安天智甲有效防护“6688123”勒索软件

近日，安天 CERT 在梳理网络安全事件时发现了一个勒索信为国语的勒索软件。该勒索软件释放相关标识内容为“6688123”字符串作为加密标识文件。安天将此勒索软件命名为“6688123”，该勒索软件最早出现于2020年9月，通过对该勒索软件分析，该勒索软件具有三种加密方式分为 RSA 加密方式、AES 加密方式以及 XOR 加密方式。在本次所分析的样本中采用的加密策略 XOR 加密方式，所以该方式加密的文件可以解密。该勒索软件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该勒索软件的加密行为。

该勒索软件使用 .NET 框架开发。该勒索软件运行后，判断 C:\Users\XXX\Documents\Driver 目录下是否存在 b.print 文件且文件内容为“6688123”，若存在则表示用户文件已加密过，无需再次加密，则退出程序。该勒索软件会对常见后缀名如 txt、doc、bat 等文件进行加密，在本次分析的样本中所采用的加密策略是 XOR 加密方式。具体加密方式为采用指定长度的字符 XOR 指定文件前 100byte 字符，并追加文件名后缀 ".locky"。加密完成后会在桌面弹出窗口，要求用户向指定比特币地址支付 0.05 个比特币。

▲“6688123”勒索软件勒索信

“6688123”勒索软件采用 XOR 形式加密文件，目前被加密的文件可以解密。

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

最终依据 BD 静态分析鉴定器、反病毒引擎鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	6bb.exe
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	128 KB
MD5	B0E68A3352D31A9DD403A5ACAE6387A0
病毒类型	木马程序
恶意判定 / 病毒名称	VCS/Instruction.JunkCode
判定依据	反病毒引擎

报告地址：https://1.119.163.6/vue/details?hash=B0E68A3352D31A9DD403A5ACAE6387A0

◆运行环境

操作系统	内置软件
WinXP 5.1.2600 Service Pack 3 Build 2600	默认、IE6、Firefox、Google Chrome、Office2003、Flash、WPS、FoxitReader、AdobeReader

◆危险行为

行为描述	危险等级
搜索文件	★★★★
在系统目录创建文件	★★★
映射内存方式注入	★★★
通过标记进程可执行堆绕过 DEP	★★★★★
创建互斥量	★★★
释放 PE 文件到临时文件夹	★★★★
自启动	★★★
修改文件后缀名	★★★★
已知的勒索软件	★★★★

◆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06月07日(总第281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

构建纯净移动互联网生态，安天移动安全提供四大解决思路

数字经济时代，如何合法合规的使用数据，保障用户的隐私和权益已成为政府监管部门关注的重要问题。对过度采集、滥用信息、恶意推送、功能欺诈等行为的遏制和治理，不再是一个单纯的网络安全技术问题，而是涉及到国家安全、社会治理安全、政企机构安全和公民个人安全等多个层级的社会性问题，应基于“良赢治理”（查看文章）的思路，从社会安全的维度进行综合考量和治理。

构建纯净移动互联网生态，安天移动安天提供四大解决思路

以往，移动恶意代码的判定和治理思路是先技术判定，然后实施规则检测，其判定方式具有一定的滞后性，属于事后处置策略。安天移动安全从风险视角出发，基于 App 恶意性、风险性和开发者信誉，构建问题 App 和问题开发者的全方位关联能力，不仅实现了提前威胁预警和风险提示，还能有效识别、判定开发者利用正常的应用功能和业务模式包装的风险问题，从而真正做到关口前移。

当前移动互联网生态治理面临多重挑战

国内移动生态中，移动应用商店更多扮演的是展示作用，而非核心应用分发方式，大量的移动应用以推荐广告或各类流式内容广告的形式分发、安装到终端上，这无疑对移动生态治理提出了更高的要求，需要覆盖面更广，发现率更高的手段来捕获线下分发的违规应用程序。

