盘点：2019 年勒索病毒灾难事件

转载自：http://www.360.cn/n/11222.html

网络攻击千千万，勒索病毒占一半。今天我们就来盘一盘，2019 年那些令人窒息的勒索病毒攻击。

今年 3 月份，全球最大铝制品生产商之一的 Norsk Hydro 遭遇勒索软件攻击，公司被迫关闭多条自动化生产线，震荡全球铝制品交易市场；

5 月，国内某网约车平台遭黑客勒索软件定向打击，服务器核心数据惨遭加密，攻击者索要巨额比特币赎金，无奈之下向公安机关报警求助；

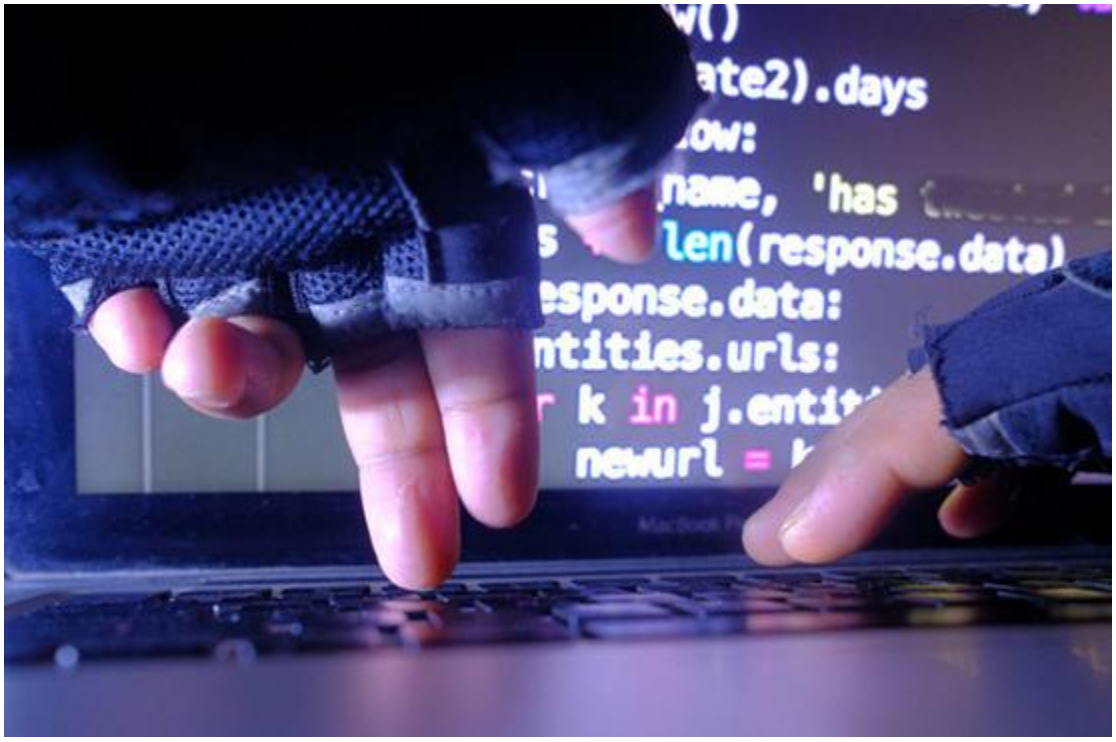
同在 5 月，美国佛罗里达州里维埃拉遭到勒索软件攻击，各项市政工作停摆几周，市政紧急会议决定支付 60 万美元的赎金。无独有偶，就在该市作出这个决定的短短一周内，佛罗里达另一个遭袭城市湖城也迫于无奈，向黑客支付价值近 50 万美元的比特币赎金。

6 月，全球最大飞机零件供应商 ASCO 遭遇勒索病毒攻击，生产环境系统瘫痪，大约 1000 名工人停工，四国工厂被迫停产；

10 月初，全球最大的助听器制造商 Demant，遭勒索软件入侵，直接经济损失高达 9500 万美元；

10 月中，全球知名航运和电子商务巨头 Pitney Bowes 遭受勒索软件攻击，攻击者加密公司系统数据，破坏其在线服务系统，超九成财富全球 500 强合作企业受波及；

