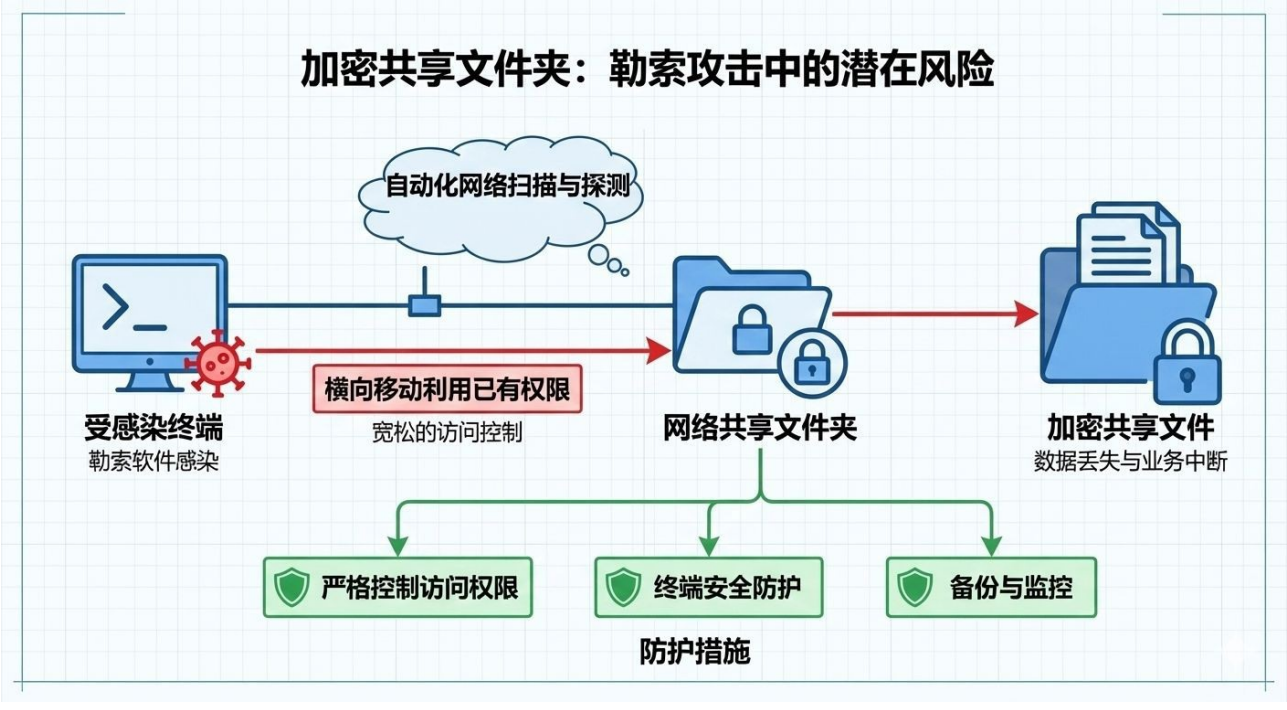
要有效防范共享文件夹被勒索软件加密的风险，可以从以下几个方面着手：

1.**实行严格的权限管理**：限制普通用户对关键共享文件的写入权限，确保只有授权的管理员或特定用户组能够对敏感文件进行修改。避免将过高的访问权限授予不必要的用户。

2.**创建网络分隔（VLAN）**：通过将关键业务系统和数据存储区域分隔到不同的虚拟局域网（VLAN）中，可以减少跨区域的网络访问。这样，勒索软件在感染某一设备后，无法轻易横向渗透至其他关键区域。

3.**定期审计用户访问权限**：对共享文件夹和其他重要资源的访问权限进行定期审计，及时撤销不再需要的权限，防止权限过度扩展而增加安全风险。

4.**定期备份共享文件夹数据**：对共享文件夹中的重要数据进行定期备份，并确保备份数据的安全性。备份可以保证在勒索攻击发生后，数据能够迅速恢复，减少企业运营中断的时间和经济损失。



（五）
僵尸网络投毒

僵尸网络（Botnet）是网络攻击者实施各类恶意活动时最常使用也最具规模化优势的工具之一。攻击者通常通过投递木马程序、蠕虫病毒，或利用系统与应用漏洞对终端和服务器进行入侵控制，将受害设备转化为可被远程操控的“肉鸡”，并逐步纳入其僵尸网络体系之中。

一旦僵尸网络构建完成，攻击者即可通过集中式或分布式的控制指令，远程操纵大量受控设备协同发起攻击活动，包括恶意程序投递、拒绝服务攻击、垃圾信息传播以及后续的勒索软件攻击等。

从今年的攻击态势来看，利用僵尸网络直接投递勒索软件的攻击行为相较以往呈现出一定程度的下降趋势，但这并不意味着僵尸网络威胁已经消退。相反，其基础设施属性和可复用特性，使其仍然是攻击者的重要资源之一。因此，对僵尸网络相关威胁的监测与防范仍需保持高度警惕，不能因阶段性变化而放松安全防护。

（六）
社会工程学

社会工程学攻击是勒索软件攻击链条中常见且极具破坏性的手段之一。攻击者往往通过操控受害者的心理预期和行为决策，诱导其主动配合完成攻击关键步骤，从而绕过技术层面的防护措施。以下案例即为一起典型的、以电信诈骗式社会工程手法为起点的勒索攻击事件。

在该事件中，受害者首先接到一个自称“工商局工作人员”的电话，对方声称接到举

报，指出受害者公司网站存在违规或不当内容，并以可能面临行政处罚为由施加心理压力，要求受害者尽快与“投诉人”取得联系进行协商处理。在对方持续诱导下，受害者添加了所谓“投诉人”的即时通信联系方式。

随后，攻击者以“投诉人”的身份向受害者发送了一封所谓“撤销举报”的邮件。该邮件在内容和形式上经过精心伪装，具有较强的迷惑性，诱导受害者点击邮件中的链接或下载并打开附件。最终，受害者按照邮件提示执行了恶意文件，导致“银狐”远控木马在系统中悄然植入。

更为严重的是，该木马程序在成功落地后，进一步下载并执行了 LockBit 5.0 勒索软件，对受害者计算机中的重要数据实施加密，并弹出勒索信息索要赎金，给用户带来了严重的数据损失和业务影响。该案例充分体现了社会工程学攻击在勒索软件传播中的关键作用，以及“木马投递 + 勒索软件加载”这一复合型攻击链条的现实威胁。

▲ 勒索软件利用社会工程学手段攻击

（七）
“自带易受攻击的驱动程序”（BYOVD）

“自带易受攻击的驱动程序”（BYOVD，Bring Your Own Vulnerable Driver）是近年来新兴的一种勒索软件攻击技战术，攻击者通过利用存在漏洞或被滥用的“正常”驱动程序绕过安全防护，直接在内核层面关闭或干扰安全软件，从而为勒索软件的部署提供便利。

攻击案例分析

Makop勒索软件：在Makop勒索软件的攻击中，攻击者利用了loldrivers技术在内核层关闭安全软件进程。攻击过程中，发现的恶意驱动程序包括ksapi64.sys、viragt64.sys和SysMon.sys，这些驱动程序通过绕过安全软件的保护，使得勒索软件能够在目标系统中顺利运行。

（八）
其它攻击因素

以上内容对国内勒索软件最为常见的传播手法进行了系统性分析。除上述方式外，勒索软件的传播途径还包括网页挂马、激活破解类软件、游戏外挂、钓鱼邮件、即时通信工具（IM）传播以及供应链攻击等多种形式。相关攻击手法在历年安全报告中已有较为充分的讨论，本文不再逐一展开。值得注意的是，随着攻击技术和地下产业链的不断成熟，勒索软件的传播策略和投递渠道已高度多样化，几乎覆盖了传统病毒和木马攻击曾采用的全部技术路径。

然而，勒索软件攻击与传统恶意软件的核心差异，并不体现在传播方式本身，而在于其攻击目标和破坏重点。勒索软件以数据为核心攻击对象，通过对关键业务数据和重要文件实施加密并索要赎金，直接冲击企业的核心资产和业务连续性。相较于以系统破坏或信息窃取为主要目的的传统恶意软件，勒索软件往往能够在短时间内造成更为严重的经济损失、业务中断以及持续性的运营风险。

第四章

勒索软件发展与趋势分析

勒索软件发展与趋势分析

进入2025年，勒索软件威胁仍旧是全球网络安全领域最严峻、最受关注的安全议题之一。过去一年中，勒索攻击在技术、组织形态和经营模式上均呈现出更深层次的演化趋势，其影响范围覆盖个人、企业、供应链、政府机构和关键基础设施等领域。勒索攻击的产业链更加成熟、攻击流程更加自动化、武器化程度持续提高，且越来越多攻击行为叠加了数据窃取、关键数据锁定、供应链劫持等混合攻击手法。

一

Ai加速勒索攻击能力进化，攻防两端全面拥抱智能化

2025年的勒索软件生态中，AI 技术的融入已从“辅助性工具”演变为“核心驱动引擎”。AI正同时改变攻击者与防御者的能力结构，使得勒索软件从工具化威胁向智能化威胁持续演变。

（一）

AI 让勒索攻击智慧化、定制化、隐蔽化

2024 年初开始出现的“AI 生成攻击链”“AI 自动渗透模块”等技术，在 2025 年已被多个活跃勒索组织证明有效。攻击者利用大模型、恶意训练模型及自动化策略生成工具，使勒索软件具备以下能力：

●自动识别目标资产与拓扑结构

基于模型推理能力，恶意程序可主动学习受害者系统布局、运行服务和薄弱点，自动生成匹配的攻击策略。

●按受害者环境动态定制攻击流程

某些新型勒索软件（如 BlackSuit、Phobos 新变体）已展示根据系统语言、行业系统特征、备份策略进行“差异化攻击”的能力。

●更强规避检测与溯源能力

Ai模拟用户行为、生成随机化流量、自动替换行为特征，使病毒更难被检测系统识

别，也更难溯源。

未来的勒索攻击将呈现明显的“千企千攻”“千机千样”特征，攻击路径、攻击强度、加密方式都根据受害者实时定制。

（二）
AI 驱动的全链路自动化勒索攻击体系形成

2025年多起攻击事件表明，勒索组织正逐步具备“从入侵到加密的全链路无人化攻击”能力：

- 自动化资产扫描
- 自动化漏洞匹配与利用
- 自动化横向移动
- 自动化窃取敏感数据并分类
- 自动化执行双重或三重勒索
- 自动化销毁痕迹与反取证
- ……

虽然还无法确定是否有真正的全自动化勒索攻击发生，但当前勒索攻击的每一个链条，都能看到AI的身影。全AI化的攻击，只是时间问题。未来勒索软件有可能形成类似 “自动运行的持续渗透机器人”，极大提升攻击密度与成功率。对勒索攻击的防御，将不再存在侥幸，任何疏漏都可能会被机器人迅速捕获并加以利用。

（三）
AI 成为新一代安全产品核心能力

为应对更智能化的攻击，2025年安全行业更深入采用AI，以解决过去依赖云体系、依赖规则的碎片化问题：

- 离线AI模型成为应对无网环境攻击的关键；
- 模型推理帮助发现未知病毒行为；
- AI自动分析注册表、系统调用、文件行为，加速应急分析；
- 大模型替代人力进行溯源整理、攻击链还原、风险预测。

安全行业正在从“规则驱动”全面迈向“模型驱动”，AI与安全的融合已成为新一轮竞争的制高点。

（四）
安全产品门槛持续降低，AI成为普惠安全的核心

AI技术的成熟和集成，进一步将复杂专业的安全能力转化为易用、高效的“一键式”服务。

安全分析的平民化：AI驱动的威胁情报分析和事件响应系统，能够自动对海量警报进行归纳、定性、优先级排序，并以自然语言的形式提供清晰的应急响应建议。这使得缺乏专业安全团队的中小企业也能高效地应对复杂的安全事件，大幅降低了企业使用高端安全产品的门槛和运营强度。AI正在成为让中小企业获得与大型企业同等安全防护能力的关键技术。

