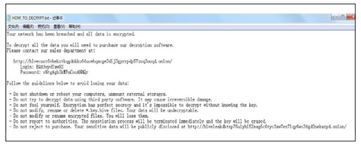
安天智甲有效防护 Hive 勒索软件

近日，安天 CERT 在梳理网络安全事件时发现了一个名为 Hive 的勒索软件。该勒索软件最早被发现于 2021 年 6 月，主要通过垃圾邮件进行传播。经验证，安天智甲终端防御系统（简称 IEP）的勒索软件防护模块可有效阻止 Hive 勒索软件的加密行为。

Hive 勒索软件运行后释放并运行一个名为“shadow.bat”的 bat 脚本文件，该脚本主要功能为调用 vssadmin.exe 命令删除系统卷影，防止恢复被加密的文件；随后创建多个线程，对特定后缀名的文档、压缩包、图片、音视频等文件进行加密，采用 AES 对称加密算法进行加密，加密后的文件名为“原始文件名 + 一段编码 +.hive”。文件加密过程中，该勒索软件在自身同目录下释放一个名为“hive.bat”文件，同时后台运行该脚本文件，功能为监控勒索软件的运行，一旦勒索软件停止运行将删除该勒索软件和 hive.bat 脚本文件。文件加密完成后，用内置的硬编码 RSA 公钥对 AES 密钥进行加密，将其写入到一个名为“一段编码 +.key.hive”的文件中并在 D 盘释放。勒索软件在每个被加密文件的同目录下生成名为“HOW_TO_DECRYPT.txt”勒索信，该勒索信内容有勒索说明、暗网聊天室的联系方式、7 条勒索警告，其中包括在勒索信中警告，如果删除以 key.hive 为后缀的文件，加密文件将无法解密。



▲Hive 勒索软件勒索信息

Hive 勒索软件采用“AES+RSA”加密算法组合的形式加密文件，目前被加密的文件暂时无法解密。

安天提醒广大用户，及时备份重要文件，且文件备份应与主机隔离；及时安装更新补丁，避免勒索软件利用漏洞感染计算机；对非可信来源的邮件保持警惕，避免打开附件或点击邮件中的链接；尽量避免打开社交媒体分享的来源不明的链接，给信任网站添加书签并通过书签访问；避免使用弱口令或统一的密码；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；可以使用反病毒软件（如安天智甲）扫描邮件附件，确认安全后再运行。目前，安天追影产品已经实现了对该类勒索软件的鉴定；安天智甲已经实现了对该勒索软件的查杀。

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，下为其自动生成的分析报告：

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（Win7sp1 x86）鉴定器、字符串分析鉴定器、文件相似分析鉴定器、智能学习鉴定器、静态特征检测鉴定器、安全云鉴定器、动态（WinXP）鉴定器、动态（Win7 x86）鉴定器等鉴定分析。

最终依据 BD 静态分析鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	2f9fc82898d718f2abe99c4a6fa79e69
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	764 KB
MD5	2F9FC82898D718F2ABE99C4A6FA79E69
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Razy
判定依据	BD 静态分析

报告地址：https://1.119.163.6/vue/details?hash=2F9FC82898D718F2ABE99C4A6FA79E69

◆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、Office2007、Flash、WPS、FoxitReader、AdobeReader

◆危险行为

行为描述	危险等级
映射内存方式注入	★★★
向服务发送控制代码	★★★
搜索文件	★★★★
修改文件后缀名	★★★★
查询软件限制策略	★★★
删除卷影副本	★★★★
疑似勒索软件篡改或加密文件	★★★★★
在系统目录创建文件	★★★

◆扫描二维码查看完整报告

安天周观察
安天对外开放资料平台　安天官方微信
主办：安天　2021年07月19日（总第287期）试行　本期4版　扫描上方二维码查询安天所有对外开放资料

XCon2021 | 移动互联网黑灰产对抗与治理

随着移动互联网技术的飞速发展，无线网络、可移动智能设备的数量正在以前所未有的迅猛态势持续增加。从技术层到实践层，伴随应用场景的日益丰富，移动网络已渗透到了社会发展的各个方面，并逐渐成为了人们生产生活不可或缺的手段和工具。

