安天发布《Remcos 远控木马分析报告》

近日，安天 CERT 在梳理网络安全事件时发现了利用 COVID-19 为主题的钓鱼邮件传播 Remcos 远控木马活动。该活动主要针对小型企业、制造企业和会计师事务所。Remcos 远控木马是 2016 年公开售卖的远控木马，该木马主要通过钓鱼邮件进行传播，目的是窃取用户个人信息。

该活动通过钓鱼邮件进行传播，附件中包含一个使用误导性 PDF 图标的可执行文件，该可执行文件一旦执行便会启动 Remcos 远控木马。该木马执行后将自身注入到系统默认浏览器中并添加到注册表。Remcos 远控木马主要功能包括远程桌面控制、键盘记录、收集主机信息、获取进程路径、获取浏览器 Cookie 信息、上传可能包含敏感信息的文本文件、获取进程列表、结束指定进程、获取屏幕截图以及打开 CMD 等。

安天 CERT 提醒广大政企客户，应提高网络安全意识。在日常工作中及时进行系统更新和漏洞修复，不随意下载非正版的应用软件，注册机等。收发邮件时应确认收发来源是否可靠，不随意点击或者复制邮件中的网址，不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良好习惯。确保所有的计算机在使用远程桌面服务时避免使用弱口令，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远控木马的鉴定；安天智甲已经实现了对该远控木马的查杀。

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、智能学习鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	18ab.exe
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	124 KB
MD5	444AF85AE5787F585CB2B554D86DBFEE
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Backdoor]/Win32.Remcos
判定依据	反病毒引擎

◆ 操作系统

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

◆危险行为

行为描述	危险等级
向其他进程内存写入数据	★★★
获取剪切板内容	★★★
检测虚拟机	★★★★★

◆常见行为

行为描述	危险等级
加载运行时 DLL	★
获取系统版本	★★
打开自身进程文件	★
读取自身	★★
创建挂起进程	★★
在其他进程中申请内存	★
获取计算机名	★
获取系统信息（处理器版本、处理器类型等）	★
消息钩子注入	★★
DNS 请求	★
创建窗口	★
获取当前激活的窗口	★★
访问文件尾部	★
隐藏文件	★
连接网络	★
检索系统内存信息	★
疑似桌面控制	★

◆进程监控

PID	创建	命令行
1376	target.exe	"c:\f7a0dc9340074c73a53a74df046706db\share\target.exe"
1352	target.exe	"c:\Program Files\Mozilla Firefox\firefox.exe"

◆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 5 月 11 日 (总第 229 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

安天移动安全智信入选工信部首批中小企业数字化赋能服务产品推荐目录

近日，工业和信息化部中小企业局发布《中小企业数字化赋能服务产品及活动推荐目录（第一期）》，安天移动安全自主研发的“智信零信任应用安全交付系统”凭借全局安全防护感知能力、高效低成本移动迁移、智能化访问策略、灵活多样交付方式等特色优势，成为网络和数据安全类产品首选推荐。

▲智信零信任应用安全交付系统入选目录

智信零信任应用安全交付系统，依托安天移动安全移动反病毒核心能力，以零信任安全架构为基础，专为解决政企等机构在构建移动化、数字化办公环境安全问题的端管云协同的企业级安全解决方案。不仅能为用户建立一套完整的虚拟安全边界，且提供更加安全的应用访问环境，为企业移动智慧化保驾护航。在未来更加开放的网络环境中，智信零信任产品为企业筑起一道安全屏障，保障企业在享受移动办公高效便利的同时，终端、数据、业务等均能得到有效保护，并基于可视化的呈现方式让安全可视、可控。

此次入选，既是对安天移动安全在移动安全领域核心技术实力的认可，也是对安天移动安全在为企业数字化赋能和推动转型等方面所作努力的肯定。未来，安天移动安全将以移动反病毒核心技术为基础，并通过独立移动威胁分析鉴定技术体系、自主工程化平台和安全专家能力，不断加强和优化移动应用系列产品的防护能力，为政企机构移动业务应用场景提供管理、监测、处置、决策的全方位安全能力支撑，严守政企数据安全底线。

