安天发布《“刑天”RAT 木马样本分析报告》

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一款新出现的 RAT 后门木马。该木马为国产软件“刑天”，对外有免费测试版和付费版，可用于网站测试和非法活动。远控启动后，会先进行安装。在注册表中注册设置好名字的服务，释放 dll 并将自身更新到封装 dll 的资源节中，之后启动服务。服务启动后，将加密的 C2 服务器地址解密然后进行连接，同时开启线程进行内网 IPC$ 攻击，循环运行等待 C2 服务器发送指令进行 DDoS 攻击。释放的 dll 启动后，检测同名互斥量是否存在，如果不存在，则从资源节中释放出原文件并执行。

样本会将自身复制到 C 盘 Windows 目录下，重命名为六位随机字符的 EXE 可执行文件。然后删除自身文件并调用 ShellExcuteExA 执行复制后的文件。将文件自身更新到资源节中并释放资源节到 %system32% 目录下，资源节为 dll，更新完成后程序将成为 dll 的资源节。接下来创建线程使用穷举 IP 的方式对内网进行 IPC$ 攻击，爆破的密码字典为硬编码。横向渗透完成后，解密 C2 地址并连接，回传系统信息，如 CPU 频率、内存大小、网卡速率、语言类型、系统版本等，而且会等待 C2 服务器指示，进行相应 DDoS 攻击、命令执行、删除服务等操作。

安天 CERT 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木马样本的检出。

木马程序

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

文件由页面手工提交，经由 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。

最终依据静态分析鉴定器、动态行为鉴定器、智能学习鉴定器将文件判定为木马程序。

文件名	49a2433466d276d400192190f49ee848
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	44 KB
MD5	49A2433466D276D400192190F49EE848
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Rootkit]/Win32.Lapka.an
判定依据	静态分析

◆ 静态启发式检测

检测类型	检测点	详细说明
PE 结构	无版本信息并且不是 GCC 编译器	除 GCC 编译器外，常规编译器均默认包含版本信息。如果不是 GCC 编译器，并且不包含版本信息，显然是作者故意抹掉版本信息，逃避追查。

◆ 文件元数据分析

描述	值
File Type	Win32 EXE
MIME Type	application/octet-stream
Machine Type	Intel 386 or later, and compatibles
Time Stamp	2014:05:18 21:54:01+08:00

◆ 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	附加信息	
使用 cmd 删除自身	★★★★	CommandLine	"C:\WINDOWS\system32\cmd.exe" /c del C:\39FEC7~1\share\target.exe > nul
删除自身	★★★★	FileName	C:\39FEC7~1\share\target.exe
延时	★★★	Sleeptime	0x0000EA60

◆ 访问 IP

IP 地址	端口	归属地	域名
127.0.0.1	2000	IANA	N/A
127.0.0.1	1028	IANA	N/A

◆ TCP 信息

源 IP	源端口	目的 IP	目的端口
127.0.0.1	null	127.0.0.1	2000

安天周观察
安天官方微博 安天官方微信
主办：安天 2018 年 01 月 22 日 (总第 121 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

安天联合电信云堤共同揭秘物联网僵尸网络 Gafgyt 家族与 NetCore 53413 后门的背后故事

近日，安天捕风小组与电信云堤联合发布了分析报告，对物联网僵尸网络 Gafgyt 家族利用 NetCore 53413 后门事件进行了分析。

NetCore 为国内电子厂商生产的一系列路由器产品，其在 2014 年便被披露存在高权限后门。此次 NetCore 53413/UDP 后门被国外物联网僵尸网络 Gafgyt 家族利用，可见目前互联网上仍存在大量具备该后门的路由器设备，易成为高危的潜在“肉鸡”。报告对 53413 端口后门的利用过程和关联捕获到的 Gafgyt 样本木马功能及攻击协议进行了分析。

结合 Gafgyt 样本分析，发现其 Tel/SSH 扫描爆破的 IP 网段重点分布在越南（占比 33.04%）、中国（占比 26.08%）以及其他亚洲国家（占比 17.82%），其地理位置与 NetCore 产品的主要销售对象重合度很大。通过安天捕风蜜网系统单日捕获的流量和云堤关联流量分析识别，全国有 33230 台“肉鸡”在线尝试与指定 Gafgyt 家族僵尸网络 C2 连接。由此可见，NetCore 53413/UDP 后门端口与 Gafgyt 家族僵尸网络的结合，对我国互联网安全存在较大威胁。

