安天周观察

安天官方微博　安天官方微信

主办：安天　2018 年 10 月 15 日 (总第 155 期) 试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天接受焦点访谈采访 曝光高级威胁、解读动态综合防御

近日，中国网络安全产业联盟理事长、安天首席架构师肖新光，安天网络安全工程师关墨辰接受了中央电视台焦点访谈栏目的采访，针对高级网空行为体的网络攻击及做好网络安全的防御工作表达了自己的观点。这是安天人第三次登上焦点访谈，接受采访。

从震网事件开始，安天持续关注高级持续性威胁的演进变化，特别是针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体及其攻击行动，进行持续监测和深度解析，发布了多篇分析报告。

在本次采访中，安天工程师介绍了安天近期披露的“绿斑”高级网空威胁行为体的窃密攻击活动。“绿斑”组织活跃数年，主要针对中国政府部门、航空、军事等相关科研机构进行攻击，主要目标是窃取高价值数据和机密信息，通过鱼叉式钓鱼邮件附加漏洞文档或捆绑可执行文件进行传播。相关威胁暴露了目前信息系统的防护缺失问题。

安天工程师对攻击者通过侵入软件供应商升级服务器，替换升级程序，达成攻击内网效果进行了简易模拟演示，初步展示了动态综合防御机制的重要作用。现实的攻防场景远比这个简单的演示复杂，威胁分析研判的过程要更加复杂困难。客观的敌情想定是做好网络安全防御工作的前提，通过物理隔离于国门之外，已经成为不切实际的想象。应以“敌已在内和敌将在内”作为重要信息系统、关键信息基础设施防护的基本想定。

安天认为，做好网络安全防护工作要按照三同步的原则，在信息化建设的规划、建设、运维全生命周期考虑网络安全问题。安天基于 SANS 的“滑动标尺”模型进行了延伸拓展，进一步提出了“叠加演进”的网络安全能力模型，为用户安全能力体系建设提供参考。该模型明确揭示了基础结构安全、纵深防御、态势感知与积极防御、威胁情报间的叠加和前置基础条件关系，说明了缺少基础安全规划和布防的高阶安全能力和手段将成为空中楼阁，没有态势感知和积极防御、缺乏威胁情报则无法应对高级别的网络攻击。

安天当前正在研发的战术型态势感知平台，能够以网络安全能力叠加演进为导向，协助用户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能用户，筑起可对抗高级威胁的网络安全防线。

研究人员披露具有高度针对性的 APT 组织 Gallmaker

赛门铁克的研究人员发现新 APT 组织 Gallmaker，该组织至少从 2017 年 12 月开始运营，最近一次活动在 2018 年 6 月，目标瞄准全球的政府、军队和国防机构进行高度针对性的攻击，包括已经袭击的东欧国家的海外大使馆，以及中东的军事和国防组织。Gallmaker 攻击活动仅使用 LotL（living off the land）策略和公开的黑客工具，包括混淆的 shellcode，WindowsRoamingToolsTask，用于安排 PowerShell 脚本和任务等，而不使用恶意软件。攻击过程为通过网络钓鱼电子邮件传递恶意 Office 文档，当受害者打开诱饵文件时，会出现一个警告，要求受害者启用内容，一旦启动，攻击者就可以使用 Microsoft Office 动态数据交换（DDE）协议远程执行受害者系统内存中的命令，因仅在内存中运行，攻击者可以避免在磁盘上留下痕迹，从而避免被检测。获得对设备的访问权限后将执行各种工具，攻击结束后将删除工具，以更好隐藏活动痕迹。

（文章来源：https://www.symantec.com/blogs/threat-intelligence/gallmaker-attack-group）

安全厂商发现 VMware Workstation 存在 DoS 漏洞

思科 Talos 发现 VMware Workstation 中可能导致拒绝服务的漏洞 CVE-2018-6977。VMware Workstation 是一种广泛使用的虚拟化平台，与操作系统一起运行，允许用户同时使用虚拟化系统和物理系统。该漏洞存在于 VMware Workstation 使用的像素着色器中，攻击者可以通过文本或二进制形式 guan 的异常像素着色器利用该漏洞，使进程崩溃，从而导致 DoS 状态。该漏洞可以从 VMware guest 或 VMware 主机触发，如果不使用 Google 的 ANGLE，也可以通过 Web 浏览器利用 WEBGL 触发。