10 月 16 日，法国最大商业电视台 M6 Group 惨遭勒索软件洗劫，公司电话、电子邮件、办公及管理工具全部中断，集体被迫“罢工”；



要命的是，距离 2019 年结束还有两个多月，但勒索病毒的攻势可能还未触顶。

迫于勒索病毒疫情形势，10 月 9 号，总部设在荷兰海牙的欧洲刑警组织与国际刑警组织发布的《2019 互联网有组织犯罪威胁评估》特别指出，**勒索软件仍是网络安全最大威胁，**全球各界需加强合作，联合打击网络犯罪。

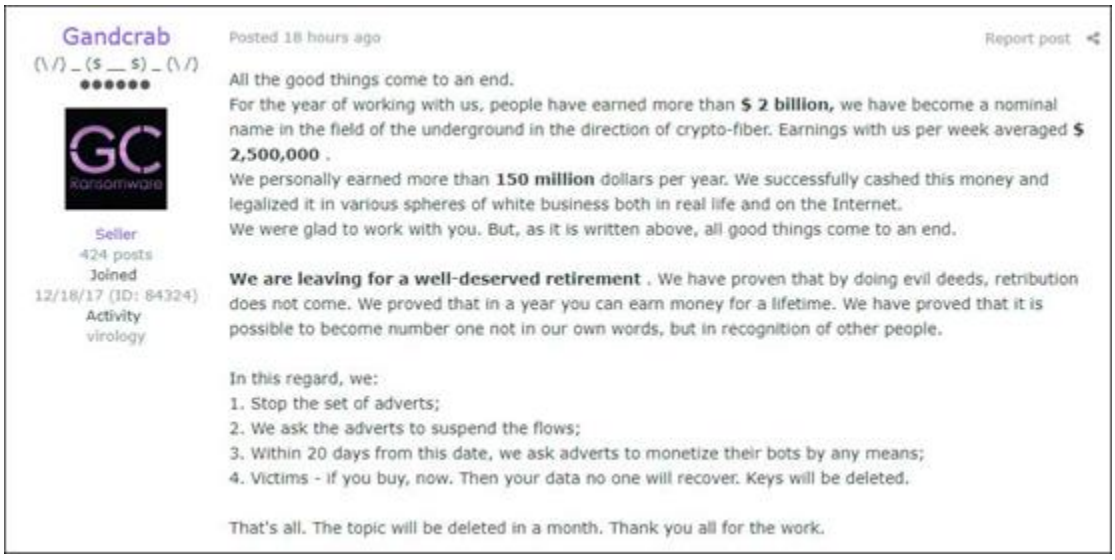
我们总结的五大勒索病毒家族

2019 开年至今，异常活跃的勒索软件高达近百种，我们总结出其中几种最为凶猛。

GandCrab 勒索病毒

在很多人看来，GandCrab 勒索病毒绝对是 2019 年最传奇的角色。2018 年 GandCrab 首次出现，之后经过 5 次版本迭代，波及罗纳尼亚、巴西、印度等数十国家地区，全球累计超过 150 万用户受到感染。还被国内安全团队称为“侠盗病毒”，因为他们后期的版本中避开了战火中的叙利亚地区。

今年 6 月，GandCrab 勒索软件团队一条官方消息刷爆了互联网。他们高调宣布，仅一年半的时间里，团队已赚进超过 20 亿美金，人均年入账 1.5 亿美金，所以决定停止更新这个恶意程序，从此风光隐退。

