安天周观察

安天官方微博　安天官方微信

主办：安天　2018 年 05 月 07 日 (总第 134 期) 试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

叠加演进 有效防护
安天助力石油石化建立动态综合防御体系

日前，“2018 中国石油石化企业信息技术交流大会暨展示会”在北京举行，本次大会的主题为“大力发展石油石化工业互联网，全面提升网络安全，有效促进企业数字化、智能化”。来自国资委、工信部、能源局等相关部委的主管领导和专家，中石油、中石化、中海油等各油气集团公司主管领导和技术专家，科研院所及相关技术服务和产品供应商参加了本次大会。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。

安天解决方案销售部负责人带来了《构建叠加演进的网络安全能力体系》的内容分享。她指出，当前网络安全威胁形势复杂，关键信息基础设施面临重大风险。我们应正视网络安全工作的历史误区，树立正确的网络安全观。应借鉴滑动标尺模

安天解决方案销售部负责人进行演讲

型构建叠加演进的网络安全能力体系，构建与关键信息基础设施重要性相适应的安全防护能力，以有效防护为目标，构建动态综合防御体系。

根据石油石化行业的网络安全需求和特点，安天分享了综合安全解决方案。为石油石化行业提供了包括安天智甲终端防御系统、安天追影威胁分析系统、安天探海威胁检测系统、安天捕风蜜罐系统，安天鉴微终端检测与响应工具集以及安天网络安全态势感知与通报预警平台、反 APT 解决方案和相关的安全服务。

安天依托下一代威胁检测引擎、多层次人机结合分析、人工智能等自主先进技术，构建关键信息基础设施叠加演进的网络安全能力体系，助力石油石化行业实现信息系统对未知威胁和异常行为进行智能监测、追踪溯源，实现威胁捕获、端点防护、流量监测及威胁深度分析，从而达到有效防护的目标。

作为引领威胁检测与防御能力发展的网络安全国家队，安天始终坚持走能力型安全厂商道路，始终站在对抗网络安全威胁的第一线，为用户提供有效防护，为保障国家网络安全全力以赴。

研究人员发现大众、奥迪易受黑客远程攻击

一家荷兰网络安全公司发现，部署在大众汽车集团部分车型上的车载信息娱乐（IVI）系统容易受到远程黑客攻击。安全研究人员表示，他们成功验证了该发现。利用汽车的 WiFi 连接来利用一个暴露的接口，并获得由电子产品供应商 Harman 制造的汽车 IVI。研究人员还可以访问 IVI 系统的根帐户，并允许他们访问其他汽车数据。在某些情况下，攻击者可以通过车载套件收听司机正在进行的谈话，打开和关闭麦克风，以及访问完整的地址簿和对话历史记录。

（文章来源 https://www.bleepingcomputer.com/news/security/volkswagen-and-audi-cars-vulnerable-to-remote-hacking/）

上百万台光纤路由器曝认证旁路漏洞，可被远程访问攻击

外媒近日消息，安全研究人员发现通过一个认证旁路漏洞能够远程访问超过一百万台光纤路由器。研究表明，该漏洞很容易通过修改浏览器地址栏中的 URL 来利用，可让任何人绕过路由器的登录页面和访问页面，只需在路由器的任何配置页面上的网址末尾添加 “?images /”，就能够完全访问路由器。由于设备诊断页面上的 ping 和 traceroute 命令以“root”级别运行，因此其他命令也可以在设备上远程运行。

调查结果表明，该漏洞在用于光纤连接的路由器中被发现。目前 Shodan 上列出了约 106 万个标记的路由器，其中一半易受攻击的路由器位于墨西哥的 Telmex 网络上，其余的则在哈萨克斯坦和越南被发现。

最近的研究表明，路由器是黑客滥用的主要目标，因为它们是大多数网络的中心点。当受到攻击时，攻击者可以进一步立足于网络。路由器也是一个很容易利用的目标，它们可以轻易地被黑客攻击，被僵尸网络劫持，并且通过互联网流量入侵目标，将它们置于离线状态。这些分布式拒绝服务（DDoS）攻击可以在精确瞄准时摧毁大量网络。

