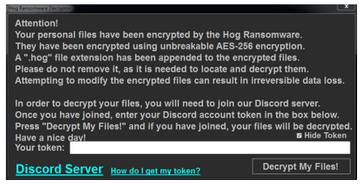
安天智甲有效防护 Hog 勒索软件

近日，安天 CERT 在梳理网络安全事件时发现一个名为 Hog 的勒索软件。该勒索软件最早于 2021 年 2 月被发现，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的勒索软件防护模块可有效阻止 Hog 勒索软件的加密行为。

Hog 勒索软件使用 AES-256 对称加密算法来加密文件，其中加密算法使用的 Key 为随机数，向量 IV 为硬编码。除了 C:\Windows 路径下的文件和后缀名为 ".exe",".dll",".ini",".scr",".sys",".vmx",".vmdk" 的文件，其余文件均会被加密，并在原文件名后追加 ".hog" 后缀，随后会从资源文件中释放解密程序（包含展示勒索信功能）DECRYPT-MY-FILES.exe 到 Windows 的启动目录，并把上文随机生成的 Key 保存到解密程序末尾，用于之后的解密。该勒索软件特殊之处为，其并非以索要赎金为目的，而是要求受害者加入指定 Discord 服务器，在解密程序中需要输入受害者的 Discord 账户令牌，解密程序会通过该令牌验证受害者 Discord 的 API，验证通过即说明受害者已加入攻击者 Discord 服务器，随后进行解密。该勒索软件不需要任何赎金，说明其可能处于开发的早期阶段。



▲Hog 勒索信

Hog 勒索软件对文件加解密时使用的是 AES-256 对称加密算法，且使用的 Key 和向量 IV 都被硬编码在解密程序中，因此即使不服从攻击者的要求，也可对被加密文件进行解密。

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、动态（Win XP）鉴定器、动态（Win7 x86）鉴定器、信标检测鉴定器、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	209eeb95b61cb7114baa21b7599641e34e825a4887ad0466c2cf2ac3cb4c4695
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	36 KB
MD5	BB90E0F1B311001AFBDA19C105C35557
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/MSIL.Filecoder
判定依据	反病毒引擎

报告地址：https://1.119.163.6/vue/details?hash=BB90E0F1B311001AFBDA19C105C35557

◆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、Office 2003、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
检测自身是否被调试	★★
镜像劫持	★★
加载运行时 DLL	★
打开自身进程文件	★
获取系统信息（处理器版本、处理器类型等）	★
获取系统版本	★
检索系统内存信息	★
获取计算机名	★
启动指定服务	★
DNS 请求	★
独占模式打开，防止复制读取，防止杀毒软件扫描上报	★
设置调试器权限	★

◆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03月29日(总第271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

“中国网络安全行业全景图”发布

近日，行业咨询机构安全牛发布“中国网络安全行业全景图(2021年第八版)”，安天入选11个细分领域中的54项，安天传统的业务优势领域，如反病毒、反APT、端点安全、流量监测响应、态势感知等毫无悬念入选。安天坚持持续系统安全底层能力研发，长期以关口前移模式赋能供应链，也逐渐转化为云安全、零信任等领域的竞争力。

安天以提升国家互联网治理能力构筑基础设施为目标，已绘就未来5年发展蓝图：充分发挥技术积累和信创的先发优势，有力覆盖云、虚拟化、智能办公等场景，加快容器防护、SASE等新兴技术防护建设。同时，为有效提升信创载体的处理能力，安天正在规划安全引擎加速芯片，并已经研发了FPGA的原型。

在20年的发展历程中，安天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。构筑出了铸岳、智甲、镇关、探海、捕风、追影、拓痕、智信组成的产品方阵，可以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。安天通过为客户建设态势感知平台体系，形成网络安全运行的神经中枢，提升客户统一安全运维水平，通过大规模感知体系，和大规模支撑平台，通过快捷精准的威胁情报持续完成客户赋能。安天的产品和解决方案保障客户从办公内网、私有云、混合云到工业生产网络的全面安全，保障客户关键数据资产安全和业务运行连续性。使客户能有效应对从病毒传播感染、网络勒索乃至情报级别的攻击窃密的不同层级的威胁，为客户数字化转型保驾护航。

安天不是以盲目拓宽产品赛道应对新需求，而是充分发挥以工程体系支撑威胁对抗的共性能力基础，通过引擎情报一体化，实现产业协同和生态赋能，从而在多个新兴领域实现绕前布局。安天长期坚持系统安全层面共性技术积累，通过ATT&CK等威胁框架的攻击技术枚举，持续提升端点侧、流量侧、分析侧、处置侧和欺骗防御环节的风险发现和防护处置水平。安天强调对异构互联的各种体系结构和应用场景中的端点实现全面防护和管理能力覆盖，并通过资产运维和管理平台实现有效产品集中管理和整合，从而全面提升用户的自动化运维处置水平。

