安天周观察

主办：安天　2017 年 6 月 26 日（总第 92 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

态势感知　响应联动
安天助力石油石化行业建立积极防御体系

6 月 21 日 -22 日，中国石油石化企业网络安全技术交流大会暨展示会在京举行，安天作为网络安全领域的重要企业积极参与本次会议及展览。

会上，安天研发副总裁王小丰发表了题为《赋能用户，保障安全》的演讲。从安天近期分析和响应的安全事件的进展汇报切入，并从安天的视角分析了目前网络安全的全貌，王小丰表示，从攻击层面来看，目前攻击者可攻击的面越来越多，攻击成本逐渐降低，攻击可利用的资源增加，以及攻击方更加立体等因素都导致防护方的防护难度增大。以“态势感知和响应联动”为核心建立安全集中管控体系、提升积极防御的能力，成为越来越多用户的选择。

王小丰结合安天在自身实践过程中总结的关于石油石化行业安全防护的四个关键点：

1. 提升基础端点的综合防护能力、建立以流量为基础的细粒度按需采集能力、融入和提升基础资产搜集和发现能力、提升多维安全数据的采集能力，是最重要的基础能力。

2. 通过深度分析和关联分析结合，才能达成全局安全态势的综合研判。

3. 重视响应和恢复，并要做到联动化和协同化。

4. 重视建立利用内外部威胁情报的作业体系，通过进行人机结合分析，做到对与自身相关威胁的及时预警。

安天根据石油石化行业的网络安全需求和特点，为其提供了包括安天捕风蜜罐、探海威胁检测系统、追影威胁分析系统等产品，以及安天态势感知与通报预警系统、反 APT 解决方案和相关的安全服务，协助实现石油石化行业信息系统实现了对威胁的捕获、端点的防护、流量监测、深度分析威胁，从而达到有效防护的目标。

在 5 月 12 日晚全球爆发勒索蠕虫“魔窟”(WannaCry) 事件后，安天第一时间到达石油石化客户现场，提供应急分析、解密和处置工具，进行数据保护和恢复，并加固了安全防护策略，得到了用户好评。

安天始终站在对抗网络安全威胁的第一线，不断“服务客户，解决问题；应对威胁，保障安全”，为我国的信息化发展保驾护航。

安天收到公安部信息中心的感谢信

6 月 5 日，公安部信息中心向安天发来感谢信，感谢安天在“永恒之蓝”勒索蠕虫病毒爆发期间参与公安网病毒免疫处置工作中做出的贡献。

在勒索蠕虫爆发期间，安天迅速响应公安部，派出应急响应团队，第一时间到达现场，连续三昼夜坚守工作一线，提出应对工作方案、提供有效技术手段，认真实施疫情分析、病毒查杀、数据恢复等工作，保障了公安信息网络安全和“一带一路”峰会安保工作的顺利进行。

安天作为网络安全应急服务支撑单位之一，多次在重大网络事故和网络安全事件的响应中发挥关键作用，曾参加过十七大、十八大、2010 年起的历届两会、北京奥运会、上海世博会、广州亚运会、2014 年 APEC 会议、抗战胜利 70 周年阅兵、G20 峰会等重大活动的安保工作，并荣获重大活动信息安全保卫工作突出贡献奖。安天会一如既往，在维护国家网络安全工作中贡献自己的一份力量。

■ 新型银行恶意软件利用受感染设备作为“HTTPS 控制服务器”通信

近日，据外媒报道，McAfee Labs 安全研究人员发现一款新型银行恶意软件 Pinkslipbot(又名 QakBot/QBot) 可使用复杂多级代理通过“HTTPS 控制服务器”通信。安全专家注意到，Pinkslipbot 使用通用即插即用 (UPnP) 功能为目标设备提供路径，以感染恶意软件 IP 地址列表中提供的 HTTPS 服务器。这些设备充当 HTTP 代理并将路径传输至另一层 HTTPS 代理，能够允许对真实的 C & C 服务器 IP 地址进行伪装。

目前，受感染机器从新 Pinkslipbot 感染源接收到控制服务器请求后，立即通过使用 libcurl URL 传输库的附加代理将所有流量路由传输至真实控制服务器中。为防止设备感染该恶意软件，用户应保留本地端口传输规则，并仅在必要时打开 UPnP。(来源：http://hackernews.cc/archives/11504)

