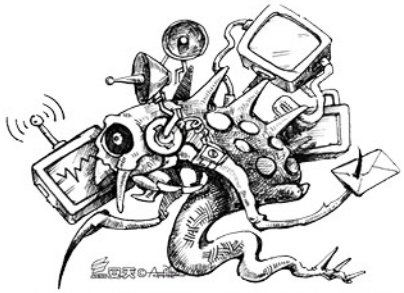
# 安天周观察

安天官方微博　安天官方微信

主办：安天　2018 年 09 月 24 日 ( 总第 153 期 ) 试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流


## 安天发布 APT 攻击组织“绿斑”分析报告



2018 年 9 月 19 日，安天发布了《“绿斑”行动——持续多年的攻击》分析报告，针对 APT 攻击组织“绿斑”（GreenSpot）多年来进行的攻击活动、攻击手法、攻击载荷、样本和组织的关联性进行了分析。为提升中国用户的安全意识，推动网络安全与信息化建设，安天公布这份报告。

“绿斑”攻击组织主要针对中国政府部门和航空、军事、科研等相关的机构和人员进行网络攻击，试图窃取机密文件或数据。目前可以确定该攻击组织的活跃时间超过 7 年，甚至可能达到 11 年以上。该攻击组织采用的主要手法是鱼叉式网络钓鱼攻击，即以邮件作为攻击前导，邮件附件使用有社工技巧的格式溢出文档或伪装为 EXE 可执行文件，进行定向投放，该组织对开源后门程序进行了大量改造，使其符合作业需要，并绕过主机防护软件。在该组织的攻击中，罕有使用 0day 攻击的情况，而反复使用陈旧漏洞，但其对漏洞免杀技巧的应用是熟练的，甚至是抢先的。在侵入主机后，通过加密和动态加载等技术手段，试图达成进入目标并在目标机器内长期潜伏而不被发现的效果。

网络入侵相对于传统空间的各种信息窃取破坏行为，无疑是一种成本更低，隐蔽性更强、更难以追踪溯源的方式。尽管“绿斑”组织不代表 APT 攻击的最高水准，但其威胁依然值得高度警惕。APT 的核心从来不是 A（高级），而是 P（持续），因为 P 体现的是攻击方的意图和意志。面对拥有坚定的攻击意志、对能够承受高昂攻击成本、团队体系化作业的攻击组织来说，不会有“一招鲜、吃遍天”的防御秘诀，而必须建立扎实的系统安全能力。以“绿斑”攻击组织常用的攻击入口邮件为例，不仅要做好身份认证、通讯加密等工作，附件动态检测分析，邮件收发者所使用终端的安全加固和主动防御等工作也需要深入到位。对于重要的政府、军队、科研人员，需要在公务邮件和个人邮件的使用条件和应用场景的环境安全方面，有明确规定和要求。邮件只是众多的攻击入口之一，所有信息交换的入口，所有开放服务的暴露面，都有可能成为 APT 攻击者在漫长窥视和守候过程中，首发命中的机会。

完整版报告请
扫描二维码进行阅读

## 安天省级态势感知平台应用案例获“2018 年网络安全解决方案优秀奖”

9 月 17 至 23 日，主题为“网络安全为人民，网络安全靠人民”的 2018 年国家网络安全宣传周在全国范围内统一举行。在 9 月 18 日成都主会区的“网络安全标准与产业分论坛”上，由安天承建的黑龙江省网络安全态势感知和应急处置平台（以下简称态势感知平台）荣获中国网络安全产业联盟颁发的“2018 年网络安全解决方案优秀奖”。

安天的态势感知平台有两个不同的版本，分别是针对主管和职能部门安全管理需求的监测型态势感知平台和应用于高资产价值、高威胁对抗、高防护等级场景的实战型态势感知平台。

黑龙江省态势感知平台是国家网信主管部门的首个省级试点，是安天监测型态势感知平台的重要案例。为贯彻落实习近平总书记“全天候全方位感知网络安全态势”的工作要求，黑龙江省网信主管部门率先启动了“网络安全态势感知和应急处置平台”的一期项目建设，并选择安天作为主承建方。

