# 安天周观察

安天官方微博　安天官方微信

主办：安天　2018 年 04 月 30 日 ( 总第 133 期 ) 试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流


# 习总书记“4·19”重要讲话发表两周年之际 安天网络民兵分队成立


在习近平总书记关于网络安全和信息化工作重要讲话发表两周年之际，安天网络民兵分队正式成立。成立仪式在军地双方领导的共同见证下隆重举行，身着夏季迷彩服的安天工程师在一楼报告厅接受了部队首长的检阅。

安天网络民兵是结合安天自身网络安全防护处置的专业特点和技术积累，对接军民融合发展战略的一次创新性尝试，在 2017 年 6 月就提出了规划构想并进行了筹备，对此，人民日报曾发表了一篇题为《党管武装：“第一书记”担起第一责任》的新闻报道。

安天网络民兵分队由安天应急响应与分析处置工程师团队组成，在长期与境内外网络攻击威胁的对抗中，“安天赛博超脑”创新技术体系起到了重要的支撑作用，形成了在网络空间中的应急、处突、分析、追踪、溯源、证据固化等能力。

安天网络民兵分队的目标是在平时和战时，能够使用安天应急处置工具箱、便携版流量监测系统、便携版沙箱分析系统等网络安全应急处置和评估分析检测工具，对基于高级持续性威胁场景下的重要信息系统和关键基础设施进行预置、毁瘫、控制、篡改等深度的响应、取证和分析。平时适应持续性对抗，战时适应高强度对抗，针对平战皆为高成本对抗和无底线对抗的特点，提升防御能力、进行有效布防，强化东三省网信安全，保障我国在东北亚地区的地缘安全。

大会现场，民兵着装严整，歌声响亮，步伐整齐。部队首长宣读了网络民兵的任职命令，并要求广大民兵牢记习总书记重托，当好代表队，不断增强政治意识、责任意识和使命意识，将网络民兵分队打造成一支网络尖兵，确保在关键时刻能够拉得出、上得去、起作用，为国防建设和经济社会发展做出更大的贡献！

在新成员集体入队宣誓后，代表苗文起进行了发言，他表示：“作为网络民兵分队，我们将深入学习贯彻习总书记‘没有网络安全就没有国家安全’的重要讲话精神，凭借自身在网络安全方面的专业知识和能力来保卫国家安全和国家发展。”

安天网络民兵分队的成立，是军民融合的重要举措，此举将安天全体工程师凝聚起来，齐心协力保卫祖国，这也是安天作为网络安全国家队所肩负的责任和使命。

使命是永恒的，捍卫国家网络空间主权、确保网络安全，是新时代的重要使命和时代课题。我们不仅要在有形的传统战场上坚决维护国家主权、安全和发展利益，也要在无形的网络空间上消除威胁，维护我国网络空间主权，明确宣示我国主张。安天作为国内知名的网络安全能力型高科技企业，主动对接国防建设需求，推进科技兴军，为国防建设提供网络技术支撑和服务，全力建设军民融合的网络安全保障能力，为建设我国网络空间国防贡献自己的一份力量！

## 谷歌被指控侵犯 Android 用户隐私

来自美国某机构的技术与人权研究员表示，谷歌新推出的名为“Chat”的信息服务完全藐视了谷歌用户的隐私。他认为，端到端加密是最起码的隐私保护手段，提供会话服务的公司尤其应当注意。而谷歌的这项服务没有采取端到端加密，相当于把用户的会话和隐私拱手让给网络犯罪分子和监控机构。在 Facebook 事件尚未结束的当下，谷歌此举不仅无视用户隐私，甚至还侵犯了用户的人权。

除了“Chat”这个产品之外，谷歌的其他产品和功能也涉嫌无视用户隐私，Android Auto 就是其中一例。Android Auto 是谷歌专为汽车所设计的 Android 功能，可以连接手机，取代汽车的原生车载系统，执行 Android 应用，服务并访问、存取 Android 手机内容。这项功能能读取行车速度、冷却剂温度和油温、油门位置、引擎温度等大量用户信息，并实时传送给谷歌，这也违反了谷歌原定的隐私政策。

（来源：https://www.bleepingcomputer.com/news/google/google-accused-of-showing-total-contempt-for-android-users-privacy/）

