安天发布《Mirai 僵尸网络变种样本分析报告》

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发现一种新型的 Mirai IoT/Linux 僵尸网络变种。这个新变种利用了大量漏洞，针对各种嵌入式设备进行攻击，如路由器、网络存储设备、IP 摄像头、NVR 等。

最新的 Mirai 样本一共包含 27 个漏洞，其中 11 个是新增加的。值得注意的是，有两个新漏洞分别针对 WePresent WiPG-1000 无线演示系统和 LG Supersign 电视机，这两个设备都被应用于企业中，这意味着 Mirai 僵尸网络攻击面扩大，并且攻击对象正由个人用户转移到企业。这些瞄准企业网络设备进行的攻击，能为僵尸网络提供更大的带宽，从而能发动更大规模的 DDoS 攻击。除此之外，Mirai 的默认凭证列表中还增加了 4 个新的用户名密码组合，用于对设备的登录账户进行爆破。目前，该木马使用的恶意脚本被托管在哥伦比亚一家被入侵的公司的服务器上，讽刺的是，该公司从事“电子安全，集成和报警监控”服务。当设备被木马攻陷后，便成为 Mirai 僵尸网络的一部分，它会接收从 C2 服务器发送过来的命令，进行 DDoS 攻击，还会扫描互联网上其他公开了 Telnet 端口的 IoT 设备，尝试使用内部的默认凭证列表来接管这些设备，或者使用 27 个漏洞中的一个来攻击未打补丁的系统。

安天 CERT 提醒广大政企客户，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。确保没有任何计算机运行直接连接到 Internet 的远程桌面服务，而是将运行远程桌面的计算机放在 VPN 之后，只有使用 VPN 才能访问它们。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、YARA 自定义鉴定器、文件来源信息鉴定器、文件元数据鉴定器、动态（CentOS）鉴定器、反病毒引擎鉴定器、聚类分析鉴定器、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、动态行为鉴定器、反病毒引擎鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	00033b5b33b59ad88aa4f196c08eb7a6d2e6ab181ec729e8ed577d55f8b1f3ee
文件类型	BinExecute/Linux.ELF
大小	164 KB
MD5	60A775F4A99420644181D1DDBD2D6D1D
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Backdoor]/Linux.Mirai.s
判定依据	反病毒引擎

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=60A775F4A99420644181D1DDBD2D6D1D

◆ 运行环境

操作系统	内置软件
CentOS release 6.8 (Final)	默认、Firefox、LibOffice

◆文件扫描

文件名	文件 MD5	家族相似性	yara 扫描
null	60a775f4a99420644181d1ddbd2d6d1d	N/A	N/A

◆ 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	192.168.122.166	68
192.168.122.166	39164	192.168.122.1	53
192.168.122.1	53	192.168.122.166	39164
192.168.122.166	56620	192.168.122.1	53
192.168.122.1	53	192.168.122.166	56620
192.168.122.166	38094	192.168.122.1	53
192.168.122.1	53	192.168.122.166	38094
192.168.122.166	50078	192.168.122.1	53
192.168.122.1	53	192.168.122.166	50078
192.168.122.166	40654	192.168.122.1	53
192.168.122.1	53	192.168.122.166	40654
192.168.122.166	52039	192.168.122.1	53
.....	.....	.....	.....

安天周观察
安天官方微博 安天官方微信
主办：安天 2019 年 05 月 13 日 (总第 182 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

安天发布《响尾蛇 APT 组织针对巴基斯坦的定向攻击事件分析》报告

近日，安天 CERT 发现响尾蛇（SideWinder）APT 组织针对巴基斯坦进行的鱼叉式钓鱼邮件攻击事件。该 APT 组织疑似来自于南亚某国，最早活跃可追溯到 2012 年，主要针对巴基斯坦等国进行攻击，近两年内被安全厂商披露过多次攻击行动 / 事件，相关攻击事件见时间图。

时间图

本次事件是响尾蛇 APT 组织仿冒巴基斯坦信德省（Sindh）警察局向旁遮普省（Punjab）政府相关人士发送了一份标题为《警察紧急威胁等级常设作业程序行动准备颜色代码》为主题的恶意攻击邮件，邮件正文与近期南亚热点问题之一“反恐怖主义”相关，并在附件中包含恶意代码文档“STANDING OPERATING PROCEDURES FOR POLICE EMERGENCY THREAT LEVELS AND COLOR CODES FOR OPERATIONAL READINESS.docx”。攻击者利用两个文档漏洞最终投放木马程序，再通过木马接收远程服务器投放的恶意 JS 脚本文件执行指定的恶意行为。

