AhnLab

安全月刊

2015.12 Vol. 38

Ransomware

勒索软件蔓延至全球，AhnLab揭开勒索软件真面目

2015年4月，通过韩国社区网站横幅链接传播的勒索软件 CryptoLocker，成为了上半年最大的网络安全主题。 CryptoLocker首次被发现于2013，2014年已在海外成为了最热门的安全主题。
经过多年的演进，勒索软件已经成为当今最主要的恶意软件类型之一，通过锁定电脑或对文件进行加密，从而对用户进行勒索。根据赛门铁克安全大数据技术显示，勒索软件威胁已经蔓延至全球范围，在过去1年里，受勒索软件影响最严重的12个国家中有11个是G20组织的直接或间接成员国，其中受影响最严重的国家包括美国、日本、英国和意大利等。[1]
最近，在韩国也陆续发生了勒索软件事件，企业和个人都受到了很大的打击。并且，这种勒索软件持续发现新的和变种。恶意软件制作者已将勒索软件看成是索取金钱利益的手段，扩大攻击目标针对广泛的对象进行狂轰。

对此，本刊将集中分析蔓延至全球的勒索软件，揭开勒索软件的真面目。

何谓勒索软件

勒索软件最早出现于2005。当时勒索软件主要活动在俄罗斯和东欧的国家。但是，随着互联网的发展和传播方式的多样化，已蔓延到全球。勒索软件是黑客用来劫持用户资产或资源并以此为条件向用户勒索钱财的一种恶意软件。勒索软件在对用户计算机中的目标文件进行加密后，就会威胁用户如果不在限定期限内通过 Paypal 或比特币等支付赎金，文件将可能永远无法解密。勒索软件通过多样的方式向不特定的多数目标传播，而且用户为了赎回遭到加密的文件支付费用，这使得一旦攻击就确保了高收入。这也是多年来勒索软件的攻击手法一再进化，并且不断出现其变种的原因。