# 每周安全事件

| 类 型 | 内 容 |
| --- | --- |
| 中文标题 | Google Project Zero 研究人员公开 Windows Lockdown 机制中的 0-day 漏洞 |
| 英文标题 | Google Project Zero hacker discloses a Zero-Day in Windows Lockdown Policy |
| 作者及单位 | Pierluigi Paganini |
| 内容概述 | Google Project Zero 研究人员近期公开了 Windows 10 的一个 0-day 漏洞，可被攻击者利用，在用户模式代码完整性（UMCI）的设备保护环境中绕过 Windows Lockdown 机制，攻击目标计算机并执行任意代码。根据发布的漏洞利用 POC，该漏洞代码主要包括两个文件：用于设置注册表的 .INF 以及使用 DotNetToJScript 免费工具创建的 .SCT（可用于将不可信的 .NET 程序集加载到内存中以显示消息框）。<br>研究人员表示，该 0-day 漏洞之所以被公开，是因为微软没有按照谷歌披露政策，在 90 天响应期内修复漏洞。目前，启用 UMCI 的 Windows 10 所有版本都有可能受到影响。 |
| 链接地址 | https://securityaffairs.co/wordpress/71689/hacking/windows-lockdown-policy-0day.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 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

| 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.CloudXSpy.a[prv]<br>2018-04-23 | 该应用程序运行窃取用户短信、通话记录、位置等隐私信息上传，造成用户隐私泄露，请卸载。（威胁等级中） |
| | | Trojan/Android.WxSpy.a[prv,spy]<br>2018-04-23 | 该应用程序伪装成系统应用，运行后隐藏图标，窃取用户短信、联系人、通话记录、位置、QQ 和微信聊天记录等隐私信息上传服务器，造成用户隐私泄露，建议卸载。（威胁等级高） |
| | | Trojan/Android.AsiaHitGroup.a[exp,prv]<br>2018-04-25 | 该应用程序伪装正常应用，运行后加载弹窗诱导点击，点击后会发送付费短信，后台监听收件箱，上传收件箱短信内容，造成用户资费损耗和隐私泄露，建议卸载。（威胁等级高） |
| | | Trojan/Android.Pornspy.a[prv]<br>2018-04-25 | 该应用程序伪装色情应用，运行上传用户短信、通讯录和通话记录，造成用户隐私泄露，建议立即卸载。（威胁等级高） |
| | | Trojan/Android.adups.a[rmt,bkd,sys]<br>2018-04-25 | 该应用程序内置在 ROM 中，会联网获取远程指令，执行下载、安装、卸载 APK 等危险行为；留有后门，可以执行任意命令，会给用户造成极大的安全隐患，建议卸载。（威胁等级高） |
| | | Trojan/Android.biquge.a[spr,exp]<br>2018-04-26 | 该应用程序运行后遍历用户联系人，并群发推广短信，造成用户资费消耗，建议卸载。（威胁等级中） |
| | | Trojan/Android.BasicfbSpy.a[prv,sys,exp]<br>2018-04-26 | 该应用程序运行后请求 Root 权限，可能私自上传用户社交软件 Viber 的数据到指定 ftp 服务器，删除用户数据，会造成用户隐私泄露和资费消耗，建议卸载。（威胁等级高） |
| | | G-Ware/Android.AccountInfoSpy.a[exp]<br>2018-04-27 | 该应用程序伪装游戏外挂，无实际功能，运行上传用户游戏账号信息文件，可能造成用户隐私泄露和资费消耗，建议卸载。（威胁等级中） |
| | 较为活跃的样本 | Trojan/Android.imobihome.b[prv,sys] | 该应用程序会获取 root 权限，上传用户手机 imei、电话号码等信息至远程服务器，造成用户隐私泄露，建议卸载。（威胁等级中） |
| PC 平台恶意代码 | 活跃的格式文档漏洞、0day 漏洞 | Adobe Flash Player 远程代码执行漏洞（CVE-2018-4878） | 攻击者通过构造特殊的 Flash 链接，当用户用浏览器 / 邮件 /Office 访问此 Flash 链接时，会被“远程代码执行”，并且直接被 getshell。CVE-2018-4878 是一个 UAF 漏洞，需要借助强制 GC 或者刷新页面来触发该漏洞。（威胁等级高） |
| | 较为活跃样本 | Trojan[Backdoor]/Win32.Hankydor | 此威胁是一种可以窃取用户信息的木马类程序。该家族样本运行后连接远程服务器接受攻击者恶意操作，收集用户信息并回传。（威胁等级中） |
| | | Trojan/Win32.Skintrim | 此威胁是一种可以下载恶意代码的灰色软件类程序。该家族样本运行后连接远程服务器下载恶意代码并安装，可以记录用户使用习惯推送广告，回传用户数据等。（威胁等级中） |
| | | Trojan[Downloader]/Win32.Axload | 此威胁是一种带有下载功能的木马类程序。该家族利用系统漏洞绕过反病毒软件，并禁用 Windows 防火墙，从而安装到用户电脑中。安装后，该家族会在开机启动项中添加注册表，并将自己捆绑到系统的核心部分，以确保自身难以被删除。（威胁等级中） |
| | | Trojan[Dropper]/Win32.Lmir | 此威胁是一种带有捆绑功能的木马类程序。该家族进入电脑后，会修改或破坏电脑文件、系统设置等，使系统性能变差。该木马可以盗取用户网络游戏传奇的账号与密码。该家族会在电脑中释放并安装其他恶意软件。（威胁等级中） |