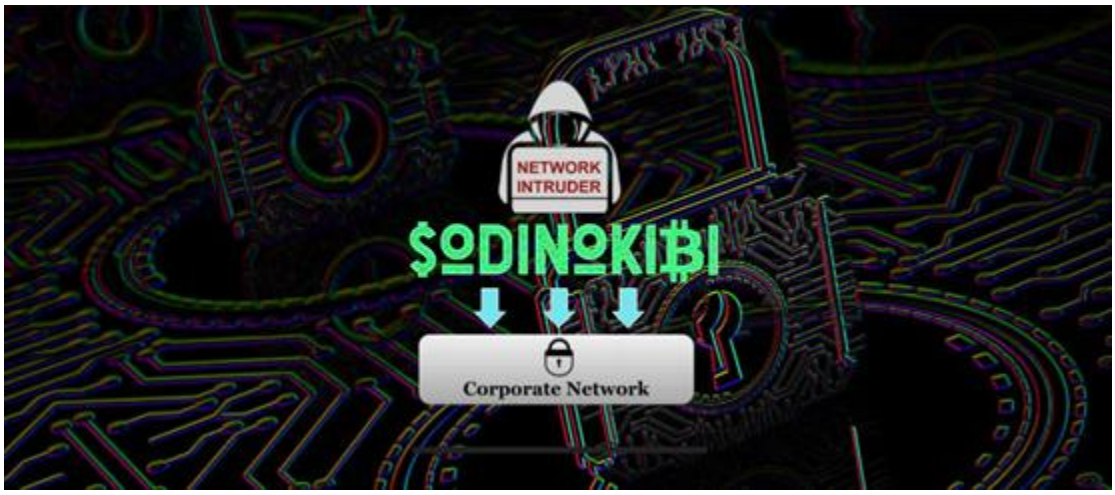


（GandCrab 勒索病毒团队官方声明，宣告钱赚够了，准备撤退，留下广大群众原地懵逼）

Sodinokibi 勒索病毒

随着 GandCrab 退出，它的继任者 Sodinokibi 勒索病毒接力登场。Sodinokibi 又称 REvil 勒索病毒，与 GandCrab 有着明显的代码重叠，因此很多人推测，GandCrab 的部分成员不愿收手，另起炉灶而运营的 Sodinokibi。

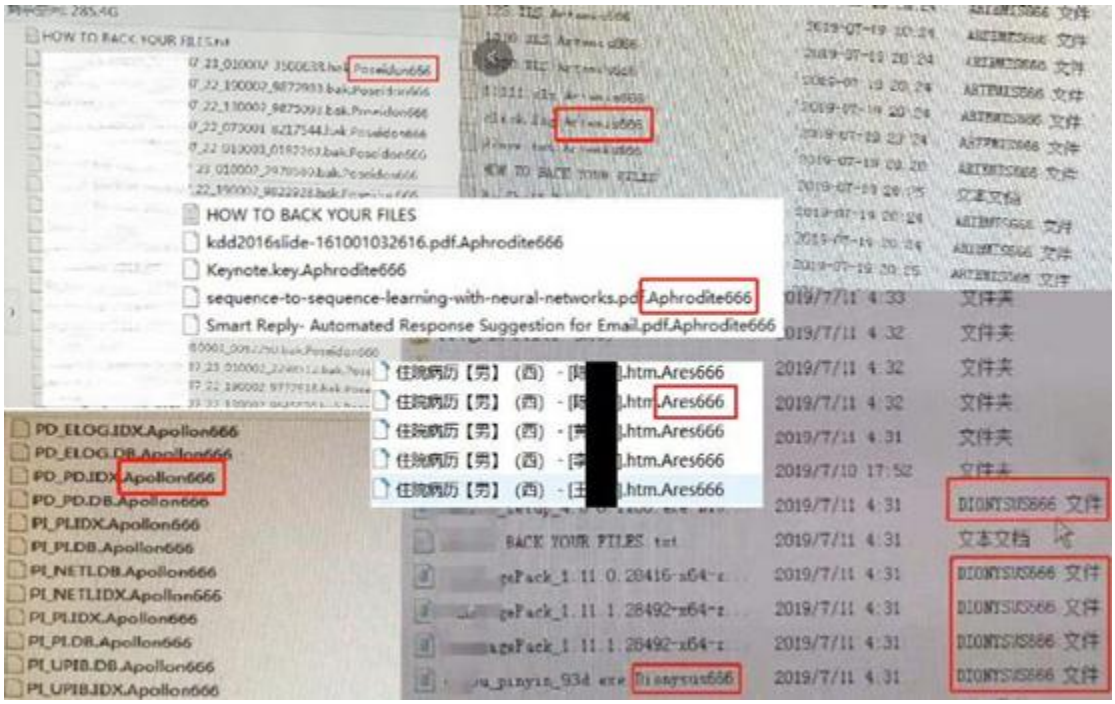
Sodinokibi 的部分变种会将受害者屏幕变成深蓝色，并且以 2500-5000 美金不等的赎金全球撒网，在不到半年时间，该勒索病毒已非法获利数百万美元。