主要传播手段

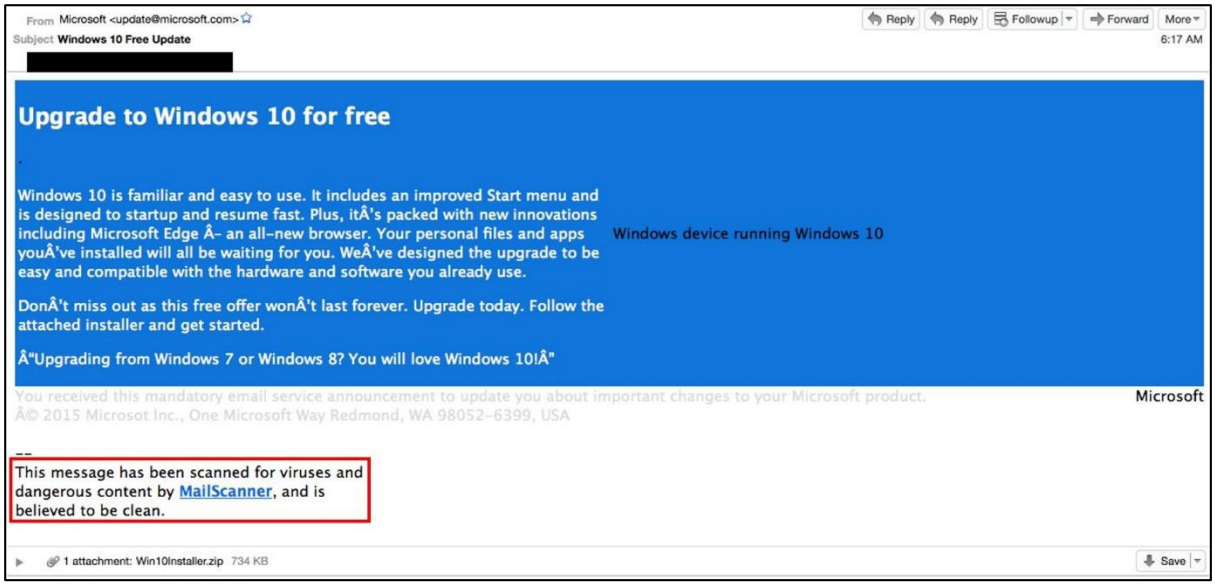
1. 通过电子邮件附件传播

通过电子邮件附件传播手段很早开始已在使用并且是很有效。电子邮件利用社会工程学手法引诱用户点击邮件文本中的链接或者打开并执行伪装成附件的恶意软件，从而导致用户计算机被感染。最近被报告的勒索软件传播手段中，最多是利用电子邮件附件传播。电子邮件表面上看起来跟正常的邮件没有区别，但仔细一看，可以看出一些可疑的地方。因此，千万不要随意打开来源不详，尤其是扩展名为 exe、scr 的电子邮件附件，也不要点击邮件文本中包含的链接。即使是来源明确，也要再三确认后谨慎打开。

[1] 工控中国http://www.gkzhan.com/news/detail/78472.html

<通过电子邮件附件传播勒索软件事例>

今年微软公司发布 Windows 10 以后，过几天就出现了伪装成 Windows 10 升级安装包的勒索软件通过电子邮件传播。



【图 1】 Win 10的开始菜单

攻击者伪装成微软公司发送 Windows 10 升级包。文本中还包含了“此消息已进行病毒扫描，并没有异常”的文章。用户丝毫没有怀疑就下载附件并运行。

2. 通过浏览器攻击程序或偷渡式下载(Drive-by-Download)来感染

当用户访问有名的社区网站，即重定向到具有漏洞的网站，同时下载勒索软件到用户的计算机并安装。为了防止被这种恶意软件感染，正在使用的各种应用程序需要更新为最新的版本。Exploit Kit 主要利用的应用程序有 Flash Player、Acrobat Reader、Inter Explorer、Silverlight 和 Java 等。当发现这些应用程序存在漏洞，制造商即刻提供补丁，用户也需要及时更新。

偷渡式下载(Drive-by-Download)方式摘要如下：

① 用户登录到存在安全漏洞的网页，用户的系统也存在着安全漏洞
② 用户打开的网页已被黑客注入了脚本形式的恶意软件或下载恶意软件的 URL
③ 因为用户系统存在漏洞，恶意软件一旦被运行，并在用户不知情的范围内运行

<通过偷渡式下载方式传播勒索软件事例>

2015年4月，韩国有名社交网站传播的勒索软件 CryptoLocker 是偷渡式下载方式的一个典型例子。黑客在网站横幅中隐藏恶意软件，当用户访问该网站时，通过浏览器和 Adobe Flash 漏洞再注入(Injection)到运行中的进程。这个过程为了不让用户认知，非常隐秘地执行，因此被称为偷渡式下载(Drive-by-Download)方式。

主要勒索软件有哪些特征？

1. CryptoLocker

CryptoLocker 首次发现于2013年9月，它可以感染大部分的 Windows 操作系统，包括：Windows XP、Windows Vista、Windows 7、Windows 8。CryptoLocker 通常以邮件附件的方式进行传播，附件运行后会使用 RSA&AES 对特定类型的文件进行加密。完成加密操作后，弹出勒索信息窗口要求用户使用 Moneypak 或比特币在72小时或4天内付款指定的金额，方可对加密的文件进行解密。偶尔，黑客对加密文件中的一个文件进行解密，是为了证明付款以后即可解密用户文件。

CryptoLocker 病毒运行后，便自我复制并为自动运行而在注册表项中添加自动启动项。之后，运行正常的 ‘explorer.exe’ 进程，嵌入 PE(Portable Executable)文件，该文件即包含了 ‘C&C服务器通信’ 及 ‘文件加密’ 等主要功能。

下面是 CryptoLocker 病毒的行为细节。

① 自动运行

病毒运行后，将自我复制文件到%WINDOWS%文件夹，同时在注册表项中添加自动启动项。

- HKCU\Software\Microsoft\Windows\CurrentVersion\Run\<随机名称>

登记到注册表项以后，每当重启系统时自动运行可执行文件。如果用户不删除该文件的话，即使支付黑客要求的赎金，很有可能再度感染勒索软件。

② 网络连接

病毒连接到网站 www.download.windowsupdate.com 以测试网络通信状态。如果网络通信畅通，连接网络上的某个C&C服务器以获取加密的密钥，然后加密用户PC的大多数常用格式的文档。最初连接成功后，获取特定IP带宽的扩展名为 '.txt' 和 'html' 的文件。确认IP带宽的理由是为了决定感染或例外对象国家。获取的文件将创建在加密文件所在的文件夹，并在文件内容中包含了勒索信息，信息包含了用户需要支付的赎金金额和支付方法。 每个文件描述的地址各不相同。

