亚信安全 2019 威胁情报态势分析

数字货币助力黑产：勒索与挖矿泛滥成灾

AsiaInfo | 亚信安全

重要发现

- 勒索病毒发展了三十年，从理想主义到利益至上，已经成长为网络世界最大的安全威胁之一。
- 2019 年，各类勒索变种愈演愈烈、肆虐全球，勒索产业化 RaaS 日趋成熟，黑产链条不断扩大，国内医疗行业恐成下一个重灾区。
- 低风险，高回报的门罗币已经成为挖矿病毒首选货币，“无文件”、“隐写术"等高级逃逸技术开始流行，安全对抗持续升级。
- 随着国内云计算产业的蓬勃发展，拥有庞大数量工业级硬件的企业云和数据中心将成为挖矿病毒重点攻击目标。
- 5G 时代的到来，作为关键基础设施的 IoT 设备和工业控制系统将暴露更多易攻击面，拥有计算能力的边缘节点或将成为挖矿病毒的下一个战场。

为了贯彻落实习近平总书记“没有网络安全就没有国家安全”，“网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题”的指导方针，2019 年中国网络安全产业相关政策不断酝酿和完善并加速落地。随着各项标准的紧密出台，网络安全产业市场规范性逐步提升。护网专项行动的展开，等保 2.0 制度的推出，工业和信息化部《关于促进网络安全产业发展的指导意见》以及《国家网络安全产业园区发展规划》的正式发布，进一步强化我国网络安全保障能力，标志着网络安全产业进入了快速发展通道。

与此同时，网络威胁也在不断升级，各种新形态的病毒及其变种层出不穷，攻击手段、途径也更加隐蔽和新颖。**旧的病毒不断变种，新的病毒层出不穷，我们要如何应对这样的情形？**本篇报告以亚信安全 2019 威胁情报数据为基础，对 2019 年最热门的勒索和挖矿病毒进行多维度、多视角、全方位的剖析，并分别给出事前、事中和事后的防护建议。

目录

勒索专题

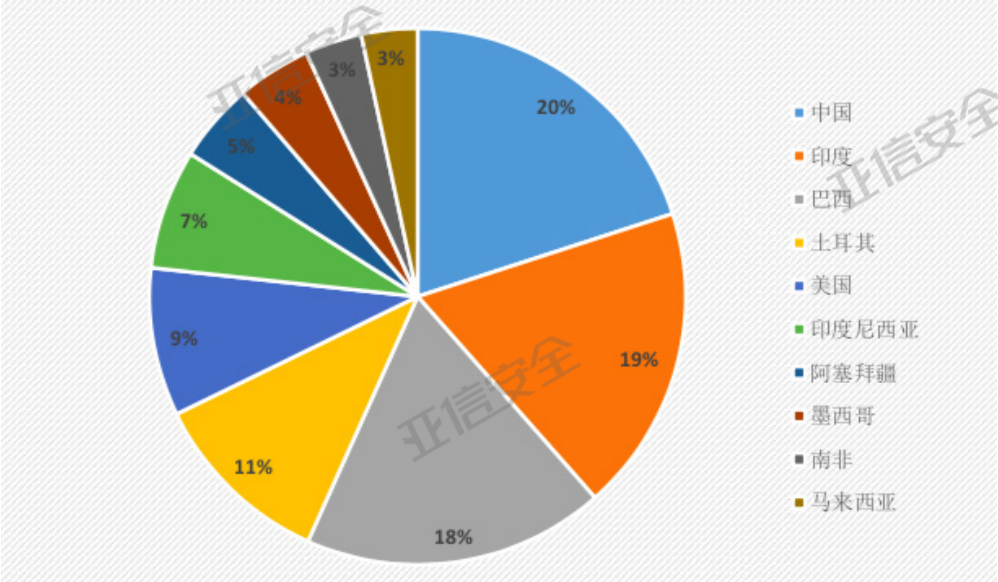
激荡三十年
勒索技术篇
勒索行业篇
勒索趋势篇
勒索防御篇

在数字世界里，勒索这门生意正蓬勃兴起，新的勒索病毒及其变种层出不穷，攻击手段、途径也更加隐蔽和新颖。勒索病毒已经成为网络安全最大的威胁，勒索攻击也成为全球最大的网络犯罪组织活动。

什么是勒索病毒?

勒索病毒，是一种流行的木马，通过骚扰、恐吓甚至采用绑架用户文件等方式，使用户数据资产或计算资源无法正常使用，并以此为条件向用户勒索钱财。这种病毒利用各种加密算法对文件进行加密后，向文件所有者索要赎金。如果感染者拒付赎金，就无法获得加密的私钥，无法恢复文件。

根据亚信安全威胁情报 2019 年的统计，中国的勒索病毒感染量已经跃居榜首，占全球总数的 20%。



【勒索软件全球感染量分布排行图】

从区域分布来看，勒索软件感染量排名靠前的是亚非拉等发展中国家，大多数西方发达国家不在榜单之中。之所以有这样的趋势，很大部分原因是由于发展中国家对于网络安全防御的意识相对薄弱，且防御能力有限，这值得我们提高警惕。

纵观勒索软件的发展史，最早的勒索病毒概念可以追溯到 1989 年，发展至今已满三十年。下面我们将盘点一下这三十年来勒索病毒的家族发展史。

1989

AIDS 木马

哈佛学者约瑟夫·L·波普开发了名为"AIDS"的木马病毒，受感染的电脑在重启90次后，该病毒程序会自动执行。在对重要文件和目录加密后，屏幕上会弹出189美元的勒索消息框。

2005

Archievus & GPCoder

Archievus 勒索病毒采用1024位RSA加密方式，对windows系统的我的文档文件夹进行加密。

GPCoder 借鉴了Archievus的设计，不过它更为全面和复杂，对windows系统的多种格式文件和文件夹进行加密。

2009

Vundo

Vundo 采用点击恶意邮件附件和恶意弹出广告的方式感染受害者电脑。该病毒在后期的版本中加入了勒索功能，并使用当时刚兴起的匿名支付平台作为勒索金额的支付途径。

2011

WinLock

WinLock勒索病毒并不会加密任何系统中的文件，而是锁定整个系统。并通过迫使受害者拨打高额电讯费用电话或发送信息的方式获取访问密码，电讯费大约为10美元。

2012

Reveton

Reveton以Zeus木马为基础开发而来。该病毒通常会显示一条警告信息，申明由于用户非法行为例如下载破解软件，已被执法机构警告，并锁定系统。此病毒也被定性为"警察病毒"。

2013

CryptoLocker

CryptoLoker 会生成2048位RSA公钥和私钥上传到病毒终端控制服务器，并用此密钥加密用户文件。随后要求用户在3天支付特定数量的比特币以获取私钥。

2016

Locky & KeRanger

Locky通过钓鱼邮件的方式进行传播，病毒脚本被写入邮件附件中的office文档中。一旦该脚本被执行，系统中包含特定后缀的文件都会被加密。

KeRanger 针对mac系统进行攻击，影响多达7000多mac用户。

2017

WannaCry & Petya

WannaCry 使用了Windows安全漏洞——EternalBlue（永恒之蓝），针对使用旧的windows操作系统的计算机进行攻击。在加密用户文件后，勒索一定数额的比特币。

Petya同样使用了EternalBlue（永恒之蓝）漏洞，该病毒主要在乌克兰爆发。

2018

GandCrab

GandCrab 依旧是针对旧版Windows系统的勒索软件，该病毒使用了RSA+AES的混合加密形式，并以Dash（达世币）作为勒索金额支付载体。

2019

SODINOKIB，Asruex, Maze...

激荡三十年

1989 – 2004 初出茅庐

勒索病毒第一次登上历史舞台是在 1989 年，哈佛学者约瑟夫·L·波普开发了名为“AIDS”的木马病毒。该病毒瞄准了医生和医疗机构的雇员，并在被感染的电脑重启 90 次后自动激活，接着对重要文件和目录进行加密和隐藏，随后屏幕上弹出勒索 189 美元的付款消息框，对受害者进行勒索。

2005 – 2009 重出江湖

16 年后，勒索病毒再次进入人们的视野。这一次，随着互联网的快速发展，黑客们又重新拾起了勒索病毒的概念。这其中，以 2005 年发现的名为 Archievus 的勒索病毒最具代表性。它使用了更难破解的 1024 位 RSA 加密方式，锁定了用户的“我的文档”文件夹以换取付款。名为 GPCoder 的木马病毒紧随其后，在目标文件已被复制和加密的基础上，将原件迅速删除。 这些被 RSA-1024 加密的文件很难破解，无法读取。GPCoder 也被广泛认为是第一个大范围传播的勒索病毒。

随着防病毒引擎的不断进化，诸如 GPCoder 这样的勒索病毒已不再构成威胁，因此，勒索病毒一度淡出大众视野。但在 2009 年，勒索病毒发展出了新的形式，一种名为 Vundo 的恐吓病毒，先对用户进行恐吓，告知其电脑已经中毒，诱导用户运行假的修复程序，实则触发勒索病毒。此外，勒索软件背后的技术和复杂度在 2005 年至 2009 年之间也得到了极大的提升。

2011 – 2012 大放光彩

2011 年是勒索病毒的转型之年。一款名为 Winlock Trojan 的勒索病毒在黑客界大放光彩，不再简单地加密几个文件，而是锁定整个系统，阻止用户访问。WinLock Trojan 以 Windows 操作系统为目标，并复制了产品激活系统，使用户保持锁定状态，直到他们购买了激活密钥。经过一系列操作，最终提示用户拨打“免费电话”获取激活密钥，该通话结束后会产生一笔昂贵的账单。

2012 年，另一种形式的勒索病毒 REVETON 开始盛行，它伪装成执法机构（例如 FBI），并声称在用户系统上发现非法文件，然后将系统锁定，并要求用户以匿名购物卡（如 Ukash 或 paysafecard）的方式支付赎金。

2013 – 2016 全面进化

2013 年，WinTrojan 这种形式的病毒日渐式微，取而代之的是一种更为激进的勒索病毒 –CryptoLocker。 它主要利用恶意邮件进行传播，并要求用户在三天内支付赎金，否则将加密并删除系统上的所有文件。CryptoLocker 采用 2048 位 RSA 公钥和私钥进行加密。这意味着，用户将必须找到两个密钥才能自己解锁系统，然而这种可能性微乎其微。

