安天周观察

安天官方微博　安天官方微信

主办：安天　2017 年 12 月 11 日（总第 115 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天移动安全出席 2017 泰尔论坛并发表演讲

2017 年 12 月 4 日 -5 日，由中国信息通信研究院泰尔终端实验室（CTTL-T）与电信终端产业协会（TAF）联合主办的“2017 泰尔论坛”在北京举行，论坛以“智能·互联”为主题，聚焦移动互联网和人工智能在电信终端产业的应用和技术发展，以物联网、测试认证、信息安全为核心，搭建信息通信全产业链沟通交流的平台。安天移动安全公司出席本次论坛，总经理潘宣辰发表演讲。

5 日，在由泰尔终端实验室（CTTL-T）、电信终端产业协会（TAF）与移动安全联盟（MSA）联合主办的泰尔信息安全分论坛上，安天移动安全总经理潘宣辰发表“移动威胁态势和多边安全合作分享”主题报告，报告从移动威胁的态和势的角度对移动生态的威胁现状和演变趋势进行了剖析，并结合安天移动安全在移动互联网全产业链的合作实践，从安全对抗和产业两个角度进行了安全价值思考和分享。报告不仅对当前比较严峻的恶意代码精细化威胁和不良应用带来的泛安全威胁进行了分享，而且对人工智能时代和移动互联网在未来发展中即将面临的重大的数据和隐私安全进行了前瞻性的分享。希望能通过产业界各方的通力合作形成安全合力，保障产业发展，号召大家“看见树木也看见森林”。

作为国内移动安全响应体系的重要节点，安天移动安全始终致力于为监管部门、政企客户、终端厂商提供最佳的移动安全技术支撑和产品服务。早在去年 6 月，安天移动安全与中国泰尔实验室签署战略合作框架协议，双方在预置应用安全检测、移动漏洞检测分析、移动生态链安全监测等方面达成了紧密合作，并进一步将合作范围扩大到移动信息安全技术、标准建设、业务拓展、客户服务等方面。此外，安天移动安全作为 TAF 信息安全组副主席单位，于今年 6 月成功承办电信终端产业协会信息安全工作组（TAF WG4）2017 年度第二次工作组会议暨技术交流会，并于近日当选移动安全联盟理事单位，与相关监管机构、协会联盟等协力推进移动互联网信息安全领域的交流、合作与发展。

安天移动安全将以世界领先的移动反病毒技术和能力为基础，凭借与国家互联网应急响应中心、泰尔终端实验室等国家监管部门以及高通等国内外近百家知名厂商的合作经验，携手移动互联网产业链各方，积极打造移动智能终端安全技术沟通、标准讨论的平台，共同提升整个产业的安全防护能力，推动移动智能终端生态环境净化，共筑移动安全生态！

哈尔滨实验小学师生参观安天

12 月 1 日，来自哈尔滨实验小学的同学们在老师的带领下来到安天进行参观学习，这是迄今为止安天迎来的年龄最小的一批参观者。

为便于同学们理解，负责讲解的同事从安天的产品覆盖、地理布局、主营业务及创业经历四个方面进行了介绍。在了解了安天的工作后，同学们对病毒的来源、监控及应对产生了浓厚的兴趣，同时对网络安全行业有了一定的认识与了解。

在互动过程中，同学们发现自己所使用的手机大部分都内置了安天的威胁检测引擎。当发现原以为距离自己十分遥远的手机引擎，就来自现在所参观的公司时，同学们表示非常激动，同时对参与研发的工程师叔叔阿姨们表示十分钦佩。

