安天发布《ArtraDownloader 木马变种分析报告》

近日，安天 CERT（安全研究与应急处理中心）发现一种名为 ArtraDownloader 的木马家族。该木马常用来下载与 BITTER 威胁组织相关的远控木马 BitterRAT，目前该木马家族被发现有三类变种。

2018 年 9 月起，持续到 2019 年初，BITTER 组织针对巴基斯坦和沙特阿拉伯发起了一波攻击，在这次攻击中大概有 80 个不同的 ArtraDownloader 恶意样本，其中最早的一个样本的时间戳是 2015 年 2 月。这些样本可大体分为三类，它们在字符串的混淆方式和 HTTP 的请求方式上有所差别。这类木马通过添加注册表自启动项来实现持久化，通过 HTTP 请求来下载并执行远程文件，字符串的混淆方式为将每个字符加上或减去一个值，并且在 HTTP 通信中也采用这样的方式进行混淆。该类木马通过恶意文档触发，攻击者通过网站入侵，将这些恶意文档上传到合法的巴基斯坦网站上，并诱骗用户下载。被入侵的网站包括政府网站、工程公司、电气供应商等。

安天 CERT 提醒广大政企客户，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。确保没有任何计算机运行直接连接到 Internet 的远程桌面服务，而是将运行远程桌面的计算机放在 VPN 之后，只有使用 VPN 才能访问它们。同时也要做好文件的备份，以防止勒索软件加密重要文件后无法恢复。

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、YARA 自定义鉴定器、文件来源信息鉴定器、数字证书鉴定器、文件元数据鉴定器、动态（Win7 x86）鉴定器、反病毒引擎鉴定器、动态（WinXP）鉴定器、聚类分析鉴定器、智能学习鉴定器、安全云鉴定器等鉴定分析。

最终依据 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	ef0cb0a1a29bcdf2b36622f72734aec8d38326fc8f7270f78bd956e706a5fd57
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	76 KB
MD5	7CC0B212D1B8CEB808C250495D83BAE4
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Casdet
判定依据	BD 静态分析

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=7CC0B212D1B8CEB808C250495D83BAE4

◆ 运行环境

操作系统	内置软件
WinXP 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	★★
打开自身进程文件	★
读取自身	★★
释放 PE 文件	★
释放加密 PE 文件	★★
Run 自启动	★
对照发现设置自启动	★
连接网络	★
疑似桌面控制	★

◆静态启发式检测

检测类型	检测点	详细说明
PE 结构	非微软的版本信息	非受信厂商的版本信息。具有较低的受信级别。
PE 结构	PE 的子系统是 GUI	基于海量恶意代码和受信白名单文件名进行数据挖掘，恶意程序通常不包含 GUI。

安天周观察
安天官方微博 安天官方微信
主办：安天 2019 年 04 月 08 日 (总第 178 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

安天发布《Windows 10 IoT Core 远程命令执行漏洞验证及建议》分析报告

近日，安天微电子与嵌入式安全研发部（安天微嵌）针对 SafeBreach 公司披露的 Windows IoT 操作系统的安全漏洞进行了详细分析和验证。攻击者利用该漏洞可实现对目标设备的完全控制，如远程命令执行、文件上传 / 下载等。安天微嵌分析验证了 SafeBreach 公司在 GitHub 中公布的该漏洞的原理及 POC，对该漏洞的影响范围进行了确认，并针对不同应用场景给出了相应的防护建议。

根据公开资料及实际验证，该漏洞目前主要影响 Windows IoT Core 的 Stock/Test Image 版本。若开发人员或厂商在最终发布的产品中使用了 Stock/Test Image 版本的系统，且该产品存在有线连接场景，则会受到此次披露的漏洞影响。构建 Custom 版本需要从 CA（Certificate Authority）购买签名证书，并使用该证书对 Custom 版本的系统进行签名，因为时间仓促，分析小组暂未对 Custom 版本的 Windows IoT 系统进行验证。

本次验证的漏洞能够不经授权便在受影响系统设备上执行上传文件和执行系统命令等高危动作，恶意软件通过本漏洞的利用很容易劫持设备成为僵尸网络的一员，成为黑客发起网络攻击的武器之一；设备也能够被黑客控制成为挖矿中的一部分；同时由于 IoT 设备应用于各行各业，一旦受到控制最直接的就是影响设备的正常运行，进而对生产生活造成影响；同时黑客也可以通过设备作为跳板进一步入侵 IoT 设备所在网络进行病毒传播、情报窃取和网络破坏等危险行为，对目标网络造成严重威胁。