2016 年，黑客界出现了迄今为止最危险的勒索病毒之一 –Locky。它主要通过钓鱼攻击的方式传播，在高峰期每天可感染多达 10000 个新系统。Locky 的主要攻击对象为医疗机构。由于医疗机构通常选择在被勒索的第一时间迅速付费，以恢复系统的正常使用。Locky 正是利用医疗机构的这一特点，攫取大量利益。

在 2016 年值得一提的勒索病毒还有 KeRanger。长久以来，Mac 系统一直被认作是免于病毒侵扰的净土，但 KeRanger 的出现让 Mac 系统用户也成为了勒索攻击的目标。此病毒不仅加密文件，还禁止 Mac 系统进行回滚。

随着新的加密技术和支付方式得以利用，勒索病毒成为全球威胁只是时间问题。

2017 – 2018 全球爆发

虽然 2016 年就已经爆发了诸多严重的勒索病毒感染事件，但真正让勒索病毒走上世界舞台的，还数 2017 年的 WannaCry。 这是一款仅用极短时间，便传播 150 多个国家和地区的勒索病毒。WannaCry 的传播速度及范围成为当时的头条新闻。

WannaCry 利用了 Windows 的较早版本中的漏洞 –永恒之蓝。 一旦网络中的一台设备被感染，WannaCry 就会尝试感染内网中的其他主机，这是 WannaCry 如此广泛传播的原因之一。WannaCry 要求使用比特币支付赎金，甚至有人认为，它推高了比特币的市值。

而亚信安全的客户在这场风暴中安然无恙，亚信安全桌面安全解决方案 OfficeScan11 SP1 的成功部署是最大“功臣”，亚信安全也因此成为成功抵御全球第一只勒索蠕虫 WannaCry 的安全厂商。

2019 年 – 2020 蓬勃发展

进入 2019 年，勒索攻击事件增加了 18%，高于往年平均 12%的增长，全球各地都有勒索攻击事件在不断发生。诸如“某单位花 197 万解密勒索病毒”，“勒索病毒制造者赚了 20 亿美金后，公然宣布金盆洗手”这样的新闻屡见不鲜，勒索的金额也从以往的以万为单位上升到几百万美元。预计到 2021 年，全球因勒索攻击造成的损失将达到 200 亿美元，是 2015 年 3.25 亿美元的 61 倍之多。

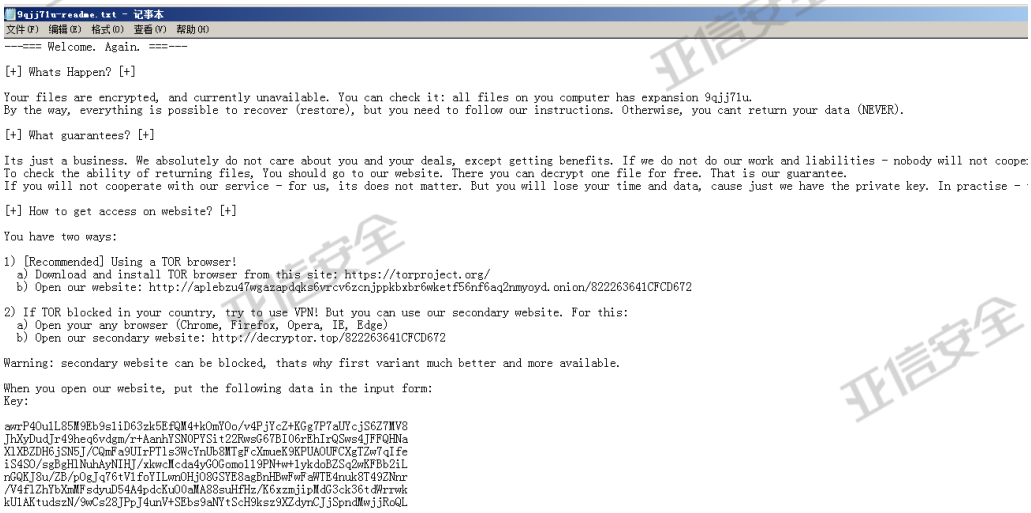
【 亚信安全威胁情报勒索病毒统计 】

不仅如此，勒索软件即服务开始兴起，不法份子可以在暗网上自由选择购买，相关黑产不光技术专业，甚至还提供推广、代理、分销以及专业客服的服务，降低了攻击者的门槛，从而受到追捧，GandCrab 和 Sodinokibi 就是其中的代表。

勒索技术篇

Sodinokib，GandCrab 家族

亚信安全于 2019 年截获 Sodinokib 勒索病毒的变种文件，该病毒与著名 GandCrab 勒索病毒相似，偏爱利用钓鱼邮件进行传播，伪装成 word 文档，实则为可执行文件。一旦用户运行该文件，磁盘中的文件就会被加密。其攻击目标为商贸、科技、机关等单位工作人员 。



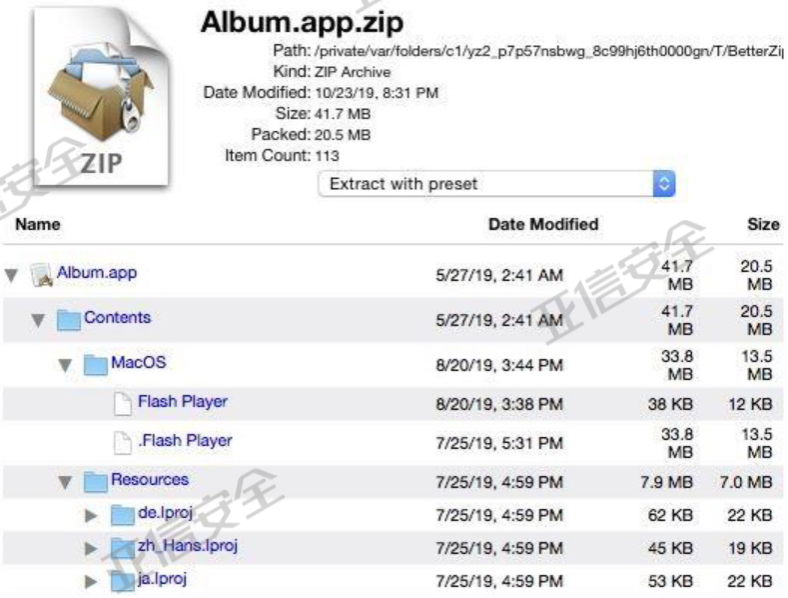
【Sodinokibi 勒索病毒提示信息 】

与此同时亚信安全还截获了通过垃圾邮件传播的 GandCrab 勒索病毒最新变种，该病毒使用不同的语言版本发动定向攻击。其主要攻击目标是使用中文繁体语言和韩语的用户， 此类邮件假冒快递公司向收件人发送虚假订单信息，诱骗用户打开包含 GandCrab 勒索病毒的邮件附件。

【包含 GandCrab 勒索病毒的邮件附件 】

Asruex 家族

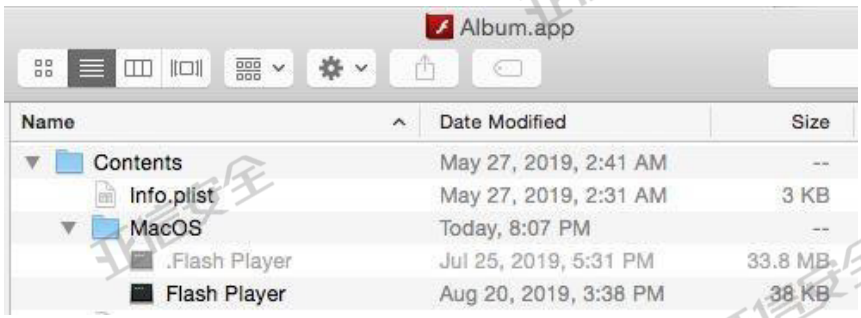
新型攻击 MacOS 的后门程序也于 2019 年被亚信安全截获。攻击 MacOS 的后门程序曾使用带有宏病毒的 Excel 文档，现在摇身一变与正常的 Flash Player 捆绑在一起。



【与正常的 Flash Player 捆绑在一起的后门程序】

当用户以为安装正常的 Flash Player 的同时，后台会悄悄执行后门程序，用户很难察觉。Asruex 后门病毒嵌入 PDF 文档，在 Word 与 PDF 中注入恶意代码。此次截获的 MacOS 后门程序，是通过 Mac 应用程序捆绑传播，其连接的 C&C 服务器与上述提及的带有宏病毒的 Excel 文档连接的 C&C 服务器类似。

该捆绑安装程序含有两个 Flash Player 文件：合法版本和恶意版本（亚信安全将其命名为 Trojan.MacOS.NUKESPED.B）。从下图中可以看到，两个 Flash Player 文件大小不相同，其中较小的是冒充 Flash Player 的恶意文件，合法版本的 Flash Player 则是隐藏文件。安装包程序被运行后，其仍然会运行合法的 Flash Player，达到隐藏恶意行为目的。



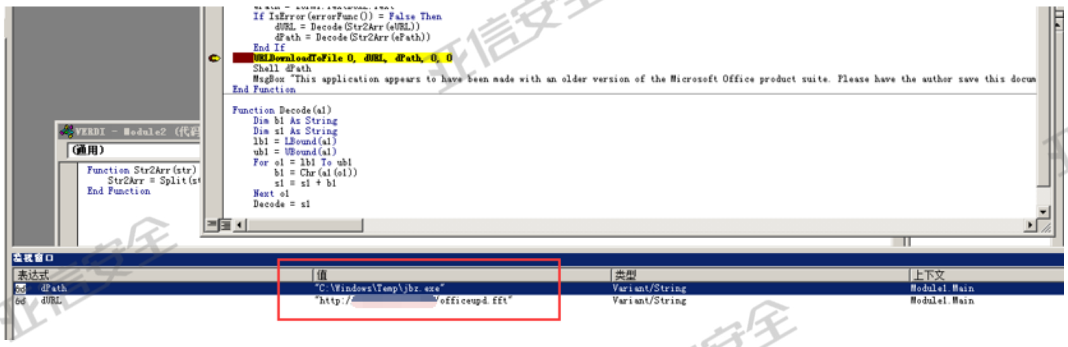
【捆绑安装程序包含两个 Flash Player 文件，一个合法版本和一个恶意版本】

