安天周观察

主办：安天　2017 年 4 月 24 日（总第 84 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

“4·19”安天人的周年记忆

2016 年 4 月 19 日，习近平总书记主持召开网络安全和信息化工作座谈会。安天创始人、首席技术架构师肖新光（安天内部称他为 Seak）作为网络安全界的代表第二个发言，向习总书记汇报。习近平总书记的重要讲话，不仅提出了工作要求，更为我们提供了理念指导——“树立正确的网络安全观。理念决定行动”。

安天人在“4·19”一周年之际，重启“4·19”记忆，从理念和实践两方面深刻思考和回顾一年来在核心技术、产品服务等方面的努力，以习近平总书记的讲话为指导，提高自身能力，树立正确认识。

风正帆悬破浪行

2016 年 4 月 19 日，习近平总书记主持召开网络安全和信息化工作座谈会。安天创始人、首席技术架构师肖新光（安天内部称他为 Seak）作为网络安全行业发言人第二个向习近平总书记进行汇报发言。

次日，公司召开员工大会，学习传达“网络安全和信息化工作座谈会”有关精神，他们为自己选择了网络安全这个行业感到骄傲和自豪。

Seak 说：“这次我作为发言代表，并不是因为安天做出了什么成绩，只是因为网络安全当前面临很多困难和问题，需要有人来向总书记做出汇报，多位专家、院士、企业家经过反复讨论，形成了汇报意见，我只是有幸成为了这个代表而已。”

凝聚“三心”思既往

当总书记讲到“核心技术要取得突破，就要有决心、恒心、重心”的时候，作为一个长期坚持核心技术自主研发的团队负责人，Seak 内心涌动着深深的共鸣。在安天研发线的学习研讨中，“决心、恒心、重心”被频频提及。

Seak 和安天工程师们永远难忘安天 17 年发展历程中多次从弹尽粮绝中站起来的情景，他们始终坚持核心技术研发。

踏梦征程齐发力

从后台转型前台，为政企客户提供安全产品和服务，是安天的第三次创业。伴随这次创业的，是与安天有着同样的梦想和情怀志同道合的战士，是筚路蓝缕一步步扎实前行的征程。

2015 年 8 月，安天商务总监胡双蕾决定放弃个人创业、加入安天的第三次创业之旅时，却惊讶地发现她竟然是安天销售部的第一名员工。2016 年，前华为企业安全副总裁胡忠华正式加盟安天，担任安天总裁。如今，安天的研发体系规模继续成长，工程师团队突破 500 人，成为国内威胁检测最大的团队之一。安天销服体系已超过 100 人，在区域及近 10 个价值行业构建了组织，树立了样板。

欲登绝顶莫辞劳

激动、兴奋、欢呼、雀跃，绝不会仅仅停留在 2016 年 4 月 19 日。

安天，作为坚持奋战在与威胁对抗一线的能力型安全厂商，在开启面向企业安全市场领域的新创业征程中，需要更努力，更高效、更扎实的工作，以更大的决心、更久的恒心、更准的重心，为网信事业的发展奉献热血和力量。

本文节选自安天公众号“安天（antiylab）”发布的文章《“419”安天人的周年记忆》。

“4·19”一周年，部分媒体对安天负责人的采访和文章刊登

媒体报告	内容
CCTV 中国中央电视台	2017 年 4 月 19 日 焦点访谈：如何让网更能 更强 更安
CCTV 央视网 .com	2017 年 4 月 20 日 网事·国事·天下事：您的网络安全吗？“4·19”参会专家为你解密
光明日报	2017 年 4 月 20 日 安天技术负责人在第 4 版刊登署名文章《努力实现网络安全核心技术的有效突破》
光明网 GMW.CN	2017 年 4 月 19 日 安天技术负责人在理论频道发表署名文章《网络安全发展需要理念与技术并行》 2017 年 4 月 19 日 时政频道和客户端刊记者特稿《谱写网络强国新篇章下好“网络安全”这盘关乎全局的大棋》、《突破核心技术“命门”谱写网络强国新篇章》
中国网 China.org.cn China.com.cn	2017 年 4 月 18 日 Features：Interconnected world requires enhanced cyber security

