安天发布《利用疫情信息传播 KPOT 窃密木马分析报告》

近日，安天 CERT 在梳理网络安全事件时发现一个利用疫情信息传播并且借助勒索软件掩盖窃密行为的 KPOT 窃密木马，该 KPOT 窃密木马的下载器主要通过钓鱼网站进行传播。

该窃密木马下载器执行后，从远程网站下载两个文件，第一个下载文件为 KPOT 窃密木马，执行后将窃取计算机上的重要信息，截取活动桌面，窃取加密货币钱包并回传到远程站点。第二个下载文件是一个名为 CoronaVirus 的勒索软件，执行后将加密计算机上的文件，在原文件名前添加“coronaVi2022@protonmail.ch___”，在计算机每个加密的文件夹和桌面上创建名为“CoronaVirus.txt”的勒索信，勒索信内容包含勒索说明、50 美金比特币的赎金金额和比特币地址等。CoronaVirus 勒索软件运行后将 C：驱动器重命名为 CoronaVirus，修改注册表值使计算机重启后显示跟勒索信相同的锁定屏幕。由于赎金金额较低等因素，推测 CoronaVirus 勒索软件的目的是通过锁屏等操作掩盖 KPOT 窃密木马窃取密码、Cookie、加密货币钱包等重要信息的行为。

安天提醒广大用户，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。确保所有的计算机在使用远程桌面服务时采取 VPN 连接等安全方式，如果业务上无需使用远程桌面服务，建议将其关闭。

目前，安天追影产品已经实现了对该类恶意代码的鉴定；安天智甲已经实现了对该恶意代码的查杀。

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、YARA 自定义鉴定器、来源信息鉴定器、数字证书鉴定器、元数据信息鉴定器、聚类分析鉴定器、反病毒引擎鉴定器、动态（WinXP）鉴定器、字符串分析鉴定器、智能学习鉴定器、静态特征检测鉴定器、安全云鉴定器、信标检测鉴定器、动态（Win7 x86）鉴定器等鉴定分析。

最终依据 BD 静态分析鉴定器、反病毒引擎鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	a08db3b44c713a96fe07e0bfc440ca9cf2e3d152a5d13a70d6102c15004c4240
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	719 KB
MD5	99785AE0679D6D3E27DE83AF403C23B0
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Zenpak
判定依据	反病毒引擎

◆ 操作系统

操作系统	内置软件
Win7 x86 6.1.7600 Build 7600	默认、IE9、Google Chrome、Firefox、Office 2007、Flash、WPS、FoxitReader、Adobe Reader

◆危险行为

行为描述	危险等级
通过 CMD 隐藏删除自身	★★★★
删除自身	★★★★

◆常见行为

行为描述	危险等级
获取系统版本	★
加载运行时 DLL	★
获取系统信息（处理器版本、处理器类型等）	★
创建窗口	★
DNS 请求	★
连接网络	★
获取驱动器类型	★
网络连通测试	★★
获取计算机名	★
检索系统内存信息	★

◆完整报告地址

安天周观察
安天官方微博 安天官方微信
主办：安天 2020 年 3 月 23 日 (总第 223 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

安天剖析 微软 SMBv3 高风险漏洞并发布免疫工具

概述

2020 年 3 月 11 日，微软在 3 月的安全更新中发布了一个位于 Server Message Block 3.1.1（SMBv3）网络通信协议的远程代码执行漏洞，漏洞编号为 CVE-2020-0796，但并未在更新中修复此漏洞。次日，微软发布 CVE-2020-0796 专项补丁。成功利用此漏洞的攻击者能够在目标服务器或客户端上执行任意代码，类似“永恒之蓝”漏洞，该漏洞存在被恶意代码利用进行大范围传播的风险，威胁等级高。

漏洞描述

该漏洞是由于 SMBv3 协议中处理压缩消息时未进行严格安全检查所导致的。针对服务器，攻击者可以通过发送特制数据包至目标服务器以利用此漏洞；针对客户端，攻击者可以通过配置恶意 SMBv3 服务器，并诱使用户连接到该服务器以利用此漏洞。目前有网友已经在 Github 上公开了该漏洞的检测工具。

受影响范围

▲主要受影响的 Windows 版本如下：

- Windows 10 Version 1903 for 32-bit Systems
- Windows 10 Version 1903 for x64-based Systems
- Windows 10 Version 1903 for ARM64-based Systems
- Windows Server, Version 1903 (Server Core installation)
- Windows 10 Version 1909 for 32-bit Systems
- Windows 10 Version 1909 for x64-based Systems
- Windows 10 Version 1909 for ARM64-based Systems
- Windows Server, Version 1909 (Server Core installation)

