AhnLab

安全月刊

2017.04 Vol. 53

Ransomware Review

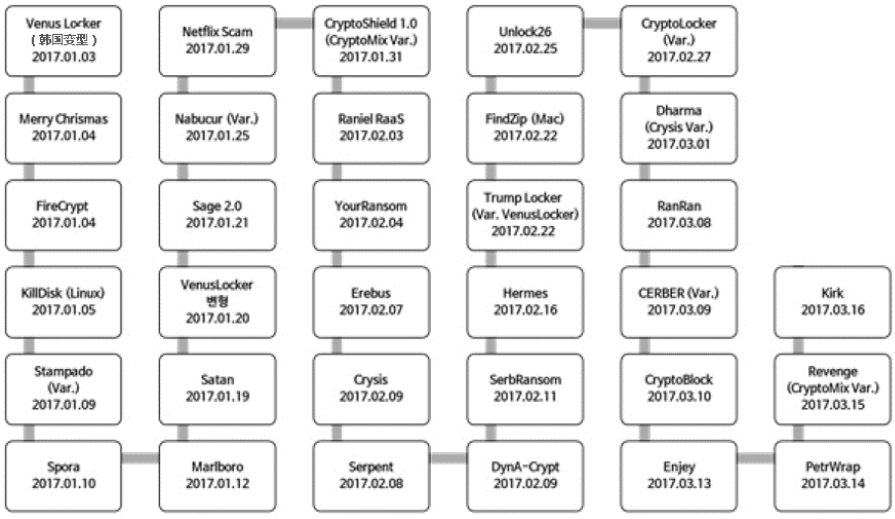
AhnLab：回顾2017年第一季度勒索软件趋势

根据AhnLab “2017年五大安全威胁展望” 报告显示，今年，勒索软件的威胁将进一步升级，攻击范围也将继续扩大。观察2017年第一季度的勒索软件趋势的结果，很显然，勒索软件目前仍然是最具威胁的网络攻击。下面，让我们来看一看2017年第一季度的勒索软件发展趋势和新型的主要勒索软件。

目前最具威胁的网络攻击仍然是勒索软件。尽管最近几年由于勒索软件的致命攻击，致使用户意识和反勒索软件安全技术得到发展，但勒索软件的破坏力依然如故。不仅如此，攻击目标已经不限定在个人PC用户，已扩大到医疗机关、金融、制造和社会基础设施等。尤其是，出现了针对各种连接网络系统的攻击事例。例如，在1月底，奥地利的一家四星级酒店的电子出入卡系统由于勒索软件而导致麻痹。如此，勒索软件攻击不减少的原因是攻击者没有理由停止作为网络攻击工具的勒索软件带来的即时和不停的货币收益。

2017年第一季度的勒索软件主要趋势总结如下：

第一，勒索软件发现数量与去年相似，但是其变型的数量呈现增加的趋势。第二，去年导致损害最大的Locky勒索软件呈现退缩趋势，而Cerber和Spora等呈现强势。第三，在传播方式方面，比起利用漏洞套件Drive-by-download的方式，传统的恶意软件传播手段，即垃圾邮件传播方式呈现增加趋势。



【图 1】2017年第一季度主要勒索软件

下面来看一下2017年第一季度全新出现的主要勒索软件。

Spora勒索软件，驻留在本地驱动器以诱导第二次感染

近年来，随着勒索软件成为恶意软件制作者赚钱的一种手段，涌出很多种勒索软件。其中，经常发现一些恶意软件是用来针对特定国家和组织劫走金钱。此次发现的Spora勒索软件主要针对俄罗斯和前苏联国家。

【图 2】Spora勒索软件感染界面

该勒索软件通过垃圾邮件传播，附件包含着HTML应用程序文件HTA文件。HTA文件是一种文件格式，旨在克服通过Web浏览器运行的HTML文件的局限。它可以使用各种脚本语言，并使用用户熟悉的Windows可执行文件图标，因此经常利用在恶意软件。

该勒索软件的特点是，删除Windows卷影复制（Volume Shadow Copy），并禁用Windows操作系统提供的文件备份和恢复功能。另外，如果被该勒索软件感染，则特定扩展名的文件全部被加密，甚至可以加密 ‘*.mdb’ 、 ‘*.sqlite’ 、 ‘*.accdb’ 等数据库相关的文件。

