安天智甲有效防护 Encrpt3d 勒索软件

近日，安天 CERT 在梳理网络安全事件时发现了一个名为 Encrpt3d 的勒索软件。该勒索软件最早于 2021 年 4 月被发现，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 Encrpt3d 勒索软件的加密行为。

Encrpt3d 勒索软件运行后拷贝自身到 C:\ProgramData\CheckServiceD.exe，在注册表路径 HKEY_CURRENT_USERSOFTWARE\Microsoft\Windows\CurrentVersion\Run 下添加键 " CheckServiceD " 并将值设为 CheckServiceD.exe 的路径，以实现持久化。该勒索软件首次运行时并不会加密文件，设置完自启动后便退出，只有在检测以上注册表键值存在时才会加密文件，其采用 AES-256 算法对非系统盘和用户目录下常见后缀的文本、文档、图片、数据库、源代码等文件进行加密，被加密的文件会在原文件名后追加后缀 ".encrpt3d"。加密完成后弹出窗口展示勒索信，要求受害者向指定 BTC 地址支付 10 个比特币以解密文件。该勒索软件没有回传或记录密钥的功能，即使受害者按要求支付赎金也无法获得密钥解密文件，但因其没有删除卷影，受害者可尝试通过卷影恢复数据。

▲Encrpt3d 勒索软件勒索信

Encrpt3d 勒索软件采用“AES-256”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、动态（Win7 x64）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	a2d60af7bebac9b299db109f8162ed6335fb5dda08f57f00e9dc809d4f138428
文件类型	BinExecute/Microsoft.EXE[:X64]
大小	30 KB
MD5	B36E5C508EFEA796731D444C189B413C
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Ransom]/Win32.Blocker
判定依据	反病毒引擎

报告地址：https://1.119.163.6/vue/details?hash=B36E5C508EFEA796731D444C189B413C

◆运行环境

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

◆常见行为

行为描述	危险等级
自启动	★★★
自我复制	★★
同步机制	★
线程操作函数	★
进程 / 线程是否处于调试状态	★
枚举进程	★
结束进程类函数	★
文件操作函数	★
可执行文件	★
.....	.....

◆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 05 月 03 日 (总第 276 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

国家工业信息安全发展研究中心领导莅临安天总部调研

4 月 29 日，国家工业信息安全发展研究中心郝志强副主任带队调研安天集团哈尔滨总部基地。

安天集团董事长、首席技术架构师肖新光向来宾介绍了安天的整体研发能力、核心引擎能力、产品技术体系、安天发展历程等，重点介绍了安天的赛博超脑云化安全基础设施、一体化智能化安全运营平台等防御体系构建情况。安天集团高级副总裁、国泰网信总经理李欣向来宾介绍了安天依托威胁对抗 + 密码可信能力深度融合的工业信息安全产品服务及方案落地案例。

国家工业信息安全发展研究中心相关领导介绍了自身的研究成果与业务建设情况，双方团队就技术与业务合作进行了深入研讨。

安天是引领威胁检测与防御能力发展的网络安全国家队，长期致力为战略客户和关键基础设施提供整体安全解决方案。安天的威胁检测引擎为全球超过一百万台网络设备和网络安全设备、超过二十六亿部智能终端设备提供了安全检测能力。面对数字化转型升级的安全防御需求和日益复杂的安全挑战，安天依托端到端的安全能力，积极发挥供应链关口前移的优势，将安全能力基因向包括办公网、云环境、物联网、工业互联网等在内全场景有效防御覆盖，并依托强大的威胁对抗体系，实现深度客户赋能，驱动客户完成从威胁情报消费，到自主安全能力生产的智能化安全运营变革。