Maze 家族

Maze（迷宫）勒索病毒被亚信安全持续追踪。其完成加密数据后会循环播放文件被加密的录音，通知受害者已被勒索病毒感染。Maze 勒索病毒此次通过诱饵文档传播，诱导受害者运行文件。

【标题为 RSA SecurID 的诱饵文档】

启动宏代码，宏代码会读取窗体中的数据，然后进行解析，其主要功能是下载迷宫勒索病毒主体文件，对于不同的变种文件，其勒索主体文件下载地址和文件名称会发生变化。宏代码执行后解密窗体中的数据，然后从远程服务器 hxxp://192.xxx.210.xxx/officeupd.fft 下载恶意程序到 C:\Windows\Temp\jbz.exe，然后执行恶意程序，如下所示：



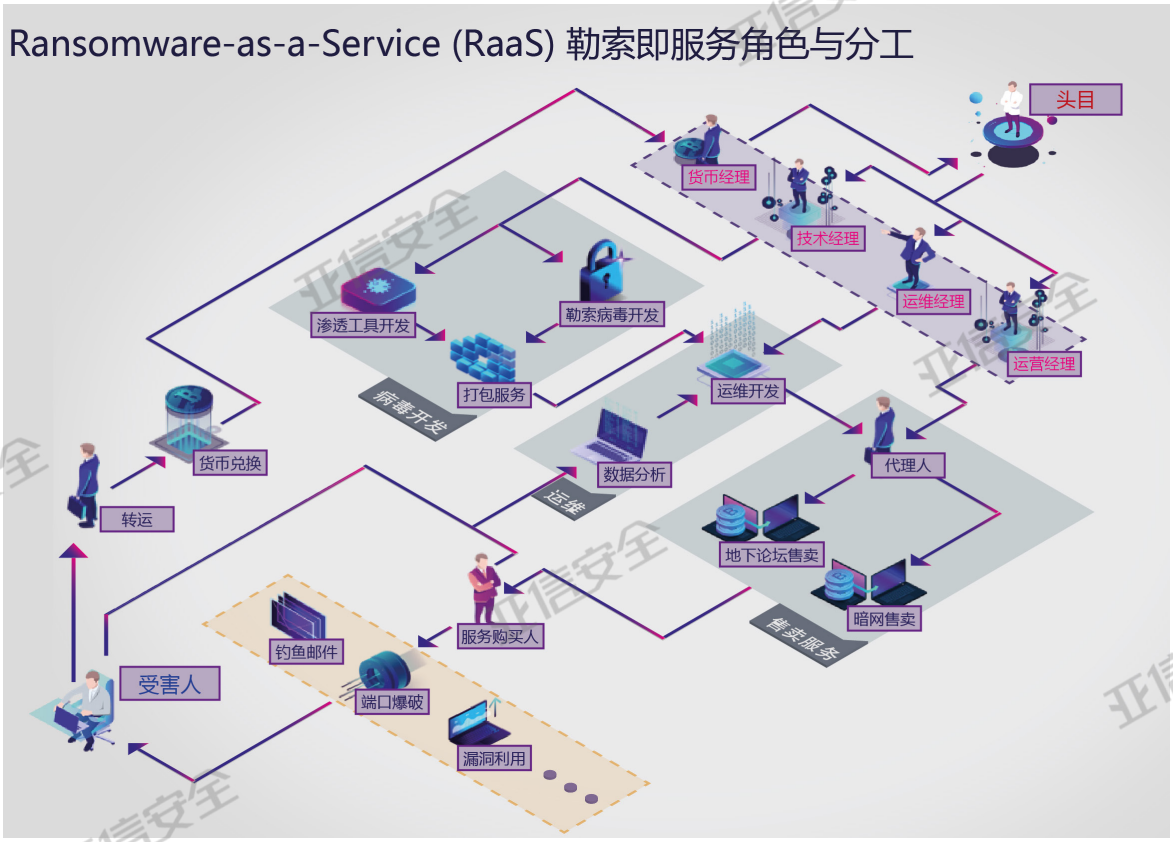
运行下载的迷宫病毒后，其会加密系统中的数据。完成加密后，该病毒不会删除自身，而是循环播放文件被加密的录音，修改桌面背景图片并通知受害人已经感染勒索病毒。

19 年下半年，Maze 勒索病毒团伙向北美领先的电缆制造商 Southwire 发起针对性勒索攻击，赎金高达 600 万美元。这次勒索组攻击不单单加密数据，还盗取数据，并以不交赎金就公布企业数据进行要挟。

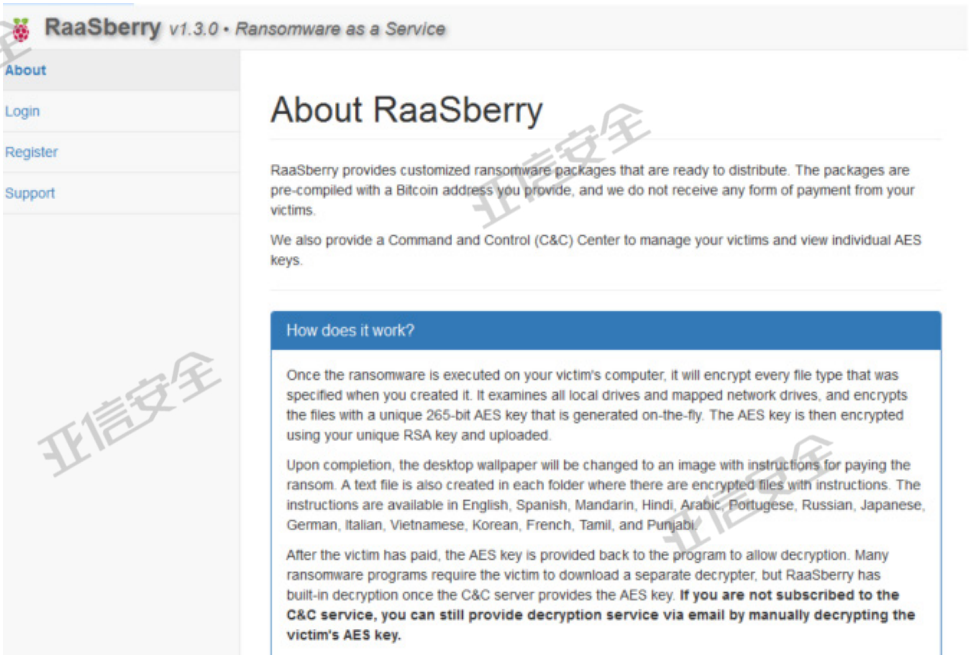
勒索行业篇

RaaS 新崛起

提到勒索软件的黑产，不得不谈谈一个热词，勒索即服务（Ransomware as a Service, RaaS），借鉴了软件即服务（Software as a Service, SaaS）的模型，这种基于订阅的模型可以使那些即使是新手的犯罪份子，也可以毫不费力的发起勒索攻击，这就更给黑客大开方便之门。



RaaS 的运作像极了 SaaS，服务提供商包含或寻找开发团队负责编写勒索病毒软件，而运营人员通过会员计划将其以出售或者出租的方式提供给意图发起勒索攻击的网络犯罪份子。并且他们还会提供使用教程，以及勒索攻击的基础知识，甚至做到可视化，实时追踪攻击状态。攻击者一旦勒索成功，还会将部分赎金分配给 RaaS 提供商和开发人员，这样已经形成了一个完备的产业闭环。这种模式吸引了很多的网络犯罪份子，甚至你都可以在暗网上看到 RaaS 提供商发出的广告。以



【RaasBerry，RaaS 服务提供商的介绍页面】

【RaasBerry 的部分会员订阅等级分化】

RaasBerry 为例，它有完备的服务网站，用户可以在网站上获得该勒索工具的介绍，使用教程，客服等资源，并可订阅成为会员，等级从普通到白金分为 5 个档次。

对于那些病毒作者，RaaS 的出现使他们可以快速赚钱，也不再需要承担过多的风险，运营人员会帮助他们处理一切事宜。而对于服务使用者，这降低了他们的技术门槛，他们只需要在暗网上从众多 RaaS 提供商中选择低价，易于使用的即可。

根据数据备份和恢复公司 Datto 的数据，每次勒索病毒造成宕机，公司蒙受的损失平均都在 46,800 美金，远远高出赎金。越早交赎金，损失越小，因此公司为了减少损失，都会尽早交赎金。应运而生的也有诸如 Proven Data 这种数据恢复公司都推出一项核心业务，那就是作为受害者的代理人，与勒索攻击者讨价还价。他们似乎已经和黑客结成某种“合作”关系，甚至有些数据恢复公司还能从黑客那拿到不少的折扣。并且，这些数据公司为了帮助雇主快速恢复数据，往往都囤积了大量的数字加密货币以备不时之需。

另一方面，一些保险公司也看到了这个商机。勒索攻击是偶然事件，既然如此，当然也可以推出保险服务。实际上，勒索病毒的扩散性影响也让网络保险市场迎来一波快速增长。买了保险服务的公司，因为有保险的索赔，也更容易接受支付赎金。在某种程度上，这也催涨了勒索攻击的势头。

医疗勒索敲响警钟

统计数据表明，由于大型组织通常会有更强的意愿花更多的钱来赎回数据，近年来勒索病毒的攻击者开始越来越关注于大型组织的敏感数据。而医疗卫生行业这个神圣纯净的地方正在成为全球勒索黑产的主要攻击目标。

