2021 年

勒索病毒流行态势报告

高级威胁研究分析中心 - 反病毒运营部

2022 年 1 月

前　　言

本次报告根据 2021 年 360 政企安全高级威胁研究分析中心反病毒部所监测、分析和处置的勒索病毒事件为基础，进行分析梳理与情况总结。内容以国内形势为基础，也加入了国际热点事件与形势的分析，旨在评估勒索病毒在 2021 年所展现出来的传播及演化态势，进而对勒索病毒在未来可能会产生的发展方向进行探究，以此帮助个人用户和企业管理员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，由一批常年在网络安全一线进行对抗防御的专家组成，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。

摘　　要

- 360 反勒索服务全年共接收并处理了超 4100 例勒索病毒攻击求助，其中超过 4000 例确认遭受勒索病毒攻击。受三款新兴勒索病毒家族影响，勒索攻击反馈在年末的 10、11、12 三个月呈现了较为明显的上涨态势。
- 国内流行勒索病毒家族以 phobos、Magniber、Stop 为主，这三大勒索病毒家族的受害者占比约为 37.3%。逐月分析流行勒索病毒各家族占比，则发现通过弱口令攻击部署病毒的传播量较为平稳，而通过其他传播方式投放的勒索病毒则传播量波动较大。
- 勒索病毒加密手段日渐趋同，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病毒将会越来越困难。
- 远程桌面依然是勒索病毒最主要的入侵方式，在所有入侵方式中占到近 6 成。
- 双重/多重勒索已成发展趋势，Conti、LockBit、Pysa 三大家族领头。重点攻击服务、加工制造、金融与贸易等行业。美国成为此类攻击的重灾区。
- 勒索病毒家族更迭不休，既有新增也有消亡。各国警方打击成为勒索病毒消亡的主要原因。
- 广东、江苏、山东三省遭勒索病毒攻击最多。桌面操作系统依然是受攻击的主要目标，但 NAS 等原本的小众设备也开始受到勒索病毒重视。加工制造、教育&科研、批发零售则成为国内最受勒索病毒“青睐”的目标行业。
- 泛欧盟地区成为勒索攻击的主要来源，保加利亚与伊朗紧随其后。勒索病毒联系邮箱超 8 成为匿名邮箱，难以溯源。
- 勒索病毒入侵手段日趋多样化，“七管齐下”给安全人员带来防御新考验。

目　　录

第一章 勒索病毒攻击形势

2021 年是错综复杂的一年，新冠疫情的全球蔓延加之不确定性进一步增加的国际环境，让整个社会的运行秩序发生了深刻改变。同时信息技术更加深入的触及到了生活的每个角落也让 2021 年层出不穷的勒索病毒攻击事件给我们带来的感知越发强烈：美国燃油管道公司被攻击、爱尔兰医疗系统被迫关闭等事件一次次挑动大众神经，勒索攻击问题也第一次被多位国家元首在国际峰会中提及并积极商讨应对之策。

2021 年，国内的勒索疫情也不容乐观，勒索攻击问题已经成为当前企业最关注网络安全风险之一。全年攻击事件不断，尤其第四季度，由于僵尸网络与多个热门漏洞利用的推动，造成勒索攻击量也大幅增长。

总体而言 2021 年的勒索病毒攻击事件数量、勒索病毒攻击引起的数据泄露问题都有显著增长，攻击带来的危害日益加深。根据 360 安全大脑统计，2021 年共处理反勒索服务求助案例 4100 余例，反馈案例中单个企业中，大量设备集中中招的情况增多，攻击影响扩大。

本章将对 2021 年全年，360 政企安全检测到的勒索病毒相关事件与数据进行分析，并给出解读。

一、 勒索病毒概况

2021 年全年，360 反勒索服平台、360 解密大师两个渠道，一共接收并处理了超 4100 位遭遇勒索病毒攻击的受害者求助，其中超 4000 位经核实确认为遭受了勒索病毒的攻击。

下图给出了在 2021 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，提交申请并确认感染勒索病毒的有效求助量情况。

数据来源：反勒索服务统计数据

其中第四季度反馈量上涨明显，主要是由三个勒索病毒家族引起的：

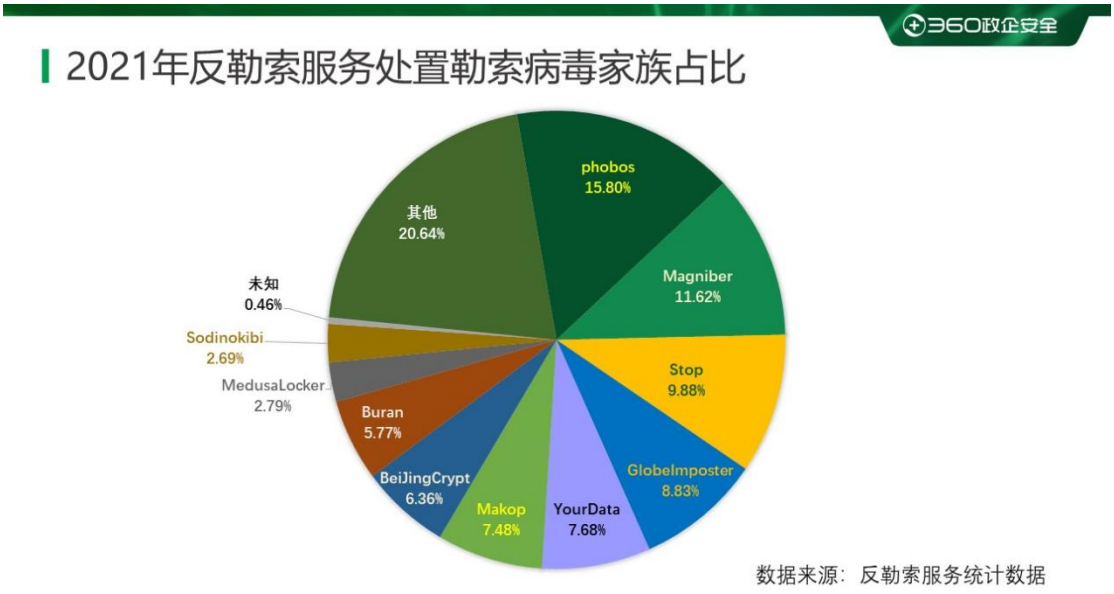
- 10 月，“匿隐”僵尸网络开始大量投递 YourData 勒索病毒；
- 11 月，使用挂马网站传播的 Magnier 家族在国内开始活跃传播；
- 12 月，新增了使用 Log4j2 漏洞进行传播的 TellYouThePass 家族勒索病毒。

以上三个月出现的三个勒索病毒家族均有较大的传播量，也在最终导致年末三个月的总体反馈量有较为明显的上涨。

(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 2021 年勒索病毒家族流行度占比分布图。

其中，PC 端 Windows 系统下 phobos、Magniber、Stop 这三大勒索病毒家族的受害者占比最多。TOP10 的勒索病毒家族中，仅 YourData 勒索病毒为今年新增家族，其它勒索病毒均在去年甚至以往数年里始终处于活跃状态。值得注意的是——通过破解软件/激活工具进行传播的 Stop 家族感染量达到历史新高，勒索病毒对个人用户的影响仍不容小觑。

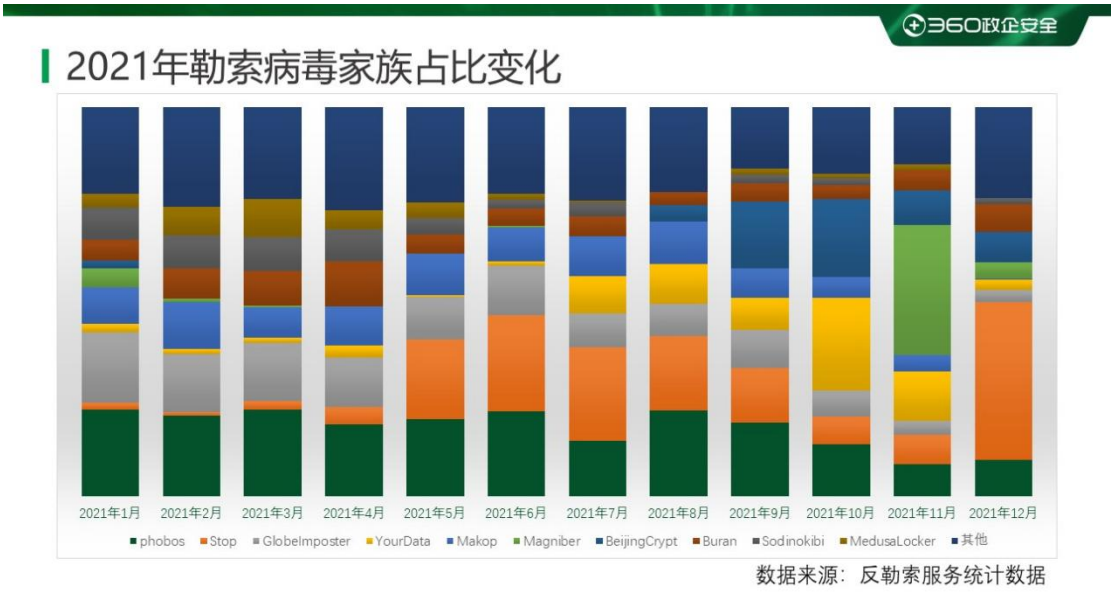


二)主流勒索病毒趋势

我们汇总了 2021 年的月度感染量 TOP10 勒索病毒家族数据，发现仅通过弱口令攻击进行传播的勒索病毒家族感染量相对平稳，不会出现较为明显的浮动——如：phobos、GlobeImposter 等；而通过其他渠道进行传播的勒索病毒家族则受传播渠道本身的不稳定性制约，导致感染量波动相对较大，例如：

- 利用破解软件或者激活工具进行传播的Stop勒索病毒家族，在5月之后出现快速增长，并在 10、11 月小幅回落后再次于 12 月出现一波新的快速上涨。

- 利用“匿影”僵尸网络进行传播的 YourData 勒索病毒家族在 10 月出现爆发式增长。
- 利用挂马网站进行传播的 Magniber 勒索病毒家族在 11 月出现爆发式增长。
- 利用 Log4j2 漏洞传播的 TellYouThePass 在 12 月出现快速增长（该勒索病毒的绝对感染量尚不足以进入下图中的 TOP10 榜单，故在图中未能呈现）。



数据来源：反勒索服务统计数据

三）加密方式分布

我们对 2021 年仍在流行且具有一定代表性的勒索病毒家族进行分析。统计了各家族的加密算法及相关信息。结论如下表：

家族	算法	加密	加密方案
LockBit2.0	RSA+AES	内置 RSA 公钥	基于文件尺寸
DarkSide	RSA+Salsa20	内置 RSA 公钥	传播者自定义
phobos	RSA+AES	内置 RSA 公钥	基于文件类型
GlobeImposter	RSA+AES	内置 RSA 公钥	基于文件尺寸
Makop	RSA+AES	内置 RSA 公钥	基于文件尺寸
BeijingCrypt	RSA+AES	内置 RSA 公钥	完整加密
Buran	RSA+AES	内置 RSA 公钥	基于文件尺寸
Sodinokibi	ECDH+Salsa20	内置 ECDH 公钥	基于文件尺寸
MedusaLocker	RSA+AES	内置 RSA 公钥	基于执行参数
YourData	RSA+AES	内置 RSA 公钥	基于文件尺寸
Magniber	RSA+AES	内置 RSA 公钥	完整加密
TellYouThePass	RSA+AES	内置 RSA 公钥	完整加密

汇总发现，虽然各个勒索病毒家族都在各自发展方向，有些甚至互相排挤，但多年的技术迭代已经让各家族病毒给出了一个相对“趋同”的技术方案。即：

- 加密算法均为非对称加密（用于加密密钥）结合对称加密（用于加密文件）的多层加密

方案。

- 初始密钥均采用内置公钥的方法，来兼顾加密强度和解密的灵活性。
- 加密方案则大多是基于文件尺寸来决定是否加密整个文件。也有一些 RaaS 的家族为了照顾传播者的针对性和便利性，提供了多重加密方案让攻击者自行决定。

以上这些共性可以看出，勒索病毒在长期对抗中，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病毒的难度将越来越大。

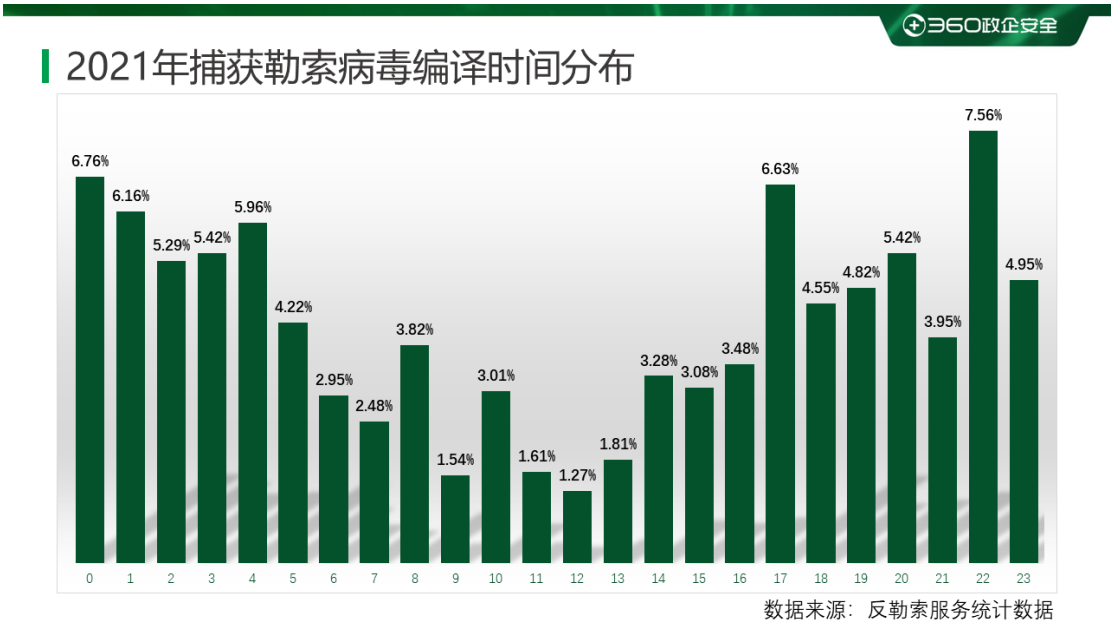
(四)编译时间看勒索病毒

我们针对 2021 年捕获到的勒索病毒样本进行分析，并提取了其编译时间。发现这些样本的编译时间有两个较为突出特点：

其一，部分样本的编译时间明显经过伪造。黑客会将编译时间戳设定为一个明显不合理的时间点或干脆直接清零。同时，此类样本在其它特征点上往往也具有混淆或人工清理过的痕迹。显然这些样本的作者并不希望分析人员通过任何的代码特征追溯出哪怕一点点关于他们的信息。

其二，通过对那些可以基本确认未经伪造的编译时间进行统计，我们发现这些样本的编译时间大多集中在每天的 17 时至次日 4 时。这么看起来，似乎病毒作者们都是名副其实的“夜猫子”。

但不可忽略的一点是：我们的统计时间是按照北京时间（UTC/GMT +8）进行展示，而实际上捕获的样本大多出自 UTC/GMT +3 或 UTC/GMT -5 这两个时区。所以按照时差推算，大部分的病毒作者不仅作息正常，甚至可以推测——编写这些病毒对于他们来说就是一份按时打卡上下班的“正常工作”。



数据来源：反勒索服务统计数据

(五)勒索赎金分析

不同类型的勒索病毒索要的赎金通常有较大区别。通过长期跟踪收集，我们将其划分为四个不同的区段：

区段一：1~1000 美元。这类型主要是“广撒网”式的攻击，受害者多为普通个人用户，被攻陷设备不一定具有很高价值，所以赎金通常设置的比较低。典型的家族有通过捆绑在破解软件中传播的 Stop，固定索要价值 490 美元或 980 美元的比特币，受害者如果在 72 小时内选择支付的话只需支付 450 美元。

Stop 勒索病毒典型勒索信息页面截图

区段二：1000 美元~10 万美元。这个区段的受害者多为中小型企业，攻击具有一定针对性，更多的因为远程桌面弱口令、数据库弱口令等主动攻击导致系统被攻陷。这类型受害者数据普遍更具价值，如企业的财务数据库等。故此类情况中，黑客更多的是会根据受害者的具体情况报价——如被加密设备量、被加密文件量、重要类型文件量、公司盈利状况、公司规模等作为参考。提供的支付方式也可能不仅限于比特币，还可能支持门罗币、达世币等其它虚拟货币。

中等价的位勒索，在国内的占比较高，比较流行的几个家族均在这个范围内，例如：

勒索病毒家族	价格范围	MDF 文件
phobos	5000 美元~15000 美元	单个文件:<4GB 4000 美元以内，>4GB 5000 美元以上
BeiJingCrypt	4000 美元~10000 美元	单个文件/累积<4GB 4000 美元以内，>4GB 不超过 10000 美元
GlobeImposter	1000 美元到上不封顶	无该项价格审核
CryLock	2000 美元-15000 美元	累计<4GB，2000USD,>4GB 根据情况索要

以上数据为针对部分家族的部分案例做的统计分析，可作为一个价格范围参考，但具体案件仍需根据具体情况来定。

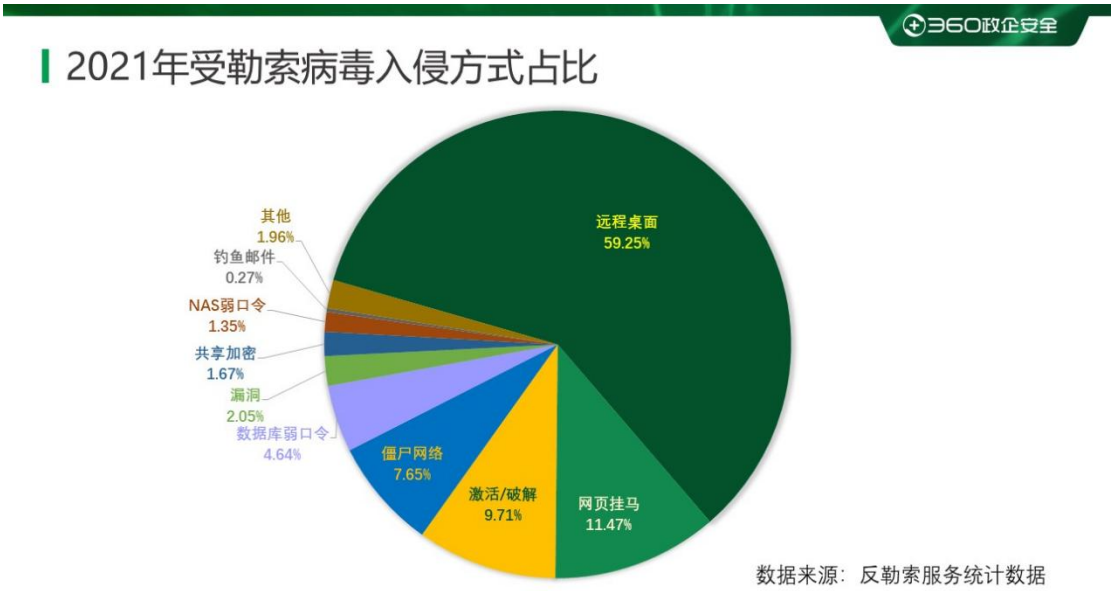
这个区段也有部分勒索病毒的攻击目标为个人。例如：索要赎金 4000 美元~7000 美元的 YourData，以及索要赎金 1000 美元~6000 美元的 Magniber。

区段三：10 万美元~1000 万美元。这类型勒索病毒主要针对中大型企业进行攻击，通常被攻击后的企业/组织通常存在数据泄露风险，这类型赎金价格在几十万美元到几百万美元之间。这区段的价位在双重勒索模式中占比较高。

