安天智甲有效防护 Venus 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 Venus 的勒索软件。该勒索软件最早被发现于 2021 年 5 月，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 Venus 勒索软件的加密行为。

Venus 勒索软件运行后结束特定数据库进程和 office 进程，在注册表路径 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run 下添加启动项，以实现开机自启动。创建名为 "R/ZSAciB3QDoYngFEx0p6WPFNbA=" 的互斥体保证单实例运行。向 franavru.xyz 域名发出请求建立连接以实现数据回传，通过 ARP 广播查找内网中其他存在的主机，利用网络共享向其他内网中的主机传播勒索软件。在含有被加密文件的目录下创建“README.txt”勒索信文件并修改用户桌面背景告知受害者已被勒索，需要通过邮箱（getdecrypt@disroot.org）与攻击者联系以获取具体勒索需求，无其他联系方式。随后遍历磁盘对特定后缀名的文档、压缩包、图片、音视频等文件进行加密，采用的加密策略为使用随机 AES 密钥加密文件，并追加文件名后缀 ".venus"；使用 RSA 非对称加密算法加密 AES 密钥。删除系统卷影，删除备份和禁用修复功能，以防止恢复被加密文件。

▲Venus 勒索软件勒索信息

Venus 勒索软件采用“AES+RSA”加密算法组合的形式加密文件，目前被加密的文件暂时无法解密。

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、动态(Win7sp1 x86)鉴定器、字符串分析鉴定器、文件相似分析鉴定器、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(WinXP)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、动态行为鉴定器将文件判定为木马程序。

◆概要信息

文件名	9aa3cc9d7c641ea22cfa3e5233e13c94
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	137 KB
MD5	9AA3CC9D7C641EA22CFA3E5233E13C94
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Filecoder
判定依据	反病毒引擎

报告地址：https://1.119.163.6/vue/details?hash=9AA3CC9D7C641EA22CFA3E5233E13C94

◆运行环境

操作系统	内置软件
Win7sp1 x86 旗舰版 service Pack 1	默 认、IE8、Google Chrome、Firefox、Office2013、Flash、FoxitReader、Adobe Reader DC

◆危险行为

行为描述	危险等级
在系统目录创建文件	★★★
自启动	★★★

◆常见行为

行为描述	危险等级
读取自身	★★
创建可执行文件	★★
释放 PE 文件	★★
获取系统版本	★
.....	.....

◆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 07 月 12 日 (总第 286 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

“苦象”组织上半年针对我国的攻击活动分析

概述

近期，安天 CERT 在梳理安全事件时，发现一批针对我国军工、贸易和能源等领域的网络攻击活动。攻击手法存在伪造身份向目标发送鱼叉邮件，投递恶意附件诱导受害者运行。经归因分析发现，这批活动具备 APT 组织“苦象”[1] 的历史特征，且在针对目标、恶意代码和网络资产等层面均存在关联，属于“苦象”组织在 2021 年上半年的典型攻击模式。相关攻击活动的特征总结如下：

事件要点	特征内容
事件概述	“苦象”组织的网络攻击活动
攻击目标	我国的军工、贸易和能源等领域目标
攻击手法	鱼叉邮件投递恶意附件，附件包含恶意 CHM 文件诱导点击
攻击意图	窃密
攻击时间	2021 年 4 月

▲ 攻击活动特征

此外，安天 CERT 还跟踪、关联到“苦象”组织上半年使用过的多个窃密插件，其攻击技术和代码功能均带有该组织的明显特征，在关联分析章节我们将对 asms 和 sthost 两个典型插件进行分析。

事件分析

1. 初始诱饵分析

攻击者会以“会议议程”等邮件主题，伪造受害者可能感兴趣的发件人向目标连续投递多封鱼叉邮件，邮件附件中包含恶意的 CHM 文件。

病毒名称	Trojan/Script.CHM
原始文件名	会议议程 .chm
MD5	D91B888205AC1CA80C40426B9F5A6105
文件大小	10.60 KB (10856 bytes)
文件格式	MS Windows HtmlHelp Data
LanguageCode	English (U.S.)

