AhnLab

安全月刊

2016.04 Vol. 41

Ransomware Trend

紧急通告，勒索病毒的扩散（上篇）

2016年第一季度，最恶勒索软件有哪些？

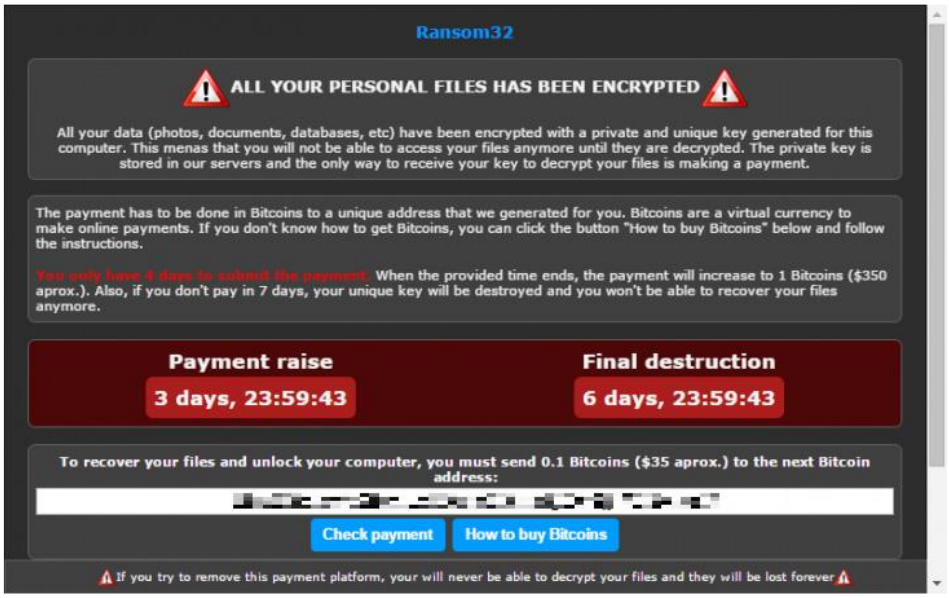
1989 年出现了PC Cyborg Trojan（AIDS），其作者为Joseph Popp。该病毒会修改系统AUTOEXEC.BAT文件来监控系统启动次数，一旦系统启动次数达到90次时，系统所有的文件也会被加密，导致系统无法正常启动。然后，显示勒索信息，声称用户的软件许可已经过期，要求用户支付赎金，以解锁系统。包括Wikipedia的计算机安全相关的记录媒体都述说PC Cyborg Trojan为最初的勒索软件（Ransomware）。

2005年出现的Gpcode勒索软件使用RSA算法加密用户文件（扩展名为 .doc, .txt, .pdf, .xls, .jpg, .png, .cpp, .h 等），然后诱导用户购买解密工具。

2013年8月出现的CryptoLocker为起点，勒索软件作为全世界黑客犯罪团伙谋利的最好的手段巩固了其地位。2016年3月，有一类被命名为“Locky”的新种勒索软件正在肆虐全球，它利用MS Office的宏功能传播病毒。本文将重点阐述2016年第一季度成为安全主题的主要的勒索软件。

01. 基于JavaScript撰写的勒索软件“Ransom32”

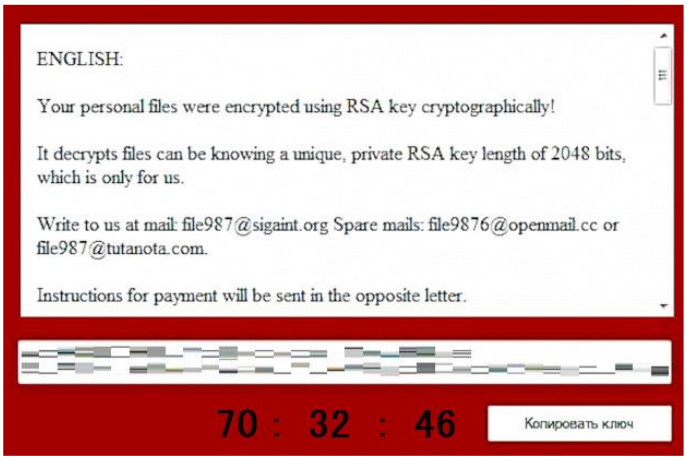
Ransom32是首款利用脚本程序语言JavaScript撰写的跨平台的勒索软件。 通常，垃圾邮件附件的JavaScript代码已进行了混淆，当运行脚本的同时下载勒索软件到用户计算机并运行。它使用Tor网络，并使用AES密钥和RSA公钥进行加密。



