Threat Thursday: Karma Ransomware

blogs.blackberry.com/en/2021/11/threat-thursday-karma-ransomware

The BlackBerry Research & Intelligence Team

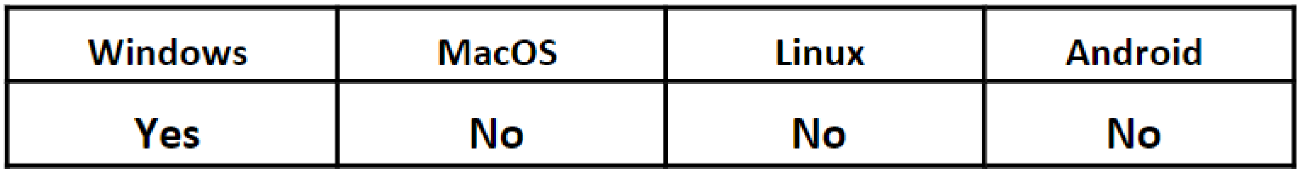
Summary

Karma is fast-acting ransomware designed to quickly encrypt data on compromised machines. In the wild since mid-2021, Karma initially used the stream cipher known as ChaCha20. Recent samples have swapped this out for Salsa20, suggesting the malware is still under development.

The Karma ransom group has created a leak site named “Karma Leaks,” which is hosted via an Onion page. This site has blog-like posts that allude to infiltration of an organization’s network before deploying their ransomware, a technique which allows them to get a better sense of the value of their victim’s data before setting a ransom amount. The group also uses this site as a double-extortion ploy. Affected organizations that refuse to pay the ransom demands or that do not pay within a specific time, have their data published.

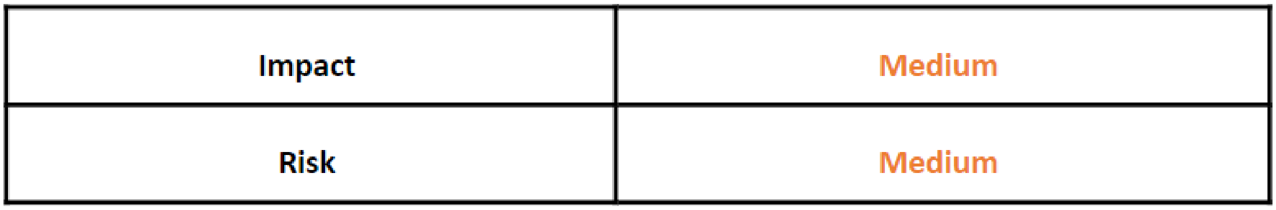
In October 2021, Karma ransomware went through an iterative change, showing rapid advancement including smaller sample-size and shifts in their encryption routine. Files encrypted by the newest version of the ransomware have the file-extension [.KARMA_V2] appended, rather than the initial [.KARMA] file-extension used in a previous version.

Operating System



Windows	MacOS	Linux	Android
Yes	No	No	No

Risk & Impact



Impact	Medium
Risk	Medium

Technical Analysis

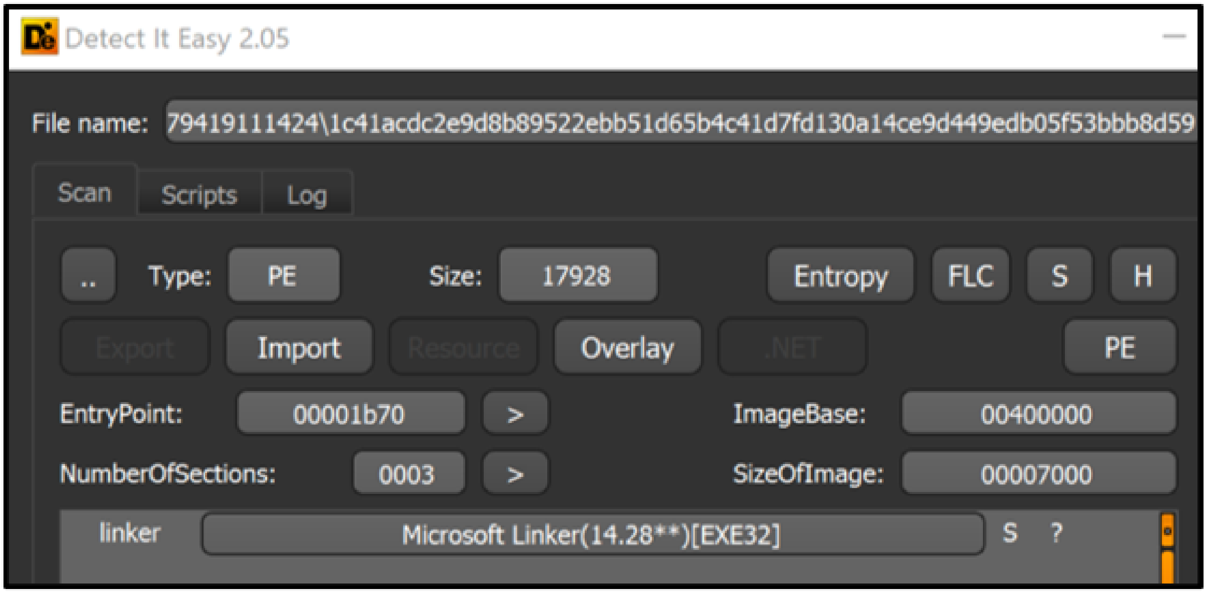
Infection Vector

The infection vector used by the Karma ransomware gang is unknown, but based on initial findings of reconnaissance performed on the victims by the threat group, it appears to vary. Once the group has established a foothold, they likely attempt to move laterally and exfiltrate any data of value. Once reconnaissance and information-stealing has concluded, they execute the Karma ransomware to encrypt victim systems that they have compromised.

