安天周观察

主办：安天　2017 年 5 月 22 日（总第 87 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天关于“WannaCry”的响应进展

北京时间2017年5月12日20时左右，全球爆发大规模勒索软件感染事件。

从 5 月 12 日 20:20 安天启动“A 级灾难”响应起，截止 5 月 19 日，安天已经针对勒索蠕虫 WannaCry 陆续发布了 4 篇分析报告，分别为《安天紧急应对新型“蠕虫”式勒索软件“WannaCry”全球爆发》（另有 1 篇更新版）、《对“魔窟 WannaCry”勒索蠕虫变种情况的分析》、《安天对“魔窟 WannaCry”支付解密流程分析》、《安天文件解密工具可有效对被加密文件进行解密》、《安天发布“魔窟 WannaCry”蠕虫解密工具》。

公众在关注事件进展时提出大量问题，安天针对用户所提高频问题发布 3 份 FAQ，以解决用户对该事件的疑问，并验证事发期间的不实传言。

而由于“魔窟 WannaCry”大规模爆发于北京时间周五晚 20 点，因此国内还有大量政企机构网络节点在病毒爆发时处于关机状态，5 月 15 日（周一）开机成为一场安全考验。对此，安天先后发布 2 篇开机指南《安天应对勒索蠕虫“魔窟 WannaCry”开机指南》，发布 1 篇《安天防勒索解决方案》及 1 篇《针对重要文件已被“魔窟 WannaCry”加密后的处置建议》，并准备 4 合 1（免疫工具 + 专杀工具 + 智甲防御勒索免费版 +“魔窟”勒索蠕虫内网响应网页）光盘、U 盘，为用户防止病毒感染计算机做了最佳保障。

5 月 16 日，安天应邀参与中国计算机学会青年科技论坛 (CCF YOCSEF) 联合 CCF 计算机安全专业委员会共同举办的“勒索病毒：凭什么能绑架我们的系统？”特别技术论坛，安天负责人王小丰参与论坛并进行题为《“魔窟 WannaCry”勒索蠕虫事件的应急过程和思考》的发言。

事件爆发后，安天技术人员始终以用户为中心做好应急支撑，及时响应客户需求，持续开展应急服务，并不断修订应急工具方面的不足，为用户提供了全面可持续应急服务。

安天携手神州数码　发力政企网络安全市场

5 月 16 日，安天与北京神州数码有限公司（下简称“神州数码”）在北京举行了合作签约仪式。据悉，神州数码通过本次合作正式成为安天的全国总经销商，将助力安天全线产品在全国的渠道销售。双方希望通过合作各取所长，互利共赢。

安天参会代表表示：安天将充分借助神州数码完备的渠道合作伙伴体

系及丰富的平台资源，为更多的政企客户提供更好的网络安全产品及服务，保障其网络安全，构建一个良性的网络安全行业生态圈。同时，通过与神州数码合作，也可以使安天这样拥有核心技术的厂商能够集中精力，更好的专注于自身技术的完善与提高，以推出更加符合客户需求的产品与服务。

安天应邀出席针对勒索病毒特别技术论坛

5 月 16 日，中国计算机学会青年科技论坛 (CCF YOCSEF) 联合 CCF 计算机安全专业委员会共同举办一次“勒索病毒：凭什么能绑架我们的系统？”特别技术论坛，安天研发负责人王小丰参加论坛并做了题为《“魔窟 WannaCry”勒索蠕虫事件的应急过程和思考》的汇报。

论坛上，安天参会代表回顾了“魔窟 WannaCry”勒索蠕虫事件始末，向与会嘉宾介绍了安天对于该事件的应急过程和相关结果，“还好病毒大爆发在上周五晚 8 点的时间，大量的内网用户处于关机状态，给同行和我们自己有相对充分的时间应急处理，有两天时间来形成包括周一开机指南、免疫专杀工具等解决方案”。他提出，相比影响力巨大的安全事件，还有更多潜在的威胁更值得关注，“我们目前认为这是一起网络军火泄密后的非受控使用事件，超级大国的网络军火的攻击性、冲击性非常强。一旦网络军火流落到第三方，并且被大规模使用，肯定会造成大面积的安全事件”。

