# 安天发布《Velar 勒索软件分析报告》

近日，安天 CERT 在梳理网络安全事件时发现一个名为 Velar 的勒索软件，Velar 勒索软件最早于 2020 年 3 月被发现，主要通过钓鱼邮件进行传播。

Velar 勒索软件执行后，加密计算机上的重要文件，在原文件名后追加名为“.Velar”的后缀，在计算机所有目录下创建名为“readme.txt”的勒索信，勒索信内容包含勒索说明、联系方式和 USER_ID 等。虽然攻击者并没有在勒索信中说明支付方式和赎金金额，但数据表明攻击者通常要求以比特币或任何其他数字货币支付 200 至 1500 美元的赎金。Velar 勒索软件使用“AES+RSA”加密算法加密文件，调用命令行命令来防止受害者恢复已加密的文件，具体操作为删除卷影副本。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，避免一切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口令；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病毒的鉴定；安天智甲已经实现了对该勒索病毒的查杀。

## 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，下为其自动形成的分析报告：

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、关联分析鉴定器、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（WinXP）鉴定器、字符串分析鉴定器、来源信息鉴定器、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 x86）鉴定器等鉴定分析。

最终依据关联分析鉴定器、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 | 106017ca2da2422722ecff4ce1fa74454f7964c0e4b5b45eacff97ec0b34903c |
| 文件类型 | BinExecute/Microsoft.EXE[:X86] |
| 大小 | 506 KB |
| MD5 | 4482844622C6CC5027927A856E8BAD57 |
| 病毒类型 | 木马程序 |
| 恶意判定 / 病毒名称 | Trojan/Win32.Wacatac |
| 判定依据 | 反病毒引擎 |

◆ 操作系统

| 操作系统 | 内置软件 |
|---|---|
| Win7 x86 6.1.7600 Build 7600 | 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 |
|---|---|
| 删除全盘所有卷影副本 | ★★★★ |

◆常见行为

| 行为描述 | 危险等级 |
|---|---|
| 加载运行时 DLL | ★ |
| 枚举进程 | ★ |
| 访问文件尾部 | ★ |
| 创建挂起进程 | ★★ |
| 文档篡改 | ★★ |
| 获取系统版本 | ★ |

◆进程监控

| PID | 创建 | 命令行 |
|---|---|---|
| 2156 | target.exe | "c:\222294fcd0e64302a58a25ae545f771e\share\target.exe" |
| 2244 | vssadmin.exe | vssadmin delete shadows /all /quiet |

◆完整报告地址



安天周观察
安天官方微博 安天官方微信
主办：安天 2020 年 4 月 13 日（总第 226 期）试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

# 针对 WannaRen 勒索软件的梳理与分析

## 概述

近日，安天 CERT 监测到国内多个论坛，贴吧等网站先后有受害者感染新型 WannaRen 勒索软件并进行求助，其名称与“WannaCry”相似，加密后会追加“.WannaRen”后缀名。

安天 CERT 捕获了近期关注度较高的 WannaRen 勒索软件样本，对该威胁事件进行梳理与分析，目前监测到该勒索软件通过 KMS 工具捆绑 PowerShell 脚本传播，同时下载另一个 PowerShell 脚本作为载体，下载相关模块文件，其中包括名为“you”的核心加密文件、“WINWORD.exe”白文件和“wwlib.dll”恶意 DLL 文件，使用白文件加载恶意 DLL 文件（俗称白 + 黑技术）来躲避查杀。勒索信中内容为繁体字，并要求受害者支付赎金完成解密，赎金价格为 0.05BTC（约 2500 元人民币）。目前，被加密的文件在未得到密钥前暂时无法解密。

前导 PowerShell 脚本除 WannaRen 核心模块下载链接外，还存在其他多个链接，其中包括永恒之蓝传播模块、挖矿模块。通过安天监测分析，该勒索软件没有大规模传播，没有发现内网传播案例。勒索信中的比特币地址收到两笔入账，约为 0.00009490 比特币。经验证，安天智甲终端防御系统（简称 IEP）可有效阻止 WannaRen 勒索软件运行过程加密操作，针对勒索软件实体有效防护。