从网信地方主管部门的角度，不仅需要了解全省暴露在互联网上的信息资产风险，更需要对所管理范围内的重要系统和关键信息基础设施进行监测、分析、研判，指导安全规划、推送风险信息、指导应急处置，这是过去管理工作的盲点。安天按照“抵近部署，集中感知，有效防护，快速响应”的创新思路进行平台建设，将主机防护能力覆盖全省重要政府网站，并对部分重要信息系统和关键信息基础设施进行了流量监测能力的试点部署。监测结果与安天推送的威胁情报数据结合，初步展现了全省网络安全整体态势，对全省网络安全监测、预警、应急处置管理流程提供了支撑，提升了全省网络安全的管理能力。

综合来看，围绕监测管理需求的宏观态势感知只是态势感知的部分功能需求，面向中观态势和实战需求的能力和体系建设更为复杂。绝非一个简单的产品形态所能涵盖，而是由大量的基础能力环节和基础产品所支撑起的一个复合型的能力体系，涉及到持续监测、协同响应、工作流程管理、知识管理、大数据分析等方方面面，也需要深度包 / 载荷向量分析提取检测、向量标签化等深度安全能力为支撑。作为致力于“感知真实态势，做真态势感知”的团队，安天人深知自己任重道远。

# 每周安全事件

| 类 型 | 内 容 |
|---|---|
| 中文标题 | 西部数据 My Cloud 被发现权限提升漏洞 |
| 英文标题 | My Cloud NAS Devices Vulnerable to Auth Bypass for over a Year |
| 作者及单位 | Ionut Ilascu |
| 内容概述 | 研究人员发现了西部数据 My Cloud 平台中的一个特权提升漏洞 CVE-2018-17153，攻击者可利用该漏洞通过 HTTP 请求获得对设备的管理级访问权限，从而运行命令、访问存储的数据、修改 / 复制数据以及擦除 NAS。对 My Cloud 设备的身份验证过程会生成绑定到用户 IP 地址的服务器端会话。完成此步骤后，可以通过在 HTTP 请求中发送 cookie“username = admin”来调用经过身份验证的 CGI 模块。<br>一年多前，就有研究人员提出这个漏洞，但该公司拒绝承认或解决该问题。研究人员表示黑客很可能利用西部数据的产品漏洞进行勒索活动，并建议使用 NAS 设备的用户启用自动更新并且不要直接将设备暴露在互联网上。 |
| 链接地址 | https://www.bleepingcomputer.com/news/security/my-cloud-nas-devices-vulnerable-to-auth-bypass-for-over-a-year/ |