特别是，与其他勒索软件不同，不仅加密文件，还可以加密文件夹。将正常文件夹设置更改为隐藏，然后在执行恶意软件后运行文件夹。此方式经常用在Autorun恶意软件，因为Windows的文件夹属性默认未打勾隐藏选项， 因此如果用户没有更改属性，则很难觉察到被感染事实。

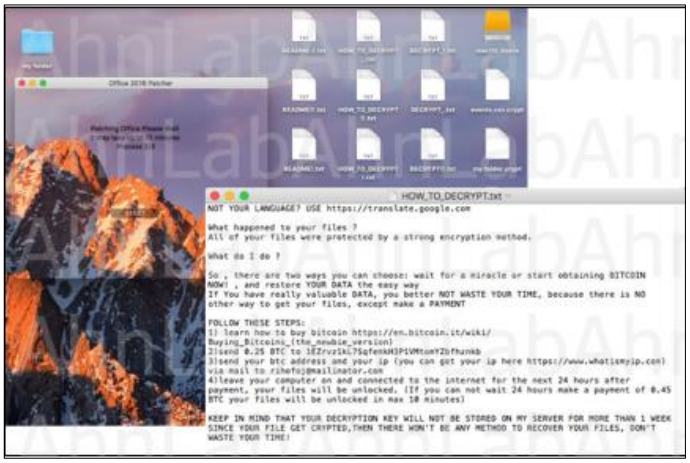
通常，勒索软件加密系统中的文件后自行删除，是为了删除感染痕迹，使其难以追踪和分析。但是，Spora勒索软件长期驻留在本地驱动器，当用户运行被感染文件夹时重新被执行。因此，要注意，如果不及时修复该文件，可能会导致2次，3次受害。

Filecoder勒索软件，面向苹果Mac用户

最近出现了一种被叫做 ‘Patcher’ 的Mac勒索软件。估计该勒索软件与2016年3月发现的KeRanger勒索软件相同，是通过Torrent程序传播的。AhnLab将该勒索软件命名为 ‘Filecoder’ 。

Filecoder勒索软件将自身伪装成补丁文件(Office 2016 Patcher/Adobe Premiere Pro CC 2017 Patcher)进行传播，并在运行时显示一个带有 “开始” 按钮的透明窗口。如果按此按钮，则开始加密文件。已确认，该加密是通过Mac操作系统的实用程序 “find” 命令来查找文件后进行。

当发生感染时，指定的文件夹中生成 ‘README’ 、 ‘HOW_TO_DECRYPT’ 等文本文件，并通过勒索记事本（Ransom Note）索要比特币。在这里，独特之处在于它不是通过网络获取公钥来进行加密，而是使用了通过随机生成的密钥来进行压缩的方式。由于这种加密方式，攻击者也无法知道密钥，即便受害者发送金钱，也无法发送恢复密钥。



【图 3】Filecoder勒索软件感染界面

但是，如果查看实际被加密的文件，可以看到已被压缩并带有一个密码。因此，如果拥有加密之前的原始文件，则可以使用破解工具来恢复该文件。与通过垃圾邮件或易受攻击的Web传播的基于Windows的勒索软件不同，大部分的Mac勒索软件伪装成正常文件后通过Torrent程序传播。为了尽可能减少勒索软件造成的损害，重要的是，必须使用正版软件并定期备份数据。

SerbRansom，塞尔维亚制造的勒索软件

过去，恶意软件制作者喜欢在恶意软件中表现自己的存在。因为当时，攻击的主要目的是通过发挥能力来感受到优越感。但是，随着通过恶意软件来获得收入，网络攻击变得更加高级，并扩大到国际纠纷。恶意软件制作者开始隐藏自身存在。
在这方面，SerbRansom可以说是偏离了最新的趋势。当然它并没有完全露出自己的身份，但至少它的出身和色彩已充分露出来。