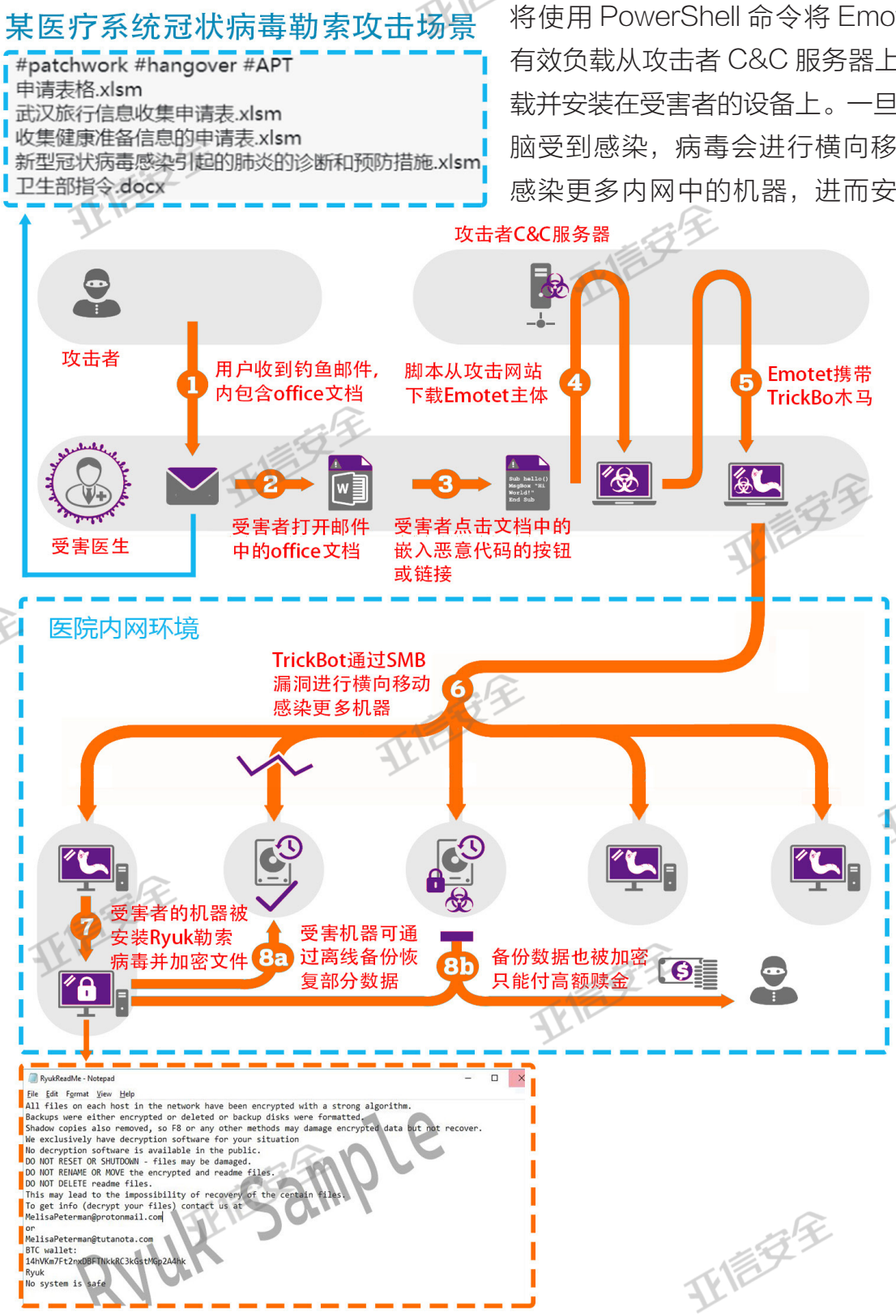
随着全球移动医疗、AI 医疗影像、电子病历等数字化程序的普及，医疗卫生组织越来越依赖电子档案来执行日常任务，一些远程医疗咨询和救生设备也依靠网络实时传送病人数据。当勒索攻击发生时，成千上万病人资料、病例、药方、学术报告等重要医疗卫生资料被恶意计算机病毒加密成一个不可查看文件，不仅造成系统瘫痪，病例丢失，外科手术取消，严重的甚至危害到患者的生命。

亚信安全威胁情报中心一直对此类犯罪活动表示关注，并持续与这类勒索软件攻击的黑产团伙进行对抗。2019 年，亚信安全服务团队在全球医疗卫生行业的勒索攻击应急响应案例中统计发现，针对医疗卫生机构的攻击往往单笔赎金金额巨大，且成功率较高，其中 2019 年美国的医疗机构损失了约 40 亿美元。

2020 年伊始，2019-nCoV 新型冠状病毒疫情的发展牵动着全国各族人民的心，而亚信安全监控到多起黑产利用冠状病毒热点事件展开的攻击活动，主要的攻击形式为针对医疗机构个人的网络钓鱼。

【亚信安全威胁情报系统总结的医疗勒索情报】

以下是亚信安全最近截获的一起针对我国某医疗机构的攻击案例，攻击者这次瞄准了医务人员的个人邮箱，邮件的附件是以“新型冠状病毒感染引起的肺炎的诊断和预防措施”命名的 Office 文档文件，并强调这些安全措施的重要性，促使受害者下载并打开恶意文档。一旦攻击目标打开这些文档，就会弹出一个 EmotetOffice365 文档模板，并要求受害者“启用内容”以查看完整文档，启用宏后，将使用 PowerShell 命令将 Emotet 有效负载从攻击者 C&C 服务器上下载并安装在受害者的设备上。一旦电脑受到感染，病毒会进行横向移动感染更多内网中的机器，进而安装



Ryuk 勒索病毒对计算机中的数据进行加密。

这几年国内医疗行业信息化发展迅速，电子医疗系统刚刚完成第一代普及，鉴于许多医疗卫生行业的网络安全防护措施并未健全，网络隔离、机器访问权限管控不够严格，人员的安全意识有待加强，因此在被定向攻击的时候，往往造成不可挽回的损失。面对可能造成的严重社会影响，亚信安全呼吁对医疗行业的勒索防范不可忽视。

勒索趋势篇

◇ 勒索病毒加速更新和变种

随着各大企业、安全厂商以及警方对勒索攻击的高度重视，针对勒索病毒的安全解决方案不断成熟，越来越多的勒索病毒被阻挡。这也使得勒索病毒制作者加速对病毒的更新迭代，攻击形式将不限于已有的垃圾邮件、漏洞利用、软件供应链攻击等。

◇ 多平台病毒陆续发现

目前勒索病毒多见于 Windows 系统，但是针对 Linux、MacOS、Android 等平台的勒索和挖矿病毒案例也陆续被发现，未来针对其他平台的病毒也会逐步增加。

◇ 勒索病毒走向产业化

以数字货币为支付方式的勒索即服务（RaaS）将更加成熟，随着更多稳定、高匿名的数字货币的出现，更多的网络犯罪分子将转向地下区块链平台进行交易。

◇ 勒索攻击将更具有针对性

勒索攻击高度针对特定企业或组织，攻击者将更注重于收集目标受害者的情报，对受害者造成最大限度的破坏，从而提高赎金，这其中医疗勒索应引起高度重视。

◇ 勒索赎金越来越高

勒索攻击的泛滥，受攻击的企业往往在第一时间交付赎金才能最小化损失，这使得更多企业和机构（如医院，学校）购买网络保险业务。同时，这也使得勒索赎金水涨船高。

勒索防御篇

事前

◇ 加强教育

加强员工的网络安全教育，工作用电脑要使用高强度密码，并使用 Multi-factor 验证增加保护强度。大量的勒索攻击都是通过恶意邮件的形式，员工应当保持高度警惕，不点击来源不明的邮件。普及最新的恶意攻击知识和勒索案例，使员工可以第一时间识别勒索攻击的征兆。

◇ 数据备份

对重要文件和数据（数据库等数据）进行定期非本地备份，仍然是抵御勒索的第一手段。数据备份三二一原则：

1. 三份备份：重要数据额外备份两份。
2. 两种不同形式：将数据备份在两种不同的存储类型，如服务器 / 移动硬盘 / 云端 / 光盘等。
3. 一份异地备份：至少一份备份存储在异地，当发生意外时保证有一份备份数据安全。

◇ 网络控制

企业内网可以关闭不必要的网络端口，降低黑客在内网攻击传播的成功率。如：445、135、139 等，对 3389，5900 等端口可进行白名单配置，只允许白名单内的 IP 连接登陆。

禁止服务器主动发起外部连接请求，对于需要向外部服务器推送共享数据的，应使用白名单的方式，在出口防火墙加入相关策略，对主动连接 IP 范围进行限制；有效加强访问控制 ACL 策略，细化策略粒度，按区域按业务严格限制各个网络区域以及服务器之间的访问，采用白名单机制只允许开放特定的业务必要端口，其他端口一律禁止访问，仅管理员 IP 可对管理端口进行访问，如 FTP、数据库服务、远程桌面等管理端口。

事中

部署防勒索攻击的邮件防护产品

事实证明 80% 的勒索攻击始于社交工程邮件，这类邮件通常含有传统邮件或终端安全产品无法侦测的恶意附件或 URL，传统的邮件网关没有办法识别社交工程邮件中的恶意行为，拥有勒索防御和沙箱检测能力的高级邮件防护产品可以在防御第一层抵御勒索的攻击。

在终端 / 服务器部署专业防护产品

亚信安全即使可以侦测电子邮件或网站链接当中 99% 的勒索病毒威胁，但仍有 1% 的勒索病毒可能会进入您的终端设备。随着勒索病毒技术的更新，绕过传统静态检测的方法越来越多，必须采用机器学习加行为分析的手段来进行对抗。机器学习可以通过对相似已知样本的不断学习来侦测新出现的未知威胁，而行为分析能够发现勒索病毒相关的可疑行为（例如：快速加密大量文件），自动终止加密执行程序，并将终端设备隔离，不让勒索病毒有机会扩散。