一周简讯

- 安全厂商发布针对 IoT 攻击统计报告
- 大数据公司暴露了近 2 亿美国选民信息
- 黑客利用连字符填充 URL 实现钓鱼攻击
- 研究者发现可使 Mirai 留存系统的漏洞
- 安全厂商发布 FIN10 的钓鱼敲诈报告
- 澳大利亚因数据泄露花费 250 万澳币

安天 CERT 搜集整理，详情请见：http://bbs.antiy.cn

每周安全事件

类 型	内 容
中文标题	新型 PHP rootkit 问世，危险系数再攀新高
英文标题	With this PHP rootkit you can take over a server hiding it in PHP server modules
作者及单位	Pierluigi Paganini；Security Affairs
内容概述	近日，据外媒报道，荷兰开发人员 Luke Paris 创建了一款隐藏在 PHP 服务器模块中的新型 rootkit 程序，允许攻击者托管 Web 服务器并可有效规避检测。众所周知，传统 rootkit 可在操作系统最低级别拦截内核操作、执行恶意活动。Paris 近期成功创建一款与 PHP 解释器交互的 rootkit 程序，从而取代了更为复杂的操作系统内核功能。Paris 在社交平台 GitHub 上发布 PHP rootkit 概念证明。据悉，该开源项目代码连接至 PHP 服务器的“哈希”与“sha1”函数，并仅由 80 行代码组成，因此极易隐藏在合法 PHP 模块中。 安全专家建议，管理员在安装 PHP 后应保留模块哈希列表。此外，还可使用定时功能尝试对扩展目录中的所有文件进行散列排序并将其与当前散列对比。目前，Paris 已发布 Python 脚本，用于检查用户设备 PHP 模块 SHA1 哈希值。
链接地址	http://securityaffairs.co/wordpress/60175/hacking/php-rootkit.html

每周值得关注的恶意代码信息

经安天检测分析，本周有 8 个移动平台恶意代码和 5 个 PC 平台的恶意代码值得关注

平台分类	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.FakeHGS.a[prv, fra]2017-06-19	该程序为虚假 HGS 应用，具有隐藏图标行为，诱骗用户输入个人银行卡相关信息，并在后台将信息上传至指定服务器中，造成用户隐私泄露和资费消耗，建议卸载。（威胁等级高）
		Trojan/Android.BankDownload.a[prv, exp, rog]2017-06-19	该应用程序伪装成正常应用，会窃取用户通讯录信息并上传，下载银行类木马诱导用户安装，造成用户隐私泄露和资费损耗，建议卸载。（威胁等级高）
		G-Ware/Android.FakeWzry.a[fra, exp]2017-06-21	该应用程序伪装成热门游戏的充值应用，会加载欺诈性充值界面，诱导用户扫码付费，造成用户资费损失，建议卸载。（威胁等级中）
	较为活跃样本	Trojan/Android.Locker.b[rog, sys, lck]	该应用程序伪装成游戏辅助工具，具有加密用户文件勒索用户付费、修改壁纸等恶意行为，造成用户手机无法正常使用，建议卸载。（威胁等级中）
		Trojan/Android.FakeInst.es[prv, exp]	该应用程序伪装成色情游戏，运行后隐藏图标，私自发送短信，后台拦截转发短信，造成用户隐私泄露和资费损耗，建议立即卸载。（威胁等级中）
		Trojan/Android.QQspy.cc[prv]	该程序伪装成 QQ 相关应用，运行后诱导用户输入 QQ 账号和密码并短信转发，造成用户隐私泄露和资费损耗，建议卸载。（威胁等级高）
		Trojan/Android.oxti.ae[exp]	该应用程序运行会隐藏图标，频繁访问推广网址，造成用户流量资费损耗，建议卸载。（威胁等级中）
		Trojan/Android.FakeInst.et[exp, fra]	该程序伪装成游戏应用，运行后弹出游戏过期提示，诱骗用户下载安装未知应用，具有上传用户固件信息、拦截用户短信、点击发送短信等恶意行为，造成用户资费消耗、隐私泄露，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	Windows Search 远程代码执行漏洞 (CVE-2017-8543)	Windows 搜索服务 (WSS) 是 Windows 的一项默认启用的基本服务。攻击者可以向 Windows Search 服务发送精心构造的 SMB 消息，从而利用此漏洞提升权限并控制计算机。（威胁等级高）
	较为活跃的样本	Trojan[Backdoor]/Win32.FinFish	此威胁是一类可以窃取用户信息并回传的木马家族。该家族样本运行后会连接远程服务器，收集系统信息并回传，运行后会自删除。（威胁等级中）
		Trojan[DDoS]/Linux.Ddostf	此威胁是一类针对 Linux 平台的具有 DDoS 功能的木马家族。该家族样本运行会连接远程服务器，向其发送系统敏感信息。它可以接收远程服务器的命令并执行 DDoS 攻击，包括 TCP、UDP 及 HTTP 的洪水攻击。（威胁等级中）
		Trojan[Exploit]/SWF.Angler	此威胁是一类通过 SWF 漏洞进行传播的木马家族。该家族因 Angler Exploit Kit 而得名。该家族的样本使用了 SWF 的漏洞对用户的设备进行感染，从而执行任意恶意代码。（威胁等级中）
		Trojan[Ransom]/Win32.Bart	此威胁是一类可以加密用户数据索取赎金的勒索软件家族。该样本遍历磁盘加密文件并添加 .bart 后缀，加密后在桌面留下 TXT 和 BMP 格式的勒索信并改变桌面，要求用户支付赎金解密。（威胁等级中）

