安天发布《FTCode 勒索软件分析报告》

近日，安天 CERT 在梳理网络安全事件时发现了一个基于 PowerShell 脚本的勒索软件 FTCode。该勒索软件最早在 2013 年被发现，主要通过垃圾邮件进行传播。邮件附件中包含恶意宏代码的 Word 文档。该文档诱使用户启用宏查看文档内容，当用户启用宏后，恶意宏代码将连接 C2 下载并执行恶意脚本。

FTCode 运行后，创建名为“WindowsApplicationService”的计划任务项，解密内置字符串生成一个 RSA 加密密钥，删除磁盘卷影和操作系统备份禁止修复。对指定的文件后缀名进行加密，并追加后缀名“.FTCODE”。加密结束后，FTCode 会在每个加密的文件目录中创建一个名为“READ_ME_NOW.htm”的网页格式的勒索信，勒索信中包含解密说明、勒索病毒解密网址、安装 Tor 浏览器教程和 UEER_ID。目前被加密的文件在得到密钥前暂时无法解密。

安天提醒广大用户，及时备份重要文件，且文件备份应与主机隔离；及时安装更新补丁，避免一切勒索软件利用漏洞感染计算机；对非可信来源的邮件保持警惕，避免打开附件或点击邮件中的链接；尽量避免打开社交媒体分享的来源不明的链接，给信任网站添加书签并通过书签访问；避免使用弱口令或统一的密码；确保所有的计算机在使用远程桌面服务时采取 VPN 连接等安全方式，如果业务上无需使用远程桌面服务，建议将其关闭；可以使用反病毒软件（如安天智甲）扫描邮件附件，确认安全后再运行。

目前，安天追影产品已经实现了对该类勒索病毒的鉴定；安天智甲已经实现了对该勒索病毒的查杀。

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 自定义鉴定器、来源信息鉴定器、元数据信息鉴定器、动态（Win7 x86）鉴定器、反病毒引擎鉴定器、动态（WinXP）鉴定器、聚类分析鉴定器、复合文档增强分析鉴定器、智能学习鉴定器、静态特征检测鉴定器、安全云鉴定器、信标检测鉴定器等鉴定分析。

最终依据动态行为鉴定器、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	b09bc9a25090cada55938367c7f12e692632afa2ed46d5e90eba29da84befafd.docx
文件类型	Document/Microsoft.DOC[:Word 98-2003]
大小	3.00 MB
MD5	A5AF9F4B875BE92A79085BB03C46FE5C
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[IM]/Win32.Downloader
判定依据	BD 静态分析

◆ 操作系统

操作系统	内置软件
Win7 x86 6.1.7600 Build 7600	默认、IE9、Google Chrome、Firefox、Office 2007、Flash、WPS、FoxitReader、Adobe Reader

◆危险行为

行为描述	危险等级
文档启动 powershell	★★★★★
宏调用	★★★★

◆常见行为

行为描述	危险等级
创建快捷方式	★
加载运行时 DLL	★
获取驱动器类型	★
获取系统版本	★
获取计算机名	★
检索系统内存信息	★
打开自身进程文件	★
镜像劫持	★★
.....	.....

◆完整报告地址

安天周观察
安天官方微博 安天官方微信
主办：安天 2019 年 11 月 04 日 (总第 206 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

安天产品巡礼（系列三）——追影威胁分析系统

追影威胁分析系统是安天自主研发的文件深度分析设备，其以文档文件、可执行文件、URL 为分析对象，采用深度静态分析与沙箱动态加载执行的组合机理，借助包括安天下一代检测引擎在内的多组鉴定机制组合对输入对象进行判定分析，实现漏洞利用触发、细粒度揭示载荷行为、形成私有化的威胁情报生产能力。追影可有效检出分析鉴定各类已知与未知威胁，尤其对基于格式文档的 0day 漏洞攻击具备优秀的检出能力，通过动静态结合的手段对各种格式的文件进行细粒度的向量提取和解析，深度揭示威胁行为细节，输出详实报告，追影在进行判定后，结合白名单过滤机制，可以输出多种样式的威胁情报，实现客户私有化的情报生产能力，辅助威胁处置和威胁猎杀工作。追影与安天威胁情报服务结合，可以实现对载荷关联 APT 攻击组织的精准指向，并基于威胁框架评估载荷的能力模型。

