安天周观察

安天官方微博　安天官方微信

主办：安天　2017 年 11 月 20 日（总第 112 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天学习十九大：牢记新使命，迈入新征程

近日，学习贯彻党的十九大精神全国网信系统宣讲活动走进安天，中央网信办党的十九大精神宣讲团成员、国家行政学院经济部教授、博士生导师丁文锋在黑龙江省网信办总工程师王希忠的陪同下，为安天百余名年轻工程师深入解读了习近平总书记的“新时代中国特色社会主义思想”，从“八个明确”、“十四个坚持”再到“四个伟大”，以及习总书记对经济、政治、文化、社会、国防、外交等领域的重大部署，使在场的工程师们对十九大精神有了更进一步的理解。

在宣讲中，丁文锋教授通过鲜活生动的实例和通俗易懂的讲解，从党的十九大主题展开至新时代、新思想、新成就、新意义、

新矛盾、新使命、新目标、新部署、新任务等多个方面，对党的十九大精神进行了深入阐述。同时丁文锋教授结合安天所处的网络安全行业，对十九大报告中网信工作相关条目进行了要点解读，为安天的工程师们明确前进的方向。

去年的 5 月 25 日，习总书记曾到安天进行视察，对安天的工作给予了高度肯定，并对安天人说：“你们也是国家队，虽然你们是民营企业。”在深入学习十九大精神后，安天将继续坚持以“国家队”的坚毅信念匹配总书记的要求，更加积极地贯彻落实十九大精神中的主要任务，把十九大确立的党的基本理论、基本路线、基本方略以及各方面的重大决策部署贯彻落实到网络安全和信息化工作的全过程和各方面，确保十九大精神在网络安全行业落地生根，通过做好网络安全工作为贯彻落实十九大精神提供有力保障。安天将继续在网络安全领域执着探索、不断创新，牢记新使命，迈入新征程！

黑龙江省军区副司令员一行莅临安天参观指导

11 月 15 日，黑龙江省军区副司令员刘文东、孙会兵等一行 60 余人莅临安天哈尔滨总部进行参观指导，安天哈尔滨总部总经理李岱做了介绍汇报。

在安天展厅，李岱向来宾介绍了安天的发展成长，特别是持续与网络安全威胁对抗的情况，特别介绍了对高级持续性威胁的发现、捕获和分析方面的工作，重点介绍了安天针对“APT-TOCS（海莲花）”、“白象”、“方程式”等攻击组织的 APT 攻击情况，所使用的攻击装备和作业风格等方面的分析，以及对 WannaCry 等严重威胁的应急处理情况。在安天安全研究与应急处理中心，李岱向来宾展示了安天网络安全防护产品体系和网络靶场演训系统，并对网络靶场演训系统在关键基础设施防护演练中所发挥的价值进行了介绍。

在参观过程中，两位副司令员对安天的技术和解决方案能力表示认可，并对安天的艰苦创业经历表示肯定及赞赏。希望安天能牢记习主席的指示，在国家安全领域做出更大的贡献。

安天始终站在人民军队网络安全需求的第一线，为军委机关、军兵种、部队院校等多家单位提供了安全服务与解决方案，特别是为探月工程、空间站工程等我国重大国防航天发射试验任务提供了全面的网络安全保障。

未来战争是多维立体信息化的，网络安全是重要的非传统安全威胁，是对抗常态化的战场。习主席在十九大报告中指出要“加快军事智能化发展，提高基于网络信息体系的联合作战能力、全域作战能力”，并在报告中三次提及“军民融合”。推进军民融合深度发展，既要技术融合，还要人力融合。在网络安全领域，不仅需要技术和装备的研发提供者，还需要网络民兵预备役力量来保障。安天团队有拥军尚武的文化传统，正在积极申请筹建网络安全预备役力量。11 月 5 日，人民日报《党管武装：“第一书记”担起第一责任（国防视线·强军兴军新征程）》文章已对此进行了报道。

