2020 年

勒索病毒疫情分析报告

360 政企安全反病毒部

2021 年 1 月

前　言

本次报告根据 2020 年全年 360 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。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 2020 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分析，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

- 2020 年国内勒索病毒攻击态势未见大规模爆发，但总量并无明显降低，与往年大体持平。
- 2020 年 360 反勒索服务共接收并处理了约 3800 例勒索病毒攻击求助，其中超过 3700 例确认遭受勒索病毒攻击。最终帮助超过 260 例反馈用户完成文件解密工作。
- 2020 年国内流行勒索病毒家族以 phobos、GlobeImposter、Crysis 为主，这三大勒索病毒家族的受害者占比约为 52.46%。世界范围内，以泄露数据敲诈为代表的二次勒索形式日渐兴起，这之中 Maze、Egregor、Conti 三款勒索病毒的占比超过了 50%。
- 超过六成半的勒索病毒依靠远程桌面入侵方式传播。而共享文件夹在今年成为了文件被加密的第二大因素，同时各种破解软件和激活工具导致的勒索病毒传播问题仍不容小觑。
- 勒索病毒所攻击的地区以数字经济发达和人口密集地区为主，全年受到攻击最多的省市前三为：广东、浙江、江苏。
- 被勒索病毒感染的系统中 Windows 10 系统占比最高，占到总量的 31.14%。在系统分类中，服务器系统占比继续保持近年来持续升高的态势，占到总量的 38.99%。
- 据统计，2020 年受到勒索病毒攻击最多的行业前三分别为：服务业、制造业、餐饮与零售业。而受到勒索病毒引发的数据泄露问题影响最严重的行业前三则分别是：服务业、加工制造业、金融与贸易产业。
- 根据反勒索服务的反馈数据统计，男性受害者占到了 93.83%，女性受害者则仅为 6.17%。
- 根据反勒索服务的问卷数据统计：98.19%的受害者在遭到勒索病毒攻击后，选择不向黑客支付赎金；近半数的受害者在受到攻击后会首先进行全盘的杀毒；而对于受害者而言，最重要的前三种文件类型分别是：办公文档、视频图片、邮件或聊天记录。
- 根据被攻击机器中的入侵记录统计，2020 年投放勒索病毒的攻击 IP 来源国前三分别是：美国、法国、俄罗斯。
- 2020 年勒索病毒的攻击手段全线“开花”，弱口令攻击、横向渗透、钓鱼邮件、漏洞利用、网站挂马、破解或激活工具、僵尸网络、供应链攻击等手段悉数登场。
- 2021 年勒索病毒形势依然严峻，经过多年的持续运营和技术沉淀，勒索病毒逐渐朝着影响扩大化、勒索手段多元化、攻击方式专业化的方向发展。
- 在勒索病毒发展的同时，无论是厂商层面的技术对抗还是政府层面的治理活动，都有了显著的加强和卓有成效的成果。相信这种相互对抗趋势在短时间内不会有显著的改观。

目　　录

第一章 勒索病毒攻击形势

2020 年全年，勒索病毒的传播和感染事件虽未再次出现引发全社会关注的爆发性事件，但与往年相比亦未有明显下降——总体而言 2020 年的勒索病毒攻击态势与往年大体相当。根据 360 安全大脑统计，2020 年共处理反勒索服务求助案例 3800 余例。案例数量上相较去年出现了一定程度的下降，但由于反馈案例中企业大量设备中招情况较多，故反馈数量的下降并不意味着受攻击的设备在减少。

本章将针给出 2020 年全年 360 政企安全检测到的勒索病毒相关数据，并进行分析和解读。

一、 反勒索服务处理情况

2020 年全年,360 反勒索服务平台、360 解密大师两个渠道(不包括来自 360 论坛求助反馈)，一共接收并处理了近 3800 位遭受勒索病毒攻击的受害者求助，其中超 3700 位经核实确认为遭受了勒索病毒的攻击。通过以上反馈渠道，反勒索服务共帮助超 260 位用户完成文件解密。

下图给出了在 2020 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。其中三月、四月反馈量最高，主要因为 WannaRen 家族中招反馈造成。

数据来源：反勒索服务统计数据

2020 年新增多款国产勒索病毒。其中：

1 月有“已锁定”家族，传播者通过在一款“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；

2 月新增有“HackedSecret”家族，隐藏在一款刷分软件中进行传播；

3 月出现的 One-OAPlugins 家族，利用通达 OA 的文件上传漏洞进行传播等；

4 月，则是被勒索病毒感染最多的一个月，感染量主要是来自于通过“匿影”进行传播的新兴勒索病毒家族 WannaRen；

5 月新增有 BalaClava 家族通过暴力破解远程桌面进行传播；

6 月新增有 Avaddon 家族通过 Phorpiex 僵尸网络进行传播；

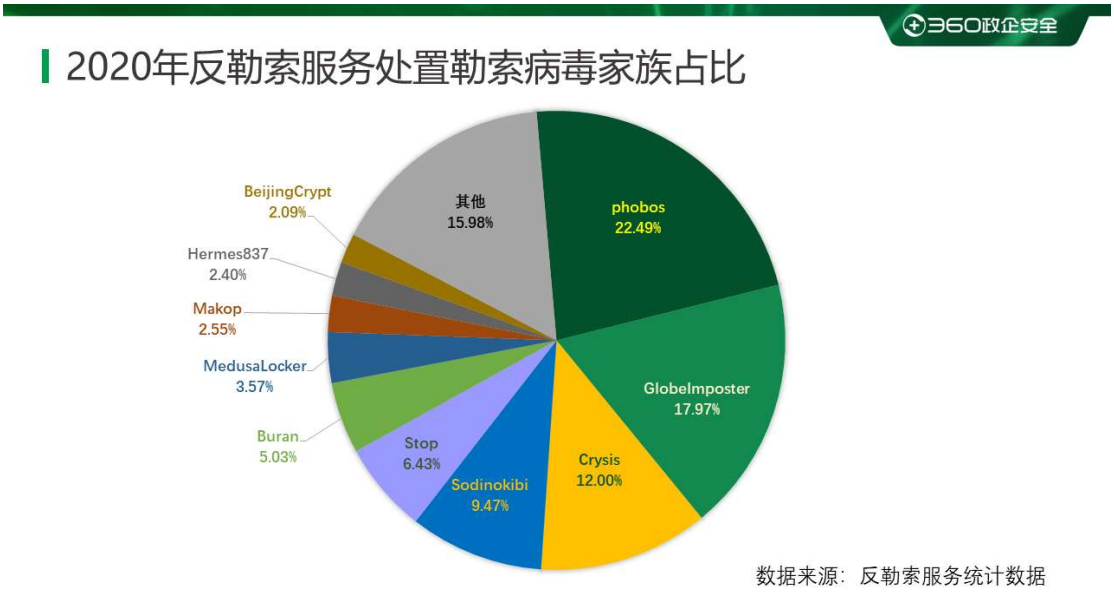
7 月新增家族中有两个家族影响较大，其中一个家族为 Panther 家族，通过供应链攻击进行传播，另一个为 BeijingCrypt 家族，通过暴力破解远程桌面口令进行传播；

8 月份一款名叫“Pojie”的勒索病毒通过伪装成“酷 Q”软件、在论坛发布“有偿修改代码”、“有偿脱壳”等方式进行传播；

9 月到 12 月，发生了多次勒索病毒团伙，在发起勒索病毒攻击之前，窃取用户大量数据，用做二次勒索。其中涉及到的勒索病毒家族已达 21 个，受害公司高达 1000 多家。其中本田、佳明、海力士等名列其中。

二、 勒索病毒家族分布

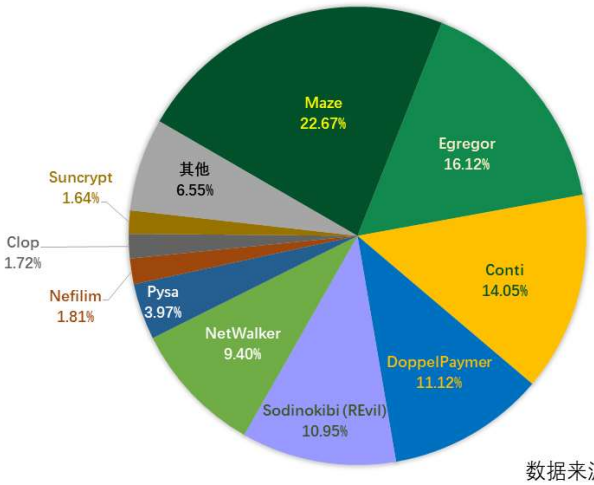
下图给出的是根据 360 反勒索服务数据，所计算出的 2020 年全年勒索病毒家族流行度占比分布图，PC 端 Windows 系统下 phobos、GlobeImposter、Crysis 这三大勒索病毒家族的受害者占比最多，合计占到了 52.46%。TOP10 的勒索病毒家族中，仅 BeijingCrypt 勒索病毒为本年新增家族，其他勒索病毒均在去年甚至几年前便一直活跃。其中的 TOP3 和去年的 TOP3 相同，均为 phobos、GlobeImposter 和 Crysis 勒索病毒家族，但三者总感染占比有所上涨。



通过对黑客发布泄露数据网站进行跟踪，所统计到的勒索病毒家族分布情况，（数据参考@darktracer_int 整理内容）。通过统计图分析参与数据泄露的家族已达 20 多个，有超过

1000 多个受害者，其中 99%的受害者为公司，且不乏大型企业，例如：富士康、佳明、海力士、LG 等。2020 年全年涉及数据泄露的勒索病毒家族占比前三依次为：Maze 家族占比 22.67%、Egregor 家族占比 16.12%、Conti 家族占比 14.05%。其中 Egregor 家族是在 Maze 逐渐退出历史舞台时才出现的一个家族，该家族被猜测为 Maze 家族的“继承者 ”。

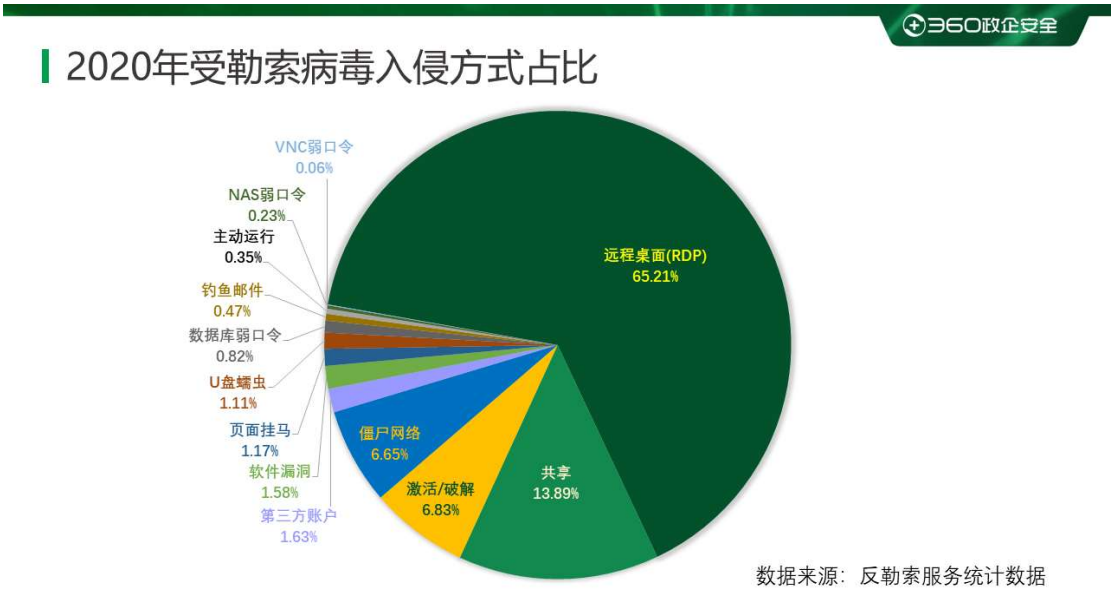
2020年通过数据泄露获利的勒索病毒家族占比



数据来源：@darktracer_int (Twitter)

