安天周观察

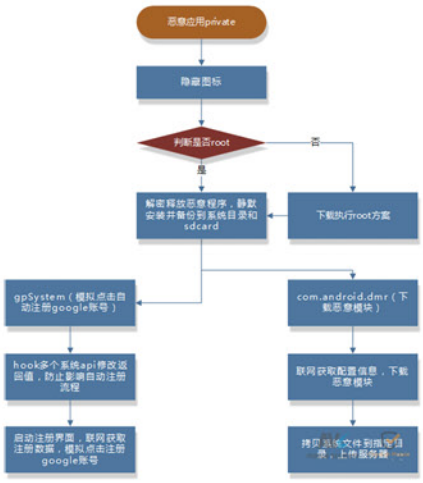
安天官方微博　安天官方微信

主办：安天　2018 年 07 月 23 日 (总第 145 期) 试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天移动安全发布《gpSystem：一种可私自注册 google 账号的病毒》分析报告

近期，安天移动安全和猎豹移动联合捕获到病毒 gpSystem。该病毒植入在应用程序 private 中，程序运行后便隐藏图标，进行下载提权相关文件、联网获取数据模拟点击注册 google 账号、上传用户账号、固件信息等一系列恶意行为，造成用户资费损耗和隐私泄露风险。

该病毒首先通过联网获取 root 方案，下载并执行提权模块，随后释放两个恶意程序，拷贝到系统目录以防被卸载。恶意程序通过辅助功能模拟点击注册 google 账号，并且通过修改系统函数返回值（忽略按键、锁屏无效等），防止其影响注册流程，以提高注册成功率。同时还会下载恶意代码，收集用户账号、authtoken（授权令牌）、固件、gcm、GooglePlay 等信息，可能用于配合自动注册相关行为。



恶意行为流程图

目前安天移动安全联合猎豹移动已实现对该病毒的检测查杀，建议用户安装猎豹安全大师等集成安天移动安全反病毒引擎的安全产品，定期进行病毒检测，一旦被感染应及时卸载恶意应用。

近年来，各种黑色产业链逐步形成，黑产的攻击手段也越来越专业化，会利用一系列手段进行自我保护，对此安全厂商应持续关注并提升对抗能力，为移动安全保驾护航。

扫描二维码
阅读报告原文

警告：移动支付 App Venmo 的 API 暴露其大多数交易记录

一名隐私提倡者发布最新调查结果表示，多数 Venmo 交易被记录在任何人均可访问的一个公共 API 中，原因是 Venmo app 默认将所有用户设置为“公开”。除非用户特别更改了这个值，否则他们通过 Venmo 转账 app 做出的所有交易都被记录且任何人均可通过 Venmo 公共 API 访问。通过该 API 暴露的数据包括发送人和收款方的姓名、Venmo 头像、交易日期、交易留言、交易类型等。

发现这个问题的隐私提倡者表示，他通过这一隐私策略查询 Venmo API 并下载了该公司所有 2017 年的公开交易记录，总计 207,984,218 条。他还建立了一个名为“Public by Default（默认公开）”的网站，列出了一些相互关联的 Venmo 支付案例，为该公司的某些客户创建了个人资料。例如，他不但追踪了与大麻经销商、玉米经销商、家庭、随机夫妇相关的交易，而且还追踪了一个有着 2033 次交易记录的妇女的故事。他还发布视频，说明 Venmo 用户如何将个人资料的设置从“公开”改为“私密”。

原文链接： https://www.bleepingcomputer.com/news/security/paypals-venmo-app-exposes-most-transactions-via-its-api/

西门子中继防护设备存在缺陷易受 DoS 攻击

西门子公司通知消费者称，其某些 SIPROTEC 中继保护设备的 EN100 通信模块中存在多个漏洞，导致其易受 DoS 攻击。SIPROTEC 设备为变电所提供控制、保护、测量和自动化功能。这些产品通过 IEC 61850、PROFINET IO、Modbus、DNP3 和 IEC 104 通信使用 EN100 以太网模块。

专注于工控和物联网安全的独立专家团队 ScadaX 发现 EN100 模块和 SIPROTEC 5 中继易受两个 DoS 漏洞攻击，攻击者可通过目标设备的 TCP 端口 102 发送特别构造的数据包。这些缺陷如遭利用可导致设备的网络功能进入 DoS 条件，西门子公司表示其会导致系统的可用性遭攻陷，恢复受影响服务需进行手动干预。

虽然这些漏洞之间存在相似之处，但其中一个漏洞 CVE-2018-11451 被评级为“高危”程度，而另外一个漏洞 CVE-2018-11452 影响示波器运行状态下的 EN100 模块，它被评为“中危”漏洞。西门子公司表示 SIPROTEC 5 中继仅受其中更严重缺陷的影响。