安天作为中国网络安全的民企国家队，将牢记使命责任，坚定投身“军民融合”伟大事业中，自觉为改革强军、转型重塑助力。

每周安全事件

类 型	内 容
中文标题	一个没有借用其他银行恶意软件代码的新的复杂银行木马
英文标题	IcedID, a new sophisticated banking Trojan doesn，t borrow code from other banking malware
作者及单位	Pierluigi Paganini; SecurityAffairs
内容概述	IcedID 采用 Emotet Trojan 的分发技术。Emotet 通过垃圾邮件发送，通常伪装在包含恶意宏的生产力文件中，并且仍然隐身以供运营商用来分发其他有效载荷，IcedID 实现了通过网络传播的能力，它通过设置一个交通隧道的本地代理来监控受害者的活动，这个概念让人想起 GootKit 木马。它的攻击策略包括 webinjection 攻击和类似于 Dridex 和 TrickBot 所使用的复杂重定向攻击，这种情况表明作者将使其针对大型企业。 恶意软件侦听目标 URL，并在遇到触发器时执行 Web 注入。受害人被重定向到假银行网站，骗子用欺骗手段欺骗受害人提交证件。攻击者控制受害者的会话，并使用社会工程手段欺骗受害者共享交易授权数据。
链接地址	http://securityaffairs.co/wordpress/65532/breaking-news/icedid-banking-trojan.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.Hinton.a[spr,rog] 2017-11-14	该应用程序伪装成短信应用，收到指定号码的短信后，静默安装恶意程序，给用户手机造成未知危害，建议卸载。（威胁等级中）
		Trojan/Android.lagertha.a[prv,rmt,spy] 2017-11-14	该应用程序伪装 Facebook 更新程序，运行后隐藏图标，接收远控信息指令，后台窃取用户短信、联系人、通话记录、社交软件记录、手机基本信息、手机存储数据等隐私信息，私自录音、录像，并上传至远程服务器。造成用户隐私泄露，请立即删除。（威胁等级中）
		Trojan/Android.jyh.a[rmt,prv] 2017-11-15	该应用程序伪装游戏交易程序，运行后请求 root 权限，加载 hook 相关工具，后台私自截屏，窃取用户其他游戏交易平台账号密码，并上传。造成用户隐私泄露和经济损失。（威胁等级中）
		Trojan/Android.Varvet.a[exp] 2017-11-15	该应用程序包含恶意代码，运行隐藏图标，私自安装恶意软件并启动，同时还会推送广告，造成用户资费，请卸载。（威胁等级高）
		Trojan/Android.FakeWhatsApp.a[exp] 2017-11-15	该应用程序伪装 WhatsApp 更新应用，无实际功能，运行推送全屏、banner 等广告，造成用户资费损耗。（威胁等级高）
		G-Ware/Android.lvhAd.a[exp,rog] 2017-11-16	该应用程序被植入恶意代码，运行后释放广告子包，频繁加载广告，造成用户资源损耗，建议卸载。（威胁等级中）
		Trojan/Android.iappliny.a[prv] 2017-11-16	该应用程序为钓鱼应用生成工具，恶意传播、制造钓鱼类应用，可能造成用户资费损失，建议不要使用。（威胁等级中）
		Trojan/Android.bbsvvs.a[pay] 2017-11-18	该应用程序为虚假色情视频应用，通过色情标题诱导用户点击下载视频，其实际下载内容为娱乐新闻等，点击图片无提示发送扣费短信，造成用户资费损失和流量消耗，建议不要使用。（威胁等级中）
	较为活跃的样本	Trojan/Android.Rootnik.af[exp,sys]	该应用程序安装无图标，后台联网下载 ROOT 文件私自提权，静默下载并安装未知文件，建议立即卸载，避免造成资费损耗。（威胁等级高）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Windows 远程及本地信息泄露漏洞（CVE-2017-11832）	Microsoft Windows 信息泄露漏洞 CVE-2017-11832，攻击者可以利用这个问题获取敏感信息，从而有助于发起进一步攻击。受影响的系统包括 Windows 2012、Windows 2008 及 R2、Win7 等版本。（威胁等级高）
	较为活跃样本	Trojan[Spy]/Win32.KeyLogger	此威胁是一种窃密类木马程序。该家族样本运行后会监视用户的键盘操作，记录用户的击键记录并上传至远程服务器，以窃取用户敏感信息。（威胁等级中）
		Trojan[Downloader]/Win32.Zurgop	此威胁是一种连接网络下载其他恶意代码的木马家族。该家族样本运行后连接网络下载其他恶意代码并执行，可能会窃取用户敏感信息并回传，有一定威胁。（威胁等级中）
		Trojan[Banker]/Win32.Tuhkit	此威胁是一种可以窃取用户银行信息的木马家族。该家族样本运行后连接远程服务器，收集用户系统中网络银行信息并回传。（威胁等级中）