三、 传播方式

下图给出了攻击者投递勒索病毒的各种方式的占比情况，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法。共享文件夹被加密，成为危害用户数据安全的第二大因素。设置共享文件需谨慎，可通过其他方式来实现文件同步、协作，例如：企业云盘。破解软件与激活工具仍是影响个人用户安全的重要风险因素，运行激活、破解工具之前应在有安全软件防护状态下进行，不应轻易将其加入信任区。



数据来源：反勒索服务统计数据

第二章 勒索病毒受害者分析

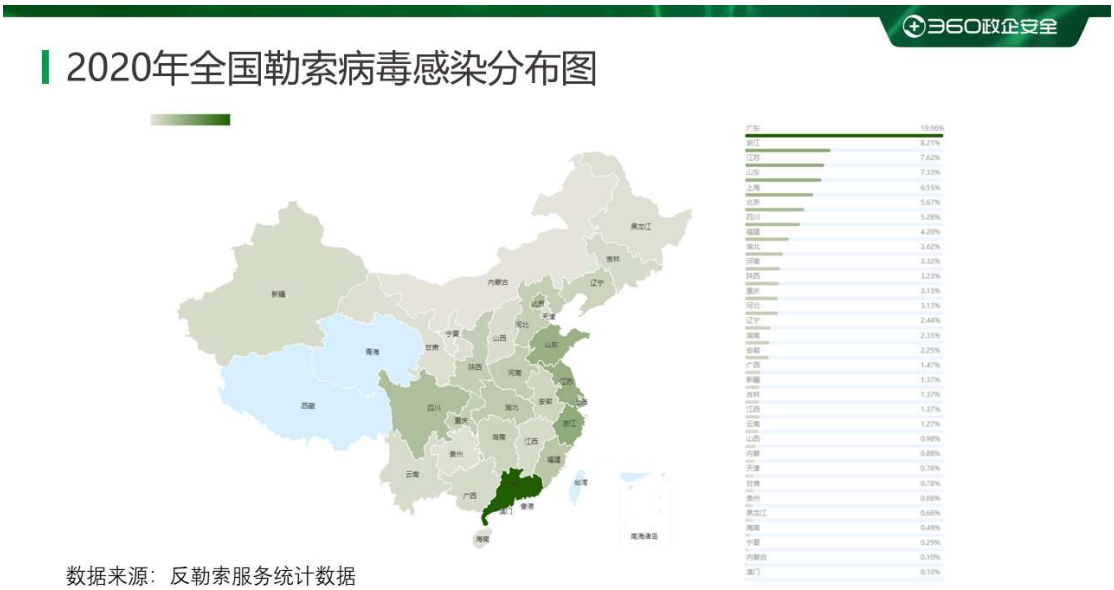
基于反勒索服务数据中求助用户所提供的信息，我们对 2020 年全年遭受勒索病毒攻击的受害人群做了分析。在地域分布方面并没有显著变化，依旧以数字经济发达地区和人口密集地区为主。而受感染的操作系统、所属行业则受今年流行的勒索病毒家族影响，与以往有较为明显的变化。勒索病毒反馈者性别依旧以男性为主。

一、 受害者所在地域分布

360 安全大脑监测显示，2020 年反馈中招案例排名前十的地区中，广东地区占比高达 19.06%。其次是浙江省占比 8.21%，江苏占 7.62%。Top10 地区与以往数据区别并不大，依然是传统的勒索病毒高发区域。下图给出了被感染勒索病毒最多的前十个地区的占比情况。

数据来源：反勒索服务统计数据

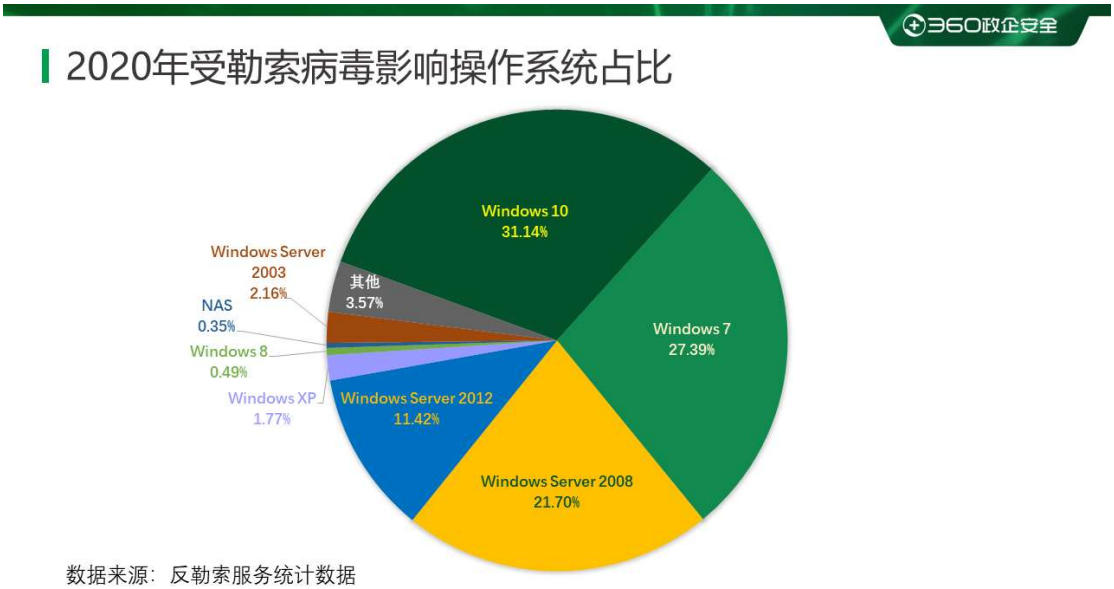
2020 年全年受害者地区占比分布图如下。其中信息产业发达地区和人口密集地区是被攻击的主要对象。



数据来源：反勒索服务统计数据

二、 受攻击系统分布

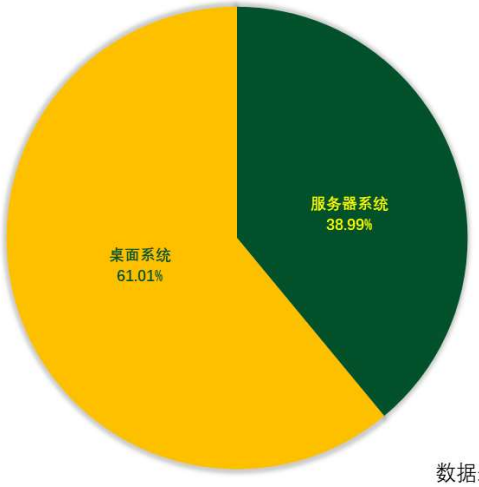
基于反勒索服务数据统计，被勒索病毒感染的系统中 Windows 10 系统占比最高，占到总量的 31.14%，而第二名的 Windows 7 系统占比仅有 27.39%。这与往年数据有较大的变化——2019 年受勒索病毒攻击的系统中超过四成是 Windows 7 系统，由此可推测在 2021 年使用 Windows 10 操作系统的人数会进一步上升。



数据来源：反勒索服务统计数据

而根据对系统类型进行统计发现，虽然桌面系统的占比依然是绝对多数，但服务器占比有升高，从 2019 年的 29.4%上升至今年的 38.99%。

2020年受勒索病毒影响操作系统类型占比

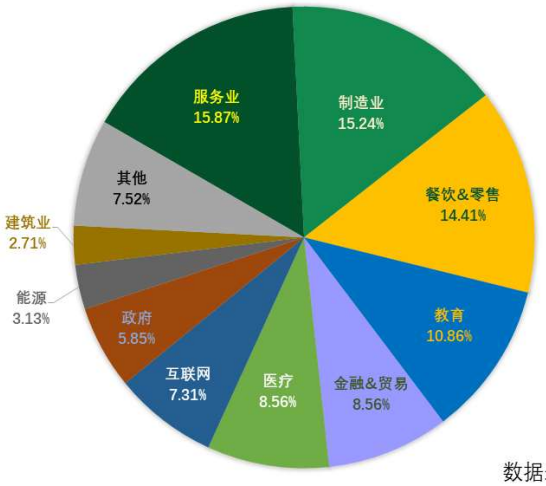


数据来源：反勒索服务统计数据

三、 受害者所属行业

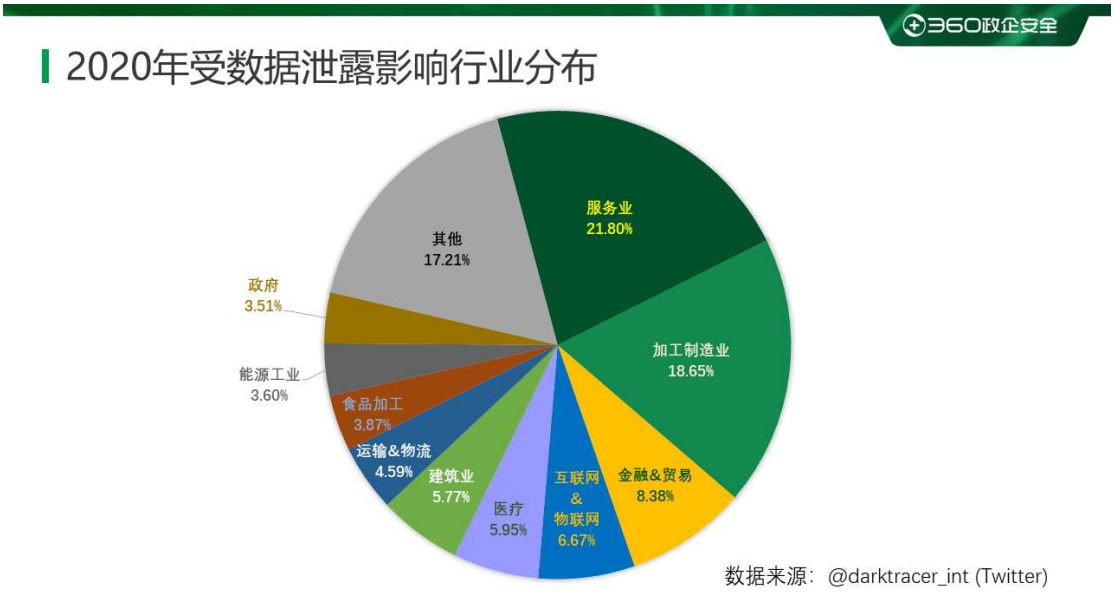
下图给出了受勒索病毒攻击的受害者所属行业分布情况。根据反馈数据统计显示，2020 年最易受到勒索病毒攻击的行业前十，分别为：服务业、制造业、餐饮&零售、教育、金融&贸易、医疗、互联网、政府、能源、建筑业。

