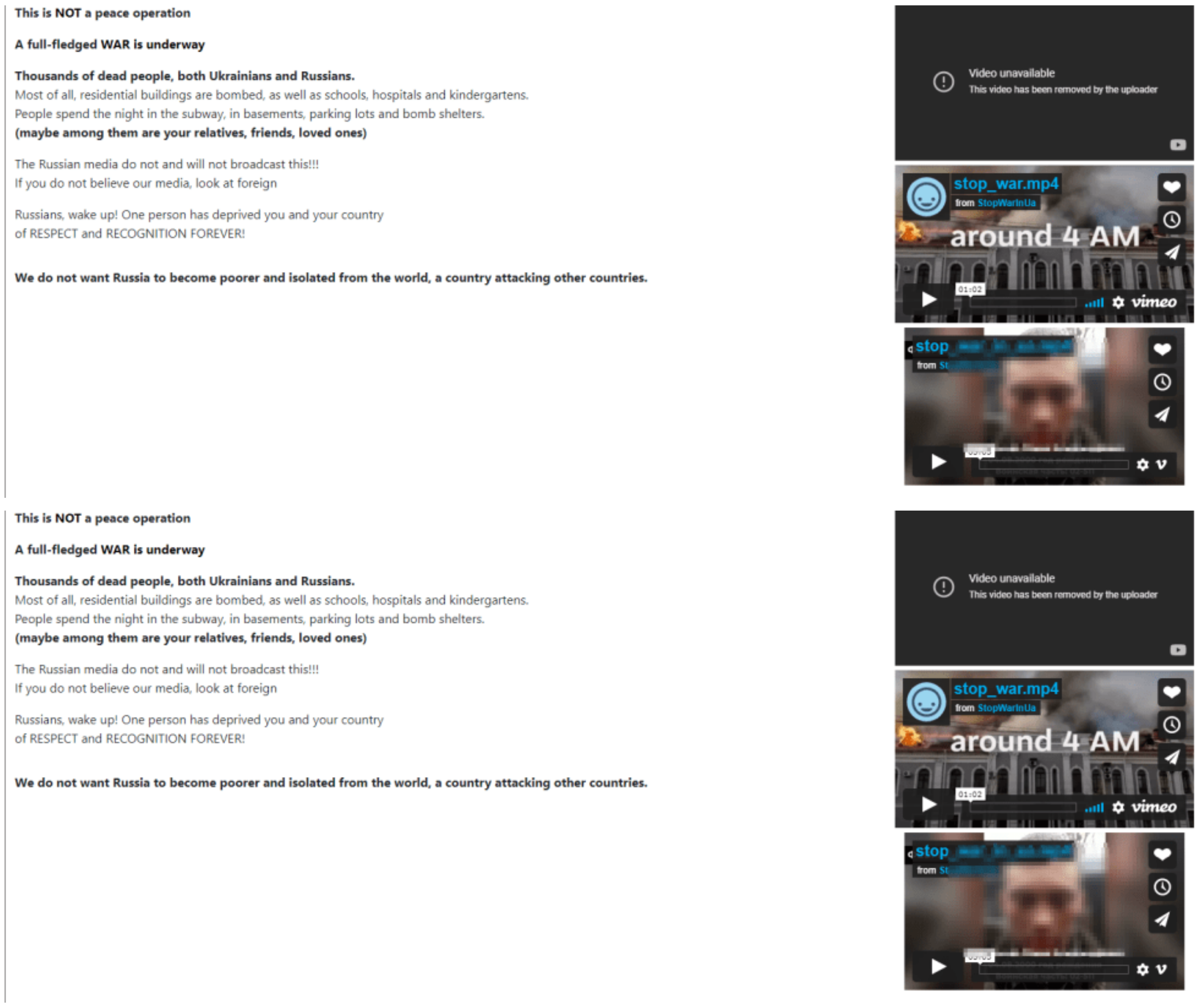
The geopolitical crisis between Russia and Ukraine has fueled multiple cyberattacks across the world. While monitoring for the latest cyber incidents that are part of the ongoing cyber warfare, the Cyble Research Labs recently came across a ransomware sample allegedly targeting Russia. What’s interesting is that instead of demanding ransom, this ransomware sends out a message to stop the war.

Upon execution, the ransomware renames encrypted files with the “.putinwillburnunhell” extension. While typically ransomware drops a .txt file as a ransom note, in this case, we saw a .html file named “RUSSKIJ VOENNIJ KORABL IDI NAHUJ”, which when translated in English means “RUSSIAN WARSHIP GO F**K”.

Our Open Source Intelligence (OSINT) analysis shows that Poland is the source of the sample. The message in the HTML file indicates that the ransomware may be targeting Russia, as shown in Figure 1.



This is NOT a peace operation

A full-fledged WAR is underway

Thousands of dead people, both Ukrainians and Russians.
Most of all, residential buildings are bombed, as well as schools, hospitals and kindergartens.
People spend the night in the subway, in basements, parking lots and bomb shelters.
(maybe among them are your relatives, friends, loved ones)

The Russian media do not and will not broadcast this!!!
If you do not believe our media, look at foreign

Russians, wake up! One person has deprived you and your country
of RESPECT and RECOGNITION FOREVER!

We do not want Russia to become poorer and isolated from the world, a country attacking other countries.