（原文链接：https://mp.weixin.qq.com/s/9v6D2E3dLq1C2flR1fFUNg）

扫描右侧二维码阅读全文

移动安全攻防重心开始迁移，风险应用成为移动终端用户侧新的安全威胁

过去的十年，是移动互联网技术和移动智能终端快速发展、普及的十年。随着安卓操作系统的安全性提升以及国内移动智能终端生态的改善，安天移动安全检测预警平台大数据显示，自 2017 年始，随着国内反病毒技术的逐渐成熟，移动终端侧的新增恶意程序数量呈逐渐下降趋势。

然而，针对移动终端用户的安全威胁并未随之递减，反而呈现出威胁泛化的趋势。由于生产要素的获取极其便利且廉价，在流量利益的驱动下，风险应用程序出现大规模扩张，早在 2017 年，安天移动安全就在年报中提出了威胁全面迁徙的观点。

近年来，安天移动安全都在持续关注移动智能终端的安全态势。从移动终端用户的安全视角出发，基于是否有违国家政策法律法规、是否存在侵害用户权益、是否存在侵害用户个人信息或资金安全三类主要的判别标准，安天移动安全发现，当前移动终端用户面临的主要安全问题有以下五个方面：

应用程序（APP）成为网络犯罪的新载体，也是用户安全最主要的威胁来源之一

当前，移动互联网应用程序（APP）逐步渗透到衣、食、住、行等与人们生活息息相关的各个领域，在给人们生活带来诸多便利的同时也引发一系列安全问题。网络诈骗、网络博彩、网络色情、网络传销四大主要网络犯罪类型基于 APP 完成整个犯罪实施的闭环，在犯罪实施过程中，让用户安装或使用相关 APP 成为不可或缺的重要环节。

网络犯罪团伙基于移动互联网应用，形成了不同的细分场景，比如，利用社交交友类 APP 进行“杀猪盘”诈骗、贷款诈骗、投资理财诈骗；开发专门的网络博彩应用，或在色情应用、棋牌游戏应用中为网络赌博、博彩引流下注；利用金字塔分层收益机制及会员等级制度进行应用推广、拉新获客，从而达到其非法牟利的目的。

开发者通过包装 APP 的功能及业务，侵害用户权益并进行非法牟利

安天移动安全风险检测预警平台发现，有些应用开发者会通过设计和开发包装成特定业务场景或者产品功能的 APP ，实现诱导付费会员、强制用户使用等目的。

（原文链接：https://mp.weixin.qq.com/s/QoKY2hIxJokuRed-BPTNQA）

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	Passwordstate 密码管理器遭受供应链攻击
英文标题	Supply chain attack on the password manager Clickstudios - PASSWORDSTATE
作者	ClickStudios
内容概述	澳大利亚公司 ClickStudio 在 4 月 20 日至 4 月 22 日之间的某个时间遭受了软件供应链攻击，攻击者入侵了该公司的密码管理器 Passwordstate，并植入了恶意代码。CSIS 研究人员发现，名为“Moserware.SecretSplitter.dll”的文件被植入了恶意代码片段，恶意代码尝试与 URL 进行联系，来检索加密代码。获取的加密代码解密后，代码将直接在内存中执行。由于发现时 C&C 已关闭，研究人员没有检索到第二阶段的有效载荷。
链接地址	https://www.csis.dk/newsroom-blog-overview/2021/moserpass-supply-chain/