二

攻击团伙更加专业化、系统化，中小企业成为高频目标

2025年的勒索生态呈现明显的“专业化攻防体系化”趋势。勒索组织虽然整体数量有所减少，但核心团伙攻击规模更大，技术水平更高，攻击行动呈现以下特征：

●攻击组织更具“准红队化”特征

以LockBit 残余组织、8Base、Mallox、Play等活跃团伙为代表，其攻击流程明显向“专业红队”靠拢。

●结构化的入侵战术

●套件化的横向移动工具

●工具链之间高度兼容

●专人负责扫描、窃取、部署、加密等流程

●RaaS模式进一步成熟

某些组织甚至对攻击成员实行KPI机制、收益分配制度，攻击行动逐渐产业化、公司化。

●n-day漏洞利用规模化加剧

2024—2025 年出现的多起大规模勒索事件，与以下漏洞利用密切相关：

●VPN/SSL网关漏洞

●OA/ERP系统漏洞

●Web中间件漏洞

●供应链组件漏洞（如Log4J类事件余波）

勒索组织对公开PoC的响应速度越来越快，从漏洞公开到武器化利用平均缩减至7天以内。成熟团伙甚至形成专门的PoC改写与漏洞适配小组。同时，由于中小企业大量依赖第三方IT运维，补丁管理不到位导致其成为 n-day 漏洞攻击的主要受害者。

●安全托管与SaaS防护将成为中小企业的主要选择

企业面临下面一些突出问题，导致应对专业化攻击与内部安全能力不足。

●运维人员不具备安全排查能力，缺乏长期实战练习

●付费解密后漏洞依旧存在，二次勒索问题凸显

●SaaS化反勒索解决方案

●云端威胁检测与监控服务

这种趋势将进一步推动 “企业外包安全能力” 的普及，越来越多企业开始使用安全托管服务（MSS）。

三

创新驱动反勒索技术发展——安全技术新突破

为应对勒索软件的演化和新趋势，2025年安全厂商持续在技术创新上投入巨大努力，旨在构建更具韧性和前瞻性的反勒索体系。

- **勒索攻击行为的纵深识别与阻断**：我们进一步优化了基于行为特征的勒索攻击识别防护技术，不仅在文件操作层面进行判断，更深入到进程行为、内存操作、系统调用链等多个维度进行实时监控和关联分析。这种不依赖白名单的轻量化技术，能够更早、更精准地识别和阻断新的、未知的勒索病毒变种。

- **信创与多平台环境的防护深化**：针对政企单位日益增长的Linux、信创国产操作系统环境的防护需求，我们全面升级了勒索防护方案，实现了对关键服务器、数据库和国产应用环境的深度兼容和高效防护，填补了特定生态下的安全空白。

- **勒索溯源增强**：反勒索溯源工具能力获得代际提升，在“渗透痕迹记录”中已收集并建立了超过千项的攻击痕迹检测点数据库，覆盖了主流勒索团伙的最新战术和技术（TTP）以及常见攻击工具，能够对绝大多数勒索攻击进行精准快速排查。工具将功能集成化，普通管理员也可轻松使用。

- **Java/Net/Web应用的深度防御**：持续扩展和优化RASP（Runtime Application Self-Protection）技术，进一步深化了Java、.Net等主流应用运行时的动态防御能力，不仅能防御已知的NDay漏洞，更通过AI模型对应用层的异常交互进行深度分析，实现了对0Day漏洞的"免疫式"告警和拦截，保障了应用系统的数据安全和业务稳定。

结论与趋势展望

2025年的勒索软件发展态势表明，我们正处于一个由AI驱动的“攻击效率极速提升”与“防御体系被动升级”的对抗螺旋中。

1.**AI的双刃剑效应将持续加剧**：AI不仅是攻击者的利器，也是防御方实现“自治防御”和“预测性防御”的唯一出路。未来的网络安全竞争，将是AI模型能力和数据生态的竞争。

2.**攻击向“服务”和“供应链”集中**：勒索软件即服务（RaaS）模式将进一步专业化，并深度融合攻击自动化平台。针对托管服务商和供应链的“上游攻击”将成为主流，迫使企业将安全投资从被动防护转向主动治理和供应链风险管理。

3.**防御体系需实现从“点”到“体系”的跨越**：企业不能再依赖单一的安全产品，而需要构建一个以AI为核心、涵盖终端、网络、应用和云环境的统一安全运营体系，尤其是中小企业必须借助外部专业力量（如SaaS化安全服务）来弥补资源和技术差距。

未来的勒索对抗，比拼的将是AI的部署速度和防御体系的韧性。掌握这项技术的安全产品将在竞争中占据主导地位。

第五章

安全建议

安全建议

面对严峻的勒索软件威胁态势，我们分别为个人用户和企业用户提供了以下安全建议。希望能够为尽可能多的用户提供全方位的计算机安全保障，最大限度地降低勒索软件感染用户系统的概率。

一

针对企业用户的安全建议

（一）

发现遭受勒索软件攻击后的处理流程

1.发现有设备感染勒索软件后不要惊慌，及时进行安全处置，在第一时间将潜在损失降至最低，并可有效减少被勒索软件二次攻击可能性。

2.对被攻击设备及时进行隔离，切断其与整个内部系统和其他设备的连接。如果同一子网下多台设备中招，可尝试对整个子网进行整体的外部隔离操作。

3.企业所面对较为常见的外部攻击入口包括：远程桌面弱口令、Web服务漏洞以及数据库弱口令。而企业的内部设备则通常会在勒索软件利用上述外部入口成功入侵后遭遇横向渗透攻击。因此，建议企业的IT管理人员在发现遭到勒索攻击的第一时间，通过防火墙等安全软件切断外部对远程桌面的访问。并关闭服务器的Web服务端及数据库的外部访问端口，作为应急防护手段。

4.在发现勒索攻击后，尽快联系安全厂商或专业安全团队，对内部网络进行全面的排查处理。如果企业拥有自己的安全团队也可自行排查，但仍需查清具体的入侵来源、攻击路径以及受影响资产情况，避免留下安全隐患。

5.根据排查结论对风险点位做对应的加固修复。同时，应假定黑客已窃取了所有相关设备中存储的凭据。对公司内部在攻击中涉及的所有设备中的各类口令及凭据，全部进行统一更新。

6.目前主流勒索软件均无法通过技术手段直接破解，因此，预防永远是面对勒索攻击最有效的应对手段。而对攻击原因进行详尽的排查，则可以最大限度地避免企业再次成为勒索攻击的目标。无视原因，一味盲目地重置系统，只会埋下更为严重的安全隐患！

（二）

企业安全规划建议

对企业信息系统的保护，是一项系统化工程，应在企业信息系统建设初期就加以考虑，但对现有环境的改善提升，也能提升企业应对网络攻击风险的能力。以下从最关键的网络建设、资产管理、人员管理方面进行介绍。

1.网络建设

●网络架构

业务、数据、服务分离。不同职能部门与区域之间通过VLAN或子网等手段进行分离，减少因为单点沦陷造成更大范围的网络受到攻击。

●内外网隔离

合理设置对外开放区域，对外提供服务的设备要做严格管控。减少企业被外部攻击的暴露面。

●安全设备部署

在企业终端和网络关键节点部署安全设备，并对安全设备告警情况进行日常监控和及时处置。

●权限控制

包括业务流程权限与人员账户权限都应该做好控制，如控制共享网络权限等。原则上应以最小权限提供服务，降低因为单个账户沦陷而造成更大范围影响的概率。

●数据备份保护

对关键数据和业务系统做备份，如离线备份、异地备份、云备份等，避免因为数据丢失、损坏、无法访问等情况造成的业务停摆，甚至被迫向攻击者妥协。

●敏感数据隔离

对敏感业务及其相关数据做好网络隔离，如有必要甚至应做好设备之间的物理隔离。避免双重勒索软件在入侵后轻易窃取敏感数据，对公司业务和机密信息造成重大威胁。

2.安全管理

●账户口令管理严格执行账户口令安全管理，重点排查弱口令问题。杜绝各类口令及凭据长期不更新、账户口令共用、直接使用应用的内置或默认账户等安全问题。

●漏洞修补

了解企业数字资产情况，将补丁管理作为日常安全维护项目。关注补丁发布情况，及时更新和修补系统、应用、服务及硬件产品的相关固件。定期执行漏洞扫描，及时发现设备中存在的安全问题。

●权限管控

定期检查账户情况，审核账户权限的适当性，及时停用非必要的账户权限，对新增账户应有足够警惕并做好各类账户的登记管理。

●内网加固

进行内网主机加固，定期排查未正确进行安全设置、未正确安装安全软件的设备，关

闭设备中的非必要服务，提升内网设备安全性。

3.人员管理

●安全教育

对员工进行安全教育，培养员工安全意识，如识别钓鱼邮件、钓鱼页面等。

●行为规范

制定工作行为规范，指导员工如何正常处理数据，发布信息，做好个人安全保障。避免员工将公司网络部署、服务器设置发布至互联网。

●设备及网络使用规范

要求员工不共享企业内网，办公设备不安装来路不明的软件等。

（三）

遭受勒索软件攻击后的防护措施

1.比照"企业安全规划建议"中的事项，对未尽事项进行及时更正或加强。

2.检测系统和软件中的安全漏洞，及时进行修补。

3.检查口令及凭据是否具有足够的长度和复杂性，并更新安全度不足或疑似已遭泄露的口令及凭据。

4.对于在勒索攻击中尚未遭到加密的重要文件进行及时备份，避免被仍处于活跃状态的勒索软件进行新一轮加密。

5.加强对敏感数据的隔离。如有条件，建议尽可能完全断开敏感数据与外界的一切连接，避免具有多重勒索功能的病毒进一步获取更多的重要信息作为勒索筹码。

二
针对个人用户的安全建议

对于普通用户，我们给出以下建议以帮助用户免遭勒索软件攻击。

（一）
养成良好的安全习惯

1.电脑应当安装具有高级威胁防护能力和主动防御功能的安全软件，不随意退出安全软件或关闭防护功能，对安全软件提示的各类风险行为不要轻易采取放行操作。

2.可使用安全软件的漏洞修复功能，第一时间为操作系统和浏览器，常用软件打好补丁，以免病毒利用漏洞入侵电脑。

3.尽量使用安全浏览器，减少被挂马攻击、钓鱼网站攻击的风险。

4.重要文档、数据应经常做备份，一旦文件损坏或丢失，也可以及时找回。

5.电脑设置的口令要足够复杂，包括数字、大小写字母、符号且长度至少应该有8位，不使用弱口令，以防攻击者破解。

（二）

减少危险的上网操作

1.不要浏览来路不明的色情、赌博等不良信息网站，此类网站经常被用于发起挂马、钓鱼攻击。

2.不要轻易打开陌生人发来的邮件附件或邮件正文中的网址链接，也不要轻易打开扩展名为js、vbs、wsf、bat、cmd、ps1等脚本文件和exe、scr、com等可执行程序。对于陌生人发来的压缩文件包，更应提高警惕，先使用安全软件进行检查后再打开。对各类通讯群发来的文件，更不要盲目打开。

3.电脑连接移动存储设备（如U盘、移动硬盘等），应首先使用安全软件检测其安全性。

4.对于安全性不确定的文件，可以选择在安全软件的沙箱功能中打开运行，从而避免木马对系统的实际破坏。

（三）

采取及时的补救措施

安装360安全卫士并开启反勒索服务，一旦电脑被勒索软件感染，可以通过360反勒索服务寻求帮助，以尽可能地减小自身损失。

三
不建议支付赎金

最后——无论是个人用户还是企业用户，都不建议支付赎金！支付赎金不仅变相鼓励了勒索攻击行为，而且解密的过程还可能会带来新的安全风险。

用户可以首先尝试通过还原备份、数据恢复、数据修复等手段挽回部分损失。例如部分勒索软件为了提高加密效率，只会对文件的头部数据进行部分加密，对于某些特定类型的文件（通常是数据库文件），可以尝试通过数据修复手段来找回被加密的文件内容。

即便在损失不可挽回又无法承受的前提下不得不支付赎金，也可尝试与黑客协商来降低赎金价格，同时在协商过程中应尽可能避免暴露自己真实身份信息和急迫程度，以免黑客漫天要价。