追影内置安天 AVL SDK 下一代威胁检测引擎，结合持续从安天获得海量病毒库和白名单库，可对已知威胁实现高精度检测，快速过滤海量已知恶意程序，有效孤立未知威胁；自主可控的威胁检测引擎，降低了外部技术依赖风险，提升了客户威胁响应的针对性和及时性。安天将分析专家团队近二十年专业的恶意代码对抗经验和近十年来对 APT 事件的长期持续分析与跟进能力，不断转化为追影的分析模型改善，可从多个维度对文件进行深度分析。AVL SDK 下一代引擎可以对监测对象进行深度向量拆解和轻量级虚拟执行与解密还原，从而实现静态分析与动态触发相互结合验证，能更好的揭示威胁载荷的功能、能力及规避检测的手段。在检测精度、检测能力和检测速度等方面均显著优于仅依赖动态监测或开源系统的普通沙箱产品。

追影可将输出的情报线索反馈给安天探海威胁检测系统、安天智甲终端防御系统以及第三方安全产品，为威胁的处置响应提供有效的数据支撑，提升用户对未知威胁的发现、监测、阻断能力；还可有效支撑态势感知系统，为关键威胁揭示以及态势跟踪提供数据基础。此外，与各种云端鉴定产品和服务相比，追影是完全本地化的安全设备，产品的动静态引擎、知识和决策机制能够确保文件的整个分析过程都在本地设备中完成，而不需要用户传递检测对象或者关联数据给安天，确保用户在保密隔离场景下获得威胁分析和情报生产能力。

追影威胁分析系统可以为政府、军队、能源、金融、交通等行业客户提供威胁深度分析能力，支撑客户的重大活动安全保障、高级威胁分析和安全事件响应。

▲追影的样本分析报告

功能简介

追影产品通过安天下一代威胁检测引擎和海量白名单等机制可直接对已知威胁进行精准识别；追影采用动静结合的鉴定方式，配合独有的智能学习功能，可对文档文件、可执行文件、URL 等对象，进行格式识别解析、Shellcode 发现、堆喷射检测、字符串信息提取、漏洞检测以及对文件数字证书、来源、元数据等进行拆解分析；针对可动态执行的文件，监控并记录其远程线程插入、文件操作、注册表操作、驱动加载、网络通信访问、系统文件的修改以及网络访问等行为，可有效检出各类已知威胁与未知威胁，尤其对基于格式文档的 0day 漏洞攻击具备优秀的检出能力；同时，结合强大的自学习能力以及关联分析能力，追影又可不断更新鉴定结果，在提高文件检测率的同时保证文件鉴定的准确率，从而帮助客户掌握网络安全状况，提高网络安全防护能力。

追影经过安天十余年的自主研发积累，形成了在漏洞触发、细粒度行为揭示以及向量级情报输出等方面的领先优势。近年来，以超级大国为背景的超高能力网空威胁行为体十分活跃，安天将产品服务体系和分析应急工作的重心逐步转入到应对高级网空威胁行为体所发动的 APT（高级持续性威胁）攻击中 ，在高级威胁发现、分析、溯源方面取得了一系列进展；在威胁情报方面，安天基于大规模主动捕获感知环节的部署、海量样本与事件自动化分析体系和样本与威胁情报交换体系，形成了对多源异构样本和数据源的分析、处理能力，形成了从信标规则到 TTP 情报的生产体系。这些均为追影的产品能力提供了有效支撑。

微信扫描二维码阅读原文

每周安全事件

类 型	内 容
中文标题	恶意软件 Xhelper 已感染超过 4.5 万台设备
英文标题	Xhelper: Persistent Android dropper app infects 45K devices in past 6 months
作者及单位	May Ying Tee Software Engineer &Tommy Dong Sr Princ Software Engineer
内容概述	赛门铁克观察到对恶意 Android 应用程序的检测激增，该应用程序可以向用户隐藏自身，下载其他恶意应用程序并显示广告。这个名为 Xhelper 的恶意软件是持久性的。它可以在用户卸载后重新安装自己，并且通过不出现在系统的启动程序上而保持隐藏。在过去的六个月里，这款恶意软件已经感染了超过 4.5 万台设备。
链接地址	https://www.symantec.com/blogs/threat-intelligence/xhelper-android-malware