原文链接：https://mp.weixin.qq.com/s/yyAJsQpTcrS_DYyPFI5k2A

扫描上方二维码阅读全文

Android 木马程序冒充 Clubhouse 应用

ESET 恶意软件研究人员 Lukas Stefanko 发现，网络罪犯正试图利用 Clubhouse 的流行传播恶意软件，目的是盗取用户的登录信息，用于各种在线服务。该恶意软件伪装成仅限邀请的音频聊天应用程序的 Android 版本（尚不存在），是从具有真正 Clubhouse 网站外观的网站提供的。该木马被 ThreatFabric 称为“BlackRock”，被 ESET 产品检测为 Android / TrojanDropper.Agent.HLR，可以盗取受害者至少 458 个在线服务的登录数据。

（原文链接：https://www.welivesecurity.com/2021/03/18/beware-android-trojan-posing-clubhouse-app/）

Black Kingdom 勒索软件针对微软 Exchange 服务器

一个被称为“Black Kingdom”的勒索软件正在利用微软 Exchange 服务器的 ProxyLogon 漏洞对服务器进行加密。根据提交给勒索软件识别网站 ID Ransomware 的信息，Black Kingdom 勒索软件活动已对其他受害者的设备进行了加密，最早的提交日期为 3 月 18 日。受害者位于美国，加拿大，奥地利，瑞士，俄罗斯，法国，以色列，英国，意大利，德国，希腊，澳大利亚，和克罗地亚。加密设备时，勒索软件将使用随机扩展名加密文件，然后创建一个名为 crypto_file.TxT 的勒索通知。

（原文链接：https://www.bleepingcomputer.com/news/security/microsoft-exchange-servers-now-targeted-by-black-kingdom-ransomware/）

每周安全事件

类 型	内 容
中文标题	PRODAFT 公司访问 SolarWinds 黑客的服务器
英文标题	Swiss Firm Says It Has Accessed Servers of a SolarWinds Hacker
作者	Daniele Lepido
内容概述	瑞士网络安全公司 PRODAFT 表示，他们已经访问了一个与 SolarWinds 漏洞有关的黑客组织使用的服务器，其中披露了攻击者针对目标以及他们如何实施行动的细节。PRODAFT 公司还表示，黑客们的活动一直持续到本月。据报道，SilverFish 对至少 4720 个目标实施了“极其复杂”的网络攻击，其中包括政府机构、全球 IT 提供商、美国和欧盟的数十家银行机构、主要审计 / 咨询公司、全球领先的 Covid-19 测试设备制造商以及航空和国防公司。据研究人员称，除了 SolarWinds 软件的漏洞外，黑客还使用了其他方法来攻击受害者。研究人员没有将这些攻击归咎于一个已知的黑客组织或某个国家，但他们将 SilverFish 描述为一个“APT 组织”。
链接地址	https://bbs.antiy.cn/forum.php?mod=viewthread&tid=85236&_dsign=60bf430c

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 Visio 安全漏洞（CVE-2021-27055）	高	Microsoft Visio 存在权限提升漏洞。由于 Visio 应用中身份验证的安全功能存在问题，攻击者可以诱骗受害者打开特制文件从而在目标系统上绕过身份验证过程，获得提升的特权。
	Microsoft PowerPoint 安全漏洞（CVE-2021-27056）	高	Microsoft PowerPoint 存在远程代码执行漏洞。由于 PowerPoint 应用中的输入验证不正确，攻击者可以创建一个特制文件，诱骗受害者打开该文件，触发释放后可重用的内存漏洞，并在目标系统上执行任意代码。
	Microsoft Excel 安全漏洞（CVE-2021-27053）	高	Microsoft Excel 中存在远程代码执行漏洞，该漏洞源于程序没有正确处理内存中的对象。攻击者可利用该漏洞在当前用户的上下文中执行任意代码。
较为活跃样本家族	Trojan/Win32.Yakes	中	此威胁是一种恶意木马家族。该家族木马可以通过白名单机制绕过系统防火墙，获取系统的最高权限。该家族木马具有下载恶意程序、监控用户操作等行为。该家族木马会在执行完成后将自身删除。
	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[Dropper]/Win32.Dinwod	中	此威胁是一种具有释放或捆绑行为的木马类家族。该家族木马在感染用户系统之后，会自动释放并安装其它恶意程序。该家族的部分变种还具有强制关闭杀毒软件的能力。
	Trojan[Backdoor]/Win32.Salgorea	中	此威胁是一种可以下载恶意代码的木马类家族。该家族样本运行后连接网络下载恶意代码并执行。
	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]/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。