每周安全事件

类 型	内 容
中文标题	洲际酒店集团二度遭遇信用卡数据泄露，超过 1,000 家酒店受影响
英文标题	InterContinental Hotels Group，the international hotel chain confirmed a second credit card breach
作者及单位	Pierluigi Paganini；Security Affairs
内容概述	近日，洲际酒店集团在官网上发布一则通告，告知客户 2016 年 9 月 29 日至 12 月 29 日期间，多家酒店再度发生信用卡数据泄露。 据通告内容显示，支付卡网络告知 IHG 在美洲运营的旗下连锁酒店，客户在这些地点合法使用信用卡之后，出现了一些未经授权的收费。酒店方面已经雇佣了一家顶级网络安全企业调查美洲地区连锁酒店的支付卡处理系统。 客户在受影响酒店进行信用卡支付后，该恶意程序从信用卡磁条中读取记录数据，包括信用卡号码、有效期、内部验证码，有些情况下还包括持卡人姓名。除此之外，酒店表示其他信息并未受到影响。
链接地址	http://securityaffairs.co/wordpress/58129/data-breach/intercontinental-hotels-group-breach.html

每周值得关注的恶意代码信息

经安天检测分析，本周有 8 个移动平台恶意代码和 5 个 PC 平台的恶意代码值得关注

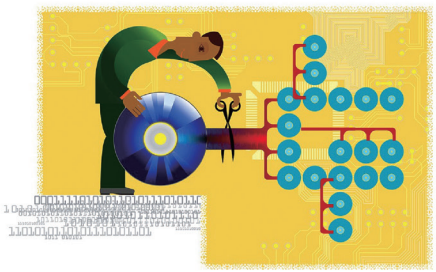
平台分类	关注方面	名称	相关描述
移动恶意代码	新出现的样本家族	Trojan/Android.intelwd.a[prv，rog]2017-04-18	该应用程序运行会请求激活设备管理器，连网上传设备固件信息和位置信息，锁定用户手机，私自下载更新，造成用户隐私泄露和资费消耗。（威胁等级中）
		G-Ware/Android.Zigyfdeb.a[exp，rog]2017-04-18	该应用程序伪装系统应用，运行后隐藏图标，私自推送广告，后台加载恶意子包发送、拦截、删除短信，连网下载恶意应用，造成用户资费损耗，影响正常使用。（威胁等级低）
	较为活跃的样本	Trojan/Android.InfoStealer.ac[prv，rmt]	该应用程序伪装成系统应用，程序运行会隐藏图标，连网获取指令根据指令上传用户短信、通讯录和通话记录、文件等隐私信息，造成用户隐私泄露。（威胁等级中）
		Trojan/Android.FakeApp.ee[exp，rog]	该应用程序伪装成正常应用，运行后加载弹窗诱导点击，并会发送付费短信，下载其他应用，后台拦截短信，上传短信运行结果，造成用户资费损耗，建议卸载。（威胁等级中）
		Trojan/Android.emial.fd[prv，exp]	该应用程序伪装成正常应用，运行会隐藏图标，激活设备管理器。跳转钓鱼界面，诱导用户输入银行账户，相关隐私会通过短信转发，后台窃取用户收件箱短信，造成用户隐私泄露，建议立即卸载。（威胁等级高）
		Trojan/Android.QQspy.bb[prv]	该应用程序伪装成 QQ 类相关应用，诱骗用户输入帐号密码并上传，造成用户隐私泄露。（威胁等级中）
		Trojan/Android.Hqwar.d[prv，exp，rmt]	该应用程序启动会隐藏图标，不断请求激活设备管理器，上传设备 ID、手机号等。会获取远程指令上传联系人信息，发送短信到指定号码。造成用户隐私泄露和资费消耗，建议立即卸载。（威胁等级中）
		Trojan/Android.Slocker.e[rmt，prv，exp]	该应用程序运行后会激活设备管理器，隐藏图标，后台接收远程控制指令，配合释放的子包获取用户联系人、地理位置、短信和程序列表等信息并上传；同时有删除短信、联系人，插入短信等行为；加载虚假银行弹窗诱导用户输入银行卡信息，造成用户隐私泄露和资费损耗，更会给用户带来经济损失，建议立即卸载。（威胁等级高）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	多个 Windows SMB 远程执行代码漏洞(MS17-010)(CVE-2017-0143\CVE-2017-0144\CVE-2017-0145\CVE-2017-0146\CVE-2017-0148)	当 Microsoft 服务器消息块 1.0(SMBv1) 服务器处理某些请求时，存在多个远程执行代码漏洞。成功利用这些漏洞则可以获取在目标系统上执行代码的权力。为了利用此漏洞，在多数情况下，未经身份验证的攻击者会向目标 SMBv1 服务器发送经特殊设计的数据包。（威胁等级高）
	较为活跃的样本	Trojan[Ransom]/Win32.SageCrypt	此威胁是一种可以加密用户文件勒索赎金的木马程序。该家族样本会加密特定后缀的文件并在文件名最后加上 .sage，向用户勒索比特币。（威胁等级中）
		Trojan[Spy]/Win32.Orcus	此威胁是一种可以监视用户系统的木马程序。该家族样本运行后连接远程服务器，记录用户系统信息并回传给攻击者。（威胁等级中）
		Trojan[Backdoor]/Win32.Danti	此威胁是一类后门家族。该家族的样本在执行后会联络控制端进行通信，将自身的信息传送给控制端，并接受控制端的控制命令。（威胁等级中）
		RiskWare[RiskTool]/Win32.QQCookie	此威胁是一类风险软件家族。该类风险软件在运行后会窃取浏览器中的 cookie 信息，该信息携带了 QQ 账号 |QQ 昵称 |ST key 的信息，这一组 key 可以用来在 QQ 空间和 QQ 邮箱中进行消息推送。（威胁等级中）

