安天发布《BabyShark 木马家族样本分析报告》

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个名为 BabyShark 的远控木马。攻击者使用鱼叉式网络钓鱼电子邮件的方式进行传播，邮件附件为恶意宏文档，文档在执行时会下载该木马。

BabyShark 是一种相对较新的恶意软件，该木马于 2018 年 11 月首次被发现，BabyShark 恶意软件的诱饵文档均采用英文编写，内容涉及东北亚安全问题。诱饵文档中的内容一部分是互联网上的公开信息，一部分是未公开的。在一个近期的样本中，攻击者使用恶意宏来下载 BabyShark 木马，文档打开并启用宏之后，会从远程位置下载 HTA 文件，下载成功之后，恶意文档以 HTTP GET 方式从 C2 服务器下载解码器，解码 HTA 文件并执行。解码后便是 BabyShark 木马，木马采用 VB 语言编写，运行后首先添加注册表项使 Microsoft Word 和 Excel 启用宏，然后执行一系列 Windows 命令并将结果保存在 %AppData% \Microsoft\ttmp.log 中，收集的数据使用 Windows certutil.exe 工具进行编码，然后通过 HTTP POST 方式传到 C2 服务器，并且添加注册表键值以达到对受害者的持久控制。

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、文件元数据鉴定器、动态（Win7 x86）鉴定器、反病毒引擎鉴定器、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	9d842c9c269345cd3b2a9ce7d338a03ffbf3765661f1ee6d5e178f40d409c3f8
文件类型	Document/Microsoft.DOCX[:Word 2007-2012]
大小	776 KB
MD5	1A6F9190E7C53CD4E9CA4532547131AF
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Downloader]/MSOffice.Agent.b
判定依据	反病毒引擎

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=1A6F9190E7C53CD4E9CA4532547131AF

◆ 运行环境

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

◆ 常见行为

行为描述	危险等级
疑似桌面控制	★

◆ UDP 信息

源 IP	源端口	目的 IP	目的端口
192.168.122.165	57211	192.168.122.1	53
192.168.122.165	60542	192.168.122.1	53
192.168.122.165	52183	192.168.122.1	53
192.168.122.165	57660	192.168.122.1	53
192.168.122.1	53	192.168.122.165	57211
192.168.122.1	53	192.168.122.165	60542
192.168.122.1	53	192.168.122.165	52183
192.168.122.1	53	192.168.122.165	57660
192.168.122.165	56787	192.168.122.1	53
192.168.122.1	53	192.168.122.165	56787
0.0.0.0	68	255.255.255.255	67
192.168.122.165	49275	224.0.0.252	5355
.....	.....	.....	.....

安天周观察
安天官方微博 安天官方微信
主办：安天 2019 年 05 月 20 日 (总第 183 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

安天助力第二届“数字中国”建设峰会网络安保工作

近日，由国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、福建省人民政府共同主办的第二届“数字中国”建设峰会于福建省福州市落幕。安天作为引领威胁检测与防御能力发展的网络安全国家队，专门组建了专业化网络安全服务小组，为峰会提供专业的网络安全保障服务，助力此次峰会顺利进行。

第二届“数字中国”建设峰会

为有效应对“数字中国”峰会期间可能发生的重大网络安全事件，最快速度地发现并处置病毒、木马、蠕虫等事件，最大限度降低其对峰会业务系统和云平台的影响，全面提高应对重大网络安全事件的能力和水平，确保数字中国峰会业务系统和云平台的安全稳定运行，**安天专业化网络安全服务小组在峰会现场使用安天探海威胁检测系统作为主要分析工具**，通过 7x24 小时的不间断安全值守，为峰会顺利开展提供人员驻点保障与网络安全监测服务。

安天专业化网络安全服务小组安保现场

安天探海威胁检测系统（英文简称 PTD，以下简称安天探海）是安天自主研发的网络侧能力型威胁检测设备，通过旁路部署，实现全流量、高精度的网络数据实时捕获和威胁检测，具备恶意代码传输检测、威胁码活跃行为（包括木马远程控制、蠕虫传播、网络入侵等）检测、漏洞利用发现等威胁监测能力的同时提供全要素的数据记录能力。在针对高价值资产的网络攻击愈演愈烈的现状下，安天探海面向关键信息基础设施和重要 IT 资产，提供业内领先的威胁监测能力的同时支撑高级威胁分析，为本次峰会业务系统和云平台提供了威胁持续监测、快速分析的能力，提升了安全服务人员响应威胁的效率。