2020年受勒索病毒影响行业分布



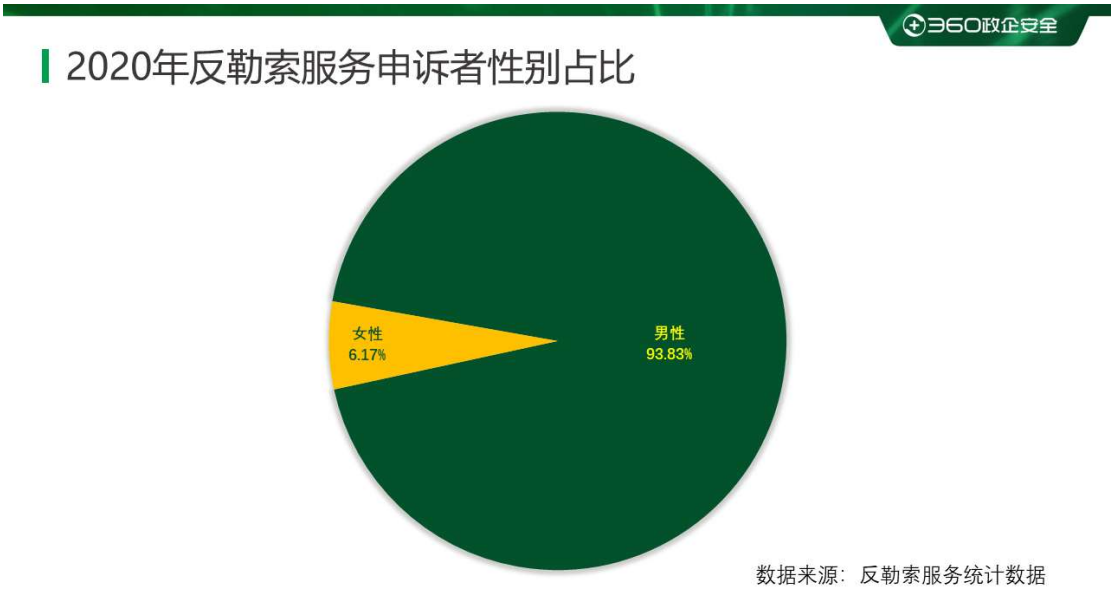
数据来源：反勒索服务统计数据

在 2020 年，数据泄露案例屡见不鲜，对数据泄露网站的公布名单进行统计发现服务业被攻击占比最高，占比 21.80%，服务业中的律师行业被攻击的概率较高；加工制造业以占比 18.65%位居第二；金融&贸易以 8.38%位居第三。（该数据来自@darktracer_int）



四、 受害者性别分布

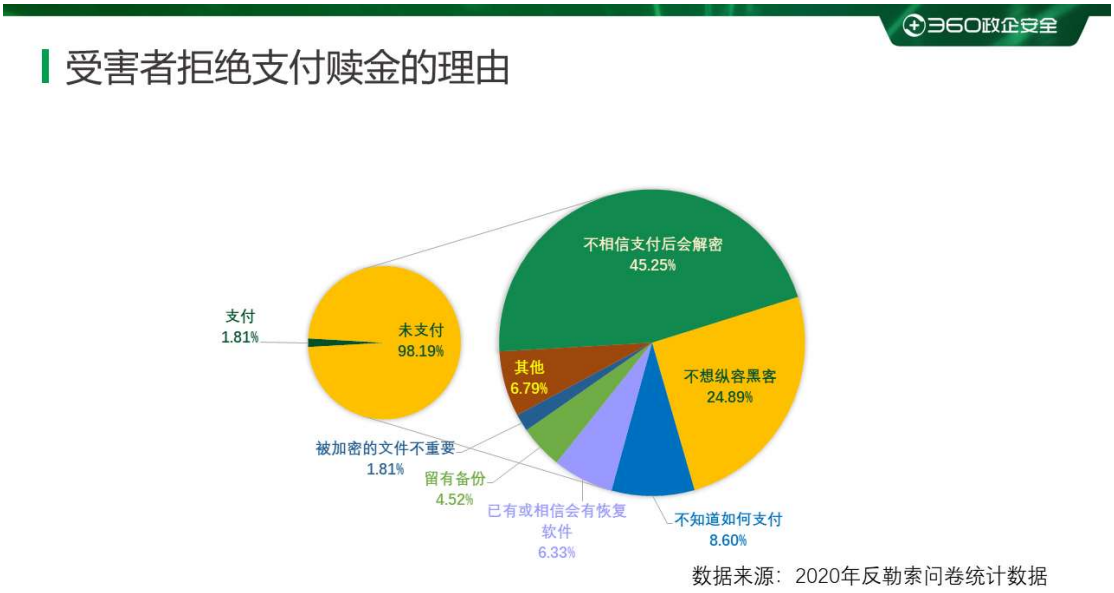
下图展示的是 360 反勒索服务平台求助用户的性别分布情况。



造成求助者男女占比悬殊的原因主要有二点：其一、与计算机接触最为频繁的 IT 技术行业或 IT 运维类岗位的男性员工占比明显多于女性。其二、很多女性用户遇到病毒问题，往往会优先选择寻求身边男性朋友的帮助。

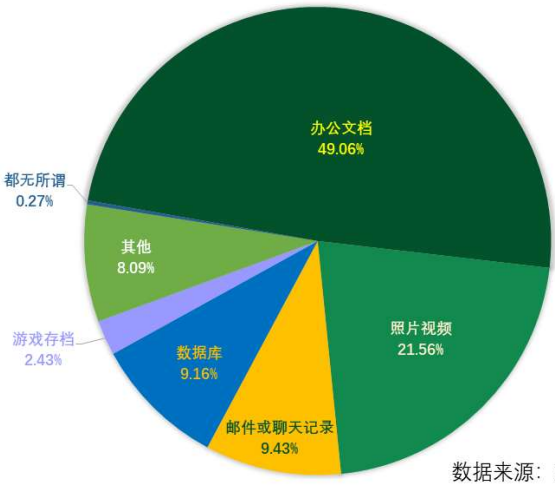
五、 受害者遭受攻击后的应对方式

360 政企安全反病毒部在受理用户的反馈同时，也对受害者进行了一定规模的问卷调查。根据问卷内容，我们发现超过 98%的用户并不会选择以任何的方式向黑客支付赎金。而在进一步询问为何不愿支付赎金后，得到的答复超过 45%是不相信支付赎金之后黑客会信守承诺为自己解密，还有将近 25%的受害则是单纯的不想纵容黑客的这种行为，而又 8.6%的受害者则是单纯的对比特币、门罗币一类的虚拟货币不会操作，想支付却无从下手。



此外，我们还对不同类型的文件重要程度进行了调查。发现近半数的受害者认为办公文档是最无法承受的损失；超过 20%的受害者则认为照片、视频的加密是最不可接受的；而认为“数据库”和“邮件或聊天记录”是最重要文件类型的受害则，则均在 9%以上。由此可见，有近 7 成（办公文档、邮件或聊天记录、数据库三项）用户认为工作相关的数据是最重要且绝不能接受损失的。

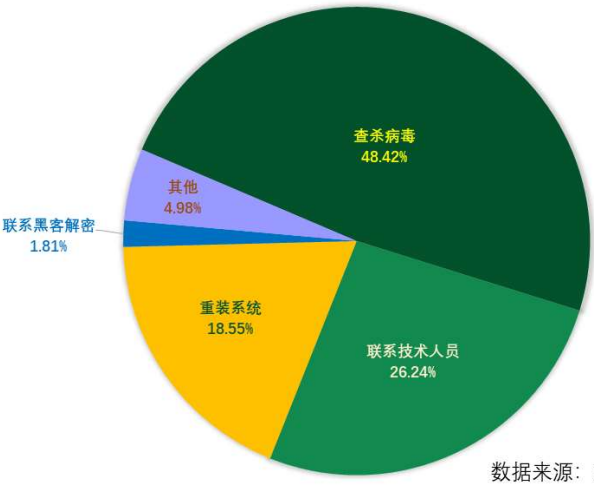
受害者认为最重要文件类型



数据来源：2020年反勒索问卷统计数据

最后，我们询问了受害者在遭受攻击后，首先采取了何种措施。发现有接近 50%的受害者第一反应是使用安全软件进行病毒查杀，而超过 26%的受害者则选择了联系技术人员寻求帮助，以上两种方式都属于较为合理的处理方案。但也有超过 18%的受害者在发现受到攻击后首先选择重装系统，这种方法虽然可以短期解决问题，但并不利于后期对文件的恢复，同时如果不查清中招原因，修补存在的安全漏洞，再次中招的概率将大大增加，建议大家谨慎操作。

受害者遭受攻击后的应对方法



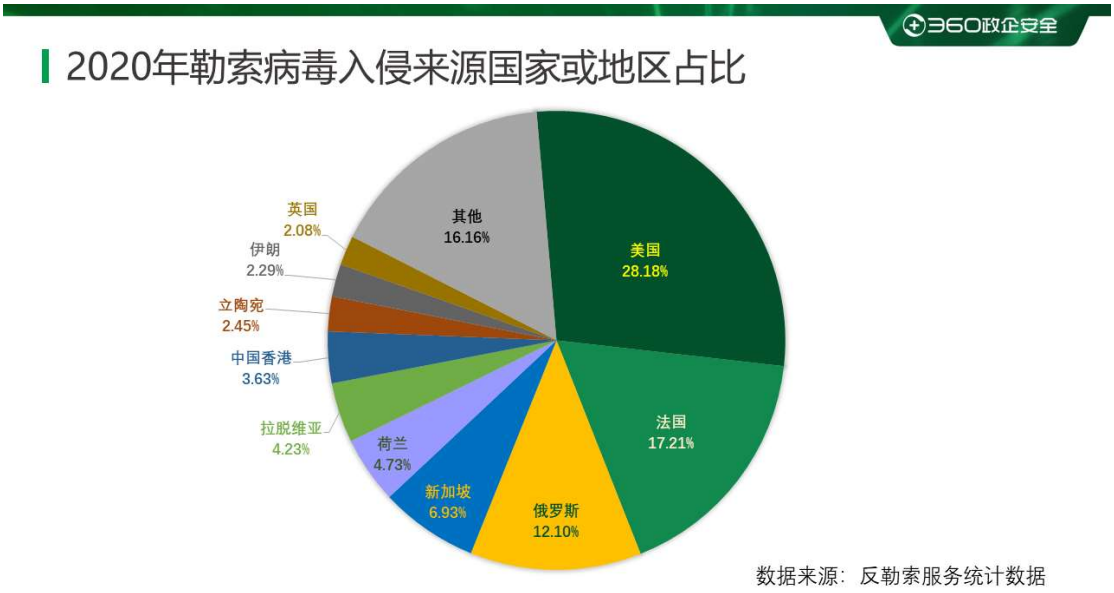
数据来源：2020年反勒索问卷统计数据

第三章 勒索病毒攻击者分析

2020 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直接投毒的方式进行传播，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、洋葱网络聊天室以及 Telegram；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