另外，应用分发和下载仅仅是其使用环节的开始，有些移动应用还具备热更新、插件积木式功能组合和精准内容推送等模式形态，可以通过技术手段动态绕过现有审查机制，蒙混过关。应用商店上、下架等静态或局部管控手段难以有效覆盖应用的全生命周期，无法达到全面治理效果。

安天移动安全从用户安全的视角出发，梳理并构建了统一的应用风险判定标准，基于十余年“国家级”攻防实战经验和技术积累，海量安全大数据、知识库，总结出了包括内容风险、权限和隐私风险、支付风险等在内的十大应用风险类型，并形成了细粒度的移动互联网应用问题取证标准。

纯净移动互联网生态的建设，需要对互联网数据采集、经济业态以及附着其上的“黑灰产”进行全面深入的梳理分析，形成全局策略，指导性的法律法规、引导性的技术规范以及警示性的惩戒机制相辅相成、共同推进，应基于“良赢治理”的理念和思路，以网络安全技术为抓手进行综合治理。（原文链接：https://mp.weixin.qq.com/s/EZNxqIFjoJU18pMoHac7Bg）

扫描右侧二维码阅读全文

针对工控的勒索软件 Cring 样本分析

概述

近年来，针对工业控制系统的勒索软件增长迅速，其中以 Sodinokibi、Ryuk 和 Maze 为首的勒索软件家族最为猖獗。近日，安天 CERT 发现一起入侵工业控制系统并最终投放勒索软件的攻击事件，此次事件影响了欧洲一些国家的工业企业，其工业控制环境的服务器被加密，导致工控业务系统临时关闭。经过分析，该起攻击事件归属于一个新的勒索软件家族 Cring（也被称为 Crypt3r，Vjiszy1lo，Ghost，Phantom 等）。该勒索软件最早出现于 2020 年末，使用 AES256+RSA8192 算法加密受害者的数据，要求支付 2 个比特币作为赎金才能恢复数据。攻击者利用 CVE-2018-13379 漏洞进行攻击，一旦获取系统中的访问权限后，会下载 Mimikatz 和 Cobalt Strike 进行横向移动和远程控制，最终下载 Cring 勒索软件并执行。工业控制系统是国家基础设施的重要组成部分，也是工业基础设施的核心，被广泛用于炼油、化工、电力、电网、水厂、交通、水利等领域，其可用性和实时性要求高，系统生命周期长，一旦受到勒索软件的影响，不仅会导致大面积停产，也会产生更广泛的负面社会效应。

样本分析

该样本首先会使用名为“kill.bat”的批处理脚本执行一系列系统命令，其中包括暂停 BMR Boot 和 NetBackup BMR 服务，配置 SQLTELEMETRY 和 SQLWriter 等服务为禁用状态，结束 mspub.exe、mydesktopqos.exe 和 mydesktopservice.exe 进程，删除特定扩展名的备份文件，并且如果文件和文件夹的名称以“Backup”或“backup”开头，则还会删除位于驱动器根文件夹中的文件和文件夹，该脚本在执行后会删除自身。（原文链接：https://mp.weixin.qq.com/s/3UUbbZewFwoNHRNqwV3YOQ）

扫描右侧二维码阅读全文

每周安全事件

类 型	内 容
中文标题	攻击者传播 Android 恶意软件 Teabot 和 Flubot
英文标题	Threat Actors Use Mockups of Popular Apps to Spread Teabot and Flubot Malware on Android
作者	Bitdefender Labs
内容概述	TeaBot 和 Flubot 是最新的银行木马家族，多个安全研究人员在 2021 年初发现了它们。攻击者使用虚假的 Ad Blocker 应用程序充当恶意软件的投放器，虚假的 Ad Blocker 应用程序没有原始版本的任何功能。他们请求允许在其他应用程序上显示、显示通知并且可以在 Google Play 之外安装应用程序，然后隐藏图标。时不时地，虚假应用程序会显示关联之外的广告，最终会按照 CnC 的指示下载并试图安装 Teabot。与 Teabot 不同的是，Flubot 的操控者使用垃圾短信作为一种传递方式。FluBot 从受感染的设备窃取银行、联系、短信和其他类型的私人数据，并拥有一系列其他可用命令，包括发送含有 CnC 提供内容的短信的能力。
链接地址	https://labs.bitdefender.com/2021/06/threat-actors-use-mockups-of-popular-apps-to-spread-teabot-and-flubot-malware-on-android/

