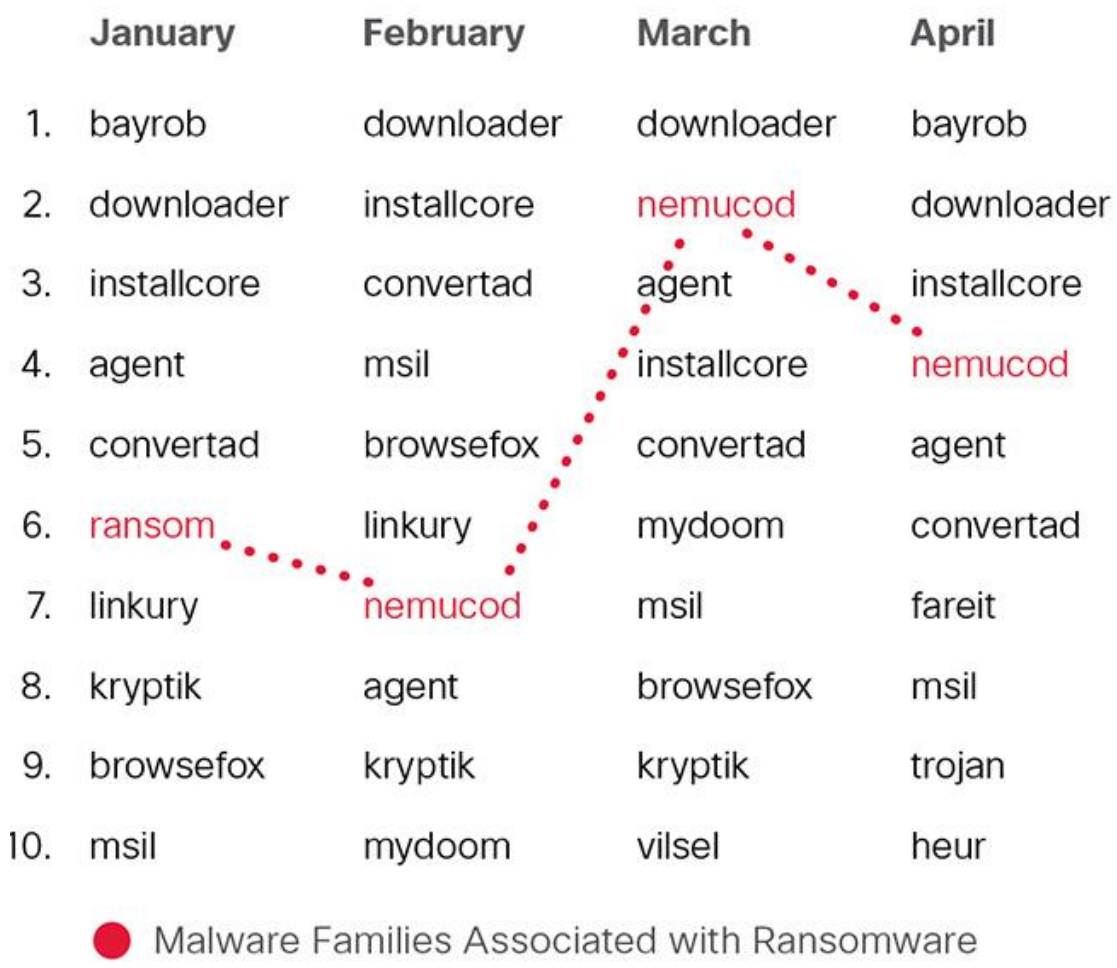
复杂勒索软件：利润最大化的新策略

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	Sophisticated ransomware: New tactics to maximize profit		
原文作者	Zeljka Zorz	**原文发布日期**	2016 年 7 月 27 日
作者简介	Managing Editor of Help Net Security and (IN)SECURE Magazine		
原文发布单位	Help Net Security		
原文出处	https://www.helpnetsecurity.com/2016/07/27/sophisticated-ransomware/		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
免责声明	本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。		

根据思科 2016 年中网络安全报告显示，很多组织机构对于一系列更为复杂的勒索软件都没有防备。脆弱的基础设施、不良的网络环境、缓慢的检出率给对手提供了充足的时间进行掩护操作。