四
勒索事件应急处置清单

在此，我们准备了一份勒索软件事件的应急排查处置清单，遇到此类问题的管理员，可对照下面清单，完成事件的初步处理，之后再由专业团队详细排查事故原因。

勒索软件应急处置清单

✧检查中招情况

检查有哪些设备被攻击，常见被攻击特征有：文件后缀名被改，文件夹留下勒索信息，桌面背景被修改，弹出勒索提示信息。

- ●公网服务器
- ●域控设备与管控设备
- ●内网共享服务器
- ●办公机（检查是否仅是共享文件夹被加密）

✧控制勒索蔓延

根据现场情况，对已经发现的被攻击设备或者存在风险的设备与网段进行临时管控，常见管控方法包括：

- ●访问控制
- ●网络隔离/主机隔离
- ●端口访问控制（常见端口包括：445、135、137、139、3389、22、6379、3306、7001）
- ●设置IP访问黑白名单：禁止国外IP访问/仅允许特定IP访问 或 仅允许本地IP访问
- ●控制重要设备的访问权限，或对重要设备做临时下线处理。
- ●物理隔离
- ●关闭设备/设备断电

●拔出网线/禁用网卡/禁用无线网卡/移除移动网卡

●密码策略

●修改全部管理员账号密码

●禁用归属不明账号

●临时停用非必要账号，修改所有普通用户账号密码

✧排查关键节点

在完成上述应急处置后，尽快确认以下事项，并联系安全团队进行进一步排查。（注意：被加密的文件本身不是病毒。）

●确定机器感染勒索软件时间

●收集可疑样本、被加密文件（少量）、勒索提示信息（一份）

●收集中招设备系统安全日志与防火墙日志

●检查存储有敏感信息设备是否被异常访问

●检查设备中账户情况，包括第三方软件账户，最近新增账户

●检查数据库账户，VPN账户，NAS账户，VNC类软件配置

●排查Web日志

●排查最近运行记录

●临时禁用发现的攻击账号

●使用安全软件进行扫描

●完成后续安全加固工作，安装补丁，修补存在的其它问题。

附录 1

2025年勒索软件大事件

P106

P124

2025年勒索软件大事件

Qilin勒索软件在2025年度全球扩张

2025年，Qilin勒索软件凭借成熟的“勒索即服务”（RaaS）商业模式，实现了全球性的迅猛扩张，成为本年度全球网络安全领域最受关注的勒索威胁之一。作为近年来崛起的勒索软件家族，Qilin在2025年的表现尤为猖獗，其攻击范围覆盖全球主要经济体，攻击频次和破坏程度均创下历史新高，对全球关键基础设施和商业组织的网络安全构成严重挑战。

据安全厂商监测数据显示，Qilin勒索软件在2025年在60多个国家和地区发起了近800起攻击，其攻击主要集中于美国、法国、加拿大、英国等发达国家。从行业分布来看，Qilin则主要针对制造业、科技行业、金融服务业、医疗健康业等高价值行业，同时还涉及政府机构、教育机构等公共领域。

Qilin勒索软件的核心竞争力在于其高度隐蔽且不断迭代的攻击策略，利用AnyDesk、SplashTop等正规远程管理工具，规避终端防御系统的检测，并通过植入未经数字签名的恶意驱动程序，绕过Windows系统的内核级防御机制，实现对终端设备的深度控制。2025年下半年，该团伙还实现了“Windows系统部署Linux版勒索软件”的跨平台攻击模式，通过在Windows服务器中搭建虚拟Linux环境运行勒索程序，大幅提升了攻击的隐蔽性和检测难度。在攻击流程上，Qilin通过钓鱼邮件诱导点击恶意链接，再利用软件、系统漏洞或窃取内部人员登录凭证来获取初始访问权限。进入系统后，其迅速与主控服务器建立通信并展开攻击，对目标系统的核心业务数据实施加密，留下勒索通知文本索要高额比特币赎金。

2025年9月5日，彭博社的内部新闻采编系统和客户数据管理系统遭Qilin勒索软件加密，导致部分财经新闻发布延迟，客户交易数据无法正常调取，最终彭博社为恢复业务支付了150万美元赎金。此外，美国斯巴达堡县政府、肯尼亚政党登记办公室等公共机构也未能幸免，斯巴达堡县政府因系统瘫痪导致车辆管理、税务申报等公共服务中断长达3天，肯尼亚政党登记办公室则因选民信息被加密，一度影响地方选举的筹备工作。

Qilin勒索软件的全球扩张背后，得益于其成熟的RaaS运营模式。这种合作运营模式极大地降低了勒索攻击的门槛，使Qilin能够快速整合全球的黑产资源，扩大攻击覆盖面。

二

马来西亚机场遭勒索攻击致运营中断

2025年3月23日，马来西亚吉隆坡国际机场遭遇疑似勒索软件攻击，引发系统大规模异常，导致机场核心运营服务中断，成为本年度东南亚地区最具影响力的关键基础设施网络攻击事件之一。据马来西亚《新海峡时报》援引机场内部工作人员的消息报道，此次攻击事件导致机场系统瘫痪持续时间超过10小时，其间机场被迫全面启用人工操作模式，工作人员通过手写登机牌、人工核对行李信息等方式保障基础运营，导致大量航班延误，部分国际

航班的延误时间长达4小时以上。更严重的是，部分航班信息牌在后续两天仍出现间歇性故障，给旅客出行带来持续困扰。

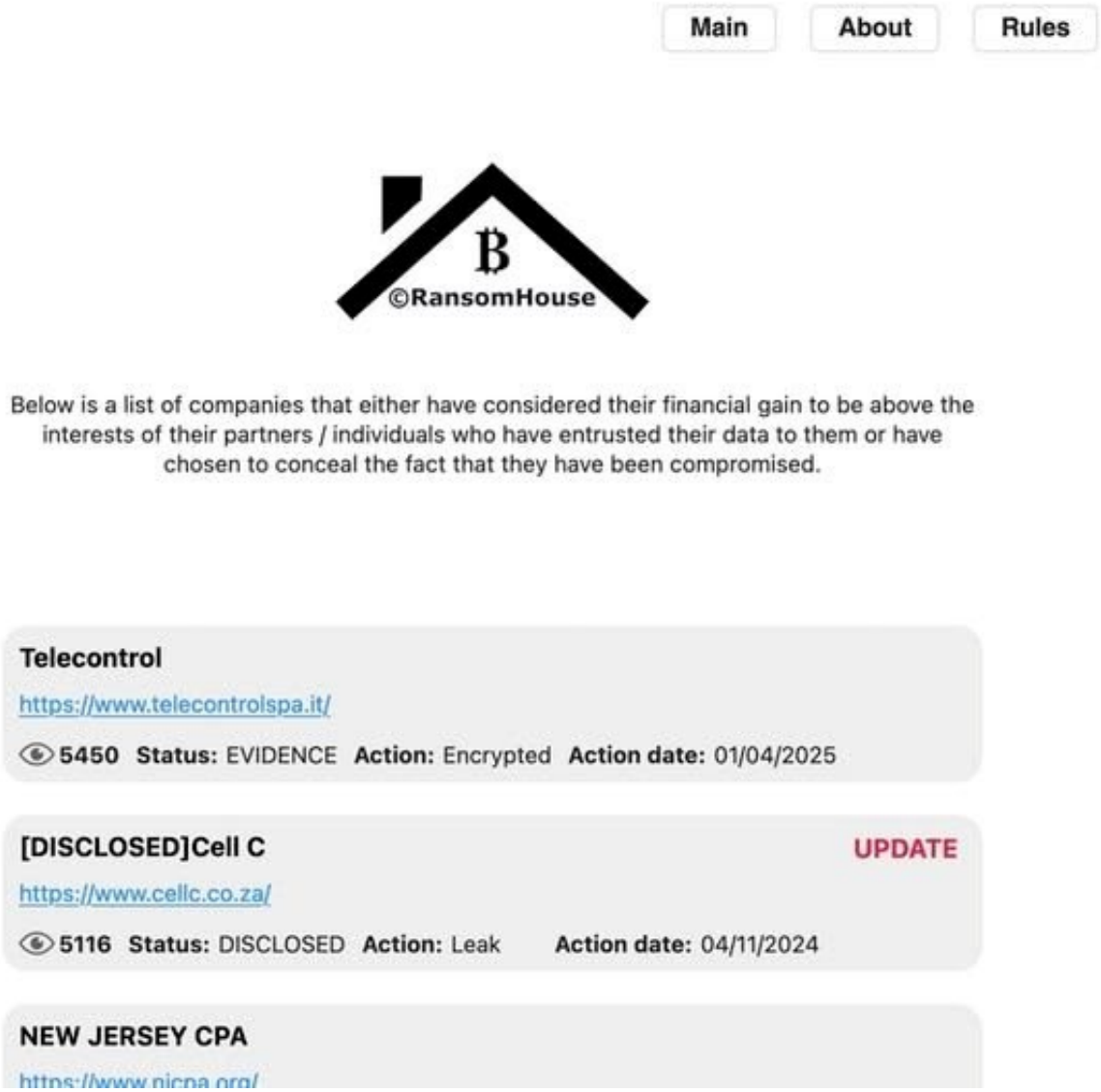
3月24日，马来西亚总理在国会公开证实，黑客已成功入侵马来西亚机场控股公司的数字系统，并且向MAHB索要1000万美元的赎金，要求以比特币形式支付。但企业明确表示，政府基于国家网络安全和公共利益原则，已决定拒绝支付赎金，并责成相关部门全力应对此次安全事件。然而，企业方面的总经理则在3月25日召开的新闻发布会上，公开否认机场运营因攻击出现中断，声称航班运行始终保持正常不存在旅客滞留情况。并称系统出现的短暂异常是由于“常规技术维护”导致，并非勒索软件攻击。

作为马来西亚负责网络安全的核心机构，马来西亚国家网络安全局在事件发生后迅速介入。其首席执行官表示，该局自3月23日收到攻击事件报告后已立即启动应急响应机制，密切跟踪事件进展，并对机场受影响的系统进行持续监测和技术支持。网络安全局明确指出，机场系统确实受到了网络安全威胁，但未进一步披露威胁的具体类型和攻击团伙的相关信息。

有行业分析师估算，此次事件给运营方造成的直接经济损失超过500万美元，包括航班延误赔偿、人工运营成本增加以及品牌声誉受损等。目前，运营方仍未披露攻击团伙的身份、攻击路径的具体细节以及系统完全恢复的时间，事件的后续调查进展仍受到行业关注。

三

RansomHouse勒索攻击全球发力



2025年，RansomHouse勒索软件组织活跃度继续提升，接连拿下多家大型企业，成为当前威胁程度最高的双重勒索软件家族之一。该组织在今年对全球多行业、多地区均发起了猛烈攻击，呈现出攻击范围广、威胁程度高、技术手段新的特点。该组织自2021年12月

成立以来，已从单纯的数据勒索转变为从自动攻击到双重勒索的全链条安全威胁。其主要借由边界设备如VPN网关入侵企业内网，擅长攻击企业VMware ESXi服务器，一旦成功便会造成企业内部系统的大规模瘫痪，重要数据被窃取丢失等问题。

1月27日，国内便有某专注数据保护领域的科技公司遭到RansomHouse攻击，500GB核心数据被窃取，涵盖客户信息、技术文档及商业机密。攻击者利用漏洞入侵后，通过横向移动获取管理员权限，不仅加密服务器数据，还擦除关键备份，导致业务中断超48小时。无独有偶，根据该组织在自己暗网主页上公布的数据公布信息，其在2月8日又对另一家从事芯片制造的中国科技企业发起攻击，共窃取了3TB的内部数据。这些事件无疑都凸显了RansomHouse对中国科技企业的精准打击，也暴露了部分企业在数据安全防护方面的短板。

除中国企业外，国外制造及零售行业也遭到了RansomHouse的针对性攻击。5月5日，RansomHouse宣称窃取了德国啤酒巨头奥丁格2022—2025年核心机密，包括商业计划、供应商合同及员工信息，威胁不支付赎金就公开数据，预估损失达数百万美元；10月初，日本电商巨头Askul遭攻击，1.1TB数据被盗，涉及74万条客户记录，导致其电商平台及供应链系统瘫痪，影响无印良品等多家零售商运营，攻击者利用外包合作伙伴管理员账户入侵，禁用终端安全软件，同时部署多款勒索工具并擦除备份文件，造成IT系统故障持续数周。