③ 删除卷影复制

执行下面的命令来删除卷影复制。这样的话，将无法正常使用 Windows 操作系统提供的文件备份及恢复功能。

"vssadmin.exe Delete Shadows /All /Quiet"

④ 文件加密

将用户PC上的文件加密导致无法打开。文件被加密后生成扩展名为 .encrypted 的文件。另外，移动硬盘和网络硬盘中的文件也可能成为勒索软件的加密对象，加密后也会生成扩展名为 .encrypted 的文件。

▲ 加密例外的扩展名

.chm, .ini, .tmp, .log, .url, .lnk, .cmd, .bat, .scr, .msi, .sys, .dll, .exe, .avi, .wav, .mp3, .gif, .ico, .png, .bmp, .txt, .html

▲ 加密例外的文件夹

- %Program Files%0
- %ProgramW6432%
- C:\WINDOWS
- C:\Documents and Settings\用户帐户\Application Data
- C:\Documents and Settings\用户帐户\Local Settings\Application Data
- C:\Documents and Settings\All Users\Application Data
- C:\Documents and Settings\用户帐户\Cookies
- C:\Documents and Settings\用户帐户\Local Settings\History
- C:\Documents and Settings\用户帐户\Local Settings\Temporary Internet Files

2. CryptoWall

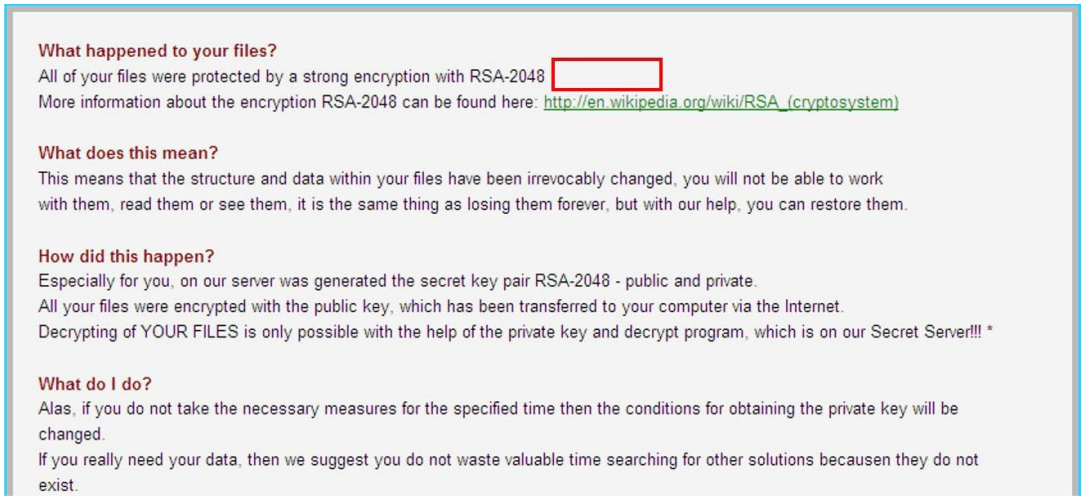
CryptoWall 出现于2013年，使用 RSA Key 对特定类型的文件进行加密。出现次数最多且最流行的勒索软件是 CryptoWall 3.0。2015年10月，据网络威胁联盟(Cyber Threat Alliance)发表的报告，黑客制作勒索软件 CryptoWall 3.0 在全世界收入达到了3.25美元。2015年11月出现了世界上最新的勒索软件 CryptoWall 4.0。

与 CrpytoLocker 相同，CrpytoWall 病毒运行后，便进行自我复制并为自动运行而在注册表项中添加自动启动项。之后，运行正常的 'explorer.exe' 及 'svchost.exe' 进程，嵌入 PE(Portable Executable)文件，该文件连接到外部C&C服务器后获取加密文件的密钥。