区段四：1000 万美元以上（不封顶）。这类被攻击的企业不仅因为是大企业，有能力支付高额赎金，还因为被攻击设备量大、被窃取数据更具有勒索价值，勒索事件被公开直接会影响到企业声誉，所以会被所要价值上千万美元的比特币。例如：全球最大牛肉生厂商被迫向黑客支付 1100 万美元恢复生产、遭 Sodinokibi(REvil)供应链攻击的 Kaseya 被所要 7000 万美元以及 IT 咨询巨头埃森哲遭遇 Lockbit 勒索软件攻击被所要 3.2 亿美元等。

二、 勒索病毒传播方式

下图给出了 2021 年攻击者投递勒索病毒的各种方式的占比情况。根据统计可以看出，远程桌面入侵仍然是用户计算机被感染的最主要方式。此外，今年因为设置共享文件，导致被加密的案例有大幅度下降，而因访问挂马网站和下载破解软件或者激活工具导致中招的案例增多。对于这些攻击手段的具体描述，将在第三章 “勒索病毒攻击者分析”的第三节“攻击手段”中进行具体分析。



三、 多重勒索与数据泄露

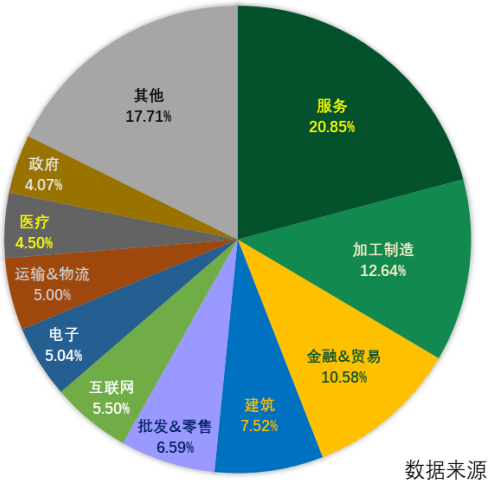
近年来，通过双重勒索或多重勒索模式获利的勒索病毒攻击团伙越来越多，勒索病毒所带来的数据泄露的风险也急剧增加。本章将通过@darktracer_int 提供的数据进行多维度分析，该数据仅反应未在第一时间缴纳赎金或拒缴纳赎金企业情况。（已经支付赎金的企业或个人，可能不会出现在这个清单中）。

(一)行业统计

从行业划分来看，服务业、加工制造业、金融与贸易分别占据了行业分布的前三位。这一现象可能与这些行业的性质有关：受影响的头部行业往往资金规模较大且业务对信息系统依赖程度较高，同时勒索病毒对企业声誉的影响也愈加明显。也正因如此，泄露关键数据对这些机构也会造成更大的威胁——进而让勒索的赎金和成功率均获得显著增加。

360政企安全

2021年受数据泄露影响行业分布

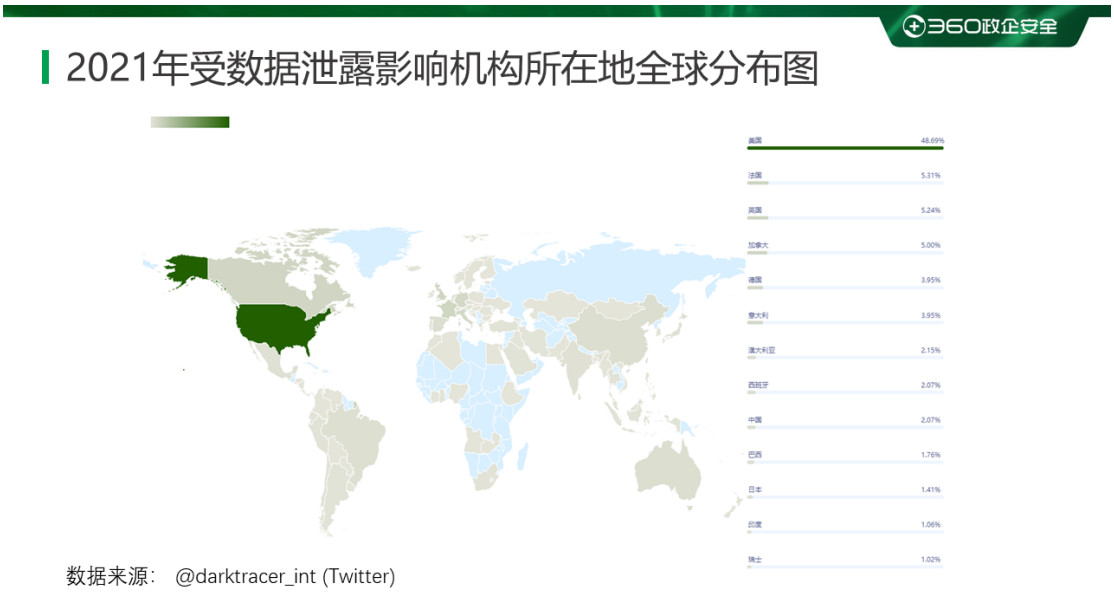


数据来源：@darktracer_int (Twitter)

（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，受影响最严重的是美国机构，占到总统计量的近一半。出现这一现象可能是由于被公开的企业多为有一定影响力的知名企业，而美国的机构无论从规模、资金量、影响力等维度都往往处于头部位置，这也势必会造成被勒索后曝光度的增加。攻击者无论是从更容易的获取赎金还是从能在业内提升知名度的角度触发，攻击大型美国机构都是一个不错的选择。

数据来源： @darktracer_int (Twitter)

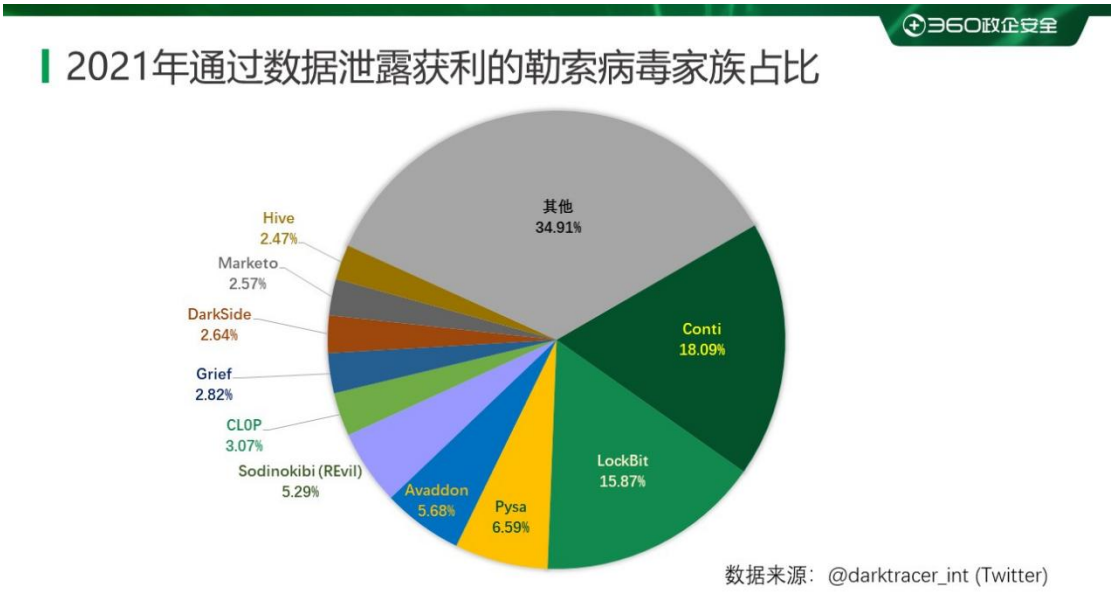


数据来源： @darktracer_int (Twitter)

（三）家族统计

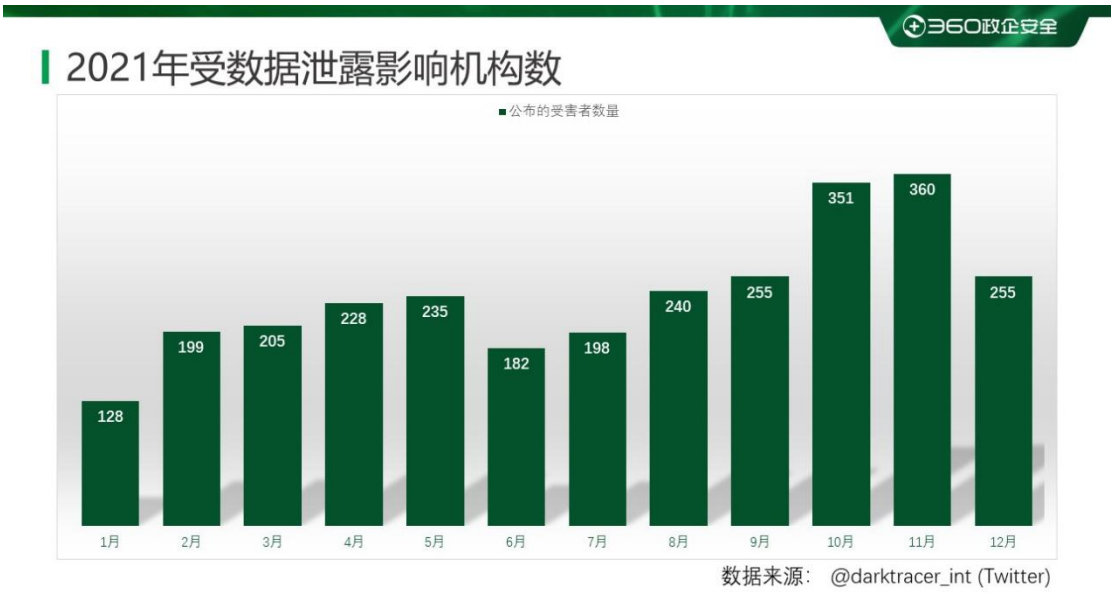
2021 年参与双重/多重勒索活动的一共有 53 个勒索病毒家族，进入 TOP10 的几个勒索病毒家族中，已有多个家族因不同原因停更，例如 Avaddon、Sodinokibi 等。而其中的 Marketo

则是一个数据泄露市场，它将勒索软件、网站泄露等非法途径获取到的数据进行出售。



(四)逐月统计

结合 360 反勒索服务接收到的感染反馈情况看，在 10 月、11 月不管是传统的勒索，还是双重/多重勒索，均有较大幅度的上升态势。



(五)数据泄露的负面影响

随着双重勒索逐渐成为主流勒索方式之一，数据泄露带来的负面影响也不断在扩大。双重勒索最早出现于 2019 年底，截止到 2021 年底已有超过 4200 个受害企业/组织数据有数据

泄露风险或已遭受数据泄露带来的危害。数据泄露不仅会给一个企业/组织造成声誉上的直接损伤，商业机密泄露、客户遭遇骚扰等威胁还可能给受害企业/组织造成二次危害。例如：

- **警方数据泄露，线人安全遭遇威胁**
  2021 年 4 月，Babuk 勒索软件运营团伙成功入侵华盛顿警方内部网络并窃取 250GB 数据，其中不仅包含对警察的“背景调查”、大量私人信息、调查报告、当地团伙文件以及行政文件等，还包含了警方的线人信息。警方线人信息一旦泄露，造成的后果不堪设想。不过是否要泄露线人信息也使 Babuk 内部出现矛盾，最后导致其发生内部分裂。

- **供应商数据泄露，客户遭遇二次勒索**
  全球第二大笔记型电脑研发涉及制造公司广达电脑遭遇 Sodinokibi(REvil)勒索病毒攻击，被索要 5000 万美元作为赎金。攻击者还表示若支付日期晚于既定日期，将需支付 1 亿美元赎金。此次攻击事件被窃取大量客户数据，目前尚不明确到底有多少客户数据被窃取，但其客户包括了苹果、戴尔、惠普 、亚马逊、思科、富士通、联想、LG 等大型公司，目前苹果的部分设计图纸已被该团伙公布到暗网中。
  在和广达电脑谈判时，广达电脑表示他们不关心客户和员工数据，允许黑客公布和出售所有数据。故此 Sodinokibi(REvil)随后转向与苹果谈判，想尝试通过威胁苹果——称若其不购回被窃取数据，便会将苹果最新产品设计数据在暗网公布。

- **计划生育协会遭遇攻击，患者面临敲诈勒索**
  洛杉矶计划生育协会（Planned Parenthood Log Angeles）被勒索病毒攻击，约 40 万患者信息遭到泄露。黑客在后续的勒索中，不仅向洛杉矶计划生育协会索要赎金，同时也将魔爪伸向了个人信息遭泄露的 40 万名患者。其中包括堕胎和其它私密手术信息，个别患者可能将面临敲诈勒索。

四、 勒索病毒家族更替

(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病毒出现。以下是传统勒索病毒(仅通过加密文件对受害者进行勒索)的部分记录信息：

月份	新增传统勒索病毒
2021 年 1 月	Vovalex、YourData、Summon、HelpYou、Encrp、Judge、Epsilon、WormLocker、Namaste
2021 年 2 月	DaddyHack、Snoopdoog、DarkWorld、HDLocker
2021 年 3 月	FancyBear、Hog、DearCry、Sarbloh、BadGopher、RunExeMemory、Phoenix CryptoLocker
2021 年 4 月	QLocker、WhiteBlackGroup、Jormungand、Cring\GEHENNALocker、Nocry、CryBaby
2021 年 5 月	Motocos、Ducky、Archangel、Galaxy、Henry、Toxin
2021 年 6 月	Spyro、APISWiper、ChupaCabra、Vice Society、Findnotfile、 Red Epsilon
2021 年 7 月	nohope、GoodMorning、MiniWorld、FancyLeaks、LegionLocker、LockFile
2021 年 8 月	Malki、GetYourFilesBack、Salma、AllDataStolen、GoodMorning
2021 年 9 月	Penta
2021 年 10 月	DeepBlueMagic、Cring、BronyaHaxxor、Mallox
2021 年 11 月	Doyuk2、HarpoonLocker、Rozbeh、BlackCocaine、CrytOy、Flowey、AvGhost
2021 年 12 月	CarckVirus、Miner、Razer、Youneedtopay

针对以上新增勒索病毒家族，我们对其中几个典型家族进行具体的说明：

- YourData

  根据360安全大脑对YourData家族的长期跟踪，该家族的传播目前分为以下几个阶段：

  1. 2021年1月
     首次发现该家族在国内采用暴力破解远程桌面口令成功后手动投毒，但并不具体针对任何特定的攻击目标。

  2. 2021年3月
     该家族开始针对性的投放勒索软件，使用带有受害者公司名的字符串作为后缀，重命名被加密文件。采用暴力破解远程桌面口令成功后手动投毒，并为每个受害者生成唯一的谈判页面。

  3. 2021年4月
     该家族针对使用某系列软件的公司进行攻击，并用该软件特征名作为后缀重命名被加密文件。仍采用暴力破解远程桌面口令成功后手动投毒。

  4. 2021年7月
     该家族开始通过“匿影”僵尸网络进行传播，不再具体针对性，但是传播量有大幅度提升，并在10月出现较大面积的感染。

- HelpYou

  1月底出现的一款勒索病毒，不仅仅是通过传统的远程桌面弱口令暴力破解后手动投毒，还会利用通过获取到用户数据库口令后通过向受害者机器新增账户登录后手动投毒。单个机器要价0.1个比特币，按当时汇率换算需要高达3万3千多人民币才能购买到解密器。

- QLocker

  2021年4月19日，黑客利用CVE-2021-28799(硬编码凭证漏洞)对QNAP发起勒索攻击，使用7z压缩加密文件。该团伙利用该手法在短短一周获利26万美元。

- LockFile

  该家族首次发现是在2021年7月20日，当时其攻击了美国一家金融机构。在2021年8月检测到该家族利用Exchange服务器的ProxyShell漏洞入侵企业内部网络，再利用PetitPotam漏洞控制AD域名服务器，然后部署勒索病毒。该勒索病毒的勒索提示信息与CryLock勒索病毒家族的高度相似，其赎金谈判页面与LockBit勒索病毒家族高度相似。

- Mallox

  Mallox勒索病毒家族利用SQLGlobeImposter渠道进行传播，该渠道还曾被GlobeImposter勒索病毒长期使用。

(二)每月新增双重/多重勒索情况

统计发现，2021 年每月都有出现新的勒索软件加入到双重/多重勒索模式的行列。全年总共新增 40 多个双重/多重勒索病毒家族。

月份	新增双重/多重勒索
2021 年 1 月	Babuk、Povlsomware
2021 年 2 月	AstroTeam
2021 年 3 月	Phonenix CryptoLocker、LV、Prometheus
2021 年 4 月	Marketo、Noname、XING LOCKER
2021 年 5 月	N3TtwOrm、GoNNaCry、Grief、Vice Society
2021 年 6 月	Hive、ElonMusKnow、PayloadBin、AvosLocker
2021 年 7 月	BlackMatter、LockBit2.0、Haron、Hotarus、LOCKDATA、Quantum
2021 年 8 月	Karma、MBC
2021 年 9 月	Groove、Colossus、BlackByte、Bonaci Group、CoomingProject、Darkrypt
2021 年 10 月	MacwLocker、yanluowang、Spook、Haron (Midas)、Moses Staff
2021 年 11 月	54BB47H (Sabbath)、Entropy、ROOK、RobinHood、Snatch
2021 年 12 月	Bl@cktOr、Karakurt

针对以上新增双重/多重勒索病毒家族，我们对其中几个典型家族进行具体的说明：

- **DarkSide**

  在其袭击美国最大的燃料管道运营商之一的 Colonial Pipeline 后，没多久就关停了所有的基础设施，并销声匿迹。7 月发现一新型勒索软件 BlackMatter(由 DarkSide 重命名而来)开始在网络犯罪论坛开始发布各种广告招募合作伙伴，并声称同时拥有 REvil 和 DarkSide 的最佳功能，该团伙在攻击受害者的同时，还积极的从其他攻击者那里购买网络访问权限以发起新的勒索攻击。该家族曾在网络犯罪论坛发布消息称，其主要目标是那些盈利超过 1 亿美元，网络中存在 500-15000 台设备的公司。

- **MBC**

  8 月份新增的 MBC 的勒索软件在其数据泄露网站宣布，他们很快会在其网站发布针对伊朗伊斯兰共和国铁路系统的攻击事件。从该勒索软件团队创建的 Telegram 群消息显示，该团队来自伊朗，并威胁政府之后还会发动更多的攻击。

- **Marketo**

  这是一款自 2021 年 4 月搭建的数据泄露市场，将通过将勒索软件、网站漏洞等非法途径获取到的数据进行出售。该团伙还会通过电子邮件将受害者部分数据发送给其竞争对手，给受害者施加压力的同时，诱惑其竞争对手购买。截止 2021 年 8 月 28 日，从该数据销售网站看，已成功窃取至少 73 个组织/企业数据，其包括日本富士通、德国 Puma、法国 GigaTribe 等大型企业。

(三)每月消失勒索病毒情况

每月也有一些勒索病毒的消失，有部分勒索病毒家族是悄无声息的消失，但有部分勒索病毒家族的消失却引起了广泛的关注，例如：内部有人员被执法部门抓捕、重命名以重塑品牌、正式宣布停更等。以下表格仅记录因以上情况消失的勒索病毒家族。

月份	消失勒索
2021 年 1 月	NetWalker
2021 年 2 月	Foinx、Egregor
2021 年 3 月	El_Cometa (SynACK)、Mount Locker
2021 年 4 月	Ziggy
2021 年 5 月	Babuk、DarkSide、DoppelPaymer
2021 年 6 月	Avaddon
2021 年 7 月	Prometheus
2021 年 8 月	Payload.bin
2021 年 9 月	-
2021 年 10 月	Sodinokibi
2021 年 11 月	-
2021 年 12 月	-

- 1 月

  2021 年 1 月 27 日，美国和保加利亚的执法机构已查封了与 NetWalker 勒索软件运营方相关的暗网站点，并在该站点挂出查封通知。同时抓捕了一名涉嫌通过传播 NetWalker 勒索盈利超 2700 万美元的加拿大人。

