A Deep-dive Analysis of KARMA Ransomware

blog.cyble.com/2021/08/24/a-deep-dive-analysis-of-karma-ransomware/

August 24, 2021

While performing our routine Open-Source Intelligence (OSINT) research, Cyble Research Labs came across a ransomware group known as KARMA, which encrypts files on the victim's machine and appends the extension of encrypted files to *.KARMA*. Subsequently, the Threat Actors (TAs) demand that the victims pay ransom for the private key to recover their data.

Based on analysis by Cyble Research Labs, we have observed that the executable payload is a console-based application.

Figure 1 shows the execution flow of the Karma ransomware. After execution, the malware takes inputs from the user and checks all A-Z drives, excludes folders and files from encryption. After this, the ransomware proceeds to drop the ransom note and replaces the original content with encrypted content. It then appends the extension as *.KARMA*.

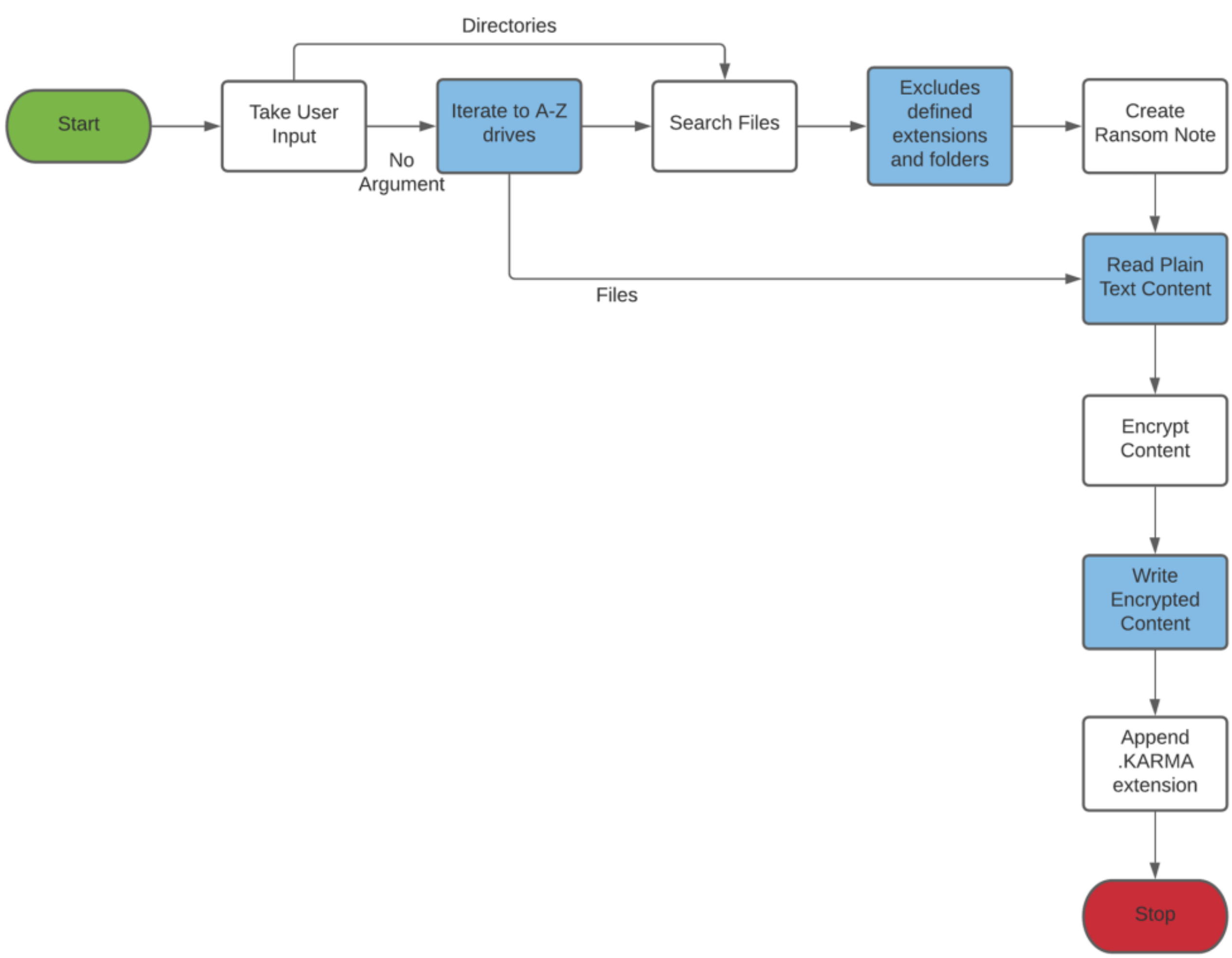


Figure 1 Execution Flow of Karma Ransomware

Technical Analysis

Our static analysis found that the malware is a console-based x86 architecture executable written in C/C++, as shown in Figure 2.

