Be Wary of Ransomware Posing as Well-known Cybersecurity Companies - Sophos and Cylance

Antiy CERT

Time of first release:25 July, 2023

The original report is in Chinese, and this version is an AI-translated edition.

1 Overview

Recently, Antiy CERT (member of the CCTGA Ransomware Prevention and Response Working Group) discovered the same name as the network security company Sophos [1] ransomware, and the network security company Sophos issued a statement saying it had nothing to do with the ransomware.[1]

The Sophos ransomware was discovered in July 2023, and its attack payload was developed through the Rust programming language, and after analysis, it was found that the sample library file path had the word Dubinin, guessing relevant information that might be the payload developer, The ransomware ransomware letter format and the logic to add the suffix is similar to that of Phobos [2] ransomware. The execution process of the Sophos ransomware is not perfect, and no information of the victim has been found until the press release, and based on various reasons, it is speculated that the ransomware is currently in the testing stage and has not been launched into formal attack activities.[2]

Table 1-1 Overview of Sophos ransomware 1

Family name	Sophos
Time of occurrence	July 2023
Typical mode of transmission	Guess is currently in the testing phase, has not found the transmission mode temporarily
Typical Encryption Suffix	.sophos (original file name + 8-digit victim device ID + contact mailbox + .sophos)
Encryption algorithm	Aes + RSA
Decryption tools	Guess is currently in the testing phase, not found decryption tools
Encryption system	Windows, Linux

Double blackmail or not	It is assumed that no site for data leakage has been found in the current testing phase
Ransom note	

There was also the Cylance ransomware, a name given to cybersecurity vendors, which was discovered in March 2023 under the same name as BlackBerry's cyber security company Cylance, without a large number of attacks. It is found that part of the code segment of the Cylance ransomware is similar to that of the REvil (also known as Sodinokibi) [3] [4] ransomware, both of which execute the ransomware payload with specific parameters. Speculation may be a new ransomware created by members of the REvil ransomware group or a rebranding of the REvil ransomware.[3][4]

Table 1-2 Overview of Cylance ransomware2

Family name	**Cylance**
Time of occurrence	March 2023
Typical mode of transmission	Phishing
Typical Encryption Suffix	. Cylance
Encryption algorithm	Salsa20 or Chacha + Curve25519
Decryption tools	No public decryption tools have been found
Encryption system	Windows, Linux
Double blackmail or not	No (no sites for data leakage have been found)

Ransom note	[[=== Cylance Ransomware ===]] [+] What's happened? All your files are encrypted, and currently unsable, but you need to follow our instructions. otherwise, you cant return your data (NEVER). [+] What guarantees? Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests. To check the ability of returning files, we decrypt one file for free. That is our guarantee. If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data, cause just we have the private key. time is much more valuable than money. [+] How to cantact with us? Please write an email to: D4nte@onionmail.org and Backup@cyberfear.com Write this U-ID in the subject: --- !!! DANGER !!! DON'T try to change files by yourself, DON'T use any third party software for restoring your data or antivirus solutions - Its may entail damage of the private key and, as result, The Loss all data. !!! !!! !!! ONE MORE TIME: Its in your interests to get your files back. From our side, we (the best specialists) make everything for restoring, but please should not interfere. !!! !!! !!!

It has been proved that Antiy IEP, Cloud Host Security Monitoring System and Container Security Detection System can effectively detect and kill Sophos and Cylance ransomware.

2 Recommendations for protection

In response to ransomware attacks, Antiy recommends that individuals and businesses take the following precautions:

2.1 Personal protection

1. Enhance network security awareness: Maintain good habits of network use and actively learn relevant knowledge of network security;
2. Install terminal protection: Install anti-virus software. It is suggested that Antiy IEP users open the ransomware defense tool module (open by default);
3. Strengthen password strength: Avoid using weak passwords, recommend using 16-digit or longer passwords, including combinations of upper and lower case letters, numbers and symbols, and avoid using the same password for multiple servers;
4. Change passwords on a regular basis: Change system passwords on a regular basis to avoid system intrusion due to password leakage;
5. Update patches in time: It is suggested to open automatic update and install system patches, and update system patches in time for vulnerable parts such as servers, databases and middleware;
6. Close high-risk ports: External services shall be minimized; if no use is needed, it is recommended to close high-risk ports such as 135, 139, 445 and 3389;

7. Close PowerShell: If PowerShell command line tools are not used, it is recommended to close them;

8. Regular data backup: Data backup of important files on a regular basis, and backup data shall be isolated from the host computer.