【图 1】被Ransomer32感染界面

02. 通过钓鱼邮件传播的勒索软件“CryptoJoker”

CryptoJoker使用AES 256密钥进行加密，并通过钓鱼邮件传播，加密后文件扩展名后缀“.crjoker”。加密后显示的勒索信息使用英语和俄语。



【图 2】 被CryptoJoker感染界面

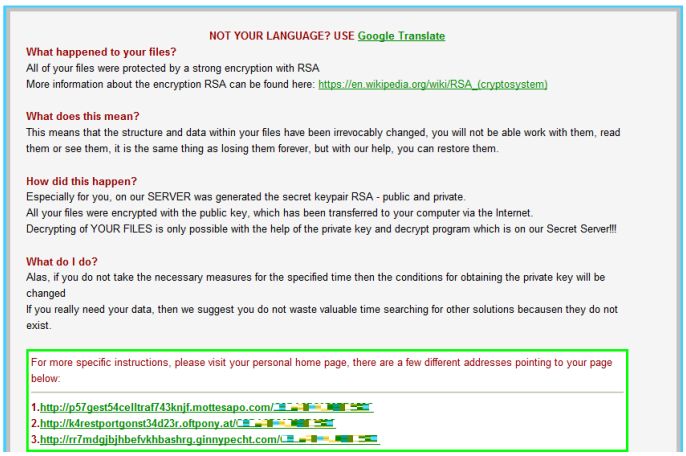
03. 通过远程控制直接感染的勒索软件“Lechiffre”

该勒索软件渊源于法国，表示“数字”或“加密”意义的“Lechiffre”跟一般的勒索软件不同。攻击者首先找到企业网络中存在安全漏洞的目标计算机，然后远程访问目标计算机，并手动进行感染。加密后文件扩展名后缀“.LeChiffre”，使用Base64加密。

【图 3】 被Lechiffre感染界面

04. 扩展名变成MP3的勒索软件“TeslaCrypt 3.0”

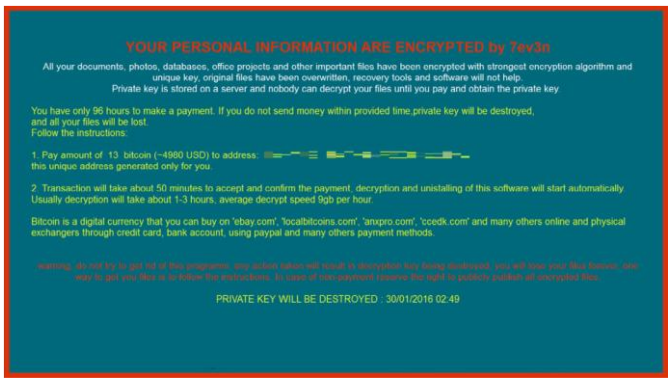
随着TeslaCrypt 3.0的出现，加密算法和文件名后缀的扩展名发生了变化。TeslaCrypt 3.0将文件加密后，文件扩展名后缀“.xxx”、“.TTT”、“.Micro”、“.mp3”等。



【图 4】 被TeslaCrypt 3.0感染界面

05. 禁用Windows键盘按键的勒索软件“7EV3N”

7EV3N伪装成情人节促销票导购广告电子邮件发送给用户，诱导用户点击邮件中的链接地址，点击的同时用户PC即被安装勒索软件。该勒索软件通过修改各种系统设置和引导选项，禁用用户PC的键盘按键及系统恢复选项。加密的文件扩展名后缀“.R5A”，文件名从1开始自动递增。



【图 5】 被7EV3N感染界面

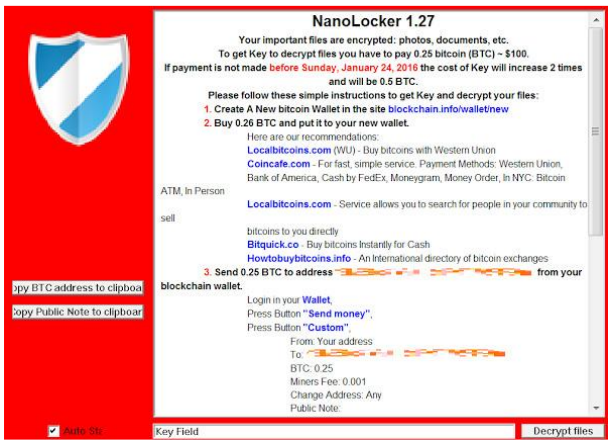
06. 利用钓鱼攻击工具包（angler exploit toolkit）的勒索软件“HydraCrypt”