- 2 月

  2021 年 2 月 16 日，法国警方与乌克兰警方联合在乌克兰抓捕了 Egregor 的一名成员。2020 年 9 月至 2021 年 2 月，该家族已成功感染 206 个目标，成员被捕后该组织的数据泄露网站已无法访问。

- 4 月

  2021 年 4 月 6 日 Ziggy 宣布不再从事勒索行业，并已退还受害者赎金以及文件。

- 5 月

  - BaBuk 因攻击华盛顿警方后内部出现分裂，随后宣布将公开勒索软件源码，并转为数据盗窃敲诈勒索。同时还宣布将搭建数据泄露售卖网站，所有有数据需要售卖的网络犯罪份子均可通过该网站售卖数据。

  - 2021 年 5 月 7 日，美国最大的燃油管道商 Colonial Pipeline 遭遇 DarkSide 勒索病毒攻击，不久 DarkSide 便遭到美国和俄罗斯政府的打击，其基础设备和数据泄露网站已无法访问。

  - 从 5 月 7 日 DarkSide 攻击 Colonial Pipeline 后，DoppelPaymer 数据泄露站点虽仍然存在，但没有在更新过受害者信息，该团伙在 5 月 17 日新编译出 Grief，试图重命名来重塑品牌。

- 6 月

  本月采用多重勒索的 Avaddon 冒充 FBI 给 BleepingComputer 发送密钥文件，经检验该

密钥可用。跟踪发现该团伙之前不仅向他们的受害者施压，要求他们快速付款，还接受用户报价且未做出任何反击。目前该团伙已关闭该项目。

- **10 月**

  2021 年 9 月才宣布回归的 Sodinokibi(REvil) 遭遇双重打击——不仅被警方通过特殊渠道获取到了之前用于解密的全部密钥，还在本月遭遇了未知来源的入侵。其支付网站以及数据泄露网站遭遇劫持，被迫再次关闭其基础设备。目前最新受害者已不能通过勒索提示信息中留下的网址联系上黑客。

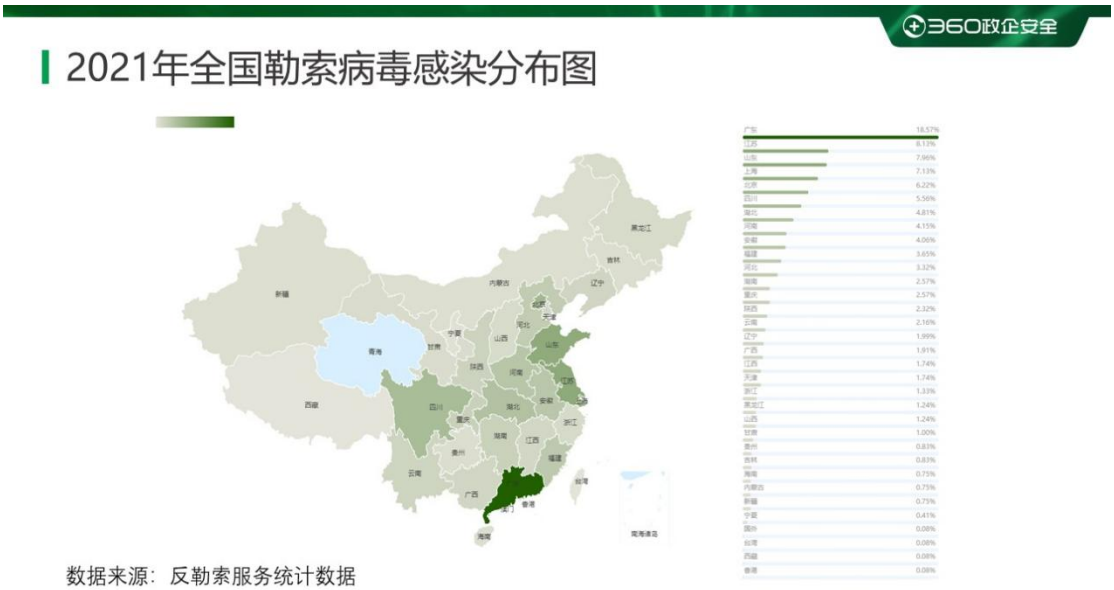
第二章 勒索病毒受害者分析

基于反勒索服务数据中求助用户所提供的信息，我们对 2021 年全年遭受勒索病毒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病毒家族影响，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 2021 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。

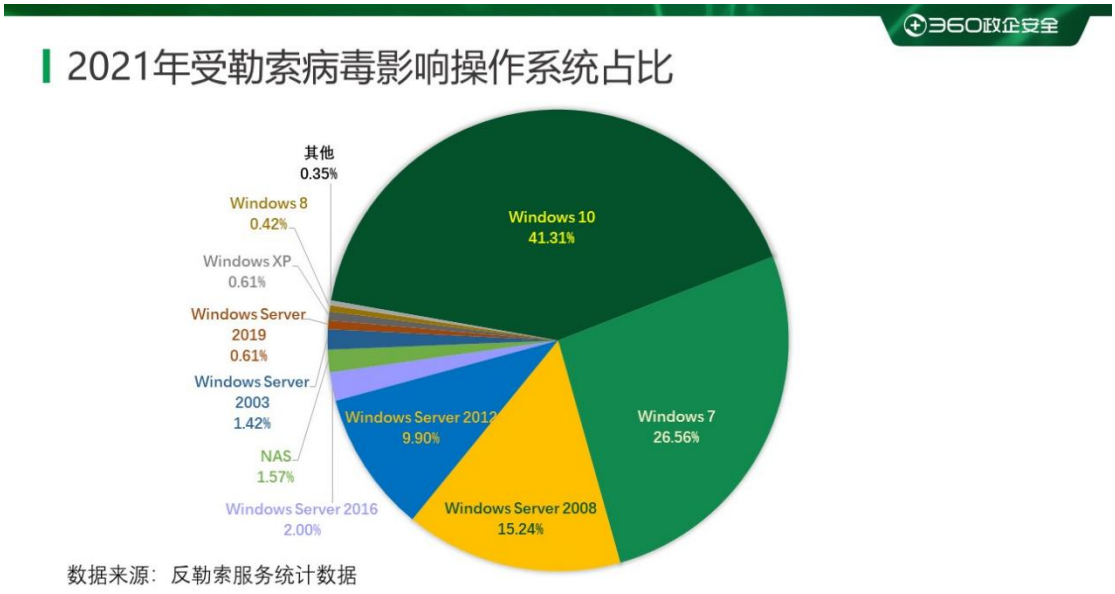
数据来源：反勒索服务统计数据



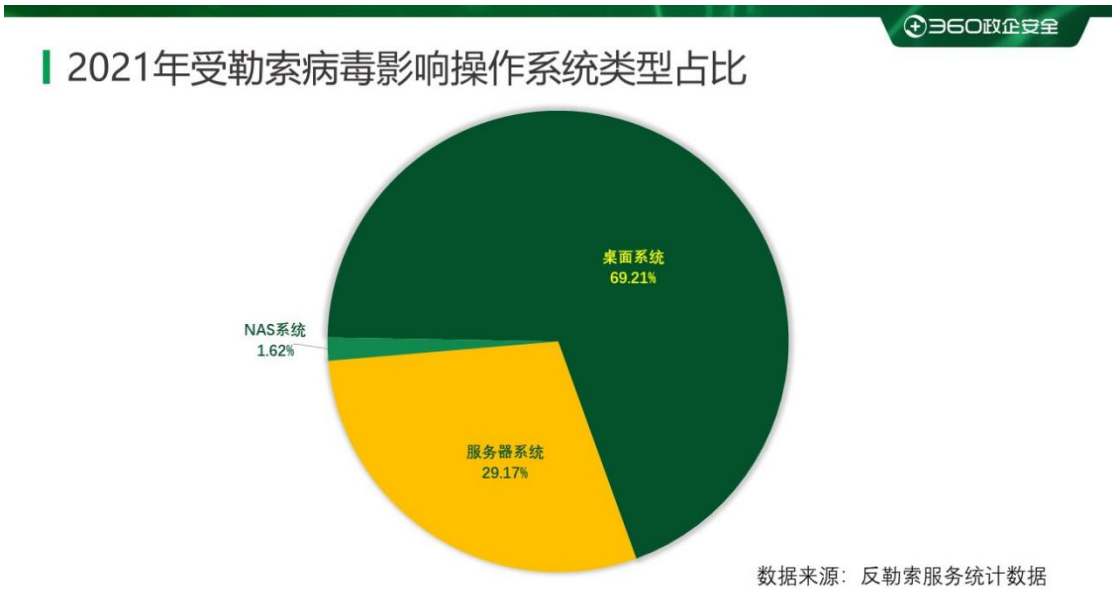
数据来源：反勒索服务统计数据

二、 受攻击系统分布

对 2021 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，整体依然是使用更广泛的系统，受攻击也更多。

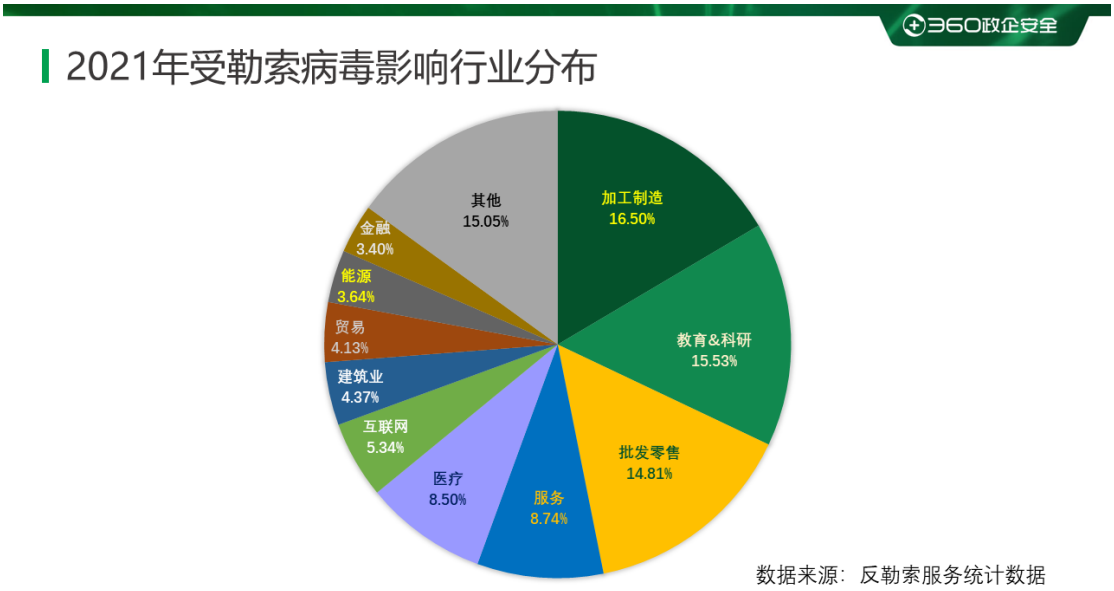


而操作系统类型而言，依然是桌面系统占据将近 7 成，服务器系统则不到 3 成。而今年较为特别的是在类型中出现了 NAS 这一特殊设备类型占到了 1.6%左右。虽然占比和绝对数量都不算高，但因其专用于数据存储的特殊功能，也成为了一个不容忽视的平台。



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，发现加工制造、教育&科研、批发零售分列受影响最为严重的前三类行业。排名靠前的行业除了机构规模和计算机设备规模拥有相对较大的数量基数之外，还有一个相对共性的特征——对网络安全的维护及管理重视程度相对不高，漏洞修补及软件更新速度、频度都有待提高。这也是造成受勒索病毒影响较为严重的主要原因之一。

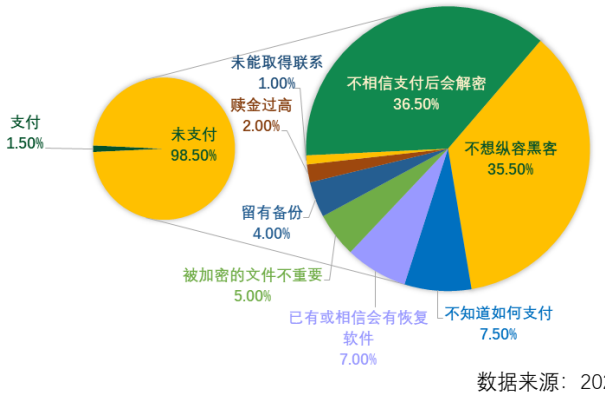


数据来源：反勒索服务统计数据

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。

受害者拒绝支付赎金的理由



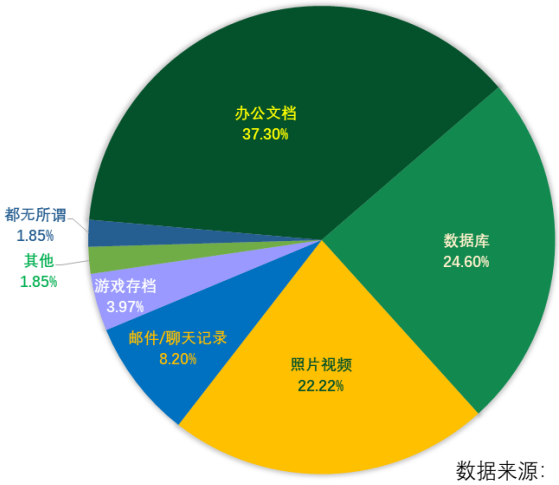
数据来源：2021年反勒索问卷统计数据

五、 对受害者影响最大的文件类型

根据问卷调查数据显示，对勒索病毒受害者而言，最为重要的文件类型分别是办公文档、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。

受害者认为最重要文件类型



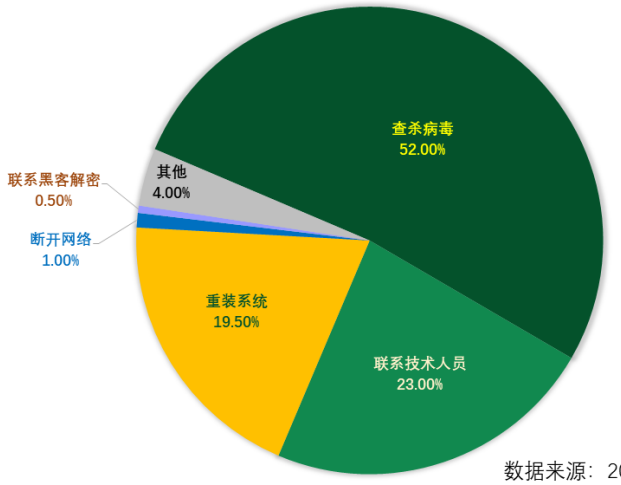
数据来源：2021年反勒索问卷统计数据

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，我们发现查杀病毒、联系技术人员属于较为常见的“本能反应”。

而重装系统的占比也相对较高，在我们对受害用户的协助处理中也印证了这一点。这一习惯其实对于勒索病毒这一特殊的病毒类型而言作用微乎其微，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断网而非重装系统的处理方式，方便技术人员的后续分析。

受害者遭受攻击后的应对方法



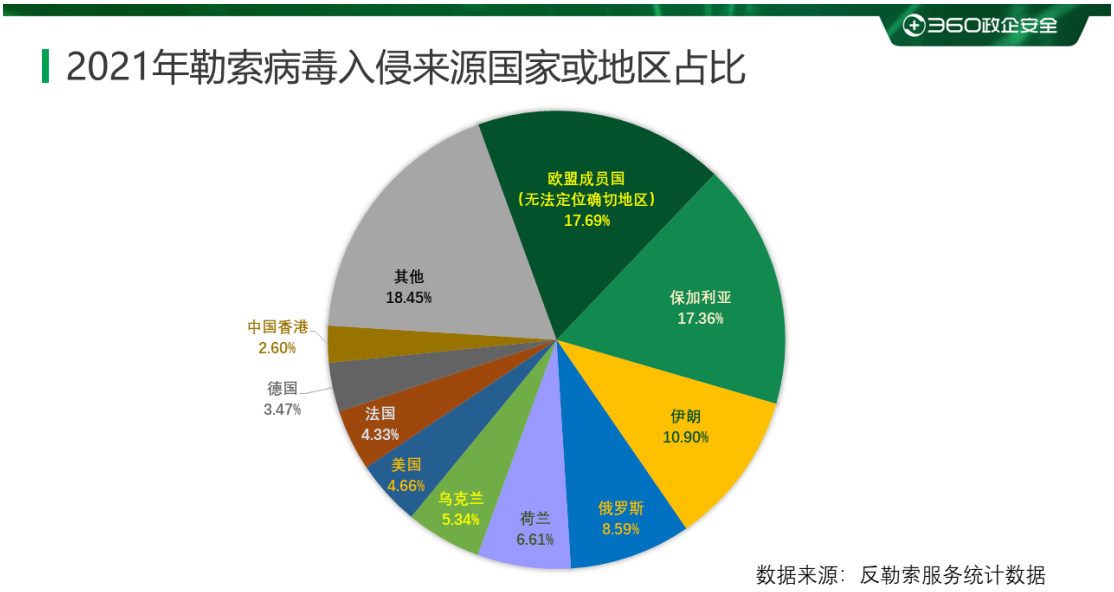
数据来源：2021年反勒索问卷统计数据

第三章 勒索病毒攻击者分析

2021 年的数据分析显示，目前流行的勒索病毒家族几乎都是采用内嵌密钥以及作为攻击载荷直接运行，使用 C&C 服务器的情况已经非常少见；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，部分情况下还会使用到洋葱网络聊天室以及 Telegram 等匿名聊天工具。黑客攻击的主要手段是对设备直接进行入侵或横向移动入侵，这其中远程桌面弱口令攻击是最常见攻击手段。

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，我们发现勒索病毒的主要入口来源于远程桌面的弱口令入侵。而此类攻击的来源 IP 进一步分析发现，其归属最多的是来自泛欧盟地区，其次则是保加利亚和伊朗。



数据来源：反勒索服务统计数据

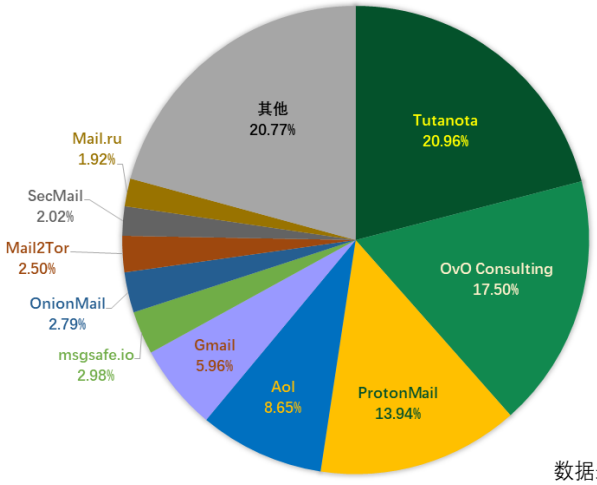
二、 勒索联系邮箱的供应商分布

目前主流的联系方式有两种，第一种是通过黑客提供的聊天室进行一对一对话，另外一种就是通过黑客提供的邮箱进行联系，其余有一些较为小众的联系方式，如例如使用 telegram 等即时聊天工具沟通。

通过对 2021 年收集到的黑客邮箱进行数据分析，我们发现勒索病毒作者更偏爱 Tutanota 、vO Consulting、ProtonMail 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。

此外，针对 TOP10 邮件服务商提供的邮箱属性进行研究发现，匿名邮箱在所有使用到的邮箱中占到了总量的 81.55%。

2021年勒索病毒联系邮箱供应商占比



数据来源：反勒索服务统计数据

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。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。

