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 16 日 (总第 131 期) 试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天发布《警惕首个卸载安全软件的勒索者“AVCrypt”》报告

2018 年 3 月 22 日，一款可卸载安全软件的勒索者病毒“AVCrypt”被研究人员发现。该勒索软件是首个在加密磁盘文件之前先卸载安全软件的勒索者病毒。不同于已经出现的关闭防火墙的恶意代码，该勒索软件可从微软 Windows 操作系统的安全中心中查询已经注册的安全软件并加以卸载。

在报告中，安天分析人员对该勒索软件的样本进行分析，发现其可以通过两种方式卸载安全软件，一种是停止并删除服务，另一种是卸载安全中心注册的安全软件。此外，其还具有调用 bcdedit 与一些其他命令关闭系统功能、显示虚假进度条、查找 / 安装 Tor 浏览器等功能，文件被加密后其文件名最前面会多一个字符“+”。

虽然该样本回传了加密密钥，但根据其不完整的勒索信息，安天分析人员认为其仍是开发中用以测试的半成品，正式版本可能会具有更多的恶意功能，因此需提高警惕。

经验证，安天智甲终端防御系统可实现对 AVCrypt 的有效防护。其具备的程序自保护能力和对注册表进行实时监控的能力可有效应对 AVCrypt 加密前卸载安全软件及对系统注册表项进行恶意修改的问题。

安天智甲对 AVCrypt 进行防御

安天智甲文档保护界面

报告二维码

黑客通过远程桌面服务安装新型 Matrix 勒索软件变体

MalwareHunterTeam 本周发现了两个新的 Matrix Ransomware 变体，这些变体正在通过被黑客入侵的远程桌面服务进行安装。这两种变体都会对计算机的文件进行加密，但其中一种更加先进，可提供更多调试消息并使用密码来擦除可用空间。

根据勒索软件执行时显示的调试消息以及 BleepingComputer 论坛中的各种报告，该勒索软件目前正在通过攻击者直接连接到互联网的远程桌面服务向受害者分发。一旦攻击者获得访问计算机的权限，他们将上传安装程序并执行它。

目前有两种不同的 Matrix 版本正在发布。这两种变体都安装在黑客 RDP 上，加密未映射的网络共享，加密时显示状态窗口，清除卷影副本以及加密文件名。不过，这两个变体之间有一些细微差别，第二个变体（[RestorFile@tutanota.com]）稍微高级一些。

文章来源：

https://www.bleepingcomputer.com/news/security/new-matrix-ransomware-variants-installed-via-hacked-remote-desktop-services/

黑客利用思科智能安装漏洞，全球 20 万台路由器“躺枪”

据外媒报道，一个名为“JHT”的黑客组织在上周五利用 Cisco（思科）CVE-2018-0171 智能安装漏洞攻击了许多国家的网络基础设施，例如俄罗斯和伊朗等 。根据伊朗通信和信息技术部的说法，目前全球已超过 20 万台路由器受到了攻击影响，其中有 3500 台受影响设备位于伊朗。

在利用 CVE-2018-0171 攻击 Cisco 路由器后，路由器的配置文件 startup-config 被覆盖，路由器重新启动。这不仅导致了网络中断，并且路由器的启动配置文件也被更改成显示一条 “不要干扰我们的选举“的消息。

攻击者透露他们扫描了许多国家的易受攻击的系统，但只袭击了俄罗斯或伊朗的路由器，并且他们还声称通过发布 no vstack 命令来修复美国和英国路由器上任何被发现的漏洞。

文章来源：

https://www.bleepingcomputer.com/news/security/iranian-and-russian-networks-attacked-using-ciscos-cve-2018-0171-vulnerability/

一周简讯

- CNVD 发布思科远程命令执行漏洞的安全公告
- Verge 虚拟加密货币系统遭受黑客攻击
- 商业军火 ThreadKit 现已集成 Flash 4878 漏洞
- 身份即服务平台 Auth0 曝出验证绕过漏洞
- 僵尸网络 Mirai 变种针对金融行业发起 DDoS
- 研究人员发现新的 ATM 恶意软件 ATMJackpot
- AMD 和微软发布针对幽灵漏洞微代码更新

