安天智甲有效防护 Buran 勒索软件

近日，安天 CERT 在梳理网络安全事件时发现一个名为 Buran 的勒索软件。该勒索软件首次出现于 2019 年 5 月，是一款基于 RaaS 模式传播的新型勒索软件。安天 CERT 研究人员分析判定 Buran 是 Jumper 勒索软件的变种。Buran 在一个著名的俄罗斯论坛中公开售卖，由于获利丰厚，使其迅速在全球传播开来，感染范围甚广。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 Buran 勒索软件的加密行为。

Buran 勒索软件此前使用 RIG Exploit Kit 漏洞利用工具包进行传播，近期发现该勒索软件利用 IQY(Microsoft Excel Web 查询文件) 进行传播。Buran 运行后搜索可加密磁盘，为每个可加密磁盘启动一个勒索软件进程，采用“AES+RSA”加密算法加密文件并在桌面释放勒索信。被加密文件重命名为受害者主机 ID。Buran 勒索软件调用命令行命令防止受害者恢复已加密的文件，具体操作为删除卷影副本、禁用修复、删除本地计算机的备份目录、清空注册表 RDP 连接记录、清空系统日志、禁用事件记录等。目前被加密的文件在未得到密钥前暂时无法解密。

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，避免一切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病毒的鉴定；安天智甲已经实现了对该勒索病毒的查杀。

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、信标检测鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	d5c9.exe
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	412 KB
MD5	99837E301D8AF9560A4E6DF01A81DC39
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Suloc
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
访问下载站点	★★★
检测虚拟机	★★★★★
删除自身	★★★★
在启动时禁用 Windows 错误恢复	★★★★
删除所有系统状态备份	★★★★
删除全盘所有卷影副本	★★★★
修改文件权限	★★★
禁用指定服务	★★★

◆常见行为

行为描述	危险等级
加载运行时 DLL	★
壳行为填充导入表	★★
获取系统版本	★
获取驱动器类型	★
读取自身	★
自我复制	★★
设置文件属性为隐藏	★★
.....	.....

◆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 6 月 1 日 (总第 232 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

纪念习近平总书记视察安天四周年集团开展主题学习活动

2016 年 5 月 25 日，习近平总书记在黑龙江考察调研期间视察了位于哈尔滨的安天总部，在听取汇报后对安天人说：“你们也是国家队，虽然你们是民营企业。”总书记的话，是对安天长期坚持自主核心技术研发和担当企业使命的认可，更为安天指明了企业定位，提出了成长要求。时隔四年，回想起总书记视察安天时的情景，所有安天人仍然难以平静，深感责任所在。“5.25”四周年来临之际，集团党委和总办再次组织所有员工进行主题学习活动，观看相关视频资料，深入学习贯彻习近平总书记对网络安全工作的系列重要讲话精神和工作要求。

（由于疫情原因，本次学习活动没有组织员工们集中进行，而是让各属地、分公司、办事处的员工自行组织小范围学习观看。）

随着网络强国战略的不断推进实施，我国当前社会的信息化、自动化、智能化程度不断提升，5G、大数据中心、人工智能、工业互联网等新型基础设施建设快速发展，网络安全所面临的风险挑战愈发严峻，对能力型网络安全企业的使命要求也在不断提高。

安天以“国家队”的坚毅信念牢记总书记的嘱托，落实总书记的要求，努力践行对国家的使命、勇于承担对网络安全领域的责任，投身于保障国家网络安全的事业中，贡献自己的一份力量。