本次事件中攻击者使用了两个文档漏洞，通过 HTA 文件进行初始恶意文件释放和配置，利用白加黑（对可信文件 credwiz.exe 加载的库文件 Duser.ll 进行替换）加载恶意载荷并连接远程服务器接收恶意 JS 脚本，具体攻击流程如流程图所示。

恶意文档打开后会触发 CVE-2017-0199 漏洞，显示掩饰文档并从以下链接下载并运行文件 main.rtf。

运行后会触发 CVE-2017-11882 漏洞，并从 http://cdn-in.net/includes/b7199e61/-1/7384/35955a61/final 下载一个 hta 文件（以下称作 final.hta）并执行。

final.hta 是一个 HTML 应用程序，它的

流程图

运行流程如下：

1. 首先寻找系统文件“C:\Windows\System32\credwiz.exe”。

2. 如果找到 credwiz.exe，则将它复制到“C:\ProgramData\drvr\srvc2.0\”目录下，并在该目录下写入 Duser.dll 文件。

3. 将“C:\ProgramData\drvr\srvc2.0\credwiz.exe”设为注册表自启动项。

4. 如果前三个步骤都执行成功，则向“http://cdn-in.net/plugins/-1/7384/true/true/”发送一条 HTTP GET 请求。如果前三个步骤有出错而导致操作终止，则将错误信息附在链接“http://cdn-in.net/plugins/-1/7384/true/true/”的最后，并发送该条请求。

final.hta 释放的 Duser.dll 为病毒文件，而 credwiz.exe 是合法的系统文件，credwiz.exe 的运行需要导入 Duser.dll，攻击者利用这一机制试图绕过安全软件检测。

credwiz.exe 运行后，Duser.dll 作为调用文件被导入。Duser.dll 运行后，每 10 分钟向链接 https://cdn-list[.]net/1SdYMUrbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/43c2a8fa/css 发送一次 GET 请求，然后解密返回的数据，得到一个 JavaScript 脚本并运行。

在我们的分析过程中，服务器端返回的 JS 脚本是用于收集系统信息，然后将这些信息组合成 JSON 数据格式，通过 HTTP POST 请求发送到以下链接，这种首先进行信息采集的攻击方式在 APT 攻击中非常普遍，攻击者会根据收到的信息对受害目标进行分析判定后采取进一步行动，如窃取信息、投放其他恶意程序等。

链接：http://cdn-list.net/1SdYMUrbdAfpgSt3Gv13U8Jca6qOvI4I2Fa1zSCT/-1/7384/134/7e711ada/res/css

收集的信息包括：

• 系统账户信息、操作权限、系统基本信息、硬件信息、网络适配器。

• 反病毒产品列表、已安装的程序、系统进程信息。

• 处理器配置、操作系统信息、时间区域、补丁信息。

• 文件目录列表。

响尾蛇（SideWinder）组织是近两年比较活跃的 APT 攻击组织，该组织的攻击目标主要在巴基斯坦等国，攻击手法采用涉及印度、中国和巴基斯坦军事边界为主题的英文网络钓鱼邮件，通过钓鱼邮件投递恶意载荷进行信息窃取。该组织十分擅长使用 Nday 漏洞、PowerShell、代码混淆技术和利用开源武器代码，相关报告还提及该组织有针对 Android 系统的恶意软件。据安全厂商公开资料和地缘关系分析来看，该组织很可能来自南亚某国，目前未发现相关活动与白象等相关威胁行为体的关联，但不排除是同一攻击背景来源方向或新的攻击组织或分支小组。