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 Raw Image Extension 远程代码执行漏洞（CVE-2021-28466）	高	Microsoft Raw Image Extension 存在远程代码执行漏洞。由于 Raw Image Extension 中的输入验证不正确，使得攻击者可以发送特制请求并在目标系统上执行任意代码。
	Microsoft Excel 远程代码执行漏洞（CVE-2021-28454）	高	Microsoft Excel 存在远程代码执行漏洞。由于该应用中的输入验证不正确，使得攻击者可以诱骗受害者打开特制文件或访问恶意网站，并在目标系统上执行任意代码。
	Microsoft Windows Media 远程代码执行漏洞（CVE-2021-27095）	高	Microsoft Windows Media 存在远程代码执行漏洞。由于 Windows Media 视频解码器中的输入验证不正确，使得攻击者可以欺骗受害者打开特制文件并在目标系统上执行任意代码。
较为活跃样本家族	Worm/Win32.AutoRun	中	此威胁是一种蠕虫类程序。该家族能够在磁盘根目录或插入的可移动存储介质的根目录下创建一个 autorun.inf 文件并自我复制，该文件中包含可执行蠕虫的名字和路径。用户将磁盘或可移动存储介质接入电脑后，系统会自动执行 autorun.inf 中指定的可执行程序。该家族除了能够感染本地电脑外，还可以通过共享文件传播至远程电脑中。
	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.Vilsel	中	此威胁是一种窃密类木马家族。该家族木马通过垃圾邮件或恶意网站进行传播。该家族木马感染用户电脑后，会为黑客建立远程连接以控制用户电脑，窃取用户敏感信息（账号和密码等），同时会下载并运行其它恶意程序。
	Trojan/Win32.Fsysna	中	此威胁是一种木马家族。该家族样本运行后会在电脑的临时文件夹下释放恶意代码，同时添加注册表启动项，并发送网络请求。
	Trojan[GameThief]/Win32.Lmir	低	此威胁是一种盗取游戏账号信息的木马类家族。该家族样本运行后会截获当前用户的键盘和鼠标消息以获取游戏的账号及密码，并将获取到的信息发送给攻击者。该家族主要以窃取网络游戏的账号和密码为主要目的。
	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.Boogr	中	此威胁是安卓平台上的伪装类木马家族。该家族木马通常伪装成游戏或流行应用程序，运行后可以下载其他恶意文件，将 SMS 消息发送给高价软件，或将受害者的智能手机连接到攻击者的命令和控制服务器。

云计算的下一个大事件：机密云

艾亚尔·约耶夫 / 文 安天技术公益翻译组 / 译

受业务驱动，企业对云服务的需求激增，对高度安全的云计算的需求也更加迫切。许多处理敏感数据的企业对于云迁移有些担忧，这并不是没有理由的。

有一段时间，公有云能够比传统现场环境提供更多的保护。举例来说，专家团队可以确保云服务器保持最佳的安全状态，且能够抵御外部威胁。

但是，达到这种安全水平是需要付出代价的。例如，专家团队会导致更高的内部人员隐私数据泄露风险，使合规性工作更加困难。

数据安全技术（芯片、软件和云基础架构）的最新发展正在改变这一现状。新的安全功能能够有效地锁定内部人员或外部攻击者的数据访问权限，将公有云转变为受信的数据安全环境。

这就消除了最后一个安全障碍。这样一来，即使是最敏感的数据和应用程序，也可以进行全面的云迁移了。利用这种机密云，企业无论何时何地都可以独有其数据、工作负载和应用程序。

现在，即使是世界上一些最注重安全性的组织，也将机密云视为存储、处理和管理数据的最安全选择。机密云的吸引力，在于其能够实现专有数据控制，将数据风险降到最低（硬件级别）。

机密云是什么？

在过去的一年中，关于机密计算的讨论有很多，包括安全飞地或 TEE（受信执行环境）。现在，基于 Amazon Nitro Enclaves，Intel SGX（软件保护扩展）和 AMD SEV（安全加密虚拟化）芯片构建的服务器已经可以进行机密计算了。

机密云利用这些技术来建立安全、不可穿透的加密边界，该边界从受信的硬件无缝扩展，以保护使用中、存储中和传输中的数据。

传统的分层安全方法在数据和攻击者之间建立屏障，或者为存储或传输中的数据提供独立的加密。机密云与此不同，它提供了与数据本身不可分离的强大数据保护。这消除了企业对传统边界安全层的需求，同时使数据所有者可以在存储、传输或使用数据的任何位置进行独有控制。