RansomHouse的攻击也并非局限于企业领域，其对公共服务与相关关键领域的攻击也不罕见。南非电信运营商Cell C便于4月遭其攻击，核心用户数据库泄露，影响超百万用户通信服务，攻击者在暗网拍卖用户数据，引发严重隐私危机；此外，法国巴黎的萨克雷大学、保加利亚最高行政法院等教育、政府机构也成为攻击目标，攻击者通过窃取敏感数据施压要求支付赎金，部分机构因拒绝支付导致数据公开，声誉受损严重。

RansomHouse在2025年的攻击覆盖了中国、德国、日本、南非、法国等10余个国家，涉及科技、制造、零售、电信、教育、政府等众多领域，其造成的经济损失据估算可能超过10亿美元，对世界各国的企业与公共机构均带来了巨大的安全威胁。

四
四川德阳连锁超市遭LockBit4.0勒索攻击

2025年5月，四川省德阳市某知名连锁超市遭遇LockBit4.0勒索软件攻击，导致其核心业务系统全面瘫痪，停业长达一周，造成重大经济损失。此次事件是本年度国内中小零售企业遭遇勒索攻击的典型案例，暴露了国内中小微企业网络安全防护薄弱的普遍问题，也引发了行业对零售行业数据安全和应急响应能力的广泛讨论。

据报道，此次攻击发生于2025年5月12日凌晨。黑客通过境外远程虚拟IP地址，利用该连锁超市数据库系统未及时修复的高危漏洞实施入侵，成功获取服务器控制权后，上传并运行LockBit4.0勒索软件，对超市的核心业务数据进行加密锁定。受攻击影响，超市的管理系统、库存管理模块、商家供货数据系统以及会员储值信息系统均陷入瘫痪，所有数据无法正常调取。勒索软件释放的勒索信息中包含一个比特币钱包地址和联系方式，黑客要求超市在72小时内支付15个比特币（当时约合人民币825万元）的赎金，否则将永久删除解密密

钥，并将泄露会员储值信息等敏感数据。由于核心业务系统瘫痪，超市无法正常开展运营活动，不得不宣布旗下5家门店全部停业。此次停业一周给超市造成的直接经济损失超过20万元，间接损失更是难以估量。

2025年5月28日，德阳市公安局专案组在重庆市警方的配合下，成功将犯罪嫌疑人王某抓获归案。警方在王某的住所查获了多台电脑、服务器以及大量的黑客工具和攻击脚本。据王某供述，他选择中小零售企业作为攻击目标，主要是因为这类企业网络安全防护意识薄弱，大多没有专业的网络安全技术人员，系统漏洞长期不修复，攻击成功率高，且企业为了尽快恢复运营，更容易选择支付赎金。目前，王某已被德阳市公安局依法采取刑事强制措施，案件已进入司法审理阶段。

此次事件给国内中小零售企业敲响了警钟。行业专家指出，当前国内大量中小微企业存在网络安全投入不足、防护意识薄弱、应急响应能力欠缺等问题，已成为勒索软件团伙的重点靶向目标。为了提升网络安全防护能力，中小微企业应加强系统漏洞管理，定期进行漏洞扫描和修复；建立完善的备份体系，对核心数据进行多副本、异地备份；加强员工的网络安全培训，提高对钓鱼邮件、恶意链接的识别能力；同时，可寻求专业网络安全厂商的支持，部署适合自身规模的安全防护产品。德阳市公安局也借此事件发布预警，提醒各类企业加强网络安全防护，一旦遭遇勒索攻击，应第一时间报案，切勿轻易支付赎金。

五
美国环球健康服务公司医疗网络瘫痪

2025年初，美国环球健康服务公司旗下核心子公司Change Healthcare遭遇BlackCat勒索软件攻击，导致全美范围内医疗网络大规模瘫痪，大量医疗数据泄露，成为美国医疗行业史上最严重的数据泄露事件之一。此次事件的影响持续蔓延数月，不仅严重扰乱了美国医疗行业的正常运营秩序，还引发了公众对医疗数据安全的信任危机，推动美国国会加强对医疗行业网络安全的监管审查。

此次攻击最早发生于2024年2月21日，BlackCat勒索团伙通过窃取Change Healthcare员工的登录凭证，入侵了未启用多因素认证的Citrix远程访问服务，成功获取了企业内部网络的访问权限。更严重的是，此次攻击导致大量患者敏感数据被窃取。

2025年1月，联合健康集团发布的最终调查结果显示，此次事件共泄露1.927亿人的敏感信息，远超初期预估的1亿人，覆盖了超过半数的美国民众。泄露的数据包括患者的诊断记录、检测结果、医保账号信息、社会安全号、驾照信息、银行卡信息等核心个人信息，这些信息一旦流入黑产市场，可能被用于身份盗窃、诈骗等违法犯罪活动，给患者带来长期的安全隐患。

为了尽快恢复系统运营并阻止数据泄露，联合健康集团向BlackCat团伙支付了2200万美元的比特币赎金，并与团伙达成协议要求其删除窃取的所有数据。然而，黑客在收取赎金后实施了“退出诈骗”，不仅未删除窃取的数据还关闭了用于协商的服务器，导致数据泄露范围进一步扩大。有消息称，部分泄露的患者数据已在暗网市场流通，引发了多起针对患者的精准诈骗案件。

2025年1月，联合健康集团开始向受影响用户发送数据泄露通知，并提供免费的信用监控服务。美国卫生与公众服务部立即将此次事件列为“美国史上最严重的医疗数据泄露事件”，并对联合健康集团展开调查，追究其在数据安全防护方面的责任。此次事件引发了美国公众对医疗数据安全的强烈担忧，超过60%的美国民众表示对医疗行业的数据安全保护能力缺乏信任，多个消费者权益组织呼吁加强对医疗数据的监管。

此次事件也推动美国国会加快了医疗行业网络安全监管立法的进程。2025年2月，美国国会提出《医疗数据安全强化法案》，要求所有医疗服务机构和医疗数据服务商必须建立符合联邦标准的网络安全防护体系，启用多因素认证、数据加密、定期漏洞扫描等安全措施；同时，要求企业建立健全数据泄露应急响应机制，发生数据泄露后必须在72小时内上报监管部门，并及时通知受影响用户。此外，法案还明确了对违反数据安全规定企业的处罚措施，最高罚款可达企业年营业额的5%。

行业专家指出，此次事件暴露了美国医疗行业网络安全防护的诸多短板，包括部分企业对网络安全重视不足、安全投入不足、多因素认证等基础安全措施未落实到位、应急响应能力欠缺等。为了提升医疗行业的网络安全水平，除了加强监管外，医疗企业还应加大网络安全投入，部署先进的安全防护技术，加强员工的网络安全培训，建立多副本、异地备份的灾备体系，提高应对勒索攻击的能力。

六

BlackSuit勒索攻击席卷450余家美国机构

2025年，BlackSuit勒索软件团伙发起大规模勒索攻击行动，席卷美国450余家机构，涵盖医疗、教育、公共安全、能源及政府部门等关键领域，成为美国本年度最具破坏性的勒索威胁之一。该团伙成立于2022年，是Royal勒索软件团伙的继任者。Royal团伙在2023年遭遇多国执法机构打击后，其核心成员重组形成了BlackSuit团伙，并继承了Royal团伙的攻击工具、技术团队和附属运营网络。

2025年，BlackSuit团伙将攻击目标重点聚焦于美国的关键基础设施和公共服务领域，其攻击的450余家机构中，医疗行业占比最高达35%，其中包括多家大型医院和医疗中心；此外，该团伙还针对教育行业、公共安全领域、能源行业、政府部门及其他领域发起攻击。其攻击具有明显的针对性，通常选择机构运营的关键时段发起攻击，以最大化攻击效果，逼迫受害者支付赎金。

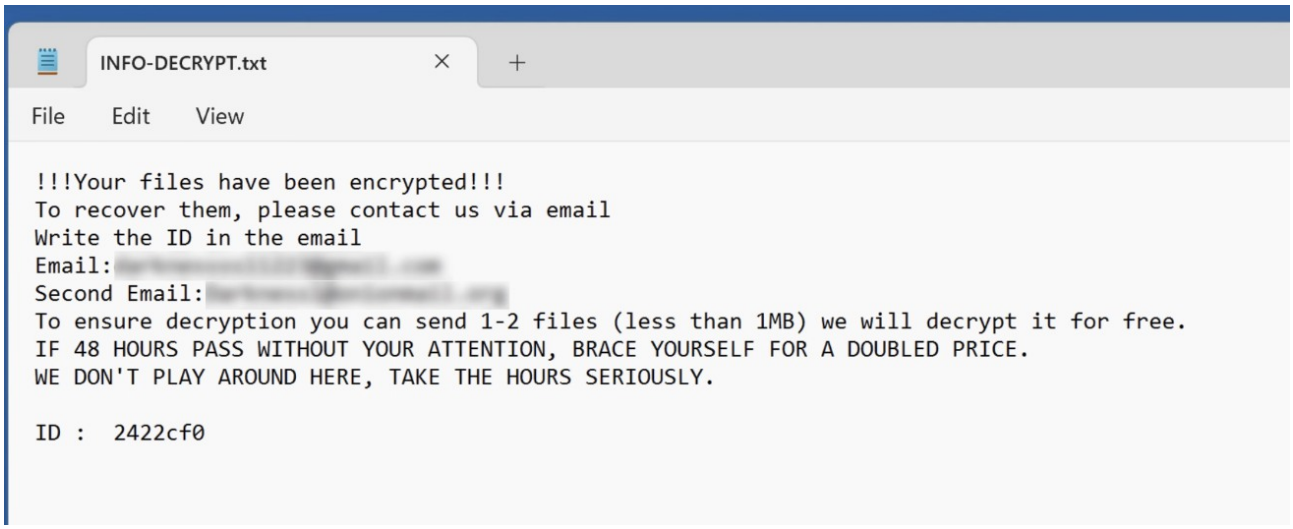
BlackSuit团伙的攻击流程高度标准化，首先通过钓鱼邮件、利用已知系统漏洞或收买内部人员等方式获取初始访问权限。随后，在目标网络内部横向移动，收集敏感数据并窃取备份系统的认证信息。接着，加密目标系统的核心业务数据，同时将窃取的敏感数据上传至团伙控制的服务器。最后，向受害者发送勒索通知，要求其在规定时间内支付赎金，否则将在暗网泄露平台公开窃取的数据。

为了遏制BlackSuit团伙的嚣张气焰，2025年7月24日，美国联合英国、德国、法国、加拿大、乌克兰、立陶宛等多国执法机构，开展了联合打击行动。此次行动中，执法机构成功捣毁了BlackSuit团伙的核心基础设施，包括查封4台用于控制攻击、存储窃取数据的核心服务器，注销了9个用于与受害者协商和发布威胁信息的域名，并冻结了价值109.15万美元的加密货币赎金。

此次联合打击行动取得了显著成效，BlackSuit团伙的攻击活动在行动后大幅减少。据报告，2025年8月—12月期间，BlackSuit团伙发起的攻击次数降至32起，明显低于此前每月平均60起的攻击频次。然而，勒索软件团伙的重组和迭代速度极快，此次打击可能只是暂时遏制了BlackSuit团伙的活动，未来仍需警惕其卷土重来或其他类似团伙的崛起。

七

国内某能源企业受Darkness勒索家族变种攻击



2025年，国内某大型能源企业遭遇Darkness勒索家族变种攻击，成为本年度能源行业网络安全领域的典型事件。尽管官方未公开该企业的具体名称，但从行业披露的信息来看，此次攻击具有明确的针对性、高度的技术专业性和较大的破坏性，不仅导致企业部分生产环节临时中断，还引发了行业对能源企业供应链安全和跨境网络安全防护的广泛关注。

