安天周观察

安天官方微博　安天官方微信

主办：安天　2017 年 11 月 13 日（总第 111 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天亮相国际反病毒大会 聚焦勒索软件有效防护

11 月 8 日 -9 日，“2017 第二届国际反病毒大会”在天津举行，会议以“万物互联背景下反病毒的新挑战”为主题。安天研发副总监庞齐带来了题为《由勒索软件引发的攻防博弈》的报告，聚焦勒索软件、探讨防护技术。

1. 勒索软件已演变为全球威胁

安天威胁通缉令扑克中对勒索软件的解读

在万物互联的背景下，勒索软件已经从早期的一种恶意代码行为发展为现在的一种黑产经济模式，并逐渐演变为全球性威胁。庞齐首先回顾了近几年勒索软件的发展趋势及带来的危害，之后以“魔窟”病毒的加密流程为例，介绍了当前通用的勒索软件的加密方式。他表示，目前绝大多数的勒索软件采用的都是强加密的方式，基本上很难进行逆向解密，因此避免遭受勒索软件攻击的根本在于终端侧的有效防护。

2. 多手段结合，防御勒索软件

安天多年来持续关注、分析勒索软件，具有丰富的勒索软件对抗经验，早在 2015 年就已经在安天智甲终端防御系统（英文简称 IEP，以下简称“安天智甲”）中专门强化了针对勒索软件的检测和防御能力。庞齐指出，针对勒索软件，单一的防护手段已经不可靠，需要多手段结合，才能真正实现对勒索软件攻击的有效防护。

安天勒索软件防护技术手段：

- 下一代威胁检测引擎；
- 云端大数据分析；
- 机器学习；
- 漏洞检测和虚拟补丁防护。

3. 安天智甲，有效防护

面对勒索软件的盛行，为能更好的保障用户数据资产安全，安天智甲嵌入了多维度的防勒索能力，通过勒索行为感知、传输文件深度检测与管控、文档访问控制等方式，对勒索软件进行多维度的安全防护。

安天智甲是一款面向政府、军工、能源、金融、交通、电信等各行业用户的企业级防护产品，产品集成了病毒检测查杀、系统加固、主动防御、介质管控、文档保护、行为画像等功能，并能有效与管理中心和安天态势感知产品互动，协助客户建立更全面的资产防护体系和风险认知能力，使态势感知能够有效落地。

勒索软件具有巨大的利益回报，在利益回报的驱动下，勒索软件会成为日后主流的安全威胁，其传播途径和破坏方式也会变得愈加复杂和难以防范。而安天将持续与之对抗，帮助更多的用户防患于未然。

Brother（兄弟）打印机存在安全漏洞，或导致设备遭受拒绝服务攻击

据外媒 11 月 7 日报道，网络安全公司 Trustwave 研究人员 SpiderLabs 近期发现 Brother 制造与出售的联网打印机存在一处安全漏洞，允许攻击者远程操控设备后展开拒绝服务攻击。目前据 Shodan 搜索结果显示，全球至少 14,989 台 Brother 打印机设备暴露于公网当中，很可能会受到这一漏洞影响。

研究人员表示，攻击者主要通过该漏洞向在线的目标打印机发送错误格式的 HTTP POST 请求来执行攻击，从而远程操控设备。从网络角度来看，虽然与普通的 HTTP 流量攻击类似，但该活动的攻击极其频繁，每隔几分钟就会针对受损设备发送一个请求并完成一次攻击。

Trustwave 威胁情报负责人 Karl Sigler 表示：“这一漏洞危及了所有具备 Debut 嵌入式网络服务器的 Brother 设备，其 1.20 版本或更早版本普遍遭受影响。不幸的是，尽管我们多次联系 Brother 公司解决这个问题，但他们至今并未发布补丁程序。”对此，为降低漏洞所产生的影响，研究人员提醒设备管理员使用防火墙或类似设备严格限制访问权限。此外经调查发现，这一漏洞似乎不会得到妥善解决，因为即使官方提供补丁更新打印机系统，也可能需要人工部署，例如攻击者可能会事先启动拒绝服务攻击，随后利用社会工程等手段冒充技术人员直接物理访问相关 IT 资源。