目前，西门子公司已为受影响设备发布固件更新以解决这些缺陷问题，并建议用户通过外部防火墙拦截对端口 102 的访问权限以阻止针对补丁尚未发布的系统的攻击。

原文链接： https://www.securityweek.com/flaws-expose-siemens-protection-relays-dos-attacks

每周安全事件

类 型	内 容
中文标题	美国最大的血液检测实验室 LabCorp 被黑
英文标题	US Biggest Blood Testing Laboratories LabCorp suffered a security breach
作者及单位	Pierluigi Paganini
内容概述	LabCorp 是美国最大的血液检测实验室，近日其发表声明称遭到了黑客的非法入侵。 根据该公司发表的官方声明，攻击者只入侵了 LabCorp 的诊断系统，目前还没有任何证据可以表明攻击者还成功入侵了 LabCorp 的药物研发系统。除此之外，调查人员还没有发现泄漏的数据被非法利用。LabCorp 已经将此次事件上报给了有关部门，并会积极配合取证人员的调查活动。 需要注意的是，此次攻击事件可能会让数百万美国公民陷入安全风险之中。不仅因为客户数据可能发生泄漏，更重要的是 LabCorp 的网络系统连接了全球上千家医院和检测机构。
链接地址	https://securityaffairs.co/wordpress/74536/data-breach/labcorp-security-breach.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 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.FakeGoogleNetwork.a[prv,spy] 2018-07-16	该应用程序伪装谷歌邮箱登陆程序，运行激活设备管理器，隐藏图标。上传用户输入的登陆账号密码，手机中的图片、视频，Facebook 相关资料等。造成用户隐私泄露，建议卸载。（威胁等级中）
		Tool/Android.Tiny.a[sys] 2018-07-16	该应用程序是免流工具，利用网络运营商漏洞来实现免流的功能，请谨慎使用。（威胁等级低）
		Trojan/Android.dataSpy.a[prv,exp,spy] 2018-07-18	该应用程序伪装系统应用，运行窃取用户短信、通讯录、浏览器历史记录和书签、社交应用数据信息，监听短信、拦截指定短信、发送短信，造成用户隐私泄露和资费消耗，建议卸载。（威胁等级高）
		Trojan/Android.FakeIns.a[prv,rog] 2018-07-18	该应用程序伪装 Instagram，运行加载子程序，访问虚假钓鱼网站，窃取用户填写的账号密码信息，可能造成用户隐私泄露，建议不要使用。（威胁等级中）
		G-Ware/Android.huixinyt.a[prv,rog] 2018-07-18	该应用程序运行无提示，发送包含用户手机号的邮件到指定邮箱，会造成用户隐私泄露，建议不要使用。（威胁等级低）
		RiskWare/Android.ApKCreaTor.a[fra] 2018-07-18	该应用程序是在线工具生成的，运行访问指定网址，其内容具有一定的风险性，可能是仿冒、伪造的网站，还包含广告，请谨慎使用。（威胁等级中）
		Tool/Android.oozhushou.a[sys] 2018-07-18	该应用程序为圈圈助手游戏修改工具，可修改游戏参数，部分功能需要 root 权限，请谨慎使用。（威胁等级低）
		Trojan/Android.MsgMonitor.a[prv] 2018-07-19	该应用程序伪装系统应用，运行后监听短信和通话记录，通过发邮件方式上传，造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.TpOsm.a[prv,exp] 2018-07-20	该应用程序运行后监听用户短信，私自发送短信。获取用户网络书签数据、通话记录并联网上传，造成用户隐私泄露，建议卸载。（威胁等级高）
		Trojan/Android.kinkin.a[pay,exp] 2018-07-20	该应用程序包含恶意代码，运行以领取道具名义诱导用户点击付费，且设置付费字体颜色不明显，造成用户资费损耗，建议卸载。（威胁等级高）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Microsoft Edge 远程代码执行漏洞（CVE-2018-8279）	当 Microsoft Edge 未能正确访问内存中的对象时，存在远程代码执行漏洞。该漏洞可能以一种使攻击者能够在当前用户的上下文中执行任意代码的方式来破坏内存。成功利用此漏洞的攻击者可以获得与当前用户相同的用户权限。如果当前用户使用管理用户权限登录，则攻击者可以控制受影响的系统。然后攻击者可以安装程序，查看、更改或删除数据，或创建具有完全用户权限的新帐户。（威胁等级高）
	较为活跃样本	Trojan/Win32.VBKrypt	此威胁是一种使用 VB 语言编写的木马类程序，该家族通过恶意网页进行传播。该家族的部分变种通过冒充一些常用软件来盗取信息。（威胁等级中）
		Trojan[Dropper]/Win32.Delf	此威胁是一种由 Delphi 编译器编写的捆绑类木马程序。该家族的变种是依据相同的编译器被划分为同一个家族的。Delf 家族木马自身并没有主动传播能力，通常都是伪装成正常软件欺骗用户下载运行，或者通过恶意网页的辅助，利用浏览器和插件的漏洞安装到用户的系统中。（威胁等级中）
		Trojan[Dropper]/Win32.Dapato	此威胁是一种木马类程序，该家族运行后会释放多个恶意代码。该家族可以注入其它进程，能够加密用户文件，下载其它恶意代码等。（威胁等级中）
		Trojan[Spy]/Win32.Zbot	此威胁是一种能够进行远程控制、组建僵尸网络、窃取用户信息的间谍类木马程序。该家族会窃取被感染电脑的重要信息，并生成工具包。该工具包允许攻击者获得更高权限来远程控制电脑。（威胁等级中）