2.2 Enterprise protection

1. Network security training and security drill: Regularly carry out network security training and security drill to improve employees "network security awareness;

2. Install terminal protection: Install anti-virus software, and recommend the installation of Antiy IEP for different platforms;

3. Update patches in time: It is suggested to open automatic update and install system patches, and update system patches in time for vulnerable parts such as servers, databases and middleware;

4. Enable log: Enable the key log collection function (security log, system log, PowerShell log, IIS log, error log, access log, transmission log and cookie log) to provide a foundation for security event tracing and tracing;

5. Set IP whitelist rules: Configure advanced secure Windows firewall, set the inbound rules for remote desktop connection, add the IP address or IP address range used to the rules, and prevent violent attack of non-rule IPs;

6. Host reinforcement: Conduct penetration test and safety reinforcement for the system;

7. Deploy Intrusion Detection System (IDS): Deploy traffic monitoring software or equipment to facilitate the discovery, tracing and tracing of ransomware. Taking network traffic as the detection and analysis object, the Antiy PTD can accurately detect a mass of known malicious codes and network attack activities, and effectively detect suspicious behaviors, assets and various unknown threats on the network;

8. Disaster backup plan: Establish a security disaster backup plan to ensure that the backup business system can be quickly enabled in case of a security event;

9. Safe service: In case of a ransomware attack, it is recommended to disconnect the network in time, and protect the site and wait for the security engineer to check the computer. Antiy 7 * 24 Service Hotline: 400-840-9234.

It has been proved that Antiy IEP, Cloud Host Security Monitoring System and Container Security Detection System can effectively detect and kill Sophos and Cylance ransomware.