File Analysis

The ransomware file itself is small, with samples ranging between 15 KB and 130 KB. Despite their small size, none of the samples found in the wild were packed by digital software packers. The observed samples were all Windows® 32-bit Portable Executables (PE) with a compilation timestamp of 2021. All samples found in the wild were compiled in Microsoft® Visual C++.

Though most samples of Karma are unsigned, lacking digital certificates, at least one known sample was signed with a currently un-revoked digital signature.



File name: 79419111424\1c41acdc2e9d8b89522ebb51d65b4c41d7fd130a14ce9d449edb05f53bbb8d59

Type: PE Size: 17928

EntryPoint: 00001b70 ImageBase: 00400000

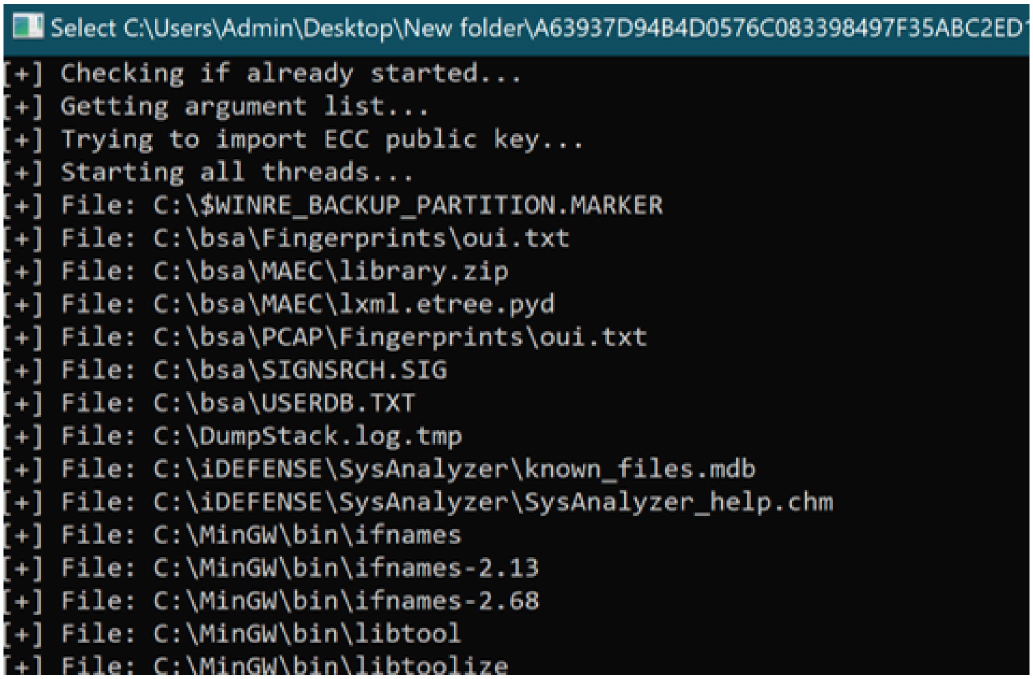
NumberOfSections: 0003 SizeOfImage: 00007000

linker Microsoft Linker(14.28**)[EXE32]

Figure 1: Static information of Karma_V2 sample

As noted, Karma appears to be still under development. BlackBerry has observed a clear lateral progression between initial samples of Karma, leading up to KARMA_V2. Over a short period of time, the samples of Karma that have been analyzed became progressively smaller, shifted their encryption routine, and increased in complexity.

The initial samples of Karma contained a console pop-up box during encryption, meaning an attentive user could attempt to terminate the process before all their data was encrypted. However, given the speed of the malware's encryption routine, it would have been difficult to act quickly enough to keep all data intact.



```
Select C:\Users\Admin\Desktop\New folder\A63937D94B4D0576C083398497F35ABC2ED
[+] Checking if already started...
[+] Getting argument list...
[+] Trying to import ECC public key...
[+] Starting all threads...
[+] File: C:\$WINRE_BACKUP_PARTITION.MARKER
[+] File: C:\bsa\Fingerprints\oui.txt
[+] File: C:\bsa\MAEC\library.zip
[+] File: C:\bsa\MAEC\lxml.etree.pyd
[+] File: C:\bsa\PCAP\Fingerprints\oui.txt
[+] File: C:\bsa\SIGNSRCH.SIG
[+] File: C:\bsa\USERDB.TXT
[+] File: C:\DumpStack.log.tmp
[+] File: C:\iDEFENSE\SysAnalyzer\known_files.mdb
[+] File: C:\iDEFENSE\SysAnalyzer\SysAnalyzer_help.chm
[+] File: C:\MinGW\bin\ifnames
[+] File: C:\MinGW\bin\ifnames-2.13
[+] File: C:\MinGW\bin\ifnames-2.68
[+] File: C:\MinGW\bin\libtool
[+] File: C:\MinGW\bin\libtoolize
```

