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 27 日 (总第 150 期) 试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

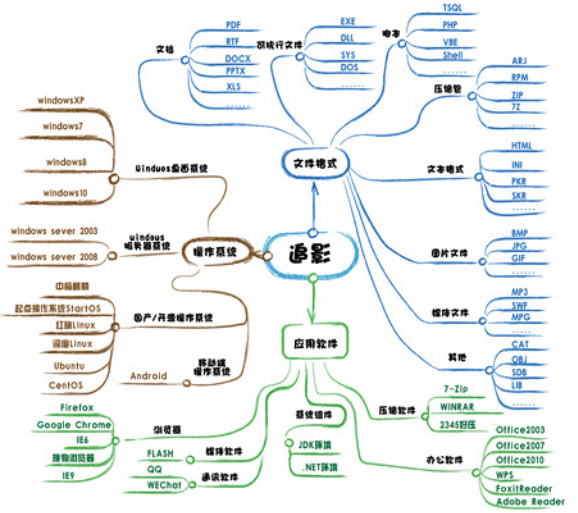
安天追影威胁分析系统获创新产品（技术）奖

由国家计算机网络应急技术处理协调中心举办的本届中国网络安全年会新增了创新评选环节，以公平、公正、客观、权威的原则，公开征集评选我国网络安全领域创新产品和创新技术成果，并颁发奖励证书。经过材料征集、材料初审和现场答辩竞选三个环节，安天追影威胁分析系统（英文简称 PTA，以下简称安天追影）获评“2018 网络安全创新产品（技术）”奖。

2018 网络安全创新产品答辩现场

追影是安天自主研发的深度威胁分析产品，其可以针对端点防护、流量监测、应急处置工作中采集、还原、提取的各种文件进行分析，发现各种格式漏洞、细粒度揭示文件执行行为，实现威胁情报生产。安天是国内恶意代码威胁自动化处理的先行厂商，2004 年便已实现了每日全量新增文件的自动化识别处理和规则输出，奠定了海量威胁自动化处理的工作基础。并从 2006 年起，依托自动化能力，为安全合作伙伴提供对象鉴定和文件分拣服务，为部署安天产品的客户提供威胁响应和鉴定的支持。

随着安全威胁的发展，仅靠非黑即白模式的恶意代码对抗机制，易于被免杀、零日漏洞利用等绕过，而导致单点失效。高级别网络安全需求下，将所有不可识别的可执行文件全部提取留存鉴定，将流量侧所有可能是攻击载荷的文件留存还原鉴定，逐渐成为刚性需求，用户威胁鉴定所需要的响应周期不断缩短。同时，攻击载荷不再仅是传统的可执行程序、脚本文件，利用 Office、PDF、WPS 等格式文档，利用 7z、ZIP 等压缩包进行的各种格式攻击、重定向执行攻击不断增多。用户将文档文件提交给厂商进行安全鉴定，存在泄密风险，形成了文件判定的安全需求和保密要求之间的矛盾。



安天在 2013 年及时跟进上述需求，将后台分析能力进行剪裁封装，推出了追影威胁分析系统。建立了与安天端点防护、流量监测产品的联动能力，协助用户形成文件采集鉴定到威胁情报反馈的自我运行闭环。安天追影将安天针对高级网空行为体分析所形成的威胁情报向态势感知等产品输送，不断提升针对高级威胁的发现能力。

安天新版追影全面增加了对国产系统的环境模拟支持，利用安天下一代威胁检测引擎的向量拆解输出能力，形成与动态行为的验证，建立了基于标签逻辑的决策森林判定机制，支持用户定制向量级规则扩展，并将动静态向量转化为上层安全管控和态势感知平台可用的分析数据资源。通过这些特性的增强，获得了“2018 网络安全创新产品（技术）”奖。

研究人员指出蜂窝网关可被用于跟踪车辆

安全研究人员已经发现了超过 100,000 个暴露在互联网的蜂窝网关，包括向世界广播确切地理位置的网络。这些特殊装置适用于车队车辆、警车、救护车等，它们的坐标位于其内置 Web 服务器从其公共 IP 地址提供的网页上，攻击者可以利用插入路由器的设置，使用端口扫描和搜索引擎（例如 Shodan.io）找到、检查和跟踪车辆。位置信息从错误配置的蜂窝网关泄漏，用于通过蜂窝网络将车辆中的设备连接到互联网，或提供通过蜂窝连接将连接路由到外部的 WiFi。