三种新兴技术能够加速事件就绪

Ashley Arbuckle / 文　安天技术公益翻译组 / 译

对事件就绪（incident readiness）和事件响应（incident response，IR）团队来说，“紫队演习”是一个福音。

网络风险被广泛认为是全球最大的商业风险之一，企业管理层向其单位的网络安全负责人问计：可以采取哪些措施来做好更充分的准备并降低风险。只在事件发生后进行响应是远远不够的。企业不仅需要强大的 IR 能力，还需要事件就绪能力。为了磨练技能，安全团队正在转向各种演习，这些演习能够帮助他们更好地预测威胁并实践响应措施，其中一种演习是“紫队演习”（Purple Teaming）。

在过去的几年中，我们看到传统的“红蓝队演习”——“红队”找出漏洞并发起攻击，“蓝队”则检测和响应攻击——发展为“紫队演习”。虽然红队 / 蓝队模型能够帮助企业了解漏洞并做好应对攻击的准备，但它们可能需要数周或数月的时间才能完成，这为攻击者提供了充足的时间。

“紫队演习”和传统的红蓝对抗不一样，不是一个持续时日的攻守游戏，而是一种协作和迭代的演习。它通过一个信息更丰富的、持续的流程——该流程旨在帮助防御者降低来自真实世界的高级攻击风险，将红蓝队结合起来。红队向蓝队告知攻击计划、执行攻击、解释他们所利用的安全漏洞，然后不断重复这一流程，以便蓝队能够迅速改进响应措施。

紫队模型能够帮助企业在演习中改善安全态势，具有即时和持续价值。但是，参与者通常严重依赖手动方法来执行和防御攻击。这限制了资源（时间和预算）紧张时可以实现的

目标。但是，如果使用相关技术来增加演习的频率和深度，会如何呢，会加速事件就绪吗？以下三种技术正在成为自动执行和微调紫队演习的新方法。

基础架构分析平台

许多企业都不了解其环境中（包括网络、数据中心和云）的所有内容，这种认知缺失使攻击者占据上风。紫队演习的第一步是了解企业的基础架构或攻击全景。借助分析平台，企业可以非常详细地了解攻击全景，更快地了解他们面临的风险。通过自动化侦察和一些攻击映射，企业可以快速了解关键资产和相关的威胁模型。例如，借助网络上所有内容的清单（包括版本和补丁级别），企业可以将相关信息与公共威胁和漏洞数据库关联起来，快速生成网络上潜在漏洞的列表。红队可以利用此列表来开发更成熟、更复杂的攻击场景，而蓝队则可以利用此列表更快地解决安全漏洞。

应用程序性能管理

应用程序性能管理（APM）工具早在多年前就出现了，早期版本操作麻烦且信息匮乏。目前的 APM 工具能够提供大量信息，可帮助分析代码安全性。这些工具可以分析应用程序使用的对象和方法、数据流以及处理数据的位置，帮助企业了解攻击者可能利用的漏洞。这种“由内而外”的应用程序分析方法比手动的“由外而内”方法更有效，并且可以大大加快安全分析活动。例如，当攻击队查看 web 应用程序中的漏洞时，他们通常会查找本不该存在的网页——测试网页、死网页或已弃用的网页。这些网页早已被遗忘，通常存在漏洞，是攻击者试图寻找的软肋。APM 工具可以自动执行侦察，为红队威胁建模提供此类详细信息，并为蓝队安全分析师提供加强防御所需的洞察力。