## 该勒索软件对应 ATT&CK 的映射图谱

该勒索软件技术特点分布图：

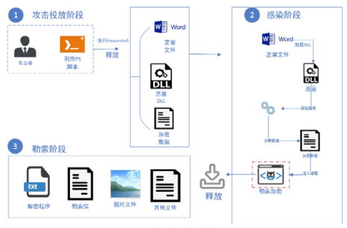
▲该勒索软件技术特点的 ATT&CK 的映射

（见该勒索软件技术特点的 ATT&CK 的映射）

## WannaRen 勒索软件概览

●执行流程

攻击者入侵计算机后，使用 PowerShell 脚本下载白文件、DLL 文件和加密的代码文件。攻击者利用 DLL 劫持技术，将文件“WINWORD.exe”设置为服务并开机启动，启动后优先加载同目录下的加密程序“wwlib.dll”。DLL 文件加载了核心加密文件“you”，加密 Windows 系统中大部分文件类型，在 C:\User\Public 目录下释放名为“fm”的文件（内容为记录加密时间），并在桌面释放“团队解密 .jpg”、“想解密请看此文本 .gif”、“想解密请看此文本 .txt”、“@WannaRen@.exe”等文件。




▲攻击流程

●信息概览


▲ WannaRen 勒索软件概览

## 样本 ++ 分析

●样本标签

| | |
|---|---|
| 恶意代码名称 | Trojan/Win32.WannaRen |
| 原始文件名 | @WannaRen@.exe |
| MD5 | 1DE73F49DB23CF5CC6E06F47767F7FDA |
| 文件大小 | 6.96 MB (7,299,072 字节) |
| 文件格式 | BinExecute/Microsoft.EXE[:X86] |
| 时间戳 | 2020 03 31 17:14:53 |
| 数字签名 | 无 |
| 加壳类型 | VMProtect v3.00 - 3.1.2 |
| VT 首次上传时间 | 2020-04-05 15:35:41 |
| VT 检测结果 | 53 /72 |

▲ WannaRen 解密程序

● WannaRen 加密程序的运行流程

PowerShell 脚本将 WINWORD.exe 和 wwlib.dll 文件下载到指定目录下，采用白文件加载黑 DLL 文件方式，利用 WINWORD.exe 的运行机制，优先加载同目录下的恶意 wwlib.dll 文件。

勒索软件核心文件 wwlib.dll 与正常的 wwlib.dll 对比，正常的文件带数字签名，且两个文件大小差异较大。

wwlib.dll 文件加载后将 WINWORD.exe 添加为服务。

服务启动后，DLL 文件读取 C\User\Public 路径下文件名为 you 的加密数据，读取后进行加密文件操作。

通过对“you”文件在内存中解密后，发现有字符串信息、RSA 公钥信息和文件时间戳。

样本运行后在本机释放多个文件，其中包括 fm 文件（记录攻击时间）、团队解密 .jpg（攻击者证明其拥有一个解密团

（下转第三版）

## 每周安全事件

| 类 型 | 内 容 |
|---|---|
| 中文标题 | Berkine 石油公司遭到 Maze 勒索软件攻击 |
| 英文标题 | Maze ransomware group hacks oil giant; leaks data online |
| 作者及单位 | Deeba Ahmed |
| 内容概述 | 在 2020 年 4 月 1 日，Berkine 成为了臭名昭著的迷宫勒索软件组织网络攻击的受害者，攻击者设法窃取了整个数据库，其中包含超过 500MB 的机密文档，涉及预算、组织策略、生产数量和类似的敏感数据。泄露的数据包括 Berkine 集团的每桶油成本价格，2020 年的组织目标，以及分配给 Berkine 的两个所有者的各种任务的预算。该数据库还包含一个 Berkine 雇员的列表，包括他们的联系方式和其中一些人的旅行证件。 |
| 链接地址 | https://www.hackread.com/maze-ransomware-group-hacks-oil-giant-leaks-data/ |