当心下一波网络威胁：物联网勒索软件

David Balaban / 文　安天公益翻译小组 / 译

目前，由于物联网的一些本质特征，导致物联网勒索软件比已经广泛传播的针对电脑和智能手机的勒索软件更加危险。

■ 物联网勒索软件不会对您的数据进行加密

众所周知的加密勒索软件，如 Locky 和 Cerber，会锁定受感染机器上的重要文件。这种加密是不可逆转的：受害者要么支付赎金获取解密密钥，或者在没有备份的情况下和他们的文件永别。相较于只锁定一些文件，物联网勒索软件可能会锁定并完全控制许多设备甚至网络。

物联网恶意软件可能会迫使车辆停下，断开电力甚至终止生产线。这样的恶意操作能够造成更大的伤害，因此黑客可能会要求更多的赎金。受害者原意支付赎金的原因在于失去系统控制期间可能发生的损失的数量和性质，而非攻击的不可逆转性。

物联网扩展了生命支持设备 (如起搏器) 或工业系统 (如泵站) 的可能性，与此同时，阻断物联网基础设施和不及时的响应造成的损害将会呈指数增长。在工业控制系统中使用物联网设备的组织会面临最大的风险，例如发电厂、大型自动化生产线等。

■ 消费者物联网设备

针对消费者物联网设备的攻击早已发生。研究人员已经展示了如何使用恶意代码来控制联网的温控器，将温度设置为最大值，迫使受害者支付赎金。

此外，物联网勒索软件可能会窃取重要数据和个人信息，例如，从联网的监控摄像头或健身工具中窃取敏感信息，威胁受害者说会公布这些信息，以此敲诈受害者。

物联网行业高度分散，并缺乏标准化的方法、通用平台和通信系统，因此很难进行大规模的攻击。在一次攻击中，黑客通常只针对特定类型的设备，这也减少了潜在受害者的数量。

目前，黑客攻击消费者物联网设备的利润空间很小。但是随着物联网进一步深入家庭和办公室，未来情况很可能会发生改变。

■ 工业部门面临高风险

物联网的工业部门面临着完全不同的情况。工业系统对勒索者具有强大的吸引力。这可能是任何影响数千甚至数百万人生活的系统，其运作成本非常高昂。

例如，最近几家美国医院遭受了一系列的勒索软件攻击。好莱坞长老会医院的正常运作被勒索攻击打断，不得不将部分病人转移到其他诊所，医生也被迫使用老式的纸质记录方法。

如果医院的系统遭到感染，所有患者的健康都会受到威胁，因此医院支付赎金的可能性非常高。针对关键基础设施的攻击基于类似的心理：如果人们的生活受到威胁，而且时间紧迫，被攻击方往往会同意支付赎金。

电网和发电站也是物联网恶意软件的重要目标。它们在现代世界中的重要作用在 2003 年美加大停电事件中得到了很好的体现。在几个小时内，大停电造成了 60 亿美元的损失，影响了 5500 万人的生活。该事件不是网络攻击，而是软件故障。而今天，黑客不断扫描互联网，寻找重要的漏洞网络，所以能源公司应该做好应对准备。

■ 如何保护物联网系统

虽然不存在通用的解决方案，但许多专家认为，遵守某些准则和方法可以帮助组织和制造商更好地保护其物联网系统免受勒索攻击。

重要的一点是：能够远程升级智能设备的固件。没有任何联网设备可以永远保持安全，使用者必须及时进行有效和安全的固件更新。

要采用安全的固件更新渠道，因为不安全的更新渠道可能会成为感染入口点。我们可以采用一些经过时间考验的措施来消除这种入口点，例如阻止处理器和固件、加密设备之间的通信通道。