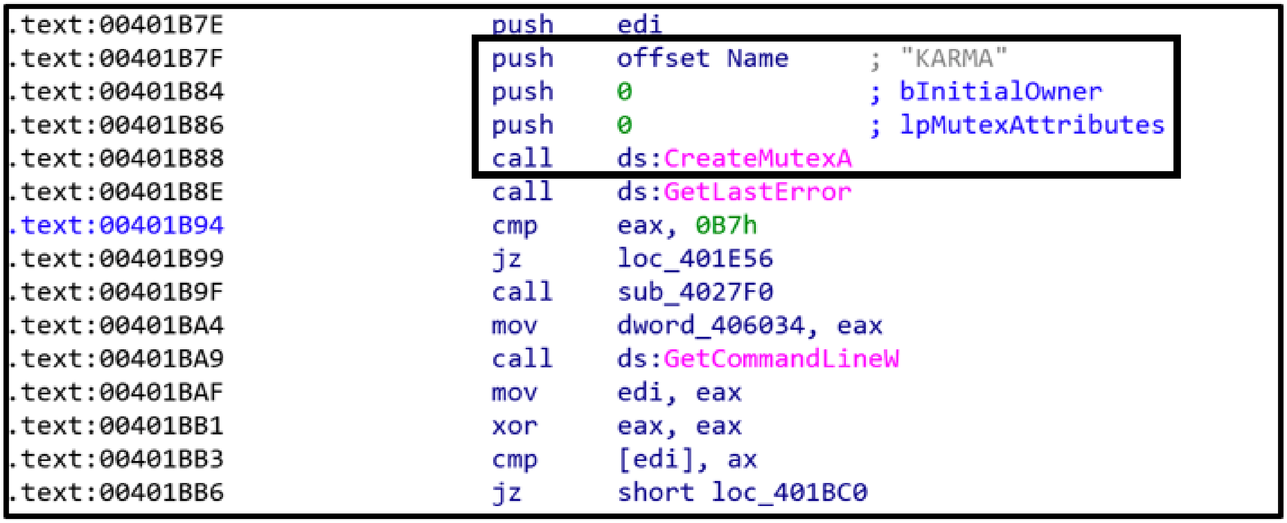
Figure 2: Initial console dialog box of Karma

More recently, samples contain the static string: **Karma_V2**. These samples share a lot of resemblance to the proceeding version, but the initial console box that was once displayed on the victim device is no longer visible. Its speed and method of encryption appear the same.

Karma Mutex

Karma_V2, like the original, initially creates a mutex called “KARMA.” This functions as a buffer to prevent another instance of the ransomware from being executed if one is already running. This is likely done to prevent re-infection, as well as double-encryption that might occur if the ransomware inadvertently executes twice.

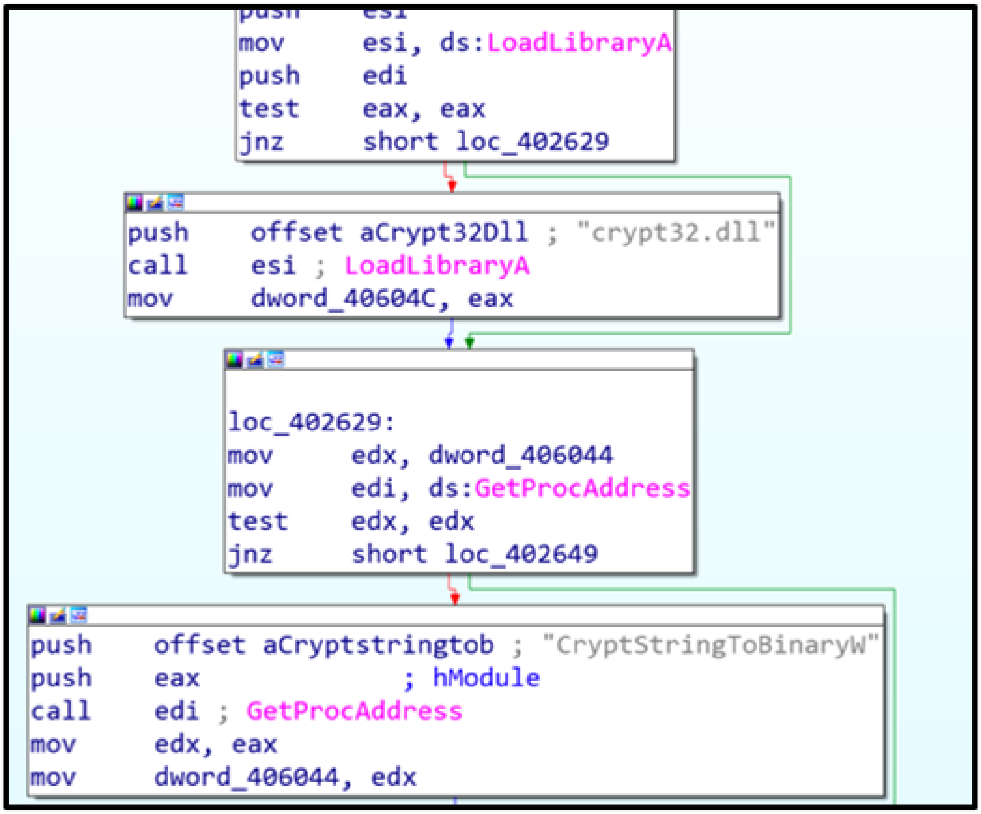
If ransomware were to be executed twice on a system, doubly-encrypted data is likely to become un-recoverable and corrupt. This would defeat the purpose of such malware demanding a payment for decrypting and recovering the user’s data.



```
.text:00401B7E                 push    edi
.text:00401B7F                 push    offset Name     ; "KARMA"
.text:00401B84                 push    0               ; bInitialOwner
.text:00401B86                 push    0               ; lpMutexAttributes
.text:00401B88                 call    ds:CreateMutexA
.text:00401B8E                 call    ds:GetLastError
.text:00401B94                 cmp     eax, 0B7h
.text:00401B99                 jz      loc_401E56
.text:00401B9F                 call    sub_4027F0
.text:00401BA4                 mov     dword_406034, eax
.text:00401BA9                 call    ds:GetCommandLineW
.text:00401BAF                 mov     edi, eax
.text:00401BB1                 xor     eax, eax
.text:00401BB3                 cmp     [edi], ax
.text:00401BB6                 jz      short loc_401BC0
```

Figure 3: Formation of the "KARMA" mutex

Karma calls on the use of crypt32.dll. This Dynamic-Link Library (.DLL) is a native module used to implement cryptographic messaging and certification functions with the Windows CryptoAPI. The DLL is used during encryption.



```
push    esi
mov     esi, ds:LoadLibraryA
push    edi
test    eax, eax
jnz     short loc_402629

push    offset aCrypt32Dll ; "crypt32.dll"
call    esi ; LoadLibraryA
mov     dword_40604C, eax


loc_402629:
mov     edx, dword_406044
mov     edi, ds:GetProcAddress
test    edx, edx
jnz     short loc_402649

push    offset aCryptstringtob ; "CryptStringToBinaryW"
push    eax                ; hModule
call    edi ; GetProcAddress
mov     edx, eax
mov     dword_406044, edx
```