## 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 8 个移动平台恶意代码和 6 个 PC 平台的恶意代码和漏洞值得关注

| 恶意代码类别 | 名称与发现时间 | 威胁等级 | 简要描述 |
|---|---|---|---|
| 移动恶意代码 | 新出现的样本家族 | Trojan/Android.FakeApp.ib[prv,rmt,fra] 2020-04-06 | 高 | 该应用程序伪装成 Paritex 程序，激活设备管理器防卸载，接受 firebase 指令，通过获取通知来获取手机邮箱信息，短信信息，窃取用户输入的邮箱和密码，造成用户隐私泄露，建议卸载。 |
| | | Trojan/Android.Homeproxy.a[exp] 2020-04-07 | 中 | 该应用程序运行后隐藏图标，把用户手机变为代理，重定向访问其他网址，导致用户资费消耗，警惕其造成用户的隐私泄露，建议卸载。 |
| | | Trojan/Android.SmsThief.ch[prv] 2020-04-08 | 中 | 该应用程序伪装成系统应用，隐藏桌面图标，窃取用户信箱信息和位置信息并上传，造成用户隐私泄露，请卸载。 |
| | 较为活跃样本 | Trojan/Android.cashnow.a[prv,spy] | 中 | 该应用程序伪装成系统应用，运行会隐藏图标，联网上传短信、通讯录、通话记录、位置信息等隐私信息，另外还会上传 WhatsApp、Facebook、telegram 等社交应用的图片音频等数据信息，造成用户隐私泄露，建议卸载。 |
| | | Trojan/Android.CallMonitor.a[prv] | 中 | 该应用程序安装无图标，运行将来电号码、去电号码、收件箱号码和发件箱号码以短信的形式发送至指定号码，造成用户隐私泄露，建议卸载。 |
| | | Trojan/Android.SpyLoan.c[prv,rmt,spy] | 中 | 该应用程序包含恶意代码，接受远程指令，上传用户短信、联系人、通话记录等隐私信息，造成用户隐私泄露，建议卸载。 |
| | | RiskWare/Android.Daikuan.x[rog] | 低 | 该应用程序运行后访问第三方网贷网站，可能没有财产权益保障，会造成用户财产损失，请谨慎使用。 |
| | | RiskWare/Android.PJbocai.ao[rog] | 低 | 该应用程序为博彩类应用，会给您带来财产损失。此类程序一般以欺骗形式引诱推荐安装，是一种典型的网络赌博诈骗手段，请立即卸载。 |
| PC 平台恶意代码 | 活跃的格式文档漏洞、0day 漏洞 | Media Foundation 内存损坏漏洞（CVE-2020-0801） | 高 | 当 Windows Media Foundation 不正确地处理内存中对象时，会触发内存损坏漏洞。成功利用此漏洞的攻击者可以安装程序；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。攻击者可能通过多种方式利用此漏洞，包括诱使用户打开经特殊设计的文档或诱使用户访问恶意网页。 |
| | 较为活跃样本 | Trojan[Dropper]/Win32.ZAccess | 中 | 此威胁是一种具有带有捆绑功能的木马类程序。该家族可以在被感染计算机上下载其它恶意程序，形成僵尸网络以进行比特币挖掘和欺诈等恶意活动，并利用先进的 rootkit 技术隐藏自身。 |
| | | Trojan[Backdoor]/Win32.Nbdd | 中 | 此威胁是一种带有后门的木马类程序。该家族会在系统中创建后门，允许其他恶意软件进入系统修改注册表并破坏系统文件。该家族会将用户个人信息泄露给黑客。该家族可以通过可移动设备、恶意链接、垃圾邮件附件及其他恶意软件等进行传播。 |
| | | Trojan[Packed]/Win32.TDSS | 中 | 此威胁是一种加壳的木马类程序。该家族会利用漏洞等缺陷在用户计算机上开启后门的服务端，操纵者通过客户端来操作用户计算机，从而获得用户计算机的控制权。 |
| | | GrayWare[AdWare]/Win32.EZula | 低 | 此威胁是一种恶意广告类程序。它在未经用户同意下发送免费优惠券、免费软件 / 共享应用程序，网络游戏等广告。占用系统资源，影响用户使用。 |
| | | GrayWare[AdWare]/Win32.Gaba | 低 | 此威胁是一种可以推送广告的灰色软件家族。主要通过捆绑于其他软件的安装文件中进行传播，在安装时一般不告知用户其存在，在安装进系统后，以弹窗等方式进行广告。软件制作者可以在黑市上出卖广告以获利。 |