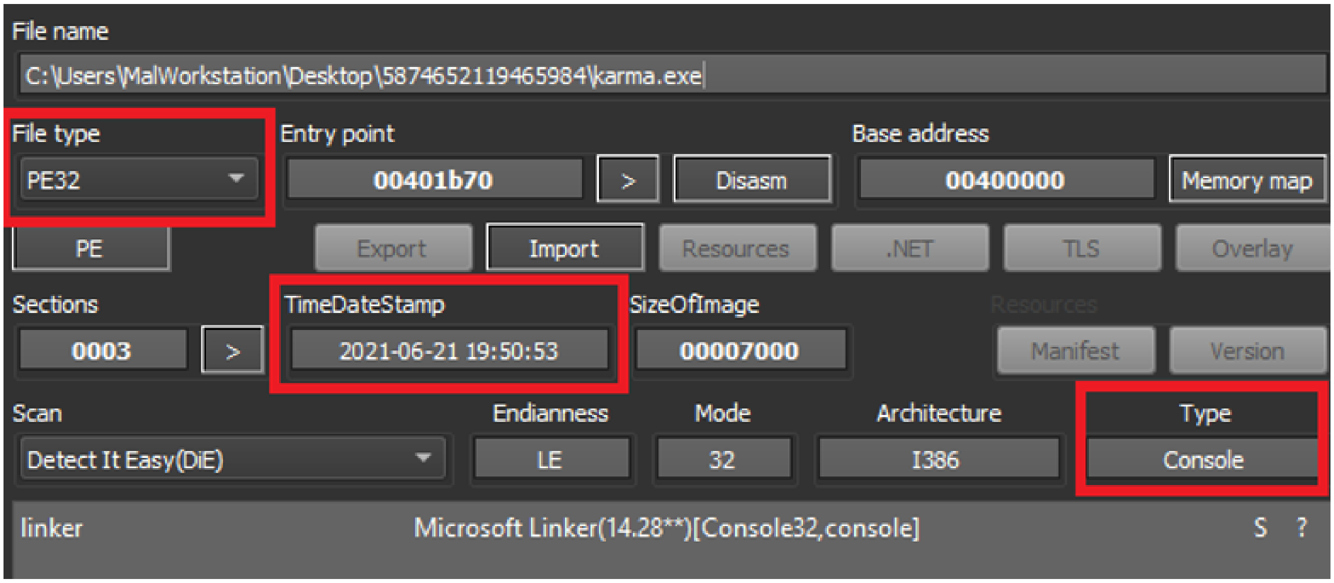
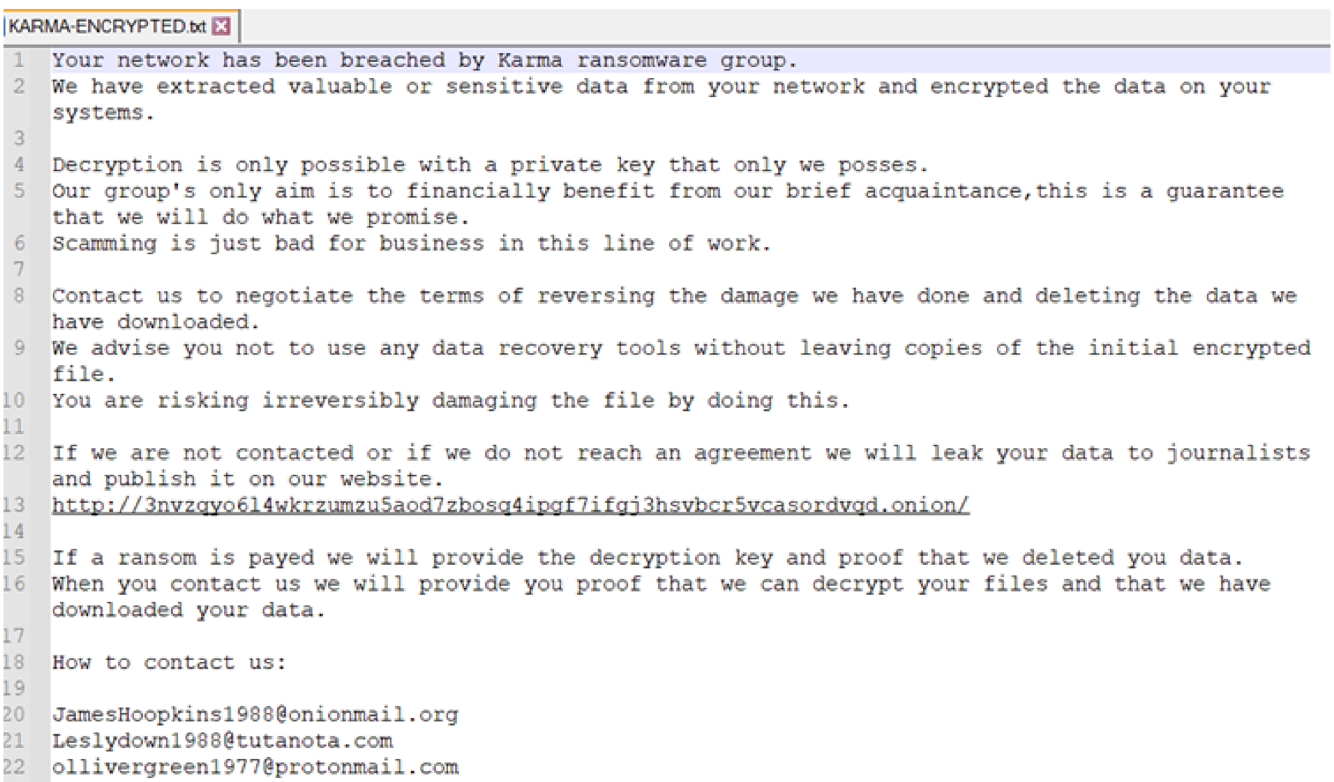