This is NOT a peace operation

A full-fledged WAR is underway

Thousands of dead people, both Ukrainians and Russians.
Most of all, residential buildings are bombed, as well as schools, hospitals and kindergartens.
People spend the night in the subway, in basements, parking lots and bomb shelters.
(maybe among them are your relatives, friends, loved ones)

The Russian media do not and will not broadcast this!!!
If you do not believe our media, look at foreign

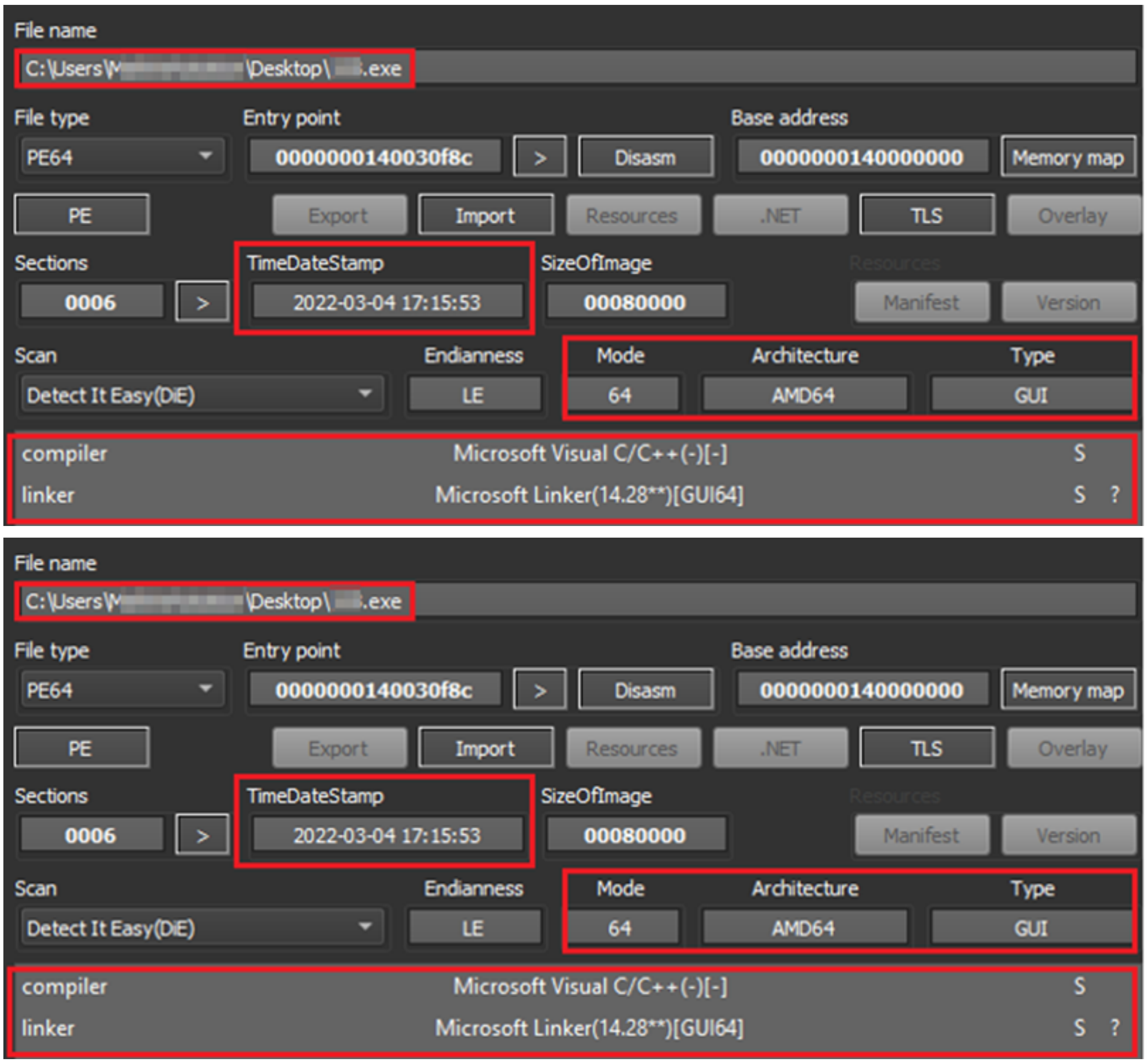
Russians, wake up! One person has deprived you and your country
of RESPECT and RECOGNITION FOREVER!

We do not want Russia to become poorer and isolated from the world, a country attacking other countries.

Figure 1 – Message in a Dropped file (Translated from Russian)

Technical Analysis

Cyble Research Labs performed an analysis of the sample with the hash value: 9f3c1668ee44bfcd1afd599215f5bd73c76609776b78cb04bb6ef1121cc80d37. Our research indicated that the malware is an x64 architecture Windows binary written in C/C++ and compiled on 2022-03-04 at 15:17:53.