在汇报中，王小丰坦陈“我国整体信息安全水平的基础防御能力相对较低，虽然在威胁检测引擎、大数据安全分析等方面取得了一些单点突破，但信息安全防御体系性依然有待完善。我国长期网络安全投入不足的客观情况，叠加上武器级水准的网络攻击，就会产生灾难性的后果。”。

王小丰认为，当前业界很重视态势感知，但也存在表面化的倾向，难以达成“全天候、全方位”的深度、广度和持续性，在防御的有效性方面，功力不够扎实。从大规模机构信息系统建设规划来看，要做到架构安全、被动防御、积极防御和威胁情报各个层次协调并举。同时要解决轻响应、缺恢复手段的局面。“我们过去过于依赖网络边界的隔离和边界防护，但内部节点的配置加固、补丁升级和安全软件的及时更新反而不能有效落实，安全规划的防御纵深和产品间协同联动没有有效达成。导致内部网络打入一点，就会全网沦陷，内部网络安全疏漏比较多，安全治理工作也任重道远”。

每周安全事件

类 型	内 容
中文标题	维基解密披露 CIA 恶意软件框架中的新工具：AfterMidnight 与 Assassin
英文标题	Vault7-Wikileaks published documentation for AfterMidnight and Assassin malware
作者及单位	Pierluigi Paganini；Security Affairs
内容概述	近日，维基解密发布 CIA Vault7 工具包中新的一批文件，详细披露了针对 Winodws 平台上的两个恶意软件框架——AfterMidnight 以及 Assassin。这次公布的 AfterMidnight 以及 Assassin 均属于 CIA 恶意软件框架。它会在受感染的计算机上监控并汇报用户行为，再由远程主机执行恶意行为。维基解密在文件中称，攻击者会使用 AfterMidnight 在目标系统上进行动态载入，执行恶意 payload。恶意 payload 中的主控制模块，会伪装成 Windows 动态链接库文件，执行 Gremlins 操作。它会检测、破坏目标软件的功能，或者为其他 gremlins 提供服务。最新披露的用户指南中也指出，AfterMidnight 的文件密钥保存在其他地方。程序中有一个叫做 AlphaGremlin 的特殊模块。AlphaGremlin 中包括了一种特别的脚本语言，可以让使用者在目标设备上设定自定义的任务，然后远程执行恶意操作。
链接地址	http://securityaffairs.co/wordpress/59130/intelligence/aftermidnight-assassin-malware-framework.html

