AhnLab

安全月刊

2016.07 Vol. 44

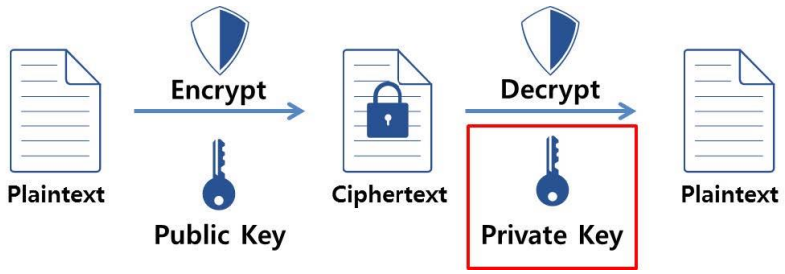
2016 年上半年勒索软件总结

勒索软件： “$how me the MONEY!”

$how me the MONEY!!! 在这里不是指最近韩国Mnet电视台正在人气播放的Hip-Hop音乐节目，也不是指风靡一时的游戏“星际大战”的游戏作弊，而是用一句话概括了最近流行的勒索软件的特点。如果直译该句子，可以翻译成“让我看到钱”或者是“给我钱”。只为钱！最近全世界广泛流行的勒索软件的目的只为钱。
本文了解今年上半期成为话题的主要的勒索软件，并详细分析这些勒索软件传播特点和预防方法。

有人在加密我的信息？

加密(Encryption)，是以某种特殊的算法改变原有的信息数据，使得未授权的用户即使获得了已加密的信息，但因不知解密的方法，仍然无法了解信息的内容。[1]



【图 1】 数据加密的基本过程

数据加密的基本过程如【图 1】所示。对原来为明文的文件或数据利用公开密钥(public key)进行处理，则生成密文。该过程的逆过程为解密。解密过程必须要使用私人密钥（private key），才能恢复为正常的数据。

加密的主体是信息创建者或具有合法权限访问的用户。加密最基本的目的是为了保障信息的可用性、机密性和完整性。愈是重要信息，愈要维持机密性并仅允许有限的用户访问。

[1] 百度百科

但是，如果数据由毫无相关的第三者来进行加密的话，这就会成为问题。当未授权的用户加密数据的话，就会发生真正要使用该数据的具有合法的访问权限的用户却无法利用该数据。甚至唆使用户购买私人密钥来对该数据进行解密。
这种过程由第三者一一执行并非容易且很麻烦。因此，制作了自动化全过程的程序，但这对具有访问权限的用户而言，明显是恶意行为。因此，将这种程序分类到恶意软件。而这种恶意软件的运行方式类似于劫持人质，因此被命名为“勒索软件(Ransomware = Ransom + Software)”。

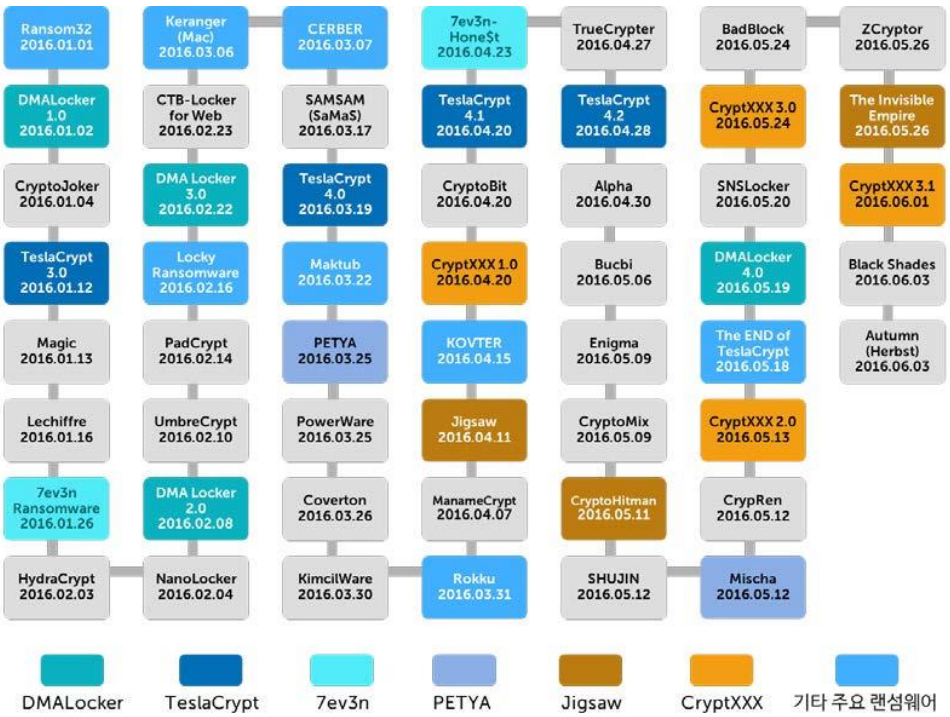
勒索软件加密用户信息的理由是什么呢？很明显，勒索软件的主要目的是只有钱。它对于用户的信息或数据多么重要、多么有价值没有任何关心，甚至对于数据的内容也是毫无关心。勒索软件制作者只要拿到钱就可以。对他们而言，拿到想要的金钱后，用户的数据是否正常解密也是不重要的。但是， 最近很多勒索软件支付赎金后提供正常恢复数据的恢复工具。这可能是为了得到好评，就是支付赎金后可以得到解密的评判，这样才可以诱导更多受害者支付赎金，