每周安全事件

类 型	内 容
中文标题	Facebook 泄漏事件再升级，受影响用户从 5000 万增长到 8700 万
英文标题	间谍软件 Agent Tesla 变种再现：通过特制 Word 文档诱导安装
作者及单位	Pierluigi Paganini
内容概述	近期，专家发现臭名昭著的间谍软件 Agent Tesla 出现了全新的变种，而变种传播是通过特制的 Microsoft Word 文件进行的。 Agent Tesla 是一种用来收集系统键击记录、剪贴板内容、屏幕截图、身份凭证的间谍软件，很多用户使用这款软件窥探受害者。为了实现这些功能，这款间谍软件在主函数中创建了不同的线程和定时函数。 在最新发现的行动中，黑客将附件文档的内容制作成模糊的样子，这样用户会遵循文档上的说明，双击文档来得到更清晰的视图。而如果用户照做了，这个文档就会提取可执行文件“POM.exe”，在本地系统的临时文件中运行。 目前看来，新变种 C & C 服务器提交数据的方式已经改变。研究员表示，过去的攻击行动中使用的都是 HTTP POST 来发送收集的数据。但在观测到的最新变体中，它会使用 SMTPS 将收集到的数据发送到攻击者的邮箱。
链接地址	https://securityaffairs.co/wordpress/71154/breaking-news/agent-tesla-campaign.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 4 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	较为活跃的样本	Trojan/Android.narutoted.h[prv,exp,rmt,spy]	该应用程序安装后隐藏图标，激活设备管理器，网络远程控制私自发送短信、彩信，上传用户联系人、短信、通话录音、相册等隐私信息，造成用户隐私泄露和资费消耗，建议立即卸载。（威胁等级高）
		Trojan/Android.FakeInst.dy[pay,fra]	该应用程序伪装其他应用的下载程序，虚假界面诱导用户点击发送付费短信，本身无实际下载功能，可能造成用户资费损失，建议不要使用。（威胁等级中）
		G-Ware/Android.HiddenAds.dy[exp,rog]	该应用程序伪装系统应用，安装无图标，无实际功能，运行加载子包，后台联网推送广告，可能会造成用户流量消耗，建议卸载。（威胁等级中）
		Trojan/Android.FakeFlashPlayer.ae[exp]	该应用程序伪装成 Flash Player，运行拦截短信、私自发送短信，造成用户资费消耗，建议卸载。（威胁等级中）
		Trojan/Android.Guerrilla.j[exp]	该应用程序伪装成系统应用，安装无图标，内嵌在其他软件中，会下载安装未知应用，造成用户资费损耗，建议卸载。（威胁等级中）
		Trojan/Android.Triada.br[exp,sys]	该应用程序安装无图标，本身无实际功能，警惕其联网后下载恶意文件并尝试获取 root 权限、修改系统文件，会造成用户流量消耗并影响系统的正常运行，建议卸载。（威胁等级中）
		Trojan/Android.Asacub.b[prv,exp,rmt,spy]	该应用程序伪装正常应用，运行诱导激活设备管理器，防卸载。接收远程指令控制，隐藏图标，发送短信、下载文件、拦截和删除短信，上传用户短信、通讯录、通话记录、程序安装列表等隐私信息，还会诱导用户输入银行账户相关信息上传，造成用户隐私泄露和资费损耗，建议卸载。（威胁等级中）
		Trojan/Android.LockerMaker.g[spr,exp]	该应用程序为锁屏勒索类恶意程序的制作工具，恶意制造、传播勒索程序，建议不要使用。（威胁等级高）
		Trojan/Android.Downloader.ee[exp]	该应用程序包含风险代码，运行私自联网下载指定文件，造成用户流量资费损耗，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	Cisco Smart Install 远程命令执行漏洞（CVE-2018-0171）	为思科 IOS 和 IOS-XE 系统 Smart Install Client 代码中存在的一个缓冲区堆栈溢出漏洞（CVE-2018-0171）。攻击者可以远程向 TCP 4786 端口发送一个恶意数据包，触发目标设备的栈溢出漏洞，造成设备拒绝服务（DoS）或造成远程命令执行，攻击者可以远程控制受到漏洞影响的网络设备。（威胁等级高）
	较为活跃样本	Trojan[Downloader]/MSIL.Agent	此威胁是一种具有代理行为的木马类程序。该家族采用 MSIL 中间语言编写。样本运行后会将自身注册为系统服务的一部分，并实现开机自动运行。该家族会在后台连接黑客指定的远程服务器，并在本地电脑中下载其它恶意软件。（威胁等级高）
		Trojan/Win32.Obfuscated	此威胁是一种木马类程序。该家族样本运行后会不停的向用户弹出广告窗口。该家族会在用户电脑上安装一个流氓反间谍软件工具，提示用户恶意软件已经被删除，但实际上恶意程序仍然存在。（威胁等级中）
		Trojan[Banker]/Win32.Agent	此威胁是一种窃取银行账号信息的木马类程序。该家族并没有统一的行为与功能，而是像一个木马集合一样，将以大量基因片段定性的恶意代码归类。（威胁等级中）