每周值得关注的恶意代码信息

经安天检测分析，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

平台分类	关注方面	名称	相关描述
移动恶意代码	新出现的样本家族	Trojan/Android.zsqqhz.a[exp, fra]2017-05-15	该应用程序伪装 QQ 刷钻工具，运行后发送短信到指定号码，并私自发送短信订阅服务，造成用户资费损失，建议立即卸载。（威胁等级高）
		Trojan/Android.Herringy.a[exp, rog]2017-05-16	该应用程序安装后无图标显示，程序运行会监听短信拦截指定短信，并私自回复；联网上传设备固件信息获取推送应用相关参数，通过通知栏推送应用，警惕其私自下载安装，造成用户资费消耗。（威胁等级中）
	较为活跃的样本	Trojan/Android.AppBotSMS.f[prv, exp]	该应用程序运行隐藏图标，上传手机号和设备 IMEI，拦截指定号码的短信并上传，诱导激活设备管理器致使无法正常卸载，造成用户隐私泄露，建议立即卸载。（威胁等级高）
		Trojan/Android.emial.fp[prv, exp]	该应用程序启动后隐藏图标，窃取用户短信并发送到指定号码，接收短信指令，并转发短信，造成用户隐私泄露和资费消耗，建议立即卸载。（威胁等级中）
		Trojan/Android.Kemoge.c[exp, rog]	该应用程序安装后隐藏图标，在后台静默下载恶意应用，造成用户资费消耗和其他安全威胁，建议卸载。（威胁等级高）
		Trojan/Android.QQspy.bo[prv, exp]	该应用程序伪装 QQ 刷钻工具，诱导用户输入 QQ 账号和密码，并通过短信转发，造成用户隐私泄露和资费消耗，建议立即卸载。（威胁等级中）
		Trojan/Android.SmsSpy.t[prv, exp]	该程序为游戏应用，会通过短信发送地理位置到指定号码，拦截短信，利用短信执行远程指令。造成用户隐私泄露和资费消耗，建议立即卸载。（威胁等级中）
		Trojan/Android.LevelDropper.c[rog, sys, exp]	运行会私自上传设备固件信息，释放恶意子包尝试获取 root 权限，篡改系统文件。后台运行恶意文件，加载广告以及流氓推广应用。造成用户资费损耗，系统破坏等，建议卸载。（威胁等级高）
		Trojan/Android.Triada.ak[exp, sys]	该应用程序伪装成系统应用，动态加载恶意子包，私自提权，推送广告，建议卸载，避免造成资费损耗。（威胁等级中）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	多个 Windows SMB 远程执行代码漏洞 (MS17-010)(CVE-2017-0143\CVE-2017-0144\CVE-2017-0145\CVE-2017-0146\CVE-2017-0148)	当 Microsoft 服务器消息块 1.0(SMBv1) 服务器处理某些请求时，存在多个远程执行代码漏洞。成功利用这些漏洞的攻击者可以获取在目标系统上执行代码的能力。为了利用此漏洞，在多数情况下，未经身份验证的攻击者可能向目标 SMBv1 服务器发送经特殊设计的数据包。（威胁等级高）
	较为活跃的样本	Trojan[Ransom]/Win32.Wanna	此威胁是一种可以通过 SMB 远程执行代码漏洞 (MS17 — 010) 进行传播，并加密用户文件勒索赎金的木马程序。该家族样本运行后加密特定后缀的文件并在文件名最后加上 .WNCRY，向用户勒索比特币。（威胁等级高）
		Trojan[Dropper]/Win32.Dapato	此威胁是一种木马类程序。该家族运行后会释放多个恶意代码。该家族可以注入其它进程，能够加密用户文件，下载其它恶意代码等。（威胁等级中）
		Trojan[Backdoor]/Win32.Simda	此威胁是一种带有后门功能的木马类程序。该家族可以通过垃圾邮件及恶意网站等方式进行传播。Simda 家族的变种有多种功能，如后门、密码盗取器、木马下载器和感染文件等。像这样拥有多种功能变种的木马类程序较为罕见。（威胁等级中）
		Trojan[Banker]/Win32.Banbra	此威胁是一种以窃取网络银行敏感信息为目的的木马类程序。该病毒伪装成正常数据，以获取认证。利用各种途径，使黑客获得数字证书来伪造文件。该家族会收集用户的机密信息，如网上银行详细信息和密码等，并将窃取的数据发送给远程黑客。（威胁等级中）

WannaCry 与 Lararus APT 样本共享代码

Michael Mimoso / 文　安天公益翻译小组 / 译

WannaCry 勒索软件爆发后，研究人员对其进行了归因分析，发现另一起攻击使用了相同的 NSA 攻击工具来传播 Adylkuzz 加密货币采矿机。

Proofpoint 知名漏洞研究员 Kafeine 周一表示，该攻击的规模可能比 WannaCry 更大。WannaCry 从上周五开始在全球传播，利用 SMBv1 漏洞感染未修复的 Windows 机器，所使用的工具是 NSA 的 EternalBlue 漏洞、DoublePulsar rootkit 和后门。一旦 Adylkuzz 感染了一台机器，它会挖掘开源的 Monero 加密货币，在很大程度上模糊其封锁链信息，使研究人员难以追踪其活动。

Kafeine 表示，Adylkuzz 攻击发生在 WannaCry 攻击之前，第一个样本可以追溯到 4 月 24 日。超过 20 个虚拟专用服务器扫描互联网，寻找运行 445 端口 (SMB 流量使用的端口) 的目标，而 EternalBlue 和 DoublePulsar 利用的也是这个端口。

