安天周观察

主办：安天　2017 年 3 月 20 日（总第 80 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

联网行业网络安全试点示范项目 安天入选工信部 2016 年电信和互

近日，安天网络安全态势感知与通报预警平台入选了工信部 2016 年电信和互联网行业网络安全试点示范项目。这是工信部首次面向网络安全企业开展网络安全试点示范项目征集，旨在贯彻实施网络强国战略，完善电信和互联网行业网络安全保障体系，进一步推进电信和互联网行业网络安全技术手段建设。

在网络安全威胁监测预警、态势感知与技术处置领域，共有 4 家网络安全企业入选了最终名单，安天网络安全态势感知与通报预警平台凭借其实用性、创新性、先进性、可推广性等方面的突出优势，入选了该试点示范项目。除了安天，其余三家为匡恩（工控相关）、知道创宇（网站监测相关）和中兴通讯（检测与防御相关）。

安天网络安全态势感知与通报预警平台拥有一套完整的网络安全威胁监测预警与态势感知体系，具备网络攻击监测、漏洞挖掘、威胁情报收集、工业互联网安全监测等能力，实现了从情报收集、威胁发现、告警、通报、感知，最终到技术处置的闭环处置流程。本平台基于高精度的网络病毒监测和捕获设备（安天探海威胁检测系统 PTD）、高级威胁鉴定系统（安天追影威胁分析系统 PTA）和安全监测处置系统（安天智甲终端防御系统 IEP），实现了数据采集、安全监测、态势感知、事件告警、通报预警、追踪溯源和系统运维支撑等要求，对安全威胁进行综合分析，实现了及早预警、态势感知、攻击溯源和精确对应，降低了系统安全风险、净化了公共互联网网络环境。

安天为国家保密局提供专用防病毒软件

2015 年，安天为国家保密局提供的国产平台防病毒软件开始参与涉密专用计算机万台规模应用示范，现已稳定运行近两年时间。安天国产平台防病毒软件目前是涉密专用计算机项目中的唯一杀毒软件。在中国科学院信息工程研究所（以下简称：信工所）的统一规划下，安天分别与中标麒麟、中科方德等国产操作系统厂商进行了深入的代码级合作。随后，安天投入了大量的资源完成了国产系统与国产硬件平台的适配工作，并参与制定了涉密专用防病毒软件的标准。

近年来，国产操作系统的安全问题在日益升温，国产操作系统遭受的各类威胁也亟待解决。虽然国产操作系统在开源 Linux 等系统下定制开发，但同样会遇到诸如恶意脚本、Webshell 等危害国产系统安全的恶意代码的威胁。据统计，Linux 环境中已经存在超过 2 万种二进制恶意代码，而其中很多都是开放源码的。国产浏览器、国产办公软件等也将会面对相关漏洞和格式文档漏洞等的攻击。安天一直以来比较重视国产平台的安全性问题，长期关注恶意代码在不同体系结构和操作系统的安全现状，对 Windows、Linux、各种商用 UNIX、Android、MAC、Android 等平台的恶意代码进行了持续采集、跟踪、分析和积累，同时还为国内主流安全厂商和科研机构提供威胁检测能力，建立了威胁感知生态体系。

安天针对国产处理器（龙芯、兆芯等）和国产操作系统（中科方德、中标麒麟等），根据涉密专用计算机的安全保密需求，研发了为国家保密局专用的防病毒软件。该防病毒软件能较好地查杀各种常见的二进制可执行文件、Rootkit、溢出文件格式、脚本等病毒，提升了国产平台的安全性。

◆ 加拿大统计局网站因 Struts2 漏洞被黑

近日，据外媒报道，黑客利用 Apache Struts 2(Java Web 服务器框架）软件中新发现的漏洞，袭击了加拿大统计局的网站。目前，加拿大政府也证实了该局网站已经被黑客入侵，并离线超过两天。此外，当局还声称加拿大税务局 (CRA) 网站虽然还没有被黑客入侵，但它存在着和加拿大统计局网站同样的漏洞，因此当局在税收季节的高峰期关闭了该网站。

CRA 发言人帕克斯·萨姆森称，此次事件已经过去了 48 个小时，CRA 还在与其他政府部门进行处理，寻求解决方案。CRA 也保证该解决方案会经过严格的测试，尽早恢复在线服务等功能。加拿大统计局的通信总监 Gabrielle Beaudoin 说，黑客入侵的服务器内并没有存储可用的个人敏感信息，所以黑客的攻击并没有造成相关数据的丢失。（来源：http://hackernews.cc/archives/7596）