安天以“达成客户有效安全价值，提升客户安全获得感，改善客户的安全认知”为企业纲领，作为被行业管理机构、客户和伙伴广泛认可的网络安全企业，安天已连续五届蝉联国家级安全应急支撑单位，亦是中国国家信息安全漏洞库六家首批一级支撑单位之一。在本次峰会中，安天积极与各友商合作，共同赋能客户，为峰会提升全天候的恶意代码安全监测能力与应急响应处置能力做出贡献。未来，安天将在网络安全领域持续创新，不断为客户创造价值。

Windows 远程代码执行漏洞 (CVE-2019-0708) 预警

概述

2019 年 5 月 14 日微软官方发布了对远程桌面服务（Remote Desktop Services）的关键远程代码执行漏洞 CVE-2019-0708 的安全补丁，受影响的 Windows 系统版本在启用了远程桌面服务时容易遭受远程代码执行攻击。该漏洞不需要用户交互，即该漏洞可以被利用发起蠕虫类攻击，类似 WannaCry（魔窟）勒索蠕虫事件。虽然目前没有发现对该漏洞的利用，但之后攻击者很可能将该漏洞利用加入到恶意代码中，就像 MS17-010（永恒之蓝）漏洞一样，微软在 2017 年 3 月 14 日发布 MS17-010 漏洞补丁，2017 年 5 月 17 日 WannaCry（魔窟）利用永恒之蓝漏洞进行传播。

根据相关数据源统计，目前，全球公共网络中有近 300 多万计算机开启了 3389 端口，即未改变端口的远程桌面服务（RDP），对于没有经过配置加固的内网更有大量机器开放相关端口服务。因此，该漏洞既可能造成互联网大面积的蠕虫传播、僵尸网络大面积感染，也能形成内网大面积横向移动攻击能力。

漏洞描述

漏洞编号：CVE-2019-0708

该漏洞允许未经身份验证的攻击者使用远程桌面服务连接到目标系统并发送精心设计过的请求，利用其身份预认证、不需要用户交互确认同意接收连接的缺陷，即可在目标系统上执行任意代码，涵盖但不限于安装程序，查看、更改或删除目标系统内数据，或创建具有完全用户权限的新账户。

利用此漏洞需要满足以下条件：

1. 在 Windows 操作系统启用了 Remote Desktop Services 远程桌面服务，且未及时安装更新补丁；
2. 攻击者通过 RDP 向目标系统远程桌面服务发送精心设计的请求。

受影响范围

受影响的 Windows 系统版本：

Windows XP SP3 x86

（下接第二版）

（上接第一版）
Windows XP 专业 x64 版 SP2
Windows XP Embedded SP3 x86
Windows 7 for 32-bit Systems Service Pack 1
Windows 7 for x64-based Systems Service Pack 1
Windows Server 2003 SP2 x86
Windows Server 2003 x64 版本 SP2
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows Server 2008 for Itanium-Based Systems Service Pack 2
Windows Server 2008 for x64-based Systems Service Pack 2
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)

修复及缓解建议

1、尽快安装此漏洞的补丁（即使已经禁用远程桌面服务）[1]。

2、如果不需要使用远程桌面服务，建议禁用该服务。

3、在受影响版本的系统上启用网络级身份验证（NLA）；启用 NLA 后，攻击者需要使用目标系统上的有效账户对远程桌面服务进行身份验证，才能成功利用该漏洞。

4、 在企业外围或边界防火墙上部署安全策略，阻止 TCP 端口 3389。

5、 安天智甲终端防御系统与安天资产安全运维系统组合使用，可以充分减少暴露面，形成威胁防御响应的基础框架。

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 7 个移动平台恶意代码和 6 个 PC 平台的恶意代码和漏洞值得关注