每周安全事件

类 型	内 容
中文标题	盗窃的数字代码签名证书签名的恶意软件继续绕过安全软件
英文标题	Malware signed with stolen Digital code-signing certificates continues to bypass security software
作者及单位	Pierluigi Paganini; SecurityAffairs
内容概述	数字代码签名证书是地下犯罪的珍贵商品，由信任的证书颁发机构（CA）颁发的数字证书用于对安全解决方案所信任的软件进行加密签名，以便在您的计算机上执行。 对恶意代码进行数字签名可能会让其在计算机上执行，从而绕过安全措施。 滥用数字代码签名证书的第一批恶意代码之一是2005年用于危害伊朗核浓缩过程的Stuxnet蠕虫。回到目前，最近针对CCleaner软件供应链的攻击还利用了已签名的受感染版本流行的应用程序，以避免检测。 来自马里兰大学学院的安全研究人员Doowon Kim，BumJun Kwon和Tudor Dumitras对这些现象进行了调查。研究小组共发现325个已签名的恶意软件样本，其中189个（58.2%）携带有效数字签名，136个携带畸形数字签名。
链接地址	http://securityaffairs.co/wordpress/65233/deep-web/digital-code-signing-certificates-malware.html

每周值得关注的恶意代码信息

经安天【CERT】检测分析，本周有10个移动平台恶意代码和4个PC平台的恶意代码值得关注

关注方面		名称与发现时间	相关描述
移动恶意代码	新出现的样本家族	Trojan/Android.StealChat.a[prv,spy] 2017-11-07	该应用程序伪装系统应用，运行隐藏图标，后台窃取用户联系人、书签、通话记录、短信和社交应用聊天数据上传到远程服务器，造成用户隐私泄露，建议卸载。（威胁等级中）
		PornWare/Android.xwplayer.a[exp,rog] 2017-11-07	该应用程序运行后播放色情视频，私自发送短信恶意推广，影响用户身心健康，造成用户资费损耗，建议卸载。（威胁等级中）
		Trojan/Android.JsMiner.a[exp,rog] 2017-11-08	该应用程序被植入恶意代码，运行后执行隐式货币挖矿脚本，会消耗手机性能、减短电池寿命、消耗手机流量，建议卸载。（威胁等级高）
		Trojan/Android.CPUMiner.a[exp,rog] 2017-11-08	该应用程序被植入恶意代码，运行后该设备后台执行隐式货币挖矿行为，长期运行会消耗手机性能、减短电池寿命、消耗手机流量，建议卸载。（威胁等级高）
		Trojan/Android.Walex.a[pay] 2017-11-09	该应用程序内嵌恶意代码，运行会私自联网获取订阅信息进行Wap订阅、发送订阅短信，造成用户资费损耗，请卸载。（威胁等级中）
		Trojan/Android.lzcyjr.a[prv,spy] 2017-11-09	该应用程序运行后隐藏图标，获取设备管理器权限，后台窃取用户短信、联系人、通话记录、手机基本信息、地理位置并上传，造成用户隐私泄露。（威胁等级中）
		Trojan/Android.weezweez.a[prv,exp,sms] 2017-11-09	该应用程序运行后私自上传用户信息，联网获取短信内容并私自发送短信，还有拦截短信发送给指定号码、下载安装恶意子包等行为，子包会解析远程指令，根据远程数据弹出不同界面，警惕其弹出虚假欺诈界面和流氓推广等行为，造成用户隐私泄露和资费损耗，建议卸载。（威胁等级高）
		Trojan/Android.bmhs.a[prv,spy] 2017-11-11	该应用程序伪装政府相关应用，运行后窃取用户短信、手机基本信息、手机号并上传，造成用户隐私泄露。（威胁等级中）
	较为活跃的样本	Trojan/Android.SlfMite.e[exp,spr]	该应用程序伪装其他应用，运行会隐藏图标，向用户联系人群发带有下载链接的传播短信，以短信的方式进行恶意传播，造成用户资费消耗，建议卸载。（威胁等级中）
		Trojan/Android.LockScreen.ar[rog,sys,lck]	该应用程序运行后请求激活设备管理器，安装恶意子包程序到系统app目录，并锁定权限无法删除，子包运行后锁屏用户界面，勒索用户付费解锁屏幕，造成系统破坏并影响手机的正常使用，建议卸载。（威胁等级中）
PC平台恶意代码	活跃的格式文档漏洞、0day漏洞	Adobe Flash 任意命令执行漏洞（CVE-2017-11292）	Adobe发布了Windows, Macintosh, Linux以及Chrome OS多个平台下的Adobe Flash Player安全升级补丁。更新修复了一个由于类型混淆漏洞导致的远程代码执行。Adobe官方注意到了CVE-2017-11292曾经有一段在野时期，被利用于有针对性的攻击Windows用户。（威胁等级高）
	较为活跃样本	Trojan[Spy]/Win32.Crimson	此威胁是一种可以监视用户系统的木马家族。该家族样本运行后连接远程服务器接受攻击者的监视，攻击者可以执行各种恶意操作，如浏览文件、上传数据等。（威胁等级中）
		Trojan[Backdoor]/Win32.Matsnu	此威胁是一类窃取用户信息的木马家族，属于后门。该家族样本运行后会连接网络、禁用注册表编辑器、允许恶意代码绕过防火墙。（威胁等级中）
		Trojan[Ransom]/Win32.Zerber	此威胁是一类可以加密用户数据的木马家族。该家族样本是勒索软件，运行后加密用户文件，加密后播放声音提示用户文件已被加密，需支付比特币才可以解密。（威胁等级中）