下图给出了 2020 年全年黑客使用过的 IP 地址对应国家或地区信息（IP 数据来自被攻击者的系统日志）。根据统计可以发现黑客登录受害者机器时，来源地址多为美国、法国以及俄罗斯的 IP。但此处必须说明的是：黑客使用的 IP 对应国家或地区不一定就是攻击者所处的真实国家或地区。使用代理服务器做跳板发起攻击，也是攻击者隐藏自身的一种常规手段。

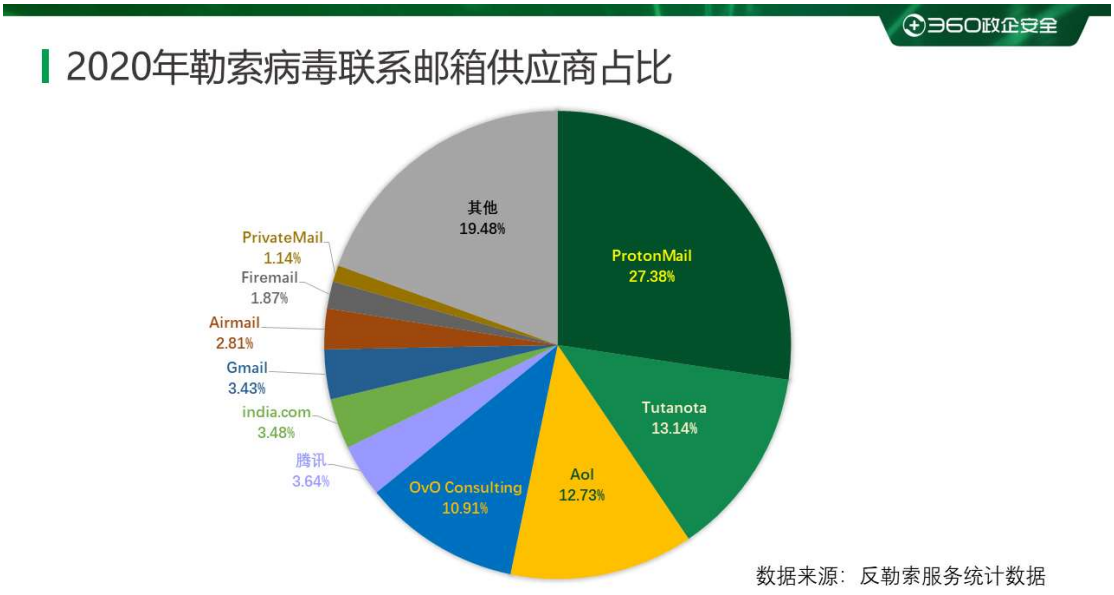


数据来源：反勒索服务统计数据

二、 勒索联系邮箱的供应商分布

虽然仍有一些勒索病毒在选择使用暗网聊天工具等更加隐蔽的方式与受害者进行沟通，但越来越多的攻击者会在加密文件后留下邮箱地址，方便用户联系支付赎金。

通过分析相关数据，我们发现勒索病毒作者更偏爱 ProtonMail、Tutanota、Aol 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。



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 9 个家族均涉及到弱口令攻击传播，其中 8 个家族弱口令攻击是其主要传播手段。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。

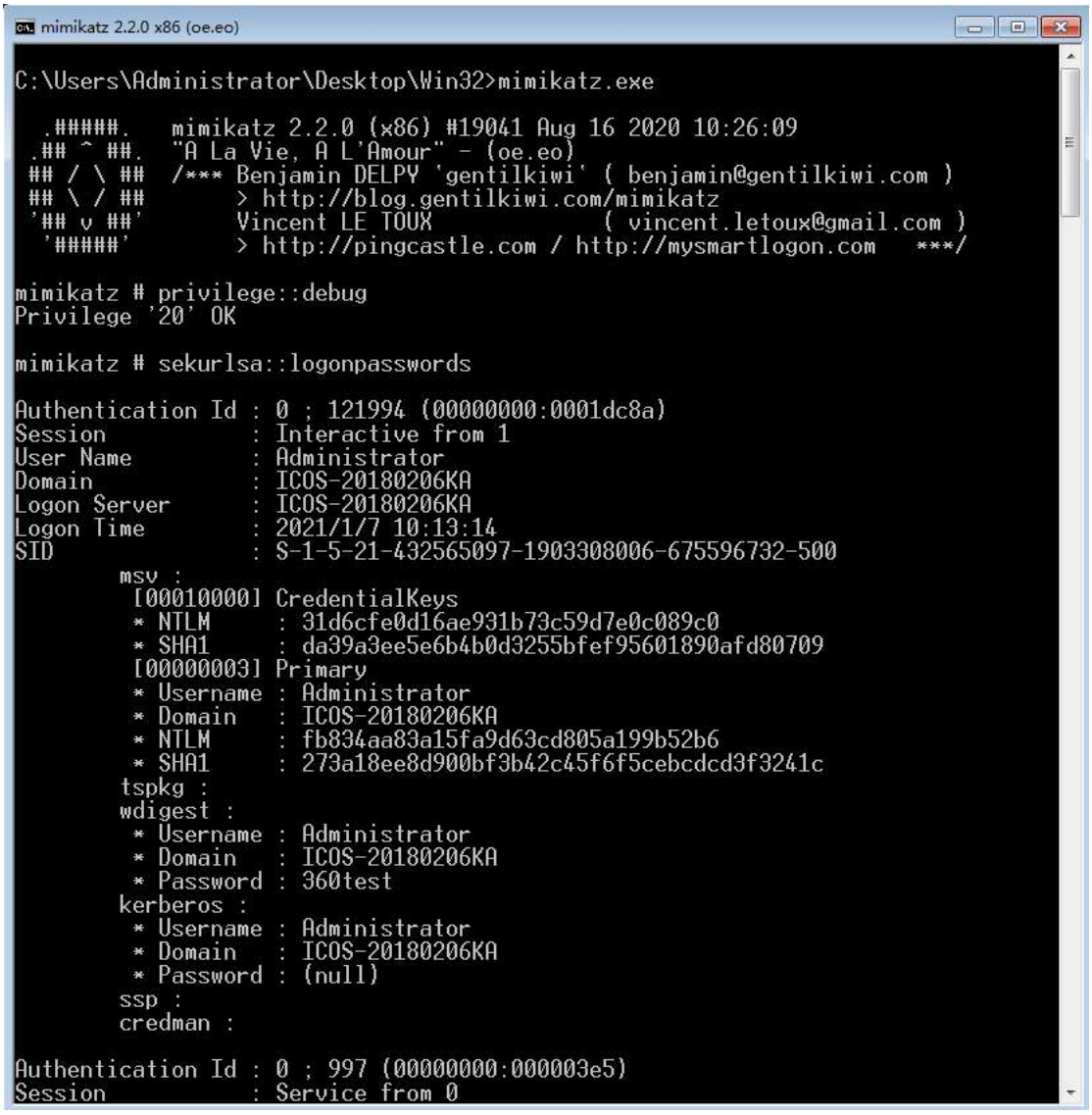
(二)横向渗透

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，对企业的勒索也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。

而很多企业内网脆弱，经常缺乏明确的网络划分和业务布局规划，各部门和各类业务没有做功能区分隔离，账号权限控制不当。这造成企业内网经常出现拿下一个点之后，黑客便可以“一马平川”横扫整个内网的现象。比如 Clop 勒索病毒团伙，其攻击团伙在拿下企业一台设备后，会通过抓密码、扫端口的方式探测内网其它机器，并寻找机会攻击企业域控服务器。在拿下域控之后，便控制整个网络投递病毒。

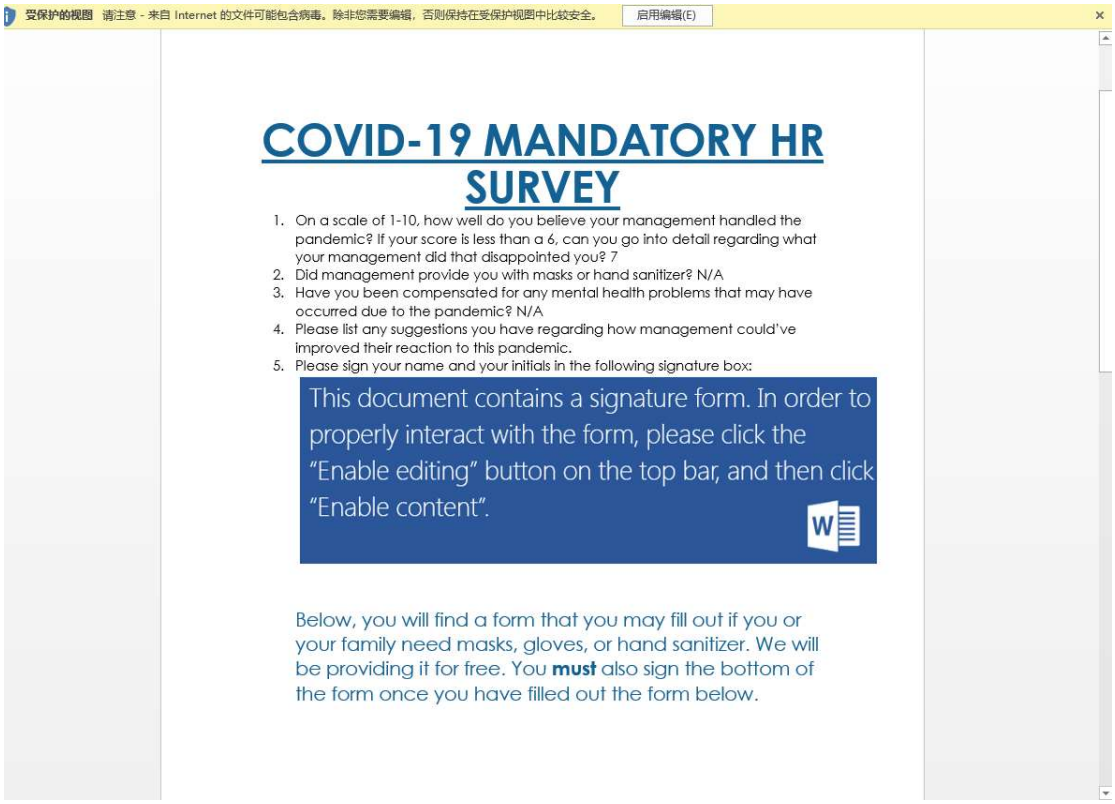
下图展示了通过 mimikatz 抓取当前计算机账户密码的过程。



(三)钓鱼邮件

钓鱼邮件一直以来都是各类病毒投递的主要渠道之一，早期（2015 年-2016 年）国内勒索病毒的主要传播源便是境外钓鱼邮件，攻击目标则主要是外贸企业。目前钓鱼邮件虽然已不是勒索病毒传播的第一大威胁因素，但在国内病毒攻击中依然能非常普遍的监测到。

“钓鱼邮件”通常使用具有诱惑力的邮件标题、内容、附件名称等，诱骗用户打开木马站点或者带毒附件。例如今年就出现使用 COVID-19 相关内容主题做为钓鱼诱饵的攻击，使用的主题有：“疫苗、口罩供应不足”、“健康调查报告”、“冠状病毒最新信息”等，攻击者总是能找到最引人关注的话题，诱骗被攻击者打开钓鱼邮件。根据 Health IT Security 报告，从一月到四月，国际刑警组织仅在该机构的合作伙伴中，检测到约 907,000 封垃圾邮件，737 恶意软件相关事件，以及 48,000 个恶意 URL 与 COVID-19 关联。