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.DownAnubis.a[exp,rog] 2019-05-11	该应用程序伪装为正常应用，运行以更新 GoolePlayService 的名义诱导用户下载银行木马 Anubis，造成用户的资费消耗和隐私泄露，存在较大的安全风险，建议卸载。（威胁等级中）
		Trojan/Android.SalesCollect.c[prv,exp] 2019-05-12	该应用程序运行会收集手机号、系统版本号、用户地理位置等信息，私自发送注册短信并且删除用户短信，造成用户隐私泄露和资费消耗，影响用户正常使用，建议卸载。（威胁等级中）
		Trojan/Android.apisyncSpy.a[prv,rmt,spy] 2019-05-13	该应用程序是一款间谍软件，运行后隐藏图标，获取 root 权限，接收远程控制命令，后台窃取用户短信、联系人、通话记录、地理位置、手机软件安装信息、wifi 信息、手机固件信息，监听用户短信和通话，私自拍照、录音、录像、截屏、下载其他 apk。并将用户隐私上传至服务器。造成用户隐私泄露，建议立即卸载。（威胁等级高）
	较为活跃的样本	Trojan/Android.Kredyt.a[prv,exp]	该应用程序伪装为金融相关应用，运行通过钓鱼页面诱导用户填写信息，后台窃取用户手机相关信息、短信、通话记录等并上传，造成用户的隐私泄露和资费消耗，警惕其造成用户的财产损失，建议卸载。（威胁等级高）
		G-Ware/Android.yueyou.a[exp,rog]	该应用程序是非官方版本，被植入了广告子包和其他软件，运行后推送流氓广告，要求用户安装推广软件，造成用户流量消耗，影响用户体验，建议不要使用。（威胁等级中）
		G-Ware/Android.FakeWhatsApp.b[exp,rog]	该应用程序伪装 WhatsApp，无实际功能，运行后私自加载推送广告，造成用户流量消耗，建议不要使用。（威胁等级低）
		Trojan/Android.nbank.i[prv,exp]	该程序运行隐藏图标，加载恶意子包，子包中存在上传用户手机固件、联系人、短信、彩信、通话录音、程序安装列表等隐私信息的行为，还会判断是否存在指定银行 app 上传包名，同时存在私发短信、修改手机设置、拨打电话、设置置顶虚假界面等高危行为，造成用户隐私泄露和资费损耗，请卸载。（威胁等级高）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Windows 远程桌面服务（RDP）关键远程代码执行漏洞（CVE-2019-0708）	该漏洞允许未经身份验证的攻击者使用远程桌面服务连接到目标系统并发送精心设计过的请求，利用其身份预认证、不需要用户交互确认同意接收连接的缺陷，即可在目标系统上执行任意代码，涵盖但不限于安装程序，查看、更改或删除目标系统内数据，或创建具有完全用户权限的新账户。（威胁等级高）
	较为活跃样本	GrayWare[AdWare]/Win32.Boran	此威胁是一种具有广告件行为的灰色软件家族。该家族的样本在执行后会在用户的计算机上弹出广告。并且该家族的样本还会下载其他恶意软件程序对计算机进行感染。（威胁等级中）
		Trojan[Backdoor]/PHP.Pbot	此威胁是一种使用 PHP 语言编写的带有后门的木马类程序。该家族基于 Linux 和 Windows 平台，该家族会在后台链接到 IRC 服务器获取恶意指令。该家族木马可以执行指定命令，下载任意文件。（威胁等级高）
		RiskWare[WebToolbar]/Win64.Agent	此威胁是一种具有安装浏览器扩展工具栏的风险软件家族。该家族样本基于 64 位系统，它并没有统一的行为与功能，是将大量基因片段定性的恶意代码进行归类。（威胁等级中）
		RiskWare[RiskTool]/Win32.Patcher	此威胁是一种风险软件家族。该家族样本使用 DNF 图标进行伪装，运行后会释放并启动多个可执行程序，版本信息显示为游戏多开程序，会窃取游戏账号密码。（威胁等级中）
		RiskWare[WebToolbar]/NSIS.Agent	此威胁是一种具有安装浏览器扩展工具栏的风险软件家族。该家族样本通过 NSIS 打包可以捆绑其他恶意代码到用户系统中。该家族是以基因片段定性的恶意代码分类，该家族并没有统一的行为与的功能，而是像一个集合一样，将大量基因片段定性的恶意代码归类。（威胁等级中）

清查社交媒体 保护数据安全

Sam Small/ 文 安天技术公益翻译组 / 译

春天到来，天气渐暖，阳光明媚，人们莫名其妙有点想要大扫除的冲动。许多人会花时间清理壁橱或清理咖啡桌上的书籍；但是，春天也是企业检查或重新评估其社交媒体和相关活动安全状况的好时机。毕竟，人们希望春天永驻，但攻击者可从未停止活动，他们一年四季都在盯着企业和社交媒体用户。

