安天周观察

主办：安天　2017 年 7 月 3 日（总第 93 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天发布《攻击乌克兰等国的“必加”(Petya) 病毒分析与应对》

北京时间 2017 年 6 月 27 日 21 时许，安天安全研究与应急处理中心 (Antiy CERT) 关注到乌克兰银行等相关机构、政府首脑计算机遭到计算机病毒攻击的信息。综合各方威胁情报后，初步判断受影响最严重的国家是乌克兰，其他部分国家均受到不同程度的影响，包括俄罗斯、西班牙、法国、英国、丹麦、印度、美国等。

安天启动了 A 级预警响应，经数小时的分析研判，发现该病毒的复合传播方式有较大风险，但鉴于该病毒初始投放具有较强的地域性特点，同时我国在“魔窟”(WannaCry) 应急工作中打下了良好基础，故现阶段该病毒尚未在我国大面积传播，建议将事件降为 B 级。

安天在 6 月 28 日凌晨 5 时发布了《攻击乌克兰等国的“必加”(PETYA) 病毒分析与应对》报告，报告对病毒的传播机理与相关样本进行了详细分析，并给出相应的解决方案。

安天在 2016 年基础威胁年报中，对比了“蠕虫时代的传播入口到勒索软件的传播入口”，对其复合型的传播趋势做了预判，而“必加”(Petya) 新版本复合手段传播感染进一步看到，通过邮件进入到内部网络，在网内传播的方式，可能会带来比类似 WannaCry 蠕虫这种单纯的扫描植入方式更严重的后果。但同时更值得警醒的是，“必加”(Petya) 所使用的并非是 0DAY 漏洞，甚至也非 1DAY 漏洞，而是陈旧的漏洞，其他传播方式也是利用类似弱口令 / 空口令这种基本的配置问题。这些问题再次说明，系统策略加固和及时的补丁升级，是安全的必修手段。

通过类似邮件或浏览器等入口的单点注入、之后横向移动扫荡内部网络，这本身是传统定向攻击到 APT 攻击的基本手段，但由于 APT 攻击的隐蔽性，使多年类似的攻击存在，并没有有效驱动内网安全治理的改善。而勒索病毒攻击，是同样具有严重后果，同时却一种后果高度可见的安全风险。从“魔窟”(WannaCry) 到“必加”(Petya)，其将许多信息系统的防护无效的情况全面暴露出来。

2015 年起，安天根据勒索软件已经成为一种地下经济的商业模式，必然会推动其大规模蔓延爆发的判断，在终端防御智甲产品中增加了“加密行为识别”、“诱饵文件”等策略，使用 2016 年 10 月的智甲版本，在不升级病毒库和模块的情况下，就有效拦截 WannaCry 等新兴勒索软件的加密行为。从安天的产品体系来看，达成有效防护、实现价值输出，则是我们一贯的追求。

报告原文　工具下载

■ Skype 曝出远程缓冲区溢出漏洞，致恶意代码执行

SecurityAffairs 网站 6 月 28 日消息，安全公司 Vunerability Lab 的研究人员发现 Skype 中的一个堆栈缓冲区溢出漏洞，漏洞编号 CVE-2017-9948，远程攻击者可利用漏洞执行恶意代码。

微软已在 Skype7.37.178 版本中修复了该漏洞，漏洞存在于 SkypeWeb 信息和通讯服务中，在团队视频会议时可以被利用触发。在无需用户交互的情况下，低权限 Skype 用户账户就能利用该漏洞，危害级别为高危，影响到 XP/7/8/10 系统中的 Skype 7.2/7.35/7.36。漏洞就位于 Skype 的剪贴板格式功能中，攻击者利用共享剪贴板的远程计算机，在向 Skype 传输时触发栈缓冲区溢出。

具体来说，攻击者构建恶意图片文件，从计算机系统的剪贴板复制粘贴到对话窗口即可利用漏洞，研究人员已经公布了 PoC。（来源：http://securityaffairs.co/wordpress/60507/hacking/skype-buffer-overflow.html）