3. TeslaCrypt

TeslaCrypt 是一款臭名昭著的勒索软件 CryptoLocker 的变种。韩国首次出现于今年的2~3月份，是在韩国发生最多感染事件之一的勒索软件。感染该病毒后出现的勒索信息中说是使用 RSA 加密，其实是使用 AES Key 加密。

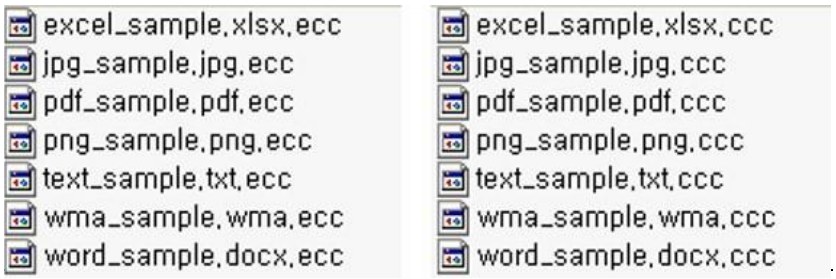
感染 TeslaCrypt 勒索软件后出现的勒索信息早期使用了 CryptoLocker 的信息，从2.0版本开始使用 CryptoWall 的勒索信息。因此被感染 TeslaCrypt 勒索软件的用户以为是被 CryptoWall 勒索软件感染。国外将 TeslaCrypt 勒索软件说成是 CryptoWall 勒索软件伪装的病毒。



【图 2】TeslaCrypt 勒索软件的勒索信息文件(只是除去了 CryptoWall 勒索软件版本信息)

今年初发现的 TeslaCrypt 和最近流行的 TeslaCrypt 的不同之处如下：

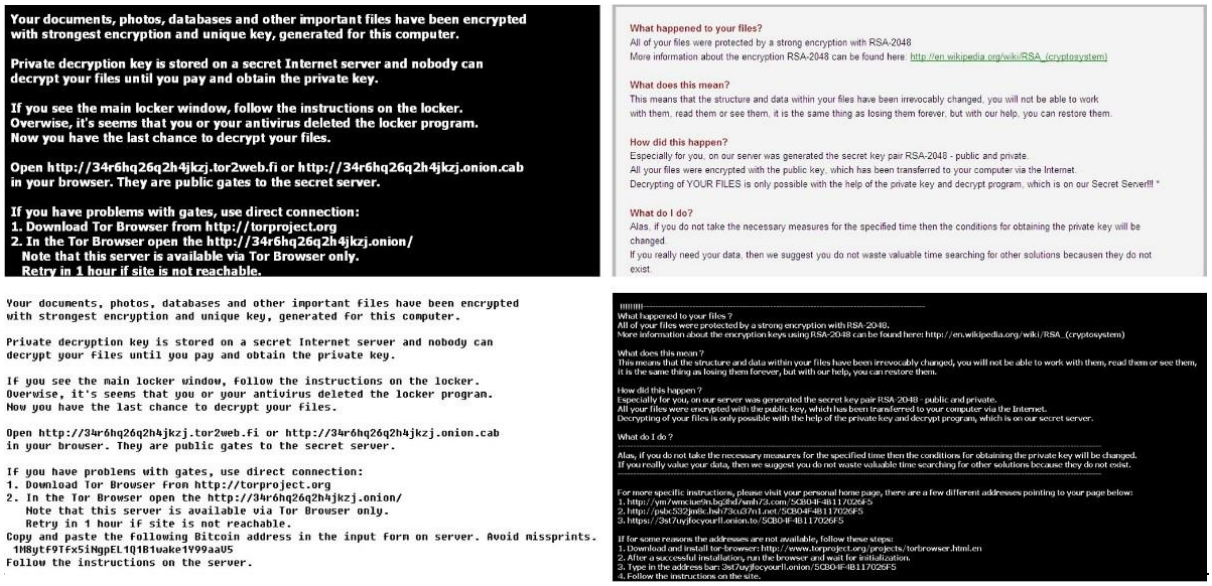
① 感染后加密文件名



② 感染后出现的勒索信息文件

今年初	最近
HELP_TO_DECRYPT_YOUR_FILES.BMP HELP_TO_DECRYPT_YOUR_FILES.TXT	HOWTO_RECOVER_FILE_.TXT HOWTO_RECOVER_FILE_.HTML HOWTO_RECOVER_FILE_[随机字符串].BMP 或 HOWTO_RESTORE_FILES.HTM HOWTO_RESTORE_FILES.TXT HOWTO_RESTORE_FILES.BMP