HydraCrytp 利用钓鱼攻击工具包进行传播，加密的文件扩展名后缀“.hydracrypt_ID_[8位随机文字]”，使用AES密钥进行加密。

【图 6】 被HydraCrytp感染界面

07. 通过伪造的PDF文件感染的勒索软件“NanoLocker”

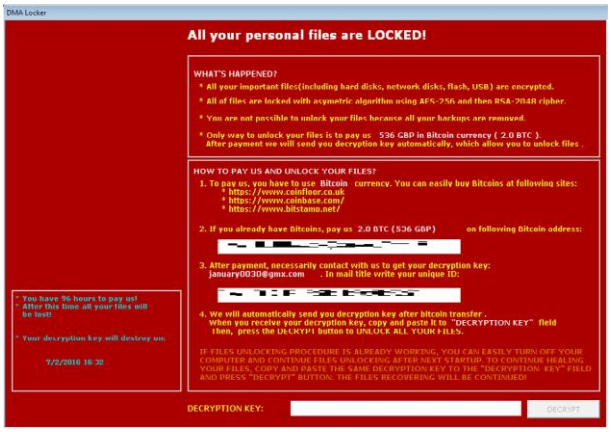
NanoLocer使用AES、RSA加密密钥，并在电子邮件附上伪造的PDF文档，诱导用户运行并感染。加密后显示感染界面，并提供付款和文件恢复按键。



【图 7】 被NanoLocer感染界面

08. 使用白名单方式的勒索软件“DMALocker”

DMALocker使用AES加密密钥，采用白名单方式加密，对于攻击者指定为白名单的一些文件夹和文件扩展名不进行加密。



【图 8】 被DMALocker感染界面

09. 扩展名后缀ID的勒索软件“UmbreCrypt”

UmbreCrypt通过电子邮件附件传播，并使用AES加密密钥。加密后文件的扩展名后缀“umbrecrypt_ID_[感染PC_id]”，采用白名单方式加密，对一些攻击者指定为白名单的文件夹不进行加密。

【图 9】 被UmbreCrypt感染界面

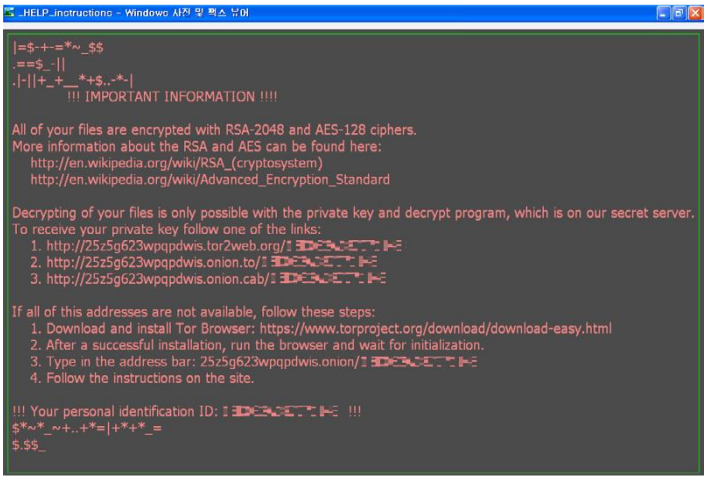
10. 弹出LiveChat在线聊天的勒索软件“PadCrypt”

PadCrypt也是通过电子邮件附件形式传播。当受害者接收电子邮件时被富有恶意勒索软件的扩展名为“.pdf.scr”的文件感染，并使用AES密钥加密用户文件。随后弹出勒索信息，要求用户支付赎金。仔细一看弹出窗口的左下角，可以发现有个“Live Chat”按钮，点击后弹出Live Chat实时在线聊天窗口。据称是首款弹出实时在线聊天Live Chat窗口的恶意勒索软件。

【图 10】 被PadCrypt感染界面

11. 通过大量垃圾邮件传播的勒索软件“Locky”

Locky是通过电子邮件附件或在执行脚本文件感染用户PC的勒索软件。Lcoky使用AES密钥进行加密，加密后文件的扩展名后缀“.Lokcy”。目前，Locky与Dyre、Dridex作者联手发送大量的垃圾邮件，加重了用户的损失。



【图 11】 被Locky感染界面

12. 首个在Mac OS X平台上运行的勒索软件“Keranger”

Keranger是第一个能够在Mac OS X平台上运行的勒索软件，使用RSA密钥加密，加密后文件的扩展名后缀“.encrypted”。该勒索软件的传播是通过Bit Torrent下载软件Transmission来实现的。