Figure 2 Malware Payload Static Information

After encrypting the files, the ransomware payload drops the ransom note named *KARMA-ENCRYPTED.txt* in various places in the victim's machine, as shown in Figure 3.



KARMA-ENCRYPTED.txt

```
Your network has been breached by Karma ransomware group.
We have extracted valuable or sensitive data from your network and encrypted the data on your systems.

Decryption is only possible with a private key that only we posses.
Our group's only aim is to financially benefit from our brief acquaintance,this is a guarantee that we will do what we promise.
Scamming is just bad for business in this line of work.

Contact us to negotiate the terms of reversing the damage we have done and deleting the data we have downloaded.
We advise you not to use any data recovery tools without leaving copies of the initial encrypted file.
You are risking irreversibly damaging the file by doing this.

If we are not contacted or if we do not reach an agreement we will leak your data to journalists and publish it on our website.
http://3nvzqyo6l4wkrzumzu5aod7zbosq4ipgf7ifgj3hsvbcr5vcasordvqd.onion/

If a ransom is payed we will provide the decryption key and proof that we deleted you data.
When you contact us we will provide you proof that we can decrypt your files and that we have downloaded your data.

How to contact us:

JamesHoopkins1988@onionmail.org
Leslydown1988@tutanota.com
ollivergreen1977@protonmail.com
```

Figure 3 Ransom Note

In the above ransom note, the TAs have given email support IDs " JamesHoopkins1988@onionmail[.]org", Leslydown1988@tutanota[.]com", " *ollivergreen1977@protonmail[.]com*“. The victims are asked to reach out to the attackers and pay the ransom amount in Bitcoin (BTC) to get the private decryption key.

After execution, the malware encrypts the files and appends the extension of encrypted files as *.KARMA* and drops ransom note as shown in Figure 4.

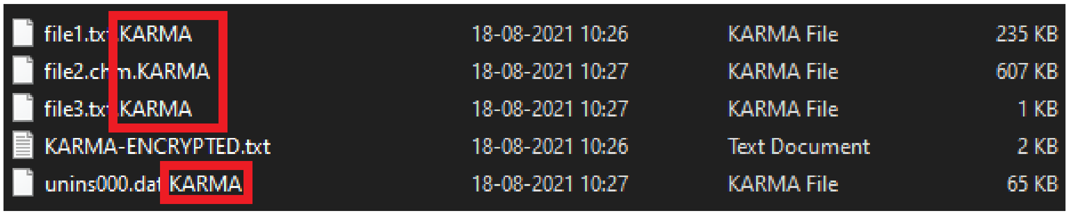


Figure 4 Encrypted Files

Upon execution, a Mutex with the name *KARMA* is createdto ensure that only one instance of this ransomware is running at a time*,* as shown in Figure 5.

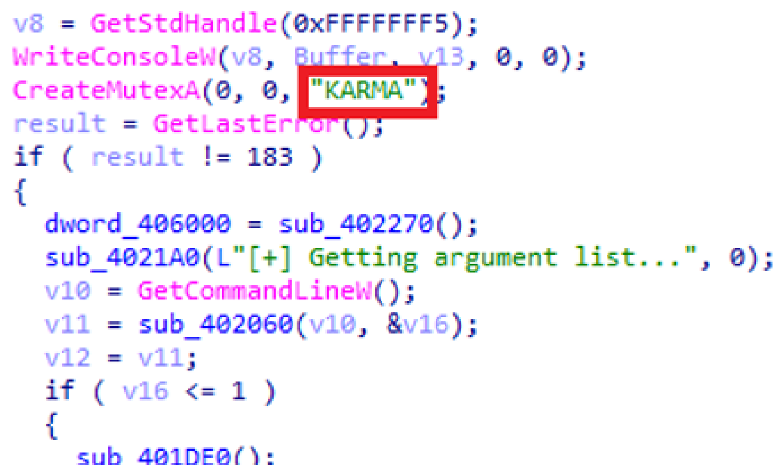


Figure 5 Malware Creates Mutex

The malware payload uses the *crypt32.dll* library, a module used to implement certificate and cryptographic messaging functions in the CryptoAPI, as shown below.