一周简讯

- 研究人员渗透勒索软件 CryptoBlock 的 C&C 服务器
- 针对金融机构垃圾邮件活动利用假冒反病毒软件
- 攻击者劫持 Magento 平台扩展来窃取信用卡数据
- 黑客利用浏览器程序漏洞破解了任天堂 Switch
- 64 万被窃的 PlayStation 玩家账号在暗网出售
- Linux 恶意软件利用 CGI 漏洞感染 IoT 设备
- 研究人员演示对手机加速计实施声波攻击方法
- 暗网出售 64 万疑似索尼游戏平台的账号信息
- 英国 NHS 数千医务人员信息被窃 因 IT 承包商被黑

安天 CERT 整理，详情请见 http://bbs.antiy.cn

每周安全事件

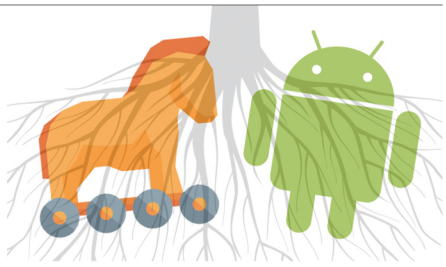
类 型	内 容
中文标题	安全公司发现暗网出售 macOS Proton RAT 新变种
英文标题	New variant of the macOS Proton RAT advertised on Russian cybercrime underground
作者及单位	Pierluigi Paganini；SecurityAffairs
内容概述	近日，安全公司 Sixgill 的专家发现一个新的 macOS Proton RAT 变种在俄罗斯地下网络犯罪市场出售。恶意软件具有获取 root 访问权限功能，允许攻击者获得受害者计算机的完全控制权。 Proton 恶意软件的制作者竟然获得了苹果的代码签名，从而可以绕过官方严格的第三方软件过滤机制。制作者可能篡改了苹果开发者 ID、或是窃取了相关凭证。此外，Sixgill 公司认为该恶意软件或许利用了 macOS“此前未修补的一个零日漏洞”来获得目标系统的 root 权限，因此该恶意软件的使用者仍需自行通过一个自定义名称（或图标）来掩饰。当然，在此之前，攻击者还得先设法引诱受害人去下载和安装该恶意软件。
链接地址	http://securityaffairs.co/wordpress/57109/malware/macos-proton-rat.html

每周值得关注的恶意代码信息

经安天检测分析，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

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.GomSpy.a[exp,prv] 2017-03-13	该应用运行后会申请设备管理器权限，尝试删除自身图标，后台收集用户未接短信、收件箱等信息并上传，造成用户隐私泄露和资费消耗，建议卸载。（威胁等级高）
		Trojan/Android.FakePorn.a[fra,prv,sms] 2017-03-14	该应用程序伪装色情应用，而无相关实际功能。安装后自动隐藏快捷启动图标，弹出界面诱骗用户点击按钮以激活设备管理器。监听并拦截短信来信，从网络获取指定号码和文字内容发送短信。还会上传用户隐私数据。造成用户隐私泄露和资费损失，建议立即卸载。（威胁等级高）
		G-Ware/Android.LockDevice.a[rog,exp] 2017-03-14	该应用伪装成系统助手应用，安装运行后请求激活设备管理器，一旦激活则重置设备密码并锁定设备，会私自向指定号码发送短信。导致用户无法使用设备并造成资费损失。建议取消激活并立即卸载。（威胁等级中）
	较为活跃的样本	G-Ware/Android.LockScreen.i[rog]	该应用程序运行后弹出置顶界面占据屏幕，同时播放音频，劫持 Home 键导致无法退出。具有流氓行为，建议立即卸载。（威胁等级低）
		Trojan/Android.HiddenAds.bl[exp]	该应用安装无图标显示，开机自启并加载广告子包，造成用户资费消耗，建议立即卸载。（威胁等级中）
		Trojan/Android.FakeApp.dj[rog,exp]	该应用伪装成其他应用，篡改加入恶意代码，程序运行会请求激活设备管理器，隐藏图标，联网推送广告，造成用户资费消耗。（威胁等级中）
		Trojan/Android.Triada.ah[exp]	该程序伪装成系统应用，安装无图标显示，动态加载恶意子包，私自下载安装未知应用，建议立即卸载，避免造成资费损耗。（威胁等级高）
		Trojan/Android.QQspy.am[prv,exp]	该程序伪装成 QQ 相关应用，会诱导用户输入账户和密码，并通过短信转发，造成用户隐私泄露和资费损耗，建议卸载。（威胁等级高）
		Tool/Android.PhoneGuard.b[prv,rmt]	该应用是远控工具，通过短信远程控制，可完成锁屏、备份联系人、定位等功能，请谨慎使用。（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 Player ActionScript 3 释放后重用漏洞 (CVE-2015-5122)	Adobe Flash Player 的 AS3 实现过程中的 DisplayObject 类存在释放后重用漏洞。远程攻击者可借助特制的 Flash 内容利用该漏洞执行任意代码，或造成拒绝服务（内存损坏）。以下版本受到影响：基于 Windows 和 OS X 平台的 Adobe Flash Player 18.0.0.203 及之前版本和 Adobe Flash Player Extended Support Release13.0.0.302 及之前版本，基于 Linux（安装 Google Chrome）平台的 Adobe Flash Player 18.0.0.204 及之前版本，基于 Linux 平台的 Adobe Flash Player Extended Support Release 11.2.202.481 及之前版本。（威胁等级高）
	较为活跃的样本	Trojan[Ransom]/Win32.DMALocker	此威胁是一类可以加密用户数据的木马家族。该家族样本为 DMA Locker 4.0，运行后会连接远程服务器，加密用户特定后缀名的文件并要求支付 1 比特币，如果在 4 天之内不支付的话，该价格会提升到 1.5 个比特币。（威胁等级中）
		Trojan[Ransom]/Win32.Democry	此威胁是一类可以加密用户数据的木马家族。该家族样本运行后遍历系统文件并加密，它会在加密的文件名后面加上攻击者的邮箱地址，与其联系后才能获取付款以及解密的方法。（威胁等级中）
		Trojan/Win64.Expiro	此威胁是一类可以感染用户系统文件并窃取信息的木马家族。该家族样本运行后会感染系统文件，插入代码的大小为 512KB，它还可以窃取用户信息，有一定威胁。（威胁等级中）
		Trojan[Downloader]/Win32.Betload	此威胁是一类可以下载恶意代码的木马家族。该家族样本运行后会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，有一定风险。（威胁等级中）