虽然本次验证的漏洞仅适用于 Stock/Test Image 版本的 Windows IoT Core 系统，但由于构建 Custom 版本需要从 Certificate Authority (CA) 购买签名证书，并使用该证书对 Custom 版本的系统进行签名，厂商可能出于成本或其它方面考虑直接使用 Stock/Test Image 版本的 Windows IoT Core 系统进行产品发布，也就是说以 Stock/Test Image 版本的 Windows IoT Core 系统 IoT 设备可能已经广泛进入供应链。并且 IoT 设备在现实应用场景中进行固件升级较为困难，容易被忽视。

为有效降低漏洞所带来的威胁，提高产品安全性的同时，有效提升产品所在网络的安全防护能力，保障客户价值，安天结合漏洞的分析和验证情况给出以下三点安全建议。

建议一：产品实际的上线过程应该严格按照官方要求的研发、测试和发布流程规范操作，使用 Custom Image 而非 Stock/Test Image 版本的 Windows IoT 系统作为实际产品的发布系统，能够有效避免本次或其它未被发现的 Stock/Test Image 版本系统漏洞所产生的影响。

建议二：本漏洞所涉及到的服务使用 29817、29819、29820 三个端口，且涉及到的服务仅用于研发阶段的兼容性测试，并不是实际产品所使用的功能。在暂时无法升级固件的情况下，并确保实际产品中没有依赖相应端口的功能，以防止在关闭相应端口后影响设备的正常使用，则可以临时在 Windows IoT Core 系统防火墙中将兼容性测试服务所使用的 29817、29819、29820 三个端口进行阻断，也可暂时避免本次披露漏洞所产生的影响。但仍需要尽快升级固件修补漏洞，才能有效避免本次或其它未被发现的 Stock/Test Image 版本系统漏洞所产生的影响。在 Windows IoT Core 系统临时阻断端口的命令如下：

```
netsh advfirewall firewall set rule name=all localport=29817 protocol=tcp new enable=no

netsh advfirewall firewall set rule name=all localport=29819 protocol=tcp new enable=no

netsh advfirewall firewall set rule name=all localport=29820 protocol=tcp new enable=no
```

建议三：根据 IoT 设备所实现功能的技术特征并结合实际运行环境，详细梳理可以访问设备的 IP 列表、端口列表、访问协议类型，以及设备可以向外主动连接的协议类型、IP 列表和端口列表，结合梳理结果使用边界防火墙产品或设备专用防火墙产品配置相应的双向 IP 地址、端口和协议的白名单访问规则列表，可最大限度的保障 IoT 设备的访问安全。该方法虽然能够有效保障 IoT 设备的访问安全，降低漏洞被利用的可能，但并未根除漏洞风险，所以尽快升级固件修补漏洞，才能有效避免本次或其它未被发现的 Stock/Test Image 版本系统漏洞所产生的影响。

详细报告可扫描二维码阅读：

每周安全事件

类 型	内 容
中文标题	研究者披露微软网络浏览器中两个零日漏洞
英文标题	Expert disclosed two Zero-Day flaws in Microsoft browsers
作者及单位	Pierluigi Paganini
内容概述	研究人员披露了微软网络浏览器中两个零日漏洞的详细信息并发布了概念验证。其中一个漏洞影响最新版本的 Edge 浏览器，远程攻击者可利用漏洞绕过受害者网络浏览器上的同源策略，执行通用跨站脚本（UXSS）攻击。攻击者只需要欺骗受害者访问一个恶意网站，就可以从同一浏览器上访问过的其他网站窃取受害者的敏感数据。问题出在 Microsoft 浏览器中的资源计时条目中，这些条目在重定向后泄漏了跨源 URL。研究人员十个月前向微软报告了这些漏洞，但微软尚未有回应。
链接地址	https://securityaffairs.co/wordpress/83080/hacking/microsoft-browser-zero-day.html