GlobeImposter 勒索病毒

谈起 2019 的勒索病毒，就必须要提到 GlobeImposter。该勒索病毒又称“十二生肖”病毒，因为它攻入计算机内部后，会以“十二生肖英文名+4444”的文件后缀，对文件进行加密。而 GlobeImposter 自 2017 年 5 月首发至今，已经历八个版本迭代，并且后缀也从“十二生肖”，变身希腊“十二主神”。

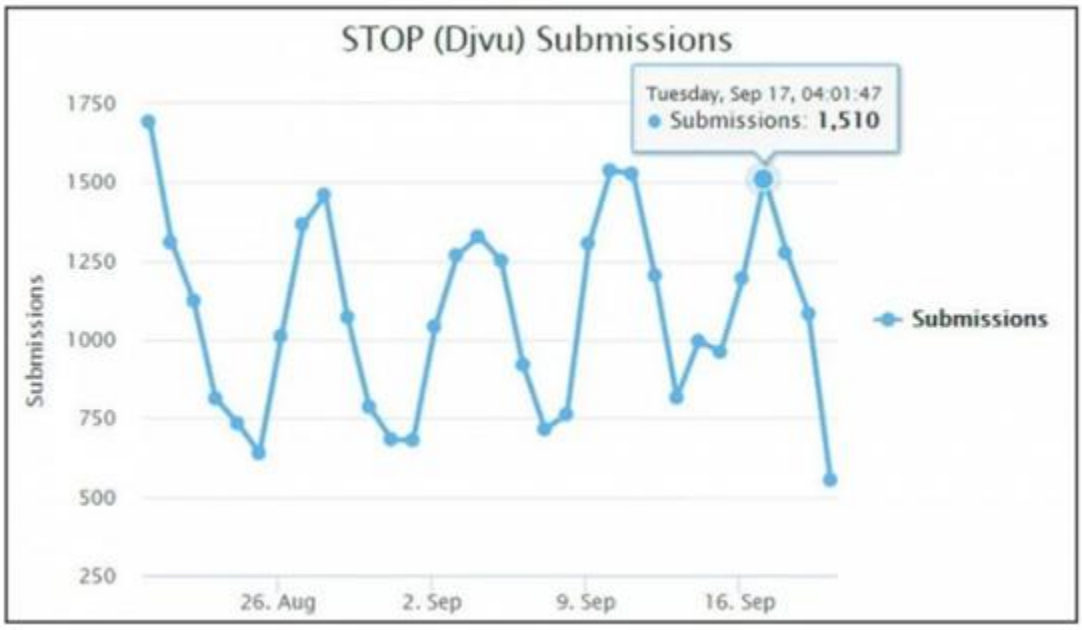
GlobeImposter 病毒主要通过 rdp 远程桌面弱口令进行攻击，去年山东 10 市不动产系统遭到它的攻击，今年国内又有多家企业、医院等机构中招。



（GlobeImposter 勒索病毒：文件后缀为希腊十二主神 + 666）

Stop 勒索病毒

Stop 勒索病毒，也被称作 djvu 勒索病毒，是 2019 年最为活跃的病毒家族之一。相比于动辄百万、千万美金的勒索软件，Stop 走薄利多销的敛财路线，解密赎金需要 980 美元，并且 72 小时联系软件作者还可享五折优惠。该病毒主要利用木马站点，通过伪装成软件破解工具或捆绑在激活软件进行传播，用户中招率奇高。