(四)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。漏洞利用最知名的案例莫属 WannaCry 勒索病毒了。该病毒使用 NSA 泄露的 EternalBlue 漏洞传播，短时间内便席卷全球。

目前，黑客用来传播勒索病毒的系统漏洞、软件漏洞，大部分都是已被公开且厂商已经修补了的安全问题，但并非所有用户都会及时安装补丁或者升级软件，所以即使是被修复的漏洞（Nday 漏洞）仍深受黑客们的青睐。一旦有利用价值高的漏洞出现，都会很快被黑客加入到自己的攻击工具中。例如，今年 7 月 Satan 勒索病毒投递，就是使用的泛微 OA 系统漏洞。而之后，又出现有利用通达 OA 系统漏洞传播的 One-OAPlugins 勒索病毒。利用漏洞传播，可在较短时间内攻陷大量机器，造成的损失也相对较大。

(五)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

与其它攻击手段伴随使用，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。而通过诱导方式发起攻击，多和钓鱼网站结合，如年初受新冠感染影响最严重的国家之一的意大利，就有攻击者创建了一个模仿意大利药剂师联合会网站的网页，用虚假的新冠感染趋势图，诱骗用户安装网站中的勒索病毒。

(六)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，伪装成 KMS 激活工具、adobe 系列软件破解工具等传播。Pojie 勒索病毒，通过破解软件“酷 Q 本地授权版”利用 IM 工具传播。当用户下载使用这些软件是，病毒便被激活，感染用户计算机，加密计算机中的文件。下图即为一款携带了勒索病毒的破解软件。

(七)僵尸网络

僵尸网络可以说是黑客最热衷的一种攻击工具，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。

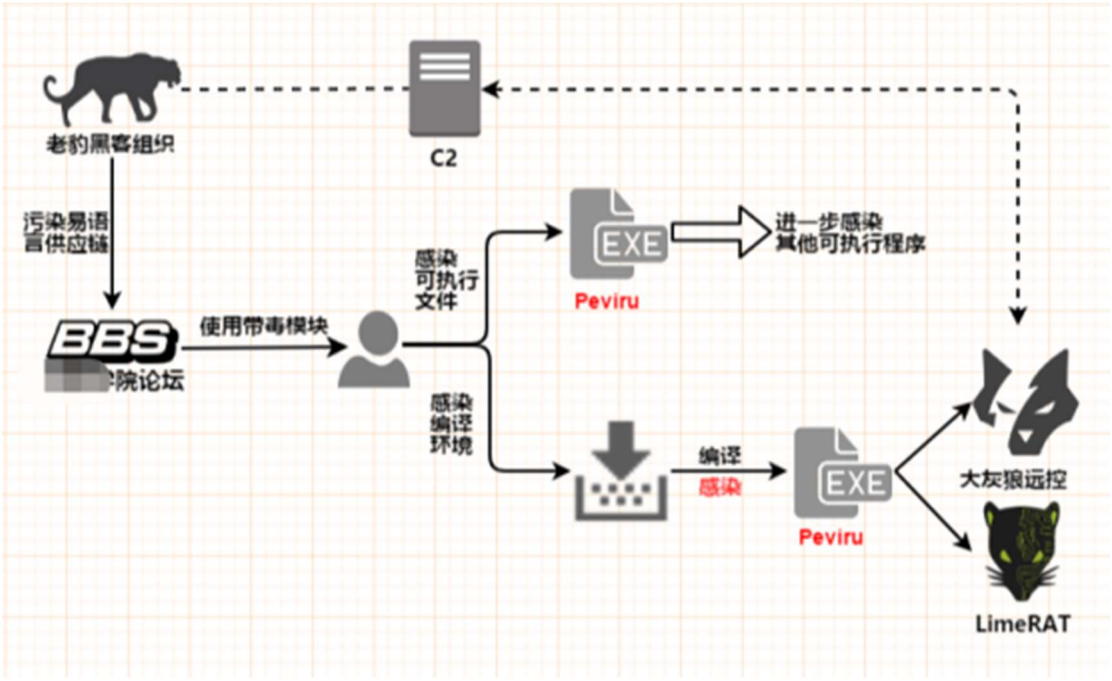
国内流行僵尸网络“匿影”便是其中一只，它通过控制的数十万客户端发起扫描攻击、推广软件、下发病毒木马。在今年 4 月，名噪一时的 WannaRen 勒索病毒便是通过该僵尸网络下发的，而在今年 11 月该僵尸网络又下发了 WannaRen 二代、CryptoJoker 勒索病毒，后续还陆陆续续对病毒做了多次更新。

(八)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 组织用来作为攻击工具。比如 2020 年底震动整个安全圈的 SolarWinds 供应链攻击——手法隐蔽，攻击持续了近一年时间。受影响大型公司、政府部

门有上千家之多，足见其威力巨大。

在勒索病毒攻击方面，来自供应链污染，造成的攻击也时有发生。比如今年 7 月发生的 Panhter 勒索病毒攻击事件，攻击者通过在开发论坛发布“带毒功能模块”，诱骗开发者使用其模块。当其他开发者一旦使用了攻击者提供的模块，其开发的软件也会受到感染，携带病毒。当这些携带病毒的软件来到用户电脑中就开始发作，下载勒索病毒执行，感染用户计算机。由于受影响的软件众多，造成大量普通用户受到影响。虽然只是一次小众软件的感染事件，也同样造成了大量设备中招，可见供应链攻击的威胁绝不容掉以轻心，万幸 360 解密大师提供了对该病毒的解密支持。下图展示了一次供应链污染攻击的全过程：



第四章　勒索病毒发展趋势分析

2020 年，勒索病毒威胁再次领跑了最热门网络安全话题，结合信息泄露的二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、　勒索病毒攻击技术发展

（一）影响扩散，从网络世界扩散到现实生活

2020 年，新冠疫情深刻影响了大众的生活、工作方式，线上办公、远程会议、各类智能识别技术等信息技术手段都参与到了我们现实生活的世界中。在我们享受信息技术带来的便利的同时，伴随而来的网络攻击——尤其是勒索病毒攻击，对现实生活秩序的影响力也越来越大。回顾过去一年的攻击事件，除了一般企业机构，还有很多市政机构、医院、学校、警察部门等公共机构遭到攻击。例如今年 9 月，德国杜塞多夫大学医院遭勒索软件攻击之后转院的病人因抢救不及时死亡。而国内的情况也不容乐观，企业、医院、政府部门因勒索病毒原因停工、停产、业务暂停的情况也有发生。勒索病毒不再只是一个安全行业的词汇，也更多的影响着普通大众。

（二）次生灾害加剧，信息泄露成为年度热点

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 Maze 率先尝试通过泄密实施勒索，在加密勒索的同时也会窃取数据，并以公开数据为要挟迫使企业就范。如佳明公司，就因此被迫支付了赎金。

而这一趋势在2020年愈演愈烈，在Maze的带领下有超过20个流行家族——例如Conti、Sodinokivi、Clop 等——都开始以窃取和泄露数据作为胁迫筹码，这也更加剧了攻击的危害和企业的担忧。

（三）攻防加剧，高级威胁、定向攻击手段层出不穷

从病毒特征的免杀对抗，到传播渠道拓展，勒索病毒在发展过程中技术手段不断加强。各种高级威胁的技术手段也在勒索病毒的传播中得到应用。如 REvil 团伙在 2020 年 3 月利用 Weblogic 漏洞结合无文件攻击技术传播 Sodinokibi 勒索病毒。Nday 乃至 0day 漏洞也被更多的应用于传播链条之中。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，攻击者已经控制企业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。当攻击者掌握足够设备和数据之后，才会发起最后的攻击。

攻击范围方面，针对大型企业的定向攻击也频繁发生。暗网公开的被攻击企业数据中，包含大量世界 500 强企业和知名跨国企业，比如惠而浦、本田、佳能都在其名单中。大型企业成为攻击目标，主要是其具有较高的支付能力和支付意愿。病毒在攻击成功后，动辄开价

上千万美元，有的甚至上亿美元。部分勒索病毒家族，攻击的行业属性也比较明显，例如GlobaImposter 针对医疗行业的攻击就较为频繁。这一点也与攻击团伙的技术手段有关，特定行业有着类似的 IT 部署方案和 IT 系统甚至使用相同的系统集成商设备，这样同样的防护弱点就可能在同行业的多家企业中同时出现。一个攻击团伙在拿下一家企业之后，能够如法炮制的攻击行业内的其它企业。

此外，虽然针对 Windows 平台的勒索病毒仍然是当前主流，但其它平台下的勒索病毒攻击也并不少见。目前在 Android、MacOS、Linux 等平台上的勒索病毒攻击事件也时有发生。而被打击的目标，也不再只局限于计算机，数据库、各种嵌入式设备、专用设备上也被曝出受到勒索病毒攻击影响。

(四) 勒索和挖矿成为网络攻击的两大变现渠道

勒索病毒和挖矿木马的经久不衰，其中一个原因就是他们为网络攻击提供了一种快速稳定的变现方式。相比传统的变现方式，如抓“肉鸡”、建设僵尸网络、数据窃取倒卖、虚拟财产窃取、流量倒卖，不仅对规模和设备资产情况有要求，而且涉及环节较多操作复杂且暴露风险高。而勒索病毒的变现方式更为粗暴直接，正被越来越多的网络“灰黑”产采用。

另一方面，勒索和挖矿本身也经常相伴相生，在被勒索病毒攻击的机器上，经常能看到曾经投递挖矿木马的身影，两者的攻击团伙也有很大重叠。

(五) 勒索软件即服务（RaaS）被广泛使用

不论是最近两年新增的勒索病毒，还是之前勒索病毒的新变种，越来越多的勒索病毒作者开始尝试通过 RaaS 的方式来分发其病毒程序。而这一趋势不仅给勒索病毒制作者之间增加了一些竞争，也让黑产从业人员获取勒索病毒变的更加方便，进一步加剧了勒索病毒的传播。勒索病毒制作、传播、获利的整个链条分工更趋于清晰明确。

另外，在一些针对地区基础设施的攻击中，也出现了勒索病毒的身影，这一现象的背后，很可能是针对特定地区的破坏行为，而不单单是商业上的勒索。勒索病毒在攻击中扮演了破坏工具的角色，同时还起到了转移视线的作用。

二、 勒索病毒的防护、处置与打击

(一) 勒索病毒防护技术发展

当前，勒索病毒攻击的防御重点是对病毒攻击迹象的早期发现预警，对病毒传播渠道的拦截防护，对主机的安全加固和对被加密文件的解密探索。

依托多年来的技术积累，360 安全卫士在勒索病毒的识别、查杀、拦截方面均有良好表现，攻击者通过免杀来绕过杀软的查杀和防御已经非常困难。目前勒索病毒在投递之前，通常会诱使用户退出安全软件或者攻击者主动关闭杀毒软件来避免病毒被查杀。因此在对抗勒索病毒攻击方面，对用户的安全科普是一方面，对病毒传播渠道的封锁拦截也是重要的一项内容。例如部分勒索病毒会捆绑在一些激活工具中进行传播，在获取用户信任之后依靠用户