■ Anthem 将支付 1.15 亿美元和解数据失窃案

2015 年 2 月，美国第二大健康保险公司 Anthem 承认遭到了极其复杂的网络攻击，攻击者未经授权访问了其 IT 系统，获得了八千万前客户和现客户的私人信息，包括名字、出生日期，医疗 ID / 社保号码，住址、电子邮件和雇佣信息。这次攻击被认为与中国有关。

近期，因这起数据窃取而提起集体诉讼的原告律师宣布，他们与 Anthem 达成了 1.15 亿美元的和解协议。和解协议还需要等待地区法官 Lucy Koh，法官计划于 8 月 17 日在加州圣何塞举行听证会。如果获得批准，这将是美国历史上金额最高的数据失窃和解。这笔赔偿金相当于每位受影响的客户每人得到 1.43 美元。（来源：http://www.solidot.org/story?sid=52870）

一周简讯

- 安天发布最新勒索蠕虫“必加”(Peyta) 分析报告。
- Shifr RaaS 允许简单设置即可获得样本。
- 英国公司人为失误向用户发送密码重置。
- 研究者发现针对 POS 终端 Neutrino 木马。
- Google 从搜索中剥离私人医疗数据。
- 研究者发现绕过微软 AV 工具的方法。
- 勒索软件 SamSam 攻击增加且赎金更高。

安天 CERT 搜集整理，详情请见：http://bbs.antiy.cn

每周安全事件

类 型	内 容
中文标题	安全专家证实：数十秒内可近距离窃取 AES-256 加密密钥
英文标题	Stealing AES-256 keys in seconds using €200 of off-the-shelf components
作者及单位	PPierluigi Paganini；Security Affairs
内容概述	近日，研究人员使用价值 224 美元的现成电子元件监测计算机电磁辐射，并在空中搜索密钥的整个过程虽然需要五分钟，但专家注意到，缩小距离至 30 厘米的同时即可缩短时间至 50 秒内提取密钥。随后，专家们组建了一台监测设备，即由一个简单回路天线连接至外部放大器与带通滤波器后，插入一款无线 USB 存储数据。该组件极其精巧，可隐藏在夹克或笔记本电脑的外壳中。专家表示，他们设计的系统能够记录由 ARM Cortex-M3 供电芯片运行产生的 SmartFusion2 无线电信号。 专家强调，该技术在目标系统附近操作更为有效，因为电磁信号辐射随距离的递增迅速下降。此外，该技术还可通过高昂设备进行改进。
链接地址	http://securityaffairs.co/wordpress/60383/breaking-news/aes-256-side-channel-attack.html