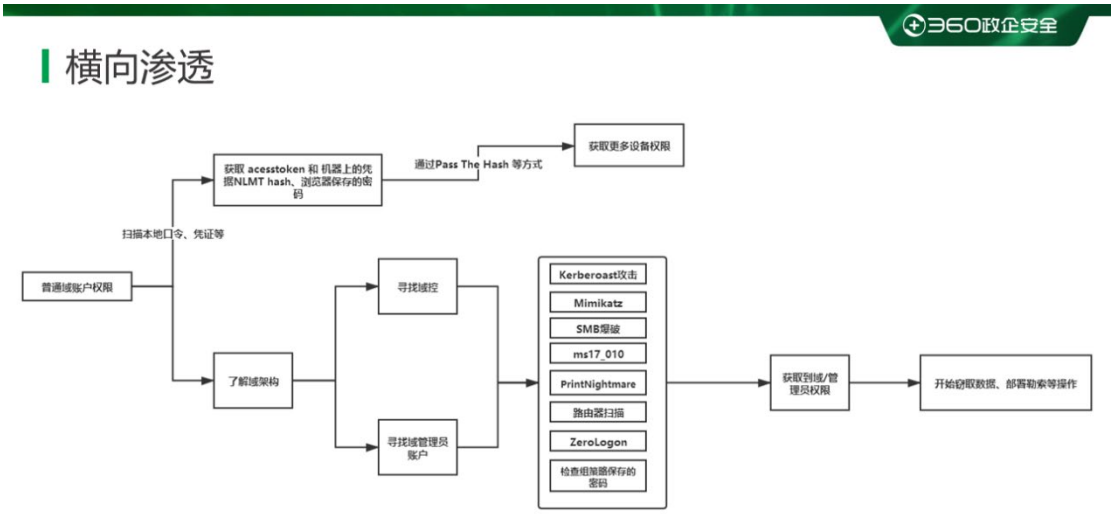
计算机中涉及到弱口令暴破攻击的暴露面，主要包括远程桌面弱口令、SMB 弱口令、RPC 远程过程调用、数据库管理系统弱口令(例如 MySQL、SQL Server、Oracle 等)、Tomcat 弱口令、phpMyAdmin 弱口令、VNC 弱口令、FTP 弱口令等。除了常见的计算机弱口令攻击，针对 NAS 设备这类家用网络设备的弱口令攻击近年来也成增长态势，比如 eChOraix 勒索软件就是通过 NAS 设备的弱口令进行传播并在成功攻入设备后加密其中存储的数据的。

今年国内排名前 10 的勒索病毒家族中有 8 个家族均涉及到弱口令攻击传播，其中 5 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

针对企业的勒索病毒攻击，是企业当前最为担忧的一类安全问题，此类攻击也向攻击者贡献了绝大部分的赎金收入。针对企业的勒索病毒攻击，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,拿下域控往往就意味着拿下了整个企业的设备管理权。其次还包括安全软件控制台、终端管理软件控制中心、IT 管理软件等。

2021 年 8 月 5 日，Conti 网络犯罪团伙因内部分赃不均导致其下属组织将其内部资料以及工具公开，其中部分已被上传至暗网论坛。在研究泄露的攻击教程文档时，我们发现他们采用的攻击手法并不算新颖：其会通过扫描本地的口令、凭证等获取更多设备的权限。而对于黑客而言，最重要的是通过该设备去了解当前设备所在域的整体架构，并尽可能去尝试攻击 IT 部门的相关设备（这样更有可能拿到域管理员权限或是域控设备）。该攻击阶段，采用到了多个公开的漏洞，例如“永恒之蓝”、ZeroLogon、PrintNightmare 等。而在成功获取到域控/域管理员权限后，攻击者就可以通过组策略向域内的所有设备进行下发恶意程序、窃取数据、部署勒索等一系列操作。



(三)利用系统与软件漏洞攻击

利用系统漏洞或应用软件漏洞进行攻击，长期以来都是安全领域的热点话题——在 APT 类攻击中这一点尤为常见。而在近年来的勒索病毒投递中，也经常能看到漏洞的利用。以下表格总结了今年勒索病毒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 ProxyShelll 漏洞、PrintNightmare 漏洞和 Log4j21 漏洞等。

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-2020-1472	NetLgon 远程协议攻击	ZeroLogon 漏洞
CVE-2021-40444	针对 IE 浏览器	IE 浏览器漏洞
CVE-2021-26411		
CVE-2021-44228	针对 Apache Log4j2 组件	Log4j2 漏洞、Log4jShell

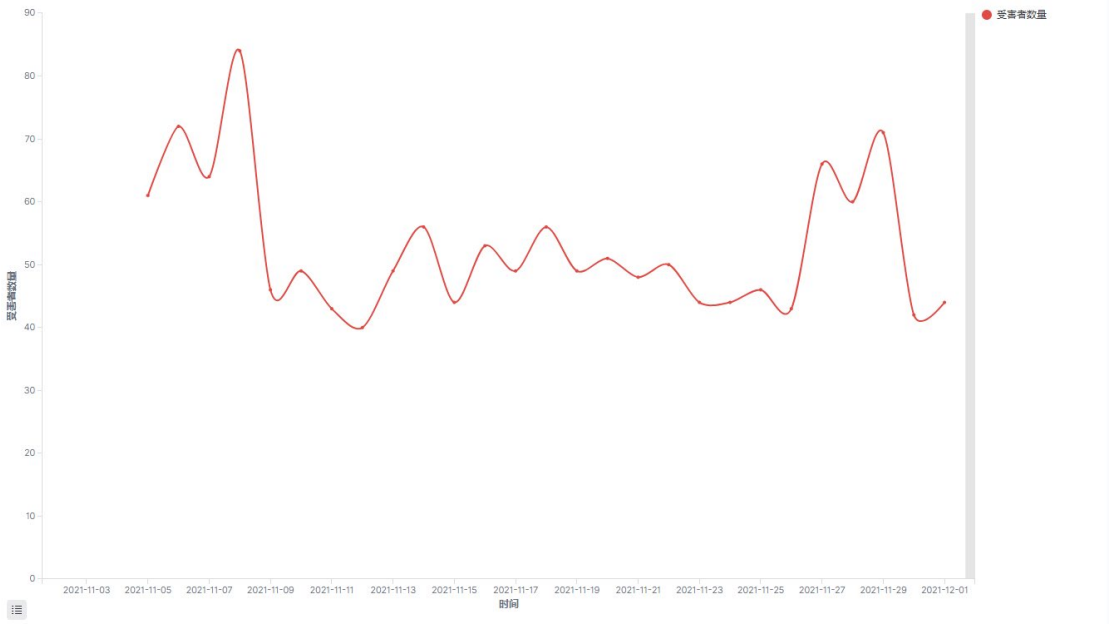
此外还有不少勒索病毒通过已有的漏洞利用工具进行漏洞检测/勒索传播，以下表格是今年被监控到勒索病毒使用过的漏洞利用工具。从统计看，RIG EK 和 Sundoen EK 最受黑客欢迎。

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	GandCrab、Locky、Hermes、Seon、Spora、CryptoShield、CryptoMix、Cerber
Spelevo EK	Maze
Fallout EK	Maze、GandCrab
Neutrino EK	Cerber
Jexboss	SamSam
永恒之蓝	Satan、TellYouthePass、WannaCry
Magnitude EK	Magniber
RadioEK	Nemty

(四)网站挂马攻击

网站挂马攻击作为常见攻击手段，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。对用户设备的攻击方式也包括：针对访问者设备中存在的漏洞进行攻击和通过诱骗方式诱导用户主动下载执行病毒木马。

360 安全大脑监控数据显示，自今年 9 月开始便有黑客团伙投放带有 CVE-2021-26411 漏洞利用代码的广告；而到了 11 月 5 日，攻击者则开始同时投放带有 CVE-2021-40444 漏洞利用代码的广告，并一同下发 Magniber 勒索病毒。当访问带有此类广告弹窗的网站时（站点多为色情、游戏相关内容），即使用户未点击广告也会自动使用新标签页打开页面上的广告，从而执行漏洞利用代码。

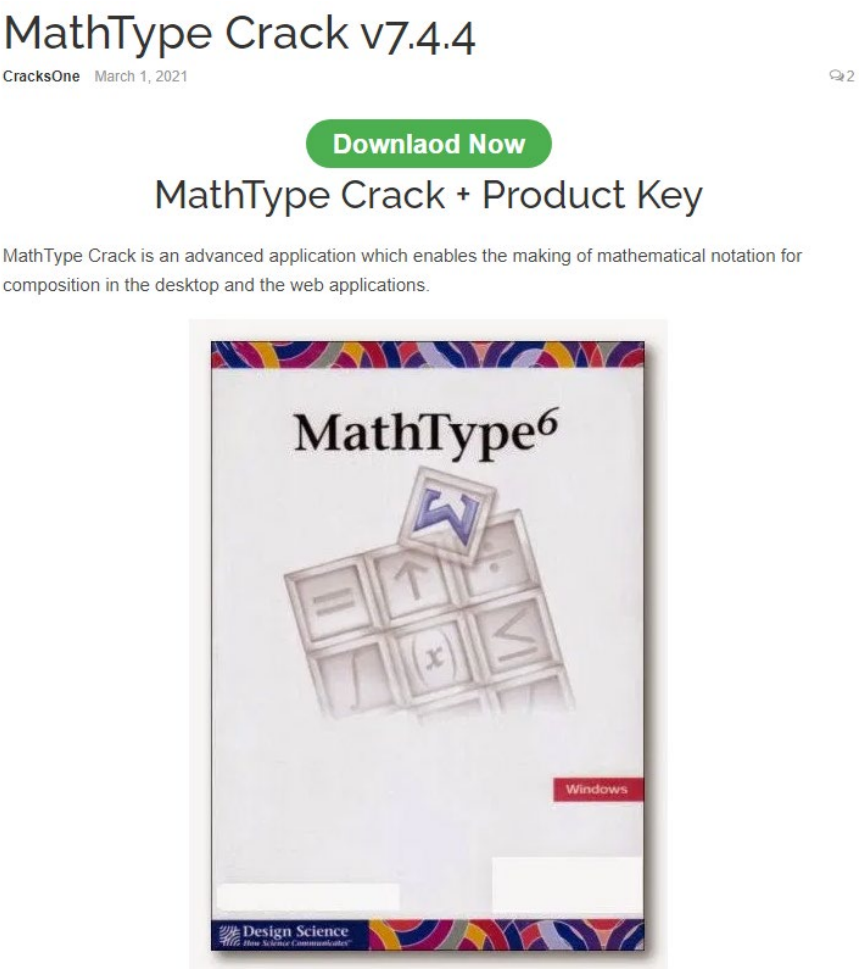


11 月 5 日以来受广告弹窗挂马攻击影响的用户量

(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病毒。于是它也成为国内个人用户感染勒索病毒的主要渠道之一。

比如 Stop 勒索病毒家族。该家族最早出现在 2018 年 8 月份，其传播渠道主要通过在破解软件网站上传激活工具或者破解软件来诱惑用户下载运行，且大部分网站为国外网站。传播至今该家族已有 300 多个变种。

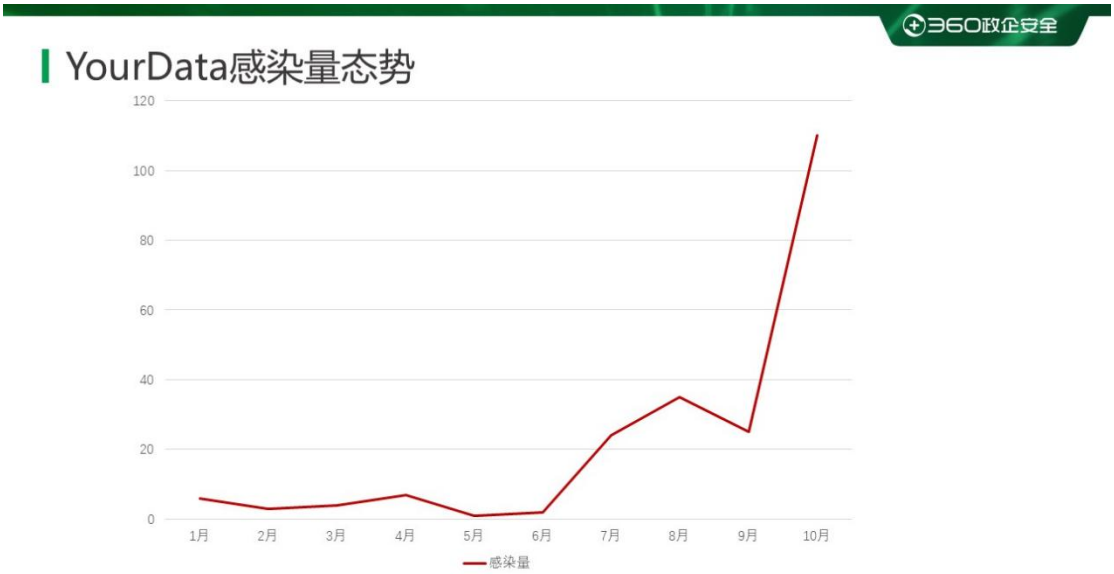


伪装成破解版软件的勒索病毒下载页面

(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。

国内流行僵尸网络“匿影”便是其中一只。它通过控制的数十万客户端发起扫描攻击、推广软件、下发病毒木马。曾有攻击者在 2020 年 4 月利用该僵尸网络投放 WannaRen 和 CryptoJoker 勒索病毒。而根据今年监控到的数据，该网络在 7 月又被开始用于投放 YourData 勒索病毒家族，最终致使 YourData 家族传播量在今年 10 月出现了一波大幅度的上涨。

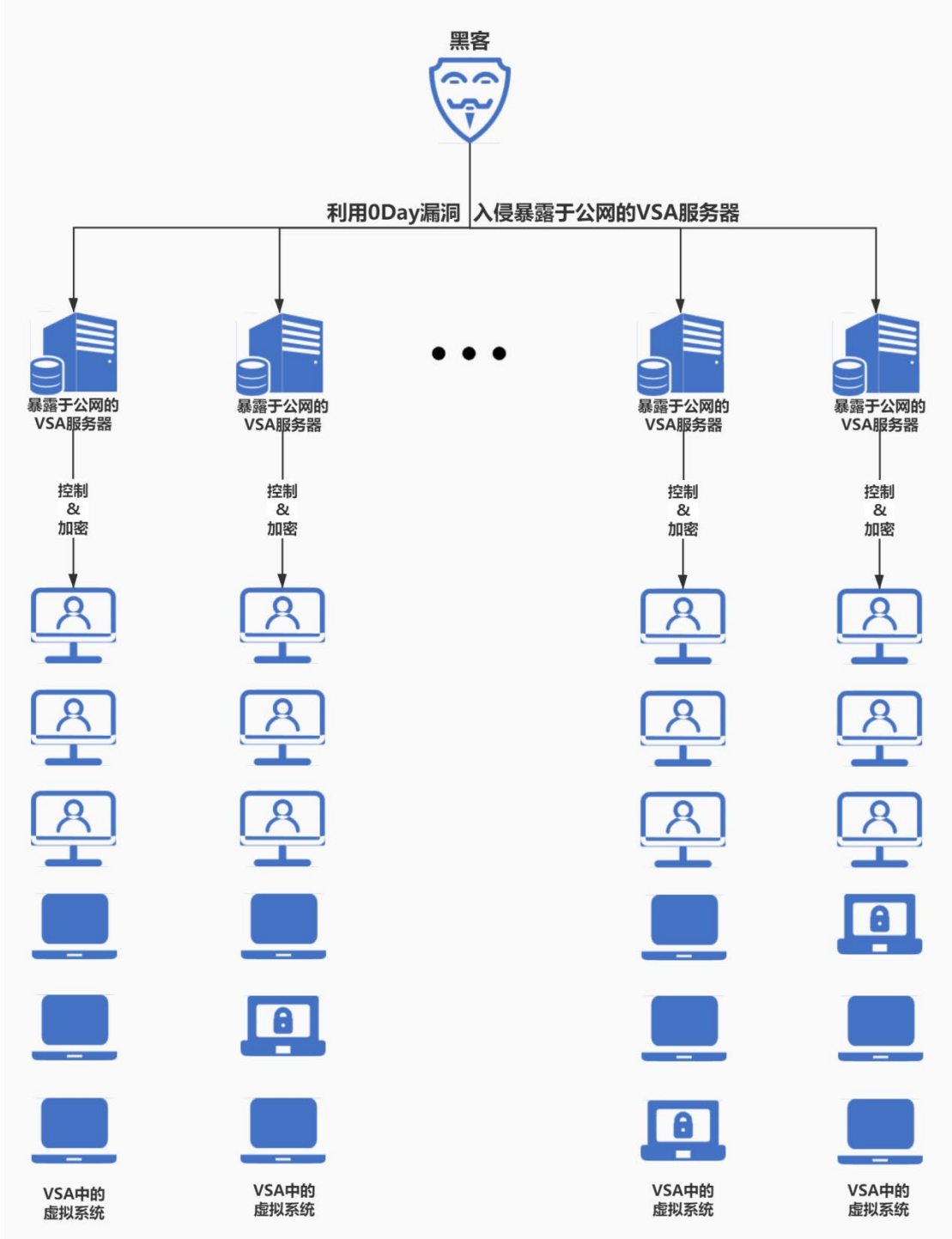


数据来源：360反勒索服务

(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。

今年 7 月，Kaseya VSA 遭遇 Sodinokibi(REvil)勒索病毒幕后团伙发起的供应链攻击，此次攻击导致 100 万个系统被感染。Kaseya VSA 是一款 IT 运维管理平台软件，被很多服务器托管商用来管理企业计算机设备。在此次攻击事件，REvil 黑客团伙利用 Kaseya VSA 产品中的 0Day 漏洞对本地客户端部署勒索病毒的方式，针对相关企业发起了大规模勒索攻击。攻击过程如下图所示：



REvil 黑客团伙供应链攻击流程示意图

第四章 勒索病毒发展趋势分析

2021 年，勒索病毒威胁再次成为最热门网络安全话题，结合信息泄露的二次勒索与多次勒索模式成为年度热点。针对个人、企业、政府机关、各类机构的攻击层出不穷，在勒索病毒威胁面前，没有人能够置身事外。随着勒索病毒的发展蔓延，以及外部环境的快速变化，整个行业也发生了一些变化，我们将从攻与防两个方面进行分析。

一、 勒索病毒攻击发展

(一)多重勒索常态化，信息泄露成企业痛点

2021 年，勒索病毒威胁早已不再是什么新兴网络安全威胁了，它已经成为企业日常必须要面对的安全风险之一。被攻击的企业从奥林巴斯、辛克莱广播集团、美国燃油管道公司这类国家级与跨国企业，到国内某服装厂、某口腔门诊等小型、微型企业。攻击跨度广泛，不论企业规模、所在行业都面临被攻击风险。企业一方面需要满足自身发展需求，提升信息化程度，而另一方面又要面临来自勒索攻击为代表的各类网络攻击问题。

传统勒索主要以加密文件、数据库、磁盘等方式，影响信息系统正常运作，迫使受害者支付赎金。而从 2019 年 11 月开始的多重勒索攻击，经过不到两年的发展，今年新增的双重勒索家族就有 40 个之多。从常规的数据窃取、数据泄露，到对被勒索公司发起 DDoS、售卖被窃取的信息、利用窃取信息、实施股票违规交易等手段层出不穷。勒索攻击的危害已经不单单是数据受损、业务中断这么简单。数据泄露和勒索事件给企业和客户带来的声誉损失，以及给企业未来发展埋下的安全隐患等各种不确定的风险，都扩大了企业的损失程度。而这些有形经济损失与无形损失也是其它网络安全风险所无法比拟的。

(二)影响社会运转，成为全球共同挑战

近年来，勒索病毒的影响逐步从新闻走到了我们身边。新冠疫情的流行也加快了数字世界更深入的融入现实世界，大数据驱动业务，整个世界构筑在软件之上。美国燃油管道公司被攻击事件，到后续接连出现的如 Cuba 勒索病毒攻击超 49 个美国关键基础设施也向各国敲响警钟。在我们身边，也不断有医疗机构、学校、工厂等受到勒索病毒攻击，造成业务中断的案例。勒索病毒开始更频繁的影响现实社会的正常运转，而像医疗机构这类公共基础设施，也正成为黑客攻击的主要目标。对于一些关键基础设施来自网络的安全威胁，也正在超越传统安全威胁。