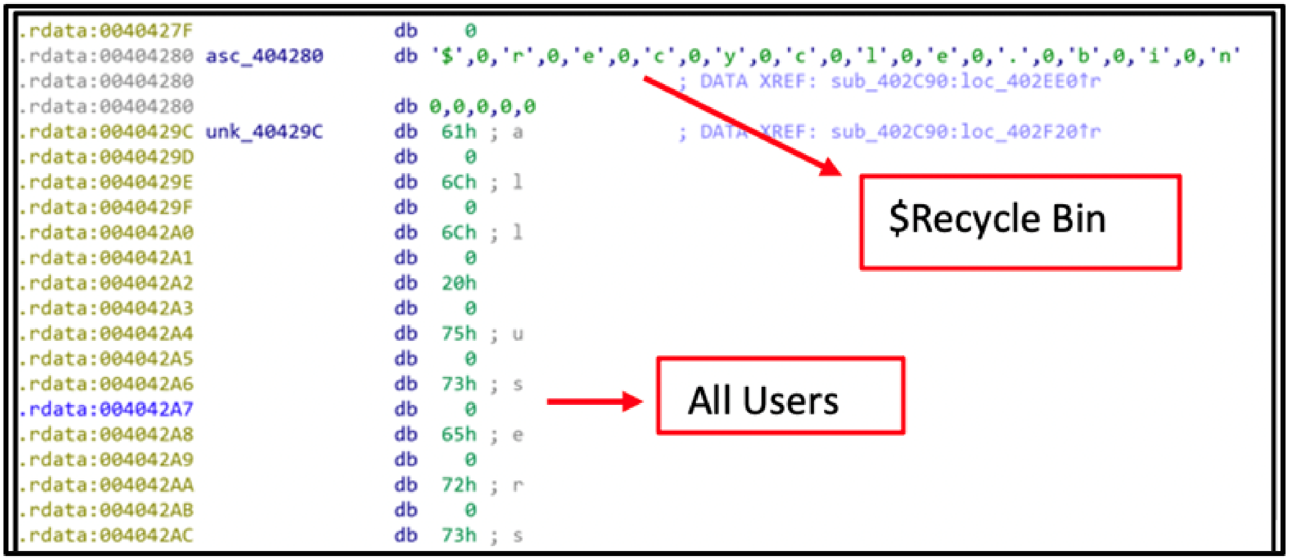
Figure 4: crypt32.dll being loaded

After loading the DLL, the malware will then iterate through all available drives connected to the victim’s device. If a logical drive is identified and verified, the malware will attempt to encrypt its contents.

Encryption

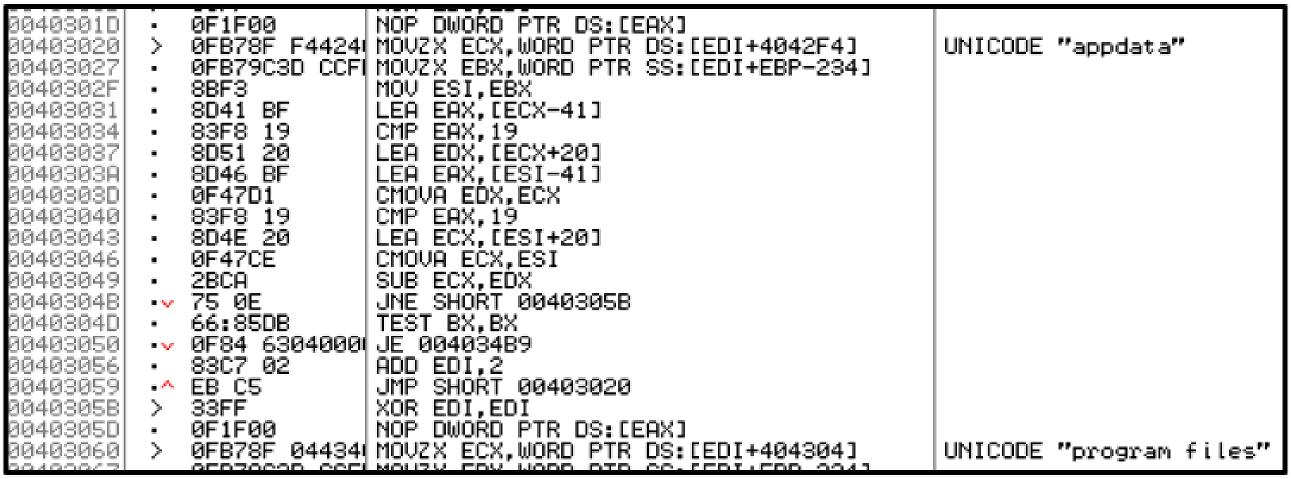
Not all samples of Karma have the same goals. Though they all operate the same, they can target different files and folders.