十大恶意软件家族月检图表

2016 年初至现在为止，勒索软件已经成为史上最为赚钱的恶意软件类型。思科预计这种趋势将因可以通过自身传播、控制整个网络的更具破坏性的勒索软件而继续，企业、抵押品也如此。一系列新型的勒索软件将很快改变策略使效率最大化。例如，未来的勒索软件攻击可以通过限制 CPU 使用率来逃避检测，避免指挥及控制行为。这些新型勒索软件种族的传播更为迅速，在组织协调勒索软件活动之前完成自身复制。

富士通 EMEIA 地区企业与网络安全主任 Rob Norris 向 Help Net Security 透露道，“事实上，许多组织机构可能并不认为自己是攻击者的‘高价值目标’，很可

能他们极少进行防护或对员工进行培训和意识培养。然而，许多恶意参与者容易将这些企业作为攻击目标，期望通过‘软攻击’组织勒索活动来泄漏其数据”。

可见性挑战

跨网络及终端的可见性仍是主要挑战。许多组织机构平均需要 200 天来识别新的威胁。思科的平均检测时间（TTD）继续领跑行业，截至 2016 年 4 月，最低需要约 13 小时即可检测出先前存在六个月的未知漏洞。

该结果低于 2015 年 10 月时的 17.5 小时。更快的威胁检测时间对于限制攻击者活动空间和减少损失来说至关重要。这个数字是基于选择性加入来自思科部署于全球的安全产品的安全遥测。

地下持续创新

随着攻击者的创新，许多防御者继续为维护其设备与系统安全而奋斗。不支持和未打补丁的系统为攻击者创建附加机遇来轻松获取访问权限、逃避检测、损失和利益最大化。思科 2016 年中网络安全报告显示，这个挑战在全球范围内持续存在。

然而在过去几个月里，许多组织机构在医疗等关键行业遭受的攻击频率大幅上升。报告结果表明，所有垂直市场和全球各区域都是目标。2016 年上半年，俱乐部、组织机构、慈善机构、非政府组织（NGO）和电子企业遭受攻击的频率都在上升。在世界舞台上，地缘政治担忧包括监管的复杂性和矛盾的国家网络安全政策。控制或访问数据的需要可能会限制和造成复杂威胁格局下的国际贸易冲突。

Arbor Networks 公司 EMEA 地区渠道&联盟主任 Richard Brown 说道，“网络犯罪分子继续非常创新，往往可以访问相同防守技术的网络攻击，因此组织机构必须利用他们的人类安全资源来主动识别威胁。缩短检测时间非常关键，也是阻止攻击与牺牲有价值数据的区别之处”。

攻击者利润飙升

对攻击者来说，越多时间操作不被检出就会带来越多的利润。2016 年上半年，

思科报道，攻击者利润飙升基于以下原因：

扩大专注：攻击者扩大其焦点，从客户端到服务器端的利用，避免检测以及潜在的损害和利润最大化。

•Adobe Flash 漏洞仍是恶意广告和开发工具包的最高目标之一。在流行核开发工具包中， Flash 占据了 80%的成功利用活动。

•勒索软件攻击利用服务器漏洞的一个新趋势——特别是在 JBoss 服务器——全球范围内，10%的 JBoss 联网服务器会受到损害。JBoss 的许多漏洞用于破坏五年前就被确认的系统，这意味着基本的修补和供应商的更新可以轻松阻止这种攻击。

