安天周观察

安天官方微博　安天官方微信

主办：安天　2018 年 08 月 13 日 (总第 148 期) 试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天发布《WannaMine 挖矿蠕虫分析报告》

安天捕风小组发现一种基于“永恒之蓝”的恶意代码正在默默蔓延，其被称之为 WannaMine。WannaMine 的目的是挖掘门罗币（Monero），而非窃取用户信息或加密，但其仍会降低受感染机器的性能。如果恶意软件连续运行数小时，会导致设备变热，笔记本电脑甚至可能会因为温度过高而损坏。据测试，WannaMine 能够感染自 Windows 2000 起的所有 Windows 系统（包括 64 位版本和 Windows Server 2003），并使其设备性能明显下降。

本次分析的样本名称为 MsraReport DataCache32.tlb，是一个压缩文件。解压后包含 7 个文件，分别为 srv/srv64，spoolsv/spoolsv64，hash/hash64 和 crypt。其中，crypt 是一个压缩包，包含有“永恒之蓝”漏洞攻击工具集（svchost.exe、spoolsv.exe、x86.dll/x64.dll 等）。

srv/srv64 为 32 位 /64 位的主服务，攻击入口点，样本启动后该文件会被重命名为 tpmagentservice.dll。该服务能开机启动，并在启动后加载 spoolsv.exe。spoolsv/spoolsv64 为 32 位 /64 位攻击母体，样本启动后该文件会被重命名为 spoolsv.exe。它对局域网进行 445 端口扫描，确定可攻击的内网主机。同时启动挖矿程序 hash，漏洞攻击程序 svchost.exe、spoolsv.exe。hash/hash64 为 32 位 /64 位挖矿程序，样本启动后该文件会被重命名为 TrueServiceHost.exe。

“永恒之蓝”漏洞的利用过程为：主控程序 spoolsv/spoolsv64 被重命名为 spoolsv.exe, 运行后会获得自身主机 HOST，然后对局域网内的主机进行扫描。通过获得的 IP 表，扫描局域网内开放的 445 端口后会将扫描结果写入到 EternalBlue 攻击程序 svchost.exe 的配置文件 svchost.xml 中。永恒之蓝攻击完成之后，会修改 DoublePulsar 后门程序 spoolsv.exe 的配置文件 spoolsv.xml，然后启动 spoolsv.exe（NSA 黑客工具包 DoublePulsar 后门）安装后门程序。完成后执行 Payload，解压 MsraReportDataCache32.tlb，直至整个内网环境被感染。

安天提醒广大互联网用户，可关闭 SMB 445 等网络共享端口，关闭异常访问，及时更新系统。可使用强密码以降低感染风险。企业应完善企业网络架构，部署相应的安全设备，加强管理机制。亦可使用安天捕风系统，对内网网络安全进行预警防护。

新 WiFi 密码破解技术被公开，能轻松破解大多数现代路由器的 WiFi 密码

其允许破解 WPA/WPA2 无线网络协议，启用了基于成对主密钥标识符（PMKID）的漫游功能。此技术是在专家分析推出 WPA3 安全标准的过程中意外发现的新攻击，而使用平等同时认证（SAE）的 WPA3 将更安全不会支持此技术攻击。

攻击者可以使用 hcxdumptool 等工具，从目标接入点请求 PMKID，并将接收到的帧转储到文件中，运行 hcxpcaptool 工具将捕获的数据从 pcapng 格式转换为 hashcat 接受的哈希格式，然后使用 Hashcat 密码破解工具获取作为目标无线网络密码的 WPA PSK（预共享密钥）密码。

此次新发现的技术有如下特点：攻击者直接与 AP 通信不再需要常规用户；不再需要等待普通用户和 AP 之间的完全 4 次握手；不再发生 EAPOL 帧的最终重传；常规用户不再发送最终的无效密码；当常规用户或 AP 离攻击者太远时，不会丢失 EAPOL 帧；不再需要修复 nonce 和 replaycounter 值；最终数据将显示为常规十六进制编码字符串，没有 pcap，hccapx 等特殊输出格式。

原文链接：https://securityaffairs.co/wordpress/75170/hacking/hacking-wifi-wpa-wpa2.html