共享威胁情报的六个步骤

Patrick Hill / 文　安天技术公益翻译组 / 译

911 恐怖袭击事件之后，威胁信息共享开始受到网络安全行业的更多关注。

你可能认为这是一个例行的过程，特别是考虑到在过去几年中发生了大量的数据泄露事件。但是，尽管联邦政府和信息共享分析中心（ISAC）之间已经取得了很大的进展，但是许多组织仍然将威胁信息共享放在次要位置。

“现在的情况是，首席信息安全官（CISO）非常忙碌，他们知道信息共享能够帮助他们成为更好的 CISO，或者至少是更好的人，但是他们却把它推迟了。”TruStar Technology 创始人兼首席执行官保罗·库尔茨（Paul Kurtz）说，“他们并不总是能认识到信息共享的好处。”

库尔茨说，威胁信息共享的主要原则是：

1. 信息共享不是利他主义的。数据交换的目的是更快地发现问题和减轻攻击。当一个行业纵向共享威胁数据时，该行业内的其他公司就不必再做重复性的工作了，每个人都会从中受益。

2. 信息共享不是事件通知。在事件发生之前，组织需要在安全周期的早期共享事件数据，例如有关可疑活动的信息。

3. 只要不共享个人身份信息，与其他组织共享有关漏洞利用代码和漏洞的数据是合法的。例如，受害者的电子邮件地址通常不被共享。共享的典型信息类型包括：可疑的 URL，散列标签和 IP 地址。2015 年的《网络安全信息共享法案》提供了更多的细节。

4. 共享系统必须易于使用。确保系统是人性化的，并且可以轻松地与安全运营中心（SOC）、威胁猎捕团队或欺诈调查团队的工作流程进行整合。

金融服务信息共享和分析中心（FS-ISAC）的首席信息风险官格雷格·泰姆（Greg Temm）警告说，企业在进行威胁信息共享时需要有足够的耐心。

以下是有关如何共享威胁情报的一些建议。

了解企业内部的威胁事件

照顾好自己的企业：首先了解企业内部的事件以及它们之间的联系。除非您了解自己组织内部正在进行的活动，否则您无法与他人分享信息。如今有很多工具可以帮助您了解事件数据。这个领域的一些供应商包括 TruStar Technology（该公司专门从事威胁情报集成，以便与其他企业和地域共享情报）以及威胁情报提供商 Anomali 和 ThreatConnect。

更有效地利用情报

确保能够使用其他提供商共享的情报，无论这些情报是来自 CrowdStrike 还是 ISAC，无论是来自金融、航空航天领域还是零售业。企业通常无法轻易使用来自专有威胁提供商或共享中心的外部威胁资源。通常他们会收到一封列出 20 个可疑 IP 地址的电子邮件，但他们无法筛选这些信息。当选择一个工具时，请询问该工具是否可以帮助完成这个过程，因为筛选列表是非常耗时的，会占用安全专家的大量时间和精力。

开始信息共享

现在您已经准备好与行业和业务伙伴的同行交换数据了。但是，在共享信息之前，一定要选择一个返回即时值的系统，让你看到你的事件数据与他人数据有何关联。例如，如果你的事件与另一家公司或行业 ISAC 相关联，则可以与他们共享信息并获得他们的信息。除非您确定威胁是真实的，否则就没有分享的动力。