【图 12】 利用在传播Keranger的官方网站

13. 篡改磁盘主引导记录(MBR)的勒索软件“Petya”

2016年3月，出现了一种名为“Petya”的变种勒索软件，通过电子邮件附件传播。该勒索软件会篡改磁盘主引导区，强制重启系统后运行引导扇区中的恶意代码，加密硬盘数据后显示勒索信息，通过Tor网络索取比特币。

【图 13】 被 Petya 感染界面

如上述的勒索软件，恶意软件制作者持续制作和传播多样的勒索软件，这些勒索软件甚至可以轻松绕过传统安全解决方案的防线，传统的安全解决方案已很难检测到这种勒索软件。另外，勒索软件使用加密算法进行加密，文件被加密后实际上很难恢复。如要防御恶意勒索软件，需要用户的努力。首先，不要随意打开来源不明的电子邮件附件，最好收到后即可删除；然后，平时注意备份重要文件等以规避恶意勒索软件可能带来的风险。

AhnLab的V3产品系列和企业版高级威胁响应解决方案AhnLab MDS可以检测上述的勒索软件。为了防止被勒索软件感染，V3用户需要将产品的引擎更新为最新版本，MDS用户则必须启用“运行保留（Execution Holding）功能。

紧急通告，勒索病毒的扩散（下篇）

勒索软件，有哪些变化？

2013年夏天，出现了一个被叫做“CryptoLocker”的史上最恶劣的恶意勒索软件，CryptoLocker的出现可以说是网络犯罪领域的新转折点。该恶意勒索软件利用RSA加密文件，如果文件被加密，短期内基本无法解密文件，使受害者遭遇前所未有的挫折。另外，为了隐藏赎金的移动路径，使用Tor网络，并要求以比特币支付赎金。还有，利用域名生成算法（Domain Generation Algorithm，DGA）生成的URL联系攻击者。这些新转折使恶意代码制作者对于勒索软件的稳定性及其带来的收益抱有期待，并确信这些手法可以用在多样的网络攻击。下面将具体介绍勒索软件的传播方式和最新的勒索软件趋势。

勒索软件的传播手段

CryptoLocker通常以电子邮件附件或者组织使用的即时信息程序来传播。这种传播手段从2000年初伴随着垃圾邮件的出现便开始恶意利用。但是，随时随地可以连接到互联网的当今IT环境下，这种传统的传播方式仍具有威胁。因为，不管是为了个人事务还是公司业务，大多数的人们通过即时信息程序、电子邮件和社区网站来进行沟通，这也正迎合我们的日常生活方式。只要在IT环境下的日常行为模式没有多大变化，这种传播方式仍然会持续。此外，攻击者为了最大提高恶意代码传播率，持续寻找更好的方法。伪造各网站提供的下载文件，或利用Windows操作系统安全漏洞、应用程序的安全漏洞、Web服务器的安全漏洞等传播恶意代码并感染。还利用恶意广告（Malvertising）手法，通过在线广告网络和网站传播恶意软件，或者利用Bit Torrent下载软件传播恶意代码。

传播文件的形式

- 扩展名为DOC、PDF及图标

初期的勒索软件伪装成DOC及PDF文件形式传播，目前仍然被黑客广泛应用。普通用户如果收到电子邮件附件为MS Word或PDF类型的文件，毫无怀疑地点击打开附件。恶意附件一旦被运行，用户PC上的文件夹和文件就会被加密导致无法打开。

- 伪装成屏保程序文件（扩展名为.SCR）

组织建立的安全策略中通常会包含设置屏保程序（Screen Saver）。但是，几乎很少直接运行屏保程序文件来设置屏保。尽管如此，屏保程序文件经常被用在恶意代码传播。这是因为SCR扩展名的文件如同EXE扩展名的文件，点击后即可执行。攻击者就是利用这一点传播恶意代码。

-文档包含宏

从伪装成文档文件形式进一步发展的恶意代码即是正常文件包含宏代码的形式。当打开这种包含宏代码的文档，则显示无法识别的文字，并诱导用户为了正确识别文内需要启用“宏”功能。文档包含的宏代码是混淆的JavaScript代码，为的是难以识破制作意图。通过该JavaScript试图与外部连接，然后下载恶意软件并安装·运行。

- JavaScript文件（.js）

最近经常被发现利用脚本程序语言JavaScript的勒索软件。攻击者将电子邮件附件的文件形式从可执行文件换成JavaScript文件，即通过JavaScript文件传播病毒。当文件被运行，即可连接外部，然后下载恶意软件并安装·运行。