漏洞原理分析

SMB 3.1.1 协议出现时间较晚，由 Windows 10 1903 引入（2019 年 5 月）。此协议涉及的模块包括 mrxsmb20.sys、srv2.sys、srvnet.sys 等。此次问题和永恒系列一样，也是出现在 srv2.sys 这个文件中。

在 SMB 3.1.1 协议中，引入了数据压缩传输的概念，以求能够提高传输效率。但在解压缩时，由于考虑不严谨导致出现此次问题，而修补后的代码加入了长度范围验证

srv2.sys 文件中负责解压缩的代码使用函数 SrvNetAllocateBuffer（srvnet.sys）申请内存，内存长度由传输数据（详见下文）中 OriginalSize 和 Offset 相加得到。

申请的内存长度类型为 unsigned int，传输数据中 OriginalSize 和 offset 也都是 unsigned int 类型。如没有进行范围验证，则可能产生溢出。

修复及缓解建议

▲更新补丁

微软已经发布了针对该漏洞的补丁，可通过微软官网下载相应补丁并安装更新（https://www.catalog.update.microsoft.com/Search.aspx?q=KB4551762）。

安天建议通过安天智甲一键扫描漏洞并下载补丁进行修复。

▲禁用 SMBv3 压缩功能

安天针对此漏洞发布了免疫工具，使用此工具可禁用 SMBv3 压缩功能，以阻止攻击者对 CVE-2020-0796 漏洞的利用，同时也可以通过工具下载相应补丁，修复漏洞。

可访问创意安天论坛下载本工具：

下载链接：https://bbs.antiy.cn/forum.php?mod=viewthread&tid=83848

微信扫描二维码
进入创意安天论坛下载工具

另外也可通过以下 PowerShell 命令暂时禁用 SMBv3 压缩功能：

（1）禁用命令：Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" DisableCompression -Type DWORD -Value 1 -Force

（2）启用命令：Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" DisableCompression -Type DWORD -Value 0 -Force

执行后无需重启，但此种方式无法防护针对 SMB 客户端的攻击。

微信扫描二维码可查看
针对企业网络管理员的建议

每周安全事件

类 型	内 容
中文标题	新 TrickBot 模块可进行 RDP 暴力破解
英文标题	New TrickBot Module Bruteforces RDP Connections, Targets Select Telecommunication Services in US and Hong Kong
作者及单位	Liviu ARSENE&Radu Tudorica&Alexandru MAXIMCIUC&Cristina VATAMANU
内容概述	Bitdefender 研究人员于 1 月 30 日发现了一个新的 TrickBot 模块 rdpScanDll，该模块可用于对选定目标进行 RDP 暴力破解。TrickBot 新模块主要针对美国和中国香港的电信、教育和金融服务行业。当 TrickBot 开始执行时，它会创建一个文件夹，其中包含加密的恶意载荷、相关的配置文件和 C2 服务器列表，插件需要与 C2 服务器通信以检索要执行的命令。rdpScanDll 通过三种攻击模式执行，当 Check 模式检查目标列表中的 RDP 连接时，TryBute 模式尝试使用从端点“/RDP/names”和“/RDP/dict”获得的预定用户名和密码列表，然后对选定的目标进行暴力破解。因其包含一组未调用的可执行函数，且不获取用户名列表，导致插件使用空密码和用户名来验证目标列表，所以研究人员认为该模块仍在开发中。TrickBot 的更新机制中，横向移动模块接收最多的更新。TrickBot 的动态的 C2 基础设施，主要位于俄罗斯，并且每月会增加上百个新的 C2 IP 地址，平均使用时间为 16 天。
链接地址	https://labs.bitdefender.com/2020/03/new-trickbot-module-bruteforces-rdp-connections-targets-select-telecommunication-services-in-us-and-hong-kong/