▲ 样本标签

“会议议程 .chm”为包含恶意脚本的 Windows 帮助文件，静态属性皆不可用，点击执行后看到的正文为空白：

▲ CHM 文件的正文及属性

此刻，其含有的经混淆的恶意脚本被自动运行，作用是添加一个每 15 分钟运行一次的系统任务计划。（原文链接：https://mp.weixin.qq.com/s/dHiYZyJXoy2LLXtFlcYeog）

扫描右侧二维码阅读全文

安天亮相 2021 中国国际金融信创专题展

2021 年 7 月 2 日，由中国人民银行科技司指导，中国金融电子化公司主办的金融行业高端品牌展会——中国国际金融展在京举办。本次展会围绕“聚力金融信创 筑牢数字新基建”主题，来自京津冀地区的近 300 位金融监管机构和金融机构代表参观参会，大家齐聚一堂，以产品展示、技术交流、经验分享等方式，致力于共同推动金融信创工作的高质量开展，合力构建互促互进、协同创新的产业发展体系。

安天作为引领威胁检测与防御能力发展的网络安全“民企国家队”，有长达 21 年威胁对抗核心技术体系和产品积累。安天坚持核心技术自主创新，产品和解决方案保障客户关键数据资产安全和业务运行连续性，为客户数字化转型保驾护航。

人民银行范一飞副行长指出金融业关键信息基础设施国产化工作重要性体现在：一是提升自主可控水平，振兴民族产业的必由之路；二是维护金融安全的必然选择；三是助力国产技术赶超的重要途经。安天未来将持续坚持技术自主创新，致力于赋能金融领域，推动金融核心业务信创进程，促进金融业以信息技术为引领，加快数字化转型、流程再造和产品服务创新，为进一步推动和保障金融信创安全贡献自己的力量。（原文链接：https://mp.weixin.qq.com/s/2DEOWvNZt0swrRhatpDt7Q）

▲ 安天高级副总裁高宏向中国银行科技部负责人讲解安天产品

扫描右侧二维码阅读全文

“2021 年中国网络安全年会”即将开幕 安天参与主办

7 月 20 日，“2021 年中国网络安全年会”即将在线上线下同期举办，本届年会在国家互联网信息办公室指导下，由国家互联网应急中心（CNCERT/CC）主办，安天科技集团股份有限公司、深信服科技股份有限公司、绿盟科技集团股份有限公司、恒安嘉新（北京）科技股份公司、杭州安恒信息技术股份有限公司、奇安信科技集团股份有限公司、长安通信科技有限责任公司、中国电信集团系统集成有限责任公司、阿里云计算有限公司、北京鸿腾智能科技有限公司（360 政企安全集团）、天融信科技集团、启明星辰信息技术集团股份有限公司、亚信安全科技股份有限公司联合主办。新华网、中国通信学会协办。（原文链接：https://mp.weixin.qq.com/s/Com0h3w9uVhoKnuYseHiIw）

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	安全厂商发布针对 APT36 组织基础设施的分析
英文标题	Transparent Tribe APT Infrastructure Mapping
作者	Joshua Picolet
内容概述	Team Cymru 安全团队发布了针对 APT36（Transparent Tribe）组织远程访问工具 CrimsonRAT 基础设施的分析。CrimsonRAT 的基础设施主要托管在越南 VPS 经销商 Pi NET LLC 租用的基础设施上。研究人员在 17 台 C2 服务器上观察到了 RDP 证书。CrimsonRAT C2 服务器在建立初始 TCP 连接时提供标准化响应。研究人员还观察到潜在的交叉登录活动，APT36 将多个 C2 服务器链接在一起，并提供一个到 AhMyth AndroidRAT 的链接。
链接地址	https://team-cymru.com/blog/2021/07/02/transparent-tribe-apt-infrastructure-mapping-2/

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 Windows Print Spooler 远程代码执行漏洞（CVE-2021-34527）	高	Microsoft Windows Print Spooler 存在远程代码执行漏洞。由于 RpcAddPrinterDriverEx() 函数中的输入验证不正确。远程用户可以向 Windows Print Spooler 发送特制的请求并使用 SYSTEM 权限执行任意代码。
	Microsoft Paint 3D 远程代码执行漏洞（CVE-2021-31945）	高	Microsoft Paint 3D 存在远程代码执行漏洞。由于 Paint 3D 在解析 GLB 文件时存在边界条件，使得攻击者可以创建一个特制的 GLB 文件，诱使受害者打开它，触发越界读取错误并执行任意代码。
	Microsoft Excel 远程代码执行漏洞（Microsoft Excel）	高	Microsoft Excel 存在远程代码执行漏洞。由于处理 Excel 文件时的 use-after-free 错误，使得攻击者可以创建一个特制的 Excel 文件，诱使受害者打开它，触发 use-after-free 错误并在系统上执行任意代码。
较为活跃样本家族	Trojan[Bacodoor]/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/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.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.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/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/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其他正常应用，运行后隐藏图标，并访问某些网站，旨在提高网络访问流量，消耗用户流量资费。

企业如何确保其供应链的安全

凯文·里德 / 文 安天技术公益翻译组 / 译

自 SolarWinds 供应链攻击事件发生以来，人们越来越关注各种规模的组织如何确保其供应商的安全。无论是大型还是小型组织，都已沦为供应链攻击的受害者。美国财政部和国土安全部也受到了 SolarWinds 攻击的影响——即使他们拥有政府资源和资金，也需要应对供应链攻击问题。

