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 20 日 (总第 149 期) 试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天亮相 2018CNCERT 中国网络安全年会

2018 年 8 月 14 至 16 日，第 15 届中国网络安全年会在北京举行，安天技术负责人带来了题为《敌情想定下的网络安全防御思考》的演讲。同时，安天的追影威胁分析系统获“2018 网络安全创新产品(技术) ”奖。

本届年会以“荟聚安全大脑，护航智能生态”为主题，旨在交流国内外网络安全工作新趋势、新问题、新思路，促进国家公共互联网网络安全应急体系成员间的合作，加强互联网行业的网络安全保障和突发安全事件的应急处置联动，促进政府部门、重要信息系统单位与网络安全产业界间的交流，普及宣传网络安全及网络安全应急工作知识，提升社会网络安全意识。

安天作为“国家级网络安全应急服务支撑单位”，始终站在应急响应的第一线，与主管部门紧密合作，联合快速响应处置威胁。安天持续跟踪分析重大漏洞、恶意代码和 APT 组织的行动线索，发布多篇公开分析报告。在今年被曝光的英特尔处理器芯片存在严重安全漏洞事件中，安天第一时间向管理部门提交威胁通报，并立刻发布了 A 级漏洞风险通告。根据管理部门的要求，安天进行了深度分析验证和应对工作，发布了《处理器 A 级漏洞 Meltdown(熔毁) 和 Spectre(幽灵) 分析报告》。

在本届年会上，安天展台集中展示了安天的产品 / 服务体系，并在现场发放了以熔毁（Meltdown）和幽灵（Spectre）漏洞为专题的最新版安天技术文章汇编及富有安天特色的“2018 版威胁通缉令”扑克。

.Net 勒索软件 Shrug 被发现新变种 Shrug2

Quick Heal 安全实验室最近发现袭击受害者的机器并要求比特币支付 70 美元的赎金以解密文件的 Shrug2 勒索软件。Shrug2 作为在 7 月 6 日首次出现的内嵌虚假软件和游戏应用程序的 Shrug 的新版本，并携带了新功能 Shrug2 勒索软件使用 .NET 框架构建，使用 AES256 位密钥加密文件，能够加密 76 种文件格式，并通过感染载体网络钓鱼电子邮件，电子邮件附件，RDP，嵌入式超链接，感染驱动器和网站及下载进行分发。如果受害者机器连接到互联网，那么它就会检查系统是否已经通过检查注册表感染了 SHRUG2，如果系统没有被感染，那么它会在 HKCU 下新建注册表项 [ShrugTwo]，然后读取勒索软件感染机器的日期和时间，并根据此显示解密文件所需的时间。Shrug2 会删除系统还原点，并且授予对所有目录和子目录执行命令。SHRUG2 枚举文件并创建一个 [FilesToHarm] 列表来加密文件，[FilesToHarm] 是要加密的文件列表（仅限于感染机器的 C 盘），[HarmedFiles] 是已经加密过的文件列表（含路径），用于支付赎金后的解密或到时间未支付赎金，则会按图索骥，删除那些被加密的文件。

macOS 被暴露在通过鼠标点击的攻击中

原文链接：https://blogs.quickheal.com/new-net-ransomware-shrug2/

安全公司 Digita Security 的首席研究官 Patrick Wardle 在 Def Con 会议上分享了他发现的 macOS 中的 0day 漏洞。

该漏洞可突破最新 macOS，去年 10 月发布的 High Sierra 的安全措施——“用户辅助内核扩展加载”。该措施强制要求用户手动点击系统安全设置界面中的“允许”按钮来批准加载任何内核扩展，以阻止恶意软件利用合成的鼠标点击动作伪装用户的点击。

然而，High Sierra 操作系统误将连续两个合成的鼠标点击解释为鼠标的“按下”和“松开”事件。更糟糕的是，解释的结果还将该“按下”事件当作直接来自操作系统（而不是合成结果），因此不会被过滤掉。换言之，High Sierra 煞费苦心的设置，其实通过连续两个合成点击就可轻易突破。