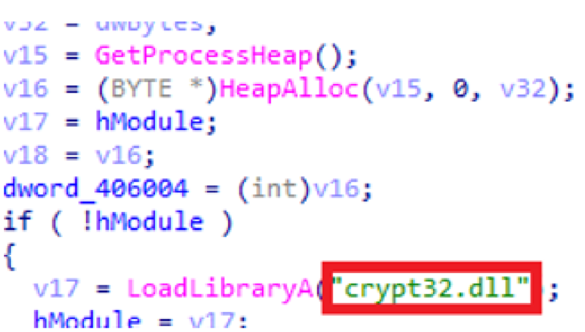


Figure 6 Malware Loads Library crypt32.dll

As shown in Figure 7, the malware payload first gets the command-line string and checks if the argument is less or equal to 1. It then creates threads depending on the logical drive present in the victim machine.

If the argument is greater than 1, the malware checks whether the passed argument is a directory.

If a directory is found, the payload encrypts the directory and its content. Furthermore, if the argument is for any specific file, the malware will start encrypting that file as well.

```
Print((int)L"[+] Getting argument list...", 0);
CommandLineW = (__int16 *)GetCommandLineW();
path_to_specific_directory_or_file = sub_402060(CommandLineW, &lenght_of_argument);
path_to_specific_directory_or_file_2 = (int)path_to_specific_directory_or_file;
if ( lenght_of_argument <= 1 )
{
  ptr_func_ransome_note(a1, a2, (int)path_to_specific_directory_or_file);
  Print((int)L"[+] Starting all threads...", 0);
  sub_403140();
}
else
{
  Print((int)L"   [-] Argument: ", (__int16 *)path_to_specific_directory_or_file[1]);
  if ( check_if_passed_argument_is_directory(*(LPCWSTR *)(path_to_specific_directory_or_file_2 + 4)) )
  {
    ptr_func_ransome_note(a1, a2, path_to_specific_directory_or_file_2);
    sub_401D00((int)Buffer, *(_DWORD *)(path_to_specific_directory_or_file_2 + 4));
    sub_401D20(Buffer, L"\\");
    Print((int)L"[+] Encrypting directory: ", Buffer);
    sub_402A80(Buffer);
  }
  else
  {
    ptr_func_ransome_note(a1, a2, path_to_specific_directory_or_file_2);
    Print((int)L"[+] Encrypting file: ", *(__int16 **)(path_to_specific_directory_or_file_2 + 4));
    func_to_check_enc_write_read(*(LPCWSTR *)(path_to_specific_directory_or_file_2 + 4));
  }
}
ExitProcess(0);
```

Figure 7 Malware Encryption Process

The malware payload iterates through all possible A-Z drives on the Windows machine and verifies if the drives are logical, after which it creates a thread. Refer to Figure 8.

```
v0 = 0;
for ( i = 0; i < 26; ++i )
{
  v10 = '\\\0:';
  RootPathName = i + 'A';
  v11 = 0;
  DriveTypeW = GetDriveTypeW(&RootPathName);
  ProcessHeap = GetProcessHeap();
  v4 = (char *)HeapAlloc(ProcessHeap, 0, 4u);
  v5 = DriveTypeW - 2;
  if ( v5 )
  {
    v6 = v5 - 1;
    if ( v6 )
    {
      if ( v6 != 1 )
        continue;
    }
  }
  *(_WORD *)v4 = RootPathName;
  *(_DWORD *)(v4 + 2) = v10;
  *((_WORD *)v4 + 3) = v11;
  hHandle[v0] = CreateThread(0, 0, StartAddress, v4, 0, 0);
  Sleep(0x1F4u);
  ++v0;
}
```

Figure 8 Malware Verifies the Windows Drives and Creates Thread

The malware excludes the list of folders shown in Table 1 from the encryption routine as shown in Figure 9.