不忘初心，牢记使命，我们在路上。

微信扫描二维码阅读原文

StrandHogg 2.0 漏洞可能影响 v10 以外所有版本安卓设备

Promon研究人员在安卓操作系统中发现一个新严重漏洞，由于该漏洞与先前披露的StrandHogg漏洞相似，因此将该漏洞命名为StrandHogg 2.0。该漏洞被追踪为CVE-2020-0096，为特权提升漏洞，一旦在v9.0及之前版本的设备上安装了恶意应用程序，攻击者就可以访问私人短信和照片，窃取受害者的登录凭据，跟踪GPS移动，制作或记录电话对话，并通过手机的摄像头和麦克风进行监视。根据谷歌数据，截至2020年4月，全球91.8%的安卓有效用户受影响，而安卓v10不受影响。目前，谷歌已推出了一个补丁，其中针对v8.0、v8.1和v9的补丁将于2020年5月向公众发布。

（原文链接：https://promon.co/strandhogg-2-0）

Konni 组织新活动冒充研究核问题的研究机构

ESTsecurity研究人员发现Konni组织新鱼叉式网络钓鱼活动冒充最近研究核问题的国际安全与合作中心（CISAC）。CISAC是斯坦福大学的一个研究中心，研究一系列国际和国内安全与合作问题，最近针对核问题进行了各种研究。 诱饵Word文档名为“CISAC关于网络和核问题的讨论_2020年5月13日_v4_ENG”。该文档初始打开时，内容使用灰色字体以提供不清楚的显示，诱使用户启用恶意宏查看文档。启用恶意宏后，文档内置的编码恶意可执行文件将通过cmd执行并下载恶意文件。同时，内容由灰色字体变为黑色字体，以使文档内容更加可见。恶意文件zx.exe将编码的C2作为参数运行，并且根据受感染的系统下载并执行其它文件。下载的文件为Cab格式，使用cmd内置程序expand解压，分别执行其包含的文件，最终有效载荷dll文件将从受感染的系统中收集信息并将其发送给攻击者，并且可以下载并执行其它恶意文件。

（原文链接：https://blog.alyac.co.kr/3014）

每周安全事件

类 型	内 容
中文标题	安全厂商披露 Turla 组织新版本的 ComRAT 后门
英文标题	Turla has updated its ComRAT backdoor and now uses the Gmail web interface for Command and Control
作者及单位	Matthieu Faou
内容概述	ESET 研究人员发现 Turla 组织新版本的 ComRAT 后门。ComRAT（也称为 Agent.BTZ），是 Turla 组织的最早使用的恶意软件家族之一，曾在 2008 年攻击美国军方。2007 年到 2012 年，该恶意软件发布了两个新版本。直到 2017 年中，攻击者对 ComRAT 进行了一些更改。最新版本 ComRAT v4 于 2017 年出现，直到 2020 年 1 月仍在使用。研究人员至少确定了其针对两个外交部和一个国民议会。ComRAT v4 是用 C ++ 开发的复杂后门程序，使用一个在 FAT16 中格式化的虚拟 FAT16 文件系统。ComRAT v4 使用现有的访问方法部署，例如 PowerStallion PowerShell 后门，使用 HTTP 和 Gmail Web 界面进行命令和控制。ComRAT v4 可以在受到感染的计算机上执行许多操作，例如执行其它程序或窃取数据。攻击者使用 OneDrive 和 4shared 等公共云服务来接受数据。
链接地址	https://www.welivesecurity.com/2020/05/26/agentbtz-comratv4-ten-year-journey/