每周值得关注的恶意代码信息

经安天检测分析，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

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	Tool/Android.ExtremeSpy.a[prv，exp] 2017-06-26	该应用程序是一款监控工具，根据需求可以监控的业务为：短信、通话记录、联系人、地理位置等，建议谨慎使用。（威胁等级低）
		Trojan/Android.woSpy.a[prv，exp] 2017-06-27	该应用程序无实际功能，运行后进行远程控制操作，私自发送短信、上传短信、手机频繁振动等，造成用户隐私泄露，建议卸载。（威胁等级高）
		Trojan/Android.Terbod.a[prv，rmt，fra] 2017-06-28	该应用程序伪装成正常应用，运行后隐藏图标，利用 Telegram 提供的通讯接口，接收远程指令，窃取用户短信和通讯录并联网上传，造成用户隐私泄露和流量消耗，建议立即卸载。（威胁等级中）
		Trojan/Android.MeihuaK.a[prv，rmt]2017-06-29	该应用安装无图标显示，会接受短信指令，收集并上传用户短信、通话记录、QQ 聊天记录等隐私信息，按指令发送指定短信、拨打指定电话，弹窗锁定手机进行勒索，同时发送邮件报告服务端软件运行情况。造成用户隐私泄露、资费消耗，建议卸载。（威胁等级高）
		Trojan/Android.DroidMiner.a[prv，exp]2017-06-29	该应用运行隐藏图标，窃取用户短信、联系人、谷歌账号、通话记录、手机基本信息等用户信息，利用前置摄像头进行人脸拍照，并发送到指定邮箱。造成用户隐私泄露和资费消耗。（威胁等级高）
	较为活跃样本	Trojan/Android.QQspy.cg[prv，exp]	该应用程序伪装成刷赞类应用，会诱导用户输入 QQ 账号密码，通过邮箱转发，造成隐私泄露和资费损耗，建议立即卸载。（威胁等级中）
		Trojan/Android.SmsFilter.h[sys，rmt]	该应用具有监听收件箱、拦截指定短信、接收短信指令进行拨打电话等恶意行为，影响用户正常使用，建议卸载。（威胁等级中）
		Trojan/Android.Triada.ap[exp，rog]	该应用程序运行后加载恶意网址，上传用户手机 IMEI 号、IMSI 号、MAC 等信息，联网下载其他软件，造成用户流量消耗和隐私泄露。（威胁等级高）
		Trojan/Android.Guerrilla.e[fra，exp]	该应用程序伪装成系统应用，启动会隐藏图标并加载广告，造成用户资费消耗，建议立即卸载。（威胁等级中）
		Trojan/Android.FakeInst.eu[prv，exp]	该应用程序运行会隐藏图标，后台联网收集用户短信、通讯录隐私上传，遍历通讯录联系人群发指定短信，建议立即卸载，避免造成隐私泄露和资费损耗。（威胁等级高）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	FFmpeg 本地文件任意读取漏洞	由于 FFmpeg 可处理 HLS 播放列表，而播放列表中已知可包含外部文件的援引。恶意攻击者可以利用精心构造的 avi 文件中的 GAB2 字幕块，上传构造的 avi 视频到使用 FFmpeg 的目标站点，可以通过 XBIN codec 获取到视频转换网站的本地文件（例如：查看 /etc/passwd 文件内容），从而导致敏感数据信息泄露。（威胁等级高）
	较为活跃的样本	Trojan[Ransom]/Win32.Petya	此威胁是一类可以加密用户数据索取赎金的勒索软件家族。该样本遍历磁盘加密文件并修改 MBR，重启后会提示勒索信息。（威胁等级中）
		Trojan[Banker]/Win32.Tuhkit	此威胁是一类可以窃取用户银行信息的木马家族。该家族样本运行后连接远程服务器，收集用户系统中网络银行信息并回传。（威胁等级中）
		Trojan[Dropper]/Win32.Brpd	此威胁是一种具有捆绑行为的木马类程序。该家族会携带恶意软件，在用户电脑中安装并运行。（威胁等级高）

可见性是增强 ICS 安全的关键

Sara Peters / 文　安天公益翻译小组 / 译

更好的可见性对于改善工业控制系统 (ICS) 和关键基础设施的网络安全至关重要，但是这要求 OT(操作技术) 和 IT(信息技术) 进行融合。

如何解决工业控制系统的网络安全问题？

专家表示，更好的可见性对于提高 ICS/SCADA 的安全性至关重要。但是，除非信息安全团队停止用 IT 专家的眼光来看待 ICS 环境，否则他们永远不会获得这种可见性。

专家指出，IT 和 OT 的装备、流程和人员有着根本的差异。在网络安全专家担心 ICS 恶意软件攻击国家电网时，OT 工程师们担心的是，他们的发电站和生产线可能不仅会遭到黑客破坏，还面临其他威胁。因此他们坚持广泛的过程安全管理控制、危害分析、变更管理、应急响应，事件调查规则等等，以便及早和迅速地应对这些威胁。

