安天发布《Prolock 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 Prolock 的勒索软件变种，Prolock 勒索软件最早于 2020 年 3 月被发现，主要通过 RDP 爆破进行传播。

Prolock 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“.proLock”的后缀，在计算机所有目录下创建名为“[HOW TO RECOVER FILES].TXT”的勒索信，勒索信内容包含勒索说明和交付赎金的方法。ProLock 勒索软件嵌入一个名为“WinMgr.bmp”的 BMP 图像中，通过 PowerShell 脚本直接注入内存中运行。ProLock 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。

安天于 3 月初发现一个名为 PwndLocker 的勒索软件，由于存在缺陷，被加密的文件存在恢复的可能。目前攻击者已修复了之前版本的缺陷并将其后缀名更改为“.proLock”，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、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（WinXP）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 x86）鉴定器等鉴定分析。

最终依据 BD 静态分析鉴定器、反病毒引擎鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	dfbd62a3d1b239601e17a5533e5cef53036647901f3fb72be76d92063e279178
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	15 KB
MD5	3355ACE345E98406BDB331CCAD568386
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.DelShad
判定依据	反病毒引擎

◆危险行为

行为描述	危险等级
检测虚拟机	★★★★★
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	★
获取驱动器类型	★
访问文件尾部	★
文档篡改	★★

◆ UDP 信息

源 IP	源端口	目的 IP	目的端口
0.0.0.0	68	255.255.255.255	67
192.168.122.1	67	192.168.122.111	68
192.168.122.61	138	192.168.122.111	138
192.168.122.111	138	192.168.122.255	138
192.168.122.111	137	192.168.122.61	137
192.168.122.111	137	192.168.122.255	137

◆ TCP 信息

源 IP	源端口	目的 IP	目的端口
192.168.122.111	1352	192.168.122.61	139

◆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 6 日 (总第 225 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

传播 CoronaVirus 勒索软件和 KPOT 窃密木马事件的分析

概述

近日，安天 CERT 发现利用钓鱼网站传播 CoronaVirus 勒索软件和 KPOT 窃密木马的威胁事件。攻击者通过伪造钓鱼网站传播窃密木马下载器，该下载器执行后，从服务器下载 CoronaVirus 勒索软件和 KPOT 窃密木马两个恶意代码。CoronaVirus 勒索软件最早出现于 2020 年 3 月初，使用“RSA+AES”算法加密文件，并创建名为“CoronaVirus.txt”的勒索信，勒索金额为 0.008 比特币（约 50 美元），该勒索软件执行后重启用户计算机，并锁定屏幕一段时间，导致用户无法进行任何操作。KPOT 窃密木马是一种窃取信息的恶意软件，该窃密木马旨在窃取浏览器、即时通信软件、电子邮箱、VPN、RDP、FTP 等凭证信息。安天 CERT 曾在 2019 年针对该木马进行过详细分析。

安天 CERT 通过以上恶意样本的运行流程及特点，判断本次事件是利用钓鱼网站作为诱饵，使用文件名为 CoronaVirus（冠状病毒的英文）的勒索软件进行掩护，在勒索软件加密的过程中窃取信息。通常勒索软件在加密过程中消耗的时间较长，而 KPOT 窃密木马完成窃密任务的时间较短，勒索软件加密完成后重启用户计算机并锁定屏幕一段时间，避免用户修改凭证信息，保证攻击者有一定的时间转移窃取的信息。

大多数勒索软件加密文件，以恢复文件要求用户交付赎金为目的，如果用户不交付赎金，部分攻击者以公布窃取的文件威胁用户交付赎金。但在本次攻击活动中，攻击者将勒索软件和窃密木马相结合，以加密文件的形式做掩护，收集用户的凭证信息。从中可以看出，窃密的攻击组织正尝试在原有的攻击流程中加入勒索软件以加强攻击行动的隐蔽性，提高取证溯源的成本。安天 CERT 建议感染勒索软件的用户及时修改凭证信息，避免造成网络财产被盗或隐私信息外泄等后果。