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

名称与发现时间		威胁等级	简要描述
活跃漏洞	Microsoft Word 安全漏洞（CVE-2020-0980）	高	当 Microsoft Word 软件无法正确处理内存中的对象时，会触发远程代码执行漏洞。成功利用此漏洞的攻击者可以使用经特殊设计的文件在当前用户的上下文中执行操作。例如，文件可以代表登录用户使用与当前用户相同的权限执行操作。
	Microsoft Windows Graphics Components 安全漏洞（CVE-2020-0907）	高	Microsoft 图形组件在内存中处理对象的方式存在远程代码执行漏洞。成功利用该漏洞的攻击者可以对目标系统执行任意代码。若要利用该漏洞，攻击者需要诱使用户打开一个经特殊设计的文件。
	Microsoft Windows Hyper-V 安全漏洞（CVE-2020-0910）	高	当主机服务器上的 Windows Hyper-V 无法正确验证来宾操作系统上经身份验证的用户输入时，会触发远程代码执行漏洞。成功利用此漏洞的攻击者可以在主机操作系统上执行任意代码。
较为活跃样本家族	Trojan[Backdoor]/Win32.Delf	中	此威胁是一种后门类木马家族。该家族是通过开发语言 Delphi 来命名的。该家族样本运行后，会在被感染的电脑中打开后门，黑客利用后门窃取用户的隐私信息。
	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.Padodor	中	此威胁是一种后门类木马家族。该家族样本会利用系统漏洞打开后门，为用户电脑带来更多威胁；它同时允许黑客远程进入并控制用户电脑。
	Trojan[Backdoor]/Linux.Gafgyt	中	此威胁是一种 Linux 平台上的具有窃密行为的后门家族。该家族样本运行后会在 Linux 上开启一个后门并允许远程控制端执行任意操作，并且会收集机器上的信息上传给远程控制端。
	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.Fakeapp	中	此威胁是一种伪装类木马家族。该家族样本通常伪装为主要应用程序（Fackbook 等），诱导用户输入账号密码，通过 firebase 联网上传或发送短信等方式窃取用户的账号密码，造成用户隐私泄露和资费消耗。
	Trojan[SMS]/Android.FakeInst	低	此威胁是一种伪装类木马家族。该家族样本通常伪装为主流应用程序（Opera、Skype 等），运行后向相关付费号码发送短信，造成用户资费消耗。

对抗撞库攻击五个建议

乔恩·古德尔德 / 文 安天技术公益翻译组 / 译

鉴于黑客很容易通过网络获取被盗凭证，我们应采取哪些措施来防止他们入侵安全账户呢？

苏米特·阿加瓦尔（Sumit Agarwal）因创造了“撞库攻击”（credential stuffing）一词而备受赞誉。奥巴马总统任职期间，他曾担任国防部副部长助理。2011 年，在五角大楼工作时，他开始注意到针对公开军事网站的暴力攻击。在这些攻击中，攻击者使用从一个网站窃取的凭证，如用户名和口令，来访问其他网站。

如今，阿加瓦尔是 Shape Security 公司的联合创始人兼首席技术官；而撞库攻击已经非常普遍，使各种企业的安全管理人员疲惫不堪。

“撞库攻击是当今的一个大问题，尤其是在新冠肺炎期间，很多企业完全转向了在线服务。”阿加瓦尔说，“疫情期间，撞库攻击更受攻击者青睐，Disney+ 遭受大量针对性撞库攻击就是一个很好的例子。每当服务获得大量流量时，撞库攻击就会激增。我们将会看到，针对在线商店、快递服务和远程医疗提供商的撞库攻击不断增加。”

简而言之，当网络犯罪分子通过某种方式（通常是暗网）获取被盗凭证，然后利用僵尸网络或其他自动化工具，尝试使用这些被盗用户名和口令来访问多个其他用户账户时，就会发生撞库攻击。

“撞库是一种网络攻击，黑客试图利用数据泄露事件中被泄露的用户名和口令，登录用户的账户。”Auth0 平台安全工程总监夏洛特·汤斯利（Charlotte Townsley）说，“黑客通过攻击窃取用户的凭证，然后在暗网上出售这些凭证，供其他黑客购买。其他黑客可以买到数十亿个泄露凭证，然后使用僵尸程序快速尝试不同的用户名和口令组合，登录从社交平台到银行应用的各种用户账户。”