高级低成本勒索软件不断增加

Ericka Chickowski / 文　安天公益翻译小组 / 译

新的勒索软件成本低至 175 美元，并具有大量的反检测功能。

恶意软件开发人员致力于开发廉价、用户友好型的勒索软件工具，帮助攻击者进入勒索行业，这种趋势将会导致 2017 年出现更多的勒索攻击。今天，Recorded Future 研究人员发布了一份报告，称相关网络犯罪分子通过软件即服务 (SaaS) 交付机制提供的一个新变种，可使成本低至 175 美元。



Recorded Future 研究人员指出，KarmenCryptolocker 恶意软件是在开源 Hidden Tear 项目的基础上创建的勒索软件即服务 (RaaS)。它遵循标准的勒索软件手法，采用 AES-256 算法加密数据，要求受害者用比特币来支付赎金，支付成功后会自动解密数据。除了成本低廉，该勒索软件还能够记录获取的赎金总额，并在出现更新时及时更新。

两年前，McAfee Labs 的研究人员发现了 Tox 恶意软件工具包，自此一直在研究类似的例子。但是，Karmen 的专业性说明勒索软件工具不断地发展。

目前，开源项目的代码广泛可用，导致许多技术高明的犯罪分子能够为低端犯罪分子开发诸如 Karmen 的变种。例如，Cylance 研究人员报告了 CrypVault 勒索软件的另一个新变种，它使用 GnuPG 开源加密工具来加密文件。

Cylance 公司的隆美尔·拉莫斯 (Rommel Ramos) 写道：“与普通的勒索软件不同，CrypVault 使用 Windows 脚本语言编写，如 DOS 批处理命令，JavaScript 和 VBScrip。因此，攻击者很容易修改其代码来创建新变种。任何具有脚本语言知识的网络犯罪分子都能够创建自己的版本来赚钱。”

举例来说，Hidden Tear 原本是作为“教育性勒索软件”开发的。但是几年前，坏家伙们开始将其代码用于自己的目的。安全专家的一线希望是：其基本代码中嵌入了漏洞，这使得勒索软件研究人员，如麦克尔·吉尔斯比 (Michael Gillespie)，能够创建解密器。现在，麦克尔正在通过 Twitter 为任何受到 Karmen 感染的人提供帮助。

尽管如此，Karmen 仍然具有一些能够阻止沙箱分析的功能，这意味着它会用来开发危险的勒索软件。

“Karmen 的一个显著特征是，如果它在受害者的计算机上检测到沙箱环境或分析软件，它就会自动删除自己的解密器。”Recorded Future 的戴安娜·格兰杰 (Diana Granger) 写到。她的同事告诉 Dark Reading，这是为了阻止安全工具和研究人员了解其代码。