参观的最后，同学们围在安天创业历程墙前，被安天创业前期的艰苦环境深深震撼，并表示，定会继续认真学习，在未来成为像叔叔阿姨一样对国家和社会有用的人。

每周安全事件

类 型	内 容
中文标题	StorageCrypt 勒索软件是最后一个利用 SambaCry 来定位 NAS 设备的恶意软件
英文标题	The StorageCrypt ransomware is the last malware in order of time exploiting SambaCry to target NAS Devices
作者及单位	Pierluigi Paganini; SecurityAffairs
内容概述	专家们发现了一个利用 SambaCry 漏洞（CVE-2017-7494）的新型恶意软件，它被称为 StorageCrypt Ransomware，因为它通过 SambaCry Exploit 来攻击 NAS 设备。 专家们发现，该恶意软件利用了 Linux Samba 漏洞，又名 SambaCry，在 5 月份进行了修补。 Samba 错误似乎是一个网络可疑的问题，可以被恶意代码利用，从脆弱的机器自我复制到易受攻击的机器，而无需用户的交互。 在六月份，卡巴斯基实验室的研究人员设立了蜜罐来检测 SambaCry 在野外的攻击。 根据 Lawrence Abrams 的说法，StorageCrypt Ransomware 依靠执行命令来下载名为 sambacry 的文件，将其作为 apache 存储在 /tmp 文件夹中，然后执行。 一旦勒索软件感染了一个设备，它会加密这些文件，并通过给它们添加 .locked 扩展名来重命名它们。
链接地址	http://securityaffairs.co/wordpress/66401/malware/storagecrypt-ransomware-sambacry.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 4 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.EvilInvisible.a[exp,rog] 2017-12-04	该应用程序包含恶意第三方插件，运行后通过 WebView 加载 HTML 页面，并模拟点击私自加载恶意脚本，恶意脚本会后台静默安装软件，模拟点击广告，模拟 googleplay 等恶意刷量行为。造成用户流量消耗，请立即卸载。（威胁等级高）
		Trojan/Android.Tizi.a[prv,bkd,spy] 2017-12-06	该应用程序包含恶意代码，私自建立远控后门，获取手机漏洞信息，上传用户手机基本信息和固件信息，下载 busybox 工具进行提权。造成用户隐私泄露，危害用户手机安全。请立即删除。（威胁等级中）
		Trojan/Android.ColdJewel.a[prv,exp,rmt] 2017-12-06	该应用程序包含恶意代码，安装后自启动，后台接收远程控制命令，私自窃取用户手机 version、androidUuid、apiKey、appId、operator 等各项基本信息，加载脚本，模拟点击广告，执行 shell 命令，下载其他软件，并 hook 用户手机。造成用户隐私泄露和流量消耗，危害用户手机安全。请立即删除。（威胁等级高）
		RiskWare/Android.APKIL.a[exp] 2017-12-06	该应用程序是一个测试程序，运行无提示拨号、发送短信，具有一定的风险性，请谨慎使用。（威胁等级中）
		RiskWare/Android.QQshare.a[exp] 2017-12-08	该应用程序运行访问指定网址，跳转加入指定 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，请谨慎使用。（威胁等级中）
		RiskWare/Android.liuxrepack.a[fra,rog] 2017-12-08	该应用程序经过重打包处理，非官方程序，植入了广告，建议不要使用。（威胁等级中）
	较为活跃的样本	Trojan/Android.Socksbot.c[rmt,prv]	该应用程序伪装成正常应用，运行后加载恶意子包，接收远程服务器发送的指令与远控服务器通过 socket 进行通讯，远控端可使用户设备变成 SOCKS 代理，这样远控端可通过用户设备访问设备所属内部网络从而窃取用户内网的隐私信息，造成用户隐私泄露，建议卸载。（威胁等级高）
		Trojan/Android.SpyPhone.f[prv,spy]	该应用程序是一款间谍软件，运行后窃取用户短信、联系人、通话记录、通话录音、浏览器记录、WhatsApp 记录等隐私信息，造成用户隐私泄露，建议卸载。（威胁等级高）
		Trojan/Android.BankerSpy.c[prv,rmt,spy]	该应用程序启动后隐藏图标，通过界面劫持强制用户激活设备管理器，窃取用户短信、联系人、通话记录等隐私信息，还会进行拦截短信，发送短信等危险行为，造成用户隐私泄露，建议卸载。（威胁等级中）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Adobe Flash 任意命令执行漏洞（CVE - 2017 - 11292)	Adobe 发布了 Windows, Macintosh, Linux 以及 Chrome OS 多个平台下的 Adobe Flash Player 安全升级补丁，更新修复了一个由于类型混淆漏洞导致的远程代码执行。Adobe 官方注意到了 CVE-2017-11292 曾经有一段在野时期，被利用于有针对性的攻击 Windows 用户。（威胁等级高）
	较为活跃样本	Trojan[Downloader]/JS.Nemucod	此威胁来自可以下载恶意代码的木马家族。该家族样本是 js 脚本，运行后连接远程服务器下载恶意代码并执行，可能会窃取用户信息，有一定威胁。（威胁等级中）
		Trojan[Backdoor]/Win32.Qakbot	此威胁来自一类可以窃取用户信息的木马家族。该家族样本运行后连接远程服务器接受攻击者恶意操作，包括文件管理，进程查看等。（威胁等级中）
		Trojan[DDoS]/Linux.Ddostf	此威胁来自一类针对 Linux 平台的具有 DDoS 功能的木马家族。该家族样本运行后连接远程服务器，向其发送系统敏感信息。它可以接收远程服务器的命令并执行 DDoS 攻击，包括 TCP、UDP 及 HTTP 的洪水攻击。（威胁等级中）