F5 安全实验室发现 Sierra Wireless 网关应用在加州公路巡逻队、丹麦国家警察局、南威尔士警察局、西雅图消防局以及其他许多人作为其客户。结合 F5 Labs 在 2016 年 10 月下旬机场感染 Bashlight 恶意软件时，发现 49,962 个面向互联网的 Sierra Wireless 网关，其中 84% 位于美国。到今年 7 月，这个数量高达 105,400 台主机，在欧洲有相当数量。显然非运营商错误配置，而是恶意攻击者。

原文链接：https://www.theregister.co.uk/2018/08/18/cellular_gateway_snafu/

每周安全事件

类 型	内 容
中文标题	安全厂商发现勒索软件新家族 Armage
英文标题	New Ransomware Family Appends ‘.Armage’ to Encrypted Files
作者及单位	David Bisson
内容概述	Quick Heal 安全实验室发现名为 Armage 的勒索软件系列，会将扩展名“.Armage”附加到它加密的所有文件中。 Armage 使用 Windows 应用程序编程接口（API）FindFirstFileA 按字母顺序找到第一个加密文档。使用 AES-256 算法加密文件，将“.Armage”添加到加密文件，然后使用 FindNextFileA API 按字母顺序搜索其它文件。一旦它加密了受感染机器上的所有文件，就会删除影卷副本，并在所有被加密的文件夹中释放一个名为“Notice.txt”的勒索说明文件。 Armage 在 7 月底通过垃圾邮件和损坏的文本文件向用户传播。
链接地址	https://securityintelligence.com/news/new-ransomware-family-appends-armage-to-encrypted-files/

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.DesertFalcons.a[prv,spy] 2018-08-20	该应用程序伪装正常应用，后台窃取用户手机通讯录、短信记录和设备基本信息，并上传到远程服务器，造成用户隐私泄露，请立即卸载。（威胁等级高）
		Tool/Android.Dokosuma.a[prv,rmt] 2018-08-22	该应用程序是一款名为 Dokosuma 的设备安全监控工具，能接收远程指令，进行位置定位、开启报警、锁定屏幕、重置密码等操作，请谨慎使用。（威胁等级中）
		Trojan/Android.watchmydroid.a[prv,spy] 2018-08-23	该应用程序是一款间谍软件，运行后隐藏图标，后台窃取用户短信、联系人、通话记录、浏览器历史记录、手机文件、社交应用记录、地理位置等大量隐私信息，私自监听用户通话、短信，私自录像、拍照、截屏，并将用户隐私上传至服务器。造成用户隐私泄露，建议立即卸载。（威胁等级高）
		Trojan/Android.eracomteck.a[prv,spy] 2018-08-23	该应用程序是一款间谍软件，后台窃取用户短信、联系人、通话记录、浏览器记录、地理位置、手机文件、邮箱等大量隐私信息，私自拍照、录音、录像、截屏，监听用户短信和通话，并将用户隐私信息上传至服务器。造成用户隐私泄露，建议立即卸载。（威胁等级中）
		Trojan/Android.jszz.a[prv,lck] 2018-08-24	该应用程序伪装 QQ 相关应用，诱导用户输入 QQ 账号密码并短信转发到指定号码，同时包含有勒索类的恶意代码，会造成用户隐私泄露，警惕其勒索代码影响用户手机的正常使用，建议立即卸载。（威胁等级中）
	较为活跃的样本	Trojan/Android.FakeFlashPlayer.ah[sys]	该应用程序伪装成 Flash Player，运行无实际功能，加密 SD 卡文件并删除原有文件，影响用户正常使用，请立即卸载。（威胁等级高）
		Trojan/Android.CuteLocker.c[rog,sys,lck]	该应用程序经过重打包处理，植入恶意代码，恶意代码会在用户的系统目录下添加锁屏勒索程序，触发安装后，重启用户手机，勒索用户付费解锁，严重影响用户体验，建议卸载。（威胁等级中）
		G-Ware/Android.FakeBatteryTool.a[exp,rog]	该应用程序运行隐藏图标，私自下载指定程序，诱导安装，造成用户资费损耗，建议卸载。（威胁等级低）
		G-Ware/Android.FakeAV.t[prv,rog]	该应用程序伪装安全应用，无实际功能，运行隐藏图标，关闭 WIFI，监听收件箱短信，设置短信已读，上传短信内容，造成用户隐私泄露，影响用户正常使用，建议不要使用。（威胁等级低）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Struts 2 远程命令执行漏洞 S2-057（CVE-2018-11776）	在使用 Struts 2 框架定义 XML 配置时，如果 namespace 值未设置且上层动作配置（Action Configuration）中未设置或用通配符 namespace 时可能会导致远程代码执行。攻击者可利用漏洞实施远程命令执行攻击。（威胁等级高）
	较为活跃样本	Trojan[Banker]/Win32.Banbra	此威胁是一木马类程序。该家族专门用于盗取银行信息。运行后能够感染硬盘的主引导记录，对包括使用 EV-SSL 的 HTTPS 在内所有类型的网络流量进行控制，在被窃取的信息发送到金融网站之前就被传送到远程服务器上。（威胁等级高）
		Trojan[Backdoor]/Win32.AutoIt	此威胁是一种后门类木马程序。该家族是通过 AutoIt 编写的后门程序。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[Dropper]/Win32.Pincher	此威胁是一种具有捆绑功能的木马类程序。该家族从用户系统窃取重要数据和信息，并把它发送给攻击者。该家族将恶意代码注入到被感染系统，并防止用户访问 Windows 的注册表文件。（威胁等级中）