防御勒索软件攻击七步走

Patrick Hill / 文　安天技术公益翻译组 / 译

如果你明天上班时发现公司遭到了勒索软件攻击，你知道该怎么办吗？你会打给谁求助？如果你的电脑被锁定，你将如何找到他们的电话号码？你将如何通知客户？

防御勒索软件攻击需要做好多方面的准备，包括技术方面，例如对数据进行离线备份。本文不讨论这些技术措施，主要谈谈可以采取的实际操作措施，以便在事件发生之后进行有效地应对。你的应急计划是什么？你希望你的团队囊括哪些人才？你将如何沟通？

很少有人能够未卜先知，但是提前规划能够帮助人们更加轻松地应对灾难。当涉及勒索软件时，提前规划也是很重要的。今年 5 月，WannaCry 勒索攻击爆发，在头几天就感染了大约 30 万台计算机。之后，联邦调查局网络司司长称勒索软件是一种“普遍的、日益增长的威胁”，并指出未来很可能会出现更多的勒索软件攻击。其他一些报告也预测勒索软件攻击会增加。

为了应对勒索攻击，我们可以采取以下 7 个措施。其中一些措施可以广泛应用于其他重大事件，而另一些则专门针对勒索软件攻击。

■ 1. 制定初步响应计划

你的团队成员可能不习惯处理紧急情况，所以要确保他们知道该怎么做。这包括他们将会聚集在哪里讨论问题，媒体问询应该在哪里举行，以及该告诉客户和员工什么内容。大多数时候，这意味着规划“谁、什么、什么时候、如何做”（who，what，when，how）的问题。一旦制定了计划，请提前与你的团队分享。

■ 2. 将响应计划存储在多个位置

如果您的事件响应计划存储在 PC 上但 PC 被锁定了，那么您将无法开始恢复过程。勒索软件可能会影响你的台式机或服务器，或两者都影响。将计划副本存储在多个位置，包括至少三个独立的云服务，并设置日历提醒以便定期更新。

■ 3. 选择团队成员

事件发生后，你想要谁参加讨论？除了首席执行官和首席信息官之外，您可能想要公关、法律、人力资源和其他部门负责人参加响应讨论。现在您需要制定一个清单，并确保清单上的每个人都知道这回事。此外，获得他们下班后的联系方式，并与其他团队成员分享。

■ 4. 制定沟通计划

您可能会发现首选的沟通方式被锁定了，因此您需要了解还有哪些沟通渠道可供使用。电子邮件可能已经无法使用，所以请准备其他沟通手段。如果你的智能手机正常运行，那么可以在团队内部使用通信应用程序——只要确保每个人都安装了这个应用程序就行。但是勒索软件也可能会攻击移动设备，所以请准备好备用方案。将电话号码和个人电子邮件地址存储在多个地点是个不错的办法。

■ 5. 确定负责人

攻击发生后还有很多事情要做，包括指挥员工，联系执法部门、客户和合作伙伴。需要有人监督和管理恢复工作，准备好随时回答问题。负责人可能是首席信息官、首席运营官、安全主管等，但是最好明确这个人的权限。提前确定这个负责人，避免出现措手不及的情况。

■ 6. 讨论一下你将如何进行响应

你决定支付赎金与否取决于事件的严重程度和性质，但是提前讨论这个话题比临时抱佛脚要强。联邦调查局表示，它不鼓励支付赎金，因为这会激励未来的攻击，但也指出每个企业都需要自己做决定。您应该提早讨论这个问题，至少要让你的团队熟悉这种权衡。

■ 7. 了解你的风险承受能力

你无法计划所有的事情，所以要弄清楚你可以承受多大的风险，以及你可以应付的潜在伤害，然后做一个权衡。例如，有些公司每个月都会做一次灾难恢复演习，以确保他们随时做好准备，这算是比较频繁的，有的公司则每季度做一次。这完全取决于你想要在系统中建立多少“保险”。这是些艰难的决定，需要事先确定。