然而技术的发展始终是双刃剑，在带来便捷高效的同时，受制于无线网络和移动设备的开放性、结构复杂性等特点，移动互联网所面临的安全问题也日渐凸显。特别是在移动电子商务、移动支付广泛应用的今天，各类智能设备越来越多的成为了恶意攻击者锁定的目标，而由此导致的用户个人信息泄露频出、财产严重损失的案例也偶有发生。安全行业与黑灰产的博弈从未停止。

在即将召开的 XCon2021 安全焦点信息安全技术峰会上，安天移动安全高级副总裁陈家林将分享议题《移动互联网黑灰产对抗与治理》，该议题是基于安天移动安全十年来针对移动互联网恶意代码、APT、黑灰产的持续跟踪和对抗基础的研究，从经验处着手，深入剖析黑灰产对抗与治理的思考与实践。

移动互联网黑灰产对抗与治理

议题简介

议题将回顾过去十年移动终端对抗技术的发展，通过移动互联网用户安全现状和变化趋势的分析，依托持续化运营、预警和检测，透过安天移动安全的风险防护、管理与应对视角分享移动互联网下的黑灰产对抗和治理问题的解决思路。

议题亮点

1. 本议题将对过去十年移动终端安全威胁进行回顾，并介绍当前移动互联网用户所面临的安全现状和问题。

2. 重点介绍近几年来，移动互联网下黑灰产的对抗升级以及安天移动安全首次提出的应用风险性的安全理念。

3. 首次介绍如何从风险视角看待移动 APP 对终端用户安全性的影响，并以此进行黑灰产对抗和治理。

安天移动安全高级副总裁陈家林，系

▲ 安天移动安全高级副总裁 陈家林

武汉大学硕士研究生学历，拥有 14 年计算机工程从业经验，曾担任全球顶尖芯片公司高级技术总监，现任安天移动安全高级副总裁。主研方向为物联网，车联网等下一代安全方向，先后与工信部泰尔实验室、中国银联、华为、蚂蚁金服等机构、厂商达成技术合作。至今已申请 10 余件国家发明专利，获得 10 余件软件著作权。（原文链接：https://mp.weixin.qq.com/s/8RHkcEAmqvgX-xA-sq67Cg）

扫描右侧二维码阅读全文

Zloader 恶意软件使用新感染技术进行传播

McAfee Labs 研究人员发现 Zloader 恶意软件使用一种新技术传播，即在初始网络钓鱼邮件附件宏中不包含任何恶意代码。初始网络钓鱼邮件包含 Microsoft Word 文档附件。打开文档后，会从远程服务器下载受密码保护的 Microsoft Excel 文件。Word 文档 VBA 读取 Excel 文件的单元格内容，并作为宏写入 Excel VBA。一旦将宏写入 Excel 文件，Word 文档将注册表中的策略设置为禁用 Excel 宏警告，并从 Excel 文件动态调用恶意宏函数，然后下载 Zloader 载荷，然后由 rundll32.exe 执行 Zloader。（原文链接：https://www.mcafee.com/blogs/other-blogs/mcafee-labs/zloader-with-a-new-infection-technique/）

Trickbot 针对高价值目标更新其 VNC 模块

网络安全研究人员揭开了恶意软件 Trickbot 持续死灰复燃的谜底，TrickBot 已经发展到使用复杂的基础设施，该基础设施会破坏第三方服务器并利用它们来托管恶意软件。根据研究人员的说法，已经发现攻击者正在积极开发一个名为“vncDll”的模块的更新版本，该模块用于针对选定的目标进行监控和情报收集，新版本已命名为“tvncDll”。新模块旨在与其配置文件中定义的九个 C2 服务器中的一个进行通信，使用它来检索一组攻击命令、下载更多恶意软件的有效载荷，并将从机器收集到的信息传回服务器。（原文链接：https://thehackernews.com/2021/07/trickbot-malware-returns-with-new-vnc.html）

研究人员发现新的 Joker 木马变种

Cyble 研究人员最近在日常威胁搜索过程中从 Google Play 商店发现了一个新的变种 Joker Dropper。该应用程序被发现是 Joker 的更新版本，它会下载其他的恶意软件到设备上，并在用户不知情的情况下向用户订阅高级服务。这是 Joker 恶意软件的常见功能。这款应用直到 2021 年 7 月 5 日都在 Google Play 商店中。尽管 Google 立即从商店中删除了该程序，但该程序已经有 500 多次安装。尽管谷歌删除了该恶意软件，但攻击者不断对应用程序和有效负载进行轻微修改，从而使该恶意软件能够逃避 Google Play 商店的检测。（原文链接：https://blog.cyble.com/2021/07/09/android-app-disguised-as-a-qr-scanner-spreads-joker-variant-trojan/）