网络攻击天然具有的国际化问题，在勒索病毒方面也不例外。勒索病毒威胁已经成为一个全球化的威胁，不是单独一个国家政府能够解决的。勒索病毒的攻击目标从个别笔记本、个人电脑、服务器，到目前对医院、学校、政府机构和基础设施实施攻击，其影响力已经大大超越以往。勒索病毒也已不单单是造成经济上的损失，它已经形成了对国家安全，公众生命健康安全的挑战。又如 Lockean 多个勒索软件分支机构袭击法国组织，Moses Staff 黑客组织对以色列发动非勒索加密攻击等，其攻击目标与意图也发生了复杂转变。勒索病毒的这一变化，也使其受到了更多国家的关注，如美国在 G7 就提出了共同打击勒索软件攻击的倡议。

(三)攻击多元化，向更多平台扩散

勒索病毒的发展，从最初的依靠钓鱼邮件传播，针对特定人群，到目前的广泛流行。在2021 年，勒索病毒攻击不论是团伙增长速度，还是资源水平都越来越快，越来越充足，这与勒索攻击获得的大量赎金不无关系。从灰黑产“小毛贼”到 APT 组织力量都有入场参与勒索病毒攻击。大量案例也显示，在针对高价值目标的攻击中，长期潜伏已经成为一种常态的攻击方式。

在发起勒索攻击之前，攻击者已经控制目标网络相当长一段时间，通过横向渗透不断扩展攻击范围和窃取更多数据。攻击者已经知道什么数据是企业最关键的核心数据，触动什么数据可以让一个企业停摆，迫使企业支付赎金。另一方面，“勒索软件即服务”(Ransomware-as-a-Service，简称 RaaS)的模式在最近两年也愈发流行。在今年国内流行的TOP10 勒索病毒中就有至少 4 款涉及到这种模式。而以 Conti 勒索团伙为代表的攻击组织，还向我们展示了另外一种攻击模式——初始访问代理业务(Initial Access Brokers，简称IAB)，这种模式简而言之就是允许攻击者直接购买攻击目标的初始访问权限。这种攻击链的细分，让发起勒索攻击的难度进一步降低，攻击者可以在地下黑市轻易购买到发起攻击所需的各种工具和线索，也加快了勒索病毒的蔓延。

除了攻击途径的多元化，被攻击目标也越来越广泛。从最常见的 Windows 系统、Andriod 系统，到 Linux 系统、各种嵌入式设备、NAS 设备均成为攻击目标。如 Pysa 勒索软件团伙就利用 ChaChi 木马攻击 Linux 系统。而活跃多年的 eChOraix 勒索病毒，今年也有多次攻击报告。针对 PL/SQL，MS SQL 等数据库的勒索病毒反馈，在 2021 年也有增无减。勒索攻击并不局限于 PC 或常规服务器，任何可以接触到的网络设备、信息系统，均可能成为勒索攻击的目标。

(四)云服务商将面临更多考验

回顾 2021 年勒索攻击事件，可以看到供应链攻击与针对云服务商的攻击。虽然此类攻击在绝对数量上不是最多的，但影响范围却是最广泛的。比如今年 7 月 REvil 团伙利用 Kaseya VSA 服务器中的漏洞来访问安装在客户系统中的 VSA 设备，被攻击的多为 MSP 提供商，造成超过 100 万个系统被感染。就在 2021 年年底，IT 服务商 Inetum 遭 Blackcat 勒索软件攻击，影响了法国的部分业务。对云服务商的攻击，往往会造成动辄数百甚至上万家企业受到波及，赎金金额上千万美元也不算罕见。使用供应链攻击与针对云服务商的攻击，将成为未来一段时间内勒索攻击的一个重要风向。

二、 勒索病毒的防护、处置与打击

(一)创新驱动反勒索技术发展

在与勒索病毒的多年对抗中，360 安全产品对勒索病毒的防御能力已经比较完备。统计360 反勒索服务的中招用户情况，可以看出事前正确使用安全产品的只有很少的一部分。但勒索病毒的对抗并不止步于此，勒索攻击问题也是近年来安全行业的重点研究对象。

解密技术，是伴随勒索病毒产生的一项勒索处置方案，早期勒索病毒多存在各种缺陷，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病毒已经比较少见

了，破解解密愈加困难，360 解密大师在本年度更新 7 个家族的勒索解密支持，多为通过各种渠道获取到了病毒的私钥实现，相交往年也有大幅减少。

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。比如 360 在可疑加密监控，敏感数据访问等维度，增加了部分探索性防护，在实验阶段能够有效发现攻击者收集窃取用户敏感数据，以及协助用户解密被可疑程序加密的文件等。依托这些创新技术手段，我们已经推出了 360 浏览器密码保护与 360 隐私保护。而业内，也有很多公司，在尝试使用一些技术手段来缓解勒索攻击，比如一个称为 SSD-Insider 的技术，通过在 SSD 固件中识别勒索攻击，尝试进行防御。

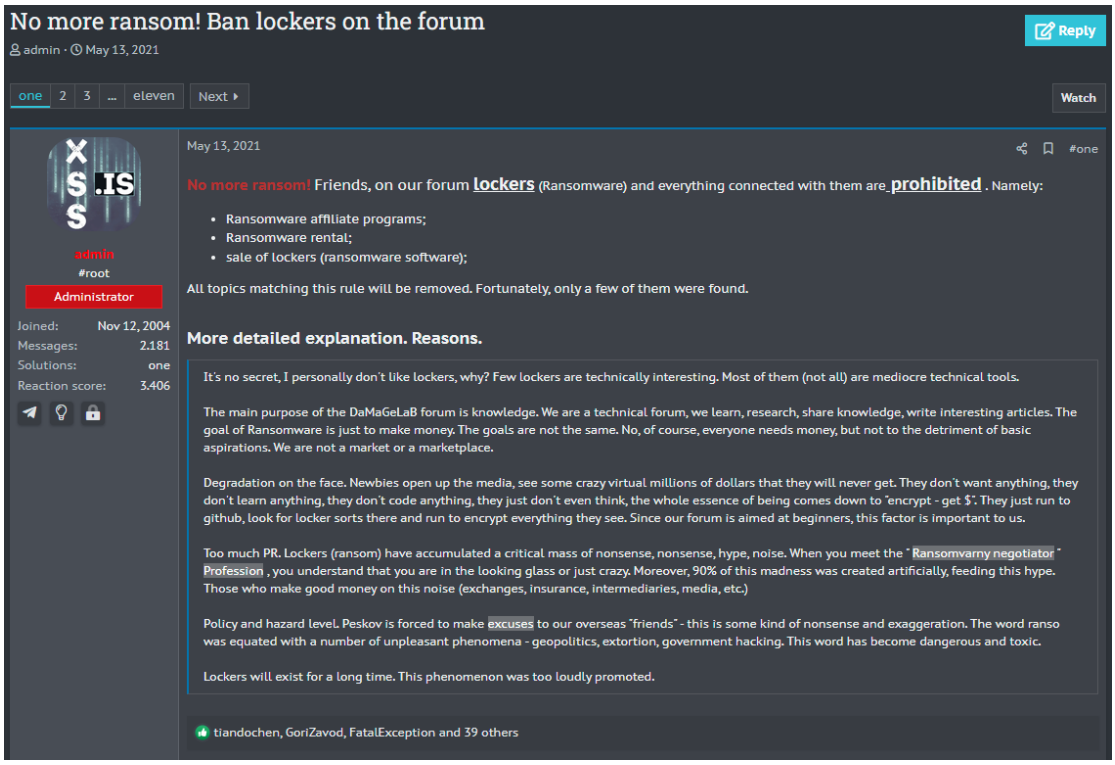
（二）加强加密货币监管

加密货币的兴起，客观上推动了勒索病毒的横行。目前流行的所有勒索病毒，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，但是匿名性使其一个重要的共同特征，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病毒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，但今年来， 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。

国内今年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。

（三）针对勒索病毒相关的犯罪打击

近年来，各国政府均加大了对勒索病毒犯罪的打击力度。美国多次宣称要提高对勒索病毒团伙的打击，并对一些黑客团伙做出了制裁，虽然并为见到明显收效，但对勒索病毒问题的处理姿态更加清晰。而多个地下黑产论坛，也在表面上开始抵制勒索行为——比如 XSS 和 exploit 论坛开始禁止投放勒索病毒相关广告，XSS 还禁止了所有宣传勒索软件的话题。



XSS 论坛禁止勒索相关主题

在欧洲，根据 BleepingComputer 在 2021 年 10 月报道，欧洲刑警组织在乌克兰逮捕了两名网络犯罪份子。他们不仅参与勒索攻击，还参与洗钱活动。从 2020 年至今，这两名犯罪分子已成功发起过大约 100 起网络攻击事件。此次抓捕共缴获 375000 美元现金，以及两辆价值约 250000 美元的豪华汽车。此外，调查人员冻结了价值 130 万美元的加密货币，据信这些加密货币与支付赎金有关。不止于此，在今年 10 月，欧洲刑警组织在乌克兰和瑞士拘留了 LockerGoga、MegaCortex、Crysis 勒索软件袭击案嫌疑人。

202 年，国内对勒索病毒的处置也更趋完善，主管部门和多家安全厂商均提供了勒索病毒的救援指引。360 在勒索病毒救援方面，依托反勒索服务，提供了救援服务，救援热线，线上勒索病毒查询服务等，协助企业应对勒索病毒问题。

近年来，国内也有多起勒索攻击事件的幕后黑手被警方抓获的新闻。比如根据南通公安通报，“撒旦”勒索病毒作者被抓获，截至案发，巨某已成功作案百余起，非法获利的比特币折合人民币 500 余万元，同案还抓获了与其合作的数据恢复公司经营者。

针对勒索病毒的打击，需要从多方面下手，单个国家很难彻底铲除其攻击网络，需要加强强国际合作，共同铲除这一毒瘤。

第五章 安全建议

面对严峻的勒索病毒威胁态势，我们分别为个人用户和企业用户给出有针对性的安全建议。希望能够帮助尽可能多的用户全方位的保护计算机安全，免受勒索病毒感染。

一、 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病毒攻击。

(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，减少遭遇挂马攻击、钓鱼网站的风险。
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。

二、 针对企业用户的安全建议

(一)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，防御勒索病毒也并非难事。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。避免双重勒索病毒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。

(二)发现遭受勒索病毒攻击后的处理流程

1. 发现中毒机器应立即关闭其网络和该计算机。关闭网络能阻止勒索病毒在内网横向传播，关闭计算机能及时阻止勒索病毒继续加密文件。
2. 联系安全厂商，对内部网络进行排查处理。
3. 公司内部所有机器口令均应更换，你无法确定黑客掌握了内部多少机器的口令。

(三)遭受勒索病毒攻击后的防护措施

1. 比照“企业安全规划建议”中的事项，对未尽事项目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病毒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。

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：部分勒索病毒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。

附录1. 2021 年勒索病毒大事件

一、 NetWalker 被执法机构查封

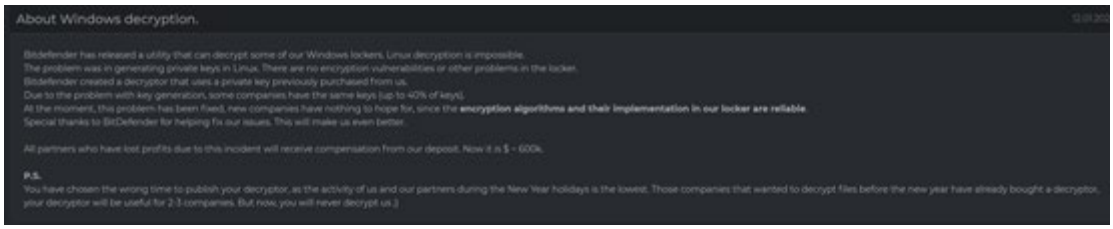
NetWalker 是由“Cricus Spider”网络犯罪组织采用“勒索软件即服务（RaaS）”模式运营的勒索病毒。2019 年传播至今至少有 27 个国家/地区有受害者被该家族攻击。在 2020 年，该家族利用疫情热点发送大量 COVID-19 相关钓鱼邮件传播勒索，并在同年 3 月开始将其主要攻击目标瞄准医疗和教育行业。从该团伙去年 8 月份报表显示，仅仅 5 个月，其获利已超 2500 万美元。

2021 年 1 月 27 日美国和保加利亚的执法机构已查封了与 Netwalker 勒索软件运营方相关的暗网站点，并在该站点挂出查封通知。同时抓捕了一名涉嫌通过传播 NetWalker 勒索盈利超 2700 万美元的加拿大人。

NetWalker 站点被查封

二、 DarkSide 的兴衰起伏

DarkSide 勒索病毒家族于 2020 年 8 月开始对企业展开针对性攻击，并在伊朗创建了一个分布式存储系统用于存储受害者数据。而知名安全厂商 BitDefender 在 2021 年 1 月发布了该家族的密钥。针对本次事件，该团伙表示：由于密钥生成问题导致有 40%的公司拥有相同的密钥，且因为 Bitdefender 的发现，目前该团队已修补了该漏洞。

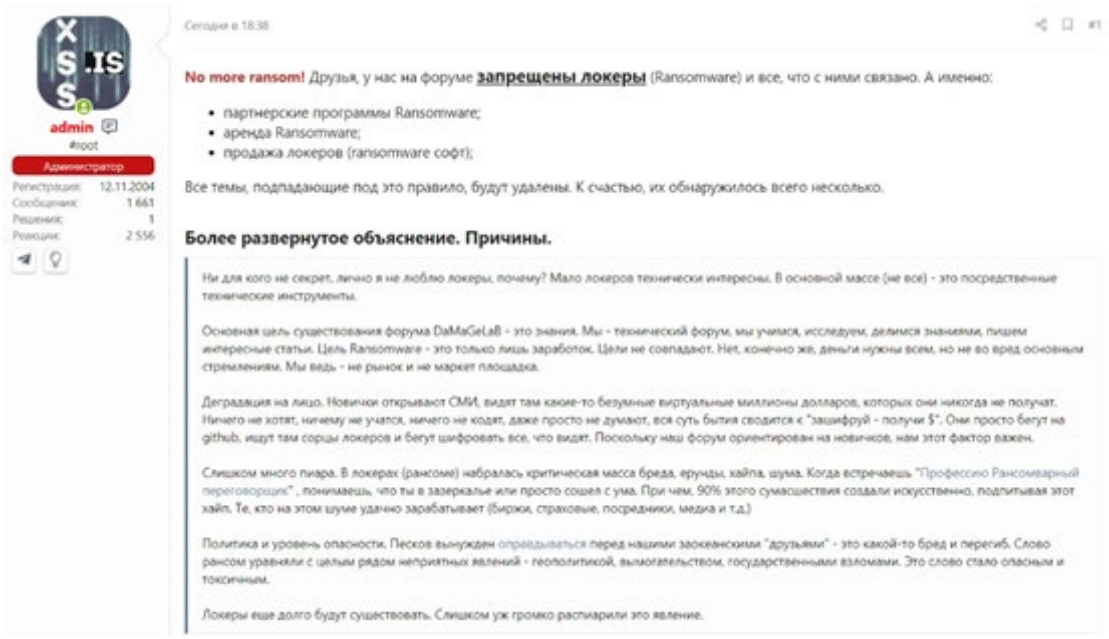


Darkside 关于解密密钥泄露的声明

时至今年 5 月 7 日，美国最大燃油管道上 Colonial Pipeline 遭遇勒索病毒攻击，迫使其关闭了向人口稠密的美国东部各州供油的关键燃油网络。17 个洲和哥伦比亚特区进入紧急状态。此次事件的幕后黑手则正是已经修补了“密钥漏洞”的 DarkSide 勒索病毒。由于该黑客团伙不仅紧密了大量设备，还窃取了大量数据，Colonial Pipeline 为了尽快恢复运营，不得不向黑客支付 500 万美元作为赎金系统。

Colonial Pipeline 遭到攻击的公告

此次事件后，DarkSide 遭到美国和俄罗斯政府的打击，其基础设备已不能正常访问，数据泄露网站已无法访问。俄罗斯两大网络犯罪论坛宣布论坛将永久禁止发布任何勒索病毒相关的主题。XSS 论坛没收了 DarkSide 在论坛存放的 22.081 个比特币作为“受害者”的补偿(此处的受害者为未从 DarkSide 团伙获取到劳动报酬的网络犯罪分子)。目前 exploit 网络犯罪论坛已将该团伙的账户 darkupp 删除。



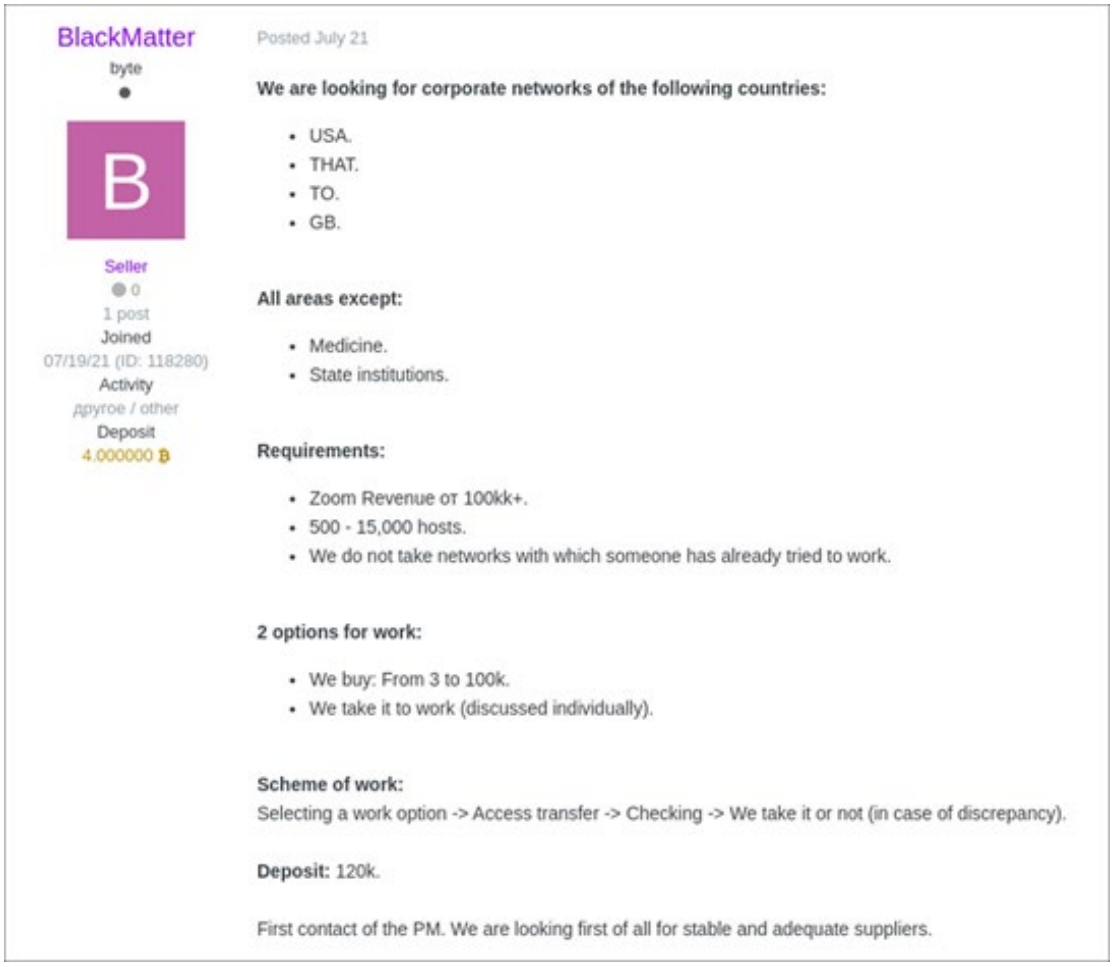
XSS 论坛公告

而受到此次攻击事件影响，美国全国各地燃料短缺且价格飙升，引起美国政府高度重视。6 月，FBI 通过找到 DarkSide 存储比特币密钥的云服务器。成功将该账户中的 63.7 个比特币转出到其他账户，该赎金来自 Colonial 向 DarkSide 支付的 440 万美元中的 230 万美元。