现实情况是，供应链攻击不会消失。在 2021 年第一季度，有 137 家组织报告称他们受 27 家第三方供应商的影响遭到了供应链攻击。供应链攻击的数量比上一季度增长了 42%。

这就引发了一个问题：随着供应链攻击威胁日益严重，企业该如何降低此类风险呢？

评估供应商风险的十个最佳实践

虽说我们不能保证在供应链攻击发生之前检测到它，但是我们可以考虑采用下述十个最佳实践，来降低风险并验证供应链的安全性。

1. 评估“如果供应商的 IT 基础设施受到损害，会对企业造成什么影响”。全面的风险评估是首选，不过较小的企业可能没有资源进行全面评估。但是，他们至少应分析最坏的情况并考虑以下问题：

（1）如果供应商的系统遭到勒索软件攻击，企业会受到什么影响？

（2）如果供应商的源代码被木马病毒破坏，企业会受到什么影响？

（3）如果供应商的数据库遭到攻击且数据被盗，企业会受到什么影响？

2. 评估每个供应商的内部 IT 资源和能力。他们是否设有由安全经理或 CISO 领导的网络安全团队？确定供应商的安全领导很重要，因为安全领导能够回答你的问题。如果供应商未设立这样的团队，或者其团队人力不足（没有安全领导），企业应重新考虑是否要与该供应商合作。

3. 与供应商的安全经理或 CISO 会面，了解他们如何保护其系统和数据。这可以是简短的会议、电话，甚至是电子邮件交谈，具体取决于步骤 1 中确定的风险。

4. 要求供应商提供证据，来验证其主张。在这方面，渗透报告是一种有用的方法。企业应确保测试的范围是适当的；如果可以，应让供应商提供两次连续测试的报告，以验证其是否根据发现的情况采取行动。

5. 如果是软件供应商，企业应要求进行独立的源代码审查。在某些情况下，供应商可能会要求企业签订保密协议（NDA），然后再与企业共享完整的审查报告；也可能不与企业共享完整报告。如果供应商不与企业共享完整报告，企业可要求其提供执行摘要。

6. 如果是云供应商，企业可以扫描供应商的网络，执行 Shodan 搜索，或要求供应商提供其自己的扫描报告。如果企业打算自己进行扫描，请从供应商处获得许可，并要求他们将客户地址与他们自己的地址分开，这样企业就不会扫描到不相关的内容。

7. 如果是软件或云供应商，企业应查明供应商是否在运行漏洞赏金计划。这些计划可帮助组织在攻击者利用漏洞之前找到并修复漏洞。

8. 询问供应商如何确定风险的优先级。例如，通用漏洞评分系统（CVSS）是一种免费、开放的行业标准，用于评估计算机系统安全漏洞的严重性并评分，以便供应商可以按优先级进行响应。

9. 要求供应商提供漏洞修复报告。如果供应商有此类报告，说明他们对安全和管理漏洞是重视的。如果可能，企业应获取由独立实体编制的报告。

10. 步骤 1 到 9 应每年执行一次，具体取决于供应商对企业的风险和影响。对于影响较小的供应商，上述步骤的执行频率可以低一些。对于对企业成功至关重要且具有高风险的供应商，企业应制定永久性的评估流程。但是，大型 SaaS 和 IaaS 提供商可能不愿意参与评估。

结论

通过采取上述最佳实践，企业可以识别与特定供应商相关的风险，了解供应商如何管理这些风险，并收集供应商如何减轻这些风险的证据。根据这些证据和风险偏好，企业可明智地决定是否与该供应商合作。最后，当执行评估时，应保持一致性并寻找随时间变化的风险。

企业应注意，他们无法保证阻止供应链攻击。但是，通过采用下一代反病毒软件来保护企业环境，对用户进行持续的网络安全培训，并遵循上述最佳实践，可以减轻企业的风险。

原文名称	How can a business ensure the security of their supply chain?
作者简介	凯文·里德（Kevin Reed），是 Acronis 公司的首席信息安全官。
原文信息	2021 年 7 月 6 日发布于 Help Net Security 原文地址 https://www.helpnetsecurity.com/2021/07/06/security-supply-chain/
摘 要	通过采取本文所述的最佳实践，企业可以识别与特定供应商相关的风险，了解供应商如何管理这些风险，并收集供应商如何减轻这些风险的证据。根据这些证据和风险偏好，企业可明智地决定是否与该供应商合作。企业应注意，他们无法保证阻止供应链攻击。但是，通过采用下一代反病毒软件来保护企业环境，对用户进行持续的网络安全培训，并遵循上述最佳实践，可以减轻企业的风险。
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。