每周安全事件

类 型	内 容
中文标题	黑客攻击伊朗铁路系统网络并发布虚假消息
英文标题	Iran’s railroad system was hit by a cyberattack, hackers posted fake delay messages
作者	Pierluigi Paganini
内容概述	伊朗铁路系统遭遇网络攻击，攻击者在全国各地车站的显示屏上发布了关于火车延误或取消的虚假信息。显示屏显示，火车因网络攻击而延误或取消，还敦促乘客致电询问信息，并提供了伊朗国家领导人阿亚图拉·阿里·哈梅内伊（Ayatollah Ali Khamenei）办公室的电话号码。伊朗国家铁路公司发言人表示，该事件并未对火车服务造成任何问题。目前，尚不清楚谁此次攻击的幕后黑手。
链接地址	https://securityaffairs.co/wordpress/119942/hacking/irans-railroad-system-cyberattack.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 3 个活跃的漏洞以及 7 个活跃的恶意代码家族值得关注

恶意代码类别	名称	威胁等级	简要描述
活跃漏洞	Microsoft Defender 远程代码执行漏洞（CVE-2021-31985）	高	Microsoft Defender 存在远程代码执行漏洞。由于 Microsoft Defender 中的输入验证不正确，使得攻击者可以在目标系统上执行任意代码。
	Apache Dubbo 远程代码执行漏洞（CVE-2021-25641）	高	Apache Dubbo 存在远程代码执行漏洞。由于处理序列化数据时存在不安全的输入验证，使得攻击者可以将特制数据传递给应用程序并在目标系统上执行任意代码。
	PHP 服务端请求伪造漏洞（CVE-2021-21705）	高	PHP 存在服务端请求伪造漏洞。由于对用户提供的输入的验证不足，使得攻击者可以发送特制的 HTTP 请求，绕过 FILTER_VALIDATE_URL 并欺骗应用程序向任意系统发起请求。
较为活跃样本家族	Trojan[Packed]/Win32.Krap	中	此威胁是一种窃取账号信息的木马类家族。该家族木马运行后会注入系统进程，并监视正在运行的窗口标题，利用键盘 hook、内存截取或者封包截取等方式窃取账户信息并将这些信息发送到指定的服务器。
	Trojan[Dropper]/Win32.Dinwod	中	此威胁是一种具有释放或捆绑行为的木马类家族。该家族木马在感染用户系统之后，会自动释放并安装其它恶意程序。该家族的部分变种还具有强制关闭杀毒软件的能力。
	Trojan[Proxy]/Win32.Qukart	中	此威胁是一种可以窃取用户信息并通过代理服务器回传信息的木马类家族。该家族样本收集系统的敏感信息，通过 http 请求发送到指定网页。该家族在后台会自动更新。
	Trojan[Backdoor]/Win32.Salgorea	中	此威胁是一种可以下载恶意代码的木马类家族。该家族样本运行后连接网络下载恶意代码并执行。
	Worm/Win32.AutoRun	中	此威胁是一种蠕虫类程序。该家族能够在磁盘根目录或插入的可移动存储介质的根目录下创建一个 autorun.inf 文件并自我复制，该文件中包含可执行蠕虫的名字和路径。用户将磁盘或可移动存储介质接入电脑后，系统会自动执行 autorun.inf 中指定的可执行程序。该家族除了能够感染本地电脑外，还可以通过共享文件传播至远程电脑中。
	Trojan[Backdoor]/Linux.Mirai	中	此威胁是一种 Linux 平台上的僵尸网络家族。该家族样本主要是利用漏洞传播并组建僵尸网络，并利用僵尸网络传播相关恶意软件。
	Trojan/Android.Boogr	中	此威胁是安卓平台上的伪装类木马家族。该家族木马通常伪装成游戏或流行应用程序，运行后可以下载其他恶意文件，将 SMS 消息发送给高价软件，或将受害者的智能手机连接到攻击者的命令和控制服务器。