Karma samples vary in which file-extensions and folders they exclude from encrypting. This information is statically hard-coded into the malware, located in the .rdata section of each sample.



```
.rdata:0040427F                 db    0
.rdata:00404280 asc_404280      db '$',0,'r',0,'e',0,'c',0,'y',0,'c',0,'l',0,'e',0,'.',0,'b',0,'i',0,'n'
.rdata:00404280                                         ; DATA XREF: sub_402C90:loc_402EE0↑r
.rdata:00404280                 db 0,0,0,0,0
.rdata:0040429C unk_40429C      db  61h ; a             ; DATA XREF: sub_402C90:loc_402F20↑r
.rdata:0040429D                 db    0
.rdata:0040429E                 db  6Ch ; l
.rdata:0040429F                 db    0
.rdata:004042A0                 db  6Ch ; l
.rdata:004042A1                 db    0
.rdata:004042A2                 db  20h
.rdata:004042A3                 db    0
.rdata:004042A4                 db  75h ; u
.rdata:004042A5                 db    0
.rdata:004042A6                 db  73h ; s
.rdata:004042A7                 db    0
.rdata:004042A8                 db  65h ; e
.rdata:004042A9                 db    0
.rdata:004042AA                 db  72h ; r
.rdata:004042AB                 db    0
.rdata:004042AC                 db  73h ; s
```

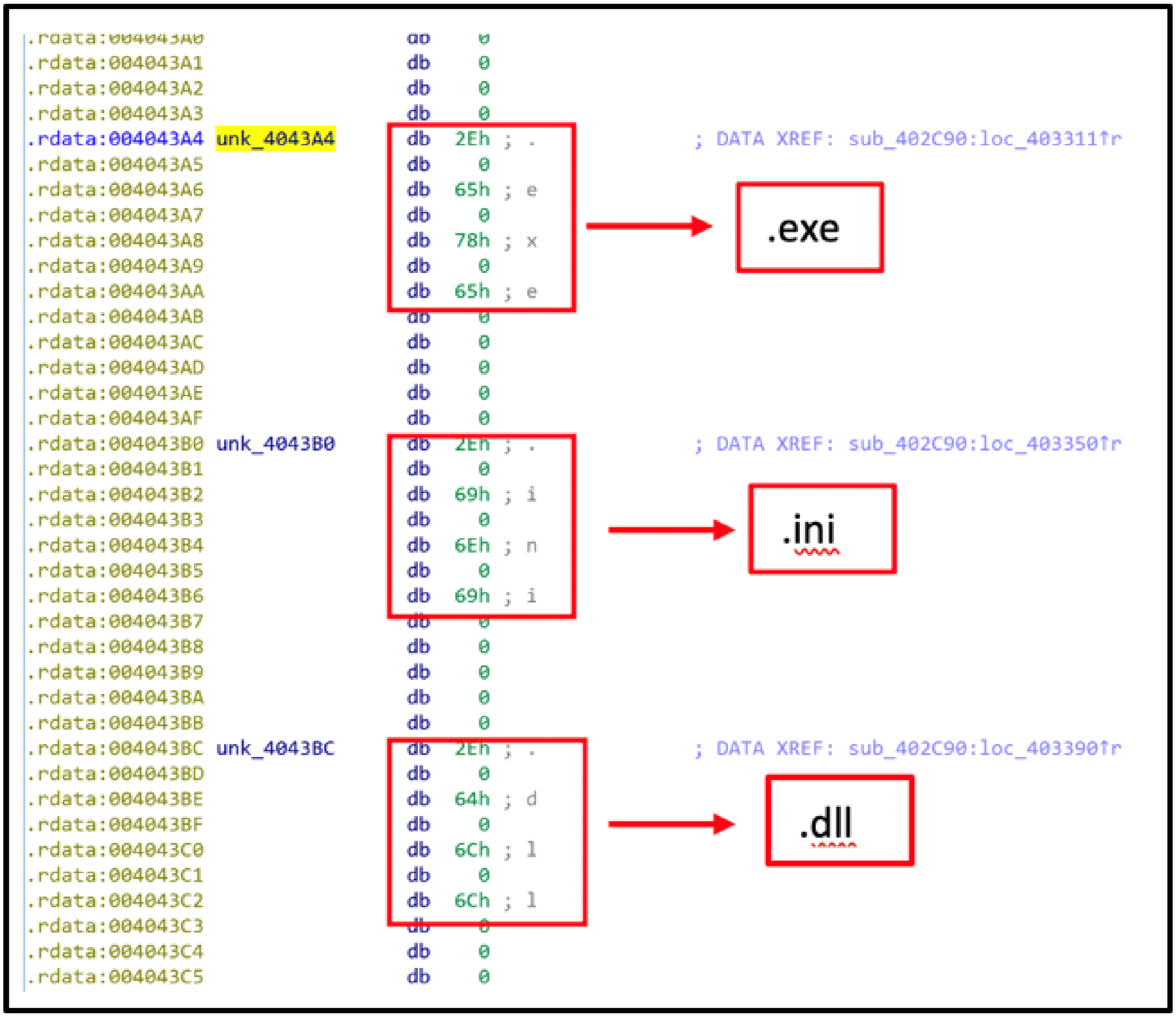
Figure 5: Static references to folder exclusions



```
0040301D  .    0F1F00         NOP DWORD PTR DS:[EAX]
00403020  >    0FB78F F4424(  MOVZX ECX,WORD PTR DS:[EDI+4042F4]     UNICODE "appdata"
00403027  .    0FB79C3D CCF(  MOVZX EBX,WORD PTR SS:[EDI+EBP-234]
0040302F  .    8BF3           MOV ESI,EBX
00403031  .    8D41 BF        LEA EAX,[ECX-41]
00403034  .    83F8 19        CMP EAX,19
00403037  .    8D51 20        LEA EDX,[ECX+20]
0040303A  .    8D46 BF        LEA EAX,[ESI-41]
0040303D  .    0F47D1         CMOVA EDX,ECX
00403040  .    83F8 19        CMP EAX,19
00403043  .    8D4E 20        LEA ECX,[ESI+20]
00403046  .    0F47CE         CMOVA ECX,ESI
00403049  .    2BCA           SUB ECX,EDX
0040304B  .v   75 0E          JNE SHORT 0040305B
0040304D  .    66:85DB        TEST BX,BX
00403050  .v   0F84 6304000(  JE 004034B9
00403056  .    83C7 02        ADD EDI,2
00403059  .^   EB C5          JMP SHORT 00403020
0040305B  >    33FF           XOR EDI,EDI
0040305D  .    0F1F00         NOP DWORD PTR DS:[EAX]
00403060  >    0FB78F 04434(  MOVZX ECX,WORD PTR DS:[EDI+404304]     UNICODE "program files"
```