经验证，安天智甲终端防御系统（简称 IEP）可实现对 KPOT 窃密木马和 CoronaVirus 勒索软件的查杀与有效防护。

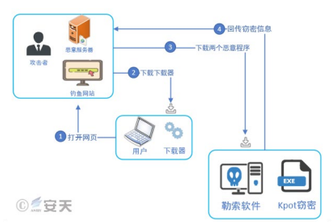
该起事件对应 ATT&CK 的映射图谱

该起事件技术特点分布图：

▲该起事件技术特点的 ATT&CK 的映射

样本传播与运行流程梳理

攻击者通过搭建钓鱼网站（wisecleaner.best），诱导受害者点击下载链接，下载恶意下载器。该恶意下载器运行后，连接恶意服务器（tryndа.xyz）下载并运行 KPOT 窃密木马和勒索软件 CoronaVirus，KPOT 窃密木马执行后窃取口令、Cookie、加密货币钱包等重要信息，并将信息回传至远程服务器。



▲运行流程

经关联分析，该钓鱼网站仿冒 wisecleaner.com 网站（Windows 系统清理优化工具），目前该钓鱼网站已无法访问。

通过对域名以及样本的更新和创建时间发现，该起攻击事件是近期展开的攻击活动。

样本/域名	时间戳/域名更新时间
CB2B4CD74C7B57A12BD822A168E4E608	2020-03-08
99785AE0679D6D3E27DE83AF403C23B0	2020-03-08
Wisecleaner.best	2020-03-14
tryndа.xyz	2020-03-06

▲样本和域名的创建或更新时间

样本分析

1. 下载器样本分析

●样本标签

病毒名称	Trojan/Win32.Zenpak
原始文件名	WSHSetup.exe
MD5	CB2B4CD74C7B57A12BD822A168E4E608
文件格式	BinExecute/Microsoft.EXE[:X86]
文件大小	898.00 KB (919,552 bytes)
时间戳	2020-03-08 9:21:22
数字签名	无
加壳类型	无
编译语言	Microsoft Visual C++
VT 首次上传时间	2020-03-11 18:22:33
VT 检测结果	52 / 71

▲下载器木马

●样本行为

下载器运行后，连接恶意域名 tryndа.xyz，下载并运行 2 个可执行文件 file1 和 file2，file1 是 KPOT 窃密木马，file2 是 CoronaVirus 勒索软件。

url	备注
http://tryndz.xyz/file1.exe	KPOT 窃密木马
http://tryndz.xyz/file2.exe	CoronaVirus 勒索软件
http://tryndz.xyz/WSHSetup.exe	下载器

▲关联的下载地址

2. 下载样本一：KPOT 窃密木马

●样本行为

KPOT 是一种信息窃取类型的恶意软件，该窃密木马旨在窃取浏览器、即时通信软件、电子邮箱、VPN、RDP、

（下转第三版）

每周安全事件

类 型	内 容
中文标题	FBI 警告多个行业感染 Kwampirs 恶意软件
英文标题	FBI Warns of 'Kwampirs' Malware Supply Chain Attacks
作者及单位	Marianne Kolbasuk McGee
内容概述	FBI 称，Kwampirs RAT 是一种模块化 RAT 蠕虫，它可以获取对受害机器和网络的系统访问权限，其主要目的是获得对受害公司的广泛但有针对性的访问权限，以进行后续的计算机网络利用活动。通过对受害者的调查和取证分析，FBI 发现，在美国、欧洲、亚洲和中东地区，医疗保健、软件供应链、能源和工程等行业都是重点针对目标。
链接地址	https://www.bankinfosecurity.com/fbi-warns-kwampirs-malware-supply-chain-attacks-a-14037