智信零信任应用安全交付系统介绍

智信零信任应用安全交付系统，在零信任安全架构基础上协助客户构建企业动态虚拟安全边界，为企业提供安全可靠的应用访问环境。通过统一身份认证、单点登录、链路透明加解密为企业提供应用统一安全入口，相比传统 VPN 更加安全便捷；通过 web 应用移动化、终端环境检测助力企业低成本构建安全移动办公环境；通过基于身份、状态、行为、内容的零信任策略，保障应用访问安全性；基于数字水印、文档不落地、邮件代理等技术保障企业数据资产全生命周期安全。由智信安全工作空间（SDK）、智信应用安全交付网关、

▲智信零信任应用安全交付系统

零信任策略优化平台组成。

产品特点

●零信任安全策略模型

基于零信任安全架构，提供基于用户身份、行为、内容、环境的动态安全访问控制策略，内置多种安全策略模型，用户可基于自身需要灵活配置和选择。

●统一身份认证及管理

统一企业应用认证入口，集中化身份管理，可基于企业组织架构和人员业务属性进行集中的身份和权限管理。为企业众多的应用提供统一的身份管理能力，保障应用低成本接入。

●数据防泄露能力

通过应用的统一管控增强数据的访问控制及审计能力；基于网关实现文档数据的透明加解密和数字水印保障数据流通过程中的安全性（针对移动端的数据共享以及邮件文档外发的场景）；链路层加密保障应用数据传输过程中安全。

●邮件安全代理能力

应用安全交付网关提供了邮件代理功能，支持 SMTP、IMAP、POP3 协议以及这三种协议的 SSL 版本。

●敏感文档检测能力

支持对邮件附件、文件分享、文件下载进行安全防泄密审查，通过对涉密文档生成 MD5 和敏感关键字配置，发送邮件、文件分享下载时对文档进行 MD5 匹配和敏感关键字匹配，配合数据防泄漏管理策略，通过附件加水印、附件公钥加密、阻断外发，防止文件被泄密。

●良好的移动端支持

为满足企业移动信息化建设的大趋势，应用交付系统可提供移动安全 SDK 和 APP 支持，保障访问企业内部应用的终端安全，并支持企业内部应用的通过第三方社交应用分享，满足员工随时随地安全的访问企业内部应用以及分享企业内部机密文档。

●多产品形态支持

交付网关产品提供硬件盒子服务器形态、盒子 mini 服务器形态和 SaaS 版本形态，满足不同的客户场景需求。盒子形态适用于企业内部应用部署在内网的场景，可根据企业员工数量灵活选择不同的型号配置，SaaS 版本适用于云数据中心场景。

微信扫描二维码阅读原文

每周安全事件

类 型	内 容
中文标题	欧洲当局捣毁名为 InfinityBlack 的网络犯罪组织
英文标题	European Authorities Dismantle 'InfinityBlack' Hacker Group
作者及单位	Eduard Kovacs
内容概述	欧洲执法当局表示，在波兰和瑞士逮捕了数人之后，捣毁了一个名为“ InfinityBlack”的网络犯罪组织。Infinity Black 是一个网站，黑客可以在其中共享被盗的用户凭据。该网站由一个组织运营，该组织建立了多个平台，专门销售受损的登录凭据。这些凭据以所谓的“组合列表”出售，其中包括许多可用于撞库攻击的用户名和密码组合。InfinityBlack 组织不仅参与了被盗凭据的分发，而且还参与了恶意软件和黑客工具以及网络欺诈的开发和分发。在波兰国家警察搜查了六个地点并没收了价值约 10 万欧元的设备后，4 月 29 日在波兰逮捕了 5 名犯罪嫌疑人。警方还关闭了两个托管数据库的平台，这些平台拥有超过 1.7 亿个条目。瑞士警方曾在 2019 年 4 月份在瑞士逮捕五名涉嫌从 InfinityBlack 账户中套现积分的个人。
链接地址	https://www.securityweek.com/european-authorities-dismantle-infinityblack-hacker-group