采购具有威胁情报能力的防护产品

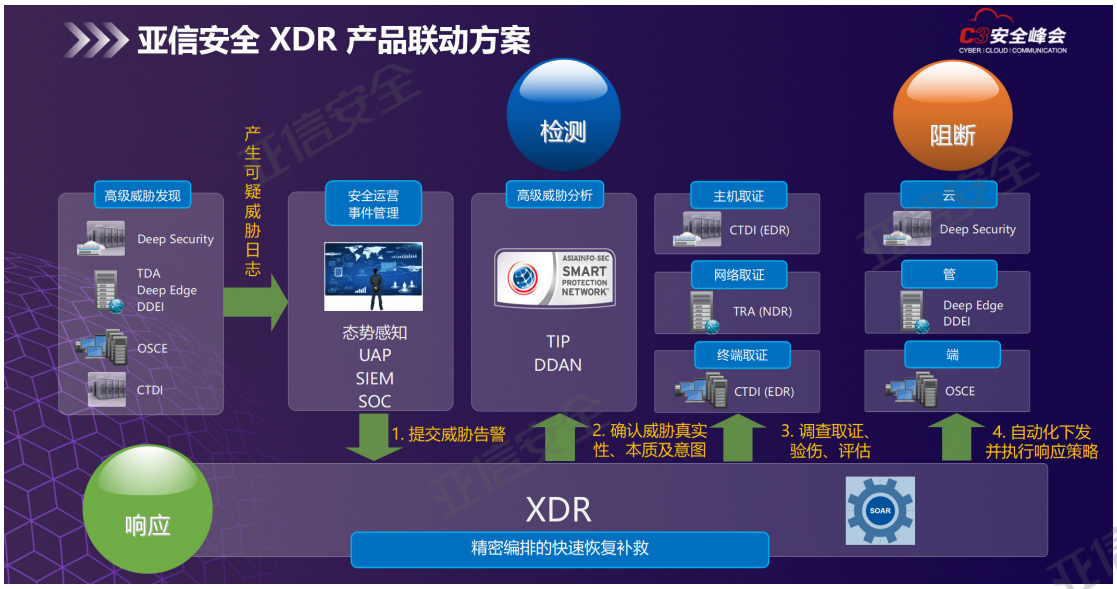
由于勒索黑产的快速发展和勒索病毒的快速迭代，攻击者可以低成本获取病毒来发动攻击，传统的安全检测手段难以与之对抗。而威胁情报有能力在全球追踪最新的勒索攻击事件，研究黑客攻击手法，提供实时更新的 IoC（入侵威胁指标）与 IoA（入侵攻击规则），进一步缩短攻击的检测和响应时间。

事后

考虑具有联动能力的全面解决方案

众所周知，勒索病毒一旦成功实施加密，基本没有灵丹妙药，因此亟需从传统的“知防不知攻”的被动防御向“知攻知防”的纵深积极防御转变，建立全面的信息安全防护体系，才能以最有效的方式减少损失，降低风险。

现有信息安全防护技术和手段已经不能满足现阶段的管理需要，必须与拥有威胁情报能力、标准预案、专业调查工具、安全响应专家为核心的高级威胁治理防御体系的专业厂商合作，建设联动运营管理解决方案，全面提升高级威胁治理中的恢复补救能力、高适应性能力、风险预测能力、遭受入侵后的对抗能力、被攻击后的恢复能力，确保数据泄露损失最小化。



打造安全虚拟空间

随着微信、钉钉等移动办公应用的流行，越来越多办公数据、敏感数据分散在各种终端设备上。由于移动勒索不断出现，在越来越复杂的网络环境中，想对所有设备进行统一的勒索防护难度很高。将数据保留在远程服务器云端，通过设备与数据分离的方式，可以有效防范勒索软件在不同平台上的攻击。

虚拟化桌面、虚拟手机技术能够满足移动应用数据不出数据中心，移动办公数据不落地的诉求。因为数据并不保存在移动终端上，即使设备被勒索也不会造成机密数据的泄露，同时集中管理更加有利于数据的备份，就算所有的安全策略失效，数据遭到勒索，通过备份数据也可以恢复。

挖矿专题

新型淘金术
挖矿病毒技术篇
挖矿病毒行业篇
挖矿病毒趋势篇
挖矿病毒防御篇

2017 年以来，数字加密货币的市场增长了 20 多倍，目前市场上不同类型的数字加密货币超过 2300 多种，并且这个数字仍不停的在增长。

#	Name	Symbol	Market Cap	Price	Circulating Supply	Volume (24h)	% 1h	% 24h	% 7d
1	Bitcoin	BTC	$157,598,070,417	$8,676.75	18,163,262 BTC	$35,439,731,366	-0.16%	-0.28%	9.15%
2	Ethereum	ETH	$17,638,344,475	$161.38	109,296,922 ETH	$14,475,280,244	-0.05%	-1.12%	15.73%
3	XRP	XRP	$9,876,105,242	$0.226237	43,653,776,034 XRP *	$2,292,612,576	-0.11%	-3.12%	9.39%
4	Bitcoin Cash	BCH	$5,836,125,182	$320.22	18,225,563 BCH	$4,198,778,916	0.47%	-3.23%	34.60%
5	Bitcoin SV	BSV	$5,268,880,389	$289.14	18,222,577 BSV	$4,529,533,278	0.09%	-16.84%	149.20%
6	Tether	USDT	$4,626,546,672	$0.998602	4,633,024,246 USDT *	$43,586,693,986	-0.21%	-0.72%	-0.31%
7	Litecoin	LTC	$3,571,806,627	$55.92	63,869,269 LTC	$4,474,581,985	0.18%	-3.14%	23.13%
8	EOS	EOS	$3,435,279,568	$3.62	948,893,139 EOS *	$4,492,426,808	0.05%	-2.05%	31.34%
9	Binance Coin	BNB	$2,599,372,764	$16.71	155,536,713 BNB *	$338,787,965	-0.29%	0.11%	15.28%
10	Dash	DASH	$1,118,912,242	$120.70	9,270,383 DASH	$2,220,802,055	2.26%	5.35%	129.40%
11	Monero	XMR	$1,117,835,154	$64.24	17,402,054 XMR	$135,811,392	-0.35%	-0.45%	10.68%
12	TRON	TRX	$1,105,266,851	$0.016575	66,682,072,191 TRX	$1,387,116,571	0.31%	-2.67%	18.56%
13	Stellar	XLM	$1,066,624,260	$0.053361	19,988,842,338 XLM *	$307,537,286	0.08%	0.76%	11.84%

什么是挖矿？

挖矿是指挖取数字加密货币，即利用计算能力在诸如比特币这样的加密货币区块链中创建新的区块。随着更多的区块加入到区块链中，便需要更多的算力。

2019 年可以说就是挖矿病毒盛行的一年，根据 eSentire Threat Intelligence 的报告，与 2017 年相比，挖矿病毒的数量暴涨 1500%。

新型淘金术

牟取暴利的病毒

“挖矿”并不等于挖矿病毒，这里的矿也不单单指大家熟悉的比特币。本质上，挖矿病毒是在未经他人允许的情况下，盗用他人的计算机进行挖掘加密货币，等于用他人的计算机的算力和电力成本为自己挖矿赚钱。

传统的矿工和矿厂进行挖矿最大的成本在于电力和矿机，然而由于诸如比特币有数量上限，电费增长，矿机更新换代成本高昂，以及币价频繁波动等因素，挖矿的收益也越来越少。2019 年，大多数矿厂都出现了亏损。而利用挖矿病毒感染计算机进行挖矿则不同，几乎是零成本，挖取的近乎是净利润。

与传统恶意软件相比，主机上所感染的挖矿病毒通常不易被发现，大多数挖矿病毒不会加密系统文件，更不会删除系统文件让系统不可用，甚至有些挖矿病毒能够在 CPU 高负载时（例如玩游戏时）停止挖矿让出系统资源。这就意味着网络犯罪的风险降低，而未被发现的时间越长，挖矿病毒也就可以挖到更多的加密货币。正是这样的低风险、高回报的特点，让制作挖矿病毒更容易赚到不义之财。

暗网新宠门罗币

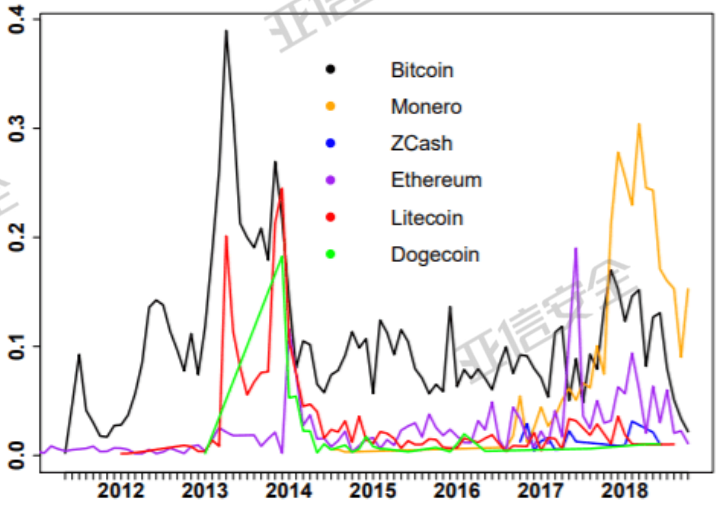
说到加密货币，大多数人第一印象是比特币。确实，早期的挖矿病毒也多是在挖取比特币，但随着挖取比特币成本的大大提升，从 ByteCoin 区块链中的一个分支增长而来的门罗币（Monero）现已成为了挖矿病毒制作者的首选。

门罗币之所以受到攻击者的如此青睐，有两个重要原因：

1. 为了保证交易不可关联、不可追踪，门罗币通过环签名技术来隐藏发送人的地址，保护发送人的隐私；通过隐地址隐藏收款人地址，保护接收方的隐私；通过环机密交易来隐藏交易的金额。

2. 与比特币不同的是，门罗币采用抗 ASIC（专用集成电路）理念，可以在算力较小的消费级硬件（例如x86，x86-64，ARM和GPU）上有效地进行开采，而比特币则需要工业级的硬件资源。