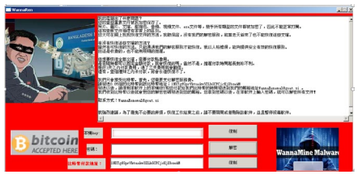
（上接第一版）

队，实则为取自网络的境外某部队培训图片）、勒索信、@WannaRen@.exe（解密程序）。

加密后的文件有如下特点，以“WannaRenkey”字符串开头，“WannaRen2”字符串进行结尾。

### ● WannaRen 解密程序测试

之前网络大量传播的勒索样本，实则为攻击者声称的解密程序。该程序运行后弹窗，如下图所示：




▲弹窗显示

通过测试发现，该解密程序从同一目录下的勒索信中读取 KEY 到解密程序中。

输入任意密码均可弹出“解密完成”对话框，但实则并没有解密。应为解密程序的 BUG，或者是根本没有解密的途径。

### ●比特币交易记录

勒索信中的比特币地址为：1NXTgfGprVktuokv3ZLhGCPCjcKjXbswAM，截至本报告发布时，该比特币钱包显示两笔入账记录。

### ●关联分析

安天 CERT 通过关联发现可疑脚本，该 PowerShell 脚本功能为下载 WannaRen 勒索软件，经分析该脚本为本次攻击事件的前导文件。

目前该脚本除了存在 WannaRen 核心模块外，还存在其他多个链接，多个文件功能如下表所示，其中包括永恒之蓝传播模块，攻击者可以自由选择下载，目前安天并未监控到存在内网大规模传播现象。

| 目前链接的部分样本 MD5 | 功能 |
|---|---|
| 124D75D7214A16635828982C6C24B8D2 | 永恒之蓝模块 |
| 39E5B7E7A52C4F6F86F086298950C6B8 | 挖矿木马 |
| 9F09350FE69026571A9869E352E2C2BC | 后门 |
| CA8AB64CDA1205F0993A84BC76AD894A | 挖矿木马 |

▲下载的功能模块

经过关联发现该 PowerShell 脚本是从域名 cs.sslsngyl90.com 下载，该域名会重定向至如下链接：

cpu.sslsngyl90.com/vip.txt

经安天威胁情报综合分析平台关联分析域名 sslsngyl90.com，发现该域名与匿影组织存在关联，此前该组织一直进行挖矿攻击，近期较为活跃。


▲安天威胁情报综合分析平台关联分析

目前，该链接中的脚本删除了勒索软件模块，只保留了挖矿模块，故现在没有大规模传播。

### ●传播分析

安天监测到该样本通过 KMS 工具捆绑 PowerShell 脚本传播，首先攻击者将伪装成激活工具 KMS 的下载器上传到某网站。

该下载器运行后，下载伪装成激活工具 KMS 的压缩包。

解压后，是一个伪装成激活工具 KMS 的程序，其中嵌入 PowerShell 代码。

解码后的 PowerShell 代码如下，具体功能为延迟 2000 秒，检查系统中是否存在 360 安全防护或 QQ 防护，存在则退出 PowerShell 进程，若不存在则创建下载勒索软件的 PowerShell 脚本的任务计划。

▲解码后的 PowerShell

将上图中加密后的代码解码，得到以下命令，其功能为下载并执行上一节提到的前导文件。

▲下载命令

### 防护建议

安天提醒广大用户，提高网络安全意识，及时进行系统更新和漏洞修复，避免下载非正版的应用软件、非官方游戏及注册机等；安装具有主动防御能力的终端防护软件（如安天智甲）以对勒索软件提供有效防护；及时备份重要文件，文件备份应与主机隔离；尽量避免打开社交媒体分享的不明来源链接，将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口令；接收邮件时要确认发送来源是否可靠，避免打开可疑邮件中的网址和附件，避免轻易下载来源不明的附件。

目前，安天智甲终端防御系统可实现对以上恶意软件的查杀与有效防护。


▲安天智甲有效防护

### 附录：IoCs

| IoCs |
|---|
| F96EB8A988E3739570CA8DBB55026965 |
| 9854723BF668C0303A966F2C282F72EA |
| 2D843372218E87A7E99245BD8B53D6EAB |
| 6355D278E4B9CAEC1F9774DB5D2C54AA |
| 06F61B51FD1B4834AA2C72A0C2E3573E |
| 90D3BC2AB0B39A17A29462F3372CA786 |
| 1DE73F49DB23CF5CC6E06F47767F7FDA |
| 235CCA78C8765FCB5CF70A77B1AE9D02 |
| 46A9F6E33810AD41615B40C26350EED8 |
| F96EB8A988E3739570CA8DBB55026965 |
| 124D75D7214A16635828982C6C24B8D2 |
| 1976D15199E5F0A8FB6C885DF9129F56 |
| 39E5B7E7A52C4F6F86F086298950C6B8 |
| 9F09350FE69026571A9869E352E2C2BC |
| CA8AB64CDA1205F0993A84BC76AD894A |
| 84DB24EF0BF045D100C200D608204600 |
| DAA1DC4AA5D91EF3FA200B5890490007A |
| img.vim-cn.com |
| sslsngyl90.com |

4 月 9 日，WannaRen 作者已经释放该勒索软件解密密钥，安天 CERT 第一时间进行测试验证确认该密钥有效。

以上内容为精简版
微信扫描二维码阅读全文