手动放行来实施攻击。杀毒软件如果能先于攻击者，在其传播渠道上就进行拦截提示，会取得更好的效果。

企业被攻击的情况，通常包括企业的对外服务器被攻击以及企业内网被渗透两方面。针对服务器的攻击占到整体勒索病毒攻击的 39%以上。服务器由于无人值守又长期暴露于公网之上等原因，造成其被攻击的攻击面相对较大。而服务器被攻击的常见原因包括口令暴破攻击和系统或软件服务漏洞攻击。针对这一系列问题，360 安全卫士提供了“远程桌面暴破防护”、RPC 暴破防护、SMB 协议暴破防护、SQL Server 暴破防护、VNC 暴破防护、Tomcat 暴破防护等一系列防护，同时还增加了对金万维、瑞友的防护支持。在漏洞保护方面，增加有 WebLogic、JBoss、Tomcat 等多种服务器常见软件的漏洞防护，以及大量系统漏洞的防护能力。而针对企业内网被渗透的问题，360 安全卫士新增了横向渗透防护、无文件攻击防护、常用软件保护等安全能力，结合漏洞防护保障企业内网不被轻易拿下。

对被加密文件的破解，一直以来都是勒索病毒攻击处置中用户最关注的问题。360 安全卫士在多年的勒索病毒对抗中积累了丰富经验。目前流行的勒索病毒也并非都无法破解，常见的破解原理包括：

1. 利用泄露的私钥破解。通过各种渠道获取到病毒作者的私钥实现破解。如知名的 GandCrab 勒索病毒的私钥就被警方获取并公开，安全公司因此可以制作解密工具来进行解密。

2. 利用加密流程漏洞进行破解。有部分勒索病毒本身编写不规范，错误使用加密算法或随机数生成算法等，造成加密密钥或关键数据能够被计算获取，从而解密。

3. 明密文碰撞解密。这类解密常用于使用流式加密生成一个固定长度的密钥串，之后加密文件的勒索病毒。通过明密文对比计算从而得到使用的加密密钥，如 STOP 勒索病毒就是使用类似方法进行的破解。

4. 数据修复解密。很多勒索病毒为了保证加密效率不会全文加密，通常会加密头部部分空间，或者加密整个文件的部分片段。由于并非全文加密，对于大文件来说，被加密部分占比空间一般较小。这时候通过一些技术手段对文件进行修复，再依靠文件格式自身的容错能力，可能就能恢复出绝大部分有价值信息。

5. 暴破解密。这类解密也是由于病毒作者对密钥处理的不规范，造成密钥空间不足，为暴破解密提供了可能。常见的如使用时间做种子产生随机数做密钥的情况。

(二)勒索病毒处置服务专业化

目前，勒索病毒的日常排除已经成为企业安全运维的一项基本内容，而勒索病毒响应处置也是一线安服人员的基本功。勒索病毒攻击事件越来越常态化，市场上也出现大量专职处置的公司和团队，来协助公司完成支付解密工作。

市场中原有的一些服务，也开始增加勒索病毒相关的处理能力。如云存储业务、个人的 NAS 文件存储设备都会将数据备份安全性和对勒索病毒的防护效果做为一个宣传亮点。之前主要从事数据恢复的一些厂商，也转型专做勒索病毒相关的恢复工作。

国外针对勒索病毒攻击的保险行业也逐步成熟。在 2017 年时，勒索病毒的攻击事件还属于网络保险的拒赔范围，到 2020 年勒索病毒相关的网络保险已经成为美国网络保险最重要的内容之一。北美最大的网络保险服务提供商之一 Coalition 发布报告表示，勒索软件事件已占 2020 年上半年网络保险索赔金额的 41%，今年国内也有多家保险公司提出了涉及勒

索软件保障的网络保险。

安全公司的处置业务也由之前的查杀病毒、协助解密，逐步扩展为：帮助企业恢复生产、查清原因以及后续的安全加固服务、网络结构规划，服务更趋专业化。安全产品对勒索病毒的防护能力，也成为企业和个人选择安全软件的一个重要关注点。

（三）针对勒索病毒相关的犯罪打击

各国政府对勒索病毒问题的重视程度也在加大，对勒索病毒的打击力度加强。如我们国内，主管单位也发起过“勒索病毒的专项治理工作”，以加强机关单位对勒索病毒的重视程度与防护能力。

其中浙江省公安厅在今年组织的“净网 2020”专项行动就将对勒索病毒的治理纳入其中。在此次行动中，浙江省湖州市警对“已锁定”勒索病毒的作者、传播者以及整个攻击链条进行了全面打击。当地警方在走访了全国 20 多个城市，并对 10 余名受害者进行了询问、调查、取证之后，锁定了分别身处重庆、广州两地的 2 名主要嫌疑人。最终犯罪嫌疑人王某、梁某均落网，并以破坏计算机信息系统罪被刑事拘留。

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。

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，将补丁管理做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) 联系安全厂商，对内部网络进行排查处理。

2) 登录口令要有足够的长度和复杂性，并定期更换登录口令

3) 重要资料的共享文件夹应设置访问权限控制，并进行定期备份

4) 定期检测系统和软件中的安全漏洞，及时打上补丁。

a) 是否有新增账户

b) Guest 是否被启用

c) Windows 系统日志是否存在异常

d) 杀毒软件是否存在异常拦截情况

5) 登录口令要有足够的长度和复杂性，并定期更换登录口令

6) 重要资料的共享文件夹应设置访问权限控制，并进行定期备份

7) 定期检测系统和软件中的安全漏洞，及时打上补丁。

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　2020 年勒索病毒大事件

一、　文档被“已锁定”，中文勒索病毒来袭

2020 年 1 月，大量网友反馈文件被加密，加密后的文件名被更改为“原文件名-(已锁定)”。经技术人员分析发现，“已锁定”勒索病毒主要通过隐藏于一款名为“DVPN”的网络代理软件中进行传播扩散。而为了提高病毒扩散率，不法黑客在破解软件广告页中大肆宣传，以诱导用户前往指定网址下载暗藏勒索病毒的代理软件。

不过该病毒的加密手段并不完善，360 解密大师在捕获病毒后第一时间即完成了对该病毒的解密工作，并在客户端中加入了对该病毒的解密支持。与此同时，分析人员也发现该病毒作者在病毒中留下了一些痕迹，分析人员对这些痕迹抽丝剥茧进行溯源分析，终于根据不法黑客使用的域名，直接追踪到了黑客的注册邮箱，及关联的支付宝微信等个人信息。

随后，浙江警方成立专案组开展侦查，对该勒索病毒的来源、传播及受害人员信息进行深入调查。专案组历时 4 个多月，走访了全国 20 多个地市，对 10 余名被害人制作了笔录，并对被害人所持有的电脑进行详细的勘察、取证。通过分析研判，专案组最终查明了涉案嫌疑人的真实身份，并先后在重庆、广州两地将该案的 2 名主要犯罪嫌疑人抓获。经审讯，主犯王某、梁某二人对制作并推广嵌入了勒索病毒的“DVPN”程序，通过对存储文件进行加密锁定的方式破坏受害人计算机信息系统并勒索比特币赎金的犯罪事实供认不讳。

二、 通达 OA 存在漏洞，勒索病毒横行办公网络

2020 年 3 月，通达 OA 官方发布安全公告，称“收到部分用户反馈遭到勒索病毒攻击”，并针对该事件所设计的产品进行了安全加固。

提醒您及时对OA服务器做好安全防护！

2020-03-13 共 4444 人次阅读此新闻

今日，我们收到部分用户反馈遭到勒索病毒攻击。为此，通达OA产品团队紧急制作了针对勒索病毒的安全加固程序。

请广大用户立即下载更新，另外推荐V11版用户直接更新到11.4.200323版本

通达OA V11版：

https://cdndown.tongda2000.com/oa/security/2020_A1.11.3.exe

通达OA 2017版：

https://cdndown.tongda2000.com/oa/security/2020_A1.10.19.exe

通达OA 2016版

https://cdndown.tongda2000.com/oa/security/2020_A1.9.13.exe

通达OA 2015版

https://cdndown.tongda2000.com/oa/security/2020_A1.8.15.exe

通达OA 2013增强版

https://cdndown.tongda2000.com/oa/security/2020_A1.7.25.exe

通达OA 2013版

https://cdndown.tongda2000.com/oa/security/2020_A1.6.20.exe

具体操作：

请根据当前OA版本号，选择压缩包中所对应的程序文件，覆盖到MYOA\webroot目录下。如不确定，请联系我们售后团队协助处理。

同时建议您定期做好数据备份。避免病毒攻击造成损失。

事件起因是一款勒索病毒利用虚假插件瞄准通达 OA 系统更新程序发动攻击，加密文档类型多达 185 种，加密文件后会在其后缀名末尾增加一个数字 1，并留下勒索信要求用户支付 0.3 个比特币的赎金。

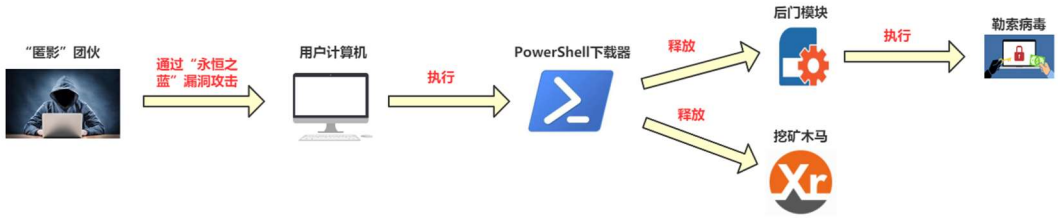
而由于通达 OA 是国内一款常用的办公系统，所以该攻击事件的覆盖面较为广泛。同时，这也是即 2019 年致远 OA 的漏洞被利用作为攻击企业网络通道之后，又一起借助国内知名 OA 系统发起的攻击事件。可见此类 OA 系统的安全问题值得重视。

三、 WannaRen 借“匿影”家族爆发

2020 年 4 月，360 安全大脑监测到一款名为“WannaRen”的新型勒索病毒正在发起攻击。该病毒会加密用户文件之后修改文件后缀为.WannaRen，并在受害机器上随机留下【@WannaRen@.exe】、【想解密请看此文本.txt】、【想解密请看此文本.gif】这三种勒索信息，

要求中招用户支付 0.05 个比特币的赎金。

后经过分析人员的进一步溯源分析，发现“WannaRen”勒索病毒的作者正是此前借“永恒之蓝”漏洞祸乱网络的“匿影”组织。“匿影”黑客团伙主要利用 BT 下载器、激活工具等传播，也曾出现过借“永恒之蓝”漏洞在局域网中横向移动扩散的情况。“匿影”黑客团伙在成功入侵目标计算机后，通常会执行一个 PowerShell 下载器，利用该加载器下载下一阶段的后门模块与挖矿木马。而此次新型比特币勒索病毒“WannaRen”的扩散活动中，从表面看与此前的“WannaCry”病毒类似，都是病毒入侵电脑后，弹出勒索对话框，告知已加密文件并向用户索要比特币。但从实际攻击过程来看，“WannaRen”勒索病毒正是通过“匿影”黑客团伙常用 PowerShell 下载器，释放的后门模块执行病毒。此外，由于该勒索病毒下载器中包含了一个“永恒之蓝”传播模块，使其具备了横向扩散能力。也就是说，内网环境下一旦有设备感染“WannaRen”勒索病毒，既有可能感染未修复“永恒之蓝”漏洞的计算机。这将直接危及企业用户网络安全。