分布式云：云计算的未来

诺曼·刘易斯 / 文 安天技术公益翻译组 / 译

越来越多的公司开始转向分布式云。分布式云是一种全新的云计算方法。Gartner 分析师认为，向分布式云的迁移是 2021 年十大技术趋势之一。为何说分布式云对企业是有益的？它们有哪些优势？本文将对此进行分析。

分布式云是什么？

分布式云是一种允许用户使用集中式资源的云服务，如有必要，用户可以在本地设备上启动计算过程。云服务提供商可以管理集中和区域数据中心的设备。分布式云还引入了具有战略优势位置的变电站。在边缘计算的情况下，能够与资源的物理位置绑定。

内容交付网络（CDN）就是分布式云的一个例子。CDN 是地理上分散的网络基础设施，旨在向不同位置的用户优化和快速交付内容（通常是视频或音频），这会显著提升下载速度。分布式云不仅有利于媒体内容的创作者和提供者，还可以应用于从运输到销售的各种业务领域。

即使是特定的地理区域，也可以使用分布式云。例如，文件传输服务提供商可以使用集中式云资源，在地理位置分散的 CDN 上以多种格式对视频和存储内容进行格式化。在服务需求会增加的特定位置，文件传输服务提供商可以将数据放置在一些居民区的本地存储中，甚至可以放置在人口稠密地区的 5G 站中，以确保在移动设备上快速下载视频。

分布式云与混合云有何不同？

分布式云还只是一种趋势，尚未被大多数人所熟知，许多人会将其与混合云搞混。实际上，分布式云和混合云都可以增加业务机会，但是它们存在根本性的区别。在混合基础设施的情况下，分布式云支持边缘计算，也能在地理上扩展计算环境。

分布式云的优势是什么？

支持边缘计算的分布式云是一种自然趋势。企业的需求已经发生了变化，混合云基础架构甚至也不再适合企业，尤其是大型企业。这主要是因为，分布式云服务有助于避免私有云和公有云之间的差距（这在使用混合基础设施时经常发生）。此外，分布式云还有其他优势。

1. 减少延迟并提高性能。云资源离特定位置越近，最终用户接收计算过程（内容交付、数据分析等）的速度就越快。

2. 扩展业务。引入分布式云的企业，可以增加计算区域的数量和可用性。

3. 降低成本。尽管混合云需要共享基础架构，但其管理是资源密集型的。企业需要控制两种环境，就需要雇佣更多的专业员工，因此需要支付更多费用。分布式云可以显著减轻企业的经济负担。

4. 降低出现网络故障的风险。不同于集中式云，分布式云能够分布到不同位置，有助于避免庞大和冗长的问题。

5. 增强合规性。不同的国家有不同的法律，企业的业务可能不符合当地法规。边缘计算可以帮助企业遵守特定国家的法律。在无法将特定数据带出某个国家的情况下，这一点尤其重要。

6. 如果企业需要自己控制和管理私有云，服务提供商将直接监控分布式云。这会降低设备管理成本，并使企业在出现技术故障时也能够专注于其任务，而非在专家的帮助下解决问题。

分布式云的未来

向分布式云的过渡正在成为最重要的趋势之一。正如分析师所说，在未来，这项技术将快速发展。目前而言，云提供商正忙于配备他们将用于边缘计算的变电站。据专家预测，到 2025 年，云服务将在信息通信技术中占据主导地位，分布式云的普及也会随之增长。

结论

企业的云迁移已经进行了很长一段时间了，到 2021 年，云变得尤为重要。具体来说，企业已经开始集体向大型供应商订购云服务。因此，谷歌等云服务提供商的利润已经翻了好几番。这仅仅是个开始，企业对云服务的需求还会不断增长。

原文名称	Distributed Cloud: The Future of Cloud Computing
作者简介	诺曼·刘易斯（Norman Lewis），一位经验丰富的数据科学家。
原文信息	2021 年 7 月 8 日发布于 Network Computing 原文地址 https://www.networkcomputing.com/cloud-infrastructure/distributed-cloud-future-cloud-computing
摘 要	分布式云是一种允许用户使用集中式资源的云服务，如有必要，用户可以在本地设备上启动计算过程。云服务提供商可以管理集中和区域数据中心的设备。分布式云还引入了具有战略优势位置的变电站。在边缘计算的情况下，能够与资源的物理位置绑定。
免责声明	本译文不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天集团一律不予承担。