38 款安卓手机预装了恶意软件



Michael Mimoso / 文　安天公益翻译小组 / 译

近日，研究人员发现，多家手机制造商生产的手机在供应链的某环节被预装了恶意软件。

Check Point 软件技术公司发现，38 款安卓手机感染了广告软件、信息窃取软件和勒索软件等多种多样的恶意软件病毒。

研究员丹尼尔·帕东 (Daniel Padon) 指出，这 38 款手机的主人都是 Check Point 的客户，他们或在一家大型电信公司工作，或在一家跨国技术公司工作。帕东并没有透露这两家公司的名称，也没有说明它们是否来自同一个国家或地区。

这些手机在到达用户手中之前，就已经被安装了恶意软件，而这并不属于供应商原始 ROM 的一部分。对于其中的 6 款手机来说，攻击者拥有手机的系统权限，如果不重新刷新手机就无法删除恶意软件。

“居然有这么多款手机被感染了，我们对此很吃惊，这实在有些奇怪”，“我们很想知道，攻击者是如何选择目标的，他们为何感染了这么多不同的设备？” 帕东这样说道。

帕东推测这些设备可能是在零售点被篡改的，而这些手机则卖给了上文提到的两家公司。所有 38 款手机都已经通过 Check Point 的产品进行了修复，帕东认为以后还会有更多设备遭到类似的感染。他还表示，Check Point 确定了原始 ROM 是何时安装的，然后在几周、几个月，甚至一年后，恶意软件在用户激活 ROM 之前就被添加到了 ROM 中。

“这同时也引发了攻击意图的问题”。帕东说：“我们认为一种恶意软件只感染一种设备。但是在该案例中，我们发现了不同的恶意软件。可能是有人在做实验，或者这只是一些没有联系的事件”。

Check Point 发现 6 款设备感染了 Loki 木马，这是一个已经传播了一年多的恶意网络广告。Loki 通过展示广告来创造收入，保持持续性的机制，能够拦截安卓设备的通信并渗漏其数据。他们还发现有些设备感染了 Slocker 移动勒索软件的病毒，该勒索软件能够加密设备上的文件，并使用 Tor 网络进行 C&C 通信。

“主要问题在于，这种攻击的潜在风险是很巨大的”，Padon 说。如果攻击者在设备返回供应链之前能够接触它们，那么即使用户从未点击过可疑链接，从未打开电子邮件附件或下载网络钓鱼应用程序，他们也会遭到恶意软件的感染。”

