安天发布《Trik 僵尸网络变种分析报告》

近日，安天 CERT 在梳理网络安全事件时发现一个名为 Trik 的僵尸网络变种。目前，在全球有近 50 万台受感染的计算机。该僵尸网络家族活跃了近 10 年，早期传播方式包括可移动存储介质和即时通讯软件，近期发现该僵尸网络变种传播方式为垃圾邮件。Trik 主要目的是以传播勒索软件和挖矿木马获利。

Trik 运行后，在受感染计算机%AppData%目录中创建 winsvcs.txt 文件，创建注册表保证开机自启动。该僵尸网络变种包含一个微型组件，该组件利用 SMB 协议和硬编码的用户名和口令列表，尝试连接到开启 139 端口的远程计算机并将 Trik 复制到其中。Trik 使用远程计算机上的 Windows 服务控制管理器启动 SMB 组件进程，检查是否存在 winsvcs.txt 文件，从而确定是否连接 C2 服务器下载并执行所传播的恶意程序。

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僵尸网络的鉴定；安天智甲已经实现了对该僵尸网络的查杀。

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、动态行为鉴定器将文件判定为木马程序。

◆概要信息

文件名	0c77b260.exe
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	272 KB
MD5	A24BB61DF75034769FFDDA61C7A25926
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Vimditator
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
删除自身	★★★★
添加防火墙规则	★★★
检测虚拟机	★★★★★
获取剪切板内容	★★★
访问下载站点	★★★

◆常见行为

行为描述	危险等级
加载运行时 DLL	★
设置调试器权限	★
自我复制	★★
Run 自启动	★
获取计算机名	★
疑似桌面控制	★

◆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 2019年11月11日(总第207期)试行 本期4版 微信搜索：antiylab 内部资料 免费交流

安天上榜全国首批“5G 创新企业”名单

近日，由工业和信息化部指导，中国通信企业协会主办，中国电信、中国移动、中国联通、中国铁塔、中国广电协办，人民邮电报社承办的“2019 中国信息通信业发展高层论坛”在京举行。会上，为表彰企业在 5G 方面的创新成果，推介了 53 家“5G 创新企业”（其中包含 7 家网络安全企业），安天集团凭借在移动安全侧的技术积累和综合布局上榜。

本次推介工作旨在深入贯彻落实中央经济工作会议精神和信息化部重点工作部署，引导信息通信企业做大做强，促进 5G 应用创新，加快 5G 商用步伐，推动信息通信行业高质量发展，为新中国成立 70 周年献礼。

安天较早开始进行移动安全领域的安全探索，在智能终端方面，安天于 2004 年和 2008 年分别研发了 WinCE 和 Symbian 平台下的安全扫描工具。并从 2010 年开始全面加速移动安全布局，成立了安天移动安全研发中心（武汉），全力研发安天 AVL SDK 反病毒引擎移动威胁检测版本。该引擎获得了 2013 年度 AV-TEST 移动设备最佳保护奖，并后续支撑使用安天引擎的友商获得国际奖项。在 2019 年公布的 AV-TEST 测试中，安天 AVL Inside 移动反病毒引擎第六次斩获 AV-Test 年度常规测试和实时测试检出率双 100% 的成绩。目前，包括华为在内的前 10 名国产手机厂商，累计超过 17 亿部手机出厂即内嵌安天威胁检测引擎，全球具有有效杀毒能力的移动反病毒软件中 20% 以上使用安天引擎，每日有超过 3.5 亿用户通过安天引擎进行安全检测。

安天安全引擎已经不只是早期单纯的安全检测模块，而是包含了系统安全监测、Wi-Fi 安全、接入安全、扫码安全、支付安全、APP 访问控制等的综合安全内生中间件，安天积极推动和华为、高通等厂商合作，推进安全中间件能力与 Trustzone 等系统芯片级安全能力的对接。