进化的勒索软件

- 采用白名单方式的加密

在IT环境下，所谓的白名单往往用在合法和不合法之区分。组织允许访问的IP、URL及业务上必须使用的一些程序列表属于这一类。勒索软件也开始使用这种白名单的概念出现，这类勒索软件具有不加密对象列表。即，对于攻击者指定的目录和文件不进行加密。另外，还出现了一种对系统语言为俄语的PC不进行加密的勒索软件。

- 实时在线聊天（Live Chat）

最近出现了一种提供实时在线聊天功能的勒索软件。测试当时因无法正常连接，无法进行聊天。但是如果连接正常的话，预计可以与攻击者或代理人进行谈话。但在聊天过程中，可能会加重受害者的损失或者导致其他的犯罪，需要多加注意。

- 高水准的设计

勒索软件的变体大多以独特的设计来炫耀自己。但是仅仅模仿功能的变体只能提供粗劣的设计和功能。最近出现的一种勒索软件展示的美丽的UI设计看似可信度很高，它与以往勒索软件的文字中心的单调的设计完全不同。比喻“被书写的”或者“这是命运”的Maktub勒索软件将受害用户重新连接到主站。和其他勒索软件相比，Maktub网站设计很漂亮，而且说明用词很文明礼貌。使受害者产生一种错觉，看到的不是受到攻击的界面，而是一个设计相当不错的网页。

- RaaS(Ransomware as a Service)

如同代办公司按客户所需提供服务，黑客也开始向大众提供RaaS（勒索软件即服务）。当有人欲想制作和发布勒索软件时，黑客即可提供该服务。黑客已制作好服务网站，正等待着委托人。服务网站还提供购买的勒索软件传播程度和感染程度等信息，努力维持与委托人的信赖关系。

勒索软件非法交易市场前景

- 勒索软件市场总结

从2013年开始勒索软件如雨后春笋般迅速成长起来，而且变得越来越高级化，逐渐具备了自己的服务体系。在此过程中，仅追求简单的功能和外形的一些二流勒索软件只是昙花一现。根据实现扩散和损失程度的技术，勒索软件的生命也有所不同。使用相同的名称而版本继续上升的Cryptowall或者TaslaCrypt等勒索软件就是代表的一个例子。除非是谁都预想不到的新的勒索方式，否则日后在市场占优势的仍然是扩散和导致付款的勒索软件。

- 通过携手扩张领域

从2000年中期开始活跃起来的垃圾邮件制作者不同于过去的简单的广告转发活动，现在已经在联系新的资金负责人开始了新的活动。2014年夏天到去年末在全世界恶意软件传播最多的Dyre恶意软件通过电子邮件附件方式传播，当用户点击打开附件时将恶意软件安装到用户电脑，随后用户的金融信息和个人信息被泄漏。与这个Dyre恶意软件携手的垃圾邮件制作者又与Locky勒索软件制作者携手大量传播恶意勒索软件。这种联手不局限于垃圾邮件制作者。勒索软件制作者根据自己拥有的勒索软件相关的基础设施、文件下载、C&C服务器基础设施及受害者的付款情况等，又谋求与其他组织的携手。

- 组织性•大规模攻击的可能性

1989年出现的最初的勒索软件PC Cyborg Trojan(AIDS)也向受害者要求支付189美金或378美金。2013年开始出现的最近的勒索软件也要求200美金到400美金之间。但是最近发生的某医院被勒索软件感染后，攻击者要求该医院支付9000比特币(360万美金)。据了解，医院支付了40比特币(1万7000美金)后，被加密的数据全部都恢复。

该事件给我们两点启示。

第一，攻击者有可能再次攻击支付过一次费用的攻击对象。当然，对此该医院也已认知，必定会对于医院的基础设施进行检验和强化安全，以防止再次受到攻击。但还要考虑到一点：攻击者也不会使用相同的方式来攻击，很有可能准备目前安全策略无法防御的攻击方式。

第二，勒索软件的攻击水准不会始终停留在400美金的赎金。通过有漏洞网站传播恶意勒索软件或利用电子邮件附件方式的勒索软件要求的赎金大同小异。但是，仅一次的攻击可以取得5倍以上利益的勒索软件事件的出现，表示攻击者也开始转向高收入的市场。根据恶意软件收集的个人和企业的各种信息，可分类收益对象。另外，我们还要留意，针对特定组织的完全以金钱利益为目的的勒索软件的组织性的传播可能会成为APT攻击的新的类型。

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