将任何新事物引入操作环境必须要非常慎重，因为任何对可用性或完整性的干扰都有可能导致不可逆转的、代价高昂的甚至危险的物理影响。最糟糕的结果是持续停电、水坝破裂、核崩溃和公共供水系统污染，除此之外，还会导致经济影响。没有经过充分测试的软件补丁一旦被释放到化工厂的操作环境中，其系统可能会在生产过程中发生故障或脱机，即使时间很短，化工厂也会遭受严重的损失。“任何 CEO 都不会因为要去修复貌似没有损坏的设备 (如不受支持的操作系统) 而同意停止抽油一周。”OT 安全公司 Claroty 的联合创始人和西门子工业安全服务前全球总监加利纳・安托娃 (Galina Antova) 解释说。企业 IT 环境可以承受比 OT 环境更多的迭代和停机时间。如果 OT 环境是稳定、运行和高效的，那么为什么要做些可能会使它变得不稳定的改变呢?

PAS 首席执行官埃迪・哈比比 (Eddie Habibi) 解释说，目前运行的许多物理和网络 – 物理系统已经用了“几代”了。

正如这些专家所说，OT 人员的一般态度是：如果设备没有损坏，就不要改动。因此，信息安全专家面临的挑战是：说服 OT 人员相信有些设备已经损坏了，并在事态变得更糟之前修复它们。

看到他人看不到的东西

正如布莱克所表示，ICS 是“提供对物理过程的可见性的系统”，它们唯一不可见的就是 ICS 系统本身。

布拉格指出：“可见性是一个大问题，在面对网络物理系统时，我们通常没有很多的可见性。”当出现问题时，“你无法确定这是网络原因还是人为原因。”

哈比比说，不幸的是“这些系统不容易被发现”。正如他所解释的，工业环境通常是一个非常复杂的专有系统，通过不同的协议进行通信，需要一定的专业知识才能运行。

布拉格补充说，许多 OT 系统已经不再受支持，供应商可能已经不存在了。其中的一些系统只能通过一个协议通信。

哈比比说：“由于人们不断地增加自动化功能，因此这种情况不断恶化。”

这种 IT-OT“融合”为环境增加了更多的传感器、更多的 I/O 卡、更多的端点、更多的协议、更多的互连和更高的复杂性，使得情况更加糟糕。

“除非你可以直观地看到资产，”布拉格说，“否则很难询问它 ... 但是如果你不知道你有哪些设备，你就不知道你有多脆弱。”此外，他指出，大量工业环境通常由具有访问权限的第三方管理。布拉格说，他们应该对此进行记录，包括谁运行什么，在哪里运行。

怎么做

布拉格解释说，对企业 IT 经理来说非常温柔的姿态可能会被操作工程师认为是危险的入侵。工业过程不能容忍有可能引入的新延迟，如果某些机械系统损坏而无法恢复，则需要更换。“如果提出‘我们要安装一个代理’，他们会说‘不行，你不能安装’”。

这并不能改变必须提高可见性的事实。没有可见性，攻击威胁可能会比一些 OT 团队意识到的更加严重，因为攻击者可能比操作者具有更好的可见性。以 CrashOverride/Industroyer 恶意软件为例，研究人员发现，该恶意软件是 2016 年 12 月对乌克兰电网攻击事件的罪魁祸首。它旨在利用 ICS 通信协议来映射、定位和攻击电网运行。该恶意软件按照设计的那样利用这些协议，以便规避检测。因此，ICS 安全团队的目标是，Antova 说，“以被动的方式提高可见性……这是我可以做的，只要不影响工程师的流程，他们将允许我这样做。”她说，这也能用最低投资获得最大的收益。

哈比比也敦促同样的做法。被动地评估环境中的所有组件，然后检查所有组件的漏洞，将该信息提供给操作员，并允许他们采取行动 (或不采取行动)。“如果你想修复那些损坏的窗户和门锁，”他说，“那就实施一个非常严格的变更管理流程吧。”