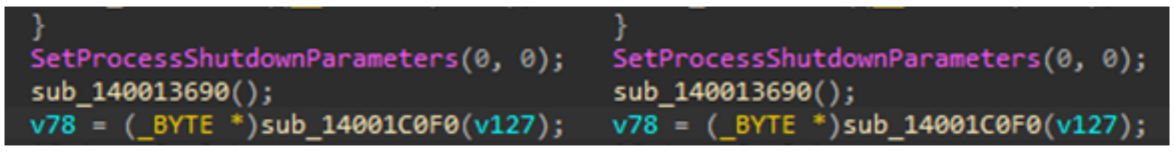
File name: C:\Users\M[redacted]\Desktop\[redacted].exe
File type: PE64
Entry point: 0000000140030f8c
Base address: 0000000140000000
Sections: 0006
TimeDateStamp: 2022-03-04 17:15:53
SizeOfImage: 00080000
Scan: Detect It Easy(DiE)
Endianness: LE
Mode: 64
Architecture: AMD64
Type: GUI

```
compiler          Microsoft Visual C/C++(-)[-]          S
linker            Microsoft Linker(14.28**)[GUI64]      S ?
```

File name: C:\Users\M[redacted]\Desktop\[redacted].exe
File type: PE64
Entry point: 0000000140030f8c
Base address: 0000000140000000
Sections: 0006
TimeDateStamp: 2022-03-04 17:15:53
SizeOfImage: 00080000
Scan: Detect It Easy(DiE)
Endianness: LE
Mode: 64
Architecture: AMD64
Type: GUI
compiler Microsoft Visual C/C++(-)[-] S
linker Microsoft Linker(14.28**)[GUI64] S ?

Figure 2 — File Information

We observed that the malware first changes the priority of the process to zero by calling the SetProcessShutdownParameters() API so that the malware's activities can be terminated only before the system shutdown. This is a way to increase the amount of time the malware gets to execute in the compromised machine.

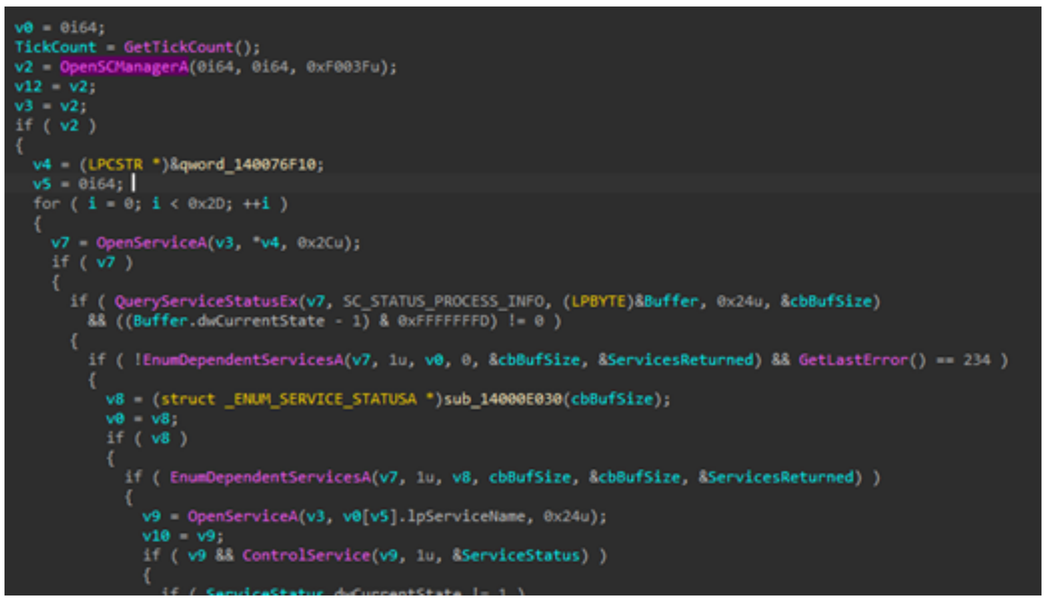


```
}                                     }
SetProcessShutdownParameters(0, 0);   SetProcessShutdownParameters(0, 0);
sub_140013690();                      sub_140013690();
v78 = (_BYTE *)sub_14001C0F0(v127);   v78 = (_BYTE *)sub_14001C0F0(v127);
```

Figure 3 — Malware Changes the Priority of the Process

The ransomware enumerates services in the compromised system and terminates those services that are actively running in the victim's machine. Some of these services include VSS, SQL, Memtas, mepocs, etc.

To identify the services in the victim's machine, it calls the OpenSCManagerA() API, which establishes a connection to the service control manager and gives the malware access to the service control manager database, as shown in Figure 4.