近年来，物联网行业迅速发展，市场需求和经济利润不断增长，但因盲目追求产品的功能进度，许多物联网设备忽略了安全的重要性，存在各种类型的高危漏洞。物联网设备基数大、高危漏洞多、防御措施少、监管措施不足，为物联网僵尸网络的形成带来了便利，也给互联网安全和日常的生活工作造成了日趋严峻的威胁，维护网络安全发展仍然任重道远！

详细报告请扫描二维码：

松北区妇联主席一行莅临安天参观调研

1 月 18 日下午，哈尔滨市松北区妇女联合会（以下简称妇联）主席一行莅临安天参观调研，安天首席财政官邵丹向来宾做了介绍，并组织召开了妇联筹备工作会议。

在安天展厅，邵丹向来宾介绍了安天的发展成长、所获专利荣誉及所参与过的应急安保项目。妇联主席表示，在网络安全这样一个有来自多方公开竞争的领域，安天始终坚持自主研发是非常不易的，安天所做的工作对国家的发展至关重要，不负总书记民企国家队的称号。

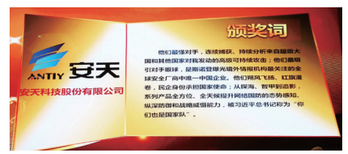
随后，邵丹、安天哈尔滨总部总经理李岱及各部门负责人与松北区妇联主席一行就安天建设妇联的相关事宜进行讨论。邵丹对安天现有的员工情况及以母婴室为代表的关爱女员工人文关怀行动进行了介绍，并表示安天将从心理疏导、女性人格独立、艺术文学等方面继续开展多样的关怀女员工活动。松北区妇联主席表示，创立妇联通常情况下都属政府行为，安天主动申请加入妇联开创了松北区“企业进妇联”的先河，具有一定的历史意义。

松北区妇联主席一行参观安天展厅

安天获评“2017 网信军民融合年度优秀企业”

近日，第十二期钱学森论坛深度研讨会暨首届网信军民融合峰会在厦门举行，安天被评为“2017 网信军民融合年度优秀企业”。

本次会议由中国工程院、中央军委军事科学院、中国航天科技集团公司、福建省人民政府指导，中国航天系统科学与工程研究院、中国航天工程科技发展战略研究院、军事科学院系统工程研究院、厦门市人民政府主办，以“钱学森智库聚焦网信强国”为主题，旨在贯彻落实党的十九大精神，激发网络强国和军民融合的战略共振效应，将习总书记战略清晰的号召力，转化为万众一心的执行力，推动网信领域军民一体、良性互动、协调发展。