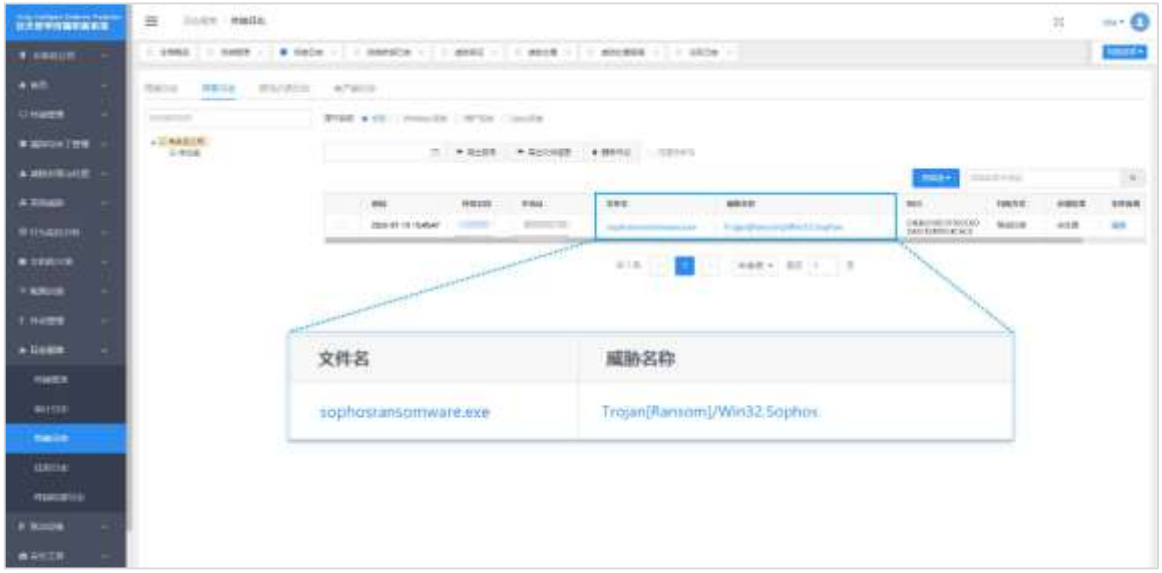

Figure 2-1 Antiy IEP can effectively detect and kill Sophos ransomware 1

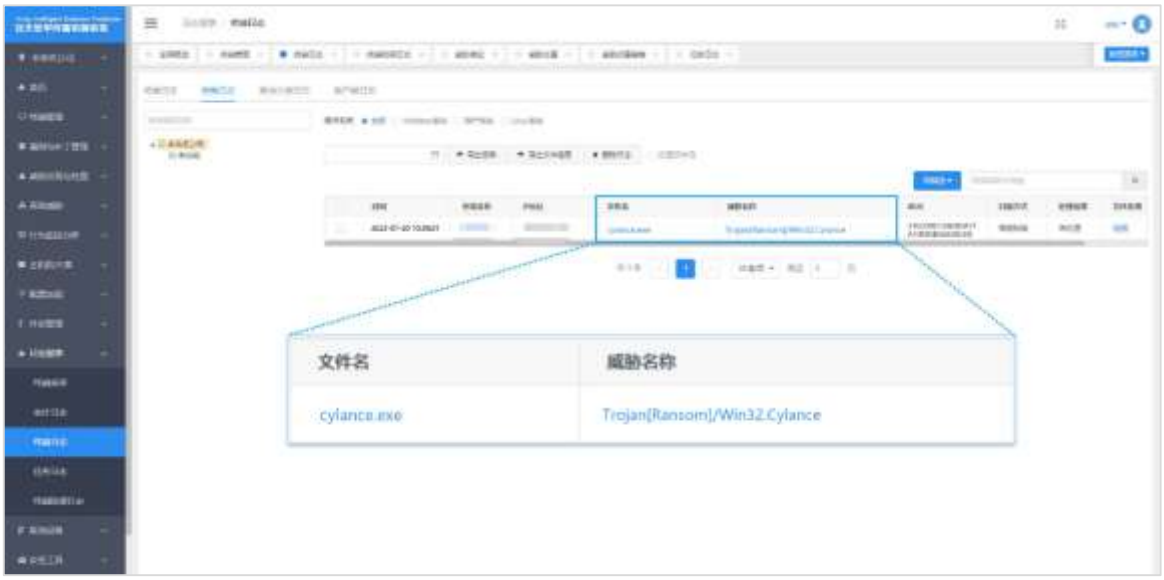

Figure 2-2 Antiy IEP can effectively detect and kill the Cylance ransomware 2

3 Suggestions on emergency response

When a machine is infected with the ransomware, do not panic, the following emergency work can be carried out immediately to reduce the harm caused by the ransomware: Isolation of the network, classified disposal, timely reporting, screening and reinforcement, and professional services.

1. The first thing to do is to disconnect the machines infected with the ransomware and prevent the ransomware from spreading sideways to infect other machines in the LAN.
2. Do not restart the machine, some ransomware writing has a logic problem, in the case of non-restart, there is the possibility of retrieving some of the encrypted files.
3. Do not be in a hurry to redo the system, format the hard disk, and other damage to the encrypted document behavior. First backup of the encrypted documents, encrypted with the suffix after the file is not infectious, can be copied to any computer for backup storage, but the possibility of recovery is extremely small. Depending on the situation, whether or not to wait for the decryption scheme, there are a small number of ransomware decryption tools that will be released for a variety of reasons.
4. Although we can determine the type of ransomware family from the suffix, the ransom note, and so on. However, due to the temporary absence of ransomware in the user network how encryption, dissemination of the specific process, it is still unable to accurately determine its type. Although virus samples with similar functions can be obtained from the threat intelligence database and confirmed by simulating the infection process, the location of the infection source needs to be refined during the infection process. It is suggested to locate and trace to the source in the form of on-site safety service.