每周值得关注的恶意代码和漏洞信息

经安天【CERT】检测分析，本周有 8 个移动平台恶意代码和 5 个 PC 平台的恶意代码和漏洞值得关注

恶意代码类别		名称与发现时间	威胁等级	简要描述
移动恶意代码	新出现的样本家族	Trojan/Android.Socksbot.f[rmt,prv] 2020-03-13	高	该应用程序无实际功能，运行后创建 socket，接收远程服务器发送的指令与远控服务器通过 socket 进行通讯，远控端可使用户设备变成 SOCKS 代理，这样远控端可通过用户设备访问设备所属内部网络从而窃取用户内网的隐私信息，造成用户隐私泄露，建议不要安装。
		Trojan/Android.b4aspy.m[prv,exp,spy] 2020-03-14	中	该应用程序伪装正常应用，运行后隐藏图标，获取用户手机相关信息、短信、位置、通讯录等信息并上传，造成用户隐私泄露和资费损耗，建议卸载。
		Trojan/Android.Banbra.g[prv] 2020-03-15	中	该应用程序伪装为正常银行应用，窃取用户填写的金融相关账号密码，造成用户经济损失和隐私泄露，建议卸载。
	较为活跃样本	Trojan/Android.MobOk.e[pay,exp,rog]	中	该应用程序伪装其他应用，内嵌恶意代码，运行加载恶意子包，警惕后台访问推广页面和付费订阅页面，私自订阅付费服务造成用资费损耗，建议卸载。
		Trojan/Android.Cerberus.c[prv,rmt]	中	该应用程序伪装为知名应用，运行激活设备管理器，隐藏图标，监听用户的短信、通知栏信息，接收远程指令，窃取通讯录、日志、短信等信息并联网上传，私自发送短信，访问未知页面，造成用户的资费消耗和隐私泄露，建议卸载。
		G-Ware/Android.Akshell.a[exp,rog]	低	该应用程序伪装其他应用，恶意重打包，推广其他软件，可能会造成用户资费损失，隐私泄露，建议卸载。
		G-Ware/Android.TipsAd.a[exp,rog]	低	该应用程序为虚假应用，无实际功能，会私自加载广告显示于其他应用之上，造成用户资费消耗，建议卸载。
		Trojan/Android.HakenClicker.a[exp,rog]	低	该应用程序开机自启，会私自模拟点击广告，造成用户资费消耗，建议立即卸载。
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Word 远程代码执行漏洞（CVE-2020-0852）	高	当 Microsoft Word 软件无法正确处理内存中的对象时，会触发远程代码执行漏洞。成功利用此漏洞的攻击者可以使用经特殊设计的文件在当前用户的上下文中执行操作。若要利用此漏洞，用户必须使用 Microsoft Word 软件的受影响版本打开经特殊设计的文件，才可触发此漏洞。
	较为活跃样本	Trojan/Win32.Scarsi	中	此威胁是一种具有多种恶意行为的木马类程序。该家族的恶意行为包括删除修改数据、监控网络连接、允许攻击者对用户系统进行远程控制等。该家族的变种可能根据不同的进攻目的而设计，一般具有多种恶意行为。该家族一旦侵入用户系统，将会对系统造成很大的破坏。
		Trojan[Backdoor]/Win32.IRCNite	中	此威胁是一种后门类木马程序。该家族样本运行后会释放可执行文件，使用 IRC 通信信道连接远程服务器，等待接收上传下载文件。该家族还会监视用户屏幕、记录键盘击键、查看进程和窗口等。
		Trojan/Win32.Refroso	中	此威胁是一种木马类程序。该家族可以逃过计算机的注意在后台运行。该家族会在系统中安装一些恶意软件，允许黑客远程访问计算机，并窃取个人信息。
		GrayWare[AdWare]/Win32.Gamevance	低	此威胁是一种广告类木马程序。用户为了获取免费的游戏服务，同意通过 Gamevance 软件的文本链接，以横幅和弹出窗口的形式接收广告。这些广告是根据用户的网页浏览历史记录和用户访问最频繁的网站确定的。

物联网的兴起如何转变 CISO 的角色

菲尔·尼雷 / 文 安天技术公益翻译组 / 译

通过采用基于风险的方法为未来做好准备。以下五个步骤会对您有所帮助。

Gartner 最近发布的一份报告显示，CISO 的角色正在迅速转变，包括要开始管理物理安全风险以及保护敏感信息。这一转变是由于实体设备的数字化系统（CPS）的部署，例如楼宇管理系统和医疗保健设施中使用的物联网（IoT）设备，以及用于制造工厂、石油和天然气设施、能源和水设施、交通、采矿和其他关键工业基础设施中的运营技术（OT）设备。

因为CPS遍布于数字世界和物理世界，所以对于那些企图造成重大物理安全和环境事故以及运营中断的攻击者来说，它们是首选目标。案例包括针对石化设施安全系统的 TRITON 攻击、乌克兰电网攻击、NotPetya 和 Norsk Hydro 勒索软件攻击。