据称 DarkSide 黑客团队使用的是 Coinbase 钱包，FBI 和司法部门通过对 Coinbase 发布强制执行命令，获取到的 DarkSide 的钱包地址和私钥。加上之前被 XSS 网络犯罪论坛锁定的 22.081 个比特币，该团伙已知的被扣押的资金已达 85.781 个比特币。

直至 7 月，安全人员发现一款新型勒索软件 BlackMatter（据信是由 DarkSide 重命名而来）开始在网络犯罪论坛开始发布各种广告招募合作伙伴，并声称同时拥有 REvil 和 DarkSide 的最佳功能。

该团伙在攻击受害者的同时，还积极的从其他攻击者那里购买网络访问权限以发起新的勒索攻击。该家族曾在网络犯罪论坛发布消息称，其主要目标是那些盈利超过 1 亿美元，网络中存在 500-15000 台设备的公司。

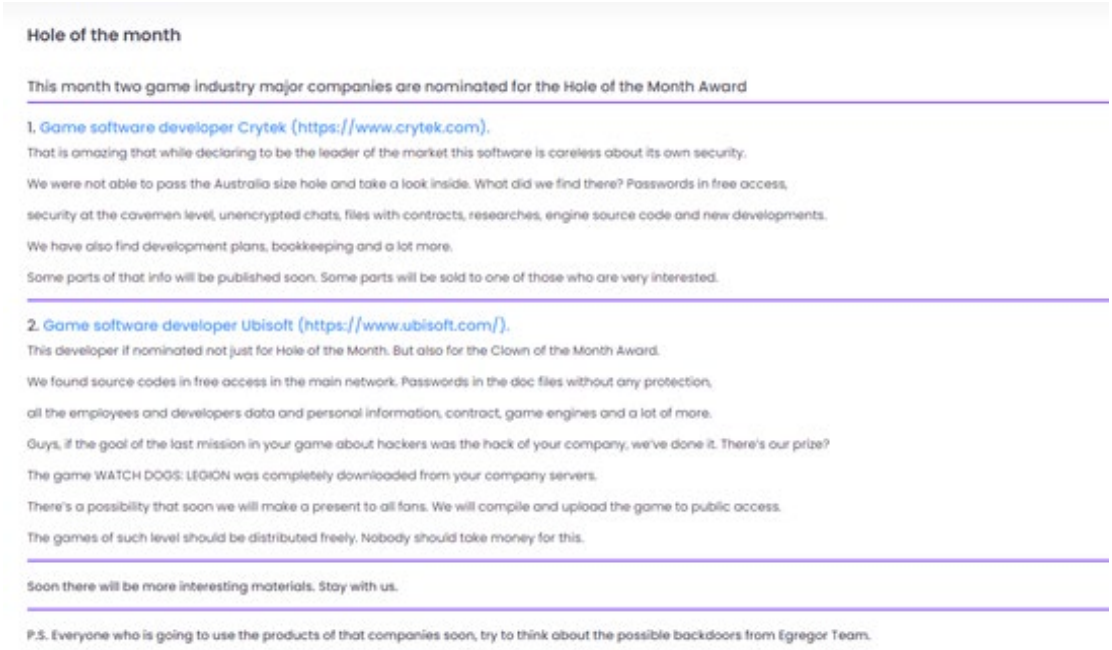


BlackMatter 团队暗网论坛招募同伙广告

此外，该勒索病毒不仅支持在 Windows 上运行，还支持在 Linux 和 ESXi 服务器上运行。目前已出现受害者被攻击，并且已有受害者向 BlackMatter 支付 400 万美元的赎金。

三、 Egregor 成员被警方逮捕

2021 年 2 月 16 日,法国警方与乌克兰警方联合在乌克兰抓捕了 Egregor 的一名成员(非团队核心成员，仅是其会员中的一员，主要负责攻击目标)。从 2020 年 9 月至今，该家族已成功感染 206 个目标，其中包含法国多个大型企业——例如游戏开发商 Ubisoft、法国报纸 Ouest France 和物流巨头捷富高 Gefko 等企业。目前该组织的数据泄露网址已关闭无法访问。且在本月未发现被该家族攻击案例。



Hole of the month

This month two game industry major companies are nominated for the Hole of the Month Award

1. Game software developer Crytek (https://www.crytek.com).

That is amazing that while declaring to be the leader of the market this software is careless about its own security.

We were not able to pass the Australia size hole and take a look inside. What did we find there? Passwords in free access,

security at the cavemen level, unencrypted chats, files with contracts, researches, engine source code and new developments.

We have also find development plans, bookkeeping and a lot more.

Some parts of that info will be published soon. Some parts will be sold to one of those who are very interested.

2. Game software developer Ubisoft (https://www.ubisoft.com/).

This developer if nominated not just for Hole of the Month. But also for the Clown of the Month Award.

We found source codes in free access in the main network. Passwords in the doc files without any protection,

all the employees and developers data and personal information, contract, game engines and a lot of more.

Guys, if the goal of the last mission in your game about hackers was the hack of your company, we've done it. There's our prize?

The game WATCH DOGS: LEGION was completely downloaded from your company servers.

There's a possibility that soon we will make a present to all fans. We will compile and upload the game to public access.

The games of such level should be distributed freely. Nobody should take money for this.

Soon there will be more interesting materials. Stay with us.

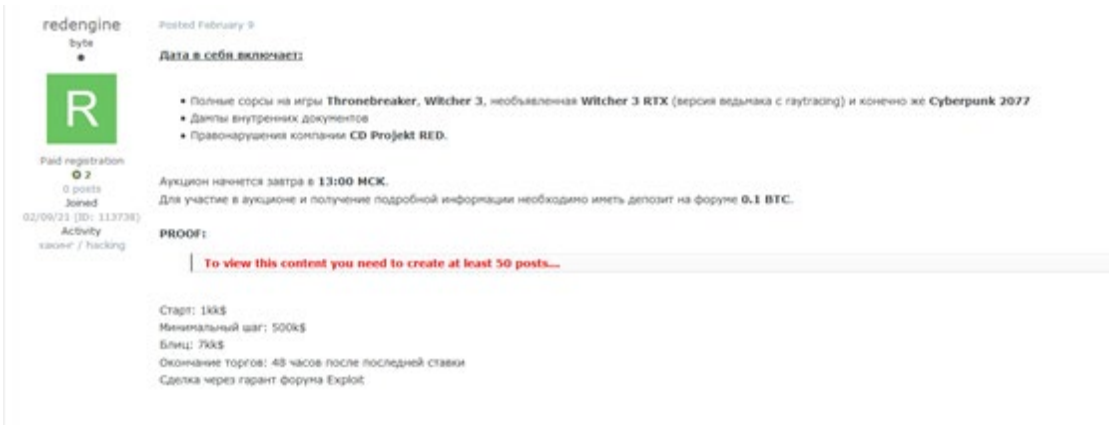
P.S. Everyone who is going to use the products of that companies soon, try to think about the possible backdoors from Egregor Team.

Crytek 及 Ubisoft 遭到攻击

四、 HelloKitty 瞄准知名游戏公司 CDPR

早在 2020 年 12 月,就有勒索病毒团队将目光瞄准 CD Project Red，但那次攻击的主要受害对象是使用该旗下的的游戏玩家。攻击者通过在假冒的 Google Play Store 上分发用勒索病毒伪装的安卓版 Cyberpunk 2077。

而在 2021 年 2 月，CD Project Red 开发商被 HelloKitty 勒索病毒攻击，导致文件被加密的同时大量数据被窃取。CDPR 第一时间回应拒绝支付赎金，并通过备份恢复了正常运作。不久黑客将窃取到的巫师 3、Thronebreaker 和 Cyberpunk 2077 等的源码在暗网论坛被公开拍卖，只要在该论坛有 0.1BTC 存款的用户均可参与拍卖。



HelloKitty 勒索病毒团队在暗网售卖 CDPR 数据

五、 DoppelPaymer 频繁攻击大型企业

DoppelPaymer 黑客组织的目标几乎都是大型企业，在 2020 年被攻击的受害者中多起案件引发社会高度关注：攻击德国医疗机构成第一起因勒索病毒攻击导致患者抢救不及时死亡案例；加密富士康 1200 台设备索要史上最高赎金 2.3 亿人民币。牵连甚广的零件制造商 Visser Precision 拒绝对该团队支付赎金后，其客户特斯拉、波音、SpaceX 等机密文件均被泄露。

2021 年 2 月，该勒索病毒团伙再次因成功入侵起亚美国的数据库引起广泛关注，该团伙向现代汽车集团索要 2000 万美元作为赎金，并承诺不会将窃取到的数据泄露。若未在规定时间内支付，赎金将会增加到 3000 万美金。最后如果双方无法达成支付协议，黑客将会公布在此次攻击中窃取到的重要数据。此次事件已影响了起亚美国的自助支付服务、网上平台以及电话支持系统，同时现代汽车的多个经销商站点、经销商技术人员使用的服务也出过中断，但现代似乎并未受到此次攻击事件太大影响。

而在美国大型燃料管道商 Colonial Pipeline 被 DarkSide 攻击后，DoppelPaymer 的活动开始下降，5 月开始其数据泄露网站未曾更新过受害者消息。

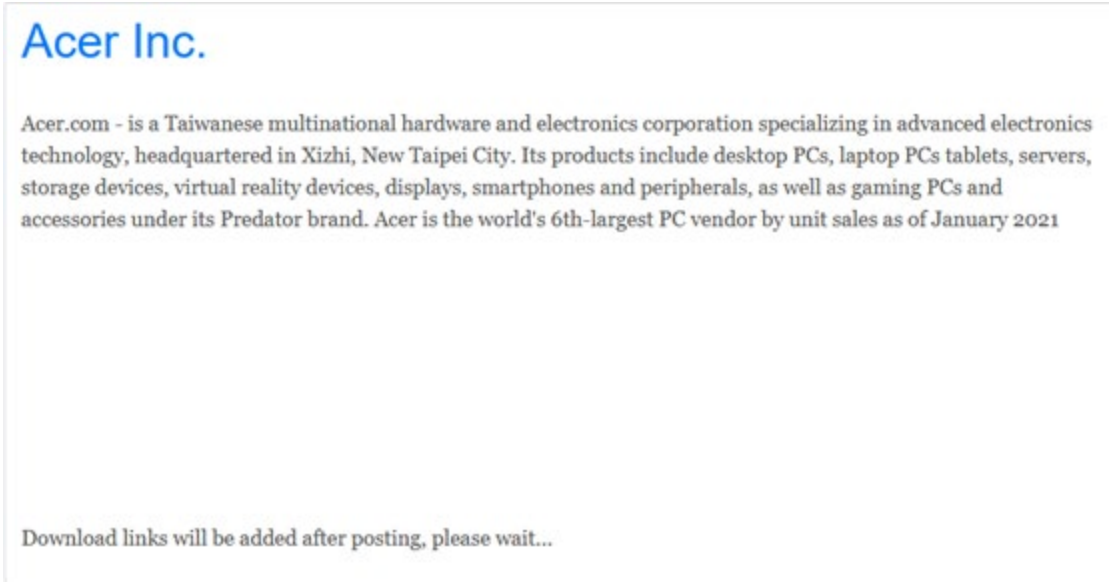
直到 7 月，研究人员发现 DoppelPaymer 可能已经进行了“品牌重塑”，并重命名为 Grief(又叫 Pay)。两者有较多相似之处：

1. 两者共享相同的加密方式。
2. 相同的分发渠道(Dridex 僵尸网络)。
3. 高度相似的代码，采用相同的加密算法(RSA2048 和 AES-256)。
4. 均使用欧盟通用数据保护条例(GDPR)作为警告，未付款的受害者仍将因违规而面临法律处罚。
5. 数据泄露站点上的防止爬虫的验证码等。

该家族最早的信息是从 2021 年 6 月开始的，但被捕获到的样本的编译时间为 5 月 17 日。同时该家族接受赎金时仅支持 XMR 虚拟货币，采用此虚拟货币很大程度是为了避免被追溯。重命名后的 Grief 勒索病毒已展开正式攻击，其中较重要的受害者 Clover Park 被索要价值 35 万美元的 XMR。

六、 Sodinokibi(REvil)，猎手终变成猎物

2021 年 3 月，Sodinokibi（REvil）勒索团伙向宏碁(Acer)索要 5000 万美元(约 3.3 亿元人民币)作为赎金，创当时历史最高赎金记录。该勒索病毒家族不仅加密了 Acer 的文件，还窃取了其财务表格、银行结余、银行通讯录文档等机密文件。若宏碁不能在规定时间内支付赎金，该团伙将在暗网公布窃取到的数据。



Sodinokibi（REvil）发布关于即将公布 Acer 数据的公告

次月，全球第二大笔记型电脑研发涉及制造公司广达电脑也同样遭遇 Sodinokibi(REvil)勒索病毒攻击，被索要 5000 万美元作为赎金。攻击者还表示若支付日期超过 4 月 27 日，将需支付 1 亿美元赎金。此次攻击事件被窃取大量客户数据，目前尚不明确到底有多少客户数据被窃取，但其客户包括了苹果、戴尔、惠普 、亚马逊、思科、富士通、联想、LG 等大型公司，目前苹果的部分设计图纸已被该团伙公布到暗网中。

在和广达电脑谈判时，广达电脑表示他们不关心客户和员工数据，允许黑客公布和出售所有数据。于是 Sodinokibi(REvil)便转向与苹果谈判，想尝试通过威胁苹果——称若其不购回被窃取数据，便将在春季发布会之前将苹果最新产品设计数据在暗网公布。

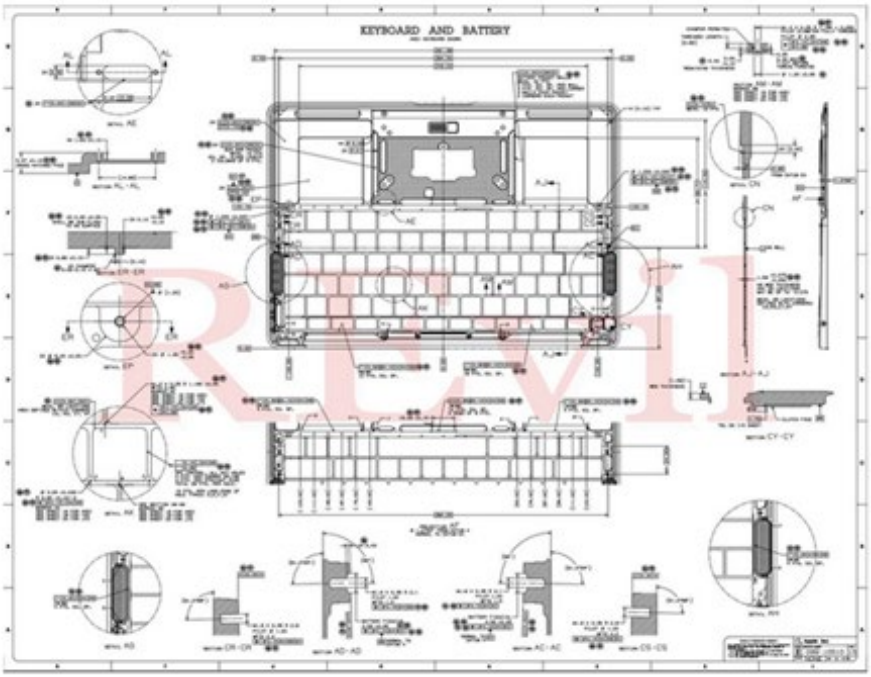
Products:
Apple Watch
Apple Macbook Air
Apple Macbook Pro
ThinkPad Z6om

In order not to wait for the upcoming Apple presentations, today we, the REvil group, will provide data on the upcoming releases of the company so beloved by many.Tim Cook can say thank you Quanta.From our side, a lot of time has been devoted to solving this problem. Quanta has made it clear to us that it does not care about the data of its customers and employees, thereby allowing the publication and sale of all data we have.

P.S.
Our team is negotiating the sale of large quantities of confidential drawings and gigabytes of personal data with several major brands.
We recommend that Apple buy back the available data by May 1.

More and more files will be added every day.
The same is in pdf format

Proofs:



遭泄露的苹果电脑设计图

至 5 月 31 日，Sodinokibi(REvil)再次出手，攻击了全球最大的牛肉生厂商 JBS 在北美和澳大利亚的部分 IT 系统，导致 JBS 被迫关闭部分食品生产站点。虽然该公司被加密的文件中除了两个特定的数据库外，大部分都有备份的，可通过备份进行恢复。但考虑到若不支付赎金被黑客窃取的数据将被在暗网公开，最终选择向黑客支付赎金 1100 万美元。

JBS USA today confirmed it paid the equivalent of $11 million in ransom in response to the criminal hack against its operations. At the time of payment, the vast majority of the company's facilities were operational. In consultation with internal IT professionals and third-party cybersecurity experts, the company made the decision to mitigate any unforeseen issues related to the attack and ensure no data was exfiltrated.

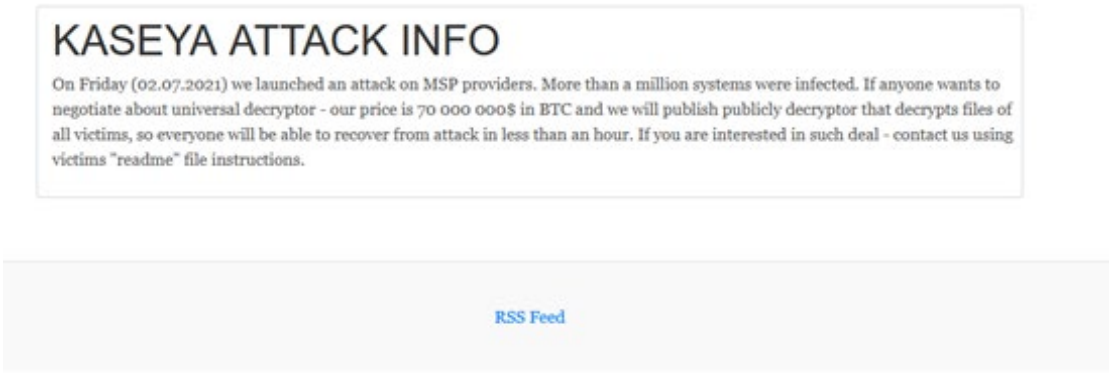
"This was a very difficult decision to make for our company and for me personally," said Andre Nogueira, CEO, JBS USA. "However, we felt this decision had to be made to prevent any potential risk for our customers."

The FBI stated this is one of the most specialized and sophisticated cybercriminal groups in the world. JBS USA's ability to quickly resolve the issues resulting from the attack was due to its cybersecurity protocols, redundant systems and encrypted backup servers. The company spends more than $200 million annually on IT and employs more than 850 IT professionals globally.

JBS USA has maintained constant communications with government officials throughout the incident. Third-party forensic investigations are still ongoing, and no final determinations have been made. Preliminary investigation results confirm that no company, customer or employee data was compromised.