2016年发现的主要勒索软件

据AhnLab安全响应中心（ASEC）统计，今年发现的勒索软件包括版本升级共计52个，按季度分别是第一季度发现25个，第二季度发现27个。[2]【图 2】显示的勒索软件仅限于根据网络安全提供商、媒体等发表的勒索软件中，可以明显区分其特点的勒索软件。如果包括网络安全提供商也没有分类的或未知的勒索软件，估计数量可能会更多。

比起2015年，2016年上半年就暴增的理由很简单。勒索软件可以赚到钱。据2015年赛博威胁联盟(Cyber Threat Alliance) 发行的“有利可图的勒索软件攻击：CryptoWall 3.0 的威胁分析(Lucrative Ransomware Attacks: Analysis of the CryptoWall Version 3 Threat)”介绍，CryptoWall 3.0 的作者在全世界范围内估计掠夺了3.25亿美金。不到一年的时间，CryptoWall 3.0 就发生了如此多的犯罪收益。

如此短短的时间能够赚取超出想象的收益，难怪恶意软件制作者纷纷涌入到勒索软件制作。甚至，据说制作网银木马Dridex的制作者也投入到了勒索软件制作和传播。尤其出现了通过勒索软件服务(Ransomware as a Service)的方式来兜售勒索软件，只要支付一定的费用，就能享受从制作到传播和管理的一系列服务。



【图 2】2016年发现的勒索软件

[2] 基准日期为2016年6月10日

金盆洗手？ TeslaCrypt 作者宣布终止恶意行为

在2016年，TeslaCrypt仍然不停地出现。TeslaCrypt是CryptoLocker的变种，针对用户计算机中的游戏文件进行感染。主要使用浏览器攻击程序(Exploit Kit)，在用户不知情的情况下重定向到具有漏洞的网站，再将漏洞注入(Injection)到运行中的进程。但也出现过利用电子邮件附件包含的JavaScript文件传播的形式。

■ TeslaCrypt 3.0的登场

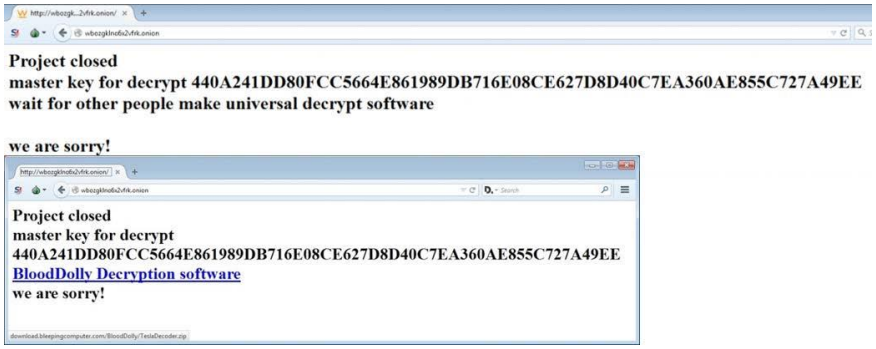
TeslaCrypt勒索软件自去年爆发以来一直不断升级，今年1月出现了TeslaCryt 3.0版本。与2.0版本不同的是，文件加密后扩展名多出了“.xxx”、“.TTT”、“.Micro”、“.mp3”等。2月发现了电子邮件附件包含了JavaScript文件的TeslaCryt勒索软件。利用JavaScript文件的传播方式同样利用在Locky勒索软件传播，引来了一场风波。TeslaCrypt作者不停地更新程序来躲避安全软件的查杀。