详情报告可扫描二维码阅读

每周安全事件

类 型	内 容
中文标题	研究人员披露利用新 0day 漏洞攻击细节
英文标题	Freedom Mobile 服务器泄露 1.5 万名客户数据
作者及单位	Zack Whittaker
内容概述	加拿大第四大蜂窝网络 Freedom Mobile 的 Elasticsearch 服务器泄漏了 500 万条日志，约有 15,000 名客户受到影响。数据库包含客户姓名、电子邮件地址、电话号码、邮政地址、出生日期、客户类型和 Freedom Mobile 等个人数据，Equifax 提交的信用检查的答案，包括申请被接受或拒绝的详细信息，以及明文形式存储的完整信用卡号、有效期和验证号。在 3 月 25 日至 4 月 15 日期间登录或修改 Freedom Mobile17 个零售点账户的用户信息遭到泄露，该公司表示事件源于 Apptium 管理的服务器配置错误。
链接地址	https://techcrunch.com/2019/05/07/freedom-mobile-data-leak/

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

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.Dropper.ct[exp,rog] 2019-05-05	该应用程序安装无图标，运行加载未知子包，警惕其频繁推送广告，造成用户资费消耗，建议卸载。（威胁等级中）
		Trojan/Android.FakeSystem.bc[exp,rog] 2019-05-06	该应用程序伪装系统升级应用，安装无图标，私自下载，诱导安装，还内嵌恶意代码，通过启动辅助服务私自模拟点击确认，会造成用户流量资费损耗，影响用户正常使用，请卸载。（威胁等级中）
		Trojan/Android.SyncDroid.a[prv,rmt,spy] 2019-05-07	该应用程序为间谍类应用，通过短信或联网获取远程指令，上传用户手机固件、短信、通话记录、位置等隐私信息，根据指令执行录音、打电话、发短信等危险行为，造成用户隐私泄露，建议卸载。（威胁等级中）
	较为活跃的样本	Trojan/Android.PreAMo.a[exp]	该应用哪个程序内嵌恶意代码，后台私自模拟点击广告，会造成用户流量资费损耗，请卸载。（威胁等级中）
		RiskWare/Android.yxzywbocai.a[exp,prv]	该应用程序是博彩应用，运行回传用户 imei、地理位置信息到指定网址，造成用户隐私泄露，请注意提示信息，避免财产损失。（威胁等级中）
		Trojan/Android.FakeInst.fi[pay]	该应用程序伪装壁纸类应用，无实际功能，运行私自发送扣费短信，造成用户资费损耗，请卸载。（威胁等级低）
		RiskWare/Android.iappFake.o[exp]	该应用程序用裕语言编写，伪装游戏辅助应用，运行诱导用户付费购买，无实际功能，建议不要使用。（威胁等级低）
		Trojan/Android.SmsSpy.bj[prv,rog]	该应用程序运行上传并删除用户短信，造成用户隐私泄露，建议卸载。（威胁等级低）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Microsoft XML 远程代码执行漏洞（CVE-2019-0790）	当 Microsoft XML Core Services 分析器处理用户输入时，存在远程代码执行漏洞。攻击者需要诱使用户点击电子邮件或即时消息中的链接诱使用户访问存在恶意代码的网站。当 Internet Explorer 分析 XML 内容时，攻击者可以远程运行恶意代码控制用户的系统。（威胁等级高）
	较为活跃样本	RiskWare[RiskTool]/Win32.ADInstaller	此威胁是一种风险软件家族。该家族的样本在安装后会修改浏览器默认的主页，并在用户搜索特定关键词的时候，在页面上弹出广告窗口。（威胁等级低）
		Trojan[Packed]/Win32.Hrup	此威胁是一种具有窃密行为的木马家族。该家族的样本在执行后会对自身进行更新，并执行特定链接处的文件，在窃取用户信息后连接到远程服务器进行回传。（威胁等级高）
		Trojan[Backdoor]/PHP.Pioneer	此威胁是一种 PHP 后门家族。该家族的样本会在网站留下后门，获取网站的各种权限从而实现对网站服务器部分目录的控制。（威胁等级高）
		Trojan[Monitor]/Win32.Perflogger	此威胁是一种能对系统进行监视的木马家族。该家族的样本以工具的形式出现，可以获取进程的资源占用情况，并在后台收集计算机相关的数据进行上传。（威胁等级中）
		GrayWare[AdWare]/Win64.MegaSearch	此威胁是一种带有广告行为的灰色软件家族。该家族可以感染微软的 64 位 Windows 操作系统。该家族伪装成搜索工具栏，在安装后会在用户的计算机上弹出广告。（威胁等级低）