该问题仅影响 High Sierra，因为它是使用操作系统版本实现 Apple 的用户辅助内核扩展加载。后续的 MacOS Mojave 版本中没有这一漏洞。

原文链接：https://securityaffairs.co/wordpress/75293/hacking/synthetic-mouse-click-attack.html

每周安全事件

类 型	内 容
中文标题	Instagram 用户被黑客进行了广泛攻击
英文标题	Widespread Instagram Hack Locking Users Out of Their Accounts
作者及单位	Mohit Kumar
内容概述	近日，Instagram 受到了广泛的黑客攻击活动的打击，并在过去一周影响了数百名用户，使其账户被锁定，并将电子邮件地址更改为 .ru 的域名。受害者称黑客在攻击中更改了他们的帐户名称、个人资料图片、密码、相关联的电子邮件地址和连接的 Facebook 帐户。黑客还入侵了启用双因素身份验证（2FA）的用户。目前还不清楚 Instagram 账户被广泛攻击的组织和原因，但从使用来自俄罗斯电子邮件提供商 mail.ru 的电子邮件地址，表明攻击者可能是俄罗斯人或相关黑客组织，也不排除有人利用俄罗斯邮件服务商进行身份仿冒。
链接地址	https://thehackernews.com/2018/08/hack-instagram-accounts.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		名称与发现时间	相关描述
移动恶意代码	新出现的样本家族	Tool/Android.xiaoxiyl.a[exp] 2018-08-13	该应用程序是一款工具合集，包含刷赞、视频 vip 账号共享、免流、短信轰炸等工具，还有黑客工具教程及其下载链接等，具有一定的风险性，请谨慎使用。（威胁等级高）
		Trojan/Android.FakeMessage.a[prv] 2018-08-15	该应用程序伪装正常应用，运行隐藏图标，后台获取位置信息、固件信息、信箱信息，上传到远程服务器，造成用户隐私泄露，建议卸载。（威胁等级中）
		Tool/Android.HVRRecorder.a[sys,rmt] 2018-08-16	该应用程序是一款监控工具，可以通过短信远程控制设备录音开启或关闭，请谨慎使用。（威胁等级中）
	较为活跃的样本	Trojan/Android.apiempello.c[prv,exp,rog]	该应用程序伪装正常应用，运行诱导激活设备管理器，隐藏图标，私自上传用户邮件地址、电话号码和手机固件信息，私自下载子包和未知应用，造成用户隐私泄露和财产损失，建议卸载。（威胁等级高）
		Trojan/Android.HiddenAds.fa[exp,rog]	该应用程序运行后隐藏图标，私自下载其他应用，后台推送广告，造成用户资费损耗，建议卸载。（威胁等级中）
		rojan/Android.Joyreach.h[exp]	该应用程序运行动态释放恶意子包，推送广告，静默下载，造成用户资费损耗，建议卸载。（威胁等级中）
		Trojan/Android.Locker.at[rog,lck]	该应用程序为勒索软件，运行后置顶自身界面，要求用户扫描二维码付费解锁，造成用户手机无法正常使用，建议卸载。（威胁等级中）
		G-Ware/Android.StealMoneyGame.bp[pay,rog]	该应用程序是游戏应用，运行弹出订购提示框，付费信息不明显，内嵌恶意支付插件，监听短信拦截指定短信，私自回复短信，会造成用户资费损耗，建议卸载。（威胁等级低）
		G-Ware/Android.FakeWzry.f[fra]	该应用程序伪装王者荣耀外挂，本身无实际功能，欺诈诱导用户付费，可能造成用户资费损失，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	Oracle 数据库服务器 Java 虚拟机漏洞（CVE-2018-3110）	CVE-2018-3110 影响 Oracle 数据库 Windows 版 11.2.0.4 与 12.2.0.1，同时对全平台 12.1.0.2 且未应用 2018 年 7 月 CPU 的版本也会产生影响。除此之外，老版本很可能均会受到其影响。此漏洞会被攻击者利用通过 Oracle Net 攻击 Java 虚拟机，虽然此漏洞存在于 Java 虚拟机中，但可被利用来攻击其他的产品与服务。攻击者攻击成功后可接管整个 Java 虚拟机。（威胁等级高）
	较为活跃样本	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。该病毒利用各种途径，使黑客获得数字证书来伪造文件。该家族还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）
		Trojan[Backdoor]/Win32.AutoIt	此威胁是一种后门类木马程序，该家族通过 Autolt 编写。样本运行后会连接远程服务器，等待接收上传下载文件、监视用户屏幕、记录键盘击键、查看进程和窗口等控制指令。（威胁等级高）
		Trojan[Dropper]/Win32.Injector	此威胁是一种带有捆绑行为的木马类程序。该家族会在被感染的电脑中安装被压缩的恶意软件，并为黑客打开后门。该家族通过用户在成人网站或共享网站上下载的编解码器和 ActiveX 更新来感染电脑。该家族进入系统后隐身运行，并会弹出恶意弹窗。（威胁等级中）
		Trojan[Rootkit]/Win32.Crypt	此威胁是一类可以窃取用户信息的木马家族。该家族样本运行后可以下载并执行其他文件，连接远程服务器发送自身信息，关闭系统防火墙，有一定威胁。（威胁等级高）