企业担心不安全的物联网设备会带来“灾难性后果”

Kelly Sheridan / 文　安天技术公益翻译组 / 译

在新的物联网安全调查中，只有 29% 的受访者表示他们积极监控第三方使用的联网设备的风险。

根据一项关于第三方设备危险性的新研究，企业对物联网（IoT）风险的担忧发展速度超过了其安全实践。研究人员报告称，风险管理还相对不成熟，并且对敏感和机密数据构成威胁。

这项研究由共享评估（Shared Assessments）委托波耐蒙研究所（Ponemon Institute）执行，对 605 名从事风险和企业治理工作，且熟悉企业物联网设备的专家进行了调查。其中 21% 的受访者表示，他们的企业遭受了不安全的物联网设备或应用程序导致的数据泄露事件——而去年这一比例是 15%。

联网设备正在扰乱企业。40% 的受访者表示，他们的企业保留着物联网设备清单，工作场所的平均设备数量为 15,874 台。60% 的受访者表示其企业将物联网设备视为网络或企业系统的端点。

“几乎所有人都认识到，与物联网设备和应用程序相关的风险可能会造成灾难性的安全事件。”共享评估高级副总裁查理·米勒（Charlie Miller）说，这与 97% 的受访者观点一致。

“人们在数据泄露和攻击方面的经验提高了他们的意识，”他继续说道，“物联网设备的频谱代表了威胁向量的增加，人们有一种恐惧 ..... 这创造了一场通过其他媒介攻击它们的近乎完美的风暴。”但数据显示企业没有采取措施来保护自己。

超过一半（56%）的企业没有盘点他们的物联网设备。在这其中，88% 认为原因是没有对这些设备和应用程序进行集中控制。不到 20% 的受访者表示其企业可以确定工作场所中的大部分物联网设备。

第三方风险

随着物联网的发展，第三方设备的风险也会增加。虽然企业更加细致地监控内部使用的物联网设备，但他们往往无法认识到外部设备的风险。

超过 70% 的受访者认为第三方风险对其宝贵资产构成严重威胁；66% 的受访者声称物联网生态系统的重要性大大增加了第三方风险。44% 的受访者表示，供应商的数量导致企业很难管理物联网平台的复杂性。

大多数企业依靠合同条款和策略来缓解第三方物联网风险。超过一半（53%）的企业使用合同协议，46% 表示他们有策略来禁用可能会带来风险的物联网设备。即便如此，不到一半的企业监控第三方合规性，接近 60% 的受访者表示无法确定物联网和第三方防护措施是否足够。只有 29% 的受访者表示其企业积极监控第三方使用的物联网设备的风险。

“这是一个很大的脱节，”米勒说，“我们看到第三方风险管理仍然不成熟。”

事实上，77% 的企业认为，在未来两年内，他们会遭受由第三方的不安全物联网设备或应用程序引起的网空攻击。75% 的受访者认为他们会遭受数据泄露事件。然而，35% 的受访者不知道他们是否可以发现第三方违规，26% 不确定其企业是否受到涉及物联网设备的网空攻击的影响。