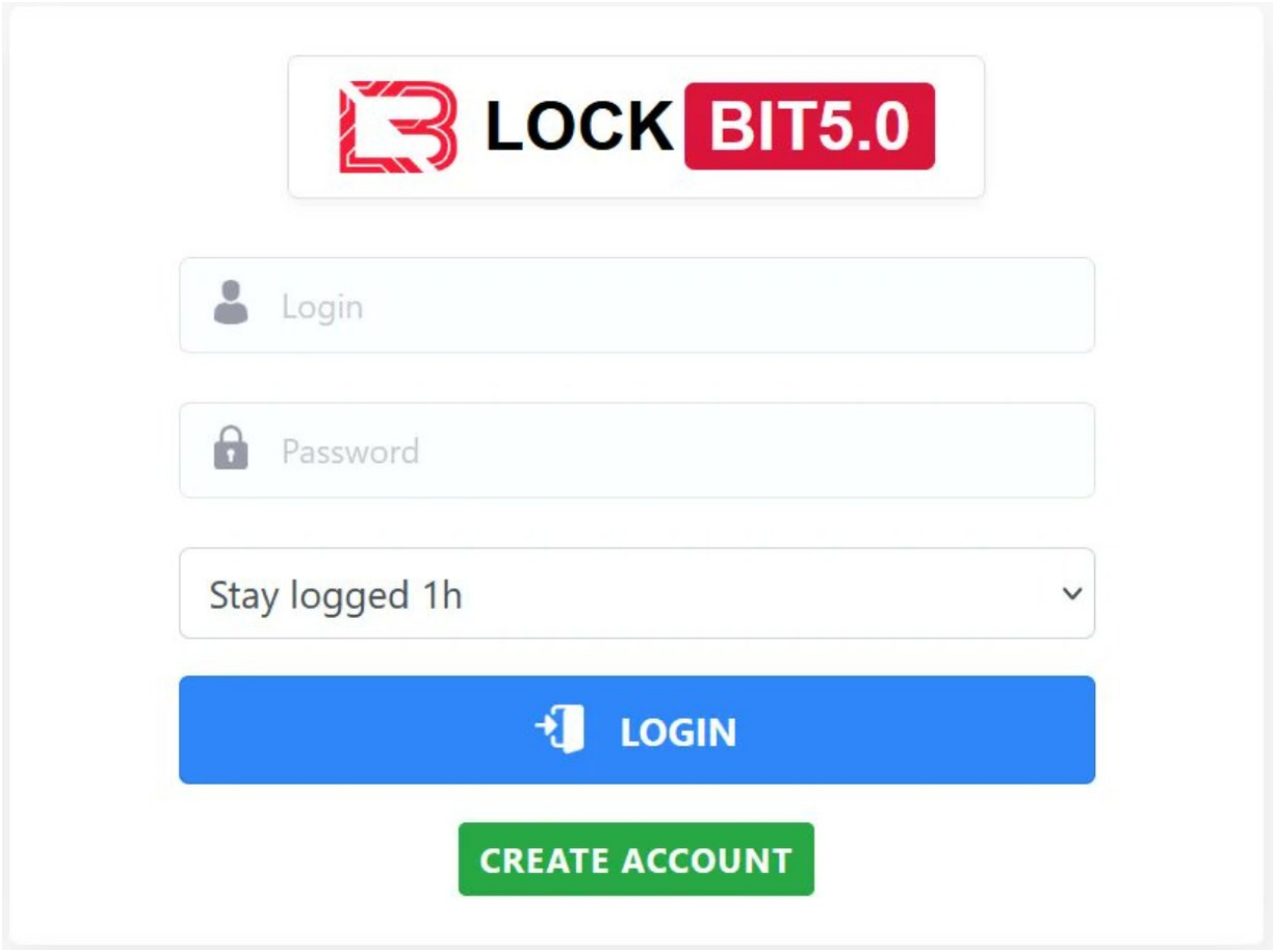
Darkness勒索软件家族最早出现于2023年，以攻击能源、制造等重工业领域企业闻名。据360安全卫士发布的《2025年7月勒索软件流行态势分析》显示，2025年Darkness勒索软件在国内的传播范围显著扩大，新增多个变种，其中攻击能源企业的该变种加密强度极高，且能自动规避主流安全检测工具的扫描，具有极强的隐蔽性。

此次攻击采用了供应链攻击的手段，这也是近年来勒索软件攻击的主要趋势之一。黑客通过渗透该能源企业的一家合作方软件供应商，在其提供的工业控制软件更新包中植入恶意代码。该能源企业在2025年6月对旗下部分生产系统进行常规软件更新时，误将含恶意代码的更新包安装到核心生产服务器中，导致恶意代码成功植入。恶意代码植入后并未立即发起攻击，而是进入了3~7天的潜伏周期，在此期间，黑客通过恶意代码收集企业内部网络的拓扑结构、核心系统账号密码等关键信息，为后续攻击做准备。据行业内部消息透露，此次攻击导致企业的一处油气勘探基地生产中断长达12小时，直接经济损失超过500万元。同时，黑客还窃取了大量企业内部的敏感信息，包括能源勘探数据、长期生产计划、员工个人信息等，以数据公开泄露为要挟，向企业索要高额比特币赎金。

事件发生后，该能源企业第一时间隔离了受感染的服务器和网络区域，并开展溯源与解密工作。应急响应团队通过对受感染系统的勘验取证，逐步还原了黑客的攻击路径，确认此次攻击为Darkness勒索家族变种所为。此外，该企业通过未被加密的异地备份数据，逐步恢复了受影响系统的正常运行。截至2025年7月初，企业的所有生产系统已全部恢复正常运行，但关于是否支付赎金，企业未向外界披露相关信息。

此次事件也推动了国内能源行业加强网络安全防护体系建设。国家能源局也发布相关通知，要求国内能源企业进一步强化网络安全责任意识，完善网络安全防护体系，加强应急响应能力建设，确保能源行业的网络安全和生产稳定。

八
LockBit5.0卷土重来并与多个勒索家族结盟



2025年9月，曾遭多国执法机构重创的LockBit勒索软件更新至5.0版本卷土重来，并与Qilin、DragonForce两大勒索家族正式结盟，形成全球极具威胁的勒索犯罪联盟。此次LockBit的卷土重来和联盟化运作，标志着勒索软件犯罪进入“集团化协同作战”的新阶段，给全球企业的网络安全防御体系带来了严峻挑战。

LockBit勒索软件自2019年出现以来，凭借其成熟的RaaS模式和强大的攻击能力，迅速成为全球最活跃的勒索软件家族之一。2024年，LockBit曾遭遇了重大打击，其34台全球服务器被执法部门关闭，200余个加密货币账户被冻结，导致其运营一度陷入停滞。然而，经过一年多的重组和准备，LockBit在2025年9月正式推出5.0版本卷土重来。

LockBit5.0版本在技术上实现了全面升级，其加密效率提升了50%以上；同时，该版本增强了对工业控制系统、核能电力等关键基础设施的攻击适配性，专门优化了针对SCADA、DCS等工业控制系统的攻击模块，能够精准识别并攻击工业控制设备；更值得警惕的是，LockBit5.0明确将工业控制系统、核能电力等高敏感领域纳入攻击范围，打破了此前多数RaaS组织回避攻击关键基础设施的惯例，被网络安全行业视为一种报复性挑衅行为。

除了技术升级外，LockBit5.0卷土重来后最大的变化是推动了与其他勒索家族的结盟。此次结盟由DragonForce勒索家族主导发起，最终LockBit、Qilin、DragonForce三大勒索家族达成了战术协同与资源共享协议，形成了全球首个具有较大影响力的勒索犯罪联盟。2025年10月，三大团伙联合对德国一家大型汽车零部件制造商发起攻击，通过LockBit的加密工具加密企业核心生产数据，利用Qilin的下属组织网络获取企业内部信息，借助DragonForce的工业控制攻击技术瘫痪企业生产线，导致企业生产中断长达3天，最终企业被迫支付800万美元赎金。

此次联盟化运作给全球网络安全防御带来了新的挑战。一方面，三大团伙的资源共享使得攻击手段更加多元化、隐蔽性更强，传统的网络安全防御手段难以有效应对；另一方面，联盟化运作扩大了攻击覆盖面，提升了攻击的频次和强度，给企业的网络安全防护带来了更大的压力。此外，三大团伙的结盟可能会引发连锁反应，导致更多勒索软件家族效仿，形成更多的犯罪联盟，进一步加剧全球勒索软件威胁的严峻性。

安全专家指出，勒索软件犯罪的联盟化趋势表明，勒索软件已从零散的个人犯罪升级为有组织、有规模的集团犯罪，给全球网络安全带来了长期的威胁。为了有效应对这一威胁，需要政府、企业和网络安全厂商形成合力。安全厂商也应加强技术研发，提升威胁检测和防御能力，为企业提供更有效的安全解决方案。

九
国内医疗行业面对spmodvf勒索攻击

2025年，后缀为.spmodvf的勒索软件在国内医疗行业持续蔓延，成为困扰医疗机构网络安全的主要威胁之一。该勒索软件专门靶向攻击医疗行业，攻击频次高、隐蔽性强、破坏性大，导致多家医疗机构核心业务系统瘫痪，患者就诊延误，引发了行业对医疗行业网络安全防护能力的广泛担忧。尽管网络安全机构和医疗机构采取了一系列应对措施，但由于该勒索软件的家族归属和攻击细节尚未完全明确，防控难度较大。

据360安全卫士发布的《2025年10月勒索软件流行态势分析》显示，.spmodvf勒索软件自2025年初出现以来，传播范围不断扩大，攻击频次持续攀升，已成功冲入月度活跃勒

索家族TOP10榜单。该勒索软件的受害者几乎全为医疗行业机构，涵盖三甲医院、二甲医院、社区医院、诊所等不同规模的医疗机构，其中中小型医疗机构由于网络安全防护薄弱，成为其主要攻击目标，占比超过70%。

2025年，国内多个地区的医疗机构都遭遇了.spmodvf勒索软件的攻击，造成了严重的后果。2025年3月，中部某省份一家二甲医院的核心业务系统遭该勒索软件攻击，CT影像系统瘫痪长达72小时，导致大量需要进行CT检查的患者无法及时就诊，部分重症患者不得不转至其他医院，引发了患者及家属的强烈不满；2025年6月，南方某城市一家中型医疗机构遭遇攻击，由于缺乏有效的数据备份，无法通过备份恢复数据，为了尽快恢复医疗服务，被迫向黑客支付0.8BTC（当时约合人民币45万元）的赎金，但最终仅恢复了部分核心数据，大量历史病历数据永久丢失；2025年9月，北方某社区医院的患者信息系统遭攻击，大量患者的个人信息和就诊记录被窃取，黑客以公开数据相要挟索要赎金，给患者的信息安全带来了严重隐患。

值得注意的是，2025年11月1日《国家网络安全事件报告管理办法》正式实施，该办法明确将医疗行业网络安全事件报告纳入法定义务，要求医疗机构在发生网络安全事件后，必须在规定时间内上报监管部门，不得隐瞒、谎报。这一办法的实施，为.spmodvf勒索软件的溯源与打击提供了重要的政策支撑，有助于网络安全机构收集更多的攻击样本和事件信息，逐步摸清该勒索软件的技术特征和攻击团伙的相关信息。

为了应对.spmodvf勒索软件的威胁，国内医疗行业采取了一系列防控措施。国家卫生健康委发布相关通知，要求各级医疗机构加强网络安全防护，定期开展网络安全自查，及时修复系统漏洞；加强员工的网络安全培训，提高对钓鱼邮件、恶意文件的识别能力；建立完善的核心数据备份体系，对电子病历、患者信息等关键数据进行多副本、异地备份；部署先进的网络安全防护产品，提升对未知威胁的检测和防御能力。同时，网络安全厂商也加大了对.spmodvf勒索软件的研究力度，推出了针对性的检测工具和应急响应方案，帮助医疗机构提升防控能力。

FIT遭INCRansom攻击

2025年8月18日，富士康旗下核心子公司FIT（富泰华工业（深圳）有限公司）遭遇INCRansom勒索软件攻击，导致其全球范围内的核心生产系统、订单管理系统及供应链协同平台全面瘫痪。该公司深圳、郑州两大主力生产基地被迫临时停产，成为本年度影响全球电子供应链的重大网络安全事件。此次事件不仅造成巨额经济损失，更暴露了全球电子代工行业网络安全防护的薄弱环节，引发了行业对供应链核心企业安全韧性的广泛探讨。