了解你的对手：如何创建成功的“威胁猎杀”计划

Jan Dyment / 文　安天技术公益翻译组 / 译

高级威胁可以在长达数月的时间里规避检测——它们在网络中驻留的时间越长，造成的损害就越大。IBM 公司《2018 年威胁猎杀报告》显示，检测高级、未知和新兴威胁是当今安全运营中心（SOC）面临的最大挑战。

“威胁猎杀”（threat hunting）利用机器分析和以人为主导的情报分析，在损害造成之前主动搜索和发现威胁。尽管威胁猎杀势头越来越强劲，但它仍然是一门尚未被充分理解的新兴学科。

“威胁猎手”训练营

新的 IBM“网空威胁猎杀训练营”（Cyber Threat Hunting Bootcamp）旨在改变这种状况。该项目致力于培训 SOC 和融合中心领导者，帮助他们创建威胁猎杀计划，利用威胁猎杀理论、手段和技术来对抗他们每日都要面对的高级攻击。（译者注：为与文中 network[网络] 相区分，我们将文中的 cyber 译为“网空”。）

该项目基于 IBM Security 的威胁猎杀解决方案 i2，由 i2 团队的高级威胁猎手和解决方案架构师保罗·奥尔蒂斯（Paul Ortiz），以及“更安全的星球计划”网空专家希德·珀尔（Sid Pearl）牵头。

奥尔蒂斯拥有超过 16 年的专业经验，曾担任美国情报界和国防部的高级情报分析师。他拥有广泛的知识，擅长使用各种技术分析工具和数据集、先进的网空技术以及众多信号情报收集和分析系统。

珀尔拥有广泛的网空情报知识，目前担任国际认证信息共享与分析组织（ISAO）协会的首席信息安全官（CISO），致力于保护美

国国家安全和关键基础设施的利益。此前，他曾担任 Unisys 公司全球安全和网空情报总监。珀尔还曾供职美国海军长达 20 年，参与了多起特种作战，包括联合特种部队的作战通信和情报作战。

情报周期

情报周期——包括收集需求、采集数据、分析信息和报告结论四个阶段——是一种经过时间考验的方法，用于在战场上猎杀敌人，也可用于在网络中猎杀攻击者。威胁猎杀是人与人之间的对抗，因此了解对手至关重要。这意味着，你要了解谁在攻击你，他们试图做什么，以及他们是如何做的。情报周期提供了一个系统的过程，用于提出和回答上述问题。

威胁信息来自各种内外部数据源，包括网空和非网空数据源。将网络和系统信息与威胁情报（包括反馈信息、报告、开源情报 [OSINT] 和暗网数据）融合在一起，可以全面了解组织面临的内外部威胁。

创建威胁猎杀平台和计划

威胁猎杀平台的关键组成部分，包括查找网空威胁所需的数据和工具。安全信息和事件管理（SIEM）系统提供关键的内部安全数据，外部威胁情报则帮助你了解可能影响组织的网空威胁活动的已知信标。借助统计分析工具，威胁猎手可以执行机器分析和异常检测，以发现高级威胁源的隐蔽方法。借助情报分析工具，威胁猎手可以收集和整理来自整个平台的数据，以发现和分析威胁。