Ramnit 恶意软件演变黑色僵尸网络

Check Point 研究人员最近发现包括两个阶段的黑色僵尸网络攻击，第一阶段使用通过垃圾邮件分发的 Ramnit 恶意软件，在近两个月内发生了 10 万次感染。第二阶段是在 2010 年首次出现的 Ngioweb 恶意软件。背后的攻击者主要致力于创建恶意代理服务器网络，很有可能在这两个中间建立一个大型的多用途代理僵尸网络，可能会发生更大规模的攻击，此次只是冰山一角。Ramnit 为 Zeus 银行木马演变，拥有广泛的信息过滤与提供后门的能力。Ramnit 的僵尸网络 C2 服务器于 2015 年被欧洲刑警在几家私企公司的配合下端掉了。此次重新启动，使用相同的载荷，架构和加密算法，增强了保护恶意软件的规避技术和僵尸程序的管理，（更新的间谍软件模块）hook 浏览器，监控 URL 网址，可实时盗取数据，并显示受害者被 web 注入情况，还针对网上银行会话的实时欺诈攻击构建了新的攻击方案。Ngioweb 是一种多功能代理服务器包括作为常规反向连接代理和中继代理，并使用自身的二进制协议和两层加密，支持反向连接模式，中继模式，IPv4，IPv6 协议，TCP 和 UDP 传输。

原文链接：https://threatpost.com/ramnit-changes-shape-with-widespread-black-botnet/134727/

每周安全事件

类 型	内 容
中文标题	Linux 内核出现漏洞可触发远程 DoS 攻击
英文标题	Linux kernel bug: TCP flaw lets remote attackers stall devices with tiny DoS attack
作者及单位	Liam Tung
内容概述	Linux 内核 4.9 版本中出现一个漏洞，可被攻击者利用，通过网络工具套件发起 DoS 攻击。研究人员表示，有很多网络设备供应商、电脑和服务器制造商、移动供应商以及操作系统制造商都可能受到影响。 此外，由于 Linux 使用范围很广，亚马逊、苹果、Ubuntu 以及 ZyXEL 也都可能中招。目前，漏洞命名为 SegementSmack，编号为 CVE-2018-5390，还没有有效的缓解措施。
链接地址	https://www.zdnet.com/article/linux-kernel-bug-tcp-flaw-lets-remote-attackers-stall-devices-with-tiny-dos-attack/

每周值得关注的恶意代码信息

经安天【CERT】检测分析，本周有 9 个移动平台恶意代码和 5 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.BankerIN.a[prv,exp] 2018-08-06	该应用程序伪装印度银行客户端，钓鱼窃取用户的信用卡信息，会对用户的财产安全造成极大的威胁，请立即卸载。（威胁等级高）
		Trojan/Android.jmelon.a[exp,rog] 2018-08-08	该应用程序安装无图标，运行会请求激活设备管理器，联网上传设备固件信息和安装应用列表信息，后台推送广告，造成用户资费消耗。（威胁等级高）
		Trojan/Android.Satori.a[sys,bkd] 2018-08-09	该应用程序包含恶意代码，利用端口漏洞，后台私自加载恶意脚本，攻击用户手机。会造成用户手机性能下降，危害用户手机安全，请立即卸载。（威胁等级中）
	较为活跃的样本	Trojan/Android.Salestracker.b[exp,rog]	该应用程序安装无图标，包含风险代码，后台私自发送注册短信，上传用户手机基本信息，联网获取未知应用，私自下载并静默安装。可造成用户资费消耗，建议卸载。（威胁等级中）
		Trojan/Android.Fakegoogleplay.f[prv,spy]	该应用程序伪装 Google Play，运行隐藏图标，后台窃取用户设备固件信息、通话录音、短信、通讯录、通话记录、QQ 和微信信息等一系列隐私信息，通过 socket 上传至服务器，造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.Locker.as[rog,lck]	该应用程序是勒索软件，运行隐藏图标，置顶勒索界面，要求用户付费解锁，影响用户手机的正常使用，造成用户资费损耗，请卸载。（威胁等级中）
		Trojan/Android.TelegramIR.c[prv,rmt,spy]	该应用程序是一款间谍软件，包含设备硬件信息采集，文件管理（文件和文件夹的预览以及移动、删除、重命名、上传、下载），短信实时监控，通话记录实时监控，通话录音、图片、账户、地理位置实时获取，远控摄像头拍照等功能，该软件通讯部分使用 Telegram Bot API 来实现，会造成用户隐私泄露和资费损耗，请立即卸载。（威胁等级中）
		Trojan/Android.FakeSystem.aq[prv,exp,rog]	该应用程序伪装系统应用，安装无图标，后台获取用户通讯录和邮箱账号并上传，私自推送广告，造成用户隐私泄露和资费消耗，建议卸载。（威胁等级高）
		Trojan/Android.Mobilespy.ax[prv,spy]	该应用程序是间谍件，运行登陆后隐藏图标，后台上传用户信箱、通讯录、浏览历史、通话记录、安装列表等隐私信息，造成用户隐私泄露，请卸载。（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 Player 远程代码执行漏洞（CVE-2018-4878）	攻击者构造特殊的 Flash 链接，当用户用浏览器 / 邮件 /Office 访问此 Flash 链接时，会被“远程代码执行”，并且直接被 getshell。CVE-2018-4878 是一个 UAF 漏洞，需要借助强制 GC 或者刷新页面来触发。（威胁等级高）
	较为活跃样本	Trojan[Downloader]/MSWord.Steamilik	此威胁是一类可以下载恶意代码的木马家族。该家族样本为 Word 宏病毒，运行后连接网络下载恶意代码并运行。（威胁等级中）
		Trojan[Downloader]/Win32.Cabby	此威胁是一种具有下载行为的木马类程序。该恶意代码通过钓鱼网站、未知链接、下载黑客发布的免费软件及垃圾邮件附件等形式进行传播。（威胁等级中）
		Trojan[Dropper]/Win32.Daws	此威胁是一种具有捆绑行为的木马类程序。该家族木马感染用户系统后，会自动释放出其它恶意程序并运行。释放的程序大多为盗号类木马程序。（威胁等级中）
		Trojan[Backdoor]/Win32.Gibbon	此威胁是一种可以窃取用户信息的木马类程序。该家族样本运行后连接远程服务器接受攻击者恶意操作，收集用户信息并回传。（威胁等级高）