每周安全事件

类 型	内 容
中文标题	RubyMiner Monero Cryptominer 仅在 24 小时内就影响了全球 30%的网络
英文标题	RubyMiner Monero Cryptominer affected 30% of networks worldwide in just 24h
作者及单位	Pierluigi Paganini; SecurityAffairs
内容概述	RubyMiner上周首次被发现是在全球范围内针对网络服务器进行的大规模活动，其中大部分是在美国、德国、英国、挪威和瑞典。 专家们认为，攻击的幕后主使是一个单独的攻击者，就在一天之内，他试图对全球近三分之一的网络进行破坏。该恶意软件针对 Windows 和 Linux 服务器，试图利用 PHP，Microsoft IIS 和 Ruby on Rails 中的旧漏洞来部署 Monero 矿工。 攻击者在 POST 请求内发送一个 base64 编码的有效载荷，企图诱骗解释器执行它。 恶意负载是一个 bash 脚本，它添加一个每小时运行一次的 cronjob，并下载一个包含 shell 脚本的 robots.txt 文件，用于获取并执行 cryptominer。调度程序被告知运行整个过程，包括每小时从服务器下载文件。 专家认为，robots.txt 文件也可以用作 RubyMiner 的 kill 开关，修改受感染的 web 服务器上的 robots.txt 文件，可以停用恶意软件。
链接地址	http://securityaffairs.co/wordpress/67865/malware/rubyminer-monero-cryptominer.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 10 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.WikoSpy.a[prv,rmt,spy] 2018-01-15	该应用程序运行后请求超级用户权限，远程控制，可能会私自安装未知应用、获取超级用户权限、私自发送短信、监听接收的短信上传到指定网址等，可能造成隐私泄露和资费消耗，建议立即卸载。（威胁等级中）
		Tool/Android.UsbPx.a[prv] 2018-01-15	该应用程序是一款测试工具，电脑和手机建立连接，然后使用电脑远程控制手机拨打电话、发送短信，请谨慎使用。（威胁等级低）
		Trojan/Android.mmcspy.a[prv,spy] 2018-01-15	该应用程序伪装成系统应用，安装无图标，开机自启动，激活设备管理器，通过 WiFi 采集地理位置，窃取通话记录，通话录音，环境录音，通过辅助助手监听微信的活动记录，对用户的个人隐私造成极大的威胁，建议立即卸载。（威胁等级中）
		Trojan/Android.Sysddl.a[exp] 2018-01-16	该应用程序伪装成系统应用，无实际功能，动态加载恶意子包，私自下载安装未知应用并启动，造成用户资费损耗，请卸载。（威胁等级中）
		Trojan/Android.Beeg.a[exp] 2018-01-18	该应用程序运行后隐藏图标，关闭 wifi，联网加载色情视频，通过加载脚本，私自点击播放，后台启动挖矿程序，占用设备 CPU，消耗手机性能，造成用户资费损耗，损耗用户设备，请立即卸载。（威胁等级中）
		Trojan/Android.flyfishdownload.a[exp,prv,rmt] 2018-01-18	该应用程序安装无图标，开机自启动，解密释放恶意子包，联网获取配置信息，下载未知应用，静默安装，上传硬件信息，造成用户大量资费消耗，且对用户的隐私造成一定威胁，请立即卸载此类应用。（威胁等级高）
		Trojan/Android.KotlinHrx.a[prv,exp,rmt] 2018-01-18	该应用程序包含恶意代码，运行后私自发短信，上传用户固件信息，接收网络远程指令，执行 URL 转发并点击广告欺诈，上传用户服务提供商的信息、登录信息、验证码图片，获取订阅信息私自订阅，造成用户隐私泄露和资费损耗，请立即卸载。（威胁等级高）
		Trojan/Android.HmdRat.a[prv,rmt] 2018-01-18	该应用程序为远控程序，运行后接收远程控制命令，进行私自录音、下载软件等行为，并上传至服务器，造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.yichuwm.a[prv] 2018-01-19	该应用程序包含恶意支付插件，运行会拦截短信并上传到指定网址，会造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.kainin.a[rog,sys] 2018-01-20	该应用程序伪装成 wifi 工具，运行诱导激活设备管理器，而后重启手机，清除用户数据，会造成用户数据丢失和系统破坏，建议立即卸载。（威胁等级中）
PC平台恶意代码	活跃的格式文档漏洞、0day 漏洞	微软 Office 公式编辑器爆出远程代码执行漏洞（CVE-2018-0802）	Microsoft Office 软件中爆出远程代码执行漏洞，CVE 编号 CVE-2018-0802，攻击者可以利用此漏洞，在当前登录用户的上下文中执行任意代码。失败的攻击尝试可能会引发 DDoS 攻击，全部版本受影响。（威胁等级高）
	较为活跃样本	Trojan[Dropper]/Win32.Injector	此威胁来自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AcitveX 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[Backdoor]/Win32.AutoIt	此威胁来自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[Banker]/Win32.Banbra	此威胁来自一种以窃取网络银行敏感信息为目的的木马类程序。该病毒伪装成正常数据，以获取认证。该病毒利用各种途径，使黑客获得数字证书来伪造文件。该家族还会收集用户的机密信息，如网上银行详细信息和密码等，并将窃取的数据发送给远程黑客。（威胁等级中）

人工智能在网络安全方面的应用

Raffael Marty / 文 安天技术公益翻译组 / 译

安全从业者如何将专业知识融入到机器学习算法中，从而揭示安全迹象、保护数据并防御攻击者？

随着人工智能（AI）这一术语以及深度学习的日益普及，许多安全从业者开始认为这些方法是我们一直在等待的、能够解决所有安全挑战的“银弹”。但深度学习或其他任何机器学习（ML）方法——只是一种工具，而且不应单独使用。我们需要将专业知识融入到机器学习算法中，以揭示实际的安全迹象。