最终“WannaRen”作者不知出于何种目的，主动公布了用于解密的密钥。之后，包括 360 解密大师在内的解密工具也都在第一时间更新了对此病毒的解密支持，整个事件才算是告一段落。

四、 知名网红受到勒索病毒攻击，党妹、歪果仁接连中招

2020 年虽然没有如 WannaCry 一样全球大范围传播的勒索病毒，但知名网红的接连中招依然让勒索病毒攻击事件受到了大众的广泛关注。

2020 年 4 月，B 站知名 UP 主“机智的党妹”发视频公开自己工作室的 NAS 中招勒索病毒，其中保存的素材全部被加密。据事主“党妹”本人介绍，其公司为了方便存储多达数百 GB 的视频素材，特地斥资十余万元在公司内部搭建了一个 NAS 系统。然而就在 NAS 系统搭建并测试完成后正式投入使用的第一天，便遭遇了黑客攻击被植入了 Buran 勒索病毒，最终导致存储的所有数据全部被加密。

无独有偶，2020 年 8 月，又一网络名人“歪果仁研究协会”也爆出中招勒索病毒。同“党妹”情况类似：公司一台重要电脑遭遇勒索病毒攻击导致文件被加密，而该电脑中存放了大量的视频素材——这其中包含了 SD 卡和电脑里的全部文件及在以色列 8 个月的视频素材。

此次事件中，黑客方面开价 980 美元，且表示如果 72 小时内付款可以享受 5 折优惠——即 490 美元的赎金金额。但“歪果仁”最终决定不支付赎金，不向黑客妥协。事实上该行为是比较明智且理性的，因为经技术人员分析发现，“歪果仁”机器中的文件实际上已经被加密了 8~12 次左右。其中包括 Stop、Crysis、Biglock、LockBit 等家族，即便付钱后可以解密其中一种，也无济于事。

2020 年的这两次“网红中招”事件，再一次将勒索病毒带回了大众视野，也提醒我们：虽然近几年勒索病毒的攻击目标始终在由个人用户向企业用户转移，但针对个人用户的攻击也从未真的消失。

五、 WastedLocker 攻击佳明，勒索赎金过千万美元

2020 年 7 月，知名智能穿戴设备和 GPS 产品厂商佳明宣布其 Garmin Connect、Garmin Pilot、Connext 以及 FlyGarmin 等多项服务关闭。

Garmin 系统和服务相关公告

我们诚挚地向各位宣布，目前暂停运作的 Garmin 系统和服务，包括 Garmin Connect 国际服务器相关服务等，已陆续恢复运行。由于目前我们仍在处理部分数据资料，因此某些功能暂时仍然不可用。我们真诚地感谢所有客户的耐心配合与理解。

2020 年 7 月 23 日，我们受到了网络攻击，该攻击导致我们许多在线服务受到了影响，导致我们许多在线服务受到了影响，包括网站功能、客户服务支持、终端应用程序和公司通讯等。Garmin 高度重视数据安全与客户服务，因此我们当下立即评估了攻击的性质、危害的范围并紧急开启了应对措施。

目前没有任何迹象显示任何用户数据（包括 Garmin Pay 的付款资料）被非法访问，丢失或被盗用。此外，除了在线服务功能之外，Garmin 产品的功能并未受影响。受到影响的系统正在积极恢复中，我们将致力于在接下来的几天内恢复系统正常运行。

由于大量的资料正在处理中，预计全面恢复仍需一段时间，Garmin 衷心感谢所有用户在此事件中的耐心与理解，并期待能够继续提供卓越的客户服务，延续 Garmin 的精神和传统。

另外，Garmin Connect 中国大陆服务器并未受到此次事件的影响，中国大陆服务器用户仍可正常使用 Garmin Connect 的相关服务。

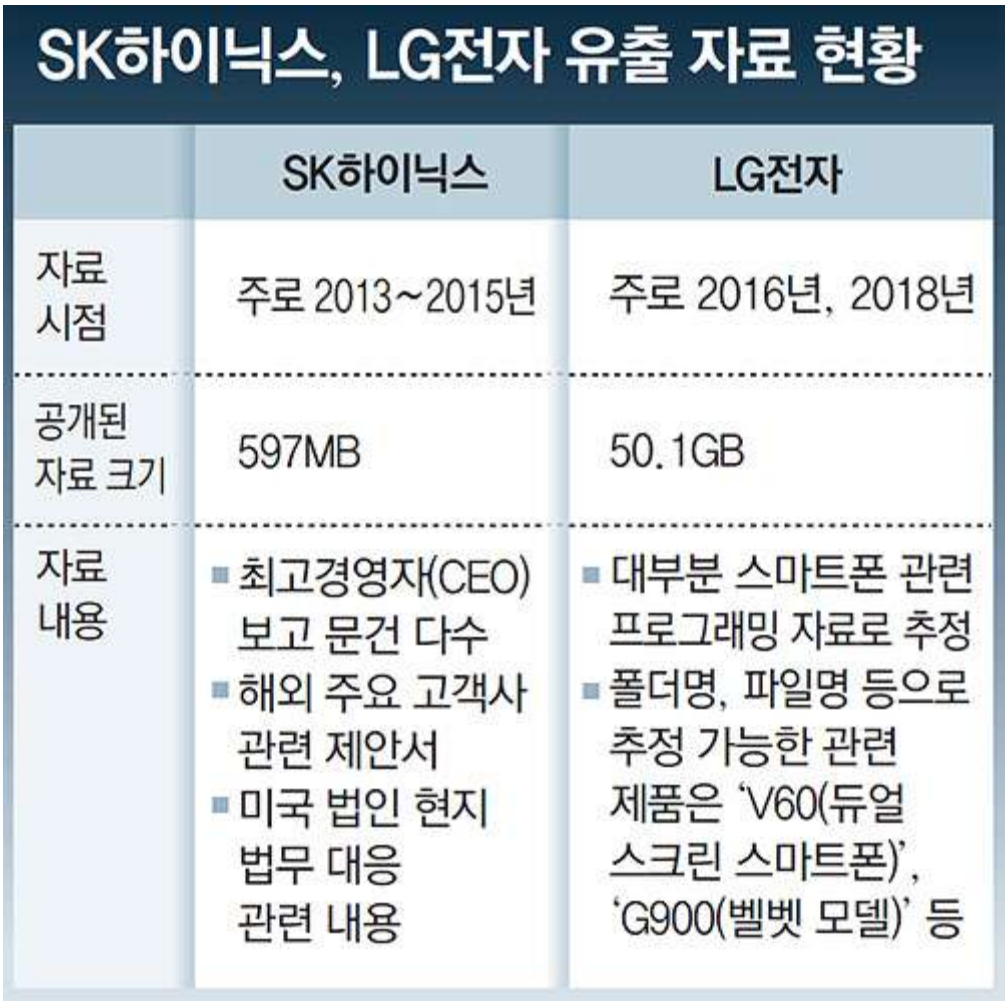
「定位 每个生命热情所在。」1989 年起从第一台导航仪开始，我们始终专注于创新与研发技术，生产横跨航空、航海、户外、健身休闲、车用等提升生活质量的高科技产品，矢志成为热爱生活者的理想品牌。Garmin 再次感谢所有用户在此事件中的耐心与理解。

原因是内部服务器和数据库收到了攻击，产品线也受到影响遭受影响停工数天。据悉，此次事件是受到了 WastedLocker 勒索病毒的大规模攻击，导致其设备中招，同时大量数据遭到加密。黑客在此次攻击后向佳明开出了 1000 万美元的赎金用以解密数据。

六、 海力士、LG 遭勒索，损失主要来自信息泄露

2020 年 8 月，韩国知名存储芯片厂 SK 海力士在美国的办事处遭到 Maze 勒索病毒攻击。攻击者窃取了电脑硬盘中存储的数据， 其中包括员工个人照片、证件副本等信息，也包含其他一些与其他公司的商业往来邮件信息。

据报道称，此次事件中 SK 海力士主要损失是 2013~2015 年间的数据，文件总大小约为 597MB（Maze 方面则声称获取了 SK 海力士 11TB 的数据）。而与 SK 海力士一同受到攻击的，还有同为知名韩国企业的 LG 电子，而 LG 电子损失的文件则有 50.1GB 左右。



事件发生后，SK 海力士和 LG 电子均声称已恢复了受到攻击的系统并加强了安全防护。但对于是否会花钱赎回泄露的机密数据，两家公司均未回应。

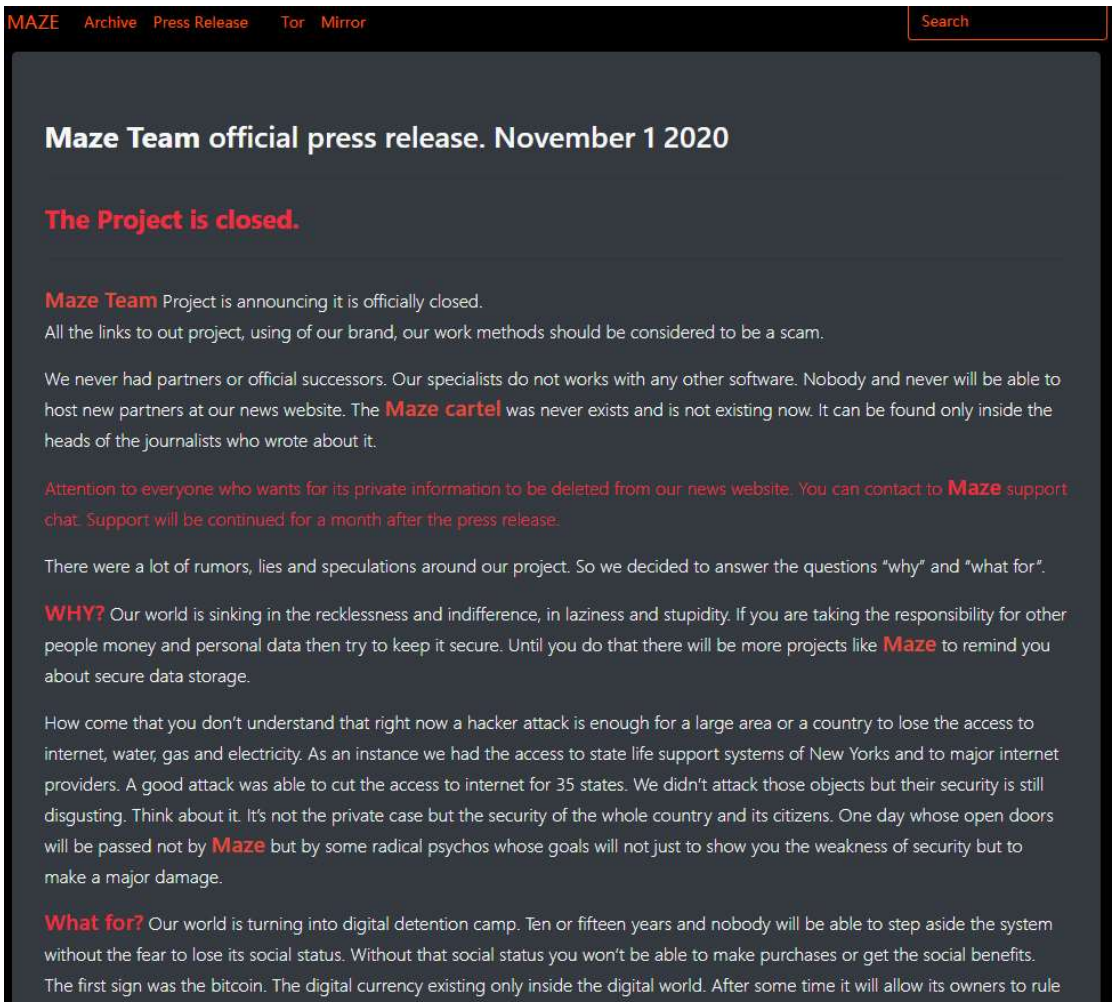
七、 德国医院遭勒索，全球首例勒索病毒攻击致死

据报道，2020 年 9 月德国杜塞多夫大学医院遭到勒索病毒攻击，被迫关闭急诊室，使得该院必须将一名急诊病人转至 20 英里外的另一所医院救治，最终导致该病人因未能得到及时治疗而死亡。这可能是目前全球公开报道中，第一例因勒索病毒攻击直接导致人员死亡的案例。