每周值得关注的恶意代码和漏洞信息

经安天【CERT】检测分析，本周有 8 个移动平台恶意代码和 6 个 PC 平台的恶意代码和漏洞值得关注

恶意代码类别		名称与发现时间	威胁等级	简要描述
移动恶意代码	新出现的样本家族	G-Ware/Android.Bianlian.b[exp,rog] 2019-10-25	高	该应用程序运行联网接收指令，变换使用界面，推送第三方贷款、投资理财类产品，该类服务没有安全保障、可能造成用户财产损失，建议卸载。
		Trojan/Android.B4ABanker.a[prv,exp] 2019-10-26	中	该应用程序伪装金融相关软件，运行后隐藏图标，诱导用户填写银行相关隐私信息，并通过短信上传。造成用户隐私泄露。
		RiskWare/Android.ArgusAPMtest.a[rog] 2019-10-27	中	该应用程序为测试程序，用户可以用其抓取 App 的 log 信息保存至本地数据库，包含恶意 windows 病毒文件，运行会释放至 sd 卡但未加载至电脑，存在一定的风险，建议卸载。
	较为活跃样本	Trojan/Android.QQspy.er[prv,exp]	中	该应用程序伪装成 QQ 相关应用，诱导用户输入 QQ 账号密码通过短信转发，造成用户隐私泄露和资费损耗，建议卸载。
		Trojan/Android.InfoStealer.bi[prv	中	该应用程序包含恶意代码，运行会后台获取用户手机短信和固件信息，手机通讯录和通话记录等并回传攻击者，造成用户隐私泄漏，建议卸载。
		RiskWare/Android.uangtech.b[prv]	中	该应用程序为某贷款相关 APP 的子包，包含风险代码，有获取用户短信、通话记录、手机设备信息、位置等敏感代码，可能会造成用户隐私泄漏，建议卸载。
		Trojan/Android.Tikmm.a[exp,rmt,fra]	中	该应用程序伪装知名应用，运行隐藏图标，私自发送短信到指定号码，根据网络回传指令执行安装、加载广告、发送短信等操作，会造成用户资费消耗，影响用户的使用体验，建议立即卸载。
		G-Ware/Android.FakeWG.d[fra]	低	该应用程序伪装游戏破解工具，运行诱导用户分享或付费购买，无实际功能，建议卸载。
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Windows 映像 API 远程代码执行漏洞（CVE-2019-1311）	高	当 Windows 映像 API 不正确地处理内存中的对象时，存在远程代码执行漏洞。该漏洞可能以一种使攻击者可以在当前用户环境中执行任意代码的方式损坏内存，为了利用漏洞，攻击者必须诱使用户打开一个专门制作的 WIM 文件。
	较为活跃样本	Trojan/Win32.Shakblades	中	此威胁是一种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，收集用户信息，复制自身通过邮件传播。
		Trojan/Win32.Hider	中	此威胁是一种具有后门行为的木马家族。该家族的样本在运行后会连接 C&C 服务器通知并接受控制。
		Trojan/Win32.Wanbag	中	此威胁是一种可以下载恶意代码的木马类程序。该家族样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并回传。
		GrayWare/Win32.ScreenSaver	低	此威胁是一种可以下载并安装屏幕保护程序的灰色软件类程序。该家族样本运行后连接远程服务器下载某屏幕保护程序并安装，可能会弹出广告，影响用户使用。
		GrayWare[AdWare]/Win32.AdAgent	低	此威胁是一种可以安装广告件的灰色软件类程序。该家族样本运行后安装推广应用并连接远程服务器，在用户浏览网页时弹出广告，占用系统资源，影响用户使用。

2020 年及以后网络安全的四大变化

Jon Oltsik / 文 安天技术公益翻译组 / 译

2020 年，技术和市场变化的步伐将会加快，这将影响安全技术、创新、投资以及整个安全行业。

随着 2019 年的结束，安全分析师开始预测安全行业下一年的趋势。目前，我还未完成预测清单，但我非常确信企业安全技术将会发生前所未有的变化。这些变化已经悄悄发生，但在 2020 年及以后将会变得更加明显。

发生了什么?