如何防御日益增长的伪造身份诈骗

伊万·赫德 / 文 安天技术公益翻译组 / 译

近年来，银行在减少银行卡诈骗方面取得了一些成功，但是，一种新的诈骗日益严重，这就是“伪造身份诈骗”。在数字平台上，金融犯罪分子将真实和伪造的信息相整合，以执行此类诈骗，而且未被追责。

伪造身份诈骗不断增加的原因有很多，银行和其他金融机构可以采取一些措施，防止这种不断增长的威胁造成损害。

伪造身份诈骗不断增加

在识别这种复杂的诈骗方面，全球银行都面临着挑战。这类诈骗者是专业的网络犯罪分子。他们通过暗网获取合法的个人信息，将其与伪造的信息相整合。之后，他们使用新生成的身份创建积极的信用报告，然后进行消费或借贷，直到该身份的支出能力达到上限。

他们经常会同时使用多个伪造身份，以最大程度地获利。诈骗者甚至为这些伪造身份创建了可以在信用局查到的档案，因此这类行为很难被发现。

滋生诈骗的经济环境

新冠疫情给世界造成了巨大的经济损失，预计今年全球 GDP 将大幅下降。这造成的结果是，企业在艰难的商业环境下努力管理营运资金需求，寻求新的信贷额度，银行贷款规模随之增加。个人客户也需要更高的信贷额度。

在存在更多借贷活动，需要监控更多投资组合，且需要弥补更多损失的经济环境中，隐藏诈骗行为就更加容易了。犯罪分子可以躲藏在经济动荡的喧嚣中，而金融机构难以应付庞大的申请量，被大量的

身份核查工作压垮。

当贷款到了偿还之际，金融机构很难区分真实客户的拖欠和违约 vs 诈骗者的蓄意攻击。

此外，在失去工作和经济安全感，又面临其他经济困难的情况下，可能会有更多人采取诈骗手段来维持其生活水平。

优先考虑客户体验

在全球疫情的特殊情况下，银行不得不远程进行更多的识别和验证，这一变化不太可能再回到以前。虽然对于消费者和银行来说这样既方便又快捷，但是当交易、支票和身份验证完全在数字领域进行时，进行诈骗就容易得多了。

如果银行采取传统的保护手段，例如更深入的身份验证，就会给消费者增加麻烦。消费者不希望在流程上花费太多时间，他们会选择流程更加便捷的银行。许多银行担心失去客户，因此为客户提供精简、无摩擦的体验，为此愿意接受这种诈骗风险。

诈骗者不断测试所有银行的漏洞，确定最简单的目标，然后集中精力攻击这些目标，直到其诈骗行为被发现和阻止。

有组织的犯罪团伙已经开发出利用这些漏洞的新方法，他们经常针对信用记录很少或没有的年轻人或老年人（这些人不太可能定期检查其信用报告）。

阻止伪造身份诈骗

尽管身份盗窃和伪造身份诈骗日益增加，日趋复杂，但是银行并未将此作为优先事项

——他们不愿为了实施适当的诈骗控制而牺牲客户体验。

许多银行希望改进身份验证流程，以证明应用程序中的“人”就是真实的用户。通过利用跨渠道情报（包括设备数据和外部数据源），金融机构可以保护自己和客户，且不会使验证过程过于复杂。

在未来几年，要想阻止伪造身份诈骗，实体解析至关重要。实体解析将各种来源的数据汇总在一起，更容易识别信息差异，而这种信息差异正是伪造身份诈骗的危险信号。通过实体解析，金融机构可以在应用程序或信用报告上查看有关人员的所有信息，分析他们是否使用一致的地址、电话号码、电子邮件地址、姓名拼写等信息。

有组织的犯罪往往会留下相互关联的痕迹，金融机构应更密切地监控网络，使用正确的技术和工具检测这些痕迹。银行需要找到更好的解决方案，使用网络分析来跟踪资金来往和流向，确定可能的诈骗模式。

银行必须看清这样一个现实：虽说伪造身份诈骗者占总客户群的比例很小，但会带来严重的信贷损失。

金融机构是时候使用实体解析和网络分析等方法来制定防御计划了，这样他们就可以有效对抗伪造身份诈骗。

原文名称	How to stay ahead of the rise of synthetic fraud
作者简介	伊万·赫德（Ivan Heard），是 Quantexa 欺诈解决方案全球负责人 。
原文信息	2021 年 03 月 22 日发布于 Help Net Security 原文地址 https://www.helpnetsecurity.com/2021/03/22/synthetic-fraud/
摘 要	近年来，银行在减少银行卡诈骗方面取得了一些成功，但是，一种新的诈骗日益严重，这就是“伪造身份诈骗”。在数字平台上，金融犯罪分子将真实和伪造的信息相整合，以执行此类诈骗，而且未被追责。
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。