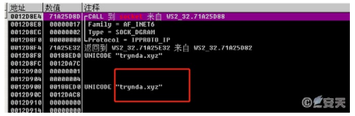
每周值得关注的恶意代码和漏洞信息

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

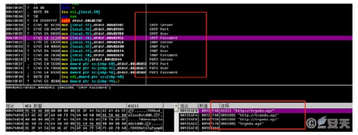
恶意代码类别		名称与发现时间	威胁等级	简要描述
移动恶意代码	新出现的样本家族	Trojan/Android.Femas.b[prv,fra,spy] 2020-03-30	高	该应用程序伪装为其他应用，运行隐藏图标，通过 tcp 连接到服务器，上传用户手机号码、固件信息、装机应用列表等隐私，包含执行下载文件、加载未知 dex 的风险代码。可能进一步获取用户短信、联系人、通话记录、地理位置、照片等隐私，私自执行录音、拍照等操作，会造成用户隐私泄露，且存在严重的安全隐患，建议立即卸载。
		Trojan/Android.dialer.f[exp] 2020-04-01	低	该应用程序伪装为其他应用，运行隐藏图标，后台会私自拨打电话，发送短信，造成资费消耗和未知风险，建议卸载
		Trojan/Android.Coro.a[exp,spr] 2020-04-02	低	该应用程序伪装为正常应用，运行私自向联系人发送短信传递推广链接，诱导收件者下载安装未知应用，造成用户的资费消耗，建议卸载。
	较为活跃样本	Trojan/Android.FakeBank.z[prv,fra]	中	该应用程序伪装为银行类软件，访问钓鱼网站，欺骗用户填写银行相关信息，下载恶意 apk。监听手机敏感权限，获取手机固件信息、地理位置、通话记录，读取短信，私发短信，可实现直接拨打电话，修改联系人。造成用户隐私泄露，建议卸载。
		Trojan/Android.SpyLoan.b[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。
		Trojan/Android.SmsSpy.cw[prv]	中	该应用程序伪装为知名应用，运行隐藏图标，获取用户短信并私自转发、上传，造成用户的隐私泄露和资费消耗，建议卸载。
		RiskWare/Android.PJbocai.ag[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。
		RiskWare/Android.FakeQQ.aw[fra]	低	该应用程序伪装为 qq，非官方应用，无实际功能，建议使用官方正版应用。
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Microsoft Dynamics Business Central 远程代码执行漏洞（CVE-2020-0905）	高	Microsoft Dynamics Business Central 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受害者的服务器上执行任意命令。要利用此漏洞，经身份验证的攻击者需要诱使受害者连接到恶意的 Dynamics Business Central 客户端。
	较为活跃样本	Trojan[Downloader]/Win32.Apropo	中	此威胁是一种具有下载功能的木马类程序。该家族会利用系统漏洞和网络漏洞入侵用户电脑、破坏用户系统。该家族通过免费软件、共享软件、垃圾邮件附件、恶意链接或黑客网站进行传播。该家族入侵电脑后，利用用户的网络，在系统中下载恶意软件等。
		Trojan[PSW]/Win32.Nilage	中	此威胁是一种木马类程序。该家族入侵电脑后，会在系统中添加恶意代码，修改 Windows 注册表和启动项。该家族会导致用户文件丢失、程序运行错误、系统启动失败、蓝品、系统崩溃等。黑客利用该木马可以远程入侵并控制用户电脑，收集用户电脑中的信息等。
		Trojan/Win32.Spamha	中	此威胁是一种可以窃取用户信息的木马家族。该家族样本运行后复制自身到 %system32% 目录中，连接远程务器接受攻击者的恶意操作，收集系统信息并回传。
		GrayWare[AdWare]/Win32.Adtomi	低	此威胁是一种可以下载并安装推广应用的灰色软件家族。该家族会在用户浏览网页时弹出广告，安装皮肤，使 IE、Outlook 及 Outlook Express 看起来有所不同。占用系统资源，影响用户使用。
		GrayWare[AdWare]/Win32.TotalVelocity	低	此威胁是一种具有推送广告行为的灰色软件类程序。该家族样本运行后会下载并安装其它程序；修改注册表使其自启动；弹出广告；占用系统资源，影响用户使用。