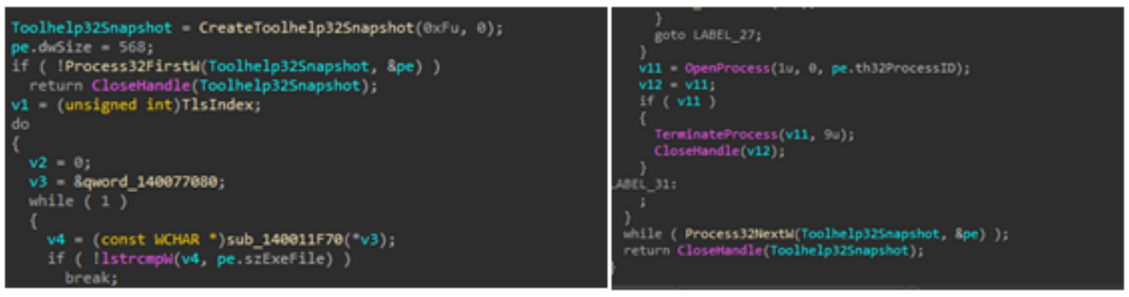


```
v0 = 0i64;
TickCount = GetTickCount();
v2 = OpenSCManagerA(0i64, 0i64, 0xF003Fu);
v12 = v2;
v3 = v2;
if ( v2 )
{
  v4 = (LPCSTR *)&qword_140076F10;
  v5 = 0i64;
  for ( i = 0; i < 0x2D; ++i )
  {
    v7 = OpenServiceA(v3, *v4, 0x2Cu);
    if ( v7 )
    {
      if ( QueryServiceStatusEx(v7, SC_STATUS_PROCESS_INFO, (LPBYTE)&Buffer, 0x24u, &cbBufSize)
        && ((Buffer.dwCurrentState - 1) & 0xFFFFFFFD) != 0 )
      {
        if ( !EnumDependentServicesA(v7, 1u, v0, 0, &cbBufSize, &ServicesReturned) && GetLastError() == 234 )
        {
          v8 = (struct _ENUM_SERVICE_STATUSA *)sub_14000E030(cbBufSize);
          v0 = v8;
          if ( v8 )
          {
            if ( EnumDependentServicesA(v7, 1u, v8, cbBufSize, &cbBufSize, &ServicesReturned) )
            {
              v9 = OpenServiceA(v3, v0[v5].lpServiceName, 0x24u);
              v10 = v9;
              if ( v9 && ControlService(v9, 1u, &ServiceStatus) )
              {
                if ( ServiceStatus.dwCurrentState != 1 )
```

```
v0 = 0i64;
TickCount = GetTickCount();
v2 = OpenSCManagerA(0i64, 0i64, 0xF003Fu);
v12 = v2;
v3 = v2;
if ( v2 )
{
  v4 = (LPCSTR *)&qword_140076F10;
  v5 = 0i64;
  for ( i = 0; i < 0x2D; ++i )
  {
    v7 = OpenServiceA(v3, *v4, 0x2Cu);
    if ( v7 )
    {
      if ( QueryServiceStatusEx(v7, SC_STATUS_PROCESS_INFO, (LPBYTE)&Buffer, 0x24u, &cbBufSize)
        && ((Buffer.dwCurrentState - 1) & 0xFFFFFFFD) != 0 )
      {
        if ( !EnumDependentServicesA(v7, 1u, v0, 0, &cbBufSize, &ServicesReturned) && GetLastError() == 234 )
        {
          v8 = (struct _ENUM_SERVICE_STATUSA *)sub_14000E030(cbBufSize);
          v0 = v8;
          if ( v8 )
          {
            if ( EnumDependentServicesA(v7, 1u, v8, cbBufSize, &cbBufSize, &ServicesReturned) )
            {
              v9 = OpenServiceA(v3, v0[v5].lpServiceName, 0x24u);
              v10 = v9;
              if ( v9 && ControlService(v9, 1u, &ServiceStatus) )
              {
                if ( ServiceStatus.dwCurrentState != 1 )
```

Figure 4 — Establishes a Connection to the Service Control Manager

The ransomware also enumerates the running processes and terminates processes that are actively running in the victim's machine. The process names checked by the ransomware include oracle.exe, ocssd.exe, dbsnmp.exe, synctime.exe, etc.



```
Toolhelp32Snapshot = CreateToolhelp32Snapshot(0xFu, 0);
pe.dwSize = 568;
if ( !Process32FirstW(Toolhelp32Snapshot, &pe) )
  return CloseHandle(Toolhelp32Snapshot);
v1 = (unsigned int)TlsIndex;
do
{
  v2 = 0;
  v3 = &qword_140077080;
  while ( 1 )
  {
    v4 = (const WCHAR *)sub_140011F70(*v3);
    if ( !lstrcmpW(v4, pe.szExeFile) )
      break;
```

```
      }
      goto LABEL_27;
    }
    v11 = OpenProcess(1u, 0, pe.th32ProcessID);
    v12 = v11;
    if ( v11 )
    {
      TerminateProcess(v11, 9u);
      CloseHandle(v12);
    }
LABEL_31:
    ;
  }
  while ( Process32NextW(Toolhelp32Snapshot, &pe) );
  return CloseHandle(Toolhelp32Snapshot);
}
```

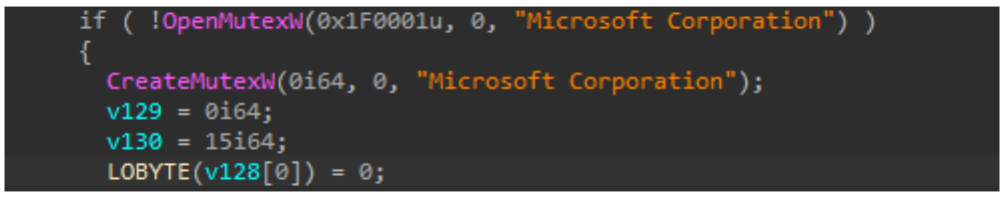
```
Toolhelp32Snapshot = CreateToolhelp32Snapshot(0xFu, 0);
pe.dwSize = 568;
if ( !Process32FirstW(Toolhelp32Snapshot, &pe) )
  return CloseHandle(Toolhelp32Snapshot);
v1 = (unsigned int)TlsIndex;
do
{
  v2 = 0;
  v3 = &qword_140077080;
  while ( 1 )
  {
    v4 = (const WCHAR *)sub_140011F70(*v3);
    if ( !lstrcmpW(v4, pe.szExeFile) )
      break;
```

```
      }
      goto LABEL_27;
    }
    v11 = OpenProcess(1u, 0, pe.th32ProcessID);
    v12 = v11;
    if ( v11 )
    {
      TerminateProcess(v11, 9u);
      CloseHandle(v12);
    }
LABEL_31:
    ;
  }
  while ( Process32NextW(Toolhelp32Snapshot, &pe) );
  return CloseHandle(Toolhelp32Snapshot);
}
```