Folders
All Users
Program Files
Program Files x86
Windows
Recycle bin

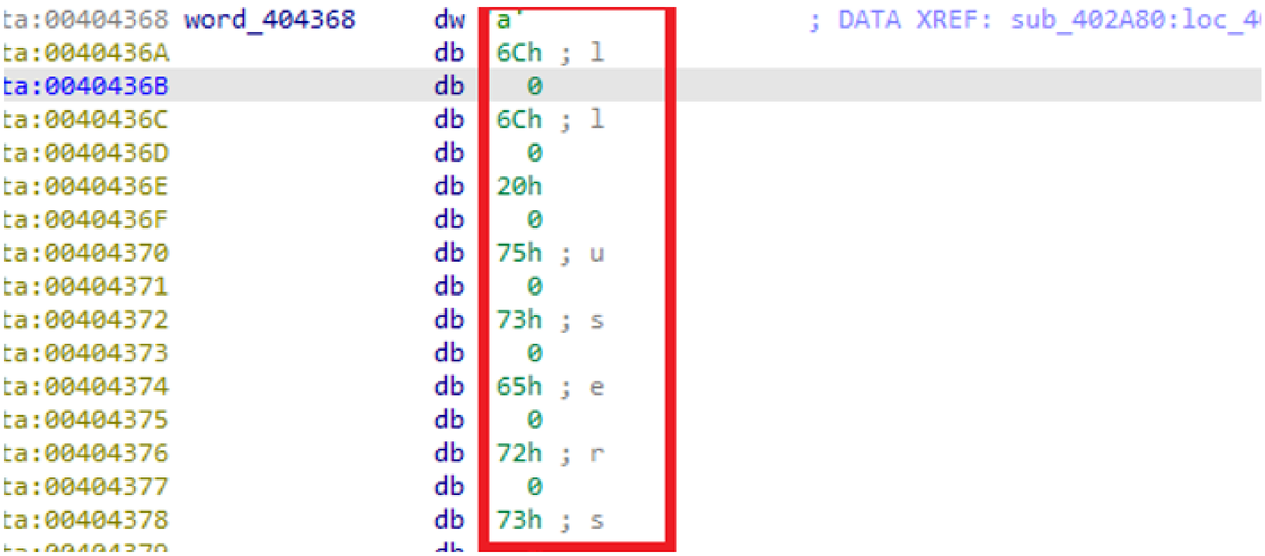


Figure 9 Malware Exclude Folders from Encryption

The malware excludes the list of types of files shown in Table 2 from the encryption routine, as shown in Figure 10.

File Type	Description
.EXE	Executable
.DLL	Dynamic Link Library
.INI	Initialization
.URL	Uniform Resource Locator
.LNK	Link

Table 2 Excluded Files List

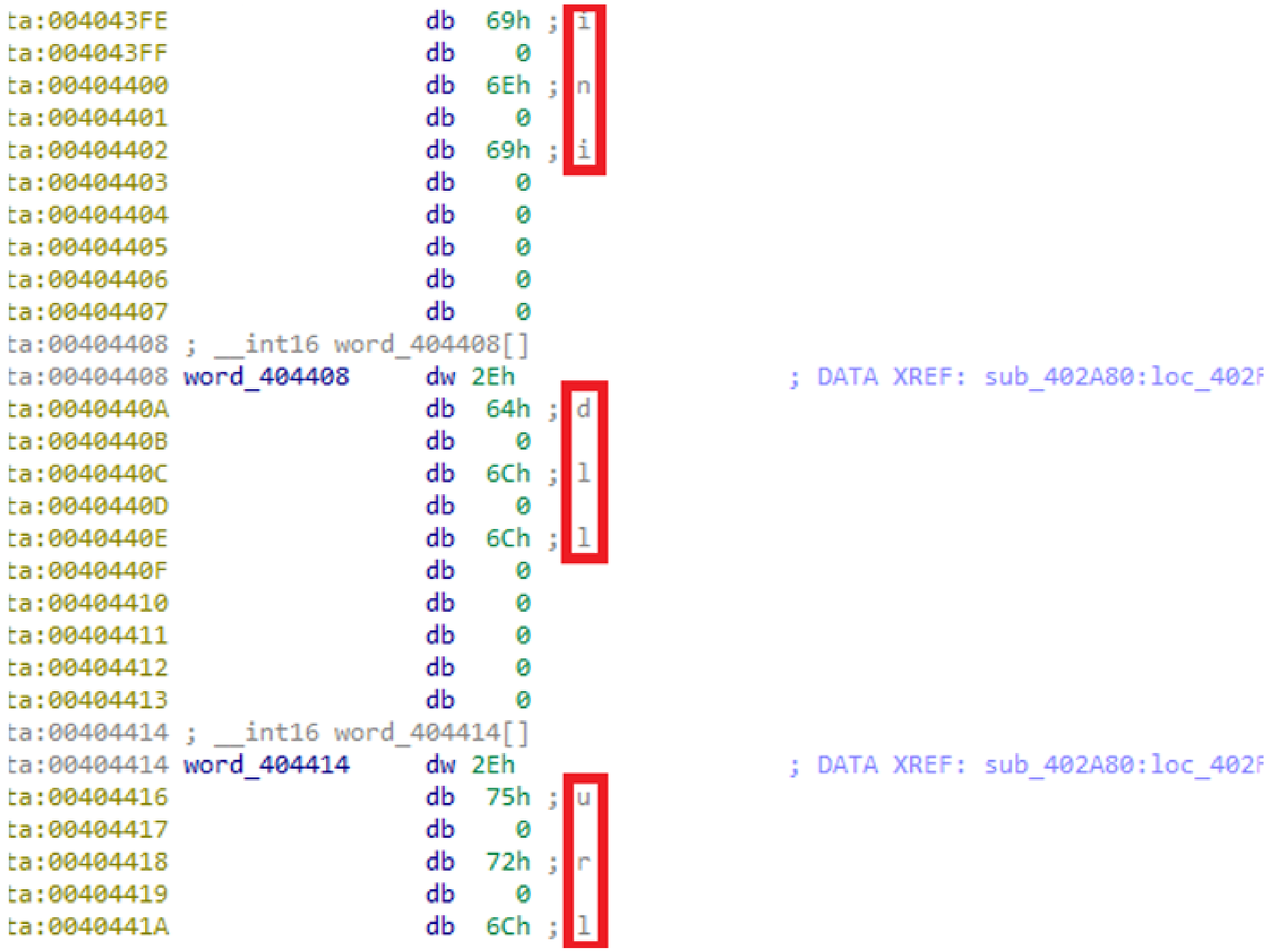


Figure 10 Malware Excludes Files from Encryption

The malware initially searches for folders, for example, *config.Msi* in C drive. If it can successfully locate these folders, it performs further actions, as shown in Figure 11.