如何保护组织免受内部威胁

Prafulla Mannewar / 文　安天技术公益翻译组 / 译

如今，技术的发展可谓“日新月异”。今天为基础设施或数据部署的新安全系统，明天很可能就不怎么安全了。在这个快速通信的时代，有很多人渴望击败新技术——以合法或不合法的方式找到系统的漏洞和弱点。但是，造成风险的并不总是外部恶意威胁源。内部威胁也是一种严重的风险，不应该被忽视。

开展内部威胁预防培训

部署最新的安全系统来对抗网络威胁是一个很好的策略，但是，组织还必须实施有效的管理系统来培训员工，主动检测危险信号，以最大限度地减少内部威胁。

精心设计和开展年度网络安全或数据隐私培训课程，是这项工作的重要一步。这些课程不应是简单地读书本、听音频和观看演示文稿。相反，它应该是互动性的，而且要包含相关的案例。如果员工对安全培训不反感，他们就更有可能吸收培训内容并将其付诸实践。

有关如何识别恶意和合法电子邮件的培训，是这些课程的重要组成部分。当你收到一封垃圾邮件时，你的第一个反应很可能是“取消订阅”。但是，这样正中垃圾邮件发送者的下怀。一旦你这样做，他们就能够确认电子邮件地址是有效的。员工必须能够识别垃圾邮件，并且知道最好的做法是将它们标记为“垃圾邮件”，并将该标记在整个组织内部分享，降低其他同事遭受该垃圾邮件侵害的可能性。

有效的风险沟通

通常，当出现新的漏洞时，组织会将

相关信息传达给员工。但是，这些沟通可能偏技术性，不是所有员工都能理解。如果这些信息过于复杂或冗长，员工可能会失去阅读的兴趣——因此可能无法了解漏洞的影响。在与员工沟通漏洞情况时，应该简洁明了。沟通越清晰，员工就越有可能避免失误，从而预防攻击。

与潜在漏洞相关的数据隐私风险，不仅会影响负责维护基础设施、系统或服务器的员工。利用这些漏洞的攻击可能会影响任何级别的组织，而且组织的任何员工都可能会受到影响。任何员工点击了可疑链接，都可能会为组织带来灾难。因此，必须事先进行清晰的沟通——而不是做“事后诸葛”。

通过员工分类将风险降至最低

员工分类是另一种降低风险的方式。你可以通过将员工分为两类——特权员工和普通员工，来实现这一点。

特权员工是指可以访问敏感信息和客户数据的员工。这些员工可能会造成最大的内部威胁，因此应该为他们提供更安全的系统。其他员工则被归为“普通”类别，需要施加的限制比较少。

