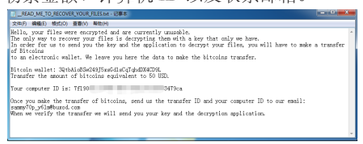
安天智甲有效防护 Encriptar 勒索软件

近日，安天 CERT 在梳理网络安全事件时发现一个名为 Encriptar 的勒索软件。该勒索软件最早于 2020 年 7 月被发现，2021 年 1 月发现新样本使用不同的扩展名，主要通过垃圾邮件进行传播，邮件附件为勒索软件程序，邮件内容诱使用户执行该程序。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 Encriptar 勒索软件的加密行为。

Encriptar 勒索软件样本运行后，创建多个线程，在短时间内完成对计算机上相关文件的加密，在被加密文件的后缀名后追加以“.solaso”命名的后缀。加密完成后，删除系统卷影副本，以防止恢复加密文件，并在加密文件所在的文件夹中创建一个名为“__READ_ME_TO_RECOVER_YOUR_FILES.txt”的勒索信，该勒索信具体内容包含了勒索说明、比特币钱包地址、勒索金额、计算机 ID 以及联系邮箱。



▲Encriptar 勒索信

Encriptar 勒索软件采用“AES + RSA”加密算法加密文件，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、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、动态（Win7 x64）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	CA67BD93E0E4BAE2B3642A611777E090
文件类型	BinExecute/Microsoft.EXE[:X64]
大小	855 KB
MD5	CA67BD93E0E4BAE2B3642A611777E090
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Ransom]/Win32.Encoder
判定依据	反病毒引擎

完整报告地址：https://1.119.163.6/vue/details?hash=CA67BD93E0E4BAE2B3642A611777E090

◆ 操作系统

操作系统	内置软件
Win7 x64 6.1.7601 Build 7601	默认、IE9、Google Chrome、Firefox、Office 2007、Flash、WPS、FoxitReader、Adobe Reader

◆危险行为

行为描述	危险等级
通过 CMD 隐藏删除自身	★★★★
删除自身	★★★★

◆常见行为

行为描述	危险等级
加载运行时 DLL	★

◆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 01 月 25 日 (总第 264 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

2020 年度中国网络安全产业联盟会员大会暨理事会成功召开，安天再获嘉奖

1 月 15 日，2020 年度中国网络安全产业联盟会员大会暨理事会通过线上线下相结合的方式成功召开。中央网信办网络安全协调局安全技术产业处副处长梁立军，联盟专家委员会主任委员顾建国，全国政协委员、联盟理事长、安天创始人 / 董事长肖新光，联盟秘书长、中国电子技术标准化研究院副院长程多福，联盟副秘书长许玉娜、方华以及会员代表参加了本次会议。联盟常务理事、绿盟科技副总裁李晨主持会议。肖新光理事长汇报了联盟 2020 年工作总结和 2021 年工作要点。

梁立军副处长在视频致辞中指出，2021 年是“十四五”开局之年，面临日趋复杂的安全形势，面对创建网络安全新发展格局的机遇，希望中国网络安全产业联盟继续充分发挥作用，支撑网络安全教育、技术、产业融合发展。一是秘书处发挥好桥梁作用，积极组织成员参与国家相关治理工作。二是参与网络安全教育技术产业融合发展事业，引导会员企业与科研院所、高校等相关机构开展合作协同育人工作。三是引导技术创新，打造良好产业生态。

顾建国主任在致辞中强调，网络安全企业要深入学习贯彻五中全会精神和中央经济工作会议精神，把握新阶段、贯彻新理念，构建新格局。一是认真研究分析网络安全产业发展当前面临的机遇和挑战，增强忧患意识、创新意识。二是要高度重视产业基础和产业链的问题，积极推进网络安全产业新生态系统的建设。三是充分发挥好联盟的作用，做好企业与主管部门沟通的桥梁，发挥好导向作用。

本次会议特别邀请了教育部高等学校网络空间安全专业教学指导委员会秘书长、北京电子科技学院副院长封化民，联盟专家委专家、国家信息技术安全研究中心原副主任兼总工、中国网络安全审查技术与认证中心首席专家李京春分别以“产学深度合作 助推人才培养”、“智能网联汽车安全焦点”为主题，发表了专题报告。北京数美时代科技有限公司作为新会员代表做了专题演讲。会议期间，举行了“中国网络安全产业联盟技术支持单位”授牌仪式，顾建国主任和程多福秘书长共同为 11 家技术支持单位授牌。联盟常务理事、盛邦安全 CEO 权小文主持增选理事单位投票，经过投票表决，北京兴汉网际股份有限公司、成都思维世纪科技有限责任公司、山东中网云安智能科技有限公司、网宿科技股份有限公司等 4 家单位成功当选理事单位。同时，大会还对 2020 年联盟突出贡献单位和优秀会员单位进行了表彰。