如果幸运的话，你永远不会遭遇勒索软件攻击，但是运营一个公司不能靠运气。您的技术团队将会投入大量的工作来防范攻击并减轻损害。但是响应、告知客户并保持公司的运营是需要进行管理的。通常很难想象从来没有遇到过的情况，但是试着想象一下，一天早上你的手机响了，得知公司遭到了勒索攻击。那个时候，你会希望做了哪些准备呢，现在就着手做这些准备吧。

原文名称	When Ransomware Strikes: 7 Steps You Can Take Now to Prepare
作者简介	Patrick Hill 是 Atlassian 的 SRE 解决方案负责人。
原文信息	2017 年 11 月 6 日发布于 Dark Reading 原文地址 https://www.darkreading.com/endpoint/when-ransomware-strikes-7-steps-you-can-take-now-to-prepare-/a/d-id/1330313?
免责声明	本译文译者为安天实验室工程师，出自个人兴趣在业余时间所译，本文原文来自互联网，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。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。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。 本译文亦不得用于任何商业目的，未授权任何人士和第三方二次分享本译文，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。

安天发布《勒索软件“ONI”分析报告》

近日，安天CERT（安全研究与应急处理中心）在梳理网络安全事件时注意到，一种新型勒索软件在日本开始大范围传播，它被命名为“ONI”，在日语中是“鬼”的意思。该勒索软件主要攻击日本企业，攻击持续了近9个月时间。在这次攻击中，基于DiskCryptor的bootkit磁盘加密工具也被使用，这与最近火热的“Bad Rabbit”勒索软件如出一辙。

“ONI”针对不同行业的日本公司的攻击都有着非常相似的手法。首先它会利用鱼叉钓鱼邮件引诱受害者上钩，打开带有恶意代码的邮件附件，接下来攻击者利用“Ammyy Admin”RAT与其他恶意代码进行横向渗透，最终获取域控制器权限，控制全部内网。除了普通的“ONI”，攻击者针对关键资产会使用“MBR-ONI”，加密系统的MBR并且还可以对磁盘任意数据进行清除。感染“MBR-ONI”的目标由Active Directory服务器和其他关键资产组成，修改后的MBR第一条指令由DiskCryptor使用的NOP-NOP-JMP组成。这也证实攻击者使用了合法的开源工具DiskCryptor的修改版本。这个工具是一个开源的加密解决方案，提供所有磁盘分区的加密。与NotPetya不同，“MBR-ONI”允许恢复加密的磁盘，攻击者会提供正确的解密密钥。但这应是攻击者为了掩盖其后一步攻击的方式。

安天CERT提醒广大网络使用者，要提高网络安全意识，在日常工作中要及时进行系统更新和漏洞修复，不要随意下载非正版的应用软件、非官方游戏、注册机等。收发邮件时要确认收发来源是否可靠，更加不要随意点击或者复制邮件中的网址，不要轻易下载来源不明的附件，发现网络异常要提高警惕并及时采取应对措施，养成及时更新操作系统和软件应用的好习惯。目前，安天追影产品已经实现了对该类恶意代码的检出。

木马程序

安天【追影威胁分析系统】无需更新病毒库，即可实现对上述木马程序进行有效检测，下为其自动形成的分析报告：

文件由页面手工提交，经由YARA自定义规则鉴定器、文件来源信息分析鉴定器、文件元数据分析鉴定器、数字证书鉴定器、静态分析鉴定器、动态行为（默认环境）鉴定器、智能学习鉴定器、安全云鉴定器等鉴定分析。

最终依据静态分析鉴定器、智能学习鉴定器将文件判定为木马程序。

根据静态启发式检测得出该文件具有以下行为：delete shadow file、自删除、获取驱动器类型、查找指定内核模块、遍历进程、获取计算机名称、独自打开文件、访问文件尾部、文档篡改。

文件名	oniMalware
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	98 KB
MD5	9C5F5CD0CEE2065605E0D114555086E3
病毒类型	木马程序
恶意判定/病毒名称	Trojan/Win32.Deshacop
判定依据	静态分析

◆ 运行环境

操作系统	内置软件
Windows XP 5.1.2600 Service Pack 3 Build 2600	默认、IE6、Firefox、Google Chrome、Office 2003、Flash、WPS、FoxitReader、Adobe Reader

◆ 危险行为

行为描述	危险等级
delete shadow file	★★★★

◆ 其他行为

行为描述	危险等级
获取驱动器类型	★
查找指定内核模块	★
遍历进程	★
获取计算机名称	★
独占打开文件	★
访问文件尾部	★
文档篡改	★★
自删除	★★

◆ 进程监控

PID		命令行
1616	vssadmin.exe	vssadmin.exe Delete Shadows /All /Quiet