SerbRansom的勒索记事本包含着如下信息： “您的文件夹是由SerbRansom2017加密的。如要解密数据，需要支付500美金的比特币(Your files has been encrypted with serbransom 2017, How to recover? To decrypt all your data you need to pay 500$ with BitCoin here)。”

另外，还包含了 ‘.velikasrbjia’ 文字，塞尔维亚语意味着 ‘大塞尔维亚(Velika Srbjia)’ 。此外，勒索记事本中央有塞尔维亚国旗，并表示每5分钟随机删除的文件的文章。但据说，实际上并没有删除文件。

【图 4】SerbRansom的勒索记事本

如果仔细查看勒索记事本的HTML代码，可以发现，代码中插入了YouTube网站地址。但是，由于水平和垂直的大小设置为0，因此屏幕上不会显示。当访问该YouTube网站时，如【图 5】所示，可以看到使用塞尔维亚面具的骨架和两个步枪制作的照片，并且播放着与“科索沃是塞尔维亚”运动相关的塞尔维亚歌曲。从这点来看，它是被塞尔维亚民族主义者制作的。

【图 5】SerbRansom的勒索记事本下端显示的YouTube视屏

同时，还发现了与SerbRansom相关的自动化工具，任何不会编程的人都可以点击几下就可以生成恶意代码。该自动化工具可以选择加密对象文件、加密密钥、电子邮件地址、加密时添加的扩展名和最大加密大小。还可以从各种选项中进行选择，包括用户帐户控制（UAC）、绕过虚拟环境、禁用卷影复制等系统恢复功能和应用代码混淆等。

通常，恶意软件制作者试图隐藏自身存在，但是该勒索软件的特点是积极向外泄透露自己是塞尔维亚人。

该勒索软件似乎还没有广泛传播，由于源代码粗劣，预计不会广泛扩散。这种勒索软件大部分是通过垃圾邮件传播，用户稍微注意一下，大可以提前预防。另外还需要注意的是，通过IP地址来确认国家信息可能会泄漏用户PC信息。最重要的是，不要随意打开不必要的或来源不明的邮件，最好是收到后即刻删除。

Hermes勒索软件，将文件加密后不修改扩展名

Hermes勒索软件特点是将文件加密后，并不会修改扩展名。通常，勒索软件将文件加密后修改其扩展名。扩展名与勒索记事本不仅可以将勒索软件品牌化和表现制作者的存在，而且有效通知用户文件已被加密。

如果不修改文件名和扩展名，一般计算机用户难以区分是由于勒索软件导致的错误还是计算机自身错误。因此，勒索软件通常会更改或添加扩展名。

【图 6】Hermes勒索软件的勒索笔记本

当被Hermes勒索软件感染，则出现一个 如【图 6】所示的窗口。该勒索笔记本表示，如何联系以进行恢复，但恢复费用并未告知。

DynA-Crypt勒索软件，删除桌面数据

勒索软件的恶毒已经是众所周知的。加密用户数据，并要求钱财的行为本身就是恶毒的。但是，DynA-Crypt勒索软件的恶毒更高一层。与典型的勒索软件不同，DynA-Crypt勒索软件是一个64位的可执行文件，不能在32位操作系统上运行。目前仍然有很多用户使用32位操作系统，即使是64位操作系统，也有可能被利用32位可执行文件的勒索软件感染。由于这种原因，大多数勒索软件制作者使用32位可执行文件。但是，DynA-Crypt勒索软件制作者大胆地选择了64位。
该勒索软件感染用户PC后要求支付比特币50美金。虽然不是很大金额，但比一般的勒索软件小得多。据说，每五分钟随机删除一个文件。

【图 7】DynA-Crypt勒索软件的勒索笔记本

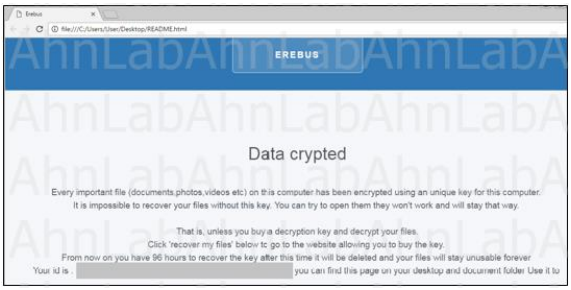
然而，这种勒索软件感染并不以文件加密结束，还删除桌面上的文件。事实上，已确认桌面上的所有快捷方式文件被删除。然后删除卷影副本以干扰文件恢复。此外，通过更改注册表来阻止任务栏管理器的运行，以妨碍用户使用PC。