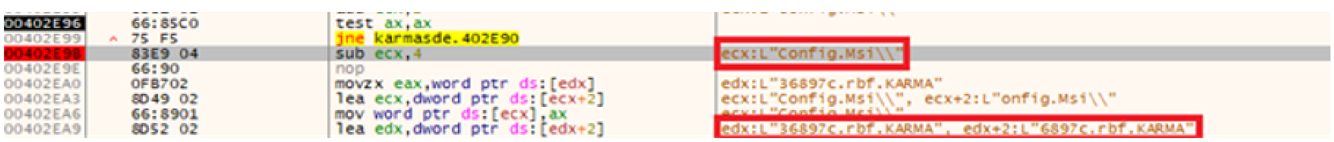


Figure 11 Malware Searches for the Folder

After finding the required folders, the malware creates the ransom note, as shown in Figure 12.

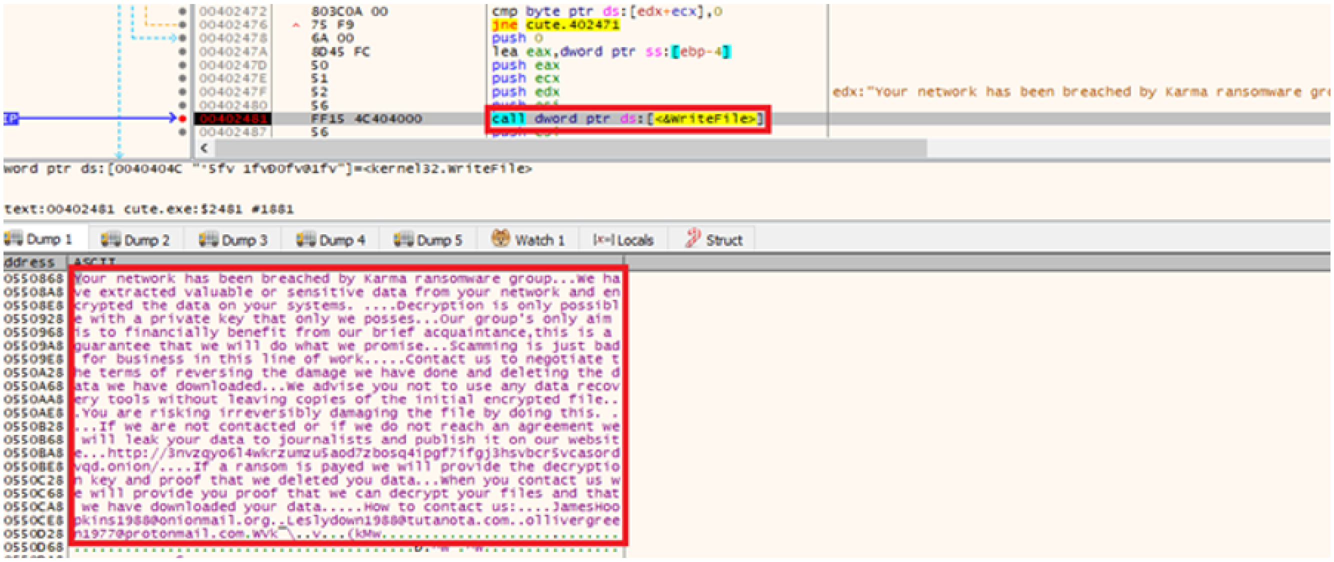


Figure 12 Malware Writes Ransom Note

As seen in Figure 13, the malware generates a seed after creating the ransom note.

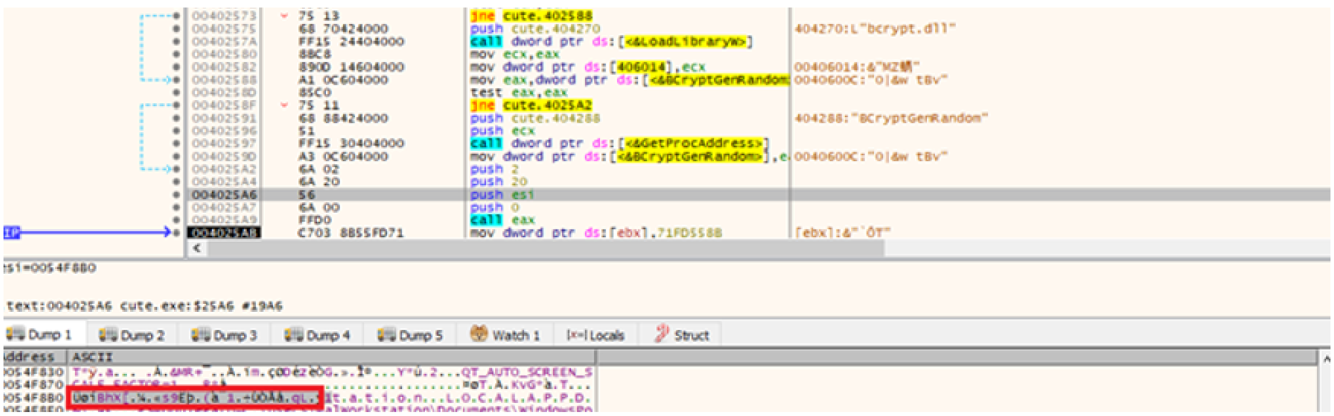


Figure 13 Malware Generates Seed

The malware reads the content and writes encrypted data, as shown in Figure 14.