“EternalBlue 成功利用漏洞后，机器就会被 DoublePulsar 感染。然后，DoublePulsar 后门从另一个主机下载并运行 Adylkuzz。”Kafeine 说，“一旦运行，Adylkuzz 会终止已经运行的实例并阻止 SMB 通信，以避免进一步的感染。它确定受害者的公共 IP 地址，下载挖掘指令，采矿机和清理工具。“

周一下午，谷歌研究人员 Neel Mehta 发表了一篇推文，指出 WannaCry 和 Lazarus APT 之间存在联系。据称，Lazarus 是 2016 年 SWIFT 攻击的幕后黑手，对孟加拉国中央银行和其他银行，赌场发动了攻击。

9c7c7149387a1c79679a87dd1ba755bc @ 0x402560，0x40F598

ac21c8ad899727137c4b94458d7aa8d8 @ 0x10004ba0，0x10012AA4 # WannaCryptAttribution

– Neel Mehta(@neelmehta)，2017 年 5 月 15 日

Mehta 的推文显示，2015 年 2 月的 Lazarus 样本和今年 2 月份出现的 WannaCry 早期版本共享代码。

此后，卡巴斯基实验室和赛门铁克的研究人员，阿联酋网络安全公司 Comae Technologies 的创始人 Matt Suiche 也证实了两者的相似之处，进一步说明朝鲜和目前的勒索软件攻击有关。

从 2014 年的索尼攻击事件开始，Lazarus 组织的历史可谓臭名昭著。该组织窃取并泄露电影剧本，敏感的企业电子邮件和私人数据，还使用擦除工具来破坏 Sony 影业的内部工作站。

2016 年的孟加拉国中央银行攻击事件利用了其与 SWIFT 网络的连接，骗取了近 10 亿美元的转账。攻击发生后，除了 8000 万美元之外，所有资金都被追回了。

在今年的卡巴斯基实验室安全分析师峰会上，卡巴斯基实验室，BAE Systems 和 SWIFT 的研究人员分享了 Lazarus 活动的更多细节，其中包括该 APT 组织的一个名为 Bluenoroff 的小组，该小组致力于窃取资金，以资助 Lazarus 的活动。

他们最终获得了 40 比特币 (约 7.1 万美元)，获利水平远不及 WannaCry。

卡巴斯基实验室在周一公布的报告中说：“现在，我们需要对旧版本的 WannaCry 进行更多的研究。我们认为这可能是解开此次攻击的一些奥秘的关键。有一件事是肯定的：就 WannaCry 起源来说，Neel Mehta 的发现是非常重要的。”

我们向谷歌发送与 Mehta 会面的请求，但被拒绝了。

谷歌发言人告诉 Threatpost，“Neel 的推文之外没有什么可以补充的。”

虽然研究人员承认证据还不够明确，但这是国家赞助的 APT 组织的工具第一次用于此等规模的攻击。

Suiche 在周一发表的一份报告中说：“将该攻击追溯到 Lararus 组织是有道理的，该组织过去一直致力于渗透金融机构来窃取资金。如果能够验证这一点，就意味着 WannaCry 实际上是第一个国家赞助的勒索软件。这也意味着一个敌对国家利用方程式组织 (Equation Group) 的进攻能力来制造全球混乱。”

卡巴斯基实验室还表示，这是假标识行动的可能性“非常低”。在过去 18 个月内，卡巴斯基实验室的研究人员就 APT 和假标识发表了数份报告。

“从理论上说，任何事情都是可能的，包括 2017 年 2 月的 WannaCry 样本复制了 2015 年的后门代码。但是，较新的版本似乎删除了这一代码。”卡巴斯基实验室说，“2017 年 2 月的样本似乎是 WannaCry 加密器的一个非常早期的变种。我们认为假标识的可能性非常低。”

原文名称	WannaCry Shares Code with Lazarus APT Samples
作者简介	Michael Mimoso，Threatpost 的编辑。
原文信息	2017 年 5 月 1 日发布于 Threatpost，原文地址 https://threatpost.com/wannacry-shares-code-with-lazarus-apt-samples/125718/
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《方程式组织攻击工具 Doublepulsar 分析报告》