会议上，安天获评“2020 年中国网络安全产业联盟突出贡献单位”和“2020 中国网络安全产业联盟技术支持单位”双项荣誉称号。

安天在 20 年的发展历程中，始终致力于有效应对安全威胁，全面提升客户的网络安全防御能力。通过 20 年自主研发积累，安天形成了威胁检测引擎、移动场景安全、高级威胁对抗、大规模威胁自动化分析等方面的技术领先优势。构筑了由铸岳、智甲、镇关、探海、捕风、追影、拓痕、智信组成的产品方阵，为客户构建资产安全运维、端点防护、边界防护、流量监测、导流捕获、深度分析、应急处置、零信任接入等安全基石。

（原文链接：https://mp.weixin.qq.com/s/KhbtulvHYsivjtDp-UExbg）

扫描二维码阅读原文

每周安全事件

类 型	内 容
中文标题	LuckyBoy 恶意广告活动针对移动和 XBox 用户
英文标题	'LuckyBoy' Malvertising Campaign Hits iOS, Android, XBox Users
作者	Ionut Arghire
内容概述	Media Trust 网络安全专家发现了一项针对 iOS、Android 和 XBox 用户的恶意广告活动，并将该活动称为“LuckyBoy”。该活动于 2020 年 12 月以来，主要针对欧洲用户，也观察到针对美国和加拿大用户的活动。恶意软件会检查一个全局变量“luckyboy”，从而检测设备上是否存在拦截程序、测试环境和运行的调试器。如果检测到其中任何一个，恶意软件将不会执行。如果在目标环境中运行，恶意软件会执行一个跟踪像素程序，将用户重定向到恶意内容，包括钓鱼页面和假冒软件更新。
链接地址	https://www.securityweek.com/luckyboy-malvertising-campaign-hits-ios-android-xbox-users

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 SharePoint 安全漏洞（CVE-2021-1707）	高	Microsoft SharePoint 存在一个远程代码执行漏洞，该漏洞源于 SharePoint 服务器未对用户输入进行有效的校验，导致攻击者可以通过对特定的 api 发送精心构造的数据实现远程命令执行，从而控制服务器。
	GDI+ 远程代码执行漏洞（CVE-2021-1665）	高	Windows 图形设备接口 (GDI) 处理内存中对象的方式中存在远程代码执行漏洞。成功利用此漏洞的攻击者可能会控制受影响的系统。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。
	Microsoft Excel 远程代码执行漏洞（CVE-2021-1714）	高	Microsoft Excel 中存在安全漏洞。当 Microsoft Excel 软件无法正确处理内存中的对象时，该软件中存在远程代码执行漏洞。成功利用此漏洞的攻击者可以在当前用户的上下文中运行任意代码。
较为活跃样本家族	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[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[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/Win32.Injuke	中	此威胁是一种可以窃取密码信息的木马类程序。该家族的样本运行后会窃取用户账户信息，记录键盘击键等。
	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[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[SMS]/Android.Opfake	中	此威胁是一种基于 Android 的恶意应用程序。该家族没有统一的行为与功能，一般会窃取用户短信、发送包含恶意 URL 的短信或进行其他与短信有关的恶意操作。

漏洞管理存在数据问题

塔尔·摩根斯坦 / 文 安天技术公益翻译组 / 译

安全团队拥有大量的数据，但是大多数数据缺乏必要的情境信息，无法改善漏洞修复结果。

如今，漏洞管理团队拥有庞大的数据，处理和分析数据所需的时间甚至能“赶超”修复漏洞所需的时间。出现这种情况的主要原因是，许多漏洞修复工具仅提供修复漏洞所需数据的片段。与此同时，安全团队希望增加云 IT 的投资，导致漏洞管理团队承受着精简和扩展修复流程的压力。如果漏洞管理团队跨数十种工具手动解析孤立的数据，则无法实现上述目标。包括首席信息安全官（CISO）在内的漏洞修复团队需要更好而非更多的数据。

数据存在的问题

漏洞管理工具能够收集基本数据，例如检测到的漏洞数量、受影响的资产和技术等。通过这些工具，安全团队可以监控大多数修复措施，但是它们无法提供相关细节，难以改善修复结果。更成熟的安全团队使用电子表格或商业智能（BI）工具来跟踪相关指标，例如已修复的漏洞数量、目前仍存在的漏洞数量，以及自上次扫描以来发现的新漏洞数量等。