从概念上看，机密云类似于网络微分段和资源虚拟化。但是，机密云不仅可以隔离和控制网络通信，还可以跨 IT、计算、存储和通信的所有基本要素，扩展数据加密和资源隔离。

在与云运维（CloudOps）内部人员、恶意软件或潜在攻击者隔离的受信环境中，机密运行任何工作负载所需的一切，都能通过机密云汇总在一起。

这也意味着，即使服务器受到物理损害，工作负载仍然能够保持安全。即使是具有服务器 root 访问权限的攻击者，也会被阻止查看数据或获得对数据和应用程序的访问权限。如今的微分段则无法提供这种安全水平。

比现场环境更安全

人们普遍认为，知名云提供商具备保护绝大部分内部 IT 基础架构所需的资源。但是，数据开放式云带来了更大的内部人员数据泄露风险，并且无法在 CISO 完全控制的情况下锁定受信环境。

迄今为止，在一些广为人知的攻击事件中 都出现了数据泄露。举例来说，一名 AWS 员工泄露了 CapitalOne 的内部数据，之后，这些数据就在云中公开了。

实施机密云能够消除云内部人员泄露数据的可能性，从而关闭数据攻击面（否则云提供商会面临这种攻击面）。机密云的数据控制措施，可以扩展到数据可能遭泄露的任何地方，包括存储位置、网络上以及多个云中。

构建自己的机密云

OEM 软件和 SaaS 供应商已经开始构建机密云，以保护其应用程序。最近，Redis 公司宣布了其高性能软件的安全版本，该版本可在多个安全计算环境中运行——创建了有可能是世界上最安全的商业数据库。

Azure 机密计算已与机密云供应商合作，以在不对基础应用程序做任何修改的情况下，在现有基础架构上安全地形成和执行任何工作负载。紧随其后，Kubernetes 也将支持多重云。

最初的机密计算，需要对代码进行修改才能运行应用程序。这是因为，最初的机密计算技术侧重于保护内存，必须修改应用程序才能在受保护的内存段中运行选定的敏感代码。对大多数公司而言，重写和重新编译应用程序是沉重的负担——对于旧版或现成的软件包，这甚至是不可能的。

提升后的实施路径，使企业能够在受保护的机密云中创建、测试和部署敏感数据工作负载，而无需修改或重新编译应用程序。如今，几乎所有云提供商（包括 Amazon，Azure 和 Google）都提供机密云支持架构。

利用机密云软件，应用程序（甚至整个环境）可以在不进行任何修改的情况下，在机密云中运作。附加软件抽象和虚拟层的优势在于，使机密云独立于英特尔、AMD、亚马逊和 ARM 开发的众多专有安全飞地技术和版本。

新一代的安全厂商，已简化了为公有云客户实施私有测试和演示环境的过程。这加快了将私有应用汇集并生成成熟机密云架构的速度。

机密计算很好，机密云更好

确保数据安全是将应用程序迁移到云和整合 IT 资源的最后障碍。通过实施机密云，除了最敏感的应用程序和数据外，企业在云迁移方面迈出了伟大的一步。消除数据漏洞后，企业能够获得广泛的新机会，能够轻松部署基于机密云构建的新的、安全的托管 IT 基础架构。

原文名称	The next big thing in cloud computing? Shh… It’s confidential
作者简介	艾亚尔·约耶夫（Ayal Yogev），是 Anjuna Security 公司的首席执行官。
原文信息	2021 年 04 月 28 日发布于 Help Net Security 原文地址 https://www.helpnetsecurity.com/2021/04/28/confidential-cloud/
摘 要	现在，即使是世界上一些最注重安全性的组织，也将机密云视为存储、处理和管理数据的最安全选择。机密云的吸引力，在于其能够实现专有数据控制，将数据风险降到最低。从概念上看，机密云类似于网络微分段和资源虚拟化。但是，机密云不仅可以隔离和控制网络通信，还可以跨 IT、计算、存储和通信的所有基本要素，扩展数据加密和资源隔离。
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。