【表 1】今年初及最近出现的 TeslaCrypt 勒索软件的解密及支付赎金的勒索信息文件名



【图 3】今年初（左）和最近 TeslaCrypt（右）

③ 生成文件

	今年初	最近
CSIDL_APPDATA (%APPDATA%)	– 随机名称.EXE (自我复制) – HELP.HTML – LOG.HTML (受感染文件的目录信息) – KEY.DAT (使用在文件解密的密钥文件)	– 随机名称.EXE (自我复制)
CSIDL_DESKTOPDIR (桌面)	– CRYPTOLOCKER.LNK (自我复制文件的快捷方式) – 勒索信息文件	– 勒索信息文件

【表 2】 今年初（左）和最近 TeslaCrypt（右）生成的文件比较

④ 设置注册表

	今年初	最近
自动运行	HKCU\SOFTWARE\MICROSOFT \WINDOWS\CURRENTVERSION\RUN 数值： CRYPTO13 数值数据：自我复制路径	HKCU\SOFTWARE\MICROSOFT\WINDOWS \ CURRENTVERSION\RUN 数值：QEWR2342 数值数据 ： 自我复制路径
在网络驱动器以 管理员权限 运行文件及访问		HKLM\SOFTWARE\MICROSOFT\WINDOWS \CURRENTVERSION\POLICIES\SYSTEM 数值：ENABLELINKEDCONNECTIONS 数值数据 ：0X1

【表 2】 今年初（左）和最近 TeslaCrypt（右）设置注册表比较

▲ 除外对象文件夹
– %Windows%
– %Program Files%
– %Application Data%

进化的勒索软件

最近媒体报道电影上的“绑架剧”实际在现实生活中发生。正是被称为“勒索软件”的新种网络犯罪。目前被发现的勒索软件有“TeslaCrypt”、“CryptoWall”、“Teerac”等。勒索软件与其他恶意软件不同的特征是不会隐藏自己的攻击，反而攻击后向用户暴露自己，即使这是一种明显的犯罪活动。

最近1~2年之间陆续发生了用户计算机文件被加密后要求赎金的事件，从此这种勒索软件被大众广泛所知。勒索软件其根源可以追溯至具有“文件加密”功能的特洛伊木马程序。另一方面，通过病毒感染要求赎金并暴露攻击目的的侧面来看可以看成是“假杀毒毒软件”或“锁定屏幕病毒”之类的 Scareware 恶意软件进化的形式。Scareware 表面上看起来类似于合法销售的安全软件，其实目的只有索取金钱利益且根本就没有杀毒功能的假冒安全软件。与此相比，最近流行的勒索软件可谓是非常恶性的病毒，带给个人和企业业务致命打击。因为当用户不按攻击者的要求支付赎金时，用户的文件将永远无法恢复。

结语

AhnLab 通过官网的安全中心提供有关勒索软件的正确有效的信息，并发表了预防勒索软件的7大安全守则。必须遵守该安全守则才可以从勒索软件的威胁中获得自由。另外，不要随意安装广告软件，防止恶意利用在 Malvertising 手法。这种广告软件在网上冲浪时频繁出现在弹出窗口，有可能一不小心点击安装该软件。尤其访问下面的网站时需要更加注意。

- Torrent 相关网站
- Crack 相关网站
- 色情相关网站
- 免费在线游戏网站

在访问上述网站时要避开被安装广告软件。如果安装了广告软件，尽快卸载或利用防病毒软件除去该软件。但是，不是所有的杀毒软件都可以检测出可疑的广告软件。从广告软件制作者的角度来看，是黑客利用广告软件的漏洞嵌入病毒的。如果只在特定的时间篡改的话，根本无法找出其入侵的证据，采取措施更是难上加难。此时，如果无法知道安装了何种软件，可以运行V3安全软件的 AhnReport 程序，将有关信息发送到 AhnLab 请求分析结果。

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