这还不是结束。它还包括一个泄漏用户PC上的信息的InfoStealer功能。这个勒索软件泄漏的数据有‘屏幕截图’、‘用户PC的录音’、‘键盘记录’，还有保存在Chrome、FireFox、Skype、Steam等的帐户信息等。

尽管DynA-Crpyt勒索软件的传播路径尚不明确，但是大部分通过垃圾邮件传播。因此，不要随意打开来源不详的电子邮件，最好是立即删除。此外，当要运行的文件要求不必要的用户帐户控制（UAC）时，建议再想一次后决定是否要运行。

Erebus勒索软件，下载Tor

Erebus是一个具有下载Tor客户端功能的勒索软件。



【图 8】Erebus勒索软件的勒索记事本

该勒索软件包含了通过绕过用户帐户控制（UAC）功能提升权限来执行的功能，需要用户的注意。

Erebus勒索软件的名称与2016年9月由另外一个安全提供商首次发现的勒索软件相同，但其特征完全不同。至于通过何种方式传播，到目前为止，尚不清楚。

当运行该勒索软件，则通过勒索记事本提供受感染文件列表和感染事实，而且提供连接到支付网站进行恢复的按钮。界面顶部标有”EREBUS”，提示0.085BTC（$90）的恢复费用。

TrumpLock勒索软件，利用社会问题

利用美国总统特朗普的TrumpLock勒索软件在文件加密后使用了特朗普总统的照片，而且他们的官方电子邮件地址也使用“TheTrunpLocker”帐户。该勒索软件在加密文件后，如【图 9】所示，更改桌面。

【图 9】TrumpLocker勒索软件将文件加密后更改的桌面

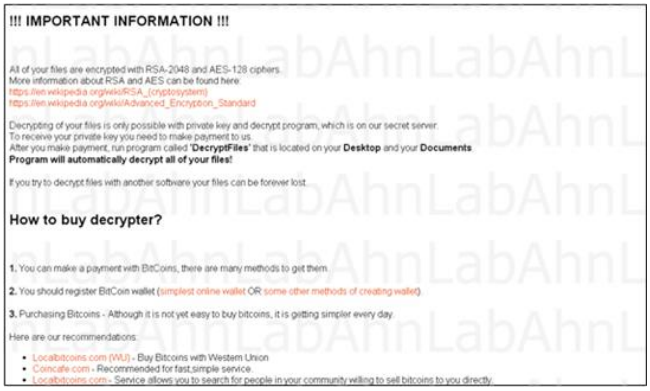
TrumpLocker勒索软件的文件加密与通常的勒索软件不同。当加密整个文件时，附加扩展名“TheTrumpLockerp”。相反，不是加密整个文件时，会对文件的前1024个字节进行加密，并附加扩展名“TheTrumpLockerp”。附加生成的RansomNote.exe文件保存到桌面。如果运行该文件，则出现特朗普总统的照片。

【图 10】执行RansomNote.ext的背景

如此，网络攻击者正在利用社会问题制作和传播。这种攻击方法可以刺激用户的好奇心，并且更加有效提升恶意代码运行概率。因此，请注意，不要随意点击来源不详的URL或运行附件。

熟悉的名字，Marlboro勒索软件

利用世界有名的烟草公司Marlboro名字的勒索软件被发现。据说，Marlboro勒索软件在垃圾邮件附上Word文档文件传播。当运行附件时，将提示用户更改MS-Word环境设置以查看和更改受保护的内容。但是，受保护的内容根本就不存在。这只是一个欺骗用户的信息，以便执行里面包含的恶意宏。当打开附件时，它会运行内部恶意宏，通过免费的虚拟Web主机帐户下载和运行EXE文件。如果文件成功下载，则会对文件进行加密，并附加“oops”扩展名。