如果可以，请不要限制威胁情报来源

选择一个允许您加入任意数量的共享组织或合作关系的系统，同时保护您认为合适的归因。一些事件可以广泛地共享，而其他事件可能需要更多的特殊处理。寻求与其他行业共享信息的好处是，您可以根据不良 URL、IP 地址或浏览器数据找到共同的模式。

选择一个可以参与美国政府的系统

与国土安全局的自动指标共享（AIS）服务部门共享信息可能有益于你的组织。在过去几年中，国土安全部一直致力于开发共享威胁情报的合作伙伴生态系统。AIS 旨在广泛分享公共和私营部门的威胁情报，使组织能够更有效地保护自己免受网络攻击。

小型组织：向 ISAC 寻求帮助

中小型企业根本没钱购买更复杂的威胁情报，他们也无法聘请威胁捕手。这些组织应该与其行业 ISAC 合作，建立一个低成本的威胁情报系统。多半的可能是，您的行业 ISAC 与供应商有联系，甚至可能有与专门的威胁情报公司建立关系的特殊交易。

原文名称	6 Steps for Sharing Threat Intelligence
作者简介	Steve Zurier 是一名自由撰稿人，拥有 30 多年的新闻和出版经验。
原文信息	2017 年 11 月 6 日发布于 Dark Reading 原文地址 https://www.darkreading.com/threat-intelligence/6-steps-for-sharing-threat-intelligence-------/d/d-id/1330386?
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）在梳理网络安全事件时注意到，拦截到了 Locky 勒索软件的最新变种，其用 .asasin 扩展名附加在加密文件后缀。目前，该变种正通过垃圾邮件进行传播活动，诱导用户打开邮件附件，间接执行恶意负载下载脚本，下载勒索软件变种加密用户文件，显示勒索信息，提供有关如何支付赎金的信息。

当用户点击邮件中的图片时，实际上图片是指向了一个快捷方式，进而调用 powershell 脚本下载 Locky 勒索软件 asasin 变种。样本执行后会生成一个字符串“Global\:a9a5aBa3aFaCa9aFa7a:aCaGa6aEaCa”，用来检查目标机器上是否已有该勒索实例在运行。然后遍历目标机器文件目录，对文档类有高价值的文件进行加密。复制文件并做加密处理，删除机器系统上的源文件和备份文件，修改加密文件，后缀名为“.asasin”。暂时未发现样本传输受害者信息的网络行为。因此，即使受害者支付赎金也不能解密文件。与之前的 Locky 样本比较，发现以下变化：不再显示任何网络行为；使用大量 JMP 指令来混淆代码，对抗安全人员分析；以及使用 sleep 函数对抗反病毒沙箱分析。同样在短时间内不会有解密 . asasin 文件的方法。恢复加密文件唯一的方法是通过文件备份。尽管 Locky 也会试图删除文件备份，但在极少数情况下，由于某种原因删除操作也存在失败的概率，存在恢复文件的可能。

安天 CERT 提醒广大网络使用者，要提高网络安全意识，在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勒索软件样本的检出。

木马程序

安天【追影威胁分析系统】无需更新病毒库，即可实现对上述勒索软件进行有效检测，下为其自动形成的分析报告：

文件由页面手工提交，经由 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。

最终依据动态行为鉴定器将文件判定为勒索软件。

文件名	c35f705df9e475305c0984b05991d444450809c35dd1d96106bb8e7128b9082f
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	646 KB
MD5	DDA37961870CE079DEFBF185EEEEF905
病毒类型	勒索软件
恶意判定 / 病毒名称	locky
判定依据	动态分析

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
延时	★★★

根据静态启发式检测得出该文件具有以下行为：延时、自获取主机用户名称、填充导入表（疑似壳）、获取驱动器类型、查找指定内核模块、获取计算机名称、独占打开文件、获取系统内存、创建特定窗体、设置调试器权限、文档篡改。

其他行为

行为描述	危险等级
获取主机用户名称	★
填充导入表（疑似壳）	★★
获取驱动器类型	★
查找指定内核模块	★
获取计算机名称	★
独占打开文件	★
获取系统内存	★★
创建特定窗体	★
设置调试器权限	★
文档篡改	★★

进程监控

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