网络安全已成为对企业至关重要、极具动态性、可大规模扩展和高度专业化的学科，但是企业面临着单点工具、依赖手动流程和人才短缺的现状。在这种情况下，企业难以保护网络安全。

在接下来的几年中，这些传统策略将会过时。大型企业将依靠基于以下趋势的网络安全技术基础架构。

一、紧密耦合的网络安全技术平台

首席信息安全官（CISO）将放弃对传统最佳单点工具的偏爱，转而使用具有以下五个紧密耦合组件的网络安全平台：端点 / 云工作负载安全、网络安全、文件沙箱、威胁情报和高级分析，以便将所有功能整合在一起。虽然有可能会出现新的标准将各种不同的工具整合起来；但许多大型企业将选择单一的供应商平台。紧密集成、供应商合作和精简操作所带来的好处将超过单点工具之间的增量差异。

二、分布式、基于云的集中化管理

随着不同的安全“服务”在基于云的管理面板下融合，网络安全技术平台的概念也将大大扩展。“弹性云网关”就是这种新兴技术趋势的一个例子。管理面板将监督诸如配置管理、策略管理、监控等活动。实际的安全控制将分布在本地、网络边缘、公有云中，并能够为单个应用程序、服务器、用户等定制极其细粒度的策略实施规则。在这种情况下，安全技术背后的“大脑”将转移到云中，而基于硬件和软件的实际安全控制将作为“神经末梢”（即高性能的安全交换机）。

三、大规模 SOAPA 引擎

安全信息和事件管理（SIEM）和其他安全分析工具也将融合在一起，作为大规模可扩展的“安全运营和分析平台架构”（SOAPA）。但是，除了架构之外，我们还将看到安全运营中心（SOC）的范围和用途呈指数级变化，机器数据的收集和处理将呈爆炸式增长。威胁和漏洞数据的关联将大大改善，使企业可以更容易地根据可利用的漏洞和经过测试的弱点制定安全决策。风险管理数据也将变得更加可见和可访问，使企业能够将业务和网络风险关联起来。当然，机器学习算法将会大大改进，并整合在一起以形成相互补充的嵌套算法，从而提高准确性。最后，SOC 工具将开始受益于多年的可视化分析研究。此外，企业将针对不同的技能，采用虚拟现实（VR）、大型等离子屏幕和各种移动设备等显示屏，对用户界面进行定制。

四、自动化技术和服务将融入产品中

大多数典型、繁琐的日常安全操作将实现自动化，从而使安全团队得以腾出时间来保护企业资产 / 流程，并专注于高优先级事件。这将包括基于用户、位置、网络流量或资产业务价值的策略自动化。一旦用户和设备通过强大的多因子身份鉴别获得访问权限，自动化技术将向其建议或强制执行端到端的最低权限 / 零信任原则，从而大大减少攻击面。为了应对安全的复杂性，自动化技术将配备高度智能的“助手应用程序”，而网络安全人员可以随时提供最佳实践、提出问题或提供帮助。

这一未来架构并不是什么秘密。我一直将其视为 SOAPA 的演变，而我的同事戴夫 · 格鲁伯（Dave Gruber）则将其视为“外部数据表示法”（XDR）。两者在开发和组件方面略有差异，但总体格局相同。国防部 / 国土安全部（DoD/DHS）和约翰霍普金斯大学（John's Hopkins）的集成式自适应网络防御（IACD）提出了类似的愿景。

上述变化不会在一夜之间发生，但是，当这些变化出现时，诸如 Check Point、Cisco、FireEye、Forcepoint、Fortinet、IBM、McAfee、Microsoft、Palo Alto Networks、Rapid7、Symantec 和 Trend Micro 等大型网络安全厂商将具有明显的优势。到 2022 年，其中一家或几家公司将超越其他公司，成为价值 50 亿美元的网络安全供应商。诸如亚马逊和谷歌这样的云供应商将会抓住这些趋势，而诸如 CrowdStrike、Cybereason、Zscaler 等一些有远见的小公司也会抓住这些趋势。

在这种情况下，网络安全技术的力量将会大大集中。初创企业将获得有限的窗口来证明自己的价值——与大公司合作，被收购或破产。

这些变化还需要一段时间才会出现，但是技术和市场变化的步伐将会比过去快得多。同时，新型威胁、大规模数据泄露和关键基础设施中断将促使 CISO 跳出固定思维，加快大规模的架构过渡。

变革即将到来，而且将比大多数人想象的规模更大，速度更快。明年，以及下一个十年，应该会非常有趣。

原文名称	4 big changes coming to cybersecurity in 2020 and beyond
作者简介	Jon Oltsik。Jon Oltsik 是 ESG 高级首席分析师，也是该公司网络安全服务的创始人。
原文信息	2019 年 10 月 25 日发布于 CSO Online 原文地址 https://www.csoonline.com/article/3447181/4-big-changes-coming-to-cybersecurity-in-2020-and-beyond.html
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。