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.b4aspy.n[prv,exp,spy] 2020-05-04	高	该应用程序运行后隐藏图标，获取手机固件信息、短信记录、通话记录、通讯录等隐私信息并上传，能上传或删除指定文件，接收远程指令并根据指令执行相关行为，造成用户隐私泄露和资费损耗，建议卸载。
		Trojan/Android.Tekya.a[exp,rog,fra] 2020-05-05	低	该应用程序存在风险代码，会模拟用户点击来自 Google、AdMob、Facebook 等机构的广告进行移动广告欺诈，会导致用户资费消耗，建议立即卸载。
		G-Ware/Android.Downloader.gw[exp,rog] 2020-05-06	低	该应用程序包含恶意代码，运行后台会下载未知子包，为避免造成用户资费消耗，建议卸载。
	较为活跃样本	G-Ware/Android.merchant.c[prv,fra	中	该应用程序伪装为 QQ 相关应用，运行监听记录用户银行类短信、支付类 app 的通知栏消息中的交易收支信息，上传到指定网址，且使用明文上传用户账号密码，可能造成用户隐私泄露，若非本人自主安装，建议不要使用。
		Trojan/Android.SmsSpy.cy[prv,exp]	中	该应用程序运行后隐藏图标，监听窃取用户短信，并上传短信内容到指定网址，造成用户隐私泄露，建议立即卸载。
		Trojan/Android.Dropper.ec[prv]	中	该应用程序包含风险代码，运行隐藏图标，可能会拦截短信、发送短信，造成用户隐私泄露，建议卸载。
		Trojan/Android.dialer.g[exp]	低	该应用程序无实际功能，会在启动时拨打电话至指定号码，造成用户资费消耗，建议立即卸载。
		G-Ware/Android.HiddenAds.ld[exp,rog]	低	该应用程序包含风险代码，安装无图标，运行后台会推广加载广告，为避免造成用户资费消耗，建议卸载。
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Microsoft Windows Media Foundation 安全漏洞（CVE-2020-0948）	高	当 Microsoft Windows Media Foundation 不正确地处理内存中对象时，会触发内存损坏漏洞。成功利用此漏洞的攻击者可以安装程序；查看、更改或删除数据；或者创建拥有完全用户权限的新帐户。攻击者可能通过多种方式利用此漏洞，包括诱使用户打开经特殊设计的文档或诱使用户访问恶意网页。
	较为活跃样本家族	Trojan[Backdoor]/Win32.Mutopy	中	此威胁是一种木马类后门程序。该家族样本运行后会释放可执行文件，连接远程服务器，等待接收上传下载文件、监视用户屏幕、记录键盘击键、查看进程和窗口等控制指令。
		Trojan/Win32.Murlo	中	此威胁是一种木马类程序。该家族样本运行后添加映像劫持使下载软件迅雷无法使用；修改注册表隐藏具有隐藏属性的文件，隐藏具有系统属性的文件；连接网络下载家族地址列表，并依照列表下载家族文件并执行。
		Trojan[PSW]/MSIL.NetPass	中	此威胁是一种窃取用户的账户密码等信息的木马类程序。该家族侵入用户系统后，会搜索存储账户密码信息的文件，找到后会通过邮件、FTP 上传等方式将文件传送给黑客。
		Riskware/Win32.GetFaster	低	此威胁是一种可以下载推广应用的风险软件程序。该家族样本运行后连接网络下载推广应用并安装，占用系统资源，影响用户使用。
		GrayWare[AdWare]/Win32.Tirrip	低	此威胁是一种可以推送广告的灰色软件家族。该家族样本运行后下载并安装推广应用，在用户浏览网页时可以弹出广告、占用系统资源、影响用户使用。

撞库攻击：日益严重的安全威胁

库纳尔·阿南德 / 文 安天技术公益翻译组 / 译

想象一下这样的情况：前门安装了带有先进报警系统的昂贵门锁，而后门却大敞四开。没有人会这样做，不是吗？然而，许多公司在网络安全防御方面却犯了类似的错误。他们将其应用程序和网站的前端作为如同诺克斯堡般的安全防御重心，而却将后端关键的 API 暴露给全世界。

Gartner 公司预测，到 2022 年，API 滥用将成为导致数据泄露的最常见攻击向量。这家分析公司表示：“尽管人们对 API 安全的认识不断提高，但数据泄露事件依旧频频发生。”如果将过去几年中发生的数据泄露事件统计起来，则可以看出，超过 50% 的数据是通过应用程序和 API 泄露的。