在下文中，我将不再使用“人工智能”这一术语，而是回归“机器学习”这个术语。我们还没有人工智能，更准确的说是通用人工智能（AGI），所以不要被这些错误的概念误导。

如今，机器学习在网络安全方面有何应用呢？我们首先需要看看我们的目标是什么：概括来说，我们试图用机器学习来识别恶意行为或恶意实体；这些被称为黑客、攻击者、恶意软件、不需要的行为等等。即利用机器学习发现异常情况。需要注意：要想发现异常情况，最大的挑战之一是定义什么是“正常”。例如，你能定义你的笔记本电脑每天的正常行为吗？不要忘了你最近下载的新应用程序，你如何区分它与攻击者触发的下载？抽象地说，只有一部分统计的异常涉及有趣的安全事件。

将机器学习应用于网络安全

机器学习可以分为两类：有监督机器学习和无监督机器学习。有监督机器学习在数据分类方面非常出色，比如学习某些东西是“好”还是“坏”。为此，这些方法需要大量的训练数据来学习这些数据类型是什么样的。有监督

算法学习训练数据的属性，然后利用习得的知识来分类新的：以前未知的数据。无监督机器学习在分析和理解大型数据集方面非常出色，但是不太擅长寻找异常。

有监督机器学习

在机器学习中，有监督机器学习对网络安全产生的影响最大。它的两个最重要的应用是恶意软件识别和垃圾邮件检测。如今的恶意软件识别方法从深度学习中获益匪浅，有助于将误报率降至极低，同时降低漏报率。恶意软件识别成效显著的原因是拥有数百万标记的样本（恶意软件和良性应用程序）或训练数据。这些样本使我们能够非常好地训练深度信念网络。垃圾邮件检测与此类似，我们有大量的训练数据来训练算法区分垃圾邮件和合法邮件。

在其他领域，我们则没有很好的训练数据，例如从网络流量中检测攻击。我们已经尝试了近二十年，希望为这些问题提供良好的训练数据集，但至今还未找到合适的。没有训练数据集，我们就无法训练算法。此外，我们还面临其他问题，如无法确定的标记数据、清理数据相关的挑战或理解数据记录的语义。

无监督机器学习

无监督机器学习非常适合数据挖掘，可以用来减少数据的维度或字段（降维），以查找或组合记录（聚类和关联规则）。然而这些算法在识别异常或攻击方面的用途有限。聚类或许可以用于发现异常，也许我们可以找到方法来聚类“正常”和“异常”的实体，如用户或设备？事实证明，根本问题在于安全领域的聚类受到良好的距离函数和聚类“可解释性”的困扰。您可以阅读此博客了解有关距离函数和可解释性挑战的更多信息。

背景和专业知识

除了已经提到的识别异常的挑战之外，还有一些重要的因素。第一个是背景。背景是指能够帮助我们更好地理解数据中存在的实体类型（设备、应用程序和用户）的任何信息。设备的背景包括设备的角色、位置、所有者等等。例如，我们不需要孤立地查看网络流量日志，而是添加背景信息来理解数据。知道哪些机器代表网络上的 DNS 服务器有助于了解哪些机器应该响应 DNS 请求。非 DNS 服务器响应 DNS 请求可能预示着攻击。

除了背景信息之外，我们还需要建立具有专业知识的系统和算法。这可不是随便抛出一个算法看看是否会产生有用的结果那么简单。知识捕获领域中一个有趣的方法是贝叶斯信念网络。有人做过这方面的研究么？敬请在评论中分享。

与其试图使用算法来解决真正的难题，我们还应该考虑构建有助于提高安全分析师效率的系统。可视化是一个不错的选择。与其让分析师查看数千行数据，不如让他们查看数据的视觉表示，从而在很短的时间内获得更深入的理解。另外，可视化也是验证和理解机器学习算法结果的一个很好的工具。

原文名称	AI in Cybersecurity: Where We Stand & Where We Need to Go
作者简介	Raffael Marty，Raffael Marty 是 Sophos 的安全分析副总裁，是全球公认的安全数据分析、大数据和可视化权威人士之一。
原文信息	2018 年 1 月 11 日发布于 Dark Reading 原文地址 https://www.darkreading.com/threat-intelligence/ai-in-cybersecurity-where-we-stand-and-where-we-need-to-go/a/d-id/1330787
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。