Figure 6: These exclusions are then used by the malware when executing

These exclusions are likely included to avoid inadvertently encrypting core and critical Windows components.



```
.rdata:004043A0                 db    0
.rdata:004043A1                 db    0
.rdata:004043A2                 db    0
.rdata:004043A3                 db    0
.rdata:004043A4 unk_4043A4      db  2Eh ; .               ; DATA XREF: sub_402C90:loc_403311↑r
.rdata:004043A5                 db    0
.rdata:004043A6                 db  65h ; e
.rdata:004043A7                 db    0
.rdata:004043A8                 db  78h ; x
.rdata:004043A9                 db    0
.rdata:004043AA                 db  65h ; e
.rdata:004043AB                 db    0
.rdata:004043AC                 db    0
.rdata:004043AD                 db    0
.rdata:004043AE                 db    0
.rdata:004043AF                 db    0
.rdata:004043B0 unk_4043B0      db  2Eh ; .               ; DATA XREF: sub_402C90:loc_403350↑r
.rdata:004043B1                 db    0
.rdata:004043B2                 db  69h ; i
.rdata:004043B3                 db    0
.rdata:004043B4                 db  6Eh ; n
.rdata:004043B5                 db    0
.rdata:004043B6                 db  69h ; i
.rdata:004043B7                 db    0
.rdata:004043B8                 db    0
.rdata:004043B9                 db    0
.rdata:004043BA                 db    0
.rdata:004043BB                 db    0
.rdata:004043BC unk_4043BC      db  2Eh ; .               ; DATA XREF: sub_402C90:loc_403390↑r
.rdata:004043BD                 db    0
.rdata:004043BE                 db  64h ; d
.rdata:004043BF                 db    0
.rdata:004043C0                 db  6Ch ; l
.rdata:004043C1                 db    0
.rdata:004043C2                 db  6Ch ; l
.rdata:004043C3                 db    0
.rdata:004043C4                 db    0
.rdata:004043C5                 db    0
```

Figure 7: File extension exclusion list

KARMA (ChaCha20)

SHA1:	a9367f36c1d2d0eb179fd27814a7ab2deba70197
File Size:	127 KB
Excluded Extensions:	• .EXE • .LOG • .BAT • .INI • .URL • .PIF • .MP4 • .MSI • .LNK

Excluded Folder:	• Windows • Program Files • Program Files (x86) • ProgramData
Ransom Extension	.KARMA
Ransom Note:	KARMA-AGREE.txt

KARMA (Salsa20)

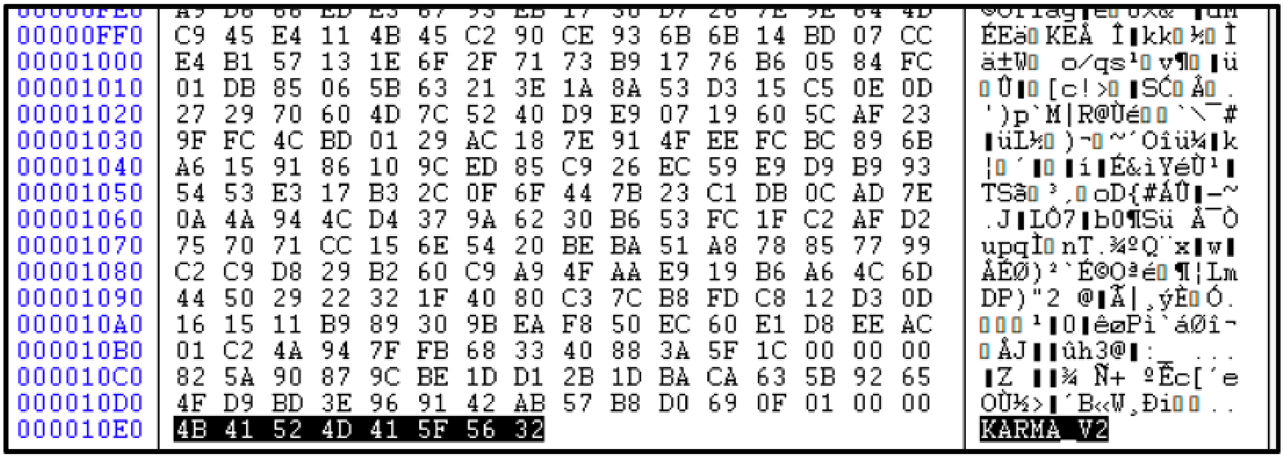
SHA1:	08f1ef785d59b4822811efbc06a94df16b72fea3
File Size:	19 KB
Excluded Extensions:	• .EXE • .INI • .DLL • .URL • .LNK
Excluded Folder:	• Windows • $Recycle Bin • All Users • Default User • Public • ProgramData • AppData • Program Files • Program Files (x86) • Default • System Volume Information • Searches
Ransom Extension:	KARMA
Ransom Note:	KARMA_ENCRYPTED.txt

KARMA_V2

SHA1:	338cff5f17663b7552fb0d687d3b67e9b47fca95
File Size:	18 KB

Excluded Extensions:	- .EXE - .INI - .DLL - .URL - .LNK
Excluded Folder:	- Windows - $Recycle Bin - All Users - Default User - Public - AppData - ProgramData - Program Files - Program Files (x86) - Default - System Volume Information - Searches
Ransom Extension:	KARMA_V2
Ransom Note:	KARMA_V2_ENCRYPTED.txt

Once files are passed through the malware encryption routine, and the file-extension has been appended, the malware will add the 8 bytes of data shown below to signify successful encryption.