# 每周值得关注的恶意代码信息

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 平台的恶意代码值得关注

| 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.HzmaSpy.a[prv,rmt,spy] 2018-09-18 | 该应用程序运行激活设备管理器，隐藏图标，获取通讯录、通话记录、短信、文件等信息，并以 xml 格式私自上传，程序可以接受远程指令执行录音、拍照、删除文件等相关操作，会造成用户隐私泄露，建议卸载。（威胁等级中） |
| | | Trojan/Android.Spyzie.b[prv,rmt,spy] 2018-09-19 | 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、通话记录、通讯录、地理位置、浏览器记录、WhatsApp 记录、手机文件、邮箱信息等大量隐私信息，私自截屏、拍照、录音、录像，监听用户短信，私自提权。并将用户隐私上传至服务器，造成用户隐私泄露，建议卸载。（威胁等级中） |
| | | Trojan/Android.fbhzl.a[exp,rtt,rog] 2018-09-20 | 该应用程序包含恶意代码，运行后利用用户手机漏洞提权，频繁推广其他应用，并私自下载静默安装推广应用，卸载杀软。造成用户流量消耗，危害用户手机安全，建议卸载。（威胁等级高） |
| | 较为活跃的样本 | G-Ware/Android.Fakerdfs.a[pay,fra] | 该应用程序伪装游戏外挂，本身无实际功能，诱导用户付费使用，会造成用户资费损失，建议不要使用。（威胁等级低） |
| | | Trojan/Android.eracomteck.b[prv,rmt,spy] | 该应用程序是一款间谍软件，伪装其他应用，运行后接收远程控制指令，窃取用户短信、联系人、通话记录、浏览器记录、地理位置、手机安装软件信息、存储文件、硬件信息等大量隐私信息，私自拍照、录音、录像监听用户短信和通话，并将用户隐私上传至服务器，会造成用户隐私泄露，建议卸载。（威胁等级中） |
| | | Trojan/Android.shubham.a[prv,spy] | 该应用程序伪装成系统应用，运行后隐藏图标，接收远程指令，上传用户通讯录、通话记录、短信、位置、浏览器书签、相机照片等隐私信息，还能执行发送短信、拍照等危险行为，造成用户隐私泄露，建议卸载。（威胁等级中） |
| | | Trojan/Android.sostation.b[exp] | 该应用程序包含恶意代码，运行后加载恶意子包，检测用户手机是否 root，频繁加载推送广告，并私自下载推广，会造成用户流量消耗，建议卸载。（威胁等级低） |
| | | Trojan/Android.B4ASmsSend.c[exp] | 该应用程序包含风险代码，运行后隐藏图标，私自发送短信。造成用户资费消耗，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 | NUUO 摄像头系统 NVRMini2 未经身份验证的远程堆栈缓冲区溢出（CVE-2018-1149） | NUUO 摄像头 NVRMini2 系统具有缓冲区溢出漏洞，成功利用可远程执行代码，控制 NVRMini2 系统以及访问和修改 NVRMini2 系统中所有用户凭证数据。（威胁等级中） |
| | 较为活跃样本 | Trojan/NSIS.GoogUpdate | 此威胁是一种使用 NSIS 制作的具有下载行为的木马类程序。该家族样本运行后安装浏览器扩展，收集用户的浏览记录并推送广告，也有可能下载恶意程序。（威胁等级低） |
| | | GrayWare[AdWare]/Win32.ConvertAd | 此威胁是一种有广告行为的灰色软件类程序。该家族通常与正常软件捆绑到一起进行传播，它会在电脑上收集用户信息，并根据这些信息获取用户习惯并推送广告。（威胁等级低） |
| | | Trojan[Rootkit]/Boot.Cidox | 此威胁是一种可以修改 MBR 并在系统内核之前加载的木马家族。该家族通常以正常的应用程序伪装，会监控网络流量和击键组合，在电脑中留下隐蔽的后门，并试图攻击局域网内的其他机器。（威胁等级中） |
| | | Trojan[Downloader]/Win32.GLDCT | 此威胁是一种具有下载行为的木马类程序。该家族的样本会在执行后启动一个下载器来下载其他的恶意文件，并把自己添加到启动项中。在执行后会进行自删除，使得自己难以被察觉。（威胁等级中） |
| | | GrayWare[AdWare]/OSX.Bnodlero | 此威胁是一种具有广告行为的灰色软件类程序。该病毒家族的样本仅在 OSX 平台上运行，在安装后会产生广告弹窗。（威胁等级低） |

# 利用网络分割来保护物联网

John Maddison / 文　安天技术公益翻译组 / 译

如今，物联网（IoT）设备的快速部署，对网络安全产生了重大而持久的影响。在十多年前让 IoT 设备首次引人注目的“自带设备”（BYOD），主要包括手机和笔记本电脑等用户自有设备。即便如此，随着系统管理员将未受保护的设备集成到封闭网络中，网络犯罪分子很快开始利用这种新的攻击媒介。

## 物联网正以前所未有的速度发展

如今，这个问题更加复杂了。传统的手机被运行着大量应用程序的智能手机取代。与此同时，其他智能设备（如可穿戴设备和平板电脑）的使用也不断增加。一些专家估计，到 2020 年，每人将有 7 台设备联网。