（文章来源：https://blog.talosintelligence.com/2018/10/vuln-spot-vmware-dos.html#more）

每周安全事件

类 型	内 容
中文标题	黑客利用基于比特币的加密货币中的漏洞窃取资金
英文标题	A hacker stole $15,000 worth of Pigeoncoin by exploiting a patched Bitcoin bug
作者及单位	Sophia Brown
内容概述	一名化名为“mrsandman1”的黑客利用比特币中的漏洞，成功窃取了 15000 美元的 Pigeoncoin。该漏洞为 CVE-2018-17144，存在于所有基于比特币的加密货币中。该漏洞是比特币网络史上最严重的错误之一，如果被利用，可能允许攻击者执行各种恶意活动，例如击垮比特币网络并打印他们想要的许多比特币。虽然该漏洞在黑客攻击之前被发现并修复，可以看出使用比特币代码的一些货币也容易受到攻击。
链接地址	https://cyware.com/news/a-hacker-stole-15000-worth-of-pigeoncoin-by-exploiting-a-patched-bitcoin-bug-f0fff96c

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.SmsSpy.aj[prv,exp] 2018-10-08	该应用程序伪装正常应用，运行隐藏图标，后台监听收件箱，通过私发短信和邮件上传用户收件箱短信，会造成用户隐私泄露，建议卸载。（威胁等级中）
		Tool/Android.Smartphone.b[prv,rmt] 2018-10-09	该应用程序运行要求用户设置账号，后台上传用户的短信、通话记录、照片、浏览器历史记录等至指定网址，通过登录账户可以查看受控手机的上传内容，发送录音指令等，请谨慎使用。若非自主安装，建议卸载。（威胁等级中）
		Trojan/Android.hundai.a[prv] 2018-10-10	该应用程序伪装成贷款应用，运行监听用户短信和通话，后台上传用户手机固件信息、电话号码、短信等信息，会造成用户隐私泄露，建议卸载。（威胁等级中）
	较为活跃样本	Trojan/Android.ZzcnSpy.a[prv]	该应用程序伪装正常应用，本身无实际功能，运行私自上传用户联系人和短信信息，会造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.QQspy.dr[prv,fra]	该应用程序伪装 QQ 相关应用，诱导用户输入 QQ 账号密码，而后短信转发到指定号码，会造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.Downloader.es[rog,exp]	该应用程序运行后通过 umeng 获取 push 消息，进行静默下载和安装，会造成用户流量消耗，建议卸载。（威胁等级低）
		RiskWare/Android.Fakejiaoyou.d[fra,exp]	该应用程序伪装交友软件，通过发送虚假诱惑性消息，诱导用户付费，可能造成用户资费损失，建议卸载。（威胁等级低）
		Trojan/Android.FakeFB.z[exp]	该应用程序是虚假应用，伪装 Facebook，运行隐藏图标，跳转推广页面，后台推送广告，造成用户流量资费损耗，请卸载。（威胁等级低）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Adobe Digital Editions 任意代码执行漏洞（CVE-2018-12813）	Adobe Digital Editions 4.5.8 版本之前的产品（包括 4.5.8）具有任意代码执行漏洞，成功利用可能导致在当前用户的上下文中执行任意代码。（威胁等级高）
	较为活跃样本	GrayWare[AdWare]/NSIS.Adwapper	此威胁是一种有广告行为的灰色软件类程序。该家族通常是使用 NSIS 打包工具生成的安装包程序，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）
		RiskWare[Downloader]/Win32.DownloadSponsor	此威胁是一种下载广告软件的风险软件类程序。该家族会自动下载并运行用户不知情或不允许安装的软件，同时也会不断检查更新文件本身。（威胁等级低）
		Trojan/Win64.Patched	此威胁是一种窃取账户信息的木马类程序。该家族样本基于 64 位系统，当用户打开 IE 浏览器时，该家族代码会执行打开文件，并将文件的 shellcode 读到内存中，同时还原 IE 浏览器入口点代码，然后创建一个线程执行恶意操作，并跳转到 IE 原入口地址继续执行。该家族会记录 Windows 登陆账户信息，试图窃取 SQL 账号密码信息，以 URL 方式发送到作者地址中。（威胁等级中）
		Trojan[Exploit]/JS.Agent	此威胁是一种使用 JS 脚本语言编写的、可以利用漏洞下载恶意代码的木马家族。该家族并没有统一的行为、统一的功能，而是像一个木马集合一样，将大量基因片段定性的恶意代码归类。（威胁等级中）
		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。（威胁等级高）