4 Technical review

4.1 Sophos ransomware

When executing a Sophos ransomware payload, you can find the contents shown in the following figure, including payload version, victim device ID, contact information and encryption method, etc. The attacker can customize the email address, Jabber address, and key used for encryption, which is currently version 0.0.9, as shown in the figure.

Figure 4-1 Load user-defined execution interface 1

A description of the ransomware payload can be seen in the file properties.

Figure 4-2 Load file attributes2

When analyzing, it was found that the file path of the sample library of both versions contains the word Dubinin.

```
.rdata:00··· 00000073   C   C:\\Users\\Dubinin\\.cargo\\registry\\src\\index
.rdata:00··· 0000006E   C   C:\\Users\\Dubinin\\.cargo\\registry\\src\\index
.rdata:00··· 00000064   C   assertion failed: min <= max/rustc/114fb86ca08c
.rdata:00··· 00000064   C   C:\\Users\\Dubinin\\.cargo\\registry\\src\\index
.rdata:00··· 00000092   C   Empty list of items given to `Select`C:\\Users\
.rdata:00··· 00000068   C   C:\\Users\\Dubinin\\.cargo\\registry\\src\\index
.rdata:00··· 00000064   C   C:\\Users\\Dubinin\\.cargo\\registry\\src\\index
.rdata:00··· 0000006C   C   C:\\Users\\Dubinin\\.cargo\\registry\\src\\index
.rdata:00··· 00000066   C   C:\\Users\\Dubinin\\.cargo\\registry\\src\\index
```

Figure 4-3 Library file path 3

Download the image file in the hard-coded address online.

```
LODWORD(ppszPath) = 0;
if ( SHGetKnownFolderPath(&rfid, 0, 0, (PWSTR *)&ppszPath) )
{
  CoTaskMemFree((LPVOID)ppszPath);
ABEL_4:
  _$LT$alloc..boxed..Box$LT$dyn$u20$core..error..Error$GT$$u20$as$u20$core..convert..From$LT$$RF$str$GT$$GT$::from::h0e9cb0c4db032a4c(
    "no cache dirwallpaperno file path",
    12);
  a1[1] = v4;
  a1[2] = (int)&
  *a1 = 0;
  return;
}
LODWORD(Src[35]) = 16777217;
url::ParseOptions::parse::h1a912c5cbc6ae6ce(v161, v148, "https://i.postimg.cc/JzpfvBFf/wallapaper.jpg", 44);
v97 = v161[0];
```

Figure 4-4 Picture of online download 4

After the online download succeeds, the picture is used to modify the desktop background.

Figure 4-5 Modification of desktop background 4-5

Discover the Tor site through association analysis, and discover it is not the site of data leakage after visiting, guess it is to attack the management interface of organization member login.

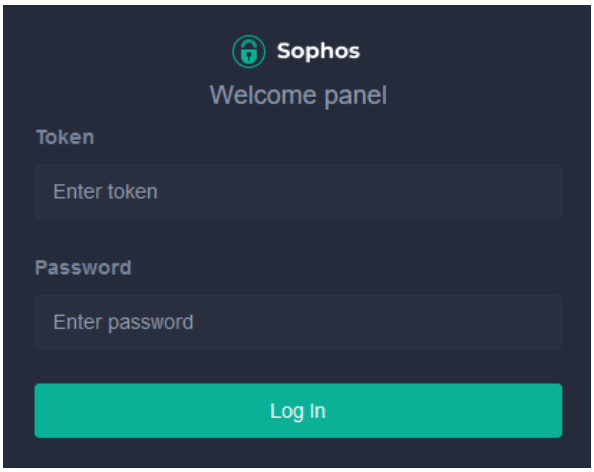

Figure 4-6 Tor site information 6

Before the encryption operation is executed, the specific process will be terminated to avoid interference with the execution of the encryption process. the specific process name is shown in the table below:

Table 4-1 List of finished processes 1

Sql.exe	Xfssvccon.exe	Ocomm.exe	Onenote. exe	Visio.exe
Oracle .exe	Mydesktopservice.exe	Dbeng50.exe	Outlook. exe	Winword.exe
Ocssd.exe	Ocautoupds.exe	Sqbcoreservice.exe	Powerpnt.exe	Wordpad.exe
Dbsnmp.exe	Encsvc.exe	Excel.exe	Steam.exe	Notepad.exe
Synctime.exe	Firefox.exe	Infopath.exe	Thebat.exe	Utweb.exe
Agntsvc.exe	Tbirdconfig.exe	Msaccess.exe	Thunderbird.exe	Ut.exe
Isqlplussvc.exe	Mydesktopqos.exe	Mspub.exe		

When performing encryption operations, specific folders will be bypassed, and the specific folder names are shown in the following table:

Table 4-2 List of bypassed folders2

Windows	$Recycle.Bin	$WINDOWS. ~ WS	Thumbs.db
Boot	$RECYCLE.BIN	Thumbs	Windows.old
Frst	Msocache	Pagefile	Windows.old
Kvrt _ Data	Documents and Settings	Hyberfil	Windows.old.000
Kvrt2020 _ Data	Recovery	$WinREAgent	Windows.old.000
Perflogs	System Volume Information	Program Files	Appdata

Adwcleaner	System.sav	Program Files (x86)	Dev
Programdata	$Windows. ~ WS	$WINDOWS. ~ BT	

In that case of encryption, file with specific extensions are bypass, as shown in the following table:

Table 4-3 List of extensions bypassed 3

Sys	Inf	Cpl	Log	Mpa	Msu	Spl
Regtrans - ms	Icos	Cur	Hlp	Msc	Nls	Themepack
Tmp	Bat	From	Icl	Msp	Msstyles	Key
Exe	Cmd	Deskthemepack	Icns	Theme	Nomedia	Hta
Ps1	Lnk	Diagcab	Ics	Wpx	Prf	Faust
Joker	Com	Diagcfg	Idx	Lock	Rtp	Devos
Ini	Ani	Diagpkg	Ldf	Mkp	Scr	Sophos
Dll	Adv	Drv	Mod	Ocx	Hs	

Delete the volume shadow backup and avoid restoring files through the volume shadow backup.

```
:process::Command::arg::h1e3d7e356221d56b(v6, aC, 2);
:process::Command::arg::h1e3d7e356221d56b(v6, "vssadmin delete shadows /all /quiet", 35);
and::output::hc785591d92fcdc59(&lpMem);
```

Figure 4-7 Delete the shadow backup 7

Generates a ransom note named information.hta.

Figure 4-8 Generation of blackmail letter8

Add the suffix in the format of. [[[8-digit device ID in combination of numbers and letters]]. [Email address]. For example: Test.doc. [1a2b3c4d]. [[Test @ aaa.com]] .sophos