FIT作为全球领先的电子制造服务提供商，主要为苹果、华为、小米等全球头部科技企业提供精密结构件、组装代工等服务，其生产系统的稳定运行直接关系到下游多家科技企业

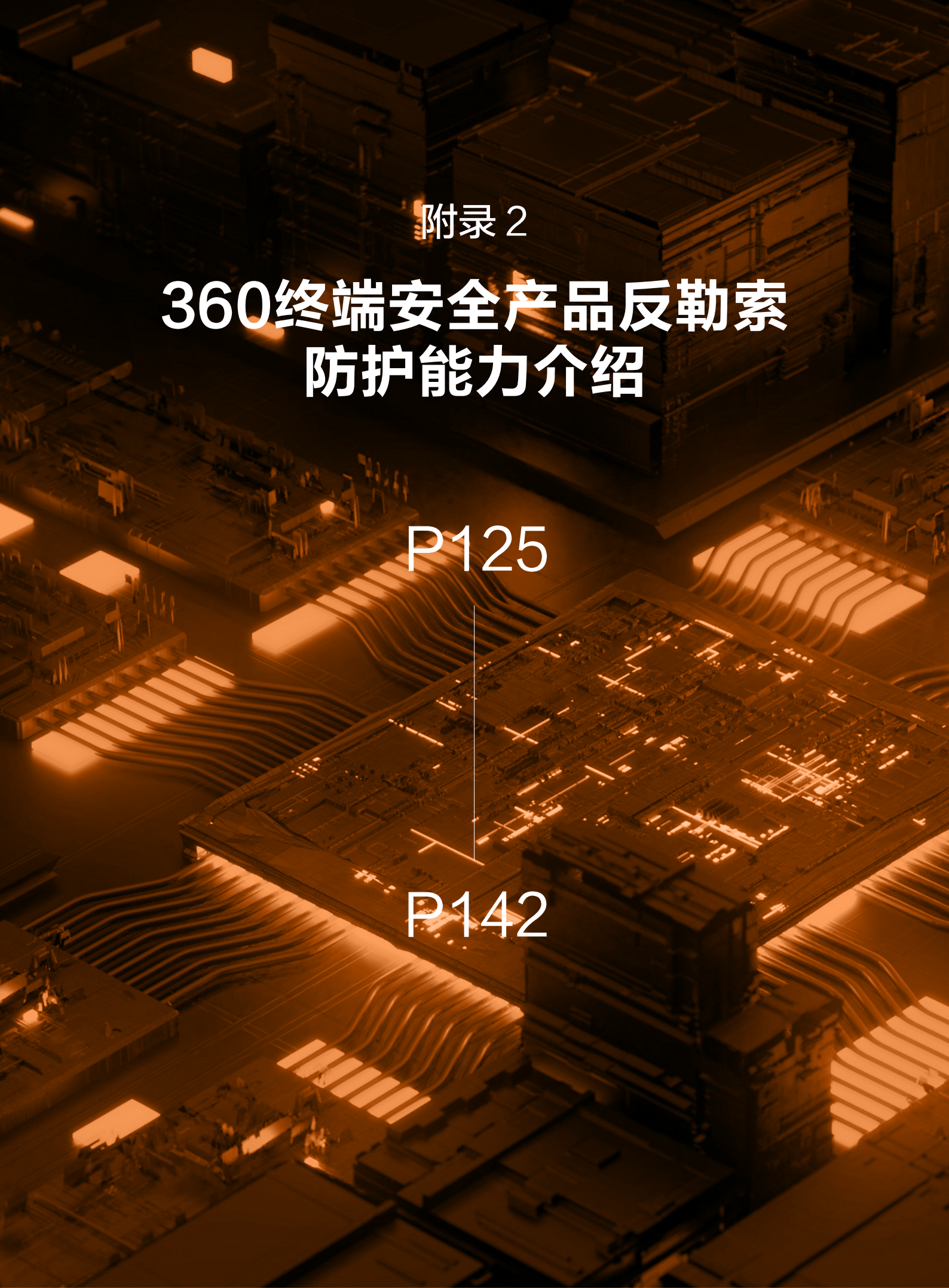
的产能交付。据公开报告显示，此次攻击始于2025年8月18日凌晨2时许，黑客通过境外服务器发起攻击，利用FIT远程访问系统的高危漏洞，暴力破解了多名员工的账号密码，成功获取了内部网络的初始访问权限。随后，黑客在网络内部横向移动，迅速渗透至生产调度、物料管理、数据中心等核心区域，部署INCRansom勒索软件对关键系统数据进行加密。

INCRansom勒索软件是2025年新出现的勒索软件家族，以攻击制造业企业为主要目标，具备极强的针对性和破坏性。该勒索软件对生产计划、物料清单、设备运行参数、客户订单等核心数据进行高强度加密，加密后的数据无法通过常规技术手段解密。更具威胁的是，该软件还具备自动识别并破坏备份系统的功能，黑客在加密核心数据前，已提前删除了FIT本地备份服务器及部分云端备份的数据，切断了企业快速恢复数据的主要路径。

8月19日，FIT技术团队在受感染服务器桌面发现黑客留下的勒索通知文本，黑客要求FIT在72小时内支付1200万美元比特币赎金，否则将永久删除解密密钥并在暗网公开窃取的客户订单信息、产品设计图纸等敏感数据。勒索通知中还附带了部分窃取数据的样本，包括某头部企业的未发布产品结构设计方案，进一步对FIT形成施压。事件发生后，FIT立即启动最高级别应急响应机制，至8月22日其已完全恢复正常生产。关于是否支付赎金，FIT官方未明确披露。

此次事件给全球大型制造企业敲响了警钟。行业专家指出，大型代工企业作为全球供应链的关键节点，往往掌握着大量客户敏感信息和核心生产数据，已成为勒索软件团伙的重点攻击目标。当前部分制造企业存在员工账号密码管理松散、远程访问权限管控不严、灾备体系不完善等问题，给黑客提供了可乘之机。为提升网络安全防护能力，制造企业应加强员工网络安全培训，强化账号密码安全管理，启用多因素认证；加大网络安全投入，部署针对工业控制系统的专项防护设备；建立完善的多副本、异地备份灾备体系，确保核心数据的安全性和可用性。

事件发生后，广东省通信管理局组织省内大型制造企业开展网络安全专项自查工作，重点排查远程访问、工业控制系统等关键环节的安全隐患，要求企业限期完成整改。富士康集团也全面升级了旗下所有子公司的网络安全防护体系，成立了集团级网络安全应急响应中心，统筹应对各类网络安全威胁。



附录 2

360终端安全产品反勒索防护能力介绍

360终端安全产品反勒索防护能力介绍

一

360攻击痕迹检测功能

360的系统日志溯源功能自2024年上线以来广受用户好评，不论用户在遭遇攻击前是否使用了360终端安全产品，该功能都可以为用户提供快速自助溯源排查服务。其可通过对当前系统日志的自动扫描及分析快速定位攻击来源，理清攻击思路以便进一步做出针对性的防护与加固。

2025年我们进一步提升了本地日志覆盖度与溯源能力。新增数千项渗透痕迹的检出点覆盖，并对每项检出都做了简要的描述。帮助遭受攻击之前未使用360终端安全产品的设备也能通过读取有限的各类日志，快速定位攻击的时段及来源，同时针对某些典型场景下的攻击思路提出专门的防护建议。

360渗透痕迹包括敏感行为、痕迹隐匿、防护致盲、攻击脚本、载荷投递、漏洞利用、远程访问、权限维持这八大类检测。

敏感行为：涵盖了包括云上环境在内的各类攻击行为中典型的检测指征，可方便安全分析人员迅速定位潜在风险来源。

痕迹隐匿：涵盖了各类攻击行为中的痕迹隐匿指征，可方便有经验的安全分析人员迅速定位疑似的攻击手法。

防护致盲：涵盖了全球范围内数百家安全厂商的安全产品防护致盲检测，可迅速检出相关产品防护被攻击者关闭的时间点。

攻击脚本：涵盖了各类攻击脚本的检测，可迅速检出各类渗透攻击载荷的加载时间点，可方便有经验的安全分析人员迅速定位攻击手法。

实施投毒：对挖矿行为、勒索病毒、远控木马、渗透工具等流行威胁指征做到应检尽检，可方便安全分析人员或系统管理员迅速定位攻击类型。

漏洞利用：对攻击过程中使用的漏洞利用指征以及各类高可疑的内存溢出行为进行检测，可方便有经验的安全分析人员迅速定位攻击链路。

远程访问：对全球范围内已知的易被恶意利用的合法远控软件与内网穿透类软件进行植入检测，可方便有经验的安全分析人员迅速定位攻击链路。

权限维持：对攻击场景下的权限维持相关行为进行检出，可方便安全分析人员或系统管理员评估后续加固策略。

下面通过一些具体的事件来说明这一产品新增的功能点。

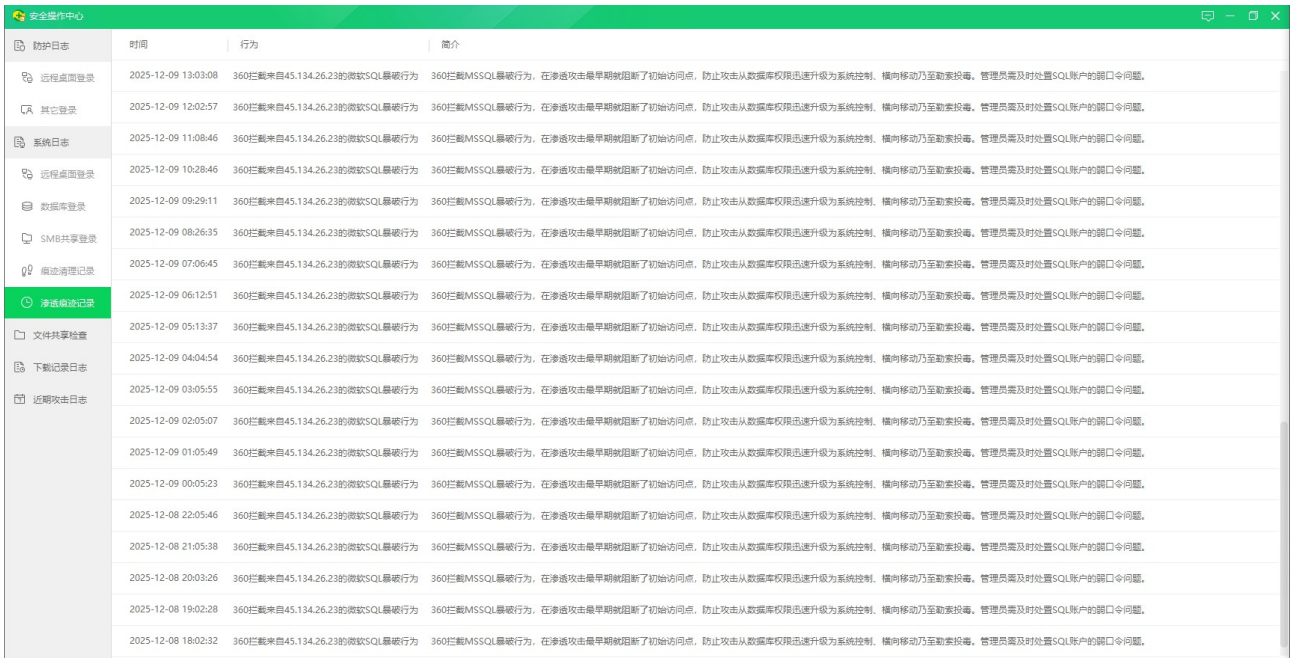
识别热门勒索家族

此处展示的是对2025年国内流行度最高的Weaxor勒索软件家族执行行为的识别结果。可以看到，痕迹检测在准确识别勒索软件执行事件的同时，清晰刻画了其攻击发起的链路方式及关键攻防要点，并给出了简明扼要的分析说明。