保护联网医疗设备：将其归类为 ICS 会有帮助吗？

Leslie K. Lambert / 文　安天技术公益翻译组 / 译

此前，联网医疗设备一直是通过“物理隔离”来保护的。现在我们来想一想，除了物理隔离，我们还可以采取哪些措施来保护它们免受安全威胁。

自今年 4 月以来，美国国土安全部（DHS）工业控制系统应急响应小组（ICS-CERT）已发出若干告警，敦促医疗机构警惕医疗成像系统和病人监护设备等设备的漏洞。此外，一些医疗设备制造商，如飞利浦、雅培和 BD，还通过 ICS-CERT 发布告警信息。

在这些告警中，有一点很有意思——在美国，医疗设备被归类为工业控制系统（ICS）。对于 IT 安全领域的许多人来说，自从 2010 年旨在感染伊朗核设施的震网蠕虫（Stuxnet）横空出世后，ICS 或 SCADA（监控和数据采集系统）的安全日益恶化。谁能想象，在安全的重要程度和关键性方面，医疗设备能与 SCADA 设备相提并论呢？

如果说医疗设备是先前隔离和独立的，而现在已经连接到网络的硬件，那么它们与 ICS 或 SCADA 系统没有什么不同。虽然医疗设备已经联网并互联了一段时间，但是直到最近，业界才开始实施物理和逻辑安全控制措施来保护它们。

幸运的是，相关方面正在采取若干举措来改善医疗设备的安全性，包括美国食品药品管理局（FDA）最近发布的《医疗设备安全行动计划》。致力于公共安全问题的网络安全志愿者协会“我是骑士”（I Am The Cavalry）也提出了“联网医疗设备希波克拉底誓言”计划，提出了保护患者和医疗系统安全的措施，以应对医疗机构对联网医疗设备日益增长的依

赖性。（译者注：Hypocratic Oath，希波克拉底誓言，俗称医师誓词。希波克拉底乃古希腊医者，被誉为西方“医学之父”，在他所立的这份誓词中，列出了一些伦理上的规范。）

此前，联网医疗设备一直是通过“物理隔离”来保护的。现在我们来想一想，除了物理隔离，我们还可以采取哪些措施来保护它们免受安全威胁。

保护联网医疗设备

就像 IT 行业一样，保护医疗设备的第一步在于资产管理，即环境中所有医疗物联网（IoT）设备的识别、评估和建档。了解这些设备的安全配置和漏洞至关重要，特别是因为许多设备使用过时和报废的操作系统，其更新配置或应用补丁的功能十分有限。

第二步是日志管理，这样能够实现对设备上活动的可见性。然而，由于医疗设备没有内置的安全和管理功能，因此与 IT 设备相比，理解医疗设备的日志数据并将其转化为行动更具挑战性。不过也有一些好消息——随着数据科学和机器学习的进步，医疗设备可以获得前所未有的洞察力，甚至可以预测即将发生的问题。

黑客已经证明了他们有能力利用勒索软件来感染和破坏医疗网络，或者通过“劫持医疗设备”来感染其他互联设备或 IT 系统。

通过日志分析，我们可以以多种方式来保护医疗设备。首先，通过第一步的“资产管理”来确定网络上存在哪些设备，然后借助日志分析来检测设备配置中的异常更改、损坏或故障的设备，甚至是由于恶意软件或勒索软件的引入而行为反常的设备。

日志分析可以实现一项重要的新功能——确认医疗设备中配置的授权模型的真实性。大多数医疗设备都在制造期间配置了默认的用户名和口令，通过这些凭证可以执行固件更新或定期的预防性维护。这些默认凭证存储在世界各地的类似设备中，如果不进行更改，就会造成巨大的安全漏洞。通过日志分析来监控医疗设备，可以减少默认配置中的许多固有风险。

此外，还可以通过日志分析来监控医疗设备的位置，特别是考虑到许多设备是便携或移动的，经常被移动到不同的病房或位置。例如，通过日志分析，我们可以了解某个医疗设备是否正在使用或上一次使用的时间，帮助管理建档和发现那些“消失的”设备。