正是由于其超强匿名性和可以使用一般 CPU 跨矿的特点，使得门罗币在



【门罗币在有关挖矿的黑产上迅速主导市场份额】

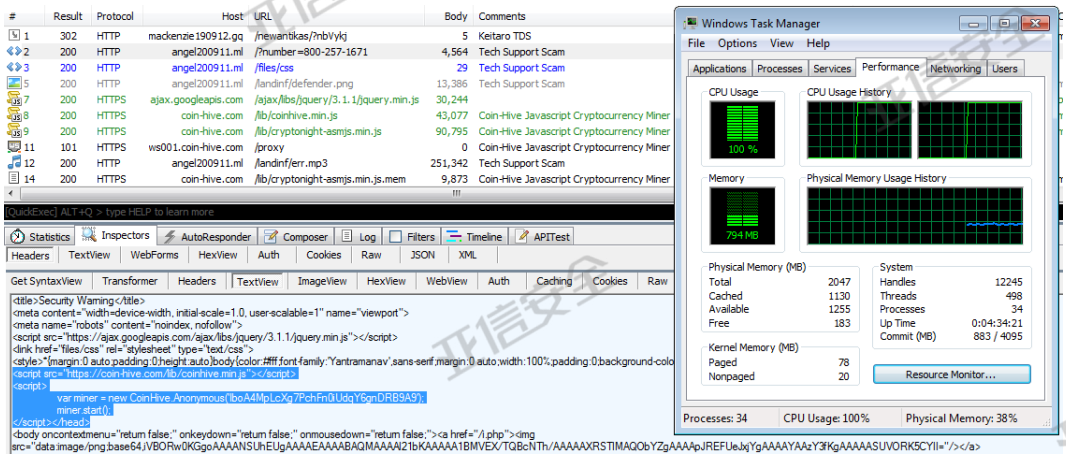
2018 年迅速成为了在暗网交易犯罪中仅次于比特币的数字加密货币。

挖矿病毒技术篇

浏览器挖矿家族

此类型挖矿病毒，主要利用开源浏览器端挖矿引擎或区块链工具，并通过感染已有网站、植入恶意代码、或者建立钓鱼网站来诱导受害者访问网站的方式，来获取不法收益。

此类型病毒主要使用 CoinHive、CryptoLoot 和 JSEcoin 等浏览器端挖矿引擎。例如 CoinHive 主要挖取门罗币，只要用户点击植入 CoinHive 引擎的钓鱼网站，CoinHive 便会调用 CPU 资源进行挖矿。即使网站窗口被关闭，病毒程序仍可打开隐藏的浏览器窗口进行挖矿，而这一系列操作，都无需用户授予权限。



【CoinHive 在浏览器中被调用，榨干 cpu 资源】

CoinHive 本身并不是挖矿病毒，但是黑客用此工具去构建钓鱼网站从而榨干用户 CPU 资源挖矿的做法，就构成了犯罪行为。

钱包小偷家族

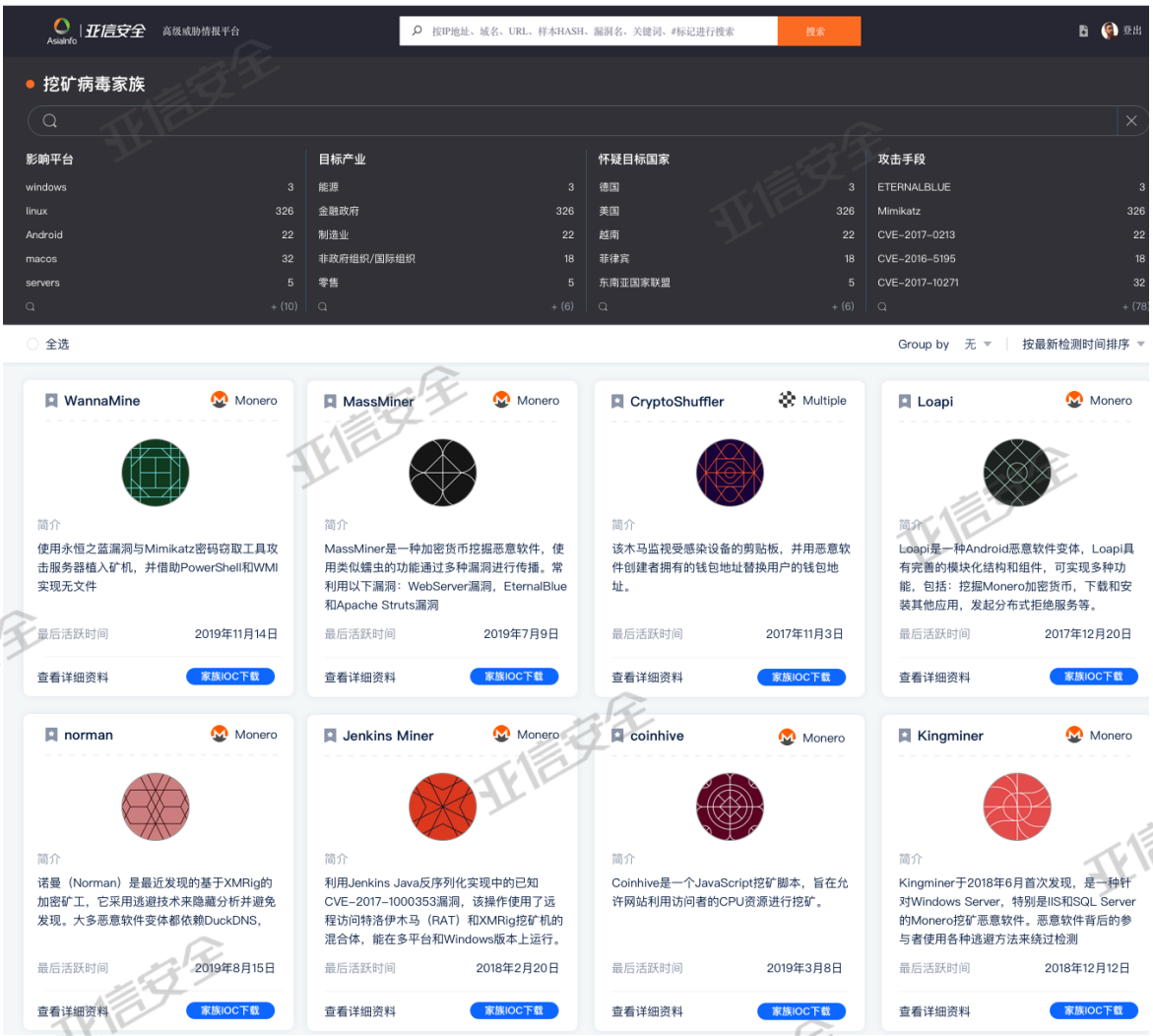
这一类型的挖矿病毒将黑手瞄准了受害者的加密货币钱包，黑客通过植入木马程序的形式监控受害者的电脑，每半秒就会扫描一次剪贴板，查找类似于加密货币钱包地址的任何内容，并将其替换为攻击者的钱包地址。受害者往往很难注意钱包地址是否被掉包，一旦受害者粘贴被掉包的钱包完成转账操作，正在交易的加密货币也就不翼而飞。

典型的病毒家族如 ComboJack（利用 CVE-2017-8579）， CryptoShuffler（利用 CVE-2017-8579）。下图为 ComboJack 所用的部分钱包地址替换表：

匹配策略	替换为	钱包类别
字符长度 42 以‘0’开头	0xE44598AB7442545069 2F7b3a9f898119968da8 Ad	Ethereum
字符长度 106 以‘4’开头	4BrL51JCc9NGQ71kWhn YoDRffsDZy7m1HUU7M RU4nUMXAHNFBE	Monero
字符长度 34 以‘1’开头	1LGskAycxvcgh6iAoigcvb wTtFjSfdod2x	Bitcoin
字符长度 34 以‘L’开头	LYB56d6TeMg6VmahcgfTZSALAQRcNRQUV	Litecoin
字符长度 13 以‘R’开头	R064565691369	WebMoney (Rubles)
字符长度 13 以‘Z’开头	Z152913748562	WebMoney (USD)
字符长度 15 以‘4100’开头	410014474125403	Yandex Money

专用恶意家族

专用的挖矿恶意软件已经发展成为多平台的威胁，它们往往被部署在可以产生最高回报率的位置。这些恶意软件主要通过网络钓鱼攻击、包含恶意代码的恶意程序或利用漏洞侵入受害者电脑，一旦感染成功，就会在内网环境中横向入侵感染更多机器。

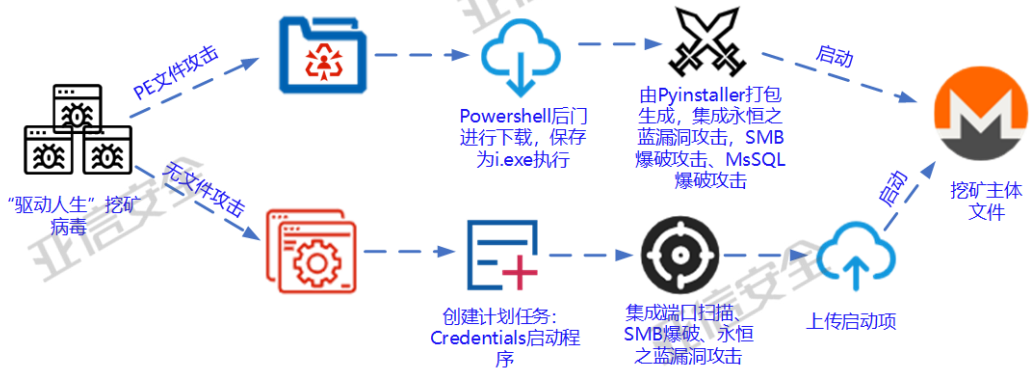


【亚信安全威胁情报团队总结的恶意挖矿病毒家族】

驱动人生

最初的 “驱动人生”挖矿病毒是利用驱动人生升级通道和永恒之蓝漏洞攻击，SMB 弱口令传播。从 2 月份开始， 该病毒不断更新，持续与杀毒软件进行对抗。根据最新发现，攻击模块不再由此前植入的母体 PE 文件进行释放，而是由 Power

Shell 后门进行下载。此次新启用的 PE 攻击模块下载地址的同时还负责 PowerShell 脚本攻击模块的下载，导致已感染的机器对其他机器发起 PE 文件攻击和无文件攻击。