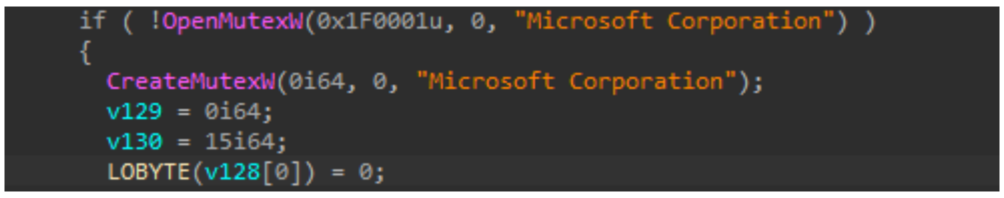
Figure 5 — Terminates Active Processes

The malware calls the SHEmptyRecycleBinA() API to empty the Recycle Bin as a step to ensure that deleted files cannot be restored after encryption.

Our research indicated that the ransomware tries to open a mutex named "Microsoft Corporation" in an infected machine. If the mutex name is not present, the malware creates the same mutex name and continues with its infection process.



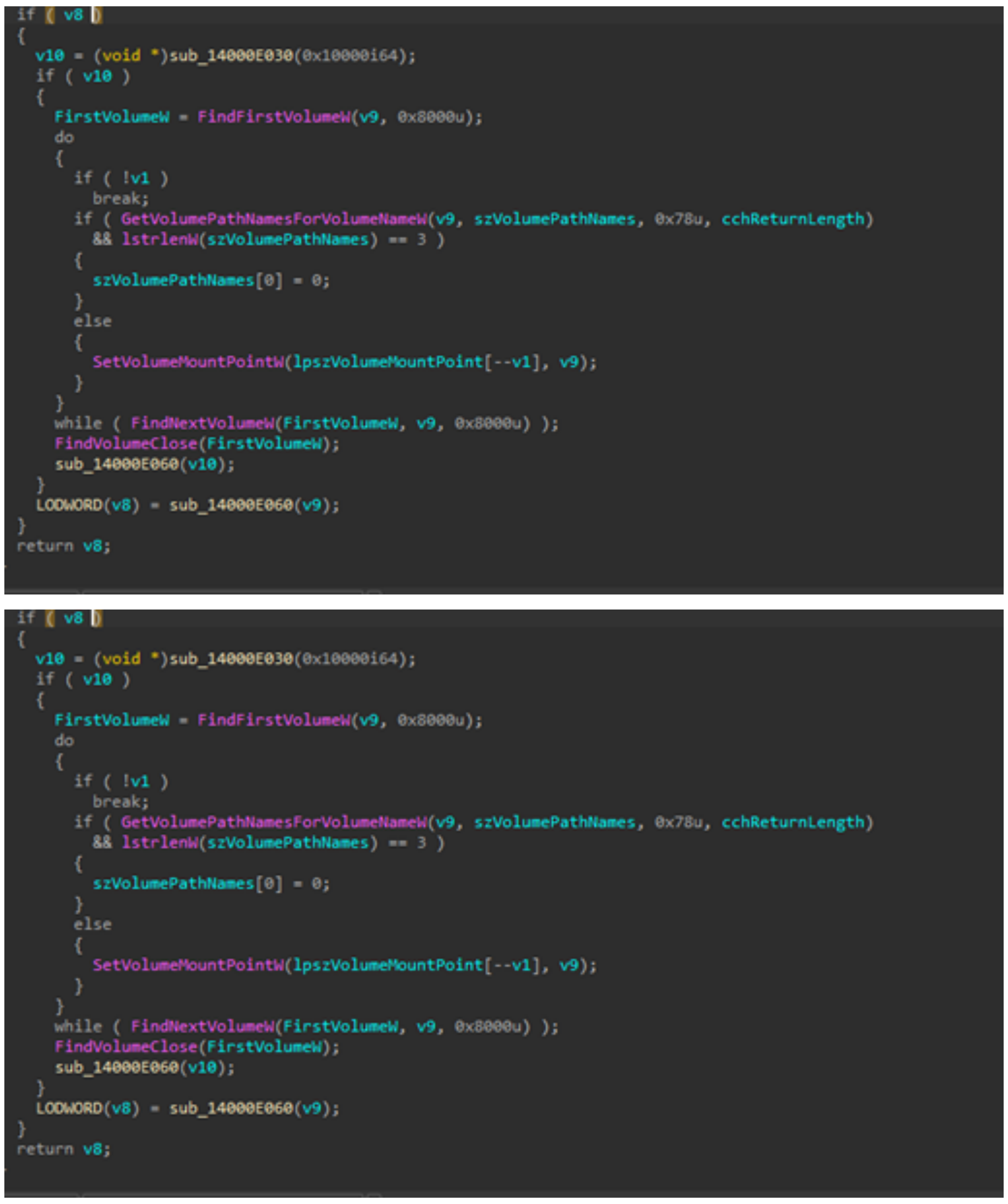
```
    if ( !OpenMutexW(0x1F0001u, 0, "Microsoft Corporation") )
    {
      CreateMutexW(0i64, 0, "Microsoft Corporation");
      v129 = 0i64;
      v130 = 15i64;
      LOBYTE(v128[0]) = 0;
```



```
    if ( !OpenMutexW(0x1F0001u, 0, "Microsoft Corporation") )
    {
      CreateMutexW(0i64, 0, "Microsoft Corporation");
      v129 = 0i64;
      v130 = 15i64;
      LOBYTE(v128[0]) = 0;
```

Figure 6 — Checks and Creates Mutex if not Present

After creating the mutex, the malware then begins the encryption process by identifying the volumes in an infected machine.