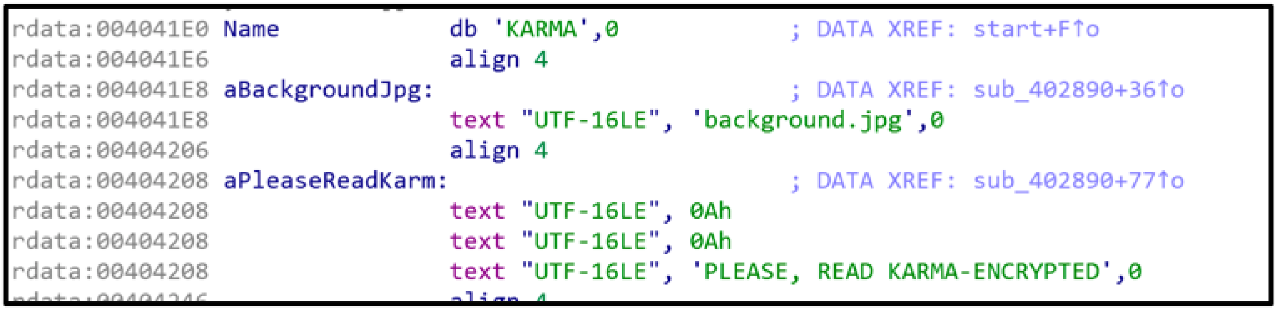


```
00000FF0  C9 45 E4 11 4B 45 C2 90 CE 93 6B 6B 14 BD 07 CC   ÉEä▯KEÂ Î▮kk▯½▯Ì
00001000  E4 B1 57 13 1E 6F 2F 71 73 B9 17 76 B6 05 84 FC   ä±W▯ o/qs¹▯v¶▯▮ü
00001010  01 DB 85 06 5B 63 21 3E 1A 8A 53 D3 15 C5 0E 0D   ▯Û▮▯[c!>▯▮SÓ▯Å▯.
00001020  27 29 70 60 4D 7C 52 40 D9 E9 07 19 60 5C AF 23   ')p`M|R@Ùé▯▯`\¯#
00001030  9F FC 4C BD 01 29 AC 18 7E 91 4F EE FC BC 89 6B   ▮üL½▯)¬▯~´Oîü¼▮k
00001040  A6 15 91 86 10 9C ED 85 C9 26 EC 59 E9 D9 B9 93   ¦▯´▮▯▮í▮É&ìYéÙ¹▮
00001050  54 53 E3 17 B3 2C 0F 6F 44 7B 23 C1 DB 0C AD 7E   TSã▯³,▯oD{#ÁÛ▮-~
00001060  0A 4A 94 4C D4 37 9A 62 30 B6 53 FC 1F C2 AF D2   .J▮LÔ7▮b0¶Sü Â¯Ò
00001070  75 70 71 CC 15 6E 54 20 BE BA 51 A8 78 85 77 99   upqÌ▯nT ¾ºQ¨x▮w▮
00001080  C2 C9 D8 29 B2 60 C9 A9 4F AA E9 19 B6 A6 4C 6D   ÂÉØ)²`É©Oªé▯¶¦Lm
00001090  44 50 29 22 32 1F 40 80 C3 7C B8 FD C8 12 D3 0D   DP)"2 @▮Ã|¸ýÈ▯Ó.
000010A0  16 15 11 B9 89 30 9B EA F8 50 EC 60 E1 D8 EE AC   ▯▯▯¹▮0▮êøPì`áØî¬
000010B0  01 C2 4A 94 7F FB 68 33 40 88 3A 5F 1C 00 00 00   ▯ÂJ▮▮ûh3@▮:_ ...
000010C0  82 5A 90 87 9C BE 1D D1 2B 1D BA CA 63 5B 92 65   ▮Z ▮▮¾ Ñ+ ºÊc[´e
000010D0  4F D9 BD 3E 96 91 42 AB 57 B8 D0 69 0F 01 00 00   OÙ½>▮´B«W¸Ði▯▯..
000010E0  4B 41 52 4D 41 5F 56 32                           KARMA_V2
```