Phobos 勒索病毒

总的来说，Phobos 是一款非常棘手的勒索病毒，它采用 RDP 暴力破解+人工投放双重方式传播，并且可以轻松加密受害者 PC 上的每个文件，把它们全部变成无法打开的.phobos。

Phobos 病毒可能与 Dharma 病毒（又名 CrySis）属于同一组织，并且该病毒在运行过程中会进行自复制，和在注册表添加自启动项，如果没有把系统残留的病毒体清理干净，很可能会遭遇二次加密。

（Phobos 病毒的勒索信息）

总体来看，勒索软件种类激增、版本迭代，但表现形式大体都逃不过数据加密、系统锁定、数据泄漏、诈骗恐吓等几大类，但从勒索软件黑产来看，却足以让人全球震惊，也无怪乎国际刑警组织会站出来发声。

我们所发现的一些攻击趋势

为了从勒索病毒的浪潮中拯救别人，我们还发现了 2019 年勒索病毒攻击的一些变化。

第一，从 To C 用户转向 To B 政企，赎金大幅涨价。

现在的勒索病毒，从广泛而浅层的普通用户，明显转向了中大型政企机构、行业组织。有安全报告表明，自 2018 年 6 月以来，全球针对 To B 的勒索攻击增加了 363%。正如我们开篇提到的，全球最大的铝制品生产商、全球最大的助听器制造商、全球最大的飞机零件供应商等“全球最大系列”相继遭到攻击，这一切都是为了获取巨大的经济收益。除此以外，赎金也在疯涨。当年席卷全球的 WannaCry，其解密赎金也只是区区 300 美金；

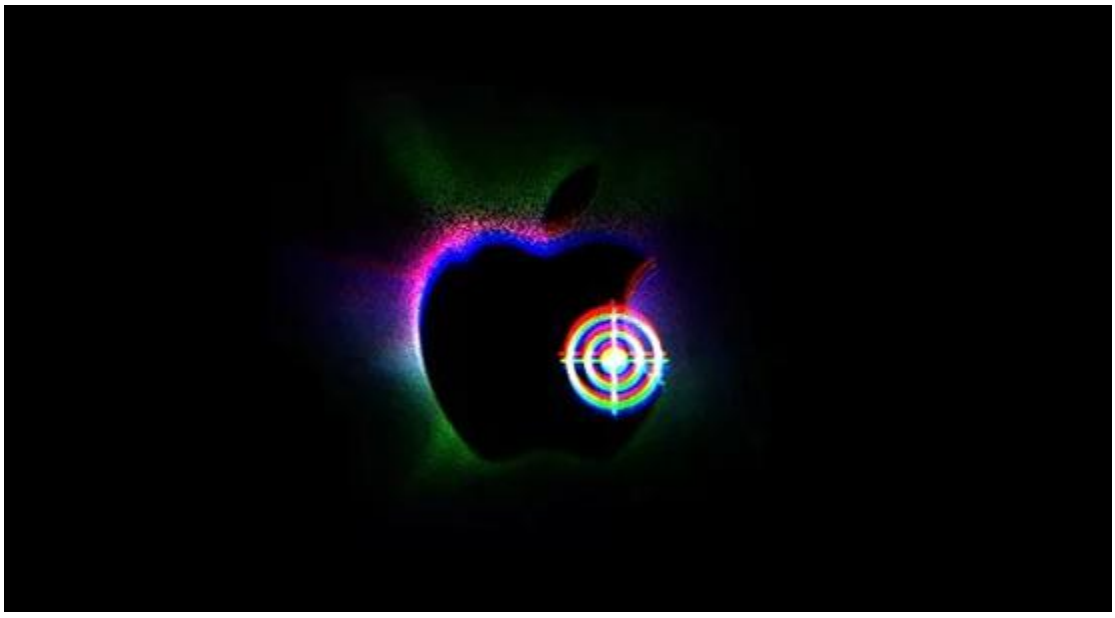
但如今——Sodinokibi 勒索病毒，赎金在 3 个比特币（大约 3 万美元）起步；Ryuk 勒索病毒， 11 个比特币（大约 12 万美元）起步；至于 MegaCortex 勒索病毒，最高赎金更高达 600 个比特币，相当于一次叫价 580 万美元；而且，或许是受到 GandCrab 家族一年半内赚了 20 亿美金的鼓舞，MageCortex 勒索病毒还特别在勒索信息中留下奋斗格言：“我们正在为赚钱而努力，这项犯罪活动的核心是获得赎金以后，以最原始形式归还您的宝贵数据。”