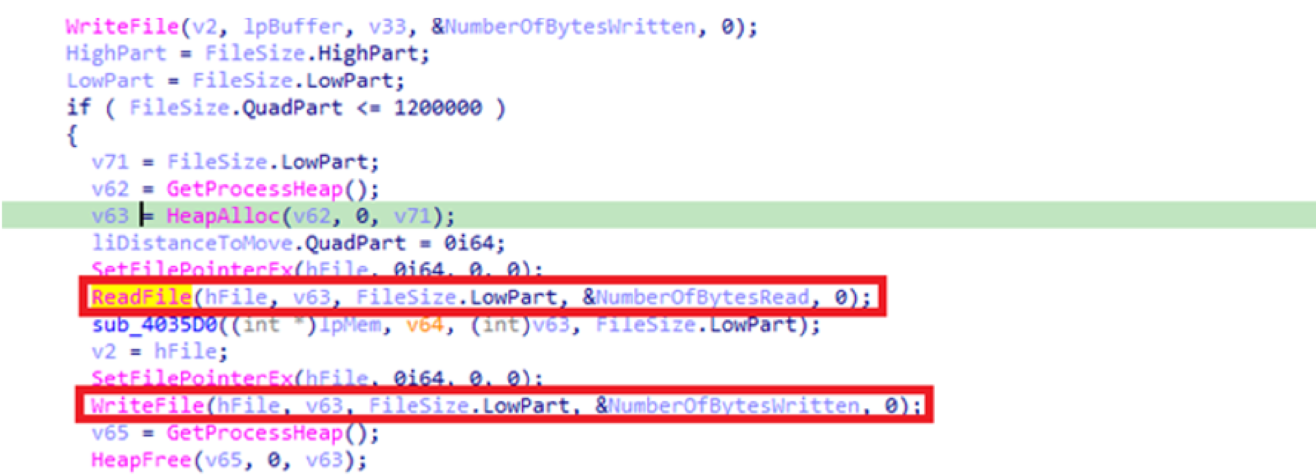


Figure 14 Malware Reads the Content and Writes Encrypted Content

Figure 15 shows the encryption routine performed by the malware.

```
nt __cdecl sub_4035D0(int *a1, int a2, int a3, unsigned int a4)

 int v4; // ecx
 _OWORD *v5; // edx
 int v6; // ecx
 unsigned int v7; // esi
 char v9[64]; // [esp+0h] [ebp-54h] BYREF
 int v10[2]; // [esp+40h] [ebp-14h] BYREF
 __int64 v11; // [esp+48h] [ebp-Ch]
 _OWORD *v12; // [esp+50h] [ebp-4h]

 v5 = (_OWORD *)v4;
 v12 = (_OWORD *)v4;
 v11 = 0i64;
 if ( !v4 || !a1 || !a3 )
   return 1;
 v6 = a1[1];
 v7 = 0;
 v10[0] = *a1;
 for ( v10[1] = v6; v7 < a4; ++v7 )
 {
   if ( (v7 & 0x3F) == 0 )
   {
     LOBYTE(v11) = v7 >> 6;
     BYTE1(v11) = v7 >> 14;
     BYTE2(v11) = v7 >> 22;
     BYTE3(v11) = v7 >> 30;
     sub_403480(v5, (char *)v10, (int)v9);
     v5 = v12;
   }
   *(_BYTE *)(v7 + a3) ^= v9[v7 & 0x3F];
 }
 return 0;
```

Figure 15 Encryption Routine

After encrypting the files, the malware replaces the original content with encrypted content with appended extension as *.KARMA,* as shown in Figure 16.

```
004029CC     66:85C0        test ax,ax
004029CF  ^  75 EF          jne cute.4029C0
004029D1     8D4424 48      lea eax,dword ptr ss:[esp+48]
004029D5     50             push eax                          eax:L"C:\\iDefense\\MAP\\delphi_filter.txt.KARMA"
004029D6     56             push esi                          esi:L"C:\\iDefense\\MAP\\delphi_filter.txt"
004029D7     FF15 6C404000  call dword ptr ds:[<&MoveFileW>]
004029DD     5F             pop edi
004029DE     5E             pop esi                           esi:L"C:\\iDefense\\MAP\\delphi_filter.txt"
004029DF     5B             pop ebx
004029E0     8BE5           mov esp,ebp
```