【"驱动人生"攻击流程】

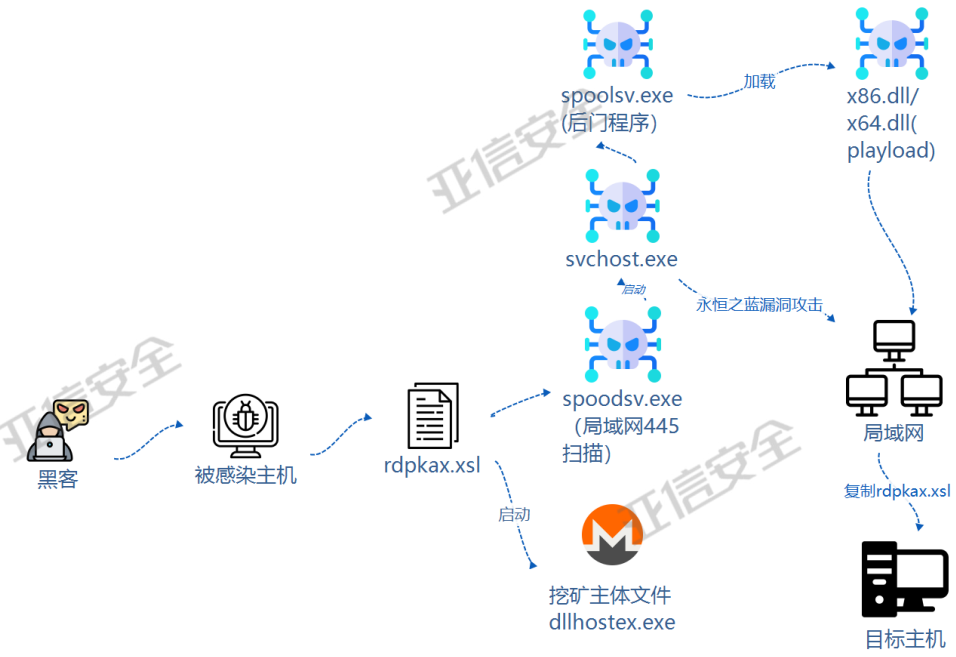
上文中我们提及了无文件攻击，无文件攻击是指攻击者无需在系统里植入具体文件就可以完成入侵。"无文件"攻击利用合法应用做掩护，甚至可以利用操作系统本身，逃过白名单的检测机制，利用位于批准列表之上且已经安装到机器上的应用进行攻击。无文件攻击的最新商业应用，就是用来感染机器挖矿。

2019 年，"驱动人生"升级了招数，改变了原有的挖矿病毒执行方式。该病毒起初利用某款软件的升级渠道下载，并通过"永恒之蓝"漏洞肆意传播，现如今，通过在 Powershell 中嵌入 PE 文件加载的形式，达到执行"无文件"挖矿的目的。这种挖矿方式没有落地文件，直接在 powershell.exe 进程中执行，这种注入"白进程"的方式完美地避开了所有检测，达到恶意挖矿的目的。

WannaMine

WannaMine 挖矿病毒的传播机制与 WannaCry 勒索病毒一致， 利用 "永恒之蓝"漏洞进行传播，在局域网内通过 SMB 快速横向扩散 。该病毒模块多，感染面广， 具备免杀功能，查杀难度高。根据亚信安全威胁情报的持续追踪，WannaMine 已发布 5.0 版本。

WannaMine 的原始"压缩包" rdpkax.xsl 含有攻击需要的所有组件 ，它是一个特殊的数据包，需要病毒自行解密分离出各个组件，组件包含永恒之蓝漏洞攻击工具集（svchost.exe 、 spoolsv.exe 、 x86.dll/x64.dll 等）。

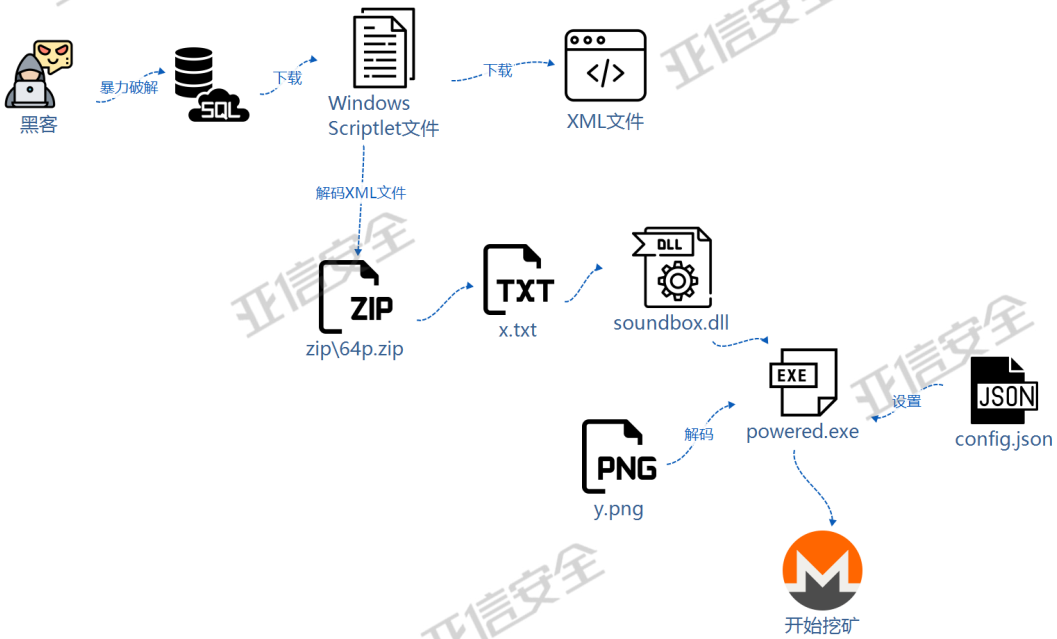


【WannaMine 攻击流程图】

KingMiner

不法分子针对特定端口，利用大量的“弱口令密码表”尝试爆破，继而控制电脑进行挖矿。由于部分 IT 管理员缺乏安全意识，在使用 SSH、数据库过程中，使用简单的弱口令，比如 123456，password，manager 等等很容易让人爆破的密码，攻击者一旦爆破成功，可随意植入木马，控制服务器。

针对 SQL 弱口令爆破已经成为黑客最常用的攻击手段，KingMiner 就是一种典型的针对 Windows 服务器的 MsSQL 进行爆破攻击的门罗币挖矿木马，可绕过虚拟机环境和安全检测。截止 2019 年年底，KingMiner 累计影响超过一万台电脑，其中广东、重庆、北京、上海等地是受 KingMiner 入侵较为严重的地区。目前可知 KingMiner 具有以下特点：针对 MsSQL 进行弱口令爆破，关闭 RDP 服务来避免其他挖矿团伙入侵、并独占服务器挖矿资源。



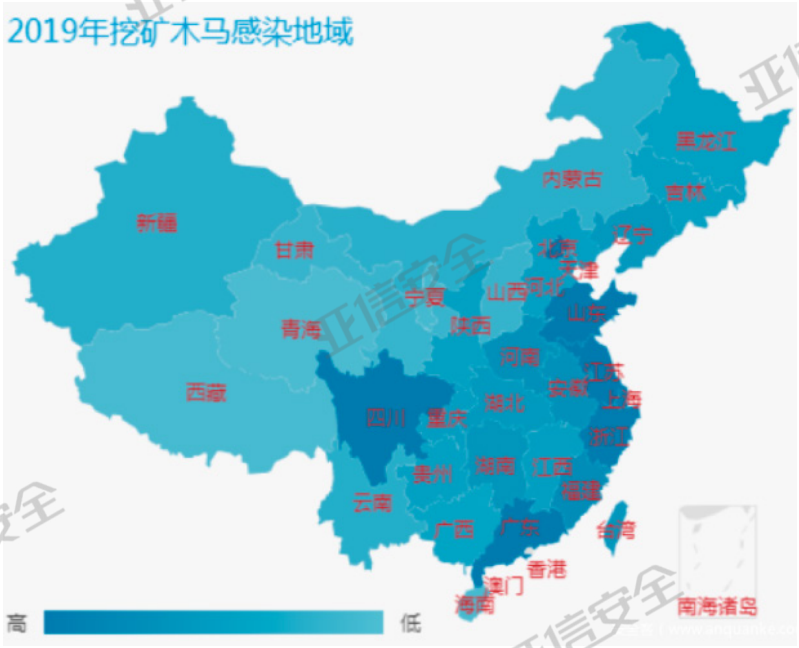
【KingMiner 攻击流程图】

挖矿病毒行业篇

挖矿病毒无处不在

根据威胁情报 2019 年的统计，在挖矿病毒数量的全球分布上，印度以 63% 位居榜首，其次是中国和泰国。从中我们可以发现一个很显著的特点：挖矿病毒青睐人口众多的发展中国家与地区，其背后一个重要原因在于，这些国家与地区有较多的 PC 保有量，而且网络安全防护意识与能力普遍较差，因此成为不法分子的重点攻击对象。

这一特点同样体现于挖矿病毒的行业分布上，不法分子更倾向于攻击制造业、能源、快速消费品等网络安全相对薄弱的企事业单位。值得注意的是，制造业占据所有行业的 47%。对于制造业来说，挖矿病毒不仅导致设备运行缓慢，而且还可能影响重要业务与数据的安全性。2019 年国内遭受挖矿病毒感染的地域分布，其中以广东、江苏、北京、四川等互联网使用人口密集区域遭受感染的情况较为严重。



许多人都坚信黑客不会盯上自己的 PC，加之现如今安全产品的防护到位，认为挖矿病毒离我们很远。殊不知挖矿病毒已修炼了隐身术悄无声息地隐藏在我们的身边。

例如，2019 年 10 月 17 日，BlackBerry Cylance 威胁研究人员最新发现：wav 音频文件中嵌入模糊恶意代码，这种将恶意代码隐藏在图片或音频文件的形式