■ 不修改加密文件名的TeslaCrypt 4.0

今年3月份，自出现TeslaCrypt3.0后不久再次出现了TeslaCrypt的最新变种TeslaCrypt 4.0。TeslaCrypt 4.0在加密文件后不修改原文件名，因此用户很难发觉文件已被感染。通常是打开文件时发生错误后，才觉察到被感染。

■ TeslaCrypt 突然终止

5月18日，发生了意想不到的事情。TeslaCrypt勒索软件作者突然公布了通用解密密钥，并向外界道歉。事情是这样的。安全公司ESET的安全专家假装是受害者询问TeslaCrypt是否愿意提供解密密钥。比较意外的是TeslaCrypt作者竟答应提供TeslaCrypt勒索软件的通用解密密钥。如【图 3】所示，TeslaCrypt在网页向受害者道歉并公开了主解密密钥。在主解密密钥被公布后，许多安全公司立即借助通用解密密钥制作了免费的TeslaCrypt解锁工具。



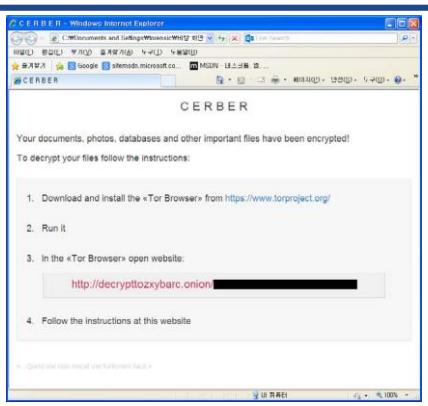
【图 3】 TeslaCrypt作者公开主解密密钥

2016年疯狂传播全世界的勒索软件“Locky”

2016年上半年最为歹毒的恶意软件莫过于Locky勒索软件。它恶名昭彰，超乎想像地速度已大量传播到全世界。初期的Locky利用MSOffice的宏功能传播病毒，主要是通过电子邮件附件传播带有恶意宏的Word文档。从今年3月到最近，利用JavaScripty文件继续传播病毒。据说在海外，利用电子邮件传播恶意软件Dyre或Dridex的作者团也加入了Locky制作。受到其影响，利用电子邮件包含JavaSripty文件传播的恶意软件数量大大增加超出想象，导致全世界防病毒软件公司大部分为了应对JavaScript文件变形而历经磨难。

通过语音提示用户的Cerber勒索软件

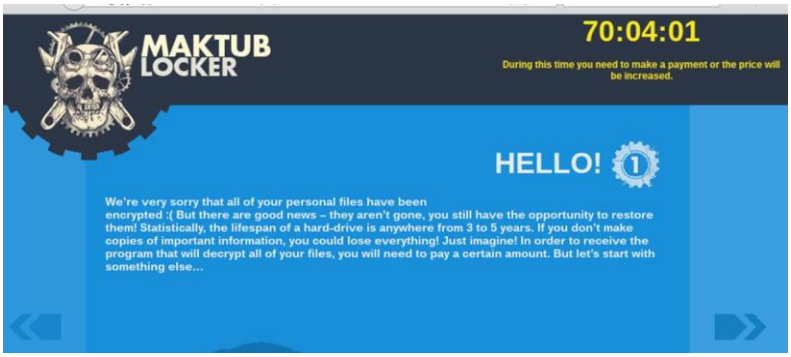
今年3月初发现的Cerber勒索软件将用户计算机的文件加密后，通过语音来提示用户。Cerber勒索软件是首款语音式的勒索软件，它会通过计算机合成音制作提示信息。当用户计算机被感染后文件被加密，则自动重新启动计算机并进入安全模式。如果用户以正常模式启动计算机，则屏幕出现勒索软件的勒索信息，即要求用户支付赎金的提示信息。该勒索软件使用了Malvertising方式，即通过具有漏洞的广告服务器的Flash文件传播恶意软件。尤其，此过程据说是使用了Nuclear Exploit Kit。据传言，俄罗斯的地下组织正在通过 RaaS(Ransomware-as-a Service)的方式贩卖Cerber勒索软件。



【图 4】 Cerber勒索软件感染界面

提高加密速度的Maktub勒索软件

今年3月末发现的Maktub是一款勒索软件。Maktub的原始名字来源于阿拉伯语言“maktub”，意思是“这是写好的(This is written)”或者“这是命运(This is fate)”。通常，一般的勒索软件会对原始文件进行加密，而Maktub勒索软件会首先对文件进行压缩，从而提高加密速度。加密文件的扩展名是随机的。