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	Nginx DNS Resolver 远程代码执行漏洞（CVE-2021-23017）	高	Nginx DNS Resolver 存在远程代码执行漏洞。由于 Nginx 的 DNS Resolver 组件在未压缩的域名处理上存在逻辑错误，使得攻击者可疑构造恶意数据执行远程代码攻击。
	Microsoft HTTP 协议栈的远程代码执行漏洞（CVE-2021-31166）	高	Microsoft HTTP 协议栈存在远程代码执行漏洞。由于 HTTP 协议栈中存在 use-after-free 错误，使得攻击者可以向受影响的系统发送特制的 HTTP 请求并执行任意代码。
	VMware vCenter Server 远程代码执行漏洞（CVE-2021-21985）	高	VMware vCenter Server 存在远程代码执行漏洞。由于对 Virtual SAN 运行状况检查插件（默认情况下已启用）中用户提供的输入的验证不足。远程未经身份验证的攻击者可以向端口 443/tcp 上可用的 vSphere Client 发送特制的 HTTP 请求，并在托管 vCenter Server 的底层操作系统上以不受限制的特权执行任意命令。
较为活跃样本家族	Trojan/Win32.Scar	中	此威胁是一种木马类程序，可以将某些金融网站重定向到攻击者设置的另一个地址，模仿登录界面从而窃取用户密码。
	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/Win32.Mansabo	中	此威胁是一种可以窃取密码信息的木马类家族。该家族的样本运行后会窃取用户账户信息，记录键盘击键信息，造成用户隐私泄露。
	Trojan/Win32.Khalesi	中	此威胁是一种具有多种恶意功能的家族木马。该家族样本运行后，会窃取系统账户信息，记录键盘击键信息，下载其他恶意软件。该家族样本通过钓鱼邮件传播，通过添加计划任务持久驻留系统。
	Trojan[Ransom]/Win32.Blocker	中	此威胁是一种赎金类木马家族。该家族木马运行后会破坏电脑系统、损坏用户的文件，对用户文件加密使用户无法打开。此时黑客会向用户索要赎金并提供所谓的“密钥”，但用户支付赎金后仍然不能修复受损的文件。
	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[Dropper]/Android.Wroba	中	此威胁是安卓平台上的一种恶意代码释放类木马家族。该家族木马运行后激活设备管理器、隐藏图标。接收短信指令，根据指令拦截指定短信，伪造新版本通知释放恶意 apk 同时卸载正常程序，上传手机用户隐私信息至远程服务器地址。

关于 SASE 的三个误解

杰伊·巴伯 / 文 安天技术公益翻译组 / 译

自从 Gartner 将“安全访问服务边缘”(SASE) 定义为将无线局域网 (WAN) 功能与网络安全功能相结合的新产品类别以来，SASE 一直是热门话题。从概念上看，SASE 是有道理的；但是当将这一理想框架转变为现实 IT 方法时，就有很多误解了。在本文中，我们将分析关于 SASE 的三个常见误解。

误解 1：SASE 要求“零菊花链”

Gartner 公司《2019 年企业网络炒作周期》报告就“虚拟机服务链”（也称为“菊花链”）发出了警告，这让很多人产生了误解。

“软件架构和实施很重要。企业应警惕那些提议通过虚拟机服务链链接大量功能来提供服务的供应商，尤其是当产品来自大量收购或合作伙伴关系时。这种方法可能会加快产品上市时间，但会导致服务不一致、可管理性差和高延迟。”

的确，解决方案架构很重要。企业希望尽量减少菊花链的数量以降低复杂性。但是，这并不意味着解决方案中不能有任何菊花链。事实上，要求“零菊花链”会带来一些问题——不是性能问题，而是安全问题。