此外，去年 8 月，微软报告称，它观察到一个由俄罗斯政府支持的威胁组织使用 IoT 智能设备作为进入企业网络的入口，并试图提升权限以发起进一步的攻击。最近，我们还发现到攻击者入侵 IoT 楼宇准入控制系统，从而深入企业网络。

行业分析人员预测，不久将在全球范围内部署约 500 亿个 IoT 设备，这将导致攻击面显著增加。由于这些嵌入式设备无法受到基于代理的技术的保护，而且通常未打补丁或配置错误，CISO 需要新的策略来缓解 IoT 安全风险。否则，不难想象，监管机构和企业律师很快就会认定企业高管存在过失，甚至需要他们对未能实施与物理安全相关的网络安全控制措施承担个人责任。

缓解 CPS 和 IoT 风险的五个步骤

爱达荷国家实验室（INL）开发了一种方法来缓解 CPS 和 IoT / OT 风险，称为结果导向、充分考虑网络状况的工程设计（CCE）。基于这种 INL 方法，以下是所有组织机构在不久的将来都应该优先考虑的五个步骤：

1. 确定“皇冠宝石”流程：

您不可能一直保护所有东西，但可以在大部分时间里保护最重要的东西。因此，坚决优先考虑那些可能造成重大物理安全或环境事故或运营中断的功能是至关重要的。通过与业务负责人、基础架构经理和 OT 人员的交流讨论，确定您最需要优先保护的东西。

2. 绘制数字地形图：

识别和分类组织机构中的所有相关资产，无论它们是 IT、IoT、楼宇管理系统（BMS）、OT 还是 Alexa 和游戏系统等智能个人设备。这包括了解信息如何在您的网络中传输以及接触设备的人员，其中包括能够进行远程访问的第三方供应商和维护承包商。

3. 标明最可能的攻击路径：

分析网络中的风险和漏洞，以确定对于最重要的资产和流程来说最可能的攻击向量。这可以通过使用自动威胁建模以及红队演练来识别其他入口点，例如社会工程和对设施的物理访问。

4. 制定缓解和保护方案：

一旦您了解了最可能的攻击路径，就应该开发一种优先处理方法来缓解风险。这可以包括以下步骤，例如减少可通过互联网访问的入口点数量，使用零信任微分段策略将 IoT 和 OT 设备与其他网络隔离，以及修补存在于最有可能的攻击路径中的关键漏洞。此外，也可采用外围连续监控的方式作为对数字解决方案的补充，或是利用设备本身的安全措施，也就是无代理模式：某些威胁行为出现会直接报警，比如当 CCTV 监控设备主动去浏览活动目录时。

5. 消除 IT、OT、IoT 和 CPS 之间的壁垒：

作为 CISO，保护企业安全意味着要对所有数字安全负责，无论是 IT、OT、IoT 还是 CPS。创建统一的网络安全监控和管理需要对人员、流程和技术采用整体方法。技术方面包括将所有 IoT / OT 安全警报发送到网络安全运营中心，并利用现有的安全信息和事件管理（SIEM）、安全编排自动化与响应（SOAR）以及预防机制（防火墙和网络准入控制系统）来快速响应 IoT / OT 事件，例如，快速隔离已被检测为恶意流量源的设备。

未雨绸缪

如今，从民族国家威胁行为体到网络犯罪分子和黑客，都有较强的目的性，坚定的决心和高能力，能够对网络造成破坏和中断。

业内专家一致认为，有坚定决心的攻击者终究会找到进入网络的方法，因此，更好的策略是在杀伤链的早期侦察阶段部署监控来发现他们，以便在攻击可能造成任何重大破坏之前缓解攻击。在 TRITON 攻击石化厂控制器的例子中，攻击者已经在其网络中潜伏了数年，结果由于恶意软件中的一个漏洞，无意导致工厂停产，TRITON 才被发现。

董事会和管理团队必须认识到 IoT 和 CPS 系统带来的新物理安全风险和网络安全风险，并使用基于风险的方法提前做好准备。

原文名称	How the Rise of IoT Is Changing the CISO Role
作者简介	菲尔·尼雷（Phil Neray）。菲尔·尼雷是物联网与工业网络安全公司 CyberX 的副总裁。
原文信息	2020 年 3 月 11 日发布于 Dark Reading 原文地址 https://www.darkreading.com/risk/how-the-rise-of-iot-is-changing-the-ciso-role/a/d-id/1337231
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。