风险管理缺失

这并不是说企业没有第三方风险管理计划；相反，60% 的企业是有的。然而，只有 28% 的受访者表示他们的计划非常有效，而大多数企业还没有准备好应对物联网设备的风险。

部分问题在于批准使用物联网设备的人与管理风险的人之间存在差距。43% 的受访者表示总经理 / 业务线副总裁批准物联网设备，但 35% 的受访者表示了这些人管理物联网设备的风险。

“通常情况下，这是一个联合模型，”Miller 说，“有一个第三方风险管理小组负责监督，联络控制小组，协调响应并聘请主题专家。”只有 49% 的企业拥有第三方风险管理委员会。

研究人员发现，最重要的风险治理实践是获得领导力。只有 17% 的企业表示其董事会对与供应商和第三方相关的安全风险有着高度的参与和理解。不到 40% 的企业表示高管认为他们对风险管理流程的有效性负责。

企业应如何制定风险管理计划？米勒建议升级库存系统，以便识别内部和外部使用的所有设备。他还建议派专人负责物联网并在整个企业内传达这一责任。“依赖合同安全策略是件好事，但我们需要一种机制来监督这些要求的有效性和发生，从而识别和减轻异常情况。”他说。

原文名称	Businesses Fear 'Catastrophic Consequences' of Unsecured IoT
作者简介	Kelly Sheridan。Kelly Sheridan 是 Dark Reading 的编辑。
原文信息	2018 年 4 月 6 日发布于 Dark Reading 原文地址 https://www.darkreading.com/author-bio.asp?author_id=837
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《恶意代码下载器“QuantLoader”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木马下载程序开始活跃，名为“QuantLoader”。该程序已经在地下论坛上发售了较长时间，其用于分发各种恶意代码，包括勒索软件、银行木马及RAT。

最新版本的QuantLoader通过使用一些网络钓鱼攻击活动传播。该活动从一个钓鱼电子邮件开始，附带一个为受害者提供初始JS下载程序的链接。有趣的是，他们选择了file://(SMB)协议而不是传统的http://，也许是为了穿透一些代理/防火墙。

攻击者首先通过钓鱼邮件使受害者打开附件中的JS下载脚本，下载QuantLoader，运行后连接C&C，下载后门，最后回传系统信息。在邮件附件中的JS脚本有很多代码，基本使用了混淆处理的方式。通过对JS的分析，可以发现下载的域名，包括chimachinenow.com、motifahsap.com、sittalhaphedver.com。QuantLoader本体样本运行后将自身复制到%appdata%后打开一个新进程，同时修改注册表使其开机自启动。它调用WinHttpCreateUrl，整合恶意代码的完整URL并下载，C&C地址为“wassronledorhad.in”。同时，它还会使用netsh命令向防火墙添加规则，指定进程，然后指定允许操作的方向。

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YARA自定义规则鉴定器、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（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。

最终依据静态分析鉴定器将文件判定为木马程序。

概要信息

文件名	db078628cdc41e9519e98b7ea56232085e203491bd2d5d8e49ef6708f129e1b8
文件类型	Script/Netscape.JS[:JavaScript]
大小	14 KB
MD5	6F2B5A20DBA3CDC2B10C6A7C56A7BF35
病毒类型	木马程序
恶意判定/病毒名称	Trojan[Downloader]/JS.Nemucod.dbp
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	附件信息	
延时	★★★	Sleeptime	0x0000EA60

常见行为

行为描述	危险等级
查找指定内核模块	★
创建特定窗体	★
获取计算机名称	★
获取驱动器类型	★
请求加载驱动的权限	★
获取主机用户名称	★
打开自身进程文件	★
查找浏览器进程	★★
获取socket本地名称	★
连接网络	★
独占打开文件	★
获取系统内存	★★
设置调试器权限	★
设置文件属性为隐藏	★★
隐藏文件	★
访问文件尾部	★

进程监控

PID	创建
1316	C:\WINDOWS\System32\WScript.exe
1852	dumprep.exe
1388	svchost.exe