【图 11】Marlboro勒索软件的勒索记事本

此外，加密文件所在的每个文件夹都会生成“_HELP_Recover_Files_.html”的勒索记事本文件，并要求支付0.2BTC（$180）的恢复费用。此外，勒索记事本还提到使用RSA-2048和AES-128对文件进行加密，但这是一个虚假的陈述。事实上，此次发现的Marlboro是使用XOR混淆的。在原始Excel文件中，可以看到填充0的部分以8个字节单位反复相同的字符串。8个字节的字符串的值在每次被感染时都会更改，可以确认加密密钥值是以8个字节为单位随机生成的。实际，当使用8个字节的字符串试图再次执行XOR运算时，可以确认它与原始文件的值相同。这是因为如果执行两次XOR运算的话，会变成原来的值。
如果电子邮件附件的恶意宏文件正常运行，则会在文件加密后生成一个解密工具。生成的解密工具名为“deMarlboro”。这就是该勒索软件为什么被称为Marlboro的原因。

再次出现的Nabucur勒索软件

VirLocker（又称为VirLock或VirRansom）过去被称为“Operation Global III”，在2017年以新的版本再次出现。AhnLab将这种类型的勒索软件通常归类为Nabucur。Nabucur不是像CryptorLocker、TeslaCrypt、Cerber这样的主流勒索软件，具有与这些勒索软件不同的特性。

大多数的勒索软件在加密文件后将自身删除，因此很难追踪恶意代码痕迹。并且使用RSA或AES等加密技术，如要恢复原始文件，则需要解密密钥。

然而，Nabucur勒索软件使用了在原始文件中添加感染代码来更改正常文件的方法，这与病毒感染正常文件的方法相似。Nabucur的另一个特点是与其他勒索软件不同，在加密文件之后，使用锁屏通知（Screen Locker）而不是勒索记事本，以阻止受害者使用PC。

【图 12】Nabucur的锁屏通知（Screen Locker）

如【图 12】所示，Nabucur加密后显示的锁屏通知包含了“由于检测到非法软件使用，锁定系统。如要解除锁定，需要支付比特币。”的信息。独特的一点是，金额用韩元（KRW）标记，如【图13】所示，Google地图显示了可以在韩国存款比特币的ATM的位置。

【图 13】Nabucur显示的在韩国可以存款比特币的ATM位置

与其他勒索软件不同，Nabucur加密的文件将其扩展更改为“exe”。由于在大多数的系统，文件夹选项中启用“隐藏已知文件类型的扩展名”选项，因此用户很难察觉文件被感染后扩展名变成“exe”的加密文件，Nabucur似乎利用了这点。另外，如果用户未认知文件受感染事实，将该文件通过移动式硬盘或即时信息程序传送个另一个用户，则其他PC可能也会感染Nabucur。

到目前为止，我们了解了今年第一季度新发现的主要勒索软件。预防勒索软件最重要的是用户的注意。不要打开不必要的或来源不明的电子邮件，最好是即刻删除。另外，不要运行来源不明的电子邮件的附件，如要运行，请在运行前使用防病毒程序检查后运行。对于一些业务文件、机密文件和各种图像文件等重要数据，建议使用PC以外的存储设备定期备份。

目前，AhnLab V3产品群和APT响应解决方案-MDS产品可以检出这些勒索软件。

AhnLab

安全月刊

http:// cn.ahnlab.com
http://global.ahnlab.com
http://www.ahnlab.com

关于AhnLab

Ahnlab的尖端技术和服务不断满足当今世界日新月异的安全需求，
确保我们客户的业务连续性，并致力于为所有客户打造一个安全的计算环境。
我们提供全方位的安全阵容，包括经过证实的适用于桌面和服务器的世界级防病毒产品、
移动安全产品、网上交易安全产品、网络安全设备以及咨询服务。
AhnLab已经牢固地确立了其市场地位，其销售伙伴遍布全球许多国家和地区。

AhnLab

北京市朝阳区望京阜通东大街1号望京SOHO塔2 B座 220502室 | 上海市闵行区万源路2158号18幢泓毅大厦1201室
电话：+86 10 8260 0932（北京） / +86 21 6095 6780（上海） | cn.sales@ahnlab.com