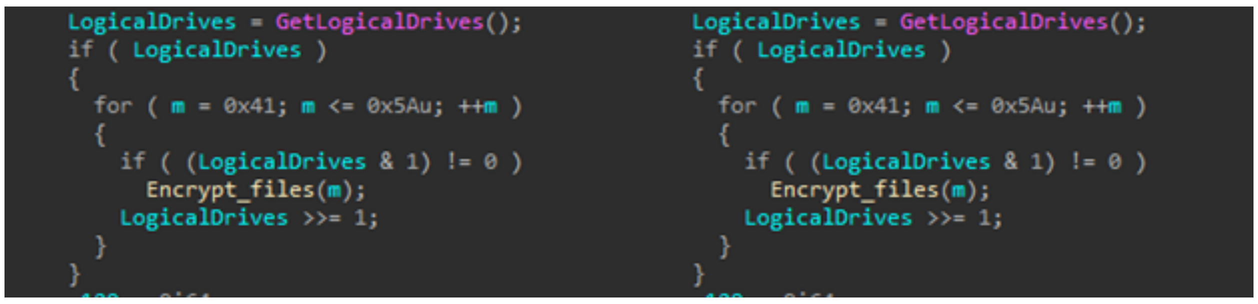


```
if ( v8 )
{
  v10 = (void *)sub_14000E030(0x10000i64);
  if ( v10 )
  {
    FirstVolumeW = FindFirstVolumeW(v9, 0x8000u);
    do
    {
      if ( !v1 )
        break;
      if ( GetVolumePathNamesForVolumeNameW(v9, szVolumePathNames, 0x78u, cchReturnLength)
        && lstrlenW(szVolumePathNames) == 3 )
      {
        szVolumePathNames[0] = 0;
      }
      else
      {
        SetVolumeMountPointW(lpszVolumeMountPoint[--v1], v9);
      }
    }
    while ( FindNextVolumeW(FirstVolumeW, v9, 0x8000u) );
    FindVolumeClose(FirstVolumeW);
    sub_14000E060(v10);
  }
  LODWORD(v8) = sub_14000E060(v9);
}
return v8;
```

```
if ( v8 )
{
  v10 = (void *)sub_14000E030(0x10000i64);
  if ( v10 )
  {
    FirstVolumeW = FindFirstVolumeW(v9, 0x8000u);
    do
    {
      if ( !v1 )
        break;
      if ( GetVolumePathNamesForVolumeNameW(v9, szVolumePathNames, 0x78u, cchReturnLength)
        && lstrlenW(szVolumePathNames) == 3 )
      {
        szVolumePathNames[0] = 0;
      }
      else
      {
        SetVolumeMountPointW(lpszVolumeMountPoint[--v1], v9);
      }
    }
    while ( FindNextVolumeW(FirstVolumeW, v9, 0x8000u) );
    FindVolumeClose(FirstVolumeW);
    sub_14000E060(v10);
  }
  LODWORD(v8) = sub_14000E060(v9);
}
return v8;
```

Figure 7 — Starts Encryption

It also identifies the mounted local drives by enumerating them from A to Z, as shown in Figure 8.

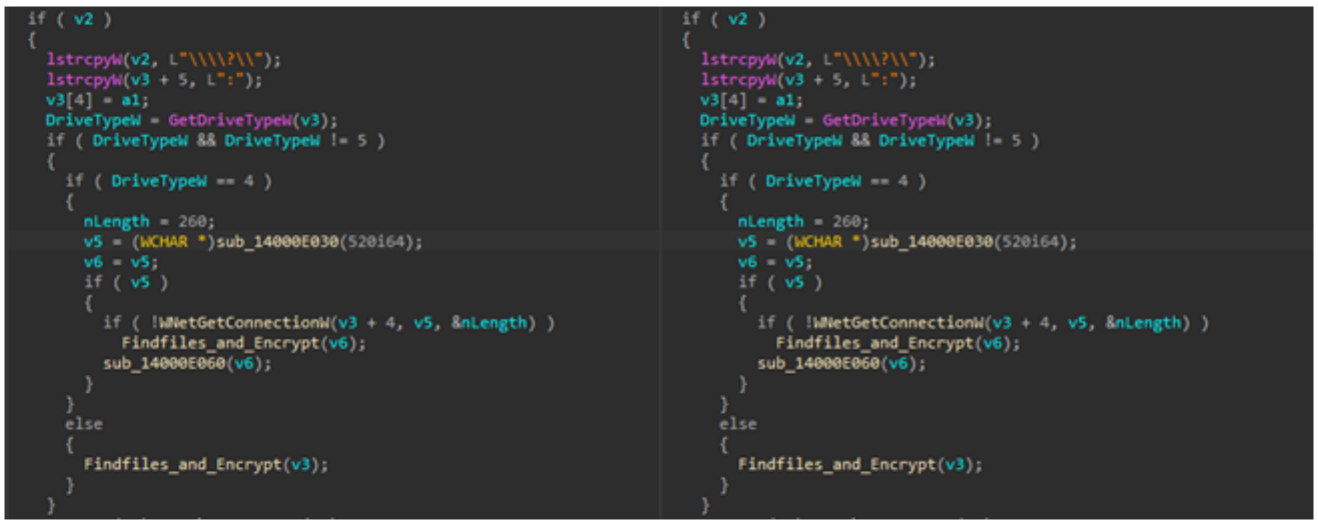


```
  LogicalDrives = GetLogicalDrives();
  if ( LogicalDrives )
  {
    for ( m = 0x41; m <= 0x5Au; ++m )
    {
      if ( (LogicalDrives & 1) != 0 )
        Encrypt_files(m);
      LogicalDrives >>= 1;
    }
  }
```

```
  LogicalDrives = GetLogicalDrives();
  if ( LogicalDrives )
  {
    for ( m = 0x41; m <= 0x5Au; ++m )
    {
      if ( (LogicalDrives & 1) != 0 )
        Encrypt_files(m);
      LogicalDrives >>= 1;
    }
  }
```