显然，与医疗 IoT 设备的实施速度相比，自动 / 手动管理功能和更新流程已经远远落后。毫无疑问，新一代医疗设备将会超越当前医疗设备的基本功能并成为真正的智能设备。但是，我们的当务之急是，找到管理和降低当前基础设施风险的方法。通过日志分析，我们可以获得所需的情报，以解决当今医疗设备（无论我们称其为 ICS 设备还是 IoT 设备）中存在的安全漏洞。

原文名称	Securing connected medical devices : Will categorizing them as ICS help?
作者简介	Leslie K. Lambert。Leslie K. Lambert 是 Juniper Networks 和 Sun Microsystems 公司的前 CISO，在信息安全、IT 风险和合规性、安全策略等方面拥有 30 多年的经验。
原文信息	2018 年 10 月 4 日发布于 CSOonline 原文地址 https://www.csoonline.com/article/3309998/internet-of-things/securing-connected-medical-devices-will-categorizing-them-as-ics-help.html
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《LokiBot 样本分析报告》

安天捕风团队捕获到一批 LokiBot 样本。经过深入分析，得出了原始 LokiBot 样本已被修改的结论。目前，发现此变种病毒被售卖于黑市，并且在多个恶意活动中被利用。LokiBot 像许多恶意软件一样，通过恶意电子邮件进行分发。这些钓鱼邮件没有固定的攻击模式，但它们的行为方式类似，均是诱使受害者下载压缩包文件或者 MS office 文件的恶意样本附件，最终从附件中提取、利用宏命令或漏洞下载 LokiBot 样本。

LokiBot 的攻击流程图是线性的，且攻击目的在于信息窃取。一旦它进入受感染的设备并安装成功，就会在受感染设备中收集用户已安装的各个应用中的凭证信息。LokiBot 对于不同的应用模块使用不同的入侵方式，当其收集齐所有所需材料后，会通过 HTTP 协议将它们压缩在数据包中发送给 C & C 服务器。

LokiBot 在受感染的设备中拥有永久权限，此权限可以使攻击者创建、修改注册表项，并且也可以将自身以指定的命名形式复制到 %APPDATA% 下的指定文件夹中，同时创建一个用于解析 C & C 服务器响应的新线程以等待新命令。每台被感染的设备都有唯一的标识符（bot ID），可作为互斥锁使用（互斥锁的作用为避免重复感染机器，提高感染效率）。

在分析的大多数变种样本中都有 5 个远控 url，这些 url 会接收被窃取的数据信息，并且会向被感染设备中的恶意代码样本发去新的指令，其中 4 个 url 用了 3 重 DES 算法进行保护，第 5 个 url 仅使用了简单的 XOR 保护。然而 LokiBot 使用 CryptDecrypt Windows API 函数解密受 3DES 算法保护的数据时，受 3DES 加密保护的解密网址被覆盖，只返回受 XOR 保护的 url 的字符串，实际上 LokiBot 在调用 CryptDecrypt 函数之后跳转到一个名为“x”部分的开头。该部分具有可写权限，受 XOR 保护的 url 和负责解密该 url 的代码均位于“x”部分，这种行为就像功能指令的跳转一样，像是有第三个人手动修改了代码，使 url 实现自定义远控修改。

目前，最新且分发最多的样本是 LokiBot v.1.8 的变种版本。变种版本 LokiBot 的代码相比 LokiBot 的原始代码，添加了“x”部分，实现了使用 XOR 保护的 url 用做控制面板网址的方法，增强了真实 url 地址的隐蔽性。安天提醒广大互联网用户不要轻易打开未知的 URL 和邮件，设备需安装杀毒、防毒软件并及时升级系统和修补设备漏洞。

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、数字证书鉴定器、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、智能学习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	463469a131f368a0f2215b0ff6146454[1]
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	126 KB
MD5	463469A131F368A0F2215B0FF6146454
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.SGeneric
判定依据	静态分析

报告链接：https://antiy.pta.center/_lk/details.html?hash=463469A131F368A0F2215B0FF6146454

◆ 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

◆ 常见行为

行为描述	危险等级
获取系统版本	★★
获取主机用户名称	★
获取计算机名称	★
独占打开文件	★
查找指定内核模块	★
连接网络	★
设置调试器权限	★
打开自身进程文件	★
释放 PE 文件	★
复制自身文件	★★
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	761af47e81e31b0ba8be80542d40c177	N/A	N/A
target.exe.dmp	e34d3e56068698066e909b1bb898447d	N/A	N/A