2018 年网络安全预测

Adam Meyer / 文　安天技术公益翻译组 / 译

又到了我们回顾过去一年并展望未来一年威胁状况的时候。我花了大部分时间来分析大量的数据、寻找威胁趋势并创建威胁情报，希望能够为客户提供重要的见解，帮助他们更好地应对即将到来的网络威胁。为了这一愿景，我将对 2018 年的网络安全情况进行预测。

1. 2018 年，个人和组织将会付出惨痛的代价，认识到个人信息不应该被用作身份验证信息。

尽管大多数组织长期以来对个人信息（identifier）和身份验证信息（authenticator）两个概念比较模糊，但是两者之间存在着重要的区别。个人信息可以是诸如社保号、驾照号甚至地址之类的信息。身份验证信息可以是一个问题，当被正确回答时，能够证明你就是本人。基于知识的验证包括一系列问题，如你的高中吉祥物是什么？你的第一辆车是什么牌子？或者，这些验证可以基于信用报告数据和许多其他信息，相对于成本更高但更安全的验证方法（如双因素认证 /2FA）来说，这些验证成本较低。

不幸的是，太多的组织将个人信息用作了身份验证信息，导致诸如 Equifax 这样的大规模数据泄露事件屡屡发生，在 2018 年这会带来更加严重的问题。Equifax 存储了数百万客户的个人身份信息（PII），这些信息被攻击者窃取，导致每个人的身份信息都面临被滥用的风险，特别是在那些将个人信息用作验证信息的组织中。举例来说，你打电话给银行，他们要求你提供社保号后四位、姓名、出生日期等 ..... 所有这些都是个人信息，而不是验证信息。Equifax 事件发生后，有多少黑客得到了这数百万客户的个人信息呢？在 2018 年，

个人和组织将会再次以惨痛的代价认识到这一点。要解决这一问题，最重要的是让组织停止将个人信息用作验证信息。

2. 2018 年，伙伴关系、供应链和即服务（as-a-service）关系将会引发更多的泄露事件。

业务越来越数字化，精明的组织正在通过伙伴关系、供应链集成和即服务功能扩展其业务范围并为客户提供便利。虽然这种广泛的外包正在成为日益流行的业务加速方法，但它也可能是一个危害安全的噩梦。在 2017 年，德勤（Deloitte）和博思艾伦（Booz Allen）都在这方面栽了跟头。明年，我们将会看到更多由于合作伙伴网络攻击引发的数据泄露事件。

在合作中，组织共享数据和品牌声誉。公司应该开发网络安全最佳实践，并要求所有伙伴遵守；应根据适用的监管要求拟定书面合同，在合同达成和 / 或续订之前，应限制与合作伙伴的业务范围。不幸的是，这可能会给采购部门带来难题。由于这些最佳实践可能会影响预算，以满足新的要求并加以执行，因此组织需要在明年建立这一要求并相应地管理成本。

3. 2018 年，小型医疗机构将成为勒索软件攻击的首选目标。

勒索软件将继续作为全球黑客的一条业务线，但是其攻击目标将会更加有侧重性：防御措施不够完善的中小企业。因此，赎金金额可能会比较低，以便较小的组织有能力支付。明年，地区诊所和医院将会成为重灾区，这主要是因为很多黑客认为它们易于攻击。以最少的投入获取最高的回报是这些“商人”所追求的目标。

4. 组织会将泄露响应的优先级排在事件响应之前。

在公司认真对待数据泄露之前，我们还要收到多少来自 CEO 的道歉信呢？随着网络安全在各地的董事会会议上成为优先处理事项，组织意识到这不仅仅是一个技术问题。这是一个组织的优先事项，虽然公司肯定会有失误，但我们将会看到更好的泄露响应计划。