由于出现人员死亡情况，德国司法机关已按照过失杀人罪对此次攻击活动展开调查，而根据医院遭受攻击的服务器中留下的勒索信息看，攻击者的目标原本是海因里希·海涅大学，而非该医院。在事发后不久，病毒作者撤回了攻击，并提供了用于解密文件的密钥。医院也通过该密钥顺利完成了解密工作。

八、 Maze 家族“退隐江湖”，只留身后洪水滔天

2020 年 11 月 1 日，臭名昭著的 Maze 勒索病毒家族在其官网“迷宫新闻网”上发表声明宣布：该项目已正式关闭。但于此同时，该声明也否认了其运营成员开始转为运营 Egregor 勒索病毒的传言。



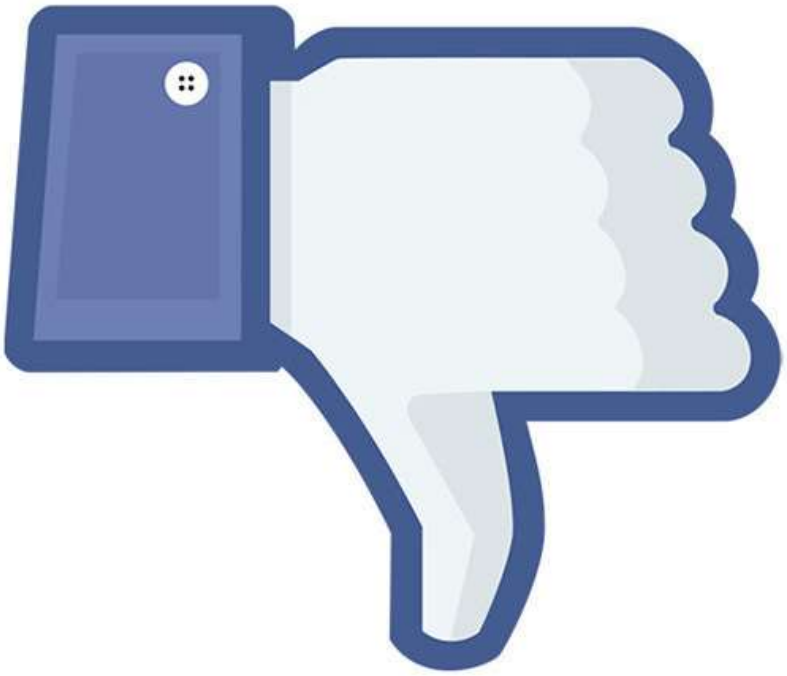
这意味着继 GandCrab 之后，又一个勒索病毒宣布“退隐江湖”。或许该勒索病毒团伙确实已经金盆洗手，但其留下的严重危害却越来越大。

Maze 家族勒索病毒最早在 2019 年 5 月首次被捕获。该家族成为首个宣布，若受害者不支付赎金将公布窃取到的数据的勒索病毒家族。也正是在这个信息公布后不久，其官方网站“迷宫新闻网”便正式对外开放，将未支付赎金的用户的数据上传到该网站供所有人下载和查看。截止到其正式宣布关闭项目，该网站已公布超 180 家公司数据。

这一行为可谓是开启了 2020 年勒索病毒新型勒索手段的万恶之源，2020 年 360 已发现超 20 个家族的勒索病毒加入了以泄露隐私数据为要挟勒索赎金的手段，而被泄露数据的企业已超过 1000 家。

九、 勒索病毒盯上 Facebook 广告位

2020 年 11 月，老牌勒索病毒家族 Locky 盯上了知名社交网站 Facebook。该病毒会通过诱导用户点击 Facebook 页面中的钓鱼图片来实现传播勒索病毒的功能，用户一旦中招，则需支付赎金才可解密。



媒体报道后，Facebook 方面做出回应称，此次事件主要是 Chrome 浏览器的扩展组件中存在漏洞导致的，网站已针对该问题进行了针对性修复，并将安全问题通报给了相关方面。目前的消息看，只要用户使用的不是 Chrome 或其他基于 Chromium 框架设计的浏览器，理论上都不会受到此次事件的影响。

十、 富士康 1200 台服务器沦陷

2020 年 12 月，国际知名电子代工厂富士康，位于墨西哥工厂的服务器遭到勒索病毒攻击，攻击者向富士康限期 21 天索要 1804.0955 枚比特币——按当时的汇率计算，约合 3468.6 万美元或 2.3 亿元人民币。富士康方面确认了其美洲工厂遭到勒索病毒攻击的信息，并称内部技术团队已完成了相关软件和系统的更新工作，并加强了安全防护。富士康同时表示此次事件受影响的厂区网络正逐步恢复，对公司整体运营影像不大。

另据报道，此次受到攻击的除了墨西哥工厂外，富士康的北美工厂可能也受到了一定程度的影响。

黑客组织 DoppelPaymer 宣布对此次事件负责，该组织声称入侵并加密了富士康北美厂区约 1200 台服务器，同时窃取了其中 100GB 的未加密文件，删除了 20~30TB 的备份。

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 2020 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。

360 安全卫士提供的弱口令攻击防护

二、 横向渗透防护能力

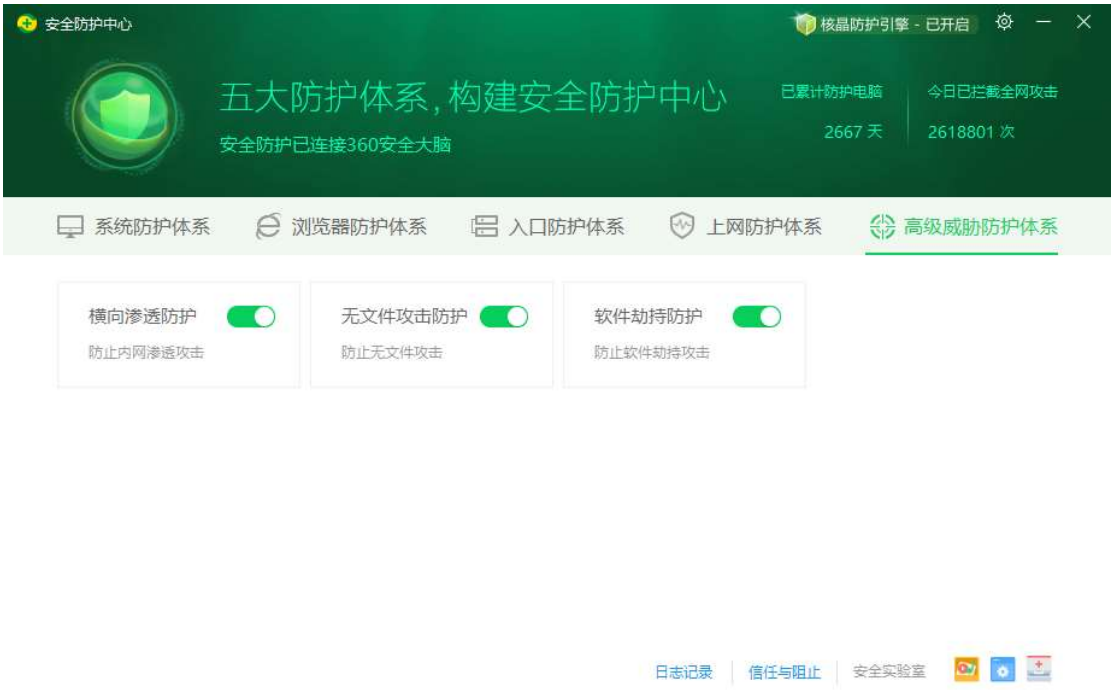
横向渗透目前是针对企业内网攻击的关键技术手段之一，而针对横向渗透的防护能力则是 360 高级威胁防护体系中的一项重要能力。勒索病毒攻击团伙，在对企业发起攻击后，往往利用该技术扩大影响范围，获取更多设备的控制权，乃至控制整个企业网络。

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

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。



三、 漏洞防护能力

新增漏洞拦截能力（部分重要功能）：

- 新增对 Windows 域控 Zerologon（CVE-2020-1472）域内提权漏洞拦截，该漏洞允许攻击者通过域内设备，提权接管整个 Windows 域控，获取整个域内最高权限。
- 新增对通达 OA 系统多个任意文件上传、webshell 执行漏洞拦截，这些漏洞被用来上传和执行勒索病毒。
- 新增对破坏力比肩“永恒之蓝”的 SMBv3 远程执行漏洞 CVE-2020-0796 SMBGhost，该漏洞允许攻击者，通过远程连接直接在目标及其执行远程代码。

- 新增对 Windows 10 下多个本地提权的 0day 漏洞拦截支持。
- 新增对如 Weblogic，Drupal，struts2 等各类应用系统漏洞的监测和防护。

四、 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。

五、 钓鱼邮件附件防护

钓鱼邮件一直以来都是勒索病毒传播的主要渠道之一。如年初的 Makop 勒索病毒攻击事

件就是通过垃圾邮件和钓鱼邮件传播，当攻击者不慎点击了钓鱼链接或打开了邮件附件，设备就可能感染勒索病毒，国内也有不少机构因此中招。针对这一情况，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。

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。

2020 年全年 360 解密大师共计更新版本 19 次，新增 25 个家族、变种的解密，累计支持解密勒索病毒超过 345 种，2020 年全年服务用户超 20651 台次，解密文件近 1354 万次，挽回损失超 4 亿元人民币*（按照单笔赎金 3000 美元估算）*。

下图给出了 360 解密大师在 2020 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。

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 以及 kraken 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 2020 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：

- GandCrab：“GandCrab”成为关键词主要由于黑客留下的文档中都会包含该“GandCrab”关键词以及版本号。该勒索病毒的传播渠道众多，导致该勒索病毒的受害者在 2019 年上半年占比也是最高的，该勒索病毒传播者在 2019 年 6 月 1 日宣布正式停播。由于其感染量多，导致 2020 年仍有大量设备需解密。
- 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。
  - 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。
  - 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 devos 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-alpha865qqz：属于 GlobeImposter 勒索病毒家族,由于被加密文件后缀会被修改为 GlobeImposter-Alpha865qqz 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。

- dewar：同 eking
- Voyager:属于 Hermes837 勒索病毒家族，由于被加密文件后缀会被修改为 Voyager 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。
- ReadInstructions：属于 MedusaLocker 勒索病毒家族，由于被加密文件后缀会被修改为 Readinstructions 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：同 GlobeImposter-Alpha865qqz