（上接第一版）

FTP 等账户口令信息。



▲ KPOT 窃密木马回传的远程站点



▲窃取邮箱的用户名和口令等信息

●样本标签

病毒名称	Trojan/Win32.Zenpak
原始文件名	file1.exe
MD5	99785AE0679D6D3E27DE83AF403C23B0
文件格式	BinExecute/Microsoft.EXE[:X86]
文件大小	718.50 KB (735,744 bytes)
时间戳	2020-03-08 10:51:10
数字签名	无
加壳类型	无
编译语言	Microsoft Visual C++
VT 首次上传时间	2020-03-10 15:42:45
VT 检测结果	57 / 72

▲ KPOT 木马

3. 下载样本二：CoronaVirus 勒索软件

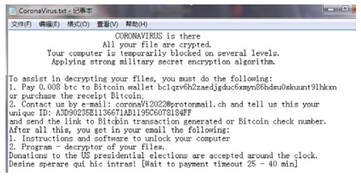
●样本标签

病毒名称	Trojan[Downloader]/Win32.Upatre
原始文件名	file2.exe
MD5	EC517204FBCF7A980D137B116AFA946D
文件格式	BinExecute/Microsoft.EXE[:X86]
文件大小	43.00 KB (44,032 bytes)
时间戳	2020-03-10 13:02:39
数字签名	无
加壳类型	无
编译语言	Microsoft Visual C++
VT 首次上传时间	2020-03-11 18:29:42
VT 检测结果	59 / 72

▲ CoronaVirus 勒索软件

●样本行为

勒索软件执行后将 C 盘驱动器重命名为 CoronaVirus，加密计算机上的文件，加密后的文件名格式为：< 电子邮箱联系地址 >+<____>+< 文件原名 >+< 文件原始后缀名 >，拷贝自身到临时目录下，在加密的文件夹和桌面上创建名为“CoronaVirus.txt”的勒索信并添加到注册表启动项，勒索信内容包含勒索说明、0.008 比特币的赎金金额和比特币地址等信息。该勒索软件使用“RSA+AES”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文件，具体操作为删除卷影副本、删除本地计算机的备份目录等，加密完成后修改注册表值使计算机重启后显示跟勒索信相似的锁定屏幕内容，勒索信中提及锁定屏幕时间为 25-40 分钟。目前被加密文件在未得到密钥前暂时无法解密。



▲ CoronaVirus 勒索软件勒索信

勒索软件执行后 C 盘驱动器重命名为疫情相关名称 CoronaVirus。

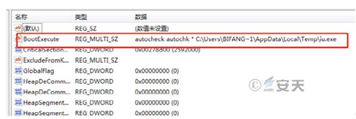
▲驱动器重命名

CoronaVirus 勒索软件运行后加密以下扩展名文件：

.txt	.dbf	.xls	.rry	.xml
.vsd	.pdf	.csv	.bmp	.tif
.tax	.gif	.qbr	.png	.mdb
.mdf	.sdf	.dwg	.dgn	.stl
.qbo	.qpd	.acc	.vpd	.odt
.ods	.rar	.zip	.zpp	.pas
.asm	.rtf	.lic	.avi	.mov
.vbs	.erf	.epf	.mxl	.chy
.mhl	.bak	.old		

▲ CoronaVirus 勒索软件加密的扩展名文件

该勒索软件运行后释放一个名为“iu.exe”（随机命名）的文件到临时目录下，并添加到注册表 HKLM\ SYSTEM\ CurrentControlSet\Control\Session Manager 项的“BootExecute”键值，实现系统启动后恶意锁屏。**安天 CERT 研究测试后发现通过启动安全模式，进入临时目录下删除该文件，可以取消恶意锁屏。**



▲修改注册表

该勒索软件加密完成后重启系统，锁定屏幕时显示类似勒索信的内容，锁定屏幕的时间是 15 分钟，进入系统操作界面并在桌面显示勒索信。

▲锁屏显示

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
CB2B4CD74C7B57A128D822A168E4E608
99785AE0679D6D3E27DE83AF403C23B0
EC517204FBCF7A980D137B116AFA946D
F272B1B21A74F74D5455DD7928AA87E1
wisecleaner.best/Soft/WSHSetup.exe
trynda.xyz/file1.exe
trynda.xyz/file2.exe
trynda.xyz/WSHSetup.exe

微信扫描二维码阅读原文