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 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.FakePay.a[prv,exp] 2019-04-01	该应用程序伪装成支付相关应用，运行后上传用户银行卡相关信息，监听短信并上传，私自回复指定短信，造成用户隐私泄露和资费消耗，建议卸载。（威胁等级中）
		Trojan/Android.foxspy.a[prv,rmt,spy] 2019-04-02	该应用程序是一款间谍软件，运行后隐藏图标，接收远程控制命令，窃取用户短信、联系人、通话记录、地理位置、浏览器历史记录、社交软件信息、手机存储文件信息，私自拍照、录音、录像、截屏、拨打电话、发送短信，并将用户隐私上传，造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.SSLoveRat.a[prv,exp,rmt] 2019-04-03	该应用程序伪装正常应用，包含风险代码，触发后隐藏图标，接收远程指令，窃取用户位置、短信、通讯录、通话记录、社交应用消息等信息，并上传至服务器，会造成用户的隐私泄露和资源消耗，建议卸载。（威胁等级高）
	较为活跃的样本	Trojan/Android.Banbra.a[prv,exp]	该应用程序伪装 WA 更新程序，运行后隐藏图标，后台联网加载钓鱼界面，诱导用户填写金融相关账号密码，诱导下载其他软件。会造成用户经济损失，建议卸载。（威胁等级中）
		Trojan/Android.fconv.a[exp,rog]	该应用程序包含恶意模块，程序运行会联网上传设备固件信息，私自下载子包并加载调用，造成用户资费消耗，建议卸载。（威胁等级中）
		Trojan/Android.judspy.a[prv,spy]	该应用程序是一款间谍软件，运行后窃取用户短信、联系人、通话记录、地理位置、手机各项基本信息、手机存储内指定后缀名文件，私自通话录音，监听用户短信，并将用户隐私上传至服务器，造成用户隐私泄露，建议卸载。（威胁等级中）
		G-Ware/Android.zdecqq.a[fra,rog]	该应用程序伪装游戏外挂，本身无实际功能，诱导用户付费使用，可能造成用户资费损失，建议不要使用。（威胁等级低）
		Trojan/Android.azyte.a[prv,spy]	该应用程序是一款间谍软件，伪装系统升级，运行后窃取用户短信、联系人、通话记录、地理位置和大量手机基本信息，并上传至服务器，造成用户隐私泄露，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	Microsoft Edge 内存损坏漏洞（CVE-2019-0779）	当 Microsoft Edge 不正确地访问内存中的对象时会触发该漏洞。成功利用该漏洞的攻击者可以获得与当前用户相同的用户权限，如果当前用户使用管理用户权限登录，攻击者便可以控制受影响的系统。攻击者可任意安装程序、查看、更改或删除数据，或者创建新账户。（威胁等级高）
	较为活跃样本	GrayWare[AdWare]/Win32.Esprot	此威胁是一种灰色软件类广告程序。该家族通常与免费软件程序捆绑在一起，它会收集用户的计算机信息，包括网络浏览器的使用情况或其它电脑习惯的信息。（威胁等级低）
		Trojan[Backdoor]/Win32.Ripinip	此威胁是一种带有后门的木马类程序。该家族进入用户电脑后会为攻击者打开后门，使其可以远程控制系统。（威胁等级高）
		Trojan[Banker]/Win32.Tinba	此威胁是一种以窃取网络银行敏感信息（如银行账号、密码、信用卡信息等）为目的的木马类程序。该家族通过恶意网站或已被感染的邮件进行传播。该家族可以监控用户的网络行为，在用户登陆银行网站时记录用户信息，并将所有收集的信息发送给黑客。（威胁等级高）
		GrayWare[AdWare]/Win32.MySearch	此威胁是一种可以下载并安装推广应用的灰色软件家族。该家族样本能够收集来自用户的计算机信息，包括网络浏览器的使用情况或其它电脑习惯的信息。（威胁等级低）
		Trojan/MSWord.Agent	此威胁是一种可以释放其他恶意代码的木马家族。该家族样本一般为 Word 文档，其并没有统一的行为与功能，而是像一个木马类程序集合一样，将大量以基因片段定性的恶意代码归类。（威胁等级中）

万物互联环境下的 IT 基础设施共享带来的安全问题

Sue Poremba/ 文 安天技术公益翻译组 / 译

谁不喜欢新技术呢，特别是当新技术能够降低任务的复杂度并提高生产力时。企业采用新技术（IT 人员经常劝说安全领导层这样做）导致了数字化转型，即，企业使用数字技术来解决问题。智能手机、平板电脑和云计算引领着企业的数字化转型，但是物联网（IoT）的日益普及可能会彻底改变 IT 基础设施的现状。