过去，黑客获取在线账户凭证的首选方法是通过面向用户的登录页面实现账户接管，这种方法被称为撞库攻击。撞库攻击利用了一个常见弱点：许多用户倾向于重复使用同一密码。这使攻击者更容易利用从一个账户窃取的用户名和密码列表在多个服务上运行，从而产生破坏性的连锁反应。

在廉价且强大的自动化工具的帮助下，网络犯罪分子执行暴力破解攻击，尤其是使用那些僵尸程序一遍又一遍地用各种用户名和密码组合尝试登录网站，直到找到正确的组合实现成功入侵。

典型的撞库攻击如同一出好戏分为三幕：

1. 攻击者从网站窃取凭证，或在某些情况下从暗网获取从网站泄露的凭证。从一次单独的数据泄露事件中获取数百万条记录并不稀奇。

2. 攻击者使用账户检查程序来测试针对多个网站的大量被盗凭证，并通过僵尸网络在成千上万个设备之间执行攻击，绕过简单的检测和缓解机制。整个网络犯罪社区都在推荐这种战术，并出售专门针对特定目标的自动化客户端配置文件。

3. 成功登录后，攻击者可以接管账户并窃取个人信息，如信用卡号码或积分。攻击者还可能将该账户用于其他恶意目的，如从电子邮件账户发送垃圾邮件。

在过去几年中，撞库攻击的受害者包括西班牙巴塞罗那足球俱乐部，其 Twitter 账户被黑客入侵，然后发送虚假推文；还有邓肯甜甜圈（Dunkin'Donuts），该公司向其 DD Perks 计划的客户发出警告，称某些账户的用户名和密码可以被未经授权地访问。

随着越来越多的公司能够更好的保护其前端应用程序和网页以防止撞库攻击，恶意行为体逐渐在后端 API 和微服务中寻找机会，因为这些方面往往缺乏防护。我们已经看到，超过一半的数据是通过应用程序和 API 泄露的，并且这一比例还将继续增加。

对攻击者来说，他们更乐于选择通过 API 入侵，因为可以避免很多麻烦：许多公司根本没有意识到他们通过 API 传输了大量的数据，并且对这些数据的保护不到位。

此外，僵尸程序产生了大量的互联网流量。我们公司每月处理的 25 PB 数据中有 40% 来自僵尸程序，而其中一半是出于恶意目的，例如撞库攻击。借助公共云和更复杂的工具，创建和启动功能更强大的僵尸程序对于黑客来说也更加容易，成本更低。

当 API 成为数字世界软件应用程序的关键部分时，对它们的攻击将成为重大威胁。开放式银行就是一个例子，它旨在通过使用 API 让第三方金融服务提供商以电子方式访问来自银行和其他金融机构的数据，从而让消费者的生活更加便利，并与外部合作伙伴在此基础上开发新的应用程序和服务。

那么，我们能做些什么呢？

首先，公司只需要像保护其基础设施的其他部分一样，高度重视后端 API 和服务的安全。API 本质上其实就是应用程序，无论 SQL 注入攻击是通过前端还是后端执行，都应该采取防御措施。

其次，像苹果和谷歌这样拥有主导移动平台的大公司，可以直接在他们各自的平台上进行密码管理和双因子认证（2FA）。这类公司拥有可以帮助消费者的无限资源，并且他们也应该这样做。其结果就是，普通人也可以拥有更强大的密码和身份管理。

为防范老套的前端撞库攻击，用户必须牢记，在不同的应用程序和网站上使用不同的密码。在缺乏平台本地密码管理选项的情况下，建议个人使用密码管理器和 2FA 解决方案。对于更重要的应用程序和服务，建议使用硬件密钥。

长期以来，撞库攻击一直是最常见的网络攻击类型之一，但这种威胁正在不断演变。企业需要认真对待威胁，并采取有效措施。

原文名称	The Evolving Threat of Credential Stuffing
作者简介	库纳尔 · 阿南德（Kunal Anand）。库纳尔 · 阿南德是 Imperva 安全公司的首席技术官。
原文信息	2020 年 4 月 23 日发布于 Dark Reading 原文地址 https://www.darkreading.com/attacks-breaches/the-evolving-threat-of-credential-stuffing/a/d-id/1337567
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。