JBS 遭攻击

6 月底，Sodinokibi(REvil)勒索团伙在暗网数据泄露网站发布了一则声明：“周五（2021.07.02）我们对 MSP 提供商发起了攻击，超过 100 万个系统被感染。如果任何人想要协商通用解密器——我们的价格是 7000 万美元的 BTC，那我们将公开发布解密器解密所有受害者的文件，然后每个系统都能在一小时内得到恢复。如果您对此类交易感兴趣——请使用受害者系统中留下的‘readme’文档与我们联系。”



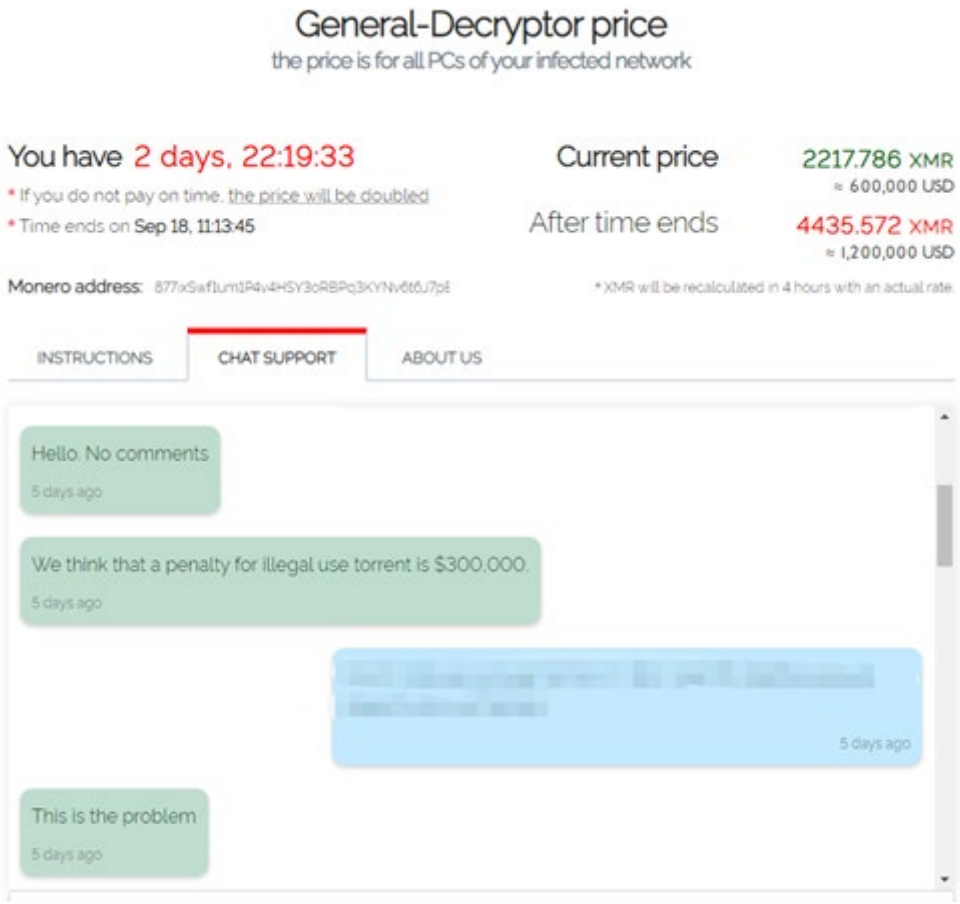
Sodinokibi(REvil)对 MSP 供应发起攻击的公告

除通用解密器的报价，REvil 还对不同类型的受害者报出了不同赎金：针对 MSP(管理服务提供商) REvil 索要 500 万美元，而向其客户则索要 4 万到 4.5 万美元作为赎金。此次攻击事件影响了多个托管服务商及其一千多名客户。其中瑞典最大连锁超市 Coop 因此次事件导致收银系统被感染，被迫关闭了 500 家商店。

针对此次事件调查事，REvil 利用 Kaseya VSA 服务器中的漏洞来访问安装在客户系统中的 VSA 设备，然后通过被感染设备转向所有连接的工作站和公司网络，并安装有效载荷并加密客户文件。该漏洞并非未知漏洞，Kaseya 正在替其用户发布补丁，但不幸的是还是被 REvil 先一步利用了。这次攻击事件不仅是近两年来感染设备量最大的一次，同时也创造了索要赎金金额最大的记录。

大部分受害者均拒绝向黑客支付赎金——在 7 月中旬仅有两名受害者向黑客妥协，而 7 月底，Kaseya 从受信任的第三方手中获取到了通用解密工具，可以协助此次受攻击影响的设备免费解密文件。

而在此次攻击中的受害企业支付了赎金之后不久，Sodinokibi(REvil)团伙便从网络上神秘消失。直到 9 月初，关停近两个月的 Sodinokibi(REvil)勒索软件正式回归，不仅重启了其基础设施，还在其数据泄露网站发布了新受害者信息。同时重置的还有赎金谈判页面的倒计时——这也意味着之前的受害者若想解密文件，仍可通过该页面与 Sodinokibi(REvil)团伙进行谈判。



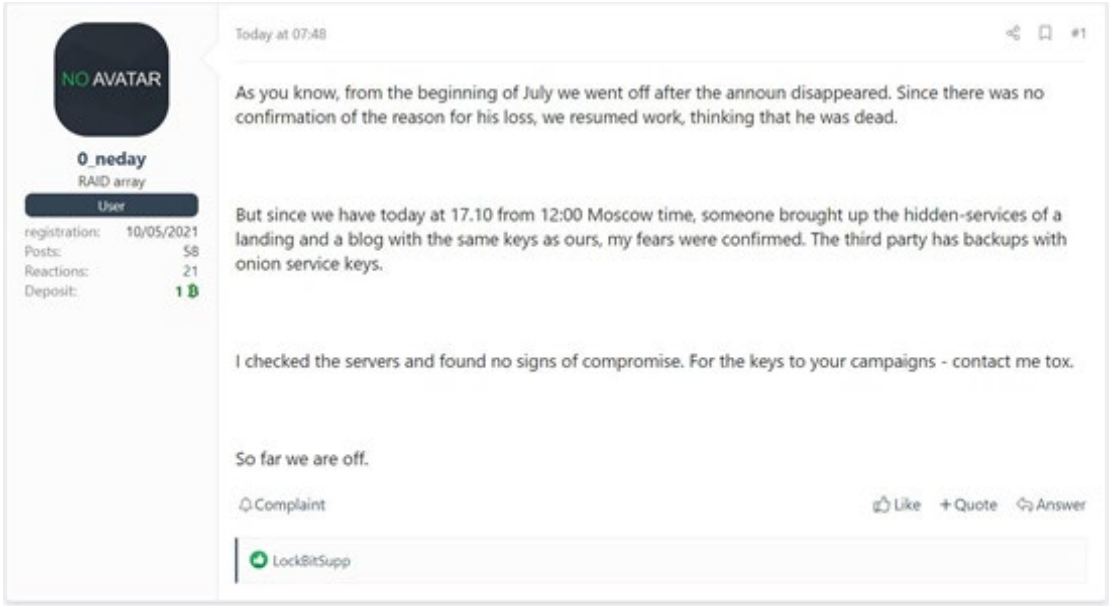
Sodinokibi(REvil)团伙索要 30 万美元赎金

就在 Sodinokibi(REvil)勒索软件宣布回归后不久，国外执法部门通过特殊渠道获取到了该家族早期的密钥，并决定在该家族发起第二波攻击之前为受害者提供解密方案

祸不单行——2021 年 10 月，Sodinokibi(REvil)又遭遇了未知来源的入侵。其支付网站以及数据泄露网站遭遇劫持，被迫再次关闭其基础设备。目前最新受害者已不能通过勒索提示信息中留下的网址联系上黑客。

Sodinokibi(REvil)的支付及数据泄露网站遭劫持

从入侵者发布的消息看，导致该团伙关闭相关基础设备主要因为匿名攻击者获取到了该团队的洋葱的私钥，并且可能有这些站点的备份。



入侵者发布的公告

七、 从新兴到分裂——Babuk 的浮与沉

Babuk 勒索病毒于 2021 年 1 月出现。4 月末，华盛顿警方便遭遇 Babuk 勒索病毒攻击，被窃取 250GB 数据。从公开的截图看，被窃取数据包括调查报告、警官纪律文件、当地团伙文件以及其他行政文件。该勒索病毒家族要求华盛顿警方在 3 天内和他们取的联系，超过时间将公布警方线人信息。同时该团伙还称他们还将继续攻击美国的州机构，并自称比 FBI 的 CSA（网络盾牌联盟）更早发现 0day，还将采取更大规模的攻击。

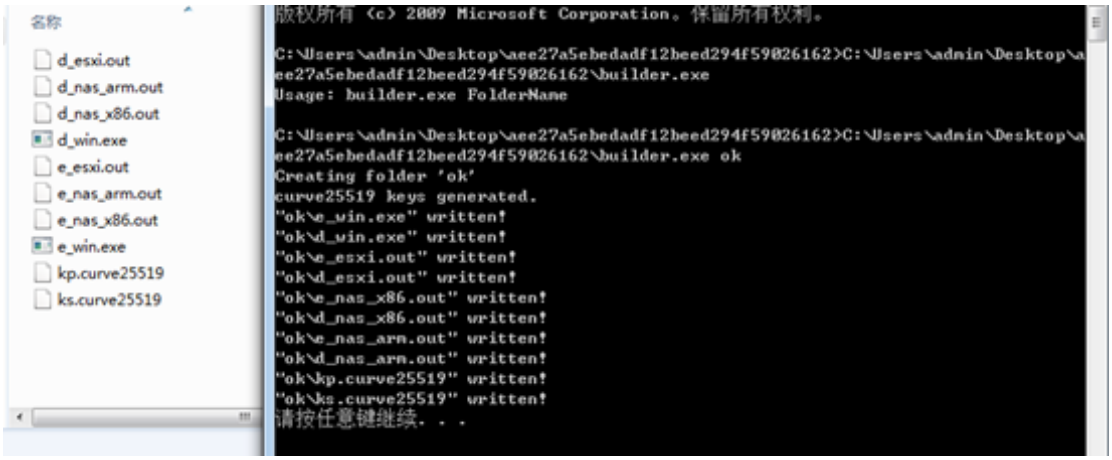
Babuk 留给华盛顿警方的勒索信息

5 月华盛顿警方给出了回应，表示只愿支付 10 万美元赎金。但这一提议遭到 Babuk 团伙拒绝，并警告若不提高支付金额就将公布从华盛顿警察局窃取到的所有数据。同时，黑客在暗网公布了更多数据，其中包括：对警察的背景调查，心理评估、测谎反应、主管面谈、住所信息、财务信息等。

不久之后改勒索病毒团伙宣布，将公开勒索软件源码，并转为纯数据盗窃敲诈勒索。同时还宣布将搭建数据泄露售卖网站，所有数据需要售卖的网络犯罪份子均可通过该网站售卖数据。纯数据盗窃在结果感知层面更具隐蔽性，受害者再不能通过被加密多少设备来了解数据泄露的情况，这可能会加大受害者的恐慌。

2021 年 6 月，有人发现 Babuk 勒索病毒的生成器被人上传到网络上。这导致更多的潜

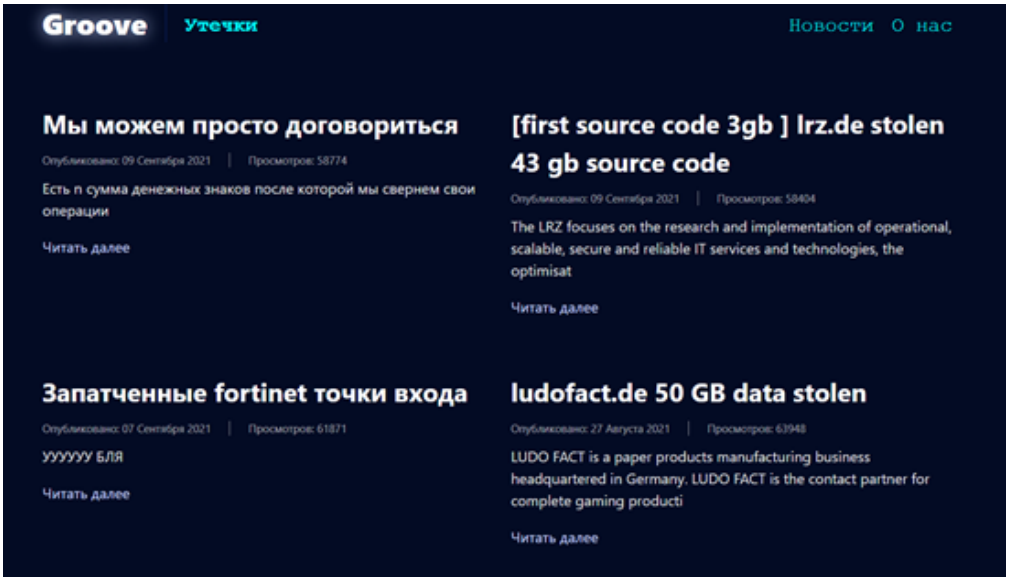
在病毒制作/传播者可使用该生成器制作并传播勒索病毒。该生成器可通过自定义选择生成勒索的运行环境。生成的病毒可在 Windows 系统或基于 ARM 平台的系统中运行并进行加密工作。整体操作流程非常简单，只需提供一个文件夹名即可在该文件夹下替使用者分别生成加密器和解密器。



Babuk 勒索病毒生成器

9 月，Babuk 团伙内部传出内讧消息。在此前对华盛顿警方的攻击事件后，其管理员就决定公布获取到的敏感信息用于宣传，但部分成员拒绝这一行为，认为泄露警方数据会带来大量不好的影响。而在管理员最终泄露数据后，该组织的部分成员便分裂出去创建 RAMP 论坛，而另一些人员则启动了 BabukV2 勒索攻击。

当月，一名 ID 为“Orange”的黑客在 RAMP 发布了一篇文章，文章中包含 12856 台设备上近 50 万个用户的 Fortiner VPN 凭证。根据 IP 定位其所属国家，发现有 11.89%的设备来自中国。同时还观察到 Groove 勒索软件的数据泄露网站发布了一篇指向 RAMP 论坛关于 Fortinet VPN 凭证泄露的文章，猜测其团伙公开这些凭证的目的是想吸引更多的黑客参与该勒索软件活动。



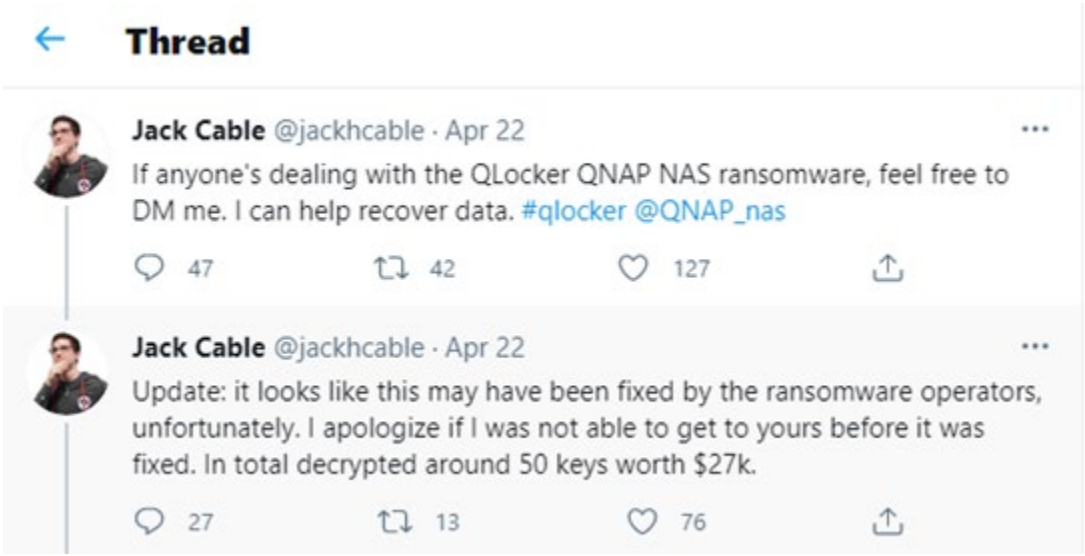
“Orange”发布公布大量敏感数据

八、 QLocker 利用漏洞攻击 NAS 设备

2021 年 4 月， QNAP（威联通）的网络存储设备再次成为勒索病毒攻击对象，受害者设备上的文件均被使用 7zip 加密。QLocker 勒索病毒首次发现于 4 月 19 日，之后便开始大量传播，每天约有数百个 QNAP 设备被其感染。短短五天时间， QLocker 家族收到的赎金便高达 26 万美元。其单个设备赎金为 500 美元左右，粗略计算已有 525 个受害者中招。

此次事件黑客利用了最新修复的 CVE-2020-36195（多媒体控制台和媒体流加载项 SQL 注入漏洞）。使用 QNAP 设备的用户应立即更新多媒体控制台、媒体流加载项和混合备份同步应用程序到最新版本，避免遭遇该勒索病毒攻击。

该勒索早期解密程序存在的 BUG 曾被国外安全研究员发现，并协助过 50 名受害者成功恢复文件，但目前黑客已修补该 BUG。



安全研究员协助 50 名受害者成功恢复文件

九、 从攻击医疗机构到复活僵尸网络，Conti 团伙无恶不作

2021 年 5 月，爱尔兰卫生服务部门被 Conti 勒索病毒攻击。此次攻击对爱尔兰的医疗系统造成了重大的影响，当地多家医院的医疗服务也被迫临时关闭，被窃取了 700GB 重要数据。黑客向其索要价值近 2000 万美元的比特币作为赎金。虽然爱尔兰卫生服务部门尚未支付赎金，但黑客已向爱尔兰卫生服务部门提供免费解密工具。不过 Conti 勒索病毒团伙表示，如果爱尔兰卫生服务部门不支付赎金，其数据仍将被出售或者公开。

从该家族传播至今，已至少攻击了 338 个组织并窃取了其数据，其中绝大部分数据均已被不同程度的公开。此外，种种迹象表明 Conti 勒索病毒的运营者同时也在运营另一款名为 Ryuk 的勒索病毒。该勒索病毒主要通过垃圾邮件、漏洞利用工具、TrickBot 银行木马等多种渠道对个人进行勒索攻击。

Intelligence Report on Ransomware Gangs on the Darkweb

DarkTracer

https://twitter.com/darktracer_int

support@darktracer.com

List of victim organizations(2,155) attacked by Ransomware gangs(34) released on the DarkWeb

No	Victim	Ransomware Gang	Date
2023		Conti	2021-04-22
2024		Conti	2021-04-22
2025		Conti	2021-04-22
2026		Conti	2021-04-22
2027		Conti	2021-04-22
2028		Conti	2021-04-22
2029		Conti	2021-04-22
2030		DarkSide	2021-04-22
2031		Conti	2021-04-22
2032		Conti	2021-04-22
2033		Astro Team	2021-04-22
2034		Everest	2021-04-22
2035		Conti	2021-04-22
2036		Conti	2021-04-22
2037		Conti	2021-04-22
2038		Conti	2021-04-22
2039		Conti	2021-04-22
2040		Conti	2021-04-22
2041		Conti	2021-04-22
2042		Conti	2021-04-22
2043		Conti	2021-04-22
2044		LV	2021-04-22
2045		Conti	2021-04-22
2046		Conti	2021-04-22
2047		Conti	2021-04-22
2048		Astro Team	2021-04-22
2049		Conti	2021-04-22
2050		Conti	2021-04-22