但是，布拉格警告说，要仔细测试产品，因为一些承诺“被动监控”的供应商比他们声称的被动性更被动。

由于 ICS 与安全流程和变更管理有关，因此，OT 和 IT 团队将有机会聚在一起。

原文名称	Look，But Don't Touch: One Key to Better ICS Security
作者简介	Sara Peters，Dark Reading 的高级编辑。
原文信息	2017 年 6 月 26 日发布于 Dark Reading，原文地址 http://www.darkreading.com/vulnerabilities---threats/look-but-dont-touch-one-key-to-better-ics-security--/d/d-id/1328987?
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《TeamSpy 家族样本分析报告》

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注意到，一种利用远程控制软件 TeamViewer 进行恶意操作的恶意代码 TeamSpy 使用针对性的垃圾邮件进行攻击。TeamViewer 是一种用于远程支持、远程管理、家庭办公在线协作和会议功能的软件。恶意软件 TeamSpy 是由远程访问工具 TeamViewer 和键盘记录器等组件组成。攻击者利用社会工程学诱骗受害者安装 TeamSpy，并通过 DLL 劫持技术进行隐藏，然后利用合法的远程访问工具 TeamViewer 执行未经授权的操作，从而从受害者的设备中窃取机密文档和密码。

TeamSpy 通过垃圾邮件传播，附件是一个带有恶意宏代码的 Office 文档，用户如果受骗上当点击启用宏，恶意代码就会感染计算机，这一切都会在后台运行，因此受害者不会发现任何攻击征兆。但如果安全人员来查看这些恶意宏，他们就可以看到经过混淆的字符串，这些经过修改的字符串通常会分割成一个或多个子串，这些子串最后又能被连接起来。该恶意宏会下载一个受密码保护的 Inno 安装程序。该程序包含恶意 DLL，它 hook 了多种 API 函数，可以阻止应用程序访问资源、隐藏 TeamViewer 界面、使 TeamViewer 以预定义的密码开始、阻止一些恶意软件创建不需要的对话框、监听传入消息，发送新消息或等待来自 C2 的回复。

受感染的计算机是通过 TeamViewer 控制的，攻击者可以连接到远程计算机，因为他们已经知道了 TeamViewer 的 ID 和密码。通过 TeamViewer 聊天的通信可以实现基本的后门功能：applist，wcmd，ver，os，vpn，locale，time，webcam，genid。

安天提醒广大网络使用者，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。目前，安天追影产品已经实现了对该类样本的检出。

木马程序

安天【追影威胁分析系统】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 (Win7) 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。

根据动态行为（默认环境）得出该文件具有以下行为：查找指定内核模块、创建特定窗体、打开自身进程文件、读取自身文件、查找特定窗体、释放 PE 文件、获取计算机名称、获取驱动器类型、请求加载驱动的权限、获取主机用户名称。

根据动态行为 (Win7) 得出该文件具有以下行为：查找指定内核模块、创建特定窗体、打开自身进程文件、读取自身文件、查找特定窗体、释放 PE 文件、获取驱动器类型、访问文件尾部。

文件名	08b9a556b239ba47c96a075ca71f7ee2
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	3.46 MB
MD5	08B9A556B239BA47C96A075CA71F7EE2
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Spy]/Win32.TeamSpy
判定依据	BD 静态分析

报告地址：https://antiy.pta.center/_lk/details.html?hash=08B9A556B239BA47C96A075CA71F7EE2

◆ 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、office2003、flash、wps、FoxitReader、adobe reader

◆ 其他行为

行为描述	危险等级	行为描述	危险等级
查找指定内核模块	★	创建特定窗体	★
打开自身进程文件	★	读取自身文件	★★
查找特定窗体	★	释放 PE 文件	★
获取计算机名称	★	获取驱动器类型	★
请求加载驱动的权限	★	获取主机用户名称	★

◆ 运行环境

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

行为描述	危险等级	行为描述	危险等级
查找指定内核模块	★	创建特定窗体	★
打开自身进程文件	★	读取自身文件	★★
查找特定窗体	★	释放 PE 文件	★
获取驱动器类型	★★	访问文件尾部	★