Figure 8: File encrypted by Karma_V2

Background Change

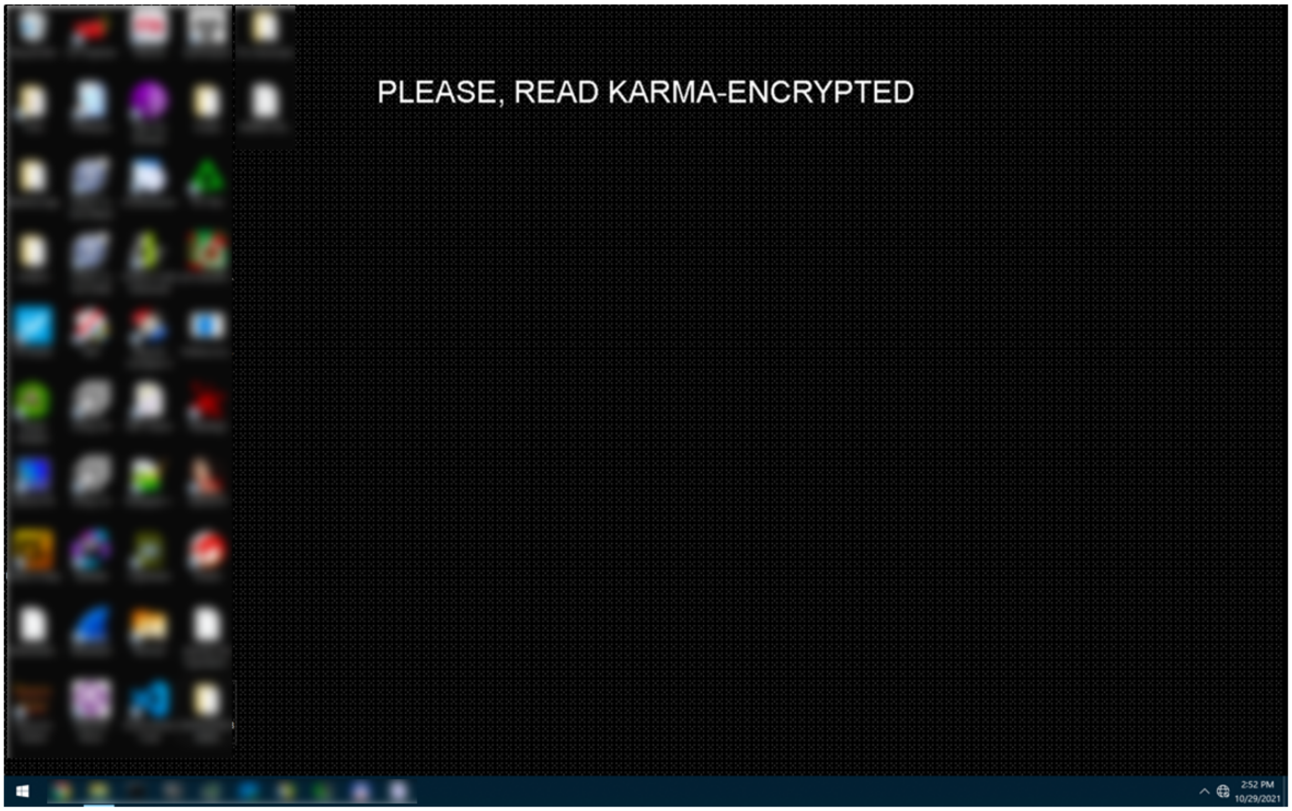
In all samples of Karma ransomware analyzed to date, once encryption is completed, the malware creates a file called “background.jpg.” This file is generated and stored in the %Temp% directory.



```
rdata:004041E0 Name            db 'KARMA',0           ; DATA XREF: start+F↑o
rdata:004041E6                 align 4
rdata:004041E8 aBackgroundJpg:                        ; DATA XREF: sub_402890+36↑o
rdata:004041E8                 text "UTF-16LE", 'background.jpg',0
rdata:00404206                 align 4
rdata:00404208 aPleaseReadKarm:                       ; DATA XREF: sub_402890+77↑o
rdata:00404208                 text "UTF-16LE", 0Ah
rdata:00404208                 text "UTF-16LE", 0Ah
rdata:00404208                 text "UTF-16LE", 'PLEASE, READ KARMA-ENCRYPTED',0
rdata:00404246                 align 4
```

Figure 9: Creating 'background.jpg'

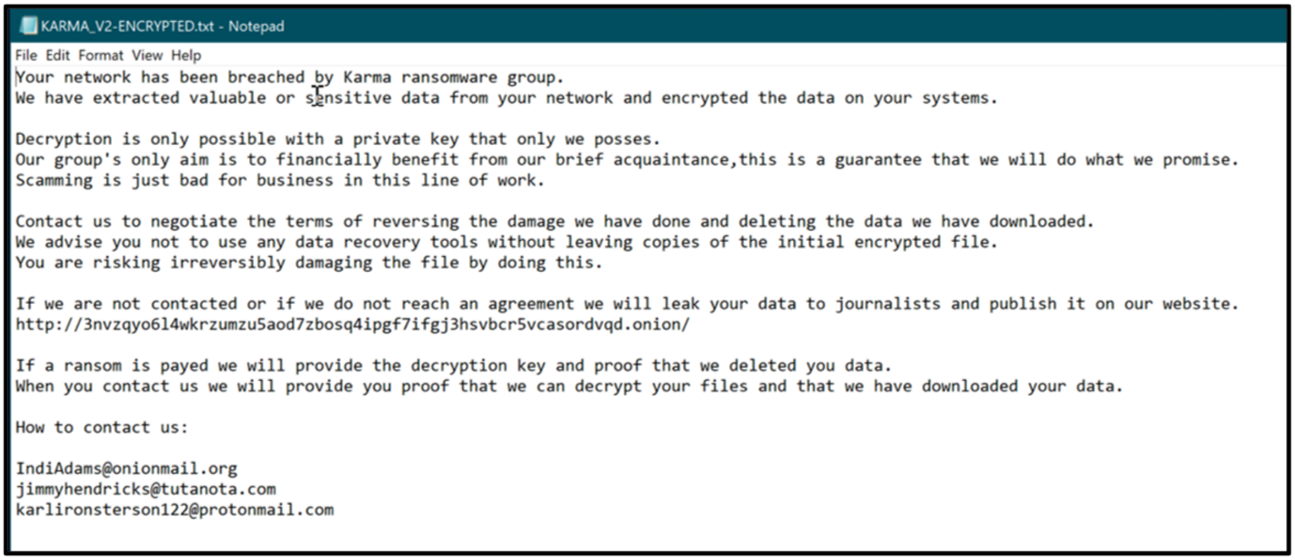
Once the malware has carried out its encryption, it will change the victim's desktop image as shown below.



PLEASE, READ KARMA-ENCRYPTED

Figure 10: System affected by Karma

Ransom Note



```
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:

IndiAdams@onionmail.org
jimmyhendricks@tutanota.com
karlironsterson122@protonmail.com
```

Figure 11: Example of Karma ransom note

There are few deviations in the Karma ransom note. However, the formatting is generally the same across all versions.

Typically, the contents of these notes are Base-64 encoded and contained within the file's static strings. The contents are decoded into memory before being placed into the text file KARMA-ENCRYPTED.txt or KARMA-AGREE.txt. These ransom notes are created and dropped in all folders where the malware has encrypted files.

The note contains an Onion link to the threat actor's leak site. It also contains unique email addresses related to that specific sample of Karma.