Figure 4-9 Encrypted file suffix 9

4.2 Cylance ransomware

The Cylance ransomware payload supports execution with specific parameters.


```
IDA Vie…   Pseudocode-A

46
47    v0 = GetCommandLineW();
48    v1 = CommandLineToArgvW(v0, &pNumArgs);
49    if ( pNumArgs > 1 )
50    {
51      v2 = 1;
52      while ( lstrcmpiW(v1[v2], L"-path") )
53      {
54        if ( ++v2 >= pNumArgs )
55          goto LABEL_10;
56      }
57      v3 = v1[v2 + 1];
58      lpString2 = v3;
59      if ( v3 )
60      {
61        v4 = 2 * lstrlenW(v3) + 2;
62        for ( i = HeapAlloc(hHeap, 8u, v4); !i; i = Heap
63          Sleep(0x80u);
64        lpThreadParameter = i;
65        lstrcpyW((LPWSTR)i, lpString2);
66      }
67    }
68  LABEL_10:
69    v6 = GetCommandLineW();
70    v7 = CommandLineToArgvW(v6, &pNumArgs);
71    if ( pNumArgs > 1 )
72    {
73      v8 = 1;
74      while ( lstrcmpiW(v7[v8], L"-mode") )
75      {
76        if ( ++v8 >= pNumArgs )
77          goto LABEL_25;
78      }
79      v9 = v7[v8 + 1];
80      if ( v9 )
81      {
82        if ( lstrcmpiW(v9, L"full") )
83        {
84          if ( lstrcmpiW(v9, L"fast") )
85          {
86            if ( lstrcmpiW(v9, L"split") )
87            {
88              v10 = lstrcmpiW(v9, L"custom");
89              v11 = encrypt_mode;
90              if ( !v10 )
91                v11 = 4;
92              encrypt_mode = v11;
93            }
94            else
95            {
96              encrypt_mode = 3;
97            }
98          }
```

```
String2:                                ; DATA XREF: ParseArgs:loc_401030↑o
                text "UTF-16LE", '-path',0
; const WCHAR aMode
aMode:                                  ; DATA XREF: ParseArgs:loc_4010C3↑o
                text "UTF-16LE", '-mode',0
; const WCHAR aFull
aFull:                                  ; DATA XREF: ParseArgs+E1↑o
                text "UTF-16LE", 'full',0
                align 10h
; const WCHAR aFast
aFast:                                  ; DATA XREF: ParseArgs:loc_4010F9↑o
                text "UTF-16LE", 'fast',0
                align 4
; const WCHAR aSplit
aSplit:                                 ; DATA XREF: ParseArgs:loc_401111↑o
                text "UTF-16LE", 'split',0
; const WCHAR aCustom
aCustom:                                ; DATA XREF: ParseArgs:loc_401129↑o
                text "UTF-16LE", 'custom',0
                align 4
; const WCHAR aPriority
aPriority:                              ; DATA XREF: ParseArgs:loc_401165↑o
                text "UTF-16LE", '-priority',0
; const WCHAR aOff
aOff:                                   ; DATA XREF: ParseArgs+183↑o
                text "UTF-16LE", 'off',0
; const WCHAR aSkip
aSkip:                                  ; DATA XREF: ParseArgs:loc_4011B3↑o
                text "UTF-16LE", '-skip',0
; const WCHAR aPower
aPower:                                 ; DATA XREF: ParseArgs:loc_401200↑o
                text "UTF-16LE", '-power',0
                align 10h
; const WCHAR aRestart
aRestart:                               ; DATA XREF: ParseArgs+21E↑o
                text "UTF-16LE", 'restart',0
; const WCHAR aShutdown
aShutdown:                              ; DATA XREF: ParseArgs:loc_401236↑o
                text "UTF-16LE", 'shutdown',0
                align 4
; const WCHAR aConsole
aConsole:                               ; DATA XREF: ParseArgs:loc_401272↑o
                text "UTF-16LE", '-console',0
                align 4
; const WCHAR aNomutex
aNomutex:                               ; DATA XREF: ParseArgs:loc_4012B0↑o
                text "UTF-16LE", '-nomutex',0
                align 4
; const WCHAR aNonetdrive
aNonetdrive:                            ; DATA XREF: ParseArgs:loc_4012F0↑o
                text "UTF-16LE", '-nonetdrive',0
; const WCHAR aNodel
aNodel:                                 ; DATA XREF: ParseArgs:loc_401135↑o
                text "UTF-16LE", '-nodel',0
```

Figure 4-10 Parameter execution10

Create a mutex named CylanceMutex to prevent the load from executing repeatedly.

```
void Mutex()
{
  if ( !dword_4257E4 )
  {
    hMutex = CreateMutexW(0, 1, L"Global\\CylanceMutex");
    if ( GetLastError() == 183 )
      ExitProcess(0);
  }
}
```