（文章来源 https://www.zdnet.com/article/over-a-million-vulnerable-fiber-routers-can-be-easily-hacked/）

每周安全事件

类 型	内 容
中文标题	大型垃圾邮件僵尸网络 Necurs 使用新技术躲避检测
英文标题	Necurs Spam Botnet operators adopt a new technique to avoid detection
作者及单位	Pierluigi Paganini
内容概述	Necurs 是全球最大的垃圾邮件僵尸网络，由数百万受感染的计算机组成，曾用于扩散 Locky、GlobeImposter、Trickbot 等多个恶意软件。近期，Necurs 再次引起了研究人员的关注，因为其背后的操纵者使用了一种新的技术躲避检测。他们向潜在受害者发送的邮件中包含一个文件夹，一旦解压，就会出现一个扩展名为 .URL 的文件。 该文件利用 Windows 快捷方式功能，一打开就指向浏览器，并执行最终的恶意 payload。在最终执行阶段，Necurs 会向受害者计算机发送装载软件，下载其他恶意软件进而彻底感染受害者计算机。
链接地址	https://securityaffairs.co/wordpress/71837/malware/necurs-evasion-technique.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	相关描述
移动恶意代码	较为活跃的样本	Trojan/Android.sunshinereal.a[prv,spy]	该程序运行诱导激活设备管理器，释放加载恶意子包，执行私自提权，后台窃取用户短信、联系人、通话记录、浏览器记录、社交应用记录等隐私信息，私自拍照、通话录音、摄像、记录键盘输入信息等并将用户隐私上传至服务器。还会拦截短信、私自发送短信，删除通话记录，造成用户隐私泄露和资费消耗，建议立即卸载。
		Trojan/Android.Adobot.a[prv,rmt,exp,spy]	该程序伪装系统应用，运行隐藏图标，后台连接到远程服务器上传设备固件信息并获取远控指令，根据指令执行窃取用户短信、通话记录、通讯录等信息，发送短信，静默安装更新、修改设置远控网址等一系列行为，造成用户隐私泄露和资费消耗，建议卸载。
		Trojan/Android.mygeekhat.a[prv,rmt,spy]	该程序伪装成系统应用，运行后隐藏图标，联网获取远程指令上传用户短信、联系人、通话记录、录音、相册、位置等隐私信息，还能执行下载安装未知应用、录音、照相和打开指定网页等危险行为，造成用户隐私泄露，建议卸载。
		Trojan/Android.djhero.b[prv,exp]	程序运行诱导激活设备管理器，隐藏图标，私自下载指定应用，诱导安装，还会上传设备固件信息和位置信息，造成用户资费损耗和隐私泄露，建议卸载。
		Trojan/Android.FakeBank.s[prv]	该程序伪装银行相关应用，运行诱导激活设备管理器，拦截短信、获取用户固件信息上传到指定网址，会造成用户隐私泄露，建议卸载。
		Trojan/Android.AtouchsimoSpy.a[prv,spy]	该程序伪装其他应用，运行获取用户固件信息、短信内容、联系人、通话记录、网页浏览记录、地理位置信息、应用列表等，私自录音、拍照，并私自上传到特定网址，会造成用户隐私泄露，建议立即卸载。
		Trojan/Android.007Spy.a[prv,rmt,spy]	该程序是间谍类软件，会通过短信接收远程指令，上传用户短信、联系人、通话记录、位置、相册、环境录音等隐私信息，还能备份社交应用数据上传到指定邮箱，同时支持隐藏图标、安装为系统应用、防止卸载等危险功能，造成用户隐私泄露，建议卸载。
		Trojan/Android.StealthBot.a[exp,rog]	该应用伪装系统服务，包含恶意代码，后台私自加载恶意插件，接收远程指令，通过模拟点击进行恶意刷量和推广行为。造成用户流量消耗，建议卸载。
		Trojan/Android.droidgate.a[prv,rmt,spy]	该程序运行后隐藏图标，通过远程指令上传短信、安装包等隐私信息，还能执行拦截短信、发送短信、设置音量等行为，造成用户隐私泄露，建议卸载。
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	CMS 系统 Drupal 严重安全漏洞（CVE-2018-7600）	Drupal 是全球三大开源内容管理系统 CMS 平台之一，被广泛应用于构造各种不同应用的网站项目。攻击者利用该漏洞对受影响版本的 Drupal 网站发动攻击，无需登录认证即可直接执行任意命令，包括下载重要文件，修改页面，上传 Webshell，篡改页面或进行挖矿等行为，最终可接管站点。
	较为活跃样本	Trojan[Backdoor]/Win32.Shabo	该病毒家族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。
		Trojan[PSW]/Win32.Neter	该病毒家族是一种可以窃取密码信息的木马类程序。该家族的样本运行后会窃取用户账户信息，如账号密码等。
		Trojan[RemoteAdmin]/Win32.NetBox	该病毒家族是一种具有远程控制行为的风险软件家族。该家族的样本在执行后会让远程控制端可以通过 VNC 访问并控制自己的机器，可能对用户的设备造成潜在的危险因素。
		Trojan[Dropper]/Win32.Freemz	该病毒家族是一种可以释放恶意代码的木马类程序。该家族样本运行后释放恶意代码到本地执行，连接远程服务器下载恶意代码。