▲图1. 识别Weaxor勒索软件执行事件

识别第三方安全厂商记录的风险内容

在识别Windows Defender检出风险的基础上，本次更新增加了第三方安全软件写入系统日志中的风险提示。方便安全分析人员对攻击链路与防护致盲行为进行梳理，快速归因与提取恶意样本路径及文件哈希。目前支持识别的第三方安全厂商包括：360、猎鹰安全（原金山毒霸）、卡巴斯基、Dr.Web、Symantec、SentinelOne、Trellix、Sophos、CrowdStrike、Palo Alto Networks。



▲图2. 识别360检出微软SQL暴破风险的提示

识别银狐等黑产组织常用的攻击手法

随着银狐木马家族与众多勒索组织积极地与安全软件做攻防对抗、加载漏洞驱动等行为都是存在黑产攻击行为的典型指征。本次更新对黑产组织常用的手法进行了检出，方便管理员快速定位攻击手法与入侵时间线。

▲图3. 识别BYOVD驱动攻击

更多功能持续提升

除上述列举的功能外，还增加了更多的攻击溯源场景优化，在此不做过多赘述，相信使用过的用户都会对此项功能的能力有很深的体会。同时，我们也会在后续的产品更新中不断根据新的攻防态势进一步增加更多检测项目及能力，与广大的系统管理人员及安服人员共同打造一个更加安全的系统环境。

此功能已集成在360安全卫士和360企业安全云的“远控勒索急救”中的“被攻击查询”项目内，欢迎有此方面能力需求的用户移步前往体验。

二

远控与勒索急救功能

360在2023年下半年，新推出了远控与勒索急救功能，用来解决用户在已经感染或怀疑感染远控木马或勒索病毒的场景下，帮助用户快速建立一个临时的安全场景，我们的防护功能将运行在一个严格监控的模式下，阻止一切可能的破坏行为，避免系统和数据进一步被攻击活动破坏。作为一个后置方案，它还将一些排查处置策略、溯源方法制作成了一键排查功能，协助管理员快速应对勒索攻击。

▲ 远控 · 勒索急救功能界面

远程控制权限：将对一些远控的关键功能进行限制，如屏幕读取，键盘记录，键盘鼠标操作等，以及提供对一些重要敏感进程与文件的保护。

访问权限：将对系统中，常见的文档、数据库、音视频等数据文件提供保护，避免被篡改或删除。对进程的运行、联网也将进行严格的限制。

一键扫描功能，可以检出是否存在高风险的启动项、系统账户的弱口令、黑客工具、高危的远控软件并进行相应处理。

▲ 远控 · 勒索急救扫描界面

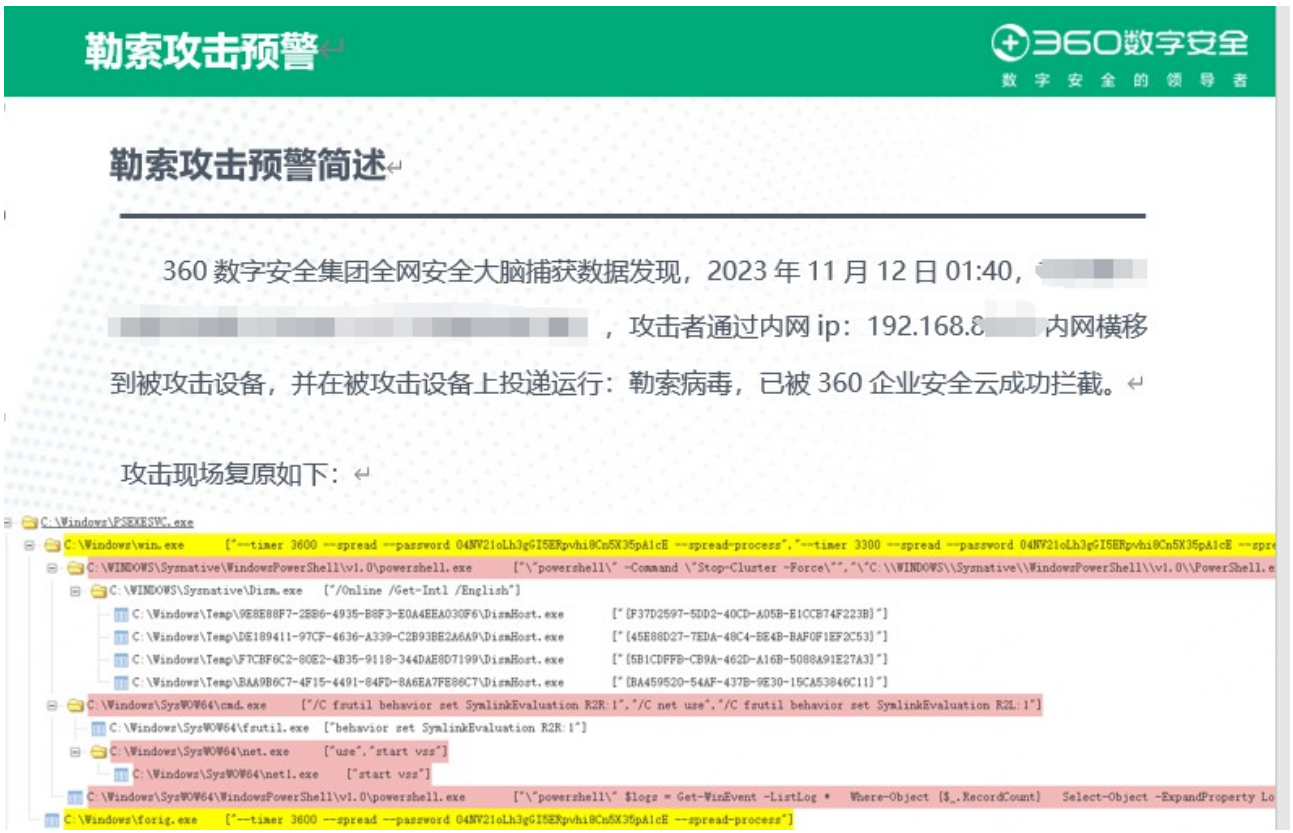
“被攻击查询”功能，可看到各类攻击信息，其中“系统日志”的“远程桌面登录”项完整记录了成功登录的IP与账户信息及时间信息。同时提供了勒索攻击常见的“数据库登录”“SMB共享登录”“痕迹清理记录”查询，方便进行攻击时段的溯源排查。

▲ 远程桌面暴破记录查询界面

三

勒索预警服务

2025年，360的勒索预警订阅服务，基于360全网安全大数据视野，监测勒索攻击的多个环节，在勒索攻击的准备阶段，以及病毒初始投递阶段，对监管、企业用户提供勒索预警订阅服务。希望在勒索的前期阶段，进行阻断，避免造成受害单位的进一步损失。2025年共计捕获勒索攻击事件线索5858起，涉及受害单位1639家，确认勒索病毒家族62个，攻击IP来源地涉及境外52个国家或地区，配合监管输出勒索攻击事件线索674起，覆盖全国多个地区。



▲ 勒索攻击预警服务

四
弱口令防护能力

弱口令攻击一直是勒索软件最重要的传播手段，360安全卫士自2017年开始提供弱口令攻击防护，为亿万用户提供了安全保护。在与勒索软件对抗的过程中，产品也一直在提升安全能力，保证了可以应对最新攻击手法，为用户提供更好的体验。

下图是2025年防黑加固功能每月所防御的攻击量，2025年，360防黑加固共保护近216万台设备免遭入侵，拦截各类弱口令入侵共计超过12亿次。

数据来源：防黑加固统计数据

▲ 勒索攻击预警服务

以下是360提供弱口令攻击防护的重要更新时间轴：

●**2017年-2018年**：新增对远程桌面弱口令防护支持。

●**2018年-2019年**：新增SQL Server暴破、VNC暴破、Tomcat暴破的防护支持。

●2019年：

■新增RPC协议弱口令暴破防护

■SMB协议暴破拦截优化版正式上线

■新增对金万维、瑞友管理软件的支持。

■对MYSQL、SQL Server、Tomcat等服务器常用软件也加入了多方位的拦截防护。

●2020年：

■用户登录提醒：如果机器在未登录阶段受到攻击，在用户下次登录时，会提醒用户之前发生攻击的概况，提醒用户加强安全防护。

■弱口令提示：对正在使用弱口令的账户主动做出提醒，建议用户及时修改口令。

■登录IP黑名单：通过云端安全大数据，动态配置IP黑名单，保护用户电脑免受攻击。

■账户黑名单：由于各种条件限制，有部分设备无法修改内置账户和口令，造成设备被攻击，360安全卫士提供了账户黑名单功能，记录了各类数据库和应用系统的内置账户密码和已经泄露的一些账户密码。限制这类账户密码组合使用的远程登录情况，保障用户设备免受攻击。

●2021年：

■支持拦截时间段控制

■来自风险地区的IP拦截

●2023年：

■增加暴破日志查询

■企业安全云增加远程接入策略，实现IP白名单功能

●2024年：

■企业安全云高级功能增强，支持更丰富防御定义

五
数据库保护能力

数据库文件是勒索软件攻击的头号目标，数据库被加密，也是企业面临的最严重勒索风险，一旦数据库被攻破，会直接对用户造成严重的数据泄露或损坏。

360终端安全针对数据库面临的勒索风险问题，也推出了数据库加强保护功能，在常规的勒索保护之外，增加了针对数据库特有情况的专门保护。针对数据库常见的SQL注入，数据库爆破等攻击，360的数据库防护功能，对恶意SQL语句进行识别和拦截。同时还加强了对数据库服务的保护，避免勒索软件对数据库服务与文件本身的破坏。

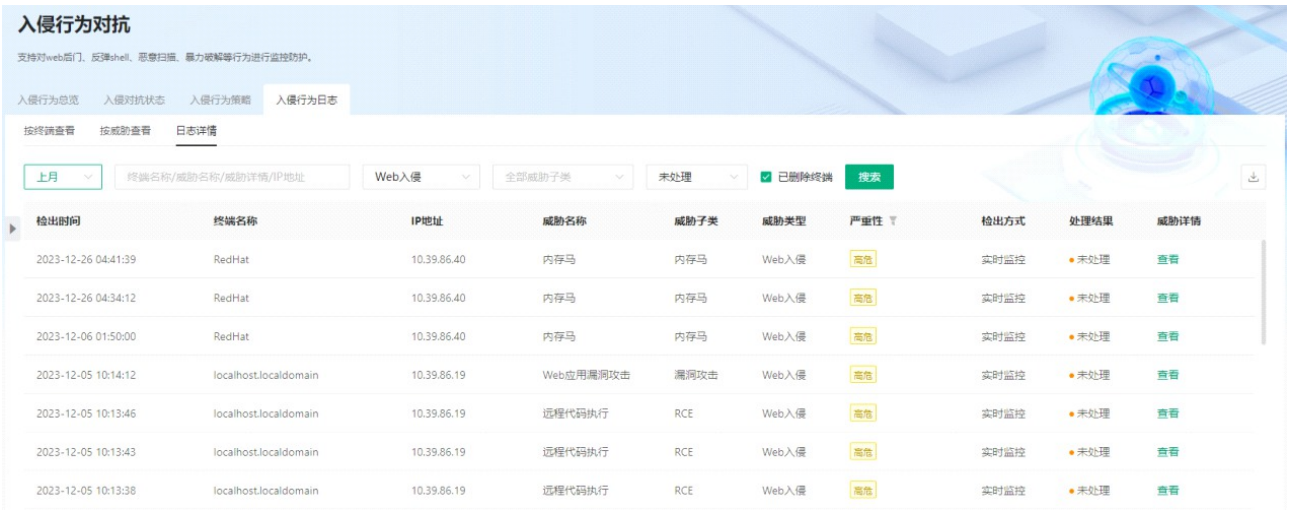
▲ 数据库攻击防护弹窗

六
Web服务漏洞攻击防护

Web服务类漏洞攻击，是目前最常见的一类针对服务器的勒索攻击手段。部署在服务器中的各类Web应用，如OA系统、财务系统经常成为勒索团伙的攻击目标。

360 RASP可以实现对Web资产的梳理和实时防护。通过应用程序执行上下文，语义分析，ASM栈帧分析，并结合360庞大的用户量和多年攻防实战经验制定的安全规则和算法。有效防护RCE漏洞、文件上传漏洞、反序列化漏洞、内存马攻击等，实现NDay漏洞的防护和0Day漏洞的告警，具备更深度的监控和威胁感知能力。RASP基本适配所有Java版本和主流的操作系统，所有防护插件使用独立的ClassLoader加载，灵活启停，支持热更新，对现有业务无影响，稳定性高，目前已在数十万服务器终端上稳定运行，目前已经支持超过280个Nday漏洞告警。