# 网络犯罪：一项每年创收 1.5 万亿美元的产业

Joe Masters Emison / 文　安天技术公益翻译组 / 译

**根据一项关于网络犯罪“利润网”的新研究，威胁源每年产生、清洗、支出和再投资的资金超过 1.5 万亿美元。**

如果网络犯罪是一个国家，它将拥有全球第 13 位的 GDP（国内生产总值）。根据一项关于网络犯罪互联经济的新研究，攻击者每年获得 1.5 万亿美元的利润，这大概相当于俄罗斯的国内生产总值。

英国萨里大学犯罪学高级讲师迈克尔·麦奎尔（Michael McGuire）博士对网络犯罪世界中收入和利润的错综关系进行了名为“探析利润网”的研究。经过 9 个多月的研究，他了解到网络犯罪“产业”如何自我维持并与合法产业重叠。

这并非 Bromium 公司赞助该研究的初衷，该研究的初衷是了解网络犯罪分子如何花钱。“它变成了一项巨大的研究，探讨围绕网络犯罪系统的资金流动情况。”麦奎尔说。该研究与全球企业、渗透进暗网的安全工作人员、国际警方和犯罪分子进行了对话。

他的研究表明，类似平台资本主义模式的“平台犯罪”正在上升，在这个平台中，亚马逊和 Facebook 等企业使用的数据是商品。该平台将恶意软件转化为产品，简化非法工具和服务的购买，并实现了更广泛的犯罪活动，包括毒品生产、贩卖人口和恐怖主义。

麦奎尔说，自 2005 年以来，市场上出现了 620 多种新型合成毒品。许多是在中国或印度生产，在网上购买，并批量运送

到欧洲的。他发现，有证据表明，从网络犯罪中获利的组织也参与了毒品生产。暗网市场 Alphabay 的下线导致非法药物、有毒化学品、恶意软件以及被盗和欺诈性数据的清单被发现。

在网络犯罪分子每年产生的 1.5 万亿美元中，包括非法在线市场的 8600 亿美元，商业秘密和知识产权盗窃的 5000 亿美元，数据交易的 1600 亿美元，“犯罪软件即服务”的 16 亿美元以及勒索软件的 10 亿美元。有证据表明，网络犯罪往往比合法公司产生更多的收入：大型跨国犯罪活动的收入可能超过 10 亿美元，较小的活动收入通常在 3 万到 5 万美元之间。

现在是时候推进“网络犯罪就像一项业务”的观点了。“它远远不止是一项业务，”他说，“它就像一项镜像合法产业的‘产业’。我们发现，合法产业日益依赖网络犯罪产业。”

### 模糊的法律线

麦奎尔说，合法产业和非法产业之间的相互依存正在推动“利润网”，导致网络犯罪加剧。犯罪组织从真实公司获取数据和竞争优势，并利用它们实现其目标。其中的一个问题是，很多公司并不知道他们在推进网络犯罪方面发挥的作用。

Facebook 和 Uber 等公司拥有丰富的数据，因而成为寻求用户信息和知识产权的攻击者的重要目标。他们给黑客提供了一个销售非法商品和服务、设立假店来洗钱或联络买卖双方的平台。这些大型公司促成了犯罪驱动的经济。