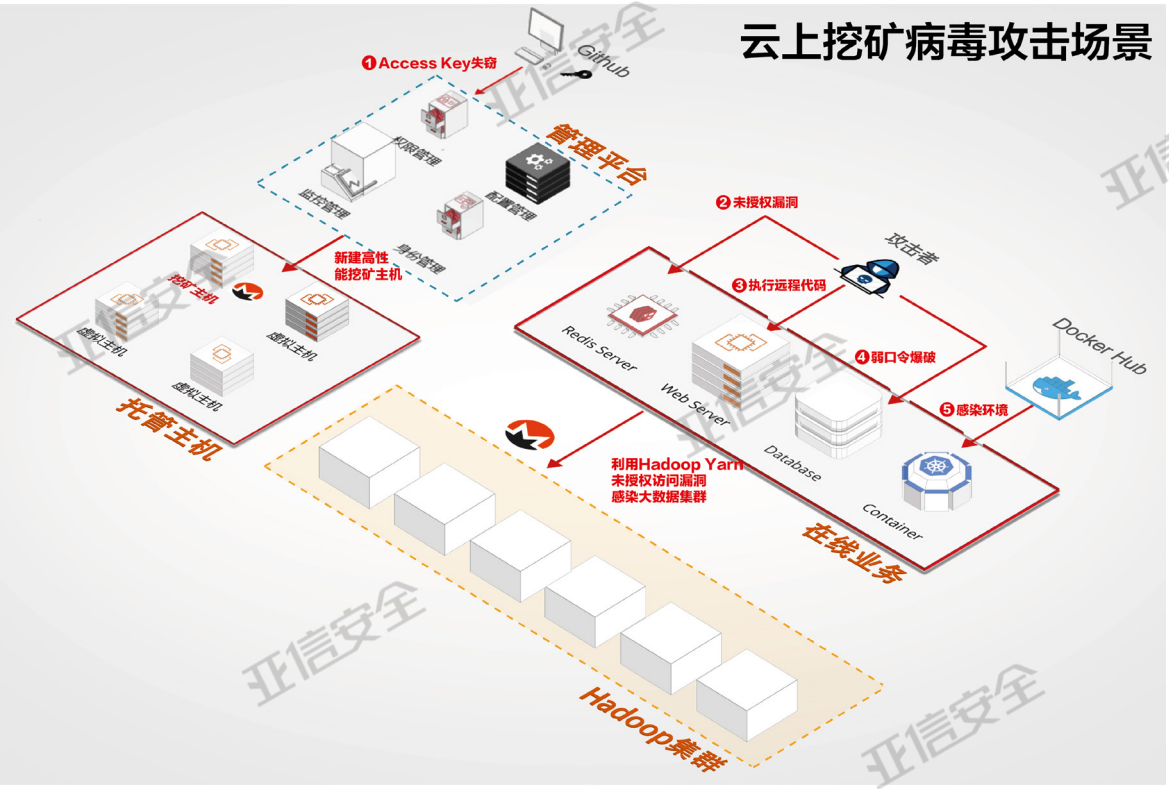
被称为“隐写术”。而且恶意代码并不影响音乐的品质，然而一旦系统加载音频解码程序，挖矿病毒就随之运行。因此如果使用者在听音乐时，即便 CPU 占用率瞬间变高，挖矿病毒也不影响音乐的正常播放，所以很难被发现。

企业云已成重灾区

普通 PC 的算力无法进行大量的加密货币挖掘，黑客需要利用特定的加密货币挖掘池注册一组受感染的计算机。根据 Bitinstant 的创始人 Charlie Shrem 的表述：“挖矿病毒只有同时渗透了一百万台计算机，才能获得可观的回报”。

相比个人电脑，企业云或是企业的数据中心拥有庞大数量的工业级硬件，一旦被挖矿病毒成功侵入，就会快速组建数量庞大的挖矿网络，贪婪的吞噬着电力，拖垮企业的计算能力。近年来国内云产业基础设施建设快速发展，政府和企业积极上云，由于挖矿病毒有一定的隐蔽性，往往发现时病毒程序已经运行数日，甚至是更长时间，并可能造成大规模机器的感染，清除起来代价不小，给企业造成极大的损失。

2019 年亚信安全的 EDR 产品在国内数据中心中就发现多起挖矿病毒感染事件，云上主机被挖矿病毒感染并组成僵尸网络进行云上挖矿。亚信安全专家团队通过对云上挖矿病毒的攻击事件进行梳理之后发现，攻击者主要通过以下方法入侵云环境。



1. 盗取 API 密钥

在这种攻击中，攻击者采取的第一步是利用盗取的 API 密钥。为了获得这些密钥，攻击者可以使用多种方法，包括从员工笔记本电脑或者开源代码网站 GitHub 上窃取，一旦员工不小心上传了他们的 API 密钥，攻击者就可以截获密钥获取云上资源的访问权限，接着通过合法的操作可以启动大量高性能主机用于挖矿。由于使用了合法的 API 密钥，这类攻击并不容易被发现，而一旦被攻击往往造成企业高额的付费账单。

2. 未授权访问

还有一类漏洞攻击是由于部署在服务器上的应用服务和组件未正确配置，导致存在未授权访问的漏洞。黑客团伙对相关服务端口进行批量扫描，当探测到具有未授权访问漏洞的主机和服务器时，通过注入执行脚本和命令进一步的下载植入恶意挖矿程序。包括利用 Redis 未授权访问漏洞，Hadoop Yarn REST API 未授权漏洞利用等。

3. 漏洞组合攻击

挖矿团伙频繁利用热门漏洞与漏洞组合对云上在线业务进行攻击。常见的漏洞包括永恒之蓝（CVE-2017-0144），WebLogic 反序列化漏洞 (CVE-2017-10271)，Jenkins (2018-1000861)，JBoss 反序列化命令执行漏洞（CVE-2017-12149），Apache Struts 远程代码执行（CVE-2018-11776）等。

4. 暴力破解

研究发现，云上暴露的公开服务如 Redis/SSH/SQLServer/RDP 仍然是挖矿利用的主要攻击目标。由于运维人员的安全意识薄弱，弱密码在互联网广泛存在。而暴力破解利用门槛低，成为挖矿木马重要的传播方式。

5. Docker 镜像染毒

自 2013 年以来微服务架构、容器化技术非常火热，特别是大部分云环境都提供这种方便的容器化部署方案。2019 年 Docker 从 Docker Hub 移除了多个含有挖扩程序或 Reverse Shell 后门的恶意 Docker 镜像，这些镜像在 Docker Hub 上已存在接近一年，估计已被下载超过 500 万次。

挖矿病毒趋势篇

利用新暴露漏洞进行攻击成为趋势

为了加强和安全厂商的对抗，挖矿病毒制作团伙会更多关注 N-day 和 1-day 漏洞的暴露并加以组合利用。由于漏洞暴露后难以在短时间修复，病毒制作者会利用漏洞暴露到被修复之间的空档期对病毒进行快速变种。

挖矿病毒仍将主要采取暴力破解进行传播

由于运维人员和开发人员的安全意识较弱，使用弱口令，甚至有些开发人员的疏忽造成 API 密钥直接暴露互联网上。这也使得针对 Redies/SQLserver/SSH/RDP 的暴力破解虽然技术门槛低，但是成效最快。

“无文件”攻击形式成新宠

挖矿病毒在系统中存活的时间越长，挖取的数字货币就越多，所以，“无文件”技术凭借其利用合法应用作掩护、不落地、易于绕过病毒检测引擎等特性成为挖矿病毒制作者的首选。

云和 IoT 安全将面临挑战

2019 年是 5G 建设的元年，IoT 设备伴随 5G 的部署将逐渐走进人们的日常生活，然而物联网设备及其与网络和云的连接安全性依然处于很薄弱的状态，数量庞大的高性能设备将成为未来挖矿攻击的主战场。

挖矿病毒防御篇

事前

◇ 管理好密钥

企业要加强 API 密钥的管理，防止密码泄露，同时防范弱口令爆破。注重密码规范性，采用多因子密码验证方案。

◇ 加强运维管理

除了加强员工的安全意识和知识的培训，对于软件项目中引入的开源库和包要做好管理和防范，特别要关注第三方代码提供者是否安全可靠，是否夹带病毒。特别加强机器的监控，时刻关注非正常计算机性能急剧下降的出现。

◇ 基于虚拟补丁的漏洞防御

报告中已经指出挖矿病毒经常使用最新出现的漏洞实施攻击，漏洞管理对防范挖矿病毒至关重要。随着 Windows 7/Windows Server 2008 正式停止更新，传统的漏洞管理方式利用漏洞扫描发现漏洞，更新补丁堵住漏洞，并不能解决接踵而来的新问题，如老旧系统无补丁更新、补丁更新导致业务中断、传统更新技术更新率不足、更新周期过长导致维护成本增加等等。

面对这样的困境，虚拟补丁（VirtualPatch）的技术概念应运而生，其能够在不中断应用程序和业务运营的情况下，建立的一个安全策略实施层，在恶意软件危及易受攻击目标之前，高效地修正有可能会攻击漏洞的应用程序输入流，也能够针对漏洞攻击行为做到有效地发现和拦截。因此，通过基于虚拟补丁的漏洞管理可以最大化降低资产受到挖矿病毒攻击的概率。

事中

◇ 在终端 / 服务器部署 EDR 产品

暴力密码破解是黑客入侵主机、获取管理员权限并植入挖矿病毒的有效手段，EDR 产品能够有效检测这种入侵行为并进行封禁，将挖矿威胁扼杀于早期阶段。

而无文件攻击通过计划任务进程调起 Powershell 下载挖矿脚本是黑客广泛采用的挖矿攻击手法，可以逃脱传统防病毒产品的扫描，但无法逃避 EDR 产品进程关联分析的火眼金睛。EDR 产品还能够记录 Powershell 执行的脚本指令，结合威胁情报的查询，精确定位挖矿脚本外联的行为。

◇ 在网络中部署 NDR 产品

挖矿程序最终需要通过网络与矿池通信进行交易，而拥有深度包检测的高性能流扫描引擎能够识别和分析多种挖矿币种协议，从而发现可疑挖矿行为，例如 stratum 协议，Cryptonight 等流量特征。同时，当一台主机被挖矿病毒控制时，企业可以利用 NDR 的阻断能力，将受感染的主机进行网络隔离，防止发生更多感染。

事后

◇ 调查分析威胁狩猎

对于已发生的挖矿病毒事件，我们需要拥有“高清”的威胁检测及响应产品，在全网范围内进行关联分析和威胁狩猎，通过对操作系统中的文件、进程、注册表和网络连接的海量信息中攻击过程进行可视化呈现，找到攻击发生的根因、还原复杂的攻击技术、并有针对性地进行响应和处置。

关于亚信安全威胁情报

亚信安全威胁情报服务采用机器学习、沙箱、NLP 等高级技术分析、处理和动态更新精准的威胁情报。对于新增目标，亚信安全威胁情报服务通过与云端对接的数十家国际情报库联动，真正做到“10 秒知天下”。我们将继续努力，紧跟互联网安全的更新潮流，努力抵御黑产，服务社会，与行业和企业一起共同面对攻击，打造晴朗的安全空间！

特别声明