安全仪表平台

这项新技术能够自动执行红队的大部分活动——在网络上执行攻击来测试事件就绪情况。安全仪表平台在网络的不同组件上使用设备和代理，有助于在企业的独特环境中展示威胁和恶意活动的影响。红队可以利用它快速确定攻击位置，例如植入某种最新的勒索软件或者进行最新的 DoS 攻击。蓝队可以利用它了解防御层是否按预期工作，确定真正的网络安全差距，并确定如何充分利用他们拥有的资源以及优先投资的事项。

对事件就绪和 IR 团队来说，紫队演习是一个福音。为了继续提高其有效性，我们需要将合适的人员、流程和技术融合在一起，以实现前瞻性的思维和安全分析技术。你可以使用上述三种技术获得必要的可视性和自动化，以便完善事件就绪和 IR 工作。你也可以使用其他一些创新技术来增强你的紫队演习流程。

原文名称	Three Emerging Technologies to Accelerate Incident Readiness
作者简介	Ashley Arbuckle。Ashley Arbuckle 是思科公司安全服务副总裁。
原文信息	2018 年 7 月 12 日发布于 SecurityWeek 原文地址 https://www.securityweek.com/three-emerging-technologies-accelerate-incident-readiness
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《Trojan/Linux.Gafgyt 漏洞利用分析报告》

近期，安天捕风蜜网系统监测并捕获到大量异常的 TCP 流量，经分析，发现针对 52869/TCP 端口的扫描、攻击次数有较为明显的增加，通信流量中存在位于美国的僵尸网络 Gafgyt 家族的控制节点（C2）。经研究分析发现，攻击者利用僵尸网络 Gafgyt 家族结合 CVE-2014-8361 漏洞对世界多个地区的路由设备进行扫描攻击，且发现 CVE-2014-8361 漏洞允许未经身份验证的攻击者使用 root 特权在受害者系统上执行任意代码。

CVE-2014-8361 漏洞是一个针对 Realtek 平台软件开发工具包（下称 Realtek SDK）的漏洞，Realtek SDK 的 miniigd SOAP 服务中存在安全漏洞，而 Realtek SDK 主要用于开发 RTL81xx 芯片组。攻击者可通过构建一个基于 SOAP 服务的含有 Payload 的 XML 文件，对集成了 RTL81xx 芯片组的供应商设备进行攻击。

Gafgyt 家族被控端木马主要有以下 3 个功能模块：

1、Downloader（Payload）模块。通过样本硬编码的 url 下载 shell 脚本并运行，执行脚本枚举下载其中的 url 并运行关联的样本，实现“肉鸡”感染。

2、Scanner 模块。使用“肉鸡”集群爆破方式实现高效率蠕虫式感染指定 IP 网段中存在弱口令的 IoT/Linux 设备。

3、DDoS 攻击模块。“肉鸡”在执行 Tel 扫描爆破的同时，会和 C2 保持正常通讯，等待 C2 的相关指令，例如 DDoS 攻击指令。

在 CVE-2014-8361 漏洞与 Gafgyt 家族木马组成的僵尸网络架构中，漏洞扫描 Vulne_Scanner 功能模块的隐蔽性较高，是独立运行在几台服务器中的。攻击者通过自定义配置对扫描 IP 网段进行扫描探测以获取存在 CVE-2014-8361 漏洞的 IP，并通过后门默认密码登录“肉鸡”，然后远程执行 Gafgyt 木马或下载植入木马的 Shell 脚本的 Payload。无论是 Vulne_Scanner 还是 Telnet 扫描爆破，获取到的远程代码任意执行权限，都会下载并运行存放在 FTP 服务器里面的 Gafgyt 家族木马。

从目前掌握的 Gafgyt 发展史判断，Gafgyt 家族后续仍将会利用更多的物联网漏洞，继续拓展其僵尸网络规模并发起攻击，同时也将增加更高效的攻击模式。安天捕风小组建议广大用户及时更新设备系统并修补相关漏洞，修改设备登陆的默认密码，避免弱口令的使用。

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：

文件来源于内部组件，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、动态行为鉴定器和静态分析鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	761af47e81e31b0ba8be80542d40c177
文件类型	BinExecute/Linux.ELF
大小	342 KB
MD5	761AF47E81E31B0BA8BE80542D40C177
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Backdoor]/Linux.Gafgyt.af
判定依据	静态分析

◆ 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	342 kB
File Type	ELF executable
MIME Type	application/octet-stream
CPU Architecture	32 bit
CPU Byte Order	Big endian
Object File Type	Executable file
CPU Type	MIPS R3000

◆ 文件扫描

文件名	文件 MD5	家族相似性	yara 扫描
null	761af47e81e31b0ba8be80542d40c177	N/A	N/A