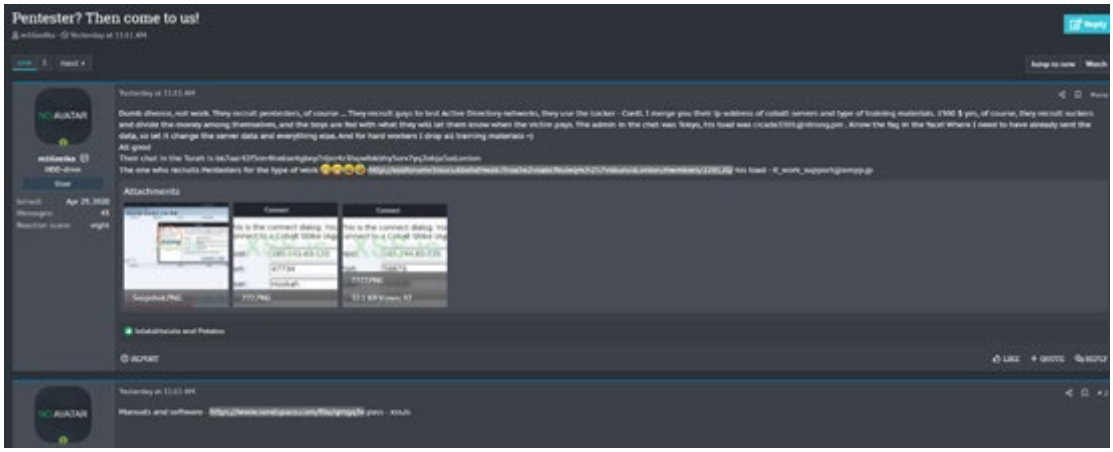
大量数据遭 Conti 泄露

而 2020 年 7 月之后 Ryuk 的传播量就显著下降，其运营者将主要渠道和精力均投入到对 Conti 勒索病毒的传播中。

而 8 月 5 日，Conti 团伙则因内部分赃不均导致其下属组织将其内部资料以及工具公开，其中部分已被上传至暗网论坛，而另一部分文件则仅展示了文件列表的截图。

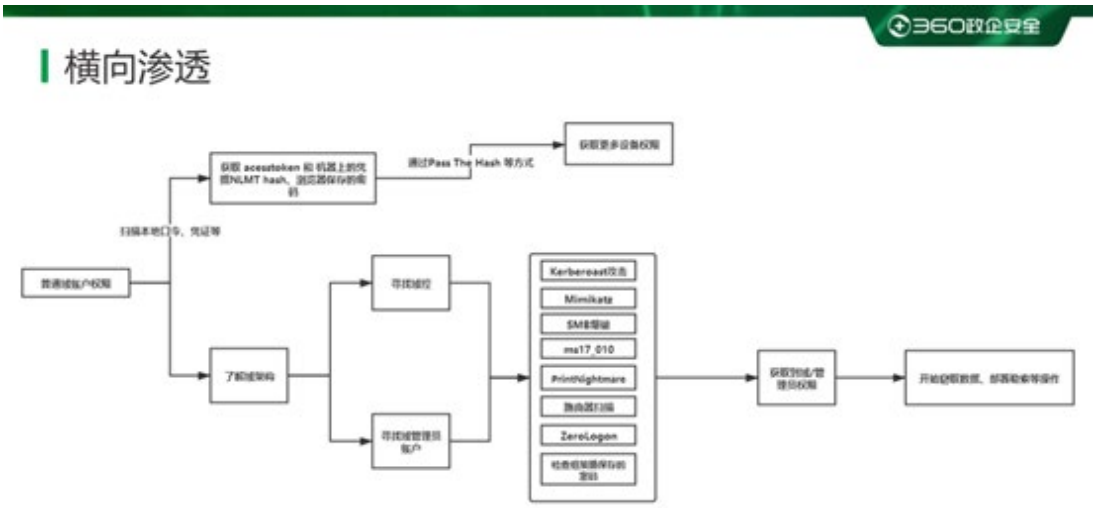
从其下属组织发布的消息看，之所以会发布这些资料是因为在一次攻击事件中 Conti 虽然收取了高达数百万美元的赎金，但该下属组织却仅得到了 1500 美元，其余部分则全部

被 Conti 核心团队占有。



Conti 分赃不均导致内讧

在研究泄露的俄语攻击教程文档时，我们发现他们采用的攻击手法并不算新颖：会先通过扫描本地的口令、凭证等获取更多设备的权限。而对于黑客而言，最重要的是通过该设备去了解当前设备所在域的整体架构，并尽可能去尝试攻击 IT 部门的相关设备（这样更有可能拿到域管理员权限或是域控设备）。该攻击阶段，采用到了多个公开的漏洞，例如“永恒之蓝”、ZeroLogon、PrintNightmare 等。而在成功获取到域控/域管理员权限后，攻击者就可以通过组策略向域内的所有设备进行下发恶意程序、窃取数据、部署勒索等一系列操作。



关于该事件的更多详情可阅读 Conti 勒索集团内部核心资料分析：

https://cert.360.cn/warning/detail?id=8d113d8786af993a847bfc2e98c92ac6

而 11 月，情报公司 Advanced Intelligence 发布消息称，Conti 勒索病毒团伙的成员成功说服知名僵尸网络程序 Emotet 的运营团队将其 “复活”。

Emotet 僵尸网络曾于约 10 个月前被关闭，而此次“复活”则会重新对分布官方的受控

端开启控制。使其充当恶意软件加载程序，为其他恶意软件提供有价值的受感染系统访问权限。而 Qbot 和 TrickBot 则是 Emotet 僵尸网络的主要客户，这两款软件又会利用获取到的访问权限部署包括 Conti 在内的诸多勒索软件。

在被曝出 Conti 策划重启 Emotet 僵尸网络前，该勒索团伙的支付站点和对应域名则均因被劫持导致关闭，但其数据泄露站点页面及域名仍可以正常工作。

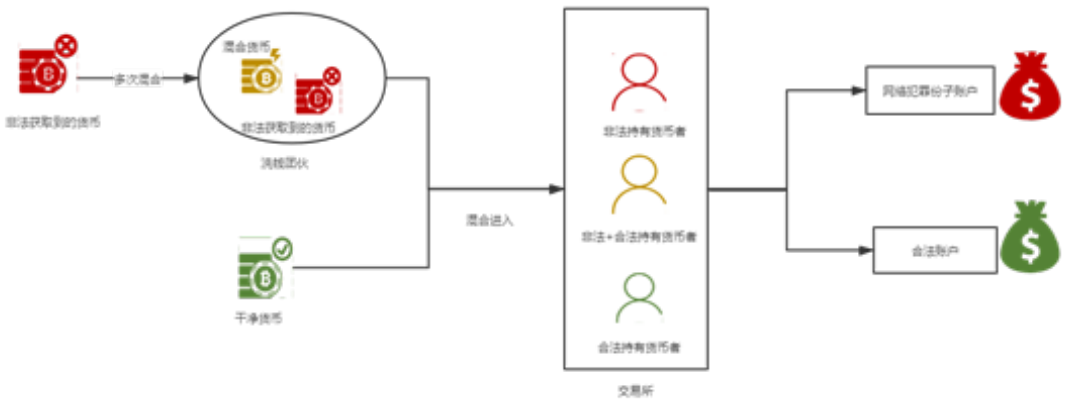
Conti 相关公告

十、 Clop 部分人员被捕

2021 年 6 月 Clop 勒索病毒家族频繁被报道，针对整个事件先做一个大概的时间线回顾：

- 6 月 17 日：乌克兰、韩国和美国联合行动，在乌克兰拘留多名与 Clop 勒索软件相关人员，关闭该组织发动过攻击的服务器基础设施，并缴获了计算机、智能手机和服务器设备、18.5 万美元现金以及多量豪车。
- 6 月 23 日：曝出 Clop 勒索软件仍在继续运作，并在暗网发布受害者数据。
- 6 月 24 日：警方通过和 Binance 币安交易所进行合作，成功锁定为 Clop 勒索软件洗钱的团伙。
- 6 月 25 日：被抓的洗钱团伙为 FANCYCAT，该团伙不仅为多个非法活动提供洗钱服务，还曾高调的发动过网络攻击（例如 Clop 和 Petya 勒索软件攻击），涉及金额高达 5 亿美

元。此次抓捕行动总共抓获了 6 名犯罪嫌疑人，但暗网数据泄露网站仍在正常运行，证明被抓捕人员仅为 Clop 勒索软件招募的一个分支，并非主力。



Clop 事件流程示意图

十一、 ADATA 被泄露 700G 数据

2021 年 5 月 23 日，中国台湾计算机内存制造商 ADATA 遭遇 Ragnar Locker 勒索软件攻击，迫使 ADATA 关闭相关受影响设备。在释放勒索软件之前，该团伙还从 ADATA 内部窃取了多达 1.5TB 的数据，目前已有 700 多 GB 的数据已被公开发布在暗网中。

从该泄露数据网站提供的下载链接发现，该团伙选择使用 MEGA 来存储非法获取到的数据，但遭到 MEGA 抵制——不仅禁止了对该数据的访问，还将该犯罪团伙账户关闭。目前大部分数据已无法下载。但从之前公开的截图看，攻击者从受害者内部已窃取到该公司的专有商业信息、机密文件、原理图、财务数据、Gitlab 和 SVN 源代码、法律文件、员工信息、保密协议等。

ARCHIVED DATA

!Attention Password for the Archives: **Byf5Cqapo6nZ#1JLDiw8**

!!Inside some Packs you will find sub-archives with separate password, for such cases there are txt file with special password, please check everything carefully

- Archive#1.7z (Size 297GB) DOWNLOAD
- DRAM-S.CHENG (Size 86.2GB) DOWNLOAD
- FIN-M.WANG (Size 58.8GB) DOWNLOAD
- FIN-M.SINYEH (Size 36.4GB) DOWNLOAD
- Archive#2.7z (Size 117GB) DOWNLOAD
- KRFS-MAIL (Size 18.6GB) DOWNLOAD
- LAFS-NDA (Size 319MB) DOWNLOAD
- MOTOR1 (Size 7.93GB) DOWNLOAD
- MOTOR-H.CHEN (Size 6.23GB) DOWNLOAD
- MOTOR-M.LI (Size 680MB) DOWNLOAD
- PACK#1.7z (Size 54.5GB) DOWNLOAD
- PACK#2.7z (Size 35.8GB) DOWNLOAD
- RD-A.LU (Size 1.01GB) DOWNLOAD

Please follow up

First batck of files is here:

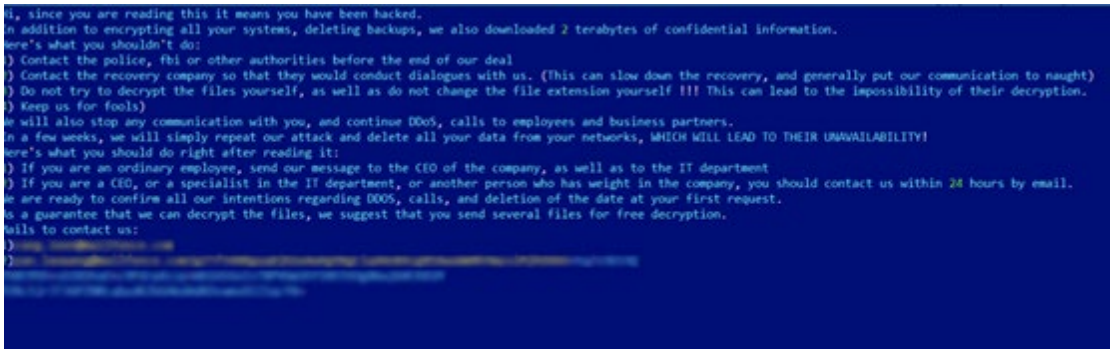
- Pack#1.7z (Size 47.3MB) DOWNLOAD
- Pack#2.7z (Size 54.1MB) DOWNLOAD

遭泄露的 ADATA 数据

十二、 “阎罗王”试图攻击美国金融部门

2021 年 11 月，“阎罗王”勒索病毒的下属机构正在尝试使用 BazarLoader 恶意软件攻击美国金融部门。自从 8 月份以来，“阎罗王”勒索病毒不仅对金融机构发起攻击，还对制造业、IT 服务、咨询及工程领域的公司进行攻击。

该攻击团伙在入侵阶段不仅部署了恶意软件，还尝试从受控设备上收集浏览器保存的登录凭证，例如：Firefox、Chrome、Internet Explorer，以及窃取 KeePass 密码管理器的主密钥等。受害者若不能在规定时间内联系黑客并支付赎金，黑客将对受害者采取 DDOS 攻击以及致电其员工和业务合作伙伴，若几周内仍未支付，黑客将删除其数据。



“阎罗王”勒索信息

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病毒最重要的传播手段，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。在于勒索病毒对抗的过程中，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 2021 年防黑加固功能每月所防御的攻击量。

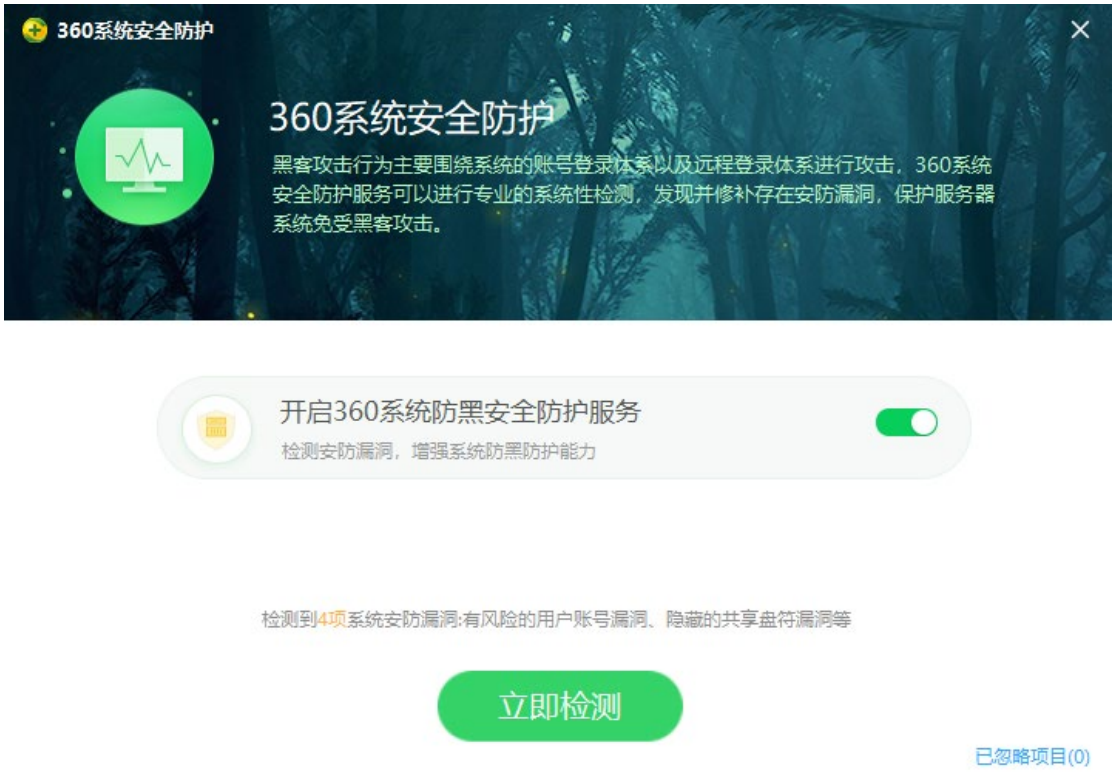
数据来源：防黑加固统计数据

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

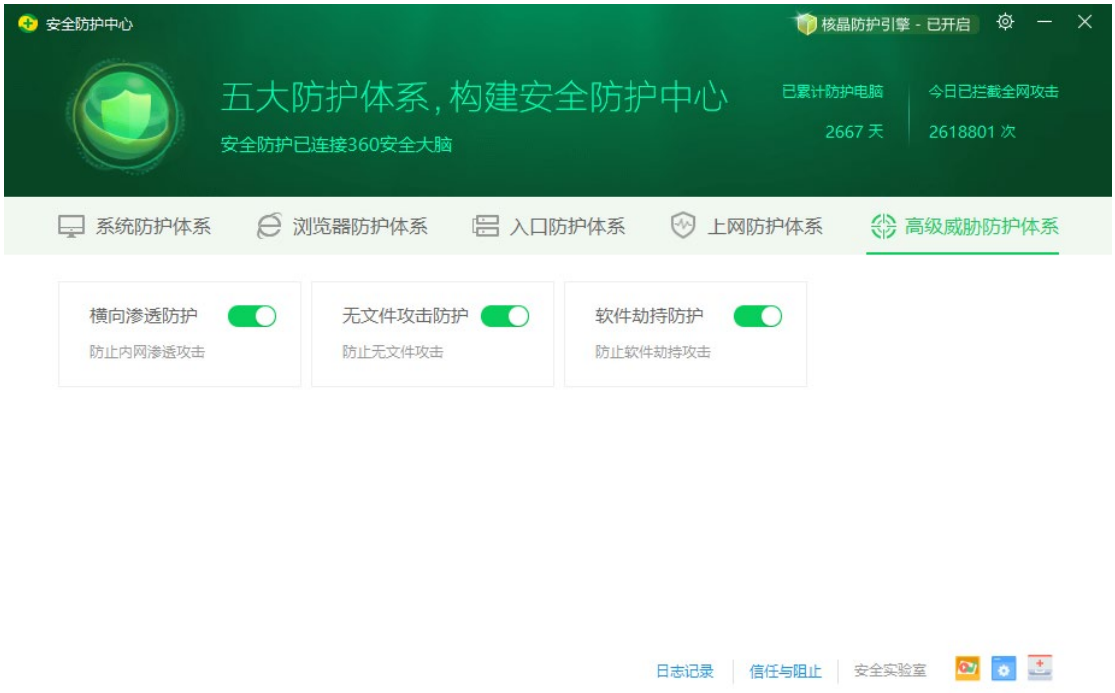
二、 横向渗透防护能力

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。勒索病毒攻击团伙，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

三、 漏洞防护能力

新增漏洞拦截能力（部分重要功能）：

- 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

四、 提权攻击防护

勒索病毒执行过程中，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

五、 挂马网站防护能力

针对包括勒索病毒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病毒的重要渠道之一，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

六、 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 安全卫士提供的勒索病毒解密工具，是目前全球范围内支持解密类型最多的一款解密工具。

2021 全年 360 解密大师共计更新版本 5 次，新增 7 个家族、变种的解密，累计支持解密勒索病毒超过 350 种，2021 年全年服务用户超 16800 台次，解密文件近 395 万次，挽回损失超 2 亿元人民币（除 Stop 家族按单笔 490 美元估算外，其它家族按均价 3000 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。

下图给出了 360 解密大师在 2021 年全年，成功解密被勒索病毒感染的文件和机器数量的 Top10。其中，GandCrab 由于本身感染基数大且全部版本均已有可靠的解密方案，所以占比最多。

数据来源：反勒索服务统计数据

附录4. 360 勒索病毒搜索引擎

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 2021 年全年勒索病毒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：

- **已锁定**
  “已锁定”成为关键词主要由于被加密文件带有 “已锁定”，该关键词属于“已锁定”勒索病毒家族。该家族转播者通过在一款“高铁采集器”上进行推广，诱导用户下载带有勒索病毒的 VPN 程序。

- **devos**
  该后缀有两种情况，均因被加密文件后缀会被修改为 devos 而成为关键词。

  1. 属于 phobos 勒索病毒家族，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。

  2. 属于 Cryptojoker 勒索病毒家，通过“匿影” 进行传播。

- **eking**
  属于 phobos 勒索病毒家族，由于被加密文件后缀会被修改为 eking 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。

- **Stop**
  Stop 勒索病毒家族，该家族的变种几乎每周都会更新，涉及到的后缀有 300 多个，主要的传播方式为：伪装成破解软件或者激活工具进行传播。

- **hauhitec**
  属于 YourData，由于被加密文件后缀会被修改为 hauhitec 而成为关键词。通过”匿影”

僵尸网络进行传播。

- **Makop**

  该后缀有两种情况，均因被加密文件后缀会被修改为 makop 而成为关键词：

  1. 属于 Makop 勒索病毒家族，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。
  2. 属于 Cryptojoker 勒索病毒家，通过”匿影” 进行传播。

- **Lockbit**

  属于 Lockbit 勒索病毒家族，由于被加密文件后缀会被修改 lockbit 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。

- **520**

  属于 BeijingCrypt 勒索病毒家族，由于被加密文件后缀会被修改 520 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。

- **GlobeImposter-Alpha666qqz**

  属于 GlobeImposter 勒索病毒家族，由于被加密文件后缀会被修改为 GlobeImposter-Alpha666qqz 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以及通过 SQLGlobeImposter 渠道进行传播。

- **eight**

  同 eking。