事件响应是 IT 运营和安全工作，旨在防止安全事件并在事件发生后进行补救。泄露响应远不止于此——它涉及整个企业如何应对影响客户数据的泄露事件，涵盖从受补救成本影响的底线数字到未来公司声誉的所有内容。泄露响应包括首席执行官、董事会、法律部门、市场营销和公关团队等的行为。

5. 机器学习技术作为一种能力将会更加清晰和成熟。

机器学习是一个流行词，对每个人来说它的意思都有些微不同，但是我认为在 2018 年这种能力将会变得更加清晰。机器学习技术的目的是减轻人们的负担，提高处理和理解大量数据的速度。安全技术不断进步，我们将会看到更好、更高质量的数据。我们正在改进数据处理，届时创建更智能的人类响应将成为可能。在 2018 年，机器学习或自动化将会继续改善，威胁情报数据的质量也将不断提高。将机器学习威胁情报功能与可以提供分析、见解和建议的人类专家相结合将是两全其美的选择。

原文名称	Analyst Perspective: 2018 Cybersecurity Forecast
作者简介	Adam Meyer 是 SurfWatch Labs 首席安全策略师。他曾在防御、技术和关键基础设施领域担任领导职务超过 15 年。
原文信息	2017 年 12 月 1 日发布于 SecurityWeek 原文地址 http://www.securityweek.com/analyst-perspective-2018-cybersecurity-forecast
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《Locky 勒索软件 asasin 变种分析报告》

近日，安天 CERT（安全研究与应急处理中心）拦截到一款名为“Discord Canary”的后门，该恶意代码功能丰富，执行后会关闭附件执行服务 (Attachment Execution Services,AES) 的安全检查，设置 Windows 防火墙对其流量放行，创建互斥量，开机自启，上传用户计算机系统盘序列号、计算机名、用户名、操作系统完整名称和发行版本、CPU 架构、摄像头信息、当前最前台窗口标题等特征信息，以微小的内存隐藏自身，进程被杀死后会蓝屏。

恶意代码样本在启动时检查是否带有参数，成功则会添加注册表项，然后获取当前进程可执行文件相对路径，比较是否为 "%TEMP%\Discord Canary.exe"。不是则检查文件 "%TEMP%\Discord Canary.exe" 是否已存在，存在则删除。然后复制当前进程可执行文件到 "%TEMP%\Discord Canary.exe"，并启动 "%TEMP%\Discord Canary.exe"。然后，增加全局环境变量 SEE_MASK_NOZONECHECKS，设置值为 1，以关闭附件执行服务（Attachment Execution Services，AES）的安全检查，执行 CMD 命令 "netsh firewall add allowedprogram "%TEMP%\Discord Canary.exe""Discord Canary.exe"，

设置 windows 防火墙对 Discord Canary.exe 流量放行。样本会获取系统盘序列号、计算机名、用户名、进程对应可执行文件最后修改时间、操作系统完整名称和发行版本号、程序文件夹，还会检查驱动程序判断是否存在摄像头，最后将数据发送至 C&C 主机“oskarrr1.hopto.org:1177”，而且还会根据不同的指令执行相应的恶意操作。

安天 CERT 提醒广大网络使用者，要提高网络安全意识，在日常工作中要保持杀毒软件常开，及时安装系统更新和漏洞修复，收发邮件时要确认收发来源是否可靠，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，不要随意下载非正版的应用软件、非官方游戏、注册机等。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的好习惯。

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 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。

最终依据静态行为鉴定器智能学习鉴定器将文件判定为木马程序。

根据页面手工提交得出该文件具有以下行为：延时、增加防火墙设置、疑似键盘记录、获取系统内存、打开自身进程文件、查找指定内核模块、创建特定窗体、获取驱动器类型、读取自身文件、释放 PE 文件、获取计算机名称、请求加载驱动的权限、获取主机用户名称、独占打开文件、增加 run 自启动项、复制自身文件、设置调试器权限、自启动

文件名	DISCORD CANARY.EXE.malw
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	69 KB
MD5	F593BB5987F8552EDE870B592283A880
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Backdoor]/MSIL.Bladabindi.p
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	行为描述	危险等级
增加防火墙设置	★★★	延时	★★★

◆ 常见行为

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

◆ 进程监控

PID		命令行
1920	wuauclt.exe	"C:\WINDOWS\system-32\wuauclt.exe" /RunStoreAs-ComServer Local\[3e0]SUSDSf24dc08108a93d40942c694ef24ebda6
.....	.....	.....