Figure 8 — Enumerates Local Drives

This is followed by the malware encrypting the files present in all of the identified drives with the exception of CD-ROM, as shown in Figure 9.



```
if ( v2 )
{
  lstrcpyW(v2, L"\\\\?\\");
  lstrcpyW(v3 + 5, L":");
  v3[4] = a1;
  DriveTypeW = GetDriveTypeW(v3);
  if ( DriveTypeW && DriveTypeW != 5 )
  {
    if ( DriveTypeW == 4 )
    {
      nLength = 260;
      v5 = (WCHAR *)sub_14000E030(520i64);
      v6 = v5;
      if ( v5 )
      {
        if ( !WNetGetConnectionW(v3 + 4, v5, &nLength) )
          Findfiles_and_Encrypt(v6);
        sub_14000E060(v6);
      }
    }
    else
    {
      Findfiles_and_Encrypt(v3);
    }
}
```

```
if ( v2 )
{
  lstrcpyW(v2, L"\\\\?\\");
  lstrcpyW(v3 + 5, L":");
  v3[4] = a1;
  DriveTypeW = GetDriveTypeW(v3);
  if ( DriveTypeW && DriveTypeW != 5 )
  {
    if ( DriveTypeW == 4 )
    {
      nLength = 260;
      v5 = (WCHAR *)sub_14000E030(520i64);
      v6 = v5;
      if ( v5 )
      {
        if ( !WNetGetConnectionW(v3 + 4, v5, &nLength) )
          Findfiles_and_Encrypt(v6);
        sub_14000E060(v6);
      }
    }
    else
    {
      Findfiles_and_Encrypt(v3);
    }
}
```

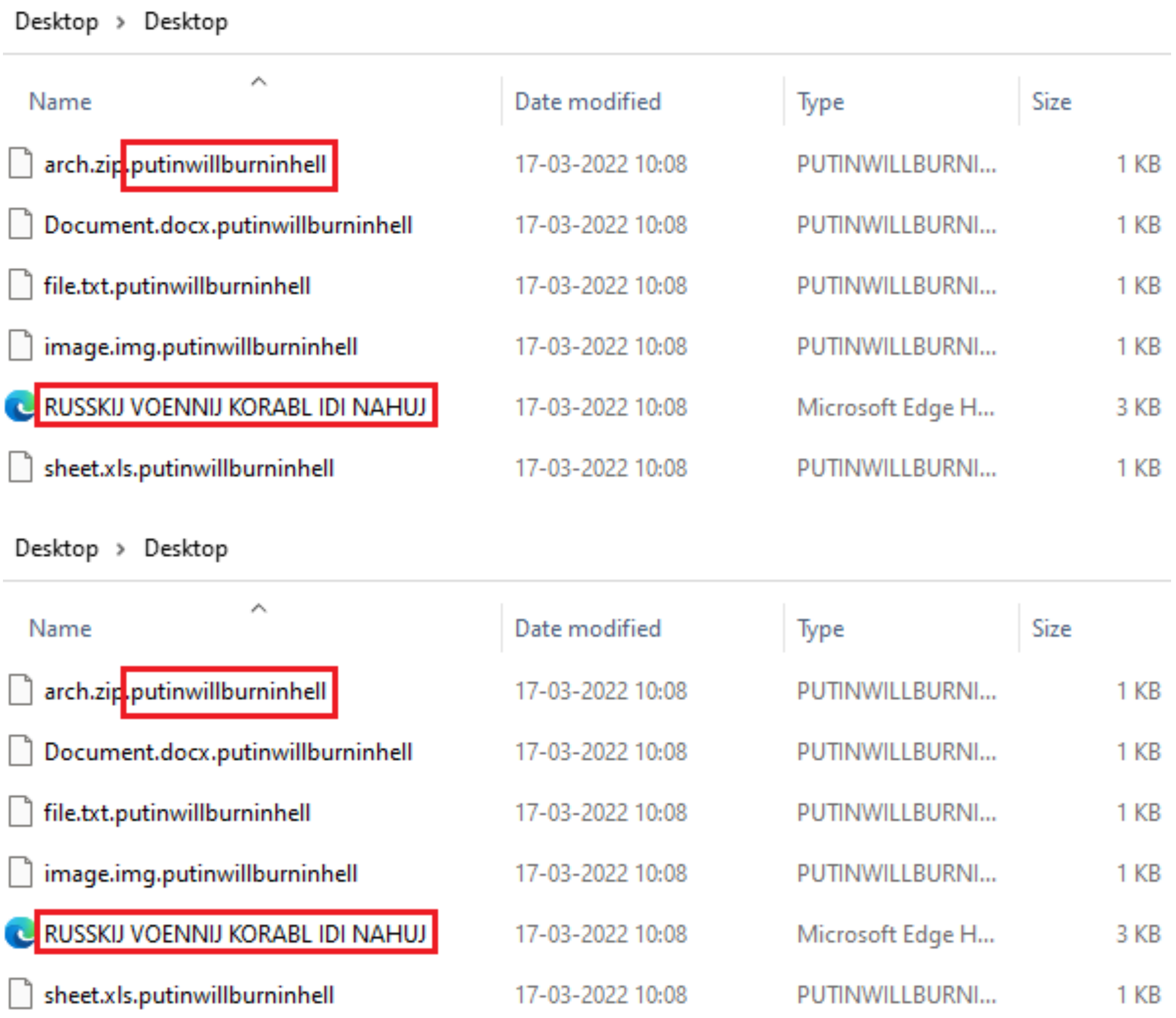
Figure 9 — Encrypts the Files present in all the Identified Drives Except CD-ROM