我们以近期席卷了社交媒体的网络钓鱼骗局为例。攻击者告知用户他们被列入了所谓的“讨厌清单”，诱骗他们登录伪造的页面来了解更多信息，从而收集用户的登录凭证。一旦获得用户的凭证，攻击者就可以攻击其关注者，进一步扩散该骗局。

这类攻击变得更频繁、更危险。企业必须花时间审查其社交媒体和数字风险流程，以更好地了解其面临的威胁。这有助于企业积极准备防患于未然，确保其业务、客户、员工和品牌免受数据泄露和信息泄露的影响。

以下是帮助企业“清查”社交媒体的三个建议。

建议 1：保护公司数据

企业需要评估与其数据相关的风险。首先，企业要了解他们有哪些数据和账户。保留社交媒体账户、域名、电子商务网站，以及企业拥有或相关的其他数字渠道的清单，将提供有价值的见解。在清点过程中，企业还应查看账户的隐私设置，确保数据得到妥善的保护。

企业需要考虑的问题包括：我们分享了什么？谁能查看我们的帖子？谁能查看我们的位置消息、联系信息或其他私人信息？

口令安全是保护数据的另一个重要方面，

包括选择强口令以及不重复使用口令。攻击者知道用户通常不会采纳此建议，因此他们经常利用窃取的凭证登录用户的其他账户，这会加剧攻击风险和损害。如果必须分享账户口令，请考虑采用具有协作功能的口令管理器，而不是分享包含敏感信息的电子表格或文本文件。

企业需要评估口令安全、策略和培训资料，精心设置口令，确保口令不重复、不会被攻击者轻易获取。

此外，公司必须监控风险账户行为的早期预警信号。攻破账户后，攻击者和网络犯罪分子通常会立即更改显示名称、头像、个人资料等信息。因此，企业应审查自己的账户及其关注者，避免意外更改，并清除可疑的关注者。

识别账户攻击迹象，有助于安全团队在账户被劫持时立即采取行动。

建议 2：保护员工及其个人网络

精明的员工可以成为企业的最佳品牌大使，特别是在社交媒体上，许多软件工具使员工可以轻松地在个人网络上分享或发布最新的公司新闻。

为确保员工的数据安全，企业可以考虑开展员工培训和教育计划，指导员工保护自己。在有利于员工安全分享公司新闻的工具方面进行投入，也有助于该工作。

在清查过程中，企业需审查可能过时的策略并进行更新。员工培训计划不仅要提供与企业社交媒体策略有关的指导，还要给出社交媒体安全最佳实践。企业需要考虑的关键问题包括：

- 可以或不可以分享的信息类型
- 与客户互动的策略
- 与内部渠道和协作工具（如 Slack）相关的策略

许多公司已经在与电子邮件等传统应用有关的员工培训方面进行了适当投入，以便更好地应对此类安全风险。但是，在当今的数字时代，开展与社交媒体和数字渠道有关的员工培训也很有必要。

建议 3：保护客户数据

保持账户安全和良好配置不仅可以保护企业品牌不被冒充者、攻击者、网络犯罪分子和垃圾邮件侵害，还可以保护企业的社交媒体关注者和客户。

在这种情况下，企业应将客户数据的使用完全透明化，并警惕和监控滥用或违规行为。在主动识别并快速修复针对性攻击或诈骗的工具或流程方面进行适当投入，有助于缓解压力并满足此类要求。企业还应配备能够识别和删除客户诈骗、恶意链接以及账户模仿 / 劫持的支持团队，以保护企业员工及客户，避免代价高昂的业务中断或声誉受损。

现在正是企业完善社交媒体安全计划和最佳实践的好时机。从数字营销策略到安全协议、数字风险识别和最小化，对于企业的业务安全都至关重要。

原文名称	Tips to spring clean your company’s social media and stay protected
作者简介	Sam Small。Sam Small 是 ZeroFOX 公司的首席安全官。
原文信息	2019 年 5 月 13 日发布于 Help Net Security 原文地址 https://www.helpnetsecurity.com/2019/05/13/company-social-media-hygiene/
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。