尽管这些数据很有帮助，但它们缺乏情境信息，很难提供修复程序的整体性视图。例如，它们无法匹配漏洞位置与受影响的业务部门，无法报告修复漏洞所需的时间，也无法确定漏洞的优先级。而此类细节恰恰是改善修复结果的基础。

真正需要的数据

安全团队需要的是，能够帮助他们根据业务风险确定修复优先级，以及指导和推动修复流程改进的数据。这些数据应帮助他们确定薄弱环节，并针对影响最关键业务领域的技术调整补救措施。

例如，扫描程序在第 7 行中发现了 SQL 注入漏洞或 Red Hat 框需要的补丁，但这些信息无法向企业传达受影响的产品、产品的所有者或对业务的影响程度。在这些漏洞中，哪一个会给电力供应带来最大的风险？如果安全团队不能同时修复所有漏洞，那么需要首先修复哪个漏洞？

另一个考虑因素是，受影响的技术风险取决于企业的业务周期。例如，许多零售商在假日购物期间风险会增加；而杂货连锁店每月推出新产品，这可能会导致风险在多个 IT 和业务部门之间转移。为了应对这些情况，安全团队需要更好的数据，以根据业务期望实时制定决策。

接下来，修复团队需要了解特定修复程序如何影响运营。虽说漏洞管理工具会跟踪平均修复时间，但这些结果基于每周一次的扫描，缺乏重要的情境信息。上周报告的哪些漏洞已被修复？修复每个漏洞需要多长时间？ 1 天，5 分钟，还是 5 天？

这些数据对于 CISO 也是很有价值的。历史数据能够显示，哪些平台需要更长的时间进行修复（以及原因），这可以帮助安全团队确定效率低下的流程、产品和人员问题，以及如何最好地解决这些问题。

漏洞为何如此难修复

改善漏洞修复的最大障碍是，数据被孤立存储在诸多不同的系统中，例如扫描程序中的漏洞数据、配置管理数据库或资产存储库中的业务情境数据；或者更糟的是，数据存储在人们的头脑中。此外，安全团队可能会在各个团队中部署多个漏洞管理工具，这些工具分别提供给漏洞扫描人员、威胁情报团队、IT 运营技术人员等。

使问题更加复杂的是，现有工具并不存储某些数据点。例如，很少有企业跟踪 DevOps 团队查找漏洞、安装补丁并检查其是否有效所需的时间。即使有企业这样做，他们也很少将这些信息纳入漏洞管理程序中。

此外，某些漏洞管理工具会忽略未存储的数据点。因此，如果 CISO 询问最近六个月修复了多少个漏洞，则大多数漏洞管理工具都没有相应的数据。

企业可以做些什么

企业面临的困难是——创建改善修复结果的工作流程。首先，漏洞修复团队必须让业务部门参与进来，要求他们确定关键的业务功能以及资产之间的关系。此外，他们要匹配业务功能与支持技术产品，然后评估每项资产的重要性，并将其与漏洞管理程序关联起来。

接下来，安全团队应从 DevOps 和 IT 运营团队中邀请合作伙伴，以帮助协调和协同进行修复工作。随着时间的推移，这些合作关系将成为安全团队根据需要改进修复流程的关键。

这种协同并不容易实现，也不直观，通常是强制性的。因此，安全团队负责人必须设法通过设立跨职能团队、培训等方法来实现。他们应讨论所需的数据，然后确定如何收集和利用这些数据，以开展有效且主动的漏洞修复活动。

最后，有效地收集、解析和分析数据是成熟漏洞修复程序的关键。无论企业使用电子表格还是 BI 工具，修复团队都必须确定要跟踪的指标，并设置合理的关键绩效指标（KPI）。根据这些数据确定目标，有助于更轻松地实现目标。

我知道，修复漏洞是一个沉重的负担。但是，这种负担也会带来强大的动力。对于安全团队来说，最痛苦的莫过于，一个本来可以避免的漏洞，因为没有在补丁首发时间给系统打补丁而成为突破口。

听起来耳熟吗？

原文名称	Vulnerability Management Has a Data Problem
作者简介	塔尔·摩根斯坦（Tal Morgenstern）。塔尔·摩根斯坦是 Vulcan Cyber 的联合创始人兼首席产品官。
原文信息	2020 年 01 月 14 日发布于 Dark Reading 原文地址 https://www.darkreading.com/vulnerabilities---threats/vulnerability-management-has-a-data-problem/a/d-id/1339827
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。