在局端监测方面，安天于 2011 年在监测分析产品 VDS（即安天“探海”威胁监测系统的前身）扩展了 M 系列型号，通过 Gn 口实现在移动运营商侧部署，解析移动通信 GTP 信令、PDSN 信令，实现对 SGSN、GGSN 的安全监测，并对 WAP、彩信等业务内容的安全性实现了针对性的解析，可全面检测 Android、Symbian 等平台的安全威胁；始终坚持关口监测设备大流量细粒度分析能力的优势，在 2014 年实现了单设备 4Gbps 的 IP 流量分析能力、单设备每秒 1 万 PDP 信令处理能力；通过“探云”等计划的部署及与运营商、合作伙伴的协作，形成了流量侧恶意代码与攻击活动的监测捕获能力。

在分析支撑方面，安天持续监测分析端点安全情况，对应用商店和其他 APP 源进行跟进分析监测。安天移动安全公司研发了安天第二代自动化分析流水线，支持全量样本和 APP 的深度静态分析和动态分析，形成可以精准判定、家族关联、同源分析、情报生产的综合分析机制，成为了安天“赛博超脑平台”的重要支撑系统。为安天威胁情报平台和情报输出服务提供了全面支持。相关平台不仅由安天自用，还在主管部门、测评机构和运营商实现了工程部署实施，有利支撑了行业安全监管能力。

安天在移动产业链中，已经构建起可对接芯片级、终端级、系统级、应用级等不同层级的合作伙伴支撑网络侧、协同侧、监管侧、政企场景侧的安全需求。当前，5G 建设方兴未艾，带来了重大发展机遇，也潜藏着重大的威胁隐患。安天移动安全研发中心已经发展成为安天移动安全公司，全面布局和发力 5G 时代的移动安全。安天会继续展开 5G 场景下智能终端安全技术的研发，全面提升引擎和安全中间件能力。发挥引擎内置、基础赋能的优势，进一步落实安全“关口前移，防患于未然”的工作要求。进一步强化场景识别模型，对可能爆发的威胁进行有效监控，基于本地静态检测和沙箱技术，制定本地训练框架，加强有场景针对性的恶意代码分类检出策略；针对 5G 终端接入可能带来的政企网络、云基础设施带来的安全挑战，深入分析如何保障低延时、高带宽、多连接的业务访问需求，逐步做好为 5G 时代提供全方位的威胁防御能力的准备。

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	安全团队发现由 VegaLocker 演变的新勒索软件 Buran
英文标题	Buran Ransomware; the Evolution of VegaLocker
作者及单位	Alexandre Mundo and Marc Rivero Lopez
内容概述	迈克菲高级威胁研究小组观察到在 2019 年 5 月出现的新勒索软件家族 Buran。Buran 由 VegaLocker 演变形成，作为 RaaS（勒索软件即服务）模式在俄罗斯暗网进行售卖。Buran 通过 Rig 漏洞利用包投送，Rig 漏洞利用包使用 CVE-2018-8174（Microsoft IE VBScript 引擎任意代码执行漏洞）对客户端进行攻击，成功后，将安装 Buran。Buran 使用 Delphi 编写，如果确定系统位于俄罗斯联邦、白俄罗斯或乌克兰，将以“ ExitProcess”结束任务。目前研究人员已检测到了两个不同的 Buran 版本，第二版本中新增了几项功能，包括使用 WMI 删除卷影副本、删除备份目录、删除系统中的系统状态备份、使用 ping 命令通过“ for 循环”来确保文件删除系统等。
链接地址	https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/buran-ransomware-the-evolution-of-vegalocker/