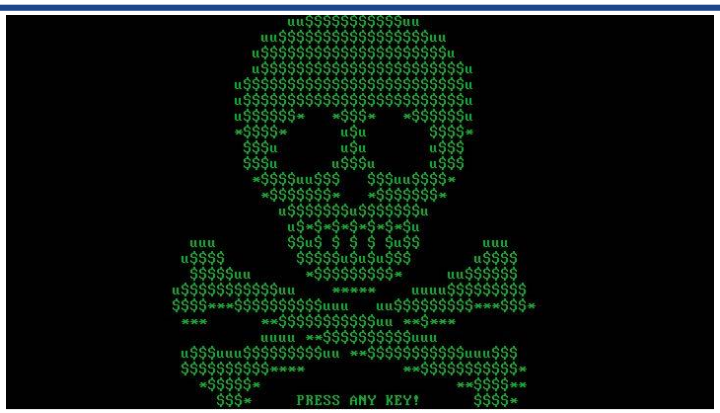
【图 5】 Maktub勒索软件感染界面

打破对勒索软件的传统概念的“Petya”和“Mischa”

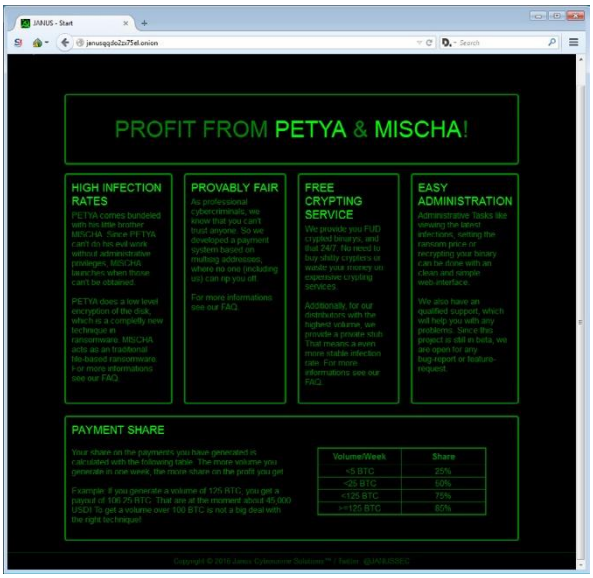
2016年3月，出现了一种名为“Petya”的变种勒索软件，通过电子邮件附件传播。Petya和其他流行的勒索软件不同，它除了加密某些类型的文件外，会篡改磁盘主引导区，强制重启系统后运行引导扇区中的恶意代码，将电脑硬盘整个加密，并通过Tor网络索取比特币。

【图 6】 Petya勒索软件感染界面

5月中旬出现了比Petya功能加强的Mischa勒索软件。Petya勒索软件只会篡改磁盘主引导区，使整个硬盘无法访问。而Mischa勒索软件可在加密MBR和用户数据中可以选择一个。通常通过钓鱼邮件进行传播，诱导用户点击电子邮件中的链接。当用户运行含有病毒的文件时，立即弹出“用户账户控制(User Account Control)”窗口。询问用户是否愿意接受该程序管理员访问权限。如果用户选择“是”，则出现与Petya勒索软件相同的感染界面；如果选择“否”，则对用户计算机的文件进行加密。Mischa勒索软件可以看作是之前勒索软件和Petya勒索软件的组合版。它还通过RaaS(Ransomware-as-a Service)的方式贩卖，受害者支付的赎金由勒索软件作者和发布者分账。



【图 7】Mischa勒索软件加密MBR的界面



【图 8】 通过RaaS提供的Mischa勒索软件

最近冒起的勒索软件“CryptXXX”

CryptXXX在4月份首次被发现后广泛流行。主要通过利用Flash或IE漏洞的浏览器攻击程序(Exploit Kit)传播。卡巴斯基的安全研究人员找出了一种方法来解密受到CryptXXX勒索软件攻击的文件，并提供给受害者。然而在5月中旬，出现了CyrptXXX 2.0版本，使得该解密工具无效。但是，卡巴斯基的安全研究人员又找出了对付CryptXXX 2.0版本的解密工具。5月末，CryptXXX的作者将该恶意软件的代码更新至了3.0版本，此次更新的主要目的就是为了封堵卡巴斯基的解密程序。但是这一版本的勒索软件代码似乎出现错误，该恶意软件原本的解密组件无法正常解密。因此发生了受害者即使支付赎金也未能得到解密事件。对此，CryptXXX的作者为了解决该错误连续发布了3.1和3.2版本。

6月初，在韩国有名的社交网站上传播的勒索软件即是CryptXXX 3.0。利用Flash制作的带有恶意软件广告传播CryptXXX，用户浏览网站时被重定向到载有攻击代码的网站，试图安装CryptXXX。