Check Point 发布了恶意软件的名称和哈希值，以及受感染的设备型号，其中包括：

- Samsung Galaxy Note 2
- Samsung Galaxy Note 3
- Samsung Galaxy Note 4
- Samsung Galaxy Note 5
- Samsung Galaxy Note 8
- Samsung Galaxy Note Edge
- Samsung Galaxy S4
- Samsung Galaxy S7
- Samsung Galaxy A5
- Samsung Galaxy Tab S2
- Samsung Galaxy Tab 2
- LG G4
- Xiaomi Mi 4i
- ZTE x500
- Google Nexus 5
- Google Nexus 5X
- Oppo N3
- Vivo X6 plus
- 5 Asus Zenfone 2
- Lenovo S90
- OppoR7 plus
- Xiaomi Redmi
- Lenovo A850

帕东表示，这是 Check Point 第一次调查此类手机供应链篡改事件。

此前，Kryptowire 的研究人员曾透露，相关科技公司生产的手机使用 BLU 产品 R1 HD 手机的无线更新系统，未经许可地监控用户。

原文名称	38 Android Devices Infected with Malware Preinstalled in Supply Chain
作者简介	Michael Mimoso，Threatpost 的编辑。
原文信息	2017 年 3 月 13 日发布于 Threatpost 原文地址 https://threatpost.com/38-android-devices-infected-with-malware-preinstalled-in-supply-chain/124275/
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《Neutrino Bot 家族样本分析报告》

近日，安天 CERT(安全研究与应急处理中心) 发现 Neutrino Bot 家族样本自新年之后开始活跃。经分析，攻击者冒充微软安全人员，发送含有恶意文档链接的电子邮件，引诱受害者打开并启用文档中包含的恶意宏，进而下载 Neutrino Bot 家族样本。该家族具有劫持 DNS 请求，实施 DDoS 攻击，下载其他恶意代码，窃取用户敏感数据，如击键记录、屏幕截图等等恶意行为。Neutrino Bot 家族在一年前已经开始在黑市上售卖，它以打包的形式出售，其中包含一个生成器，一个 C&C 面板和一个恶意的载荷文件。

目前，泄露出的生成器版本为 v3.9.4，它由 VisualStudio 2013 编写，功能非常简单，只需要填入 C&C 地址就可以生成。与原始载荷不同的是，生成器生成的版本会将攻击者提供的 URL 加密并存放在特定的位置。安装自带的控制面板后，攻击者可以对受感染的客户端进行多种操作，包括“DDoS”、“Find File”、“Cmd Shell”、“Keylogger”、“Update”、“Visit URL”、“Bot Killer”、“DNS Spoofing”等。

本次出现的 Neutrino Bot 家族样本首先安装自身，在 %APPDATA% 下创建了文件夹“UmJn”，该文件名代表的是 NeutrinoBot 的版本。接下来恶意代码开始连接 C&C 获取攻击者的恶意指令，请求的 URL 地址是硬编码在样本之中的，使用了 Base64 加密。解密之后可以得到四个 php 页面地址。关于身份验证，在之前的版本中，它发送一个硬编码的 cookie，值为字符串“admin”的 md5，而本次则将该字符串更换为了“just for fun”。本次的 5.2 版本比之前的 3.9.4 版本有了一些改变，分离了一些实现功能的函数，增加了攻击者对代码的可控性，其次取消了可以使分析人员看出攻击者意图的字符串，并且一些重复使用的函数会被动态加载以降低代码的可读性。

最近一段时间，使用包含恶意宏代码文档的钓鱼邮件、垃圾邮件来进行攻击的事件越来越常见。它们伪装成订单、发票或大公司，通过诱惑性的文字和图片引诱用户开启宏，下载恶意代码，进而窃取用户敏感数据。安天提醒网络使用者，除非完全信任该文件或在虚拟环境中运行，否则不要启用宏及点击邮件中的链接。

目前，安天追影产品已经实现了对 Neutrino Bot 家族样本的检出。

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、安全云鉴定器等鉴定分析。

最终依据静态分析鉴定器将文件判定为木马程序。

根据动态行为 (默认环境) 得出该文件具有以下行为：延时、获取计算机名称、设置调试器权限、查找指定内核模块、独占打开文件、获取 socket 本地名称、连接网络、遍历进程。

文件名	./ca64848f4c090846a94e0d128489b80b452e8c89c48e16a149d73ffe58b6b111
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	78 KB
MD5	084F562DA639BD4BFC6B92B7D5CDC014
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Invader
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

◆ 危险行为

行为描述	危险等级
延时	★★★

◆ 其他行为

行为描述	危险等级	行为描述	危险等级
获取计算机名称	★	设置调试器权限	★
查找指定内核模块	★	独占打开文件	★★
获取 socket 本地名称	★	连接网络	★★
遍历进程	★		

报告地址：https://antiy.pta.center/_lk/details.html?hash=084F562DA639BD4BFC6B92B7D5CDC014