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.Banbra.c[prv,exp] 2019-11-03	高	该应用程序运行私自下载恶意子包动态加载，下载安装银行木马，窃取用户隐私，会造成用户资费损耗和隐私泄露，请卸载。
		RiskWare/Android.Fakemayi.b[fra,exp] 2019-11-04	中	该应用程序伪装成蚂蚁金融产品，运行后推广其他借贷产品，存在风险隐患，建议卸载。
		RiskWare/Android.carefulsupport.a[prv,exp] 2019-11-05	中	该应用程序为一款音频文本服务软件，运行后会获取用户联系人、地理位置、通话记录、手机号信息用于注册，若非本人安装，请卸载。
	较为活跃样本	G-Ware/Android.Hidebocai.a[exp,rog]	中	该应用程序为虚假应用，运行联网获取配置信息，加载博彩内容，下载博彩应用，会造成用户流量资费损耗，并且给用户财产带来安全风险，建议卸载。
		Trojan/Android.lojaok.b[prv]	中	该应用程序伪装正常应用，无实际功能，运行上传固件信息、屏幕参数信息，可能配合其他应用窃取银行相关隐私，造成用户隐私泄露，请卸载。
		Trojan/Android.Zumba.a[prv,fra,spy]	中	该应用程序伪装系统升级程序，运行隐藏图标，窃取用户固件信息、位置信息、电话录音、通知栏消息、通话记录、短信、whatsapp 消息等隐私数据并上传，会造成用户隐私泄露，建议立即卸载。
		Trojan/Android.QQspy.es[prv]	中	该应用程序伪装 QQ 安全中心，诱导用户输入 QQ 账号密码并上传到远程服务器，会造成用户隐私泄露，请卸载。
		G-Ware/Android.Ashas.a[exp,rog]	中	该应用程序包含风险代码，运行后联网上传用户手机基本信息，隐藏其图标并创建快捷方式，私自加载并推送流氓广告。造成用户流量消耗，建议不要使用。
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Windows 远程桌面客户端远程代码执行漏洞（CVE-2019-1333）	高	当用户连接到恶意服务器时，Windows 远程桌面客户端会触发远程代码执行漏洞。若要利用此漏洞，攻击者需要控制服务器，然后利用社会工程学、病毒、中间人攻击等手段诱导用户连接到该服务器。成功利用此漏洞的攻击者可以在目标系统上执行任意代码。攻击者可随后安装程序、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。
	较为活跃样本	Trojan[Dropper]/Win32.Metel	中	此威胁是一种具有捆绑行为的木马类程序。该家族会在后台记录收集用户信息并回传。该家族会从互联网上下载恶意代码并执行，控制感染者计算机。
		Trojan/Win32.Gobot	中	此威胁是一种后门类的恶意木马类程序。该家族入侵用户计算机后，会在计算机中创建后门程序，允许黑客远程登陆计算机，并窃取用户隐私信息。
		Trojan/Win32.Cospet	中	此威胁是一种木马程序，该家族在未经用户同意的情况下，获取系统信息，尝试连接网络，下载恶意代码到用户系统中运行。
		GrayWare[AdWare]/Win32.NaviPromo	低	此威胁是一种有广告行为的灰色软件家族。该家族会在电脑上产生弹窗，并在 IE、Chrome、Firefox 等浏览器上安装扩展程序，推送广告。
		GrayWare[AdWare]/MSIL.BrowseFox	低	此威胁是一种有广告行为的灰色软件家族。该家族会在电脑上产生弹窗，推送广告，收集用户信息。

撞库攻击：如何预防、检测和防御

Lucian Constantin / 文 安天技术公益翻译组 / 译

对网络犯罪分子来说，自动利用窃取的用户名和口令访问用户账户的“撞库攻击”（credential stuffing）具有低风险和高回报。本文将介绍一些增大此类攻击难度的方法。

撞库攻击是什么？

撞库攻击是指自动利用收集的用户名和口令访问用户账户。在过去的几年中，由于各种数据泄露事件，数十亿的登录凭证已落入攻击者手中。这些凭证助长了地下经济，被用于从垃圾邮件到网络钓鱼和账户劫持的各类攻击。撞库攻击是网络犯罪分子滥用被盗用户名和口令的最常见方法之一。

这是一种暴力攻击技术，但是攻击者并非使用常见单词组合“字典”来猜测口令，而是使用从数据泄露事件中窃取的已知有效凭证列表。由于大量用户在不同的网站上重复使用口令（从低价值网站窃取的凭证，很可能也是包含更敏感数据的网站的凭证），因此这种攻击更容易执行且成功率更高。

撞库攻击有多严重？

安全研究员特洛伊·亨特（Troy Hunt）运营了一款免费数据泄露通知服务 HaveIBeenPwned.com（HIBP），该服务跟踪了 410 多起数据泄露事件中泄露的超过 85 亿个凭证。该服务仅追踪公开数据集或在地下论坛上广泛传播的数据集中的凭证。而许多数据库转储是私有的，只有一小部分攻击者能够访问。