一旦平台建成，SOC 或融合中心应制定策略并确定实施该策略所需的资源。然后，他们应针对这些要求执行差距分析，确定弥补这些差距所需的数据和工具。接下来，SOC 领导者应创建团队和标准操作规程（SOP）。最后，通过培训、系统优化和持续计划评估来实施该策略。

将事件分析的时间从几小时缩短到几秒

SOC 和融合中心分析师面临的主要挑战包括：海量数据、数据的快速增长以及难以区分误报和真实威胁。为了应对这些问题，SOC 团队必须将看似无关的低级别事件关联起来，它们被关联起来以后，可能会指示高级威胁的线索。如果没有威胁猎杀工具和技术，就需要分析师手动关联，这会非常繁琐。一家美国银行的案例显示，使用可视化分析工具，关联低级别事件的时间可以从几小时缩短到几秒。

威胁猎杀实践

为了使威胁猎杀理论和工具发挥作用，IBM 开发了一个“动手”实验室，教导参与者利用 i2 和其他工具来搜索和发现隐藏在噪声中的网空威胁。

该训练营的网空专家指出，好的威胁猎手对信息技术、网络和威胁全景（包括对手的战术、技术和规程 [TTP]）有着深刻的理解。此外，拥有威胁情报收集和分析经验也是一个优势。

原文名称	Know Your Enemy: How to Build a Successful Threat Hunting Program
作者简介	Jan Dyment。Jan Dyment 是 IBM Security 公司 i2 威胁猎杀产品营销经理。
原文信息	2018 年 8 月 10 日发布于 Security Intelligence 原文地址 https://securityintelligence.com/know-your-enemy-how-to-build-a-successful-threat-hunting-program/
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《ORCUS 远控木马分析报告》

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 Orcus 的恶意代码。该木马样本可以感染 Windows 操作系统，感染后攻击者可以完全控制受害者的电脑。2015 年 10 月，开发者先将样本以“Sorzus”命名并在黑客论坛上开源发布，之后将其命名为“Orcus”并进行商业化出售，出售价格 40 美元。

Orcus 木马有以下功能：远程执行代码、键盘记录、麦克风录音、远程管理、反向代理、拒绝服务、窃取密码、禁用网络摄像头指示灯、摄像头监控、截取屏幕、信息回传、插件系统等。Orcus 不仅有远控木马的共性，还有其它远控木马不具备的特点。例如“插件系统”功能，该插件系统功能允许 Orcus 用户创建自己的插件或下载已经由开发者开发的插件。Orcus 远控木马会将窃取到的受害者信息，回传到其指定的服务器上。服务器上的信息可供该木马的众多使用者共享，以达到管理受害者网络的目的，并通过部署多个服务器来实现其可扩展性。该木马的使用者可以通过控制器工具访问存有窃取到信息的服务器以及受害者的电脑，其控制器不仅有 Windows 版本也有 Android 版本。

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、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、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、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、智能学习鉴定器将文件判定为木马程序。

概要信息

文件名	E887D9443E2022E27A57A944907D0503
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	658 KB
MD5	E887D9443E2022E27A57A944907D0503
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[:HEUR]/Win32.AGeneric
判定依据	静态分析

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=E887D9443E2022E27A57A944907D0503

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、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
疑似键盘记录器	★★★	疑似键盘记录	★★★

常见行为

读取自身文件	★★
创建特定窗体	★
释放 PE 文件	★
获取驱动器类型	★
获取系统内存	★★
独占打开文件	★
打开自身进程文件	★
获取 CPU 信息	★★

文件扫描

文件名	文件 MD5	家族相似性	yara 扫描
target.exe	e887d9443e2022e27a57a944907d0503	N/A	N/A
target.exe.dmp	d41d8cd98f00b204e9800998ecf8427e	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	192.168.122.97	68
192.168.122.97	137	192.168.122.255	137
.....	.....	.....	.....