麦奎尔发现，网络犯罪平台的所有者是最大的赢家。每个黑客每年可能只能赚 3 万美元；而管理人员每份工作（只需 50 张信用卡）可以赚取高达 200 万美元。他们没有犯罪，但他们出售犯罪平台，他们的犯罪平台已经演变为为其买家提供服务、说明和技术支持的渠道。

麦奎尔分享了这些收入背后的一些数字。举例来说，一个零日 Adobe 漏洞售价高达 3 万美元，而一个零日 iOS 漏洞的售价则高达 25 万美元。一个恶意软件漏洞利用包售价大约 200–600 美元；一个 blackhole 漏洞利用包每月租金为 700 美元，年租金为 1500 美元。定制间谍软件售价为 200 美元，短信诈骗服务的费用为每月 20 美元，而“黑客租用”的每次小型攻击的费用为 200 美元左右。

大部分资金都被投入新的犯罪活动。犯罪分子将其收入的 20% 用于追加犯罪，这说明高达 3000 亿美元的资金用于驱动非法活动。

| 原文名称 | Cybercrime Economy Generates $1.5 Trillion a Year |
|---|---|
| 作者简介 | Kelly Sheridan。Kelly Sheridan 是 Dark Reading 的高级编辑。 |
| 原文信息 | 2018 年 4 月 20 日发布于 Dark Reading<br>原文地址 https://www.darkreading.com/vulnerabilities-threats/cybercrime-economy-generates-$15-trillion-a-year/d/d-id/1331613 |
| 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。<br>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《基于 Python 的广告件“PBot”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例基于 Python 的样本，它通过一个漏洞利用工具包（EK）传播，伪装成 MinerBlocker，但其是一种基于 Python 的广告软件。

漏洞利用工具包下载样本的下载器，该下载器的功能是下载包含所有恶意 Python 脚本的程序，名为 MinerBlocker。下载完成后会进行安装，安装过程是静默操作，安装目录为 %appdata%。其中在目录 js 中，可以发现一个 JS 脚本，它通过配置文件进行注入，可以攻击 Firefox、Chrome、IE 等主流浏览器。样本首先会将脚本插入到每个被访问的网站中，一旦被注入，攻击者就可以控制浏览器中显示的内容，并可以注入广告，也可以注入其他的恶意代码。同时，该恶意代码也可以使用伪造的证书替换合法证书。样本的注入功能由 Python 实现，注入的恶意 DLL 可以实现挂钩到浏览器，可解析证书以及负责发送和接收数据的函数，所有的请求都会被重定向到恶意代码，它可以作为代理，在途中改变数据，代理完成后，它将跳回原始函数，因此用户不会意识到任何功能的更改。

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、数字证书鉴定器、文件元数据分析鉴定器、动态行为鉴定器、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 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 | 22b823021d45299276285a0bbdfcc734f8ee95bb1a8c650030c9dbb4d8208fb0 |
| 文件类型 | BinExecute/Microsoft.EXE[:X86] |
| 大小 | 938 KB |
| MD5 | E5BA5F821DA68331B875671B4B946B56 |
| 病毒类型 | 木马程序 |
| 恶意判定 / 病毒名称 | Trojan/Win32.Graftor |
| 判定依据 | BD 静态分析 |

### 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 | |
|---|---|---|---|
| 延时 | ★★★ | Sleeptime | 0x0000EA60 |

### 常见行为

| | |
|---|---|
| 获取系统版本 | ★★ |
| 获取计算机名称 | ★ |
| 获取驱动器类型 | ★ |
| 查找指定内核模块 | ★ |
| 独占打开文件 | ★ |
| 读取自身文件 | ★★ |
| 获取主机用户名称 | ★ |
| 查找浏览器进程 | ★★ |
| 查找特定窗体 | ★ |
| 获取系统内存 | ★★ |
| 创建特定窗体 | ★ |
| 获取 socket 本地名称 | ★ |
| 疑似查找浏览器进程 | ★★ |

### 文件扫描

| 文件名 | 文件 MD5 | 家族相似性 | yara 扫描 |
|---|---|---|---|
| target.exe | e5ba5f821da68331b875671b4b946b56 | N/A | N/A |
| target.exe.dmp | 159e320dc73d513cea2a440a69fe81d6 | N/A | N/A |
| …… | …… | …… | …… |