还有针对.Net漏洞的专项防御DNRSP，支持.Net Framework 4.0及其以上的主流.Net版本，具有广泛的适用性。DNRSP的原生SDK基于系统原始API设计，提供统一的防护和识别接口，对系统运行无额外负担，除此之外，考虑到.Net应用的场景已经使用问题，DNRSP支持热更新，在不影响业务运行情况下实现防护功能的动态更新与防护能力的增强。



▲Web服务漏洞攻击防护界面

七
横向渗透防护能力

横向渗透目前是针对企业内网攻击的关键技术手段之一，而针对横向渗透的防护能力则是360高级威胁防护体系中的一项重要能力。勒索软件攻击团伙，在对企业发起攻击后，往往利用该技术扩大影响范围，获取更多设备的控制权，乃至控制整个企业网络。

在我们处置的企业被攻击案例中，几乎都可以见到横向渗透攻击的身影。为此360安全卫士推出了体系化的横向渗透防护方案，从攻击源头、攻击方法、攻击资源、技术素材等多维度入手，全方位地阻断横向渗透攻击。下面列举了其中部分防护能力：

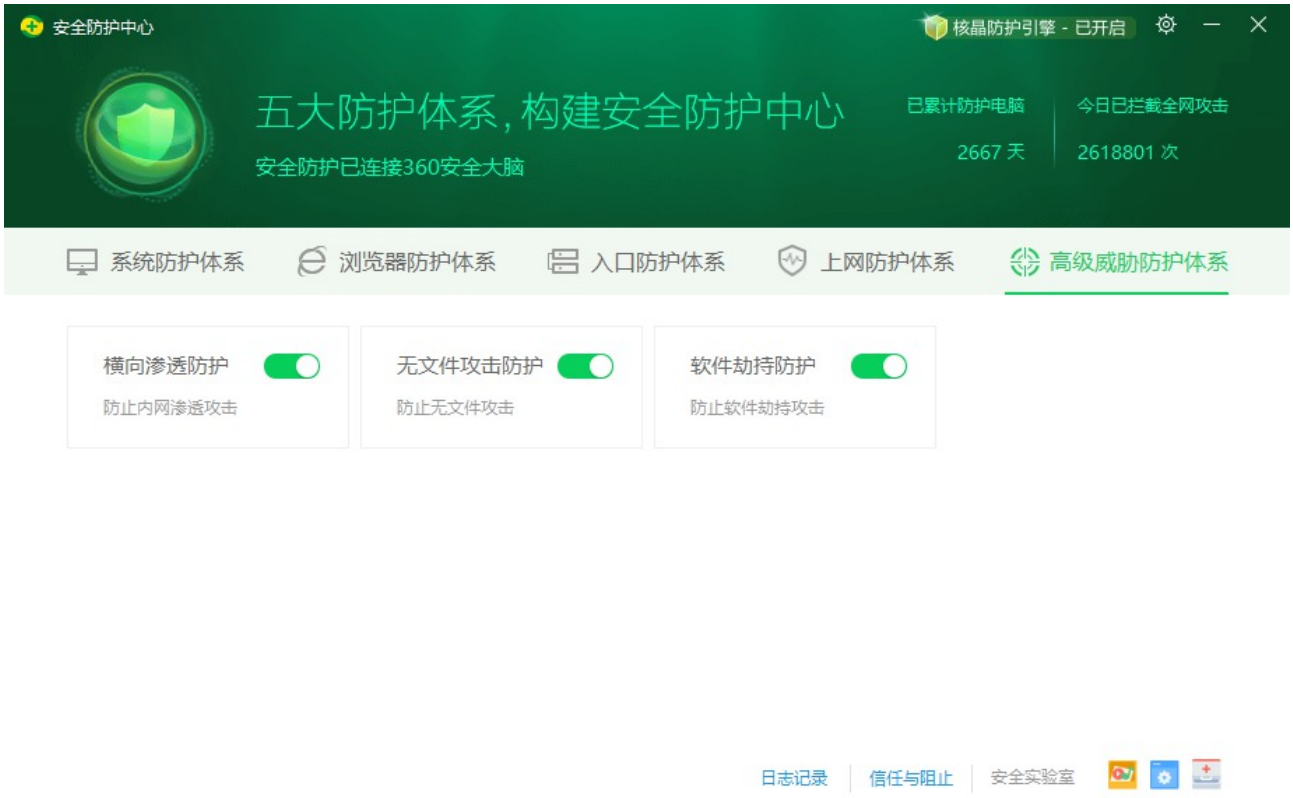
- 共享文件访问控制
- 远程WMI执行控制
- 远程计划任务控制
- 远程MMC控制
- 远程DCOM控制/远程RPC调用防护
- 远程服务创建控制
- 远程注册表操作控制
- 远程WINRM监控

●远程PSEXEC防护

●共享文件写入监控

●域环境下的组策略拦截

这些防护能力，结合对无文件攻击防护和LOLBAS（Living Off The Land Binaries and Scripts）防护能力，有效阻断了攻击者在企业内网的刺探和攻击扩散。



▲ 360安全卫士防护横向渗透防护模块

八
提权攻击防护

勒索软件执行过程中，为了提升其权限，尽可能多地加密系统中的文件，会尝试利用各种方法去提升程序的运行权限，针对这一攻击方式，360安全卫士对其进行了严格的行为限制。

▲ 360安全卫士提权攻击防护功能

九
挂马网站防护能力

针对包括勒索软件在内的各类木马病毒攻击，更早的防护往往能取得更好的效果。360安全卫士致力于在病毒木马攻击的早期就将其遏制，遏制传播渠道便是早期防御的一个重要部分。挂马网站是传播勒索软件的重要渠道之一，针对这一情况360安全智能体能第一时间监控并识别该网站的恶意行为并做出拦截。

+

钓鱼邮件附件防护

针对从邮箱中下载回来的附件，360安全智能体精准识别邮件附件中潜藏的病毒木马，替用户快速检测附件中是否存在问题。

▲ 360安全卫士拦截钓鱼邮件附件

附录 3

360解密大师

360解密大师

360解密大师是360终端安全产品提供的勒索软件综合解密工具，是目前全球范围内支持解密类型最多的一款解密工具。

2025年360解密大师依然继续对最新出现的勒索软件保持着持续响应，今年新增支持8款勒索病毒的解密，其中7款为全球独家解密。协助2271位用户，完成486万文件的解密，挽回损失超4700万元。

下图给出了360解密大师在2025年全年，成功解密被勒索软件感染的文件和机器数量的Top10。其中，解密量较大的有phobos和FreeFix，都是2025年新增支持解密的家族。

数据来源：解密大师统计数据

附录 4

360勒索软件搜索引擎

360勒索软件搜索引擎

该数据来源lesuobingdu.360.cn的使用统计。（由于WannaCry、AllCry、TeslaCrypt、Satan、GandCrab、WannaRen、Sodinokibi等几个家族在过去曾出现过大规模爆发，之前的搜索量较高，长期停留在推荐栏里，对结果有一定影响，故在统计中去除了这几个家族的数据。）

▲ 360勒索软件搜索页面

通过对2025年全年勒索软件搜索引擎热词与家族进行归集分析发现，搜索量靠前的关键词情况如下：

●roxaew、wxx、wxr、rx、wexor、weaxor

属于Weaxor勒索软件家族，该家族目前的主要传播方式为：利用各类软件漏洞利用方式进行投毒，通过powershell加载攻击载荷并注入系统进程多轮加载不同的漏洞驱动与安全软件进行内核对抗。部分版本会通过暴力破解登录数据库后植入Anydesk远控进行手动投毒。

●bixi、baxia

属于BeijngCrypt勒索软件家族，由于被加密文件后缀会被修改为beijing而成为关键词。该家族主要的传播方式为：通过暴力破解远程桌面口令与数据库弱口令成功后手动投毒。

●mkp、svh、wis、air

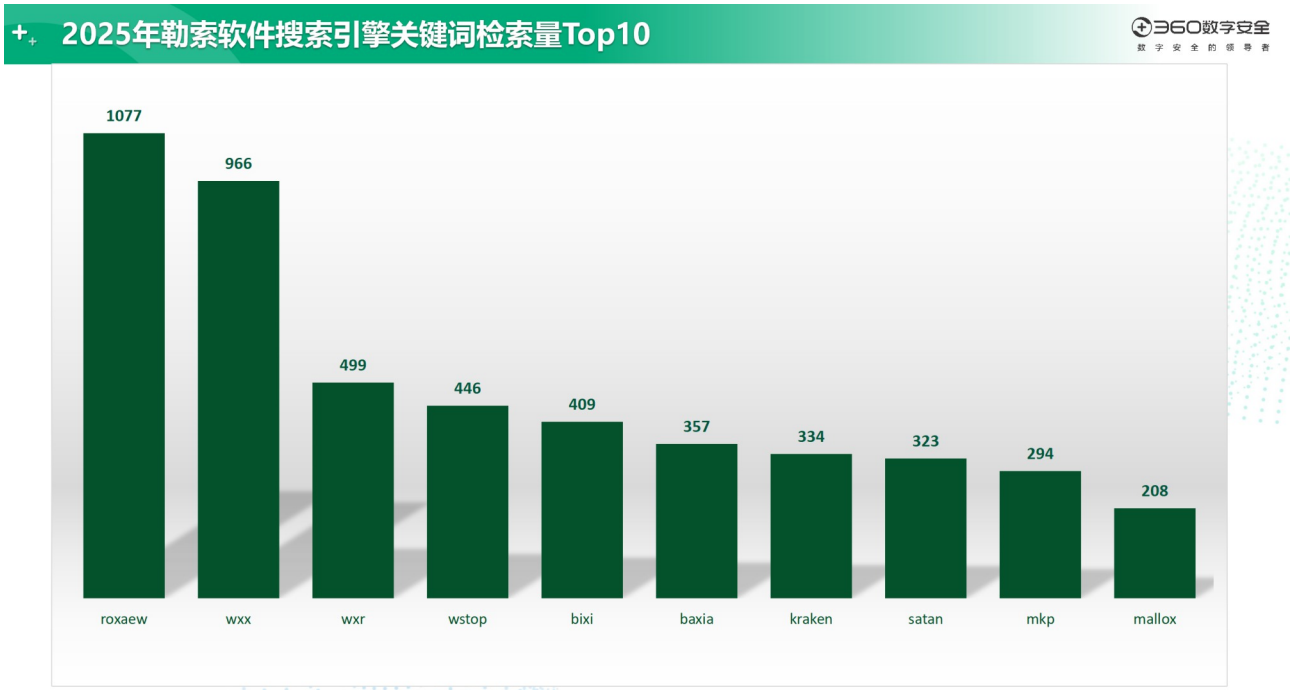
属于Makop勒索软件家族，由于被加密文件后缀会被修改为mkp而成为关键词。该家族主要的传播方式为：通过暴力破解远程桌面口令成功后手动投毒。同时存在加密共享目录的行为。

●peng、wman

属于Wmansvcs家族，高度模仿phobos家族并使用Rust语言编译，目前仅在国内传播。该家族的主要传播方式为：通过暴力破解远程桌面口令，成功后手动投毒。

●wstop、sstop

属于RNTC勒索软件家族，由于最初版本被加密文件后缀会被修改为rntc而成为关键词。该家族主要的传播方式为：通过暴力破解远程桌面口令成功后手动投毒。同时存在加密共享目录的行为。



数据来源：勒索软件搜索引擎

360勒索软件搜索引擎在2025年为用户提供了近4万次查询服务，对这近4万次关键词的搜索结果进行详尽分析后发现，与第一章勒索软件攻击形式的勒索家族分布相比，整体占比基本一致。

数据来源：勒索软件搜索引擎

RANSOMWARE
THREAT REARCH REPORT
2025

2025年
勒索软件流行态势报告

THE END

360数字安全 360安全大模型

360安全能力中心反病毒部

2026年1月