然而，在系统管理员需要关注的设备中，最终用户设备只是冰山一角。其他 IoT 设备，从智能家电和库存跟踪器到联网医疗和职业治疗设备，也在以前所未有的速度激增。这种激增是大数据增长的关键驱动因素，并且导致网络流量大幅增加。专家指出，到 2023 年，全球将有近 320 亿台 IoT 设备，它们产生的移动数据流量将以 43% 的复合年增长率增长。

## 大多数 IT 安全架构都未做好准备

此类数据大多是加密的，源于需要在各种网络（包括多云环境）之间传输的应用程序和处理的业务。系统中已安装的安全设备处理当下的网络流量已经捉襟见肘，如果再加上处理 SSL 等加密流量，那么整体处理速度会更加缓慢，使得网络安全解决方案更加雪上加霜。然而，处于网络边界以及内部的网络安全设备还将其作为其主要功能设置。

对于在新兴数字市场中竞争的组织而言，网络安全跟不上是很糟糕的。更糟糕的是，经


验表明，用户认为一些安全措施是“瓶颈”，总能找到绕过它们的方法。对于安全团队而言，为了充分应用安全检查和协议而拖慢设备的速度，并不是一个好办法。然而，鉴于安全预算无法满足需求，他们无法升级到可以处理此类性能要求的安全设备。

即使这样，挑战也会变得更加复杂，因为组织需要确保数据在网络之间传输时实施一致的安全策略，这意味着组织需要在各种联网生态系统中部署具有相同功能的工具。

## 通过网络分割来保护物联网

我们的解决方案是：更聪明地运作。实现这一目标的关键是实施全面的网络分割策略，包括三个基本措施。

### 1. 建立广泛的可见性

大多数组织面临的最大挑战是，识别和跟踪连接到网络的所有 IoT 设备。网络访问控制能够帮助组织安全地对 IoT 设备进行身份验证和分类。在设备接入网络时对它们进行实时身份验证和分类，使 IT 团队能够构建风险配置文件，并自动将 IoT 设备以及相关策略分配给适当的设备组。

### 2. 将物联网与生产网络分割开来

一旦 IoT 设备连接到网络，IT 团队就需要建立 IoT 攻击面控制措施。将 IoT 设备和相关通信分割出来，归到基于策略的组和安全网络区域。这样一来，网络可以自动为特定 IoT 设备配置文件授权。虽然库存管理工具可以跟踪这些设备，行为分析可以监控其行为，但是还需要应用内部分割防火墙，这样不仅能够快速、动态地建立和控制网段，还能检查需要跨越网段边界的应用程序和其他流量。

### 3. 保护网络

建立策略驱动的 IoT 组，然后将它们（无论它们部署在分布式企业架构的何处）与内部网络分割相结合，实现基于活动的设备策略的多层监控、检查和实施。在这种集成的自动化安全框架下，当 IoT 流量流经网络时（甚至在不同网络生态系统中的设备之间传输时），隔离的安全设备能够将威胁情报关联起来。然后，这些集成工具可以自动将高级安全功能应用于任何 IoT 设备，或捕获网络中任何位置（包括接入点、跨网段以及跨多云部署）的异常流量。

组织不能再将 IoT 设备视为其业务的隔离或独立部分。IoT 设备及其相关数据与网络中的其他设备和资源进行交互，包括终端设备、多云环境以及日益互联的 IT 和 OT 网络。

传统上看，隔离的 IoT 安全解决方案不仅会增加成本，降低可见性，而且完全无法跟上当今 IoT 设备产生的流量。为了充分保护网络和 IoT 设备，组织需要可以跨越联网环境的广泛安全架构，以及可以动态分割 IoT 设备、同时快速检查其加密流量的强大安全工具。他们还需要深度集成一些安全解决方案，以便在分布式物联网的任何位置关联威胁情报、自动响应检测到的威胁。

| | |
|---|---|
| 原文名称 | Leveraging Segmentation to Secure IoT |
| 作者简介 | John Maddison。John Maddison 是 Fortinet 公司产品和解决方案高级副总裁。 |
| 原文信息 | 2018 年 9 月 13 日发布于 SecurityWeek<br>原文地址 https://www.securityweek.com/leveraging-segmentation-secure-iot |