总之，看着这届黑客的勒索留言，能明确的感受到他们对于割韭菜的渴望。

第二，从垃圾邮件到利用漏洞传播。

虽然勒索病毒有垃圾邮件、RDP 口令爆破、网页挂马等多种传播途径，**但万物皆有漏洞，那可能就是勒索病毒进来的地方。**

例如 Sodinokibi 勒索病毒就集成了多个漏洞进行传播，包括 Windows 内核提权漏洞（CVE-2018-8453）、Confluence 漏洞 (CVE-2019-3396)、UAF 漏洞(CVE-2018-4878)、Weblogic 反序列化漏洞（CVE-2019-2725）等；又例如，BitPaymer 勒索软件就利用了 Apple 的 0day 漏洞；GETCRYPT 勒索病毒则利用 RIGEK 漏洞工具包；别忘了，还有连续利用 IE+Flash 双重漏洞，假冒 Chrome 浏览弹窗传播的勒索病毒 Spora 勒索病毒。总之吧，勒索病毒利用漏洞打出组合拳，不仅中招率骤升，威胁层级也远超以往，从这个角度来讲，勒索病毒对杀软的拦截查杀技术，提出了更具挑战的要求。

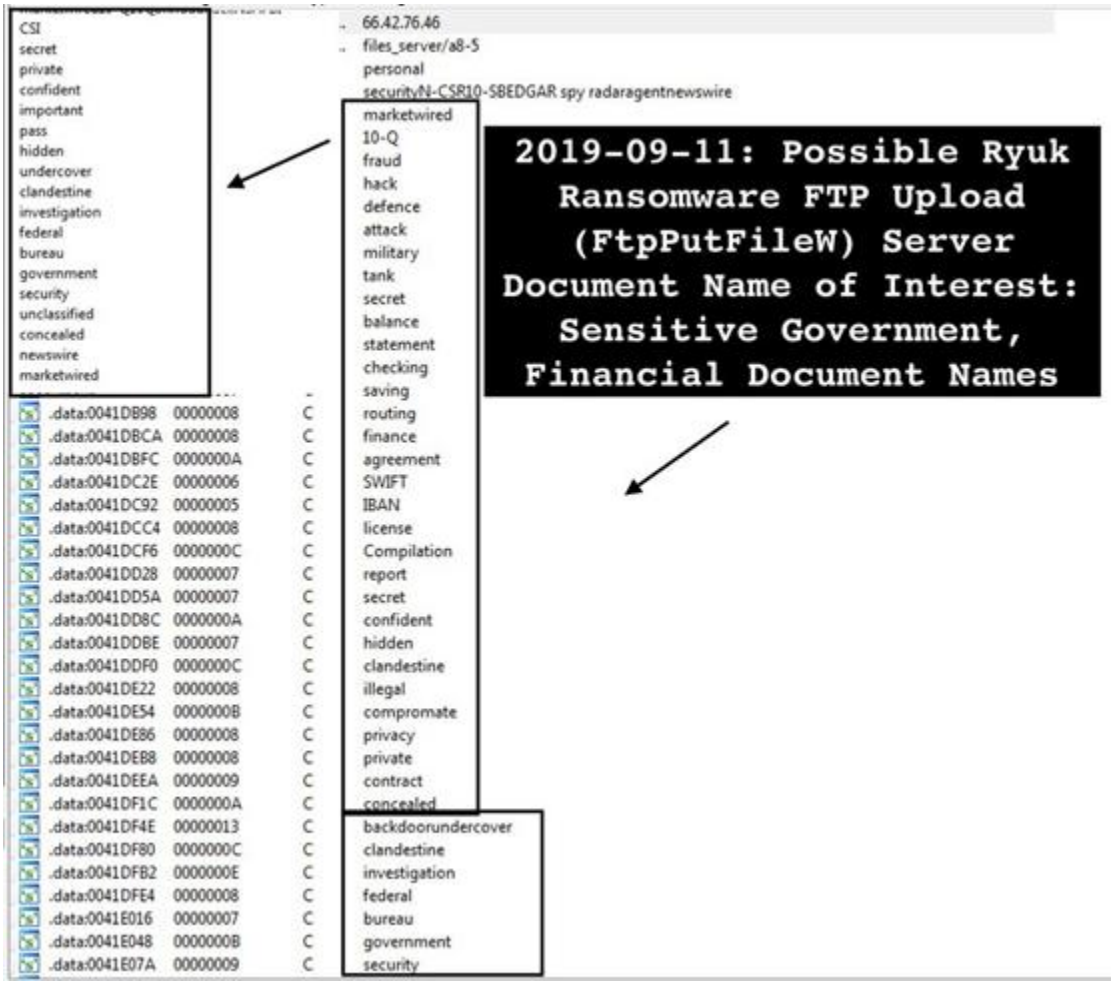


（勒索病毒利用 Apple 的 0day 漏洞传播）

第三，打着勒索的幌子，实为获取情报或破坏数据。

今年有个案例就与窃取情报有关，9 月份 MalwareHunterTeam 披露了一次不同寻常的勒索病毒事件。它在感染目标中不断搜寻敏感信息，包括军事机密、银行

信息、欺诈/刑事调查文件，行动举止完全不像为了图财。更可疑的是，该“勒索病毒”还会查找 Emma、Olivia、Noah、Logan 和 James 等美国社会保障部列出的 2018 年最常见的婴儿名字。