“撞库攻击实际上是暴力攻击的一种。”Vigilante 情报总监亚当·达拉（Adam Darrah）补充说，“主要区别在于，攻击者利用的是以前破解的口令，以及被其他攻击向量（例如键盘记录程序和其他恶意软件）窃取的口令，因此他们在攻击前就已经拥有了一批凭证。攻击者利用一系列复杂程度各异的暴力攻击检查程序，针对公司基础设施和网站进行针对性的账户劫持攻击。”

当然，一旦攻击者登录了公司账户，就意味着公司的敏感信息可能会泄漏，或者攻击者可能会获得对其他私人账户的访问权限，或者诱导毫无戒心的同事共享信息。攻击造成的损害可能是无限的。

攻击越来越多且易于执行

从阿加瓦尔早期发现针对政府网站的撞库攻击开始，此类攻击已经无处不在。2019 年最新的 Verizon《数据泄露调查报告》（DBIR）披露，在所有数据泄露事件中，有 29％使用了撞库攻击方法。目前，提供数据泄露通知的免费网站 HaveIBeenPwned.com（HIBP）已经披露了数百起数据泄漏事件中泄露的近 90 亿个凭证的信息。

鉴于犯罪分子很容易以低廉的价格获取被盗凭证，撞库攻击越来越受其青睐，这毫不奇怪。

“利用一下午进行谷歌搜索，就能够了解如何购买受害者银行账户或在线零售账户的凭证。”达拉说，“有无数的深网和暗网市场在售卖账户凭证。根据服务或网站的不同，账户凭证的价格甚至会低至 2 美元。在某些情况下，如果凭证不像广告中所宣传的那样有用，甚至可以退款。”

尽管如此，安全管理人员还是可以使用一些工具和技术来减轻撞库攻击。我们与之交谈的安全研究人员建议采取以下措施。

1. 增强用户对口令管理的认识

汤斯利说，由于许多用户仍在各个账户之间重复使用口令，因此首先要对用户进行培训。“改善用户口令习惯是对抗撞库攻击的一个良好开端。对员工进行最佳实践培训，并提醒他们定期更改口令，会使黑客更难执行攻击。”

2. 实施多因子身份鉴别

如果可以，应对每个账户启用双因子 / 多因子身份鉴别。这会增加另一层安全性，使攻击者更难渗透账户。

3. 使用异常检测工具

“企业可以使用免费的，或者企业级的在线威胁情报工具，帮助识别风险信号，例如口令泄露或身份鉴别失败的次数异常。”汤斯利说，“利用这些工具，企业还可以发现访问网站的 IP 地址数量突然或异常增加——这可以作为发生恶意活动的信标。”

4. 部署口令管理器

有几个免费的企业口令管理器可供使用，它们可以帮助用户为每个安全账户创建唯一且强效的口令，减少口令重用问题。Ovum 公司（现已成为 Omdia 的一部分）的最新市场研究披露，有很多口令管理器适用于大型企业和小型公司。其中，1Password Business、Dashlane Business、Keeper for Business、LastPass Enterprise、ManageEngine Password Manager Pro、Pleasant Password Server 和 RoboForm for Business 是佼佼者。此外，Ovum 还对 Bluink、Passwork、Bitwarden、TeamPassword 和 Passbolt 的独特功能表示了赞赏。

5. 在网站设计时考虑到安全性

“安全专家和 Web 开发人员可以在网站中使用任何可用的暴力攻击对策（包括验证码 [CAPTCHA] 和双因子身份鉴别 [MFA]），以增加攻击难度。”达拉说，“还可以对网站功能进行简单的更改，例如，发现登录尝试后给出提示。”

原文名称	5 Tips for Fighting Credential Stuffing Attacks
作者简介	乔恩·古德尔德（Joan Goodchild）。乔恩·古德尔德是一位屡获殊荣的资深作家和编辑。
原文信息	2020 年 5 月 22 日发布于 Darking Reading 原文地址 https://www.darkreading.com/edge/theedge/5-tips-for-fighting-credential-stuffing-attacks/b/d-id/1337896
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。