一般计算机用户如何预防勒索软件？

黑客电影“Who am i”中，有这样的台词。“没有一个系统是安全的”，“人不能总藏在他的计算机后面，最大的安全漏洞并不是存在于什么程序或者服务器内，人类才是最大的安全漏洞”。即使引进和应用最好的安全解决方案，最终用户还是具有自由意志的人，这也说明很难控制。不仅如此，如果硬是强调安全的重要性并加强规范，企业会陷入给用户带来的不便是不用说，就连组织的生产率也会受到影响的进退两难的境地。因此，这也成了安全专家的永远的课题。反过来想一想，这意味着只要用户按照安全守则使用计算机，很大程度上可以脱离预防勒索软件的威胁。

如何有效防范勒索软件，保护用户重要数据：

1. 及时更新操作系统和应用程序上存在的最新安全漏洞
2. 及时应用微软每月第二个星期的星期三发布的Windows安全更新

3. 最好使用IE以外的其他浏览器，如Edge、Chrome、Firefox等
4. 使用最新版的IE、java、Flash等程序
5. 如果不是有必要，最好从计算机删除Java、Flash Play等程序
6. 随时备份重要数据，尽量将数据备份在脱离网络的存储设备中
7. 正确使用防病毒程序
8. 计算机不要乱用在原来目的以外的
9. 切记！免费网站是恶意软件的温床
10. 不要随意打开可疑的电子邮件附件

上述的预防方法已在早期的月刊中都有提到，没有新鲜的内容。如果觉得按照这些预防方法去做嫌麻烦，那么只要做好“随时备份重要数据”这一项也可以降低勒索软件带来的损失。这个预防方法只要投入早期购买移动硬盘的费用，不会发生另外的费用，因此积极推荐加入“数据备份”这保险。

参考资料

1. 残酷的邪恶的化身，勒索软件 Top 6 *http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?curPage=1&menu_dist=2&seq=23631&dir_group_dist=0*
2. 上篇：要想预防勒索软件，需要先了解勒索软件 *http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?curPage=&menu_dist=1&seq=24340&key=&dir_group_dist=&dir_code=*
3. 下篇：理想的 vs. 现实的勒索软件响应方案 *http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?curPage=&menu_dist=1&seq=24337&key=&dir_group_dist=&dir_code=*
4. 2016年第一季度，最恶勒索软件有哪些？ *http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menu_dist=2&seq=24838*
5. 勒索软件，都有哪些变化？ *http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menu_dist=2&seq=24838*
6. 快速演变的勒索软件，注意变种！ *http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?seq=24288*
7. Criminals behind CryptoWall 3.0 Made $325 Million *http://securityaffairs.co/wordpress/41642/cyber-crime/cryptowall-3-0-325-million.html*
8. Lucrative Ransomware Attacks: Analysis of the CryptoWall Version 3 Threat *http://cyberthreatalliance.org/cryptowall-report.pdf*
9. Locky ransomware, disguised in Word docs, latest from Dridex creators *http://www.scmagazine.com/dridex-actors-likely-behind-vicious-locky-ransomware-strain/article/475420/*
10. ESET releases new decryptor for TeslaCrypt ransomware *http://www.welivesecurity.com/2016/05/18/eset-releases-decryptor-recent-variants-teslacrypt-ransomware/*
11. TeslaCrypt shuts down and Releases Master Decryption Key *http://www.bleepingcomputer.com/news/security/teslacrypt-shuts-down-and-releases-master-decryption-key/*
12. TeslaCrypt Developers recommend TeslaDecoder to Decrypt Files *http://www.bleepingcomputer.com/news/security/teslacrypt-developers-recommend-tesladecoder-to-decrypt-files/*
13. What's cooking? Dridex’ s New and Undiscovered Recipes *https://blog.fortinet.com/2016/03/23/what-s-cooking-dridex-s-new-and-undiscovered-recipes*
14. Group Behind CryptoWall 3.0 Made $325 Million: Report *http://securityaffairs.co/wordpress/41642/cyber-crime/cryptowall-3-0-325-million.html*
15. Antivirus is Dead: Long Live Antivirus! *http://krebsonsecurity.com/2014/05/antivirus-is-dead-long-live-antivirus/*
16. Ransom32 – look at the malicious package *https://blog.malwarebytes.org/threat-analysis/2016/01/ransom32-look-at-the-malicious-package/*
17. Locky Ransomware Installed Through Nuclear EK *http://researchcenter.paloaltonetworks.com/2016/03/locky-ransomware-installed-through-nuclear-ek/*

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