Figure 4-11: Creating a mutex11

Create a scheduled task named Windows Update BETA to persist.

```
GetModuleFileNameW(0, Filename, 0x104u);
v0 = GetCommandLineW();
v1 = CommandLineToArgvW(v0, &pNumArgs);
if ( pNumArgs <= 1 )
{
  wsprintfW(
    Parameters,
    L"/c SCHTASKS.exe /Create /RU \"NT AUTHORITY\\SYSTEM\" /sc onstart /TN \"Windows Update BETA\" /TR \"%s\" /F",
    Filename);
}
else
{
  v2 = StrStrIW(v0, v1[1]);
  wsprintfW(
    Parameters,
    L"/c SCHTASKS.exe /Create /RU \"NT AUTHORITY\\SYSTEM\" /sc onstart /TN \"Windows Update BETA\" /TR \"%s\" /F",
    Filename,
    v2);
}
ShellExecuteW(0, L"open", L"cmd.exe", Parameters, 0, 0);
```

Figure 4-12 Create a scheduled task 12

When performing encryption operations, specific file names will be bypassed, as shown in the following table:

Table 4-4 Bypasses specific file names4

Ntldr	Autorun.inf	Boot.ini	Bootnxt	Bootmgr
Ntuser.dat	Thumbs.db	Desktop.ini	Cylance _ README.txt	Llkfp.bmp
Bootsect.bak	Iconcache.db	Ntuser.ini	Lpw5.tmp	Bootfont.bin
Ntuser.dat. log				

In that case of encryption, specific file extension are bypassed, as shown in the follow table:

Table 4-5 Bypass specific file extensions5

Dll	Exe	Sys	Drv
Efi	Msi	Lnk	Cylance

When performing encryption operations, specific folders will be bypassed, and their names are shown in the following table:

Table 4-6 Bypasses a specific folder6

Windows	$Windows. ~ bt	$Windows. ~ WS	Windows.old	Windows NT
All Users	Public	Boot	Intel	Perflogs
System Volume Information	Msocache	$RECYCLE.BIN	Default	Config. Msi
Tor browser	Microsoft	Google	Yandex	

When performing an encryption operation, a file with a specific file extension must be encrypted, as shown in the table below:

Table 4-7 List of file extensions that must be encrypted 7

Mdf	Ndf	Edb	Mdb	Accdb	Db	Db2
Db3	Sql	Sqlite	Sqlite 3	Sqlitedb	Database	Zip
Rar	7z	Tar	Whim	Gz	Xld	Xls
Xlsx	Csv	Bak	Back	Backup		

Generate a ransom note named CYLANCE _ README.txt, the contents of which are as follows:

```
[[=== Cylance Ransomware ===]]

[+] What's happened?
All your files are encrypted, and currently unsable, but you need to follow our instructions.
otherwise, you cant return your data (NEVER).

[+] What guarantees?
Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we
do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.
To check the ability of returning files, we decrypt one file for free. That is our guarantee.
If you will not cooperate with our service - for us, its does not matter. But you will lose your time
and data, cause just we have the private key. time is much more valuable than money.

[+] How to cantact with us?
Please write an email to: D4nte@onionmail.org and Backup@cyberfear.com
Write this U-ID in the subject:

---------------------------------------------------------------------------------------

!!! DANGER !!!
DON'T try to change files by yourself, DON'T use any third party software for restoring your data or
antivirus solutions - Its may entail damage of the private key and, as result, The Loss all data.
!!! !!! !!!
ONE MORE TIME: Its in your interests to get your files back. From our side, we (the best specialists)
make everything for restoring, but please should not interfere.
!!! !!! !!!
```

Figure 4-13 Generates a ransom note

Add the .Cylance suffix at the end of the encrypted file, for example: Test.doc. Cylance

Figure 4-14 Encrypted file suffix 13

5 IoCs

IoCs
C4e82318d5f902c6dda61e2b00c4cac8
948aee0ffbbdefa431714c5001eb960

179.43.154.137
Hxxps: / / i.postimg.cc / JzpfvBFf / wallapaper.jpg
31ed39e13ae9da7fa610f85b56838dde
521666a43aeb19e91e7df9a3f9fe76ba
1bcc1640fa355cd1ab330c88d4d7f4cb
3cfccbf5a5138b51d569a487c1d558ea
4601076b807ed013844ac7e8a394eb33
139.99.233.175