采用区块链技术实现 GDPR 合规性

Claudio Lima / 文　安天技术公益翻译组 / 译

是的，采用区块链技术可以实现欧盟《通用数据保护条例》（GDPR）合规性。

数据保护和隐私是区块链风靡全球的两个重要原因。采用区块链技术，使得互联网上的交易可信、透明并且可追溯。

GDPR 正是为了加强消费者数据的保护和隐私，因此，一些认为区块链不适用于 GDPR 的想法颇为讽刺、肤浅和无益。仔细研究区块链的基本概念和技术，可以发现该技术能改进 GDPR 规定的数据隐私和安全的基本方面，这取决于具体的方案实现方式，以最终满足 GDPR 的要求。

区块链技术是去中心化的 P2P 方法，而GDPR 则基于传统的中心化互联网方法。因此，将区块链技术应用于 GDPR 面临挑战。

区块链技术的替代方案可以实现 GDPR 合规性，这要求我们深入理解区块链分布式账本技术（DLT）及其生态系统。在设计符合 GDPR 的区块链解决方案时，其身份识别管理流程（例如存储和处理个人身份信息 [PII] 的流程）至关重要。

解决不变性问题

GDPR 的一个关键原则是第 17 条的“删除权”（或“被遗忘权”）。基于该原则，消费者可以在需要时要求其数据处理者（或“控制者”）删除其个人信息。

但是，由于区块链的“记录不变性”原则，区块链交易中包含的所有数据几乎都无法修改。数据被复制到 P2P 节点，这

些节点用作分布式数据库或分布式账本，是区块链的重要组成部分。被添加到公开、任何人都可以参与的区块链中的数据会永远存在，而且从技术上讲，这些数据（或其他元数据）无法篡改。由于区块和交易的构造方式，输入分布式账本的所有信息和记录都是公开可见、不可篡改和不可变的。

那么，这种分布式账本固有的数据不变性，是否会导致区块链无法符合 GDPR 第 17 条呢？不一定。采用混合“链外”（off-chain）架构进行分布式数据存储，就是应对该挑战的一种方法。还可以采用其他方法，即将 PII 数据保留在用户的设备中，创建这些数据的元数据和哈希，然后使用第三方服务器或区块链层访问本地数据。这些方法会产生不同的区块链 -GDPR 合规级别。

为了符合第 17 条的规定，可以将所有 GDPR 敏感信息和数据“链外”存储在分布式或云服务器中，只将相应的哈希存储在区块链层中。通过这种方式，哈希用作 GDPR 敏感数据（链外存储）的控制指针。这些指针不是GDPR 寻求保护的用户数据，而是原始用户数据的假名。实际上，存储原始数据的数据库不受区块链“记录不变性”的影响。因此，服务提供商可以在需要时删除指针的“链接”，使其不再指向链外服务器中的数据。