剖析企业物联网安全的可能性与挑战

Bill Kleyman / 文　安天技术公益翻译组 / 译

当谈及物联网时，大多数人通常会想到他们熟悉的设备，比如 Nest 恒温器或 Philips Hue 智能灯。然而，如今物联网组件正在以闪电般的速度向医疗、企业以及数据中心等方向发展。

我们举例来说。Raritan 最近推出了一系列“智能机架”，将环境监测提升到了一个新的水平。这些数据中心就绪的物联网技术经过测试，可在全球数据密集度最高的环境中承受数十亿小时的运行时间。其中一种物联网组件是位于整个机架内的环境传感器。这些组件与智能锁集成，帮助隔离热点、优化冷却、防止停机，甚至保持安全。此外，这些物联网设备收集数据，然后将数据输入数据中心基础设施管理平台，使数据中心和企业领导者可以做出更好的决策。

在 UPS（美国联合包裹服务）中，物联网传感器通过监控运输卡车的里程、速度和整体发动机健康状况来帮助保护车况。再加上大数据解决方案，UPS 还能够有效监控运输的包裹并优化整个路线。最近，微软和劳斯莱斯进行合作，向航空公司提供先进的运行情报。这与通用电气公司（GE）对其喷气式发动机所做的类似。好处在哪？在飞机降落之前，地勤技术人员就可以确定特定部件的磨损。这样，他们可以安排好修复和部件团队，从而大幅削减维护时间。

根据 IDC 的数据，物联网市场完全没有放缓的迹象，预计 2021 年的规模将达到 1.4 万亿美元。然而，当谈到企业采用物联网设备时，人们有一些担忧。你如何设计正确的物联网用例？它可以与你现有的网络和数据中心系统联接吗？最重要的是，安全性如何：你如何处理和保护个人身份信息或个人医疗信息等数据？企业希望利用物联网解决方案，但难以设计正确的架构，最重要的是，难以利用和量化这些设备创建的数据。

当物联网遇见边缘计算

毫无疑问，数据中心和企业领导者正在积极投资物联网解决方案。在我协助撰写的 AFCOM（计算机操作管理协会）数据中心行业状态的研究报告中，81% 的受访者认为扩展边缘计算能力的主要目的是支持物联网；40% 的受访者已经部署或计划部署边缘计算。为什么说这很重要呢？因为边缘计算的目标是处理接近最终用户或来源的数据和服务。IoT 几乎完全符合这个用例。

在现代企业组织中，领导者和 IT 专家将物联网组件概念化并将这些概念应用到他们自己的企业中至关重要。这是一个架构和业务的探索过程，可以真正了解联网设备如何为企业带来价值。无论是联网卡车还是增强引擎，将企业的一部分连接到数字领域的方法将是独一无二的。