# 安天发布《Ganiw Linux DDoS 木马分析报告》

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DDoS木马，其病毒家族名为Trojan[Backdoor]/Linux.Ganiw。该木马自2014年开始出现，拥有多个变种，该木马家族包含多个模块，包括atddd，cupsdd，cupsddh，ksapdd，kysapdd，skysapdd，xfsdxd等，分别负责不同的功能。

该样本原始文件名为sfewfesfs，属于模块cupsdd，比其他模块复杂。样本运行后首先从一个字符串中取值用于初始化变量，“116.10.189.246:30000:1:1:h:578856:579372:579888”，利用RSA算法进行解密，恶意代码释放并执行一个文件，该文件位于原始文件的偏移0xb1728，大小是335872字节。如果文件没有运行，恶意代码检查文件是否试图将一个套接字绑定到127.0.0.1:10808。如果尝试成功，这意味着该文件没有运行，它需要释放并执行。如果文件已经运行，样本会在/tmp/bill.lock中找到进程的PID并终止它，之后再释放并覆盖原文件。文件运行后，如果标志g_iIsService = = 1，该后门创建自启动脚本DbSecuritySpt /etc/init.d/，接下来文件读取配置文件，配置文件读取完成后，读取控制指令，该数据被储存在g_cmdDoing。之后，恶意代码获取所有必要的系统信息，包括：操作系统名称及内核版本（通过调用unname()）、CPU时钟频率（从/proc/cpuinfo中获取）、CPU核心数量（/proc/cpuinfo）、负载（/proc/stat）、网络负载（/proc/net/dev）、内存大小（/proc/meminfo）、网络接口信息（proc/net/dev），所有这些数据被存储在g_statBase结构体中。恶意代码会开启多个线程，同时执行几个额外的操作，最后从C&C接收并处理命令。

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。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、静态分析鉴定器、动态行为（LinuxCentos）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、静态分析鉴定器、智能学习鉴定器将文件判定为木马程序。

### ◆ 概要信息

| | |
|---|---|
| 文件名 | oledbg.dll50e3c0c9f6827aa3b6a8922e7b5d892fe69cb542af4d5c0f745f6ea92afe3f02 |
| 文件类型 | BinExecute/Linux.ELF |
| 大小 | 1.24 MB |
| MD5 | F9AD37BC11A4F5249B660CACADD14AD3 |
| 病毒类型 | 木马程序 |
| 恶意判定 / 病毒名称 | Trojan[Backdoor]/Linux.Ganiw.a |
| 判定依据 | 静态分析 |

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=F9AD37BC11A4F5249B660CACADD14AD3

### ◆ 运行环境

| 操作系统 | 内置软件 |
|---|---|
| Centos release 6.8 (Final) | 默认、Firefox、LibOffice |

### ◆ 文件元数据分析

| 描述 | 值 |
|---|---|
| File Size | 1265 kB |
| File Type | ELF executable |
| MIME Type | application/octet-stream |
| CPU Architecture | 32 bit |
| CPU Byte Order | Little endian |
| Object File Type | Executable file |
| CPU Type | i386 |

### ◆ 常见行为

| | |
|---|---|
| 获取CPU信息 | ★ |
| 获取内存使用情况 | ★ |
| 连接网络 | ★ |
| 获取网卡信息 | ★ |
| 释放PE文件 | ★ |

### ◆ 进程监控

| PID | 创建 | 命令行 |
|---|---|---|
| null | /.061837107499/analyzer/../share/target.elf | [/.061837107499/analyzer/../share...] |
| null | ba4dfc2462e8d1e846d220bdb65bc411 | [sh,-c,/.061837107499/share/target.elfh] |
| null | /bin/sh | [/.061837107499/share/target.elfh] |
| null | /.061837107499/share/target.elfh | [sh,-c,insmod/usr/lib/xpacket.ko] |
| null | /bin/sh | [insmod,/usr/lib/xpacket.ko] |
| ..... | ..... | ..... |