然而，对于安全人员来说，数字化转型并不是什么有趣的事。虽然安全团队喜欢新技术，但新技术会增加网络安全的复杂性，特别是当这些技术共享基础设施时。

符合 PCI 标准的自动售货机

在 2 月份的 CPX 360 大会上，Check Point 公司北美工程副总裁杰夫·施瓦茨（Jeff Schwartz）发表了主题演讲，讲述了其公司休息室中升级版自动售货机的故事。他指出，越来越少的员工会随身携带现金或零钱，因此公司决定升级其自动售货机，允许信用卡支付。对于想要在下午 3 点加点餐的员工来说，这是个好消息——他们只需要拿着信用卡。

然而，正如施瓦茨所述，既然自动售货机接受信用卡支付，它就必须遵守支付卡行业（PCI）合规标准。如果忽视这一点，公司就会面临罚款。此外，自动售货机也会联网，以便处理交易。因此，它也面临着黑客攻击风险。如果自动售货机遭到攻击，就会为攻击者打开入侵企业网络的大门。

因此，最初的便利演变成了安全问题。随着物联网和数字化转型的发展，这将成为一种新的风险。施瓦茨说，共享资源和 IT 基础设施会带来更大的数据丢失风险。

对技术的日益依赖会带来风险

简而言之，新技术总是会带来风险。新的端点为攻击者提供了新的机会。这并不是说我们不需要新技术；相反，为了更好地保护网络和数据，我们需要更好地了解这些新端点的情况。

我们以前从未想过的各种设备和机器都已经连接到互联网，但是，这种联网会带来什么风险呢？以现在的智能电梯为例，它们不仅是联网端点，而且还会收集数据。

诸如电梯之类的设备可能由第三方控制，这意味着第三方也可以访问客户的网络和数据。如果一栋大楼里进驻了十几家公司，那么这十几家公司的数据和网络都会面临风险。谁来负责电梯的安全？谁来负责这些公司的数据安全？这些公司对电梯公司的安全实践又了解多少呢——他们或许从未想过电梯的安全问题。

关注客户数据安全

数字化转型不仅要考虑到业务效率，还要考虑到客户的便利性。事实上，客户希望与公司进行更轻松的互动，而这通常依赖于人工智能（AI）、机器学习（ML）和物联网等技术。例如，面向客户的 AI（例如聊天机器人）可以改善客户通信。

麻省理工学院斯隆数字经济倡议的首席研究科学家乔治·韦斯特曼（George Westerman）指出，“客户的期望远超公司能够做到的水平，这意味着公司要重新思考他们使用技术的方式。”

是的，对于能够促进更好客户关系的技术，客户抱有很高的期望。但是，随着数据泄露事件的不断发生，以及客户对数据隐私法规的认识不断提高，客户还希望公司确保其数据的安全。施瓦茨在演讲中指出，如果消费者开始根据公司收集、使用和存储客户数据的方式制定购买决策，也没什么可惊讶的。

公司能否掌控其 IT 基础设施

我们回到共享 IT 基础设施这个问题上。这不是了解网络上有哪些端点和收集数据的问题，而是了解这些端点如何随着技术的变化而变化的问题。对公司员工来说，通过一款应用操作咖啡壶非常方便，但这对数据收集有何影响呢？聊天机器人也有同样的问题：对于建立客户关系来说，它确实很方便且具有成本效益；但是，安全团队最好知道它是如何收集对话数据的，以及公司会如何使用这些数据。否则，这会导致隐私噩梦。

我们仍在研究基础设施上会发生哪些信息共享。例如，智能电视可能是查看敏感公司或消费者（例如，医院病房中的患者）信息的绝佳途径；但同时，员工（或患者）可以使用同一台电视机在午休期间登陆他们的 Netflix 或 Hulu 账户。突然之间，公司数据与个人数据就混在一起了。如果 Netflix 遭遇数据泄露事件，那么敏感的公司数据就会面临风险。

在企业中，物联网等新兴技术越来越普遍，首席信息安全官（CISO）、IT 领导者和其他决策者需要考虑使用该 IT 基础设施的每台设备都会带来什么影响。这不是哪些设备连接到企业网络的问题，而是它们如何连接以及企业是否能够掌控联网安全的问题。

原文名称	A Busy IT Infrastructure Can Lead to Security Disaster
作者简介	Sue Poremba。Sue Poremba 从 2011 年开始撰写文章，专长是网络安全和技术领域。
原文信息	2019 年 3 月 29 日发布于 Security Intelligence 原文地址 https://securityintelligence.com/a-busy-it-infrastructure-can-lead-to-security-disaster/
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。