另一个重要的措施是可靠的认证机制。您可能会遇到这样的情况：当设备连接到互联网却没有进行任何身份验证。

如果验证缺失成为一种普遍现象，攻击者可以利用这一点禁用数百万台设备。如果一台连接了数百万机器的服务器被感染，这种攻击将会尤其危险。

为了阻止入侵，我们必须引入可靠的安全证书生命周期管理，并规范安全系统的代码库。这将有助于减少攻击向量。

当然，保护物联网仍然是一个艰巨的任务，目前业界正在朝这个方向摸索。目前，网络犯罪分子只是在衡量和评估新市场的风险、机会和潜在的盈利能力。

原文名称	Beware the next wave of cyber threats: IoT ransomware
作者简介	David Balaban，计算机安全研究员，在恶意软件分析和反病毒软件评估方面拥有超过 15 年的经验。
原文信息	2017 年 6 月 12 日发布于 Information Management 原文地址 https://www.information-management.com/opinion/beware-the-next-wave-of-cyber-threats-iot-ransomware
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《新型物联网恶意软件 Persirai 分析报告》

近日，安天追影小组发现一个名为 Persirai 的新型物联网恶意软件，该恶意软件已影响了 1000 多种型号的网络摄像机。目前，约有 12 万的设备易受到这种恶意软件的影响。Persirai 利用最近公开的 0day 漏洞入侵网络摄像头，并进行大范围的传播，发动 DDoS 攻击。

安天追影小组的分析人员对 Persirai 家族中的样本进行了简要的分析。当网络摄像机被攻击者入侵后，被入侵的设备会尝试连接一个下载站点，站点返回命令要求网络摄像机执行恶意 shell 脚本。其中某一脚本”wificam.sh”将会下载并执行一些恶意样本。

这些恶意样本在被执行后，会删除自身，仅在内存中运行。恶意样本还会采用一些方法来确保被入侵的网络摄像机不再被其他攻击者入侵。一旦重启，受感染设备将变得更易被攻击。

通过分析，被感染的网络摄像在接收到 C&C 的命令后，会通过利用一个 0day 漏洞，开始自动地扫描并入侵其他的网络摄像机。攻击者利用某个漏洞可以获得用户的密码文件，这意味着无论用户设置的密码强或弱，攻击者都可以控制该网络摄像机。被 C&C 服务器控制的网络摄像机，还可接受包含目标 IP、端口号的攻击指令，之后通过 UDP 协议对其他的主机进行 DDoS 攻击。

Persirai 和同为物联网平台恶意软件的 Mirai 存在许多相同点：相似的扫描方案，部分函数同源。但同时两者之间也存在许多的不同点：Persirai 将 C2 明文编码在代码中，Mirai 使用异或算法加密 C2；Persirai 采用 Mirai 从未采用的 81 端口进行传播；二者通信协议完全不同；Persirai 仅存在两种 DDoS 攻击向量，而 Mirai 包含 10 种。

随着物联网的爆发式发展，物联网设备成为了黑客攻击的一大领域。设备中使用了默认的简单密码是物联网设备易被入侵的主要原因。另外，路由器上的即插即用功能，使得网络中的设备将端口直接对外开放。

在此，安天提醒广大网络用户，使用网络摄像机以及其他物联网设备时，应当尽快修改默认的密码，并禁用路由器上通用的即插即用功能，及时将物联网设备固件更新升级，减少被漏洞利用的机会。

木马程序

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

文件被内部组件发现，经由 BD 静态分析鉴定器、美国软件交叉索引（NSRL）鉴定器、可交换信息（EXIF）鉴定器、静态分析鉴定器、智能学习鉴定器、安全云鉴定器等鉴定分析。

最终依据静态分析鉴定器将文件判定为木马程序。

文件名	7e1c3834c38984c34b6fd4c741ae3a21.danger
文件类型	BinExecute/Linux.ELF
大小	161 KB
MD5	7E1C3834C38984C34B6FD4C741AE3A21
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Backdoor]/Linux.Gafgyt.aw
判定依据	静态分析

报告地址：https://antiy.pta.center/_lk/details.html?hash=7E1C3834C38984C34B6FD4C741AE3A21

◆ EXIF 信息

描述	值
File Size	161 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