很多种类的恶意软件都会使用规避技术。Tripwire 的高级安全研究工程师特拉维斯·史密斯 (Travis Smith) 表示：“这是一种典型的猫鼠游戏，犯罪分子在技术上进行了创新，防御者也是如此。一旦犯罪分子的活动受到防御措施的阻挠，他们就会继续改变战术。就这些规避技术的严重性而言，最终用户不会面临额外的风险。”

不幸的是，SecureWorks 最近的一项研究指出，尽管有 76% 的组织认为勒索软件是一种严重的威胁，但是只有 56% 的组织具有勒索软件响应计划。SecureWorks 高级安全研究员基思·贾维斯 (Keith Jarvis) 指出，担心勒索软件的组织不仅需要确保到位的备份和端点保护协议，还需要关注电子邮件过滤和补丁管理。

他说：“我们发现，大部分勒索软件都是通过电子邮件和浏览器漏洞利用包传播的，这些工具包依赖于未修复的环境。”他指出 Adobe Flash 漏洞很常见，“电子邮件防御的第一步是阻止可执行文件和脚本最常滥用的文件扩展名，然后是阻止包含宏的 Word 文档。如果您采取了这些措施，就能够阻止绝大多数的勒索软件了。”

原文名称	Advanced，Low-Cost Ransomware Tools on the Rise
作者简介	Ericka Chickowski，进入信息安全领域已将近 10 年，专注于研究信息技术和业务创新。
原文信息	2017 年 4 月 18 日发布于 Darkreading 原文地址 http://www.darkreading.com/attacks-breaches/advanced-low-cost-ransomware-tools-on-the-rise/d/d-id/1328675?
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《远程控制家族 njRAT 分析报告》

近日，安天 CERT（安全研究与应急处理中心）发现 njRAT 远程控制家族样本在今年四月份比较活跃。njRAT 是一类著名的远程控制恶意代码，使用 .NET 框架编写，存在多个变种，并采取混淆代码模式以防止恶意代码逆向分析和杀毒软件的检测。该家族样本主要利用捆绑流行游戏、破解软件及注册机来进行传播，曾用于“人面狮”APT 攻击行动中。

njRAT 远程控制恶意代码又称 Bladabindi，具有依靠插件来升级恶意代码的新功能，主要插件有 sc2.dll（远程桌面控制插件）、ch.dll（实现与受控端的聊天对话功能）、pw.dll（实现对受控端密码内容的抓取）。

在恶意服务端样本运行后，该恶意样本会创建互斥体、添加防火墙规则、在临时目录下释放样本本身、获取计算机名、获取主机用户名、添加启动项：SOFTWARE\Microsoft\Windows\CurrentVersion\Run。此外，它会对受控端的文件、进程、服务、注册表进行操控，将获取的敏感信息通过 BASE 加密发送至远程 C&C 服务器，并具有键盘记录、抓取屏幕、浏览保存密码、摄像头监控、麦克风监控等恶意功能。

该恶意代码为了防止杀毒软件的查杀，将获取的键盘记录加密保存在注册表中，以及相应插件也保存到注册表键值中。需要回传时，再将读取注册表内容进行回传。

安天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更新系统并修复漏洞，不要随意下载非正版应用软件、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应用的好习惯。安天会持续对此木马家族进行监测，并及时提出更安全的防护策略。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【追影高级持续威胁分析系统】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：

文件被内部组件发现，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、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。

文件名	./20170411.exesss
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	24 KB
MD5	6D536844AD44C91D661D8CBF8E71B1EB
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Backdoor]/MSIL.Bladabindi.as
判定依据	静态分析

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、Office 2003、Flash、WPS、FoxitReader、Adobe Reader

报告地址：https://antiy.pta.center/_lk/details.html?hash=6d536844ad44c91d661d8cbf8e71b1eb

根据动态行为（默认环境）得出该文件具有以下行为：

增加防火墙设置、延时、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、设置调试器权限、自启动、疑似键盘记录。

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	★★★

其他行为

行为描述	危险等级	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	★
获取计算机名称	★	获取驱动器类型	★
获取主机用户名称	★	读取自身文件	★
请求加载驱动的权限	★	释放 PE 文件	★
独占打开文件	★	设置调试器权限	★
增加 run 自启动项	★	自启动	★
疑似键盘记录	★★		