实现安全架构的自动化

Laurence Pitt/ 文 安天技术公益翻译组 / 译

企业最大的网络安全挑战仍然是：如何持续保持领先于攻击者。在企业为安全漏洞打补丁的同时，新的漏洞会不断出现，并且成为下一次攻击的目标。犯罪分子已经开始使用自动化技术，如利用 AutoSploit 这类工具自动扫描网络并利用漏洞，或者控制代理，利用 Sentry MBA 在代理机器上执行“撞库”（credential stuffing）攻击。此外，攻击者还使用自动化工具来渗透网络、收集数据或创建用户帐户，为下一次攻击做准备。随着攻击者工具的成熟，将会出现更多的自动化攻击，例如由软件执行的攻击。企业是时候认真看待自动化技术了，并将其作为防御攻击的下一道防线。

妥善部署的自动化技术（编排工具、用于分析的数据、机器学习和人工智能）能够为不断变化的全天候威胁全景中的企业提供优势。

安全自动化架构使用各种技术来改善企业的安全态势，包括精确执行重复性任务，为日志文件分析等领域提供更强大的情报，在识别和遏制网络攻击方面完全取代人为干预等。虽然自动化技术很强大，但它并非解决安全问题的“银弹”。事实上，许多企业都在努力实施正确的安全自动化架构。

在决定如何、何时以及在何处实施正确的自动化功能，以提高生产力、降低成本、支持云部署并增强企业的安全态势时，需要考虑诸多因素。

获得董事会的支持

安全自动化很复杂，将影响整个企业的安全管理方式。该计划的第一步是获得董事会的支持，以防止出现障碍。此外，还需向董事

会提供全面的信息——不仅仅是自动化技术的成功经验，还有失败的教训和面临的挑战。

全面了解企业的安全态势

在确定必要的工具和合作伙伴之前，企业应对其安全态势进行全面的了解。例如，企业是否有任何集成问题或关键技术。一旦了解了当前的安全态势，就可以更容易地确定投资过多或不足的领域，或识别严重的风险。安全计划通常只关注负面问题和风险，例如未妥善管理的物联网。但实际上，物联网也是一个机会，可以将任何联网设备作为安全架构的一部分——例如创建动态安全策略来部署访问控制列表，从而识别非安全设备。

从小处着手

很多时候，企业会部署不恰当的自动化工具，或部署过多的自动化工具。这会增加不必要的部署成本和时间。安全工程师最具重复性的日常任务之一是，监控跨设备的日志文件以发现潜在风险。这就是部署自动化技术的一个不错的起点。安全工程师每天扫描相同的日志文件，但是可能会遗漏某些内容；而自动化扫描则会准确无误。

获取经验

一旦 IT 部门获得了自动化技术和工具的经验，他们就可以自动执行更复杂的任务了，例如威胁猎杀、事件驱动的自动化、取证和日志数据关联等主动措施。IT 团队一直不愿意从流程中删除人为因素，但是自动化意味着，IT 团队有时间专注于更具战略性的安全措施，以更好地保护企业。

持续测试

所有计划都需要持续测试。安全自动化涉及企业的多个领域，因此其测试更加重要。在被工程师发现之前，脚本中的用户错误可能会运行一次；但是自动化进程中的一个错误可能会运行数百次。

员工培训

自动化能够增强安全团队的主动性，使其专注于更具价值的工作。只有与必要的员工技能有效结合，自动化才能真正获得成功。如果员工存在技能差距，企业应考虑对他们进行培训，来弥补差距，使其熟悉自动化技术和工具。为员工制定持续的培训计划必不可少，以确保他们的技能不断更新。

网络安全领域涌现了各种产品，这些产品可以保护从文档和硬件到物联网的所有内容。但是，这给企业带来了巨大的管理负担，而企业的安全性也只是好了一点点而已。企业需要一种利用数据和网络基础设施获得更好的安全态势的方法。自动化安全架构是第一步——这是一项复杂的工作，但是，只要部署得当，将有助于企业安全防御者保持对攻击者的先发优势。

原文名称	You Want to Automate Your Security Architecture - Now What?
作者简介	Laurence Pitt。Laurence Pitt 是 Juniper Networks 公司的全球安全战略总监。
原文信息	2019 年 5 月 2 日发布于 Security Week 原文地址 https://www.securityweek.com/you-want-automate-your-security-architecture-now-what
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。