解决匿名问题

在 GDPR 条例中，与区块链适用性相关，最有趣且最有争议的是第 25 条“设计和默认的数据保护”，它涉及消费者存储数据的假名化（pseudonymization）技术。

区块链的假名化技术是哈希化（hashing），存在两种解释。第一种解释是，因为数据假名化是通过区块链哈希化（而非匿名化）完成的，所以在假名化完成后，数据链接就不再是“私密的”。如果链接被删除，那么就符合第 17 条。第二种解释是，即使假名是加密哈希，它仍然可以链接到原始 PII 数据。然而，这需要一些数学证据——对哈希化的链外数据进行暴力破解——来支撑。

我们的结论是，随着区块链技术的不断加速创新发展，与 GDPR 的适配是一个动态过程。就像现在 GDPR 已经颁布实施，随之而来的是很多法律和技术的交锋。根据出现的问题、或者产生的机遇，GDPR 条例必须积极适应和调整，这样才能使得采用区块链技术的下一代去中心化的互联网成为可能。

原文名称	Adapting Blockchain for GDPR Compliance
作者简介	Claudio Lima。Claudio Lima 是 IEEE 区块链标准副主席和 BEC 区块链工程委员会联合创始人。
原文信息	2018 年 8 月 7 日发布于 Information Week 原文地址 https://www.informationweek.com/strategic-cio/security-and-risk-strategy/adapting-blockchain-for-gdpr-compliance-/a/d-id/1332499?
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《Moker 木马样本分析报告》

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发现一种名为 Moker 的恶意代码。该家族至少从 2012 年开始流行，现在通过漏洞利用工具包 Rig-v EK 进行传播，包括恶意广告行为以及挂马网站。

恶意代码首先将自身注入 svchost.exe，然后连接 C&C 服务器，其使用加密的通信方式，典型的请求格式为：<gate_name>.php?img=<number>，服务器使用加密内容响应，然后它会将自身注入到其他应用程序并发送进一步的请求，包括受感染机器的数据。Moker 通过在注册表中添加 Run 键来实现持久性，它将真正的可执行文件隐藏在合法的 Microsoft 应用程序 Rundll32.exe 之后。微软工具套件中的 autoruns 工具在默认情况下也不显示这样的注册表键。Moker 载荷会释放在用户目录下的 tester 文件夹中，与原样本相比，删除了一些加密信息，而这个信息会保留在注册表中。样本的执行分二个阶段，第一个阶段解密自身，下载执行主要功能的恶意 DLL，第二阶段将该 DLL 注入应用程序。DLL 模块负责恶意代码的所有恶意操作，它还主动与 C&C 进行通信。该 DLL 提供典型 RAT 的各种功能，它使用了非常简单的混淆技术，多数字符串与 API 调用并不会被进行混淆处理。它可以执行某些命令或创建并保存屏幕截图，还可以使攻击者通过远程桌面访问受害者计算机。

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。同时也要做好文件的备份，以防止勒索软件加密重要文件后无法恢复。

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 BD 静态分析鉴定器、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、动态行为鉴定器、智能学习鉴定器、安全云鉴定器等鉴定分析。

最终依据 BD 静态分析鉴定器、静态分析鉴定器、智能学习鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	af1bd82bf11e5a386abf5e1a1dc9773b66f7936f6e2e8f3ea4cc913794bf5a81
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	159 KB
MD5	76987E1882EF27FAAB675C4A5CE4248D
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Enchanim
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	行为描述	危险等级
检测虚拟机	★★★★★	映射内存方式注入	★★★

◆ 常见行为

获取主机用户名称	★
查找指定内核模块	★
遍历进程	★
打开自身进程文件	★
查找特定窗体	★
获取计算机名称	★
释放 PE 文件	★

◆ 文件扫描

文件名	文件 MD5	家族相似性	yara 扫描
target.exe	76987e1882ef27faab675c4a5ce4248d	N/A	N/A
target.exe.dmp	9e8447624b9f28e9f52f52977719ebc2	N/A	N/A
139d2e78	4c03c7a73d6d4d28e34cae317dd574bc	N/A	N/A

◆ UDP 信息

源 IP	源端口	目的 IP	目的端口
0.0.0.0	68	255.255.255.255	67
192.168.122.1	67	192.168.122.246	68
192.168.122.246	137	192.168.122.255	137
192.168.122.246	1025	192.168.122.1	53
.....	.....	.....	.....