制定社交媒体指南

另一个重要事项是制定社交媒体指南。虽然许多组织禁止在内部使用流行的社交媒体平台，但组织可能不会对内部交流平台或协作工具进行风险评估。与邮件相比，员工更有可能会点击内部交流平台或协作工具上的链接。

例如，在内部交流平台上传播的恶意假新闻。员工可能不知道这种帖子的真实目的，但仅仅因为有朋友或同事分享了它，员工可能就会点击该链接。更糟糕的是，员工可能还会点击“分享”，进一步将链接传播给其他人。员工对内部员工的信任或者缺乏安全意识导致未经证实的新闻和恶意软件迅速蔓延。

注意危险信号

由内部人员引起的大多数攻击都是无意的，但这并不意味着不存在有意的内部攻击。员工有可能会行事反常并窃取机密。但是在发生此类事件之前，通常会有很明显的危险信号。

员工突然开始在公司加班，或者在下班时间或周末登录公司网站，可能就是危险信号。此外，员工经常在与其工作无关的区域走动，或拷贝敏感的商业信息，也应该引起注意。

考虑到内部攻击导致的损失越来越大，安全团队需要主动关注这些信号，以避免内部威胁对组织造成伤害。组织应保持警惕，尽量减少内部风险（无论是有意还是无意的），这样可以节省数百万美元的补救成本。

原文名称	How to Protect Your Organization From Insider Threats
作者简介	Prafulla Mannewar。Prafulla Mannewar 是 IBM 公司合规与控制顾问。
原文信息	2018 年 8 月 17 日发布于 Security Intelligence 原文地址 https://securityintelligence.com/how-to-protect-your-organization-from-insider-threats/

安天发布《Crysis 勒索软件变种分析报告》

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发现 Crysis 勒索软件变种开始活跃。该木马家族自 2017 年公布通用解密密钥后沉寂了一段时间，现在又卷土重来。Crysis 目标大多针对各类服务器，攻击方法多数采用远程RDP暴力破解，加密文件后缀名为 .java。由于 RSA 密钥已经不同于之前黑客公布的 Crysis 原样本，因此现在暂时无法解密。

Crysis 木马样本会复制自身到多个目录以实现驻留，如：%windir%\System32、%appdata%、%sh(Startup)%、%sh(Common Startup)%。该样本会结束硬编码的进程，包 括 1c8.exe、1cv77.exe、outlook.exe、postgres.exe、mysqld-nt.exe、mysqld.exe、sqlserver.exe，可以看出，该勒索软件的主要目标为数据库程序，结束与数据库有关的进程，防止占用数据库文件会使加密失败。恶意代码加密文件时，先判断文件的大小，当文件大小大于 0x180000 字节（约 1.5MB）时，直接对文件内容进行加密，并将文件重命名；当文件大小小于等于 0x180000 字节（约 1.5MB）时，则创建新文件并加密旧文件内容后写入新文件之后删除旧文件。对于文件大小大于和小于 0x180000 字节的文件，在文件尾部写入特定信息，以供攻击者解密文件时使用。

安天 CERT 提醒广大网络使用者，关闭相应的RDP服务，关闭不必要的端口如：445，3389 等。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、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 BD 静态分析鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	e121bedebfbb0a49b3e7fe86827fe06b1faae846e7cbe9bcbc8e0a3eae6e8a70
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	459 KB
MD5	06143482CFE284535C01BA538FEF4367
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Generic
判定依据	BD 静态分析

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=06143482CFE284535C01BA538FEF4367

◆ 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
添加 IPC 共享	★★★	可疑进程名称	★★★★

◆ 常见行为

查找指定内核模块	★
查找特定窗体	★
独占打开文件	★
遍历进程	★
打开自身进程文件	★
读取自身文件	★★
释放 PE 文件	★
从资源中释放 PE 文件到系统目录	★★
增加 run 自启动项	★
设置自启动项	★★
释放 PE 文件	★★
获取驱动器类型	★

◆ 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	192.168.122.246	68
192.168.122.246	137	192.168.122.255	137
.....	.....	.....	.....