出售被盗取凭证和专用工具的地下经济促进了自动撞库攻击的发展。这些工具使用所谓的“组合清单”，即，破解泄露数据库中的哈希口令，然后将不同的口令相互组合。这意味着发动此类攻击不需要任何特殊技能或知识，只要花几百美元购买工具和数据，任何攻击者都可以执行此类攻击。

从 2017 年 11 月到 2019 年 3 月底的 17 个月中，安全和内容交付公司 Akamai 检测到针对数十个垂直行业的 550 亿次撞库攻击。尽管某些行业更常遭受攻击——例如游戏、零售和媒体流行业，但没有哪个行业能幸免于难。

该公司在 6 月份发布的一份报告中指出：“目前，攻击者将凭证滥用视为一种低风险、高回报的活动。在可预见的将来，这类攻击很可能会增加。”

如何检测和缓解撞库攻击

撞库攻击是通过僵尸网络和自动工具发起的，这些僵尸网络和工具使用代理将恶意请求传播到不同的 IP 地址。此外，攻击者经常对其工具进行配置，以模仿合法的用户代理——例如，识别浏览器和操作系统 web 请求的标头就是这样来的。

这使得防御者很难区分攻击和合法登录尝试，尤其是在流量高的网站上，突然出现大量登录请求的情况并不罕见。也就是说，短时间内登录失败率的增加，可能是正在发生撞库攻击的迹象。

某些商业 web 应用程序防火墙和服务使用更高级的行为技术，来检测可疑的登录尝试。网站所有者也可以采取措施来防止此类攻击。

一种有效的缓解措施是：实施多因子身份鉴别（MFA）。即使某些自动网络钓鱼和账户劫持工具可以绕过 MFA，但这些攻击需要更多的资源，并且更难大规模执行。

鉴于 MFA 的成本较低，因此许多企业将其作为“用户可自行选择是否开启”的选项。如果认为强制对所有用户账户启用 MFA 对干扰业务，则可以采取一种折衷办法：即为确定为“高风险”的用户自动启用 MFA。例如，用户账户多次登录失败后，自动启用 MFA。

大型公司也开始采取主动措施，如监控公共数据转储，并检查其系统中是否存在受影响的电子邮件地址。对于在其系统中找到的已被攻击账户，公司会强制用户重置口令，并强烈建议用户启用 MFA。

员工使用其工作邮箱设置的账户是否受到外部泄露事件的影响？公司要想监控这一点，可以使用 HIBP 之类的服务来为其所有域名设置告警。 HIBP 的公共 API 已用于开发各种编程语言的脚本，这些脚本可以集成到网站或移动应用程序中。

最后，在针对员工的安全意识培训中，公司应关注口令安全问题。口令重用是攻击者执行撞库攻击的关键，因此强烈建议用户无论在工作场所还是在家中，都不要重复使用口令。

用户可以使用口令管理器为每个在线账户生成唯一且复杂的口令，且无需记忆这些口令。 如果在公共数据转储中检测到用户的电子邮件地址，一些应用甚至会自动通知用户。

Akamai 在其《互联网状况》报告中总结道：“撞库攻击无处不在。鉴于这类攻击无法完全阻止，因此我们应该增大攻击者获取凭证的难度。弱口令和口令重用是账户安全的祸根——无论游戏、零售、媒体和娱乐行业，还是任何其他行业，都是如此。如果用户使用弱口令或在多个账户中重复使用口令，则最终将遭到攻击。与推广口令管理器和多因子身份鉴别一样，口令安全意识也需要提高。”

原文名称	Credential stuffing explained: How to prevent, detect and defend against it
作者简介	Lucian Constantin。Lucian Constantin 为 CSO Online 撰写信息安全、隐私和数据保护方面的文章。
原文信息	2019 年 10 月 30 日发布于 CSO Online 原文地址 https://www.csoonline.com/article/3448558/credential-stuffing-explained-how-to-prevent-detect-and-defend-against-it.html
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。