Figure 16 Malware Replaces Original Content with Encrypted Content

The TOR website *hxxp://3nvzqyo6l4wkrzumzu5aod7zbosq4ipgf7ifgj3hsvbcr5vcasordvqd[.]onion/*shown in Figure 17 was present in the ransom note, in the contact section of the website, TAs have mentioned two email IDs *jeffreyclinton1977@onionmail.org* and *jackiesmith176@protonmail.com*, which the victims can use to communicate with them to recover the data

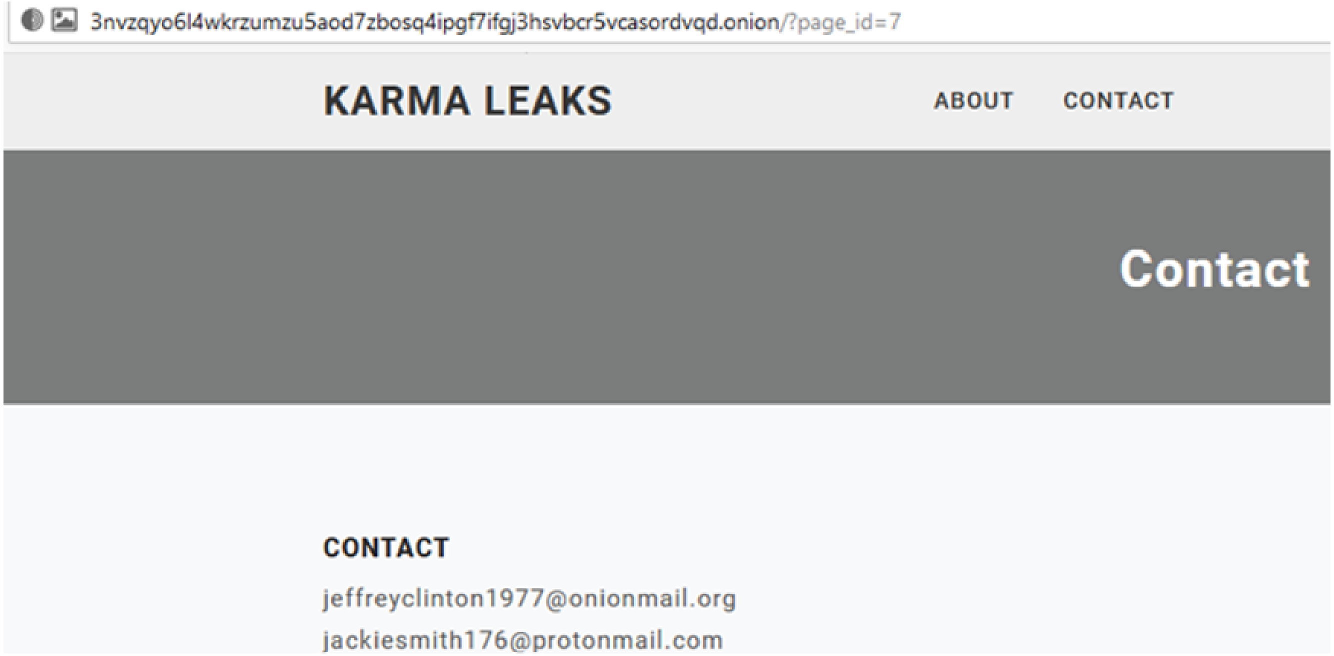


Figure 17 Ransomware Tor Website

Conclusion

Ransomware groups continue to pose a severe threat to firms and individuals. Organizations need to stay ahead of the techniques used by TAs, besides implementing the requisite security best practices and security controls.

Ransomware victims are at risk of losing valuable data as a result of such attacks, resulting in financial loss and lost productivity. In the event that the victim is unable or unwilling to pay the ransom, the TA may leak or sell this data online. This will not only compromise sensitive user data in the case of banks, online shopping portals etc, but it will also lead to a loss of reputation for the affected firm.

Cyble Research Lab is continuously monitoring KARMA's extortion campaign and will keep our readers up to date with new 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 these suggestions given below:

- Conduct regular backup practices and keep those backups offline or on a separate network.
- Regularly perform the vulnerability assessment of the organizational assets majorly which are exposed on internet.
- Refrain from opening untrusted links and email attachments without verifying their authenticity.
- Avoid using software cracks or keygens from torrent or third-party servers.
- 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.

MITRE ATT&CK® Techniques

Tactic	Technique ID	Technique Name
Initialaccess	T1190	Exploit Public-Facing Application
DefenseEvasion	T1112 T1027 T1562.001	Modify Registry Obfuscated Files or Information Impair Defences: Disable or Modify Tools
Discovery	T1083 T1135	File and Directory Discovery Network Share Discovery
Impact	T1486 T1490	Data Encrypted for Impact Inhibit System Recovery

Indicators of Compromise (IoCs):

Indicators	Indicator type	Description
a63937d94b4d0576c083398497f35abc2ed116138bd22fad4aec5714f83371b0	SHA256	HASH
hxxp://3nvzqyo6l4wkrzumzu5aod7zbosq4ipgf7ifgj3hsvbcr5vcasordvqd[.]onion/	URL	URL

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 https://cyble.com.