进化攻击方法：2016 年上半年，对手利用防御者缺乏可见性来继续改进他们的攻击方法。

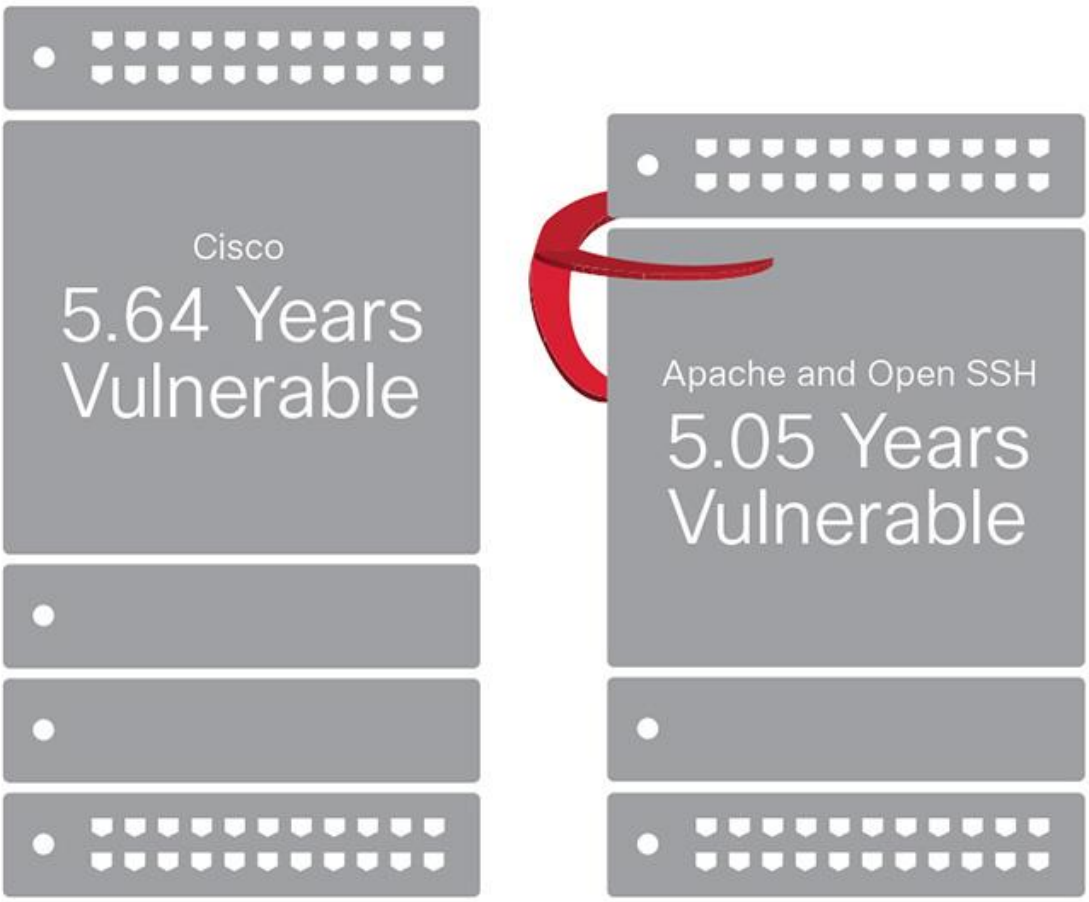
•在过去的六个月里，Windows 二进制利用上升为第一网络攻击方法。这种方法在网络基础设施上提供了一个强大的立足点，使这些攻击更难识别和移除。

•在同一时间内，社会工程学通过 Facebook 诈骗从 2015 年的第一降至第二。

覆盖跟踪:为有助于防御者的可见性挑战，对手越来越多的使用加密作为屏蔽其操作的方法。

•加密货币使用的增加，Transport Layer Security 及 Tor 促成了跨网匿名通信。

•显然，加密版 HTTPS 恶意软件用于恶意广告活动从 2015 年 12 月到 2016 年 3 月增加了 300%。加密恶意软件进一步使对手隐藏他们的网络活动，扩大活动时间。



软件安全状态

防御者难以减少漏洞，封闭间隙

面对复杂的攻击、有限的资源以及基础设施老化，防御者都在努力跟上他们的敌人。数据显示防御者不太可能标记足够的网络安全状态，如修补，更主要的技术是业务操作。例如：

•浏览器空间（Google Chrome 自动更新）方面，75%至 80%的用户使用最新版本的浏览器。

•软件方面，Java 注意到缓慢的迁移，三分之一的系统被检出运行已被甲骨文淘汰（当前版本是 SE 10）的 Java SE 6。

•微软 Office 2013（版本 15 x）方面，10%或更少的用户使用的是最新版本的服务包。

此外，思科发现大部分基础设施是不受支持的，或者用已知漏洞操作。这个

问题是系统供应商和终端。具体来说，思科公司研究人员检查了 103121 件联网的思科设备，发现：

•每个设备平均运行 28 已知漏洞。

•设备中活跃运行已知漏洞的平均时间为 5.64 年。

•9%以上的已知漏洞已活跃超过 10 年。

相比之下，思科检查了 300 多万安装样本中的软件基础设施，大多数是 Apache 和 OpenSSH，平均 16 个已知漏洞，运行时间平均 5.05 年。

浏览器更新是最轻量级的终端更新，而企业应用程序和服务器端基础设施则更难更新，还会导致业务连续性问题。从本质上讲，应用程序业务操作越关键，就越不可能被经常处理，因为会为攻击者创建间隙和机会。