近日，勒索软件 WannaCry 在世界各地爆发，安天 CERT 连续发布了多篇分析报告。WannaCry 使用了方程式 Eternalblue 攻击工具和 Doublepulsar 后门。

Doublepulsar 后门是“影子经纪人”在 2017 年 4 月 14 日泄露出的方程式组织攻击工具包中的一个模块。与 Etenalblue 相同，Doublepulsar 利用 SMB 漏洞，通过 445 端口进行攻击。首先，攻击者使用“use Doublepulsar”命令调用该模块，设置完目标主机、回连主机后，进而进行五项功能选择。

第一个选项“OutputInstall”，选择后可以将安装功能的 shellcode 导出到二进制文件中。

第二个选项“Ping”，Ping 用来测试是否存在后门，攻击者可以利用该功能对目标主机进行漏洞扫描。这也为分析人员检测主机是否存在漏洞提供了便利，通过抓取 Ping 功能的流量，能够帮助分析人员及开发人员识别设备是否已经被植入后门和改进产品。

第三个选项“RunDLL”，使用异步调用向用户模式的进程植入 DLL，攻击者利用 msf 等自动化工具生成可供利用的 DLL，加载该 DLL，通过“RunDLL”选项将其植入到系统进程中。

第四个选项“RunShellcode”，可以通过该选项直接运行 shellcode。

最后一个选项是“Uninstall”，可以移除系统中的后门，这也为分析人员提供了一个解决问题的好方法。

虽然微软在三月份已经发布了 MS17-010 补丁，但是很多用户并没有安装该补丁，多名研究人员在微软发布补丁之后进行了互联网扫描，结果发现全球数万台 Windows 计算机感染了 Doublepulsar，由此可见，本次 WannaCry 勒索软件在全世界大面积传播并不是偶然。

安天建议广大用户，对未打补丁的电脑进行如下操作。首先，在开机前首先拔掉网线，与内网机器隔离。然后使用安天对于勒索软件 Wannacry 开发的免疫工具设置免疫，并使用专杀工具清除病毒。此后，使用 PE 盘进入操作系统进行备份数据，最后再打开计算机。目前，安天追影威胁检测系统已经实现了对于 Doublepulsar 样本的检出。

木马程序

安天【追影高级持续威胁分析系统】无需更新病毒库，依据行为即可实现对上述木马程序进行有效检测，以下为其自动形成的分析报告：

文件被内部组件发现，经由 BD 静态分析鉴定器、美国软件交叉索引 (NSRL) 鉴定器、可交换信息 (EXIF) 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 (Windows7) 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。

文件名	Doublepulsar-1.3.1.exe
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	45 KB
MD5	C24315B0585B852110977DACAFE6C8C1
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Backdoor]/Win32.ShadowBrokers
判定依据	静态分析

运行环境

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

操作系统	Windows 7 6.1.7600 Build 7600
内置软件	默认、ie9、office 2007、flash、wps、FoxitReader、adobe reader

其他行为

检测类型	检测点	详细说明
编译指令	未知壳	未被公开的壳，经常被恶意代码使用，用来保护恶意程序被查杀。
PE 结构	无版本信息并且不是 GCC 编译器	除 GCC 编译器外，常规编译器均默认包含版本信息。如果不是 GCC 编译器，并且不包含版本信息，显然是作者故意抹掉版本信息，逃避追查。
PE 结构	入口点遮蔽	使用了入口点遮蔽 (Entry-Point Obscuring，EPO) 的病毒编码技术。EPO 技术可以躲避杀毒软件的检测。

EXIF 信息

描述	值
File Size	44 kB
File Type	Win32 EXE
MIME Type	application/octet-stream
Machine Type	Intel 386 or later, and compatibles
Time Stamp	2013:01:03 04:03:18+08:00

报告地址：https://antiy.pta.center/_lk/details.html?hash=C24315B0585B852110977DACAFE6C8C1