Before initiating encryption, the ransomware checks and excludes specific folders from encryption, such as AppData, Boot, Windows, Windows.old, Tor Browser, Internet Explorer, Google, Opera, Opera Software, Mozilla, Mozilla Firefox, ProgramData, Program Files, and Program Files (x86).

It also excludes certain files from encryption, such as autorun.inf, boot.ini, bootfont.bin, bootsect.bak, bootmgr, bootmgr.efi, bootmgfw.efi, desktop.ini, iconcache.db, ntldr, and ntuser.dat.

Additionally, specific extensions are also exempted from encryption, including
.putinwillburninhell, .hta, .exe, .dll, .cpl, .ini, .cab, .cur, .drv, .hlp, .icl, .icns, .ico, .idx, .sys, .spl, .ocx.

After encrypting the files on the victim's machine, the malware appends them with the extension ".putinwillburninhell" and drops an HTML file with the name "RUSSKIJ VOENNIJ KORABL IDI NAHUJ" as shown in Figure 10.



Desktop › Desktop

Name	Date modified	Type	Size
arch.zip.putinwillburninhell	17-03-2022 10:08	PUTINWILLBURNI...	1 KB
Document.docx.putinwillburninhell	17-03-2022 10:08	PUTINWILLBURNI...	1 KB
file.txt.putinwillburninhell	17-03-2022 10:08	PUTINWILLBURNI...	1 KB
image.img.putinwillburninhell	17-03-2022 10:08	PUTINWILLBURNI...	1 KB
RUSSKIJ VOENNIJ KORABL IDI NAHUJ	17-03-2022 10:08	Microsoft Edge H...	3 KB
sheet.xls.putinwillburninhell	17-03-2022 10:08	PUTINWILLBURNI...	1 KB

Desktop › Desktop

Name	Date modified	Type	Size
arch.zip.putinwillburninhell	17-03-2022 10:08	PUTINWILLBURNI...	1 KB
Document.docx.putinwillburninhell	17-03-2022 10:08	PUTINWILLBURNI...	1 KB
file.txt.putinwillburninhell	17-03-2022 10:08	PUTINWILLBURNI...	1 KB
image.img.putinwillburninhell	17-03-2022 10:08	PUTINWILLBURNI...	1 KB
RUSSKIJ VOENNIJ KORABL IDI NAHUJ	17-03-2022 10:08	Microsoft Edge H...	3 KB
sheet.xls.putinwillburninhell	17-03-2022 10:08	PUTINWILLBURNI...	1 KB

Figure 10 — Encrypted Files on the Victim's Machine

Conclusion

With the geopolitical crisis causing a surge in cyberattacks across the world, ransomware has emerged as a serious threat worldwide. As a result of the ongoing cyber warfare, we have witnessed an uptick in the use of ransomware and data wiper malware targeting both nations in conflict. Threat Actors are also devising attack techniques of increasing sophistication.

With cybercrime on the rise, it is imperative for organizations to strengthen their security posture. Our researchers are continuously gathering more information on the latest cyberattacks, and we will keep updating this space as and when we have more information.

Our Recommendations

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

Safety measures needed to prevent ransomware attacks

- Conduct regular backup practices and keep those backups offline or in a separate network.
- 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.

Users should take the following steps after the ransomware attack

- Detach infected devices on the same network.
- Disconnect external storage devices if connected.
- Inspect system logs for suspicious events.

Impacts and cruciality Of Ransomware

- Loss of valuable data
- Loss of reputation

- Loss of critical businesses information
- Disruption in an organization's operation
- Financial loss

MITRE ATT&CK® Techniques

Tactic	Technique ID	Technique Name
Execution	T1059	Command and Scripting Interpreter
Privilege Escalation	T1548 T1134	Abuse Elevation Control Mechanism Access Token Manipulation
Defense Evasion	T1112 T1027 T1562.001	Modify Registry Obfuscated Files or Information Impair Defenses: Disable or Modify Tools
Discovery	T1082 T1083	System Information Discovery File and Directory Discovery
Impact	T1490 T1489 T1486	Inhibit System Recovery Service Stop Data Encrypted for Impact

Indicators of Compromise (IoCs):

Indicators	Indicator type	Description
9f3c1668ee44bfcd1afd599215f5bd73c76609776b78cb04bb6ef1121cc80d37	SHA-256	AntiWar Ransomware
7b74a50352bb16ba94201c8a9e35b3c1d8a9dc8c	SHA-1	AntiWar Ransomware
3b3a50b242841e1789a919b1291051f1	MD5	AntiWar Ransomware