很多时候，企业认为联网设备必须是新的东西。但是，在很多情况下，我们正在对模拟系统进行数字化改造。例如，通过为大型起重机安装物联网传感器，建筑公司可以在几秒钟内发现故障，而不用花费几个小时进行故障排除。就此而言，你的 IT 基础设施中哪些模拟系统可以数字化？你想收集或了解的数据点在哪里？对于许多企业来说，这些可能是很大的好处，也是物联网革命的一部分。但要真正了解企业物联网的可能性，需要采取多方面的方法：

1. **边缘的演变。**边缘解决方案有助于传输和处理距离用户很近的数据，了解这一点至关重要。而且，就物联网而言，边缘是主要的推动因素。

2. **基于上下文的物联网安全。**物联网安全从来不是线性的。最好的安全模型将始终采用设备访问和询问的上下文方法。

3. **“智能”数据中心。**你的数据中心越来越智能。从机器人到智能机架，这些都是需要安全和效率的物联网设备。

4. **黑客攻击成为一种产业。**黑客攻击已经成为一种产业。了解你的数据在暗网上的价值并围绕物联网进行考虑对于良好的安全最佳实践至关重要。

5. **设计物联网安全策略的关键因素。**将边缘、物联网组件、业务用例以及良好的总体安全策略结合起来是设计安全的物联网架构的关键。除此之外，确保数据安全将成为重中之重。

原文名称	Deconstructing the Possibilities and Realities of Enterprise IoT Security
作者简介	Bill Kleyman。Bill Kleyman 是 MTM Technologies 公司的首席技术官。
原文信息	2018 年 4 月 25 日发布于 Dark Reading 原文地址 https://www.darkreading.com/vulnerabilities---threats/deconstructing-the-possibilities-and-realities-of-enterprise-iot-security/a/d-id/1331625
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《WebMonitor RAT 商业远控分析报告》

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款使用 C2-as-a-Service（C2aaS），即“命令与控制服务器即服务”的商业远控 RAT，其名为 WebMonitor。

WebMonitor RAT 通常在地下论坛中出售，2017 年 5 月出现在 hackforums 论坛中，分为三种版本，价格分别为 14.99、24.99、29.99 欧元。除了在 hackforums 上进行出售，revcode.eu 也是其主要销售与服务的网站。

WebMonitor 的服务器商拥有基于 Web 的界面，提供了包含 VPN 和 C2 的服务。其有两种界面选项，原始的“精简版”与功能复杂的“企业版”。其提供了一系列功能，其中包括注入 DLL、蓝牙管理、浏览器插件及其图像缓存、系统各项证书密码、键盘记录、摄像头操作、系统各项信息等。WebMonitor 的客户端使用 Visual Basic 6 编写，使用 UPX 加壳，运行后会安装到 \%USERNAME%\AppData\Roaming\REVCODE-***.EXE，在注册表中会创建自启动键。客户端生成器可以选择安装时不弹出安装窗口，生成功能与 C2aaS 相关联，使用者并不能运行他们自己的 C2，WebMonitor 为使用者提供虚拟主机名，使用者可以直接通过 Web 界面进行访问，其 C2 域与销售网站 revcode.eu 相同。

WebMonitor RAT 虽然拥有多种访问和控制受害者的功能，但由于其使用了“C2aaS”模式，对其检测就变得较容易。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、静态分析鉴定器、动态行为鉴定器将文件判定为木马程序。

概要信息

文件名	5db1d88363e52ca06cf491a7213f2431
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	444 KB
MD5	5DB1D88363E52CA06CF491A7213F2431
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.VBKrypt
判定依据	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

查找指定内核模块	★
创建特定窗体	★
创建挂起的进程	★★
访问其他进程内存	★
获取计算机名称	★
设置调试器权限	★
获取系统内存	★★
打开自身进程文件	★
读取自身文件	★★
独占打开文件	★
获取驱动器类型	★

文件扫描

文件名	文件 MD5	家族相似性	yara 扫描
target.exe	5db1d88363e52ca06cf491a7213f2431	N/A	N/A
target.exe.dmp	6da132c72b57978c1487826ac0bd6886	N/A	N/A
edb.chk	191fe952c573fc5980293e0ed0430015	N/A	N/A
WindowsUpdate.log	987f25a4b1ce69bf555a7bc97152a68a	N/A	N/A
.....	.....	.....	.....