Appendix I: Reference

[1]. Sophos Discovers Ransomware Abusing "Sophos" Name

Https: / / news.sophos.com / en-us / 2023 / 07 / 18 / sophos-discoverers-ransomware-abusing-sophos-name /

[2]. Phobos ransomware variant analysis report

Https: / / www.antiy.cn / research / notice & report / research _ report / 20191016.html

[3]. The Association Analysis of the Operating Organization of the Ransomware Sodinokibi

Https: / / www.antiy.cn / research / notice & report / research _ report / 20190628.html

[4]. Review of recent activities of Sodinokibi / REvil extortion organization and analysis of the latest samples

Https: / / www.antiy.cn / research / notice & report / research _ report / 20210918.html

Appendix II: About Antiy

Antiy is committed to enhancing the network security defense capabilities of its customers and effectively responding to security threats. Through more than 20 years of independent research and development, Antiy has developed technological leadership in areas such as threat detection engines, advanced threat countermeasures, and large-scale threat automation analysis.

Antiy has developed IEP (Intelligent Endpoint Protection System) security product family for PC, server and other system environments, as well as UWP (Unified Workload Protect) security products for cloud hosts, container

and other system environments, providing system security capabilities including endpoint antivirus, endpoint protection (EPP), endpoint detection and response (EDR), and Cloud Workload Protection Platform (CWPP) , etc. Antiy has established a closed-loop product system of threat countermeasures based on its threat intelligence and threat detection capabilities, achieving perception, retardation, blocking and presentation of the advanced threats through products such as the Persistent Threat Detection System (PTD), Persistent Threat Analysis System (PTA), Attack Capture System (ACS), and TDS. For web and business security scenarios, Antiy has launched the PTF Next-generation Web Application and API Protection System (WAAP) and SCS Code Security Detection System to help customers shift their security capabilities to the left in the DevOps process. At the same time, it has developed four major kinds of security service: network attack and defense logic deduction, in-depth threat hunting, security threat inspection, and regular security operations. Through the Threat Confrontation Operation Platform (XDR), multiple security products and services are integrated to effectively support the upgrade of comprehensive threat confrontation capabilities.

Antiy provides comprehensive security solutions for clients with high security requirements, including network and information authorities, military forces, ministries, confidential industries, and critical information infrastructure. Antiy has participated in the security work of major national political and social events since 2005 and has won honors such as the Outstanding Contribution Award and Advanced Security Group. Since 2015, Antiy's products and services have provided security support for major spaceflight missions including manned spaceflight, lunar exploration, and space station docking, as well as significant missions such as the maiden flight of large aircraft, escort of main force ships, and Antarctic scientific research. We have received several thank-you letters from relevant departments.

Antiy is a core enabler of the global fundamental security supply chain. Nearly a hundred of the world's leading security and IT enterprises have chosen Antiy as their partner of detection capability. At present, Antiy's threat detection engine provides security detection capabilities for over 1.3 million network devices and over 3 billion smart terminal devices worldwide, which has become a "national-level" engine. As of now, Antiy has filed 1,877 patents in the field of cybersecurity and obtained 936 patents. It has been awarded the title of National Intellectual Property Advantage Enterprise and the 17th (2015) China Patent Excellence Award.

Antiy is an important enterprise node in China emergency response system and has provided early warning and comprehensive emergency response in major security threats and virus outbreaks such as "Code Red", "Dvldr",

"Heartbleed", "Bash Shellcode" and "WannaCry". Antiy conducts continuous monitoring and in-depth analysis against dozens of advanced cyberspce threat actors (APT groups) such as "Equation", "White Elephant", "Lotus" and "Greenspot" and their attack actions, assisting customers to form effective protection when the enemy situation is accurately predicted.