SASE 将广泛的安全技术整合到一个服务中，但如今这些技术都是相互独立的，它们都有各自的行业领先者和落后者。要求“零菊花链”的企业认为，一个 SASE 供应商就可以构建涵盖一系列功能的最佳技术，而且这些功能会越来越强大。实际上，少数菊花链能够极大地提高企业整合最佳技术的能力，由此看来，只使用一家供应商并不实际。企业需要菊花链的原因还包括：

1. 没有任何一家供应商（尤其是初创公司）可以有效地提供 SASE 的所有功能，以使其产品成熟度和最佳实践水平足以抵御攻击者。在严酷的网络战场上，如果不具备 SASE 功能，大多数初创公司将无法生存。

2. 战略性配置的一两个菊花链会增加一些复杂性，这些复杂性应由供应商管理，不应影响客户。如果 SASE 平台的性能超出预期，那干嘛还要介意菊花链的数量呢？

3.“零菊花链”意味着技术收购和大规模市场整合，这意味着少数大型 SASE 供应商拥有强大的市场力量，他们会扼杀创新并抬高价格。这对 IT 购买者来说并不是好事。

误解 2：必须对 SASE 采取全云方法

SASE 以云为中心，通过云部署安全实现速度和敏捷性。但是，SASE 并不意味着云是唯一的出路。IT 领导者不应忽略其他方法，他们必须站在更实际的立场，根据实际情况和问题使用最好的技术。例如，本地下一代防火墙设备通常是大型办公室的最佳选择；在这方面，提高性能和降低总拥有成本是关键目标。如果企业的 SASE 方法是云优先的但非仅依靠云，则应确保其解决方案符合实际情况。

误解 3：SASE 能够解决所有安全问题

企业不应认为 SASE 是全方位的解决方案。SASE 涵盖了很多领域，但并未涵盖公司保护远程工作和多重云环境所需的所有技术。例如，云工作负载保护 (CWP) 和端点检测和响应 (EDR) 对于保护用户和云计算环境至关重要，但却不是 SASE 框架的一部分。EDR 是一种应对勒索软件的重要技术，但它不属于 SASE 的范围，因为它不需要网络流量检查即可运行。相反，它是一种基于代理的解决方案，用于监控操作系统活动和完整性。

此外，SASE 仅解决有效安全计划的技术部分，而忽略了全天候安全监控和成熟事件响应所需的安全专家。如果没有专门的安全分析师团队，安全技术将是无效的——无论它们是否包含在 SASE 中。企业若想调查威胁并在其造成重大损害之前予以阻止，就需要安全专家。

采取务实的方法

SASE 风头正盛，能够帮助 IT 领导者实现多年来梦寐以求的安全状态。但是，企业不应过于偏颇，他们应放松对菊花链和云的限制，以最大限度地提高安全和业务成果。同样，企业需要将 SASE 解决方案与更广泛的安全和网络战略进行比较，看看它在哪些方面增加了价值，哪些方面仍然存在不足。通过采取务实的方法，企业可以使想法能切实落地，通过现成的安全方法提升敏捷性和生产力。

原文名称	3 SASE Misconceptions to Consider
作者简介	杰伊·巴伯（Jay Barbour），是 Masergy 公司安全产品管理总监。
原文信息	2021 年 5 月 31 日发布于 Dark Reading 原文地址 https://www.darkreading.com/cloud/3-sase-misconceptions-to-consider-/a/d-id/1341088
摘 要	SASE 风头正盛，能够帮助 IT 领导者实现多年来梦寐以求的安全状态。但是，企业不应过于偏颇，他们应放松对菊花链和云的限制，以最大限度地提高安全和业务成果。同样，企业需要将 SASE 解决方案与更广泛的安全和网络战略进行比较，看看它在哪些方面增加了价值，哪些方面仍然存在不足。通过采取务实的方法，企业可以使意识形态变得有形，通过现成的安全方法提升敏捷性和生产力。
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。