（该冒牌“勒索病毒”搜索关键词）

除了窃取情报，还有其他更奇怪的攻击案例，有些“勒索病毒”会对文件玩了命似的多次加密，甚至对文件进行无法修复的破坏，完全断了收赎金的后路。而据分析，这很可能是 APT 黑客组织，在实施渗透、窃取国家企业机密数据之后，而进一步投递的破坏性勒索病毒。为的是以勒索病毒作掩护，毁坏数据，消除入侵痕迹，掩盖真实攻击意图。

第四，手动投毒在变多。

手动投毒的好处是精准定位，黑客可以瞄准高价值定制服务器和系统。

（黑客组织正在手动植入病毒）

所以手动植入病毒在增多，像 Ryuk 勒索病毒的感染和传播过程都是由攻击者手动执行的；而 GlobeImposter 勒索病毒也不具备主动传播性，是由黑客渗透进入内网后，在目标主机上人工植入；

还有 MegaCortex 病毒也是攻击者设法获得管理凭据作为“手动闯入”的一部分。除了精准定位目标之外，这种方式还有其他好处：延长“驻留时间”，即从初始感染到安装勒索软件之间的一段时间。

在这种操作下，攻击者有时间对被感染网络进行分析，从而确定网络中最关键的系统，并获取感染这些系统的密码，随后才释放勒索软件，从而最大限度地造成损害。

更多零日反思

递增、扩散、高发的网络安全威胁，让我们开始思索：

高级持续性威胁呈常态化发展趋势的当下，“互联网更安全了”也许只是一种错觉，凶猛且异常活跃的勒索病毒，撕碎了人们沉醉的安全假象。

在网络这个从未有过绝对安全的世界，相对的安全也变得越发可贵。

网络安全最终是一直延续螺旋上升的“攻防”战，还是裂变出全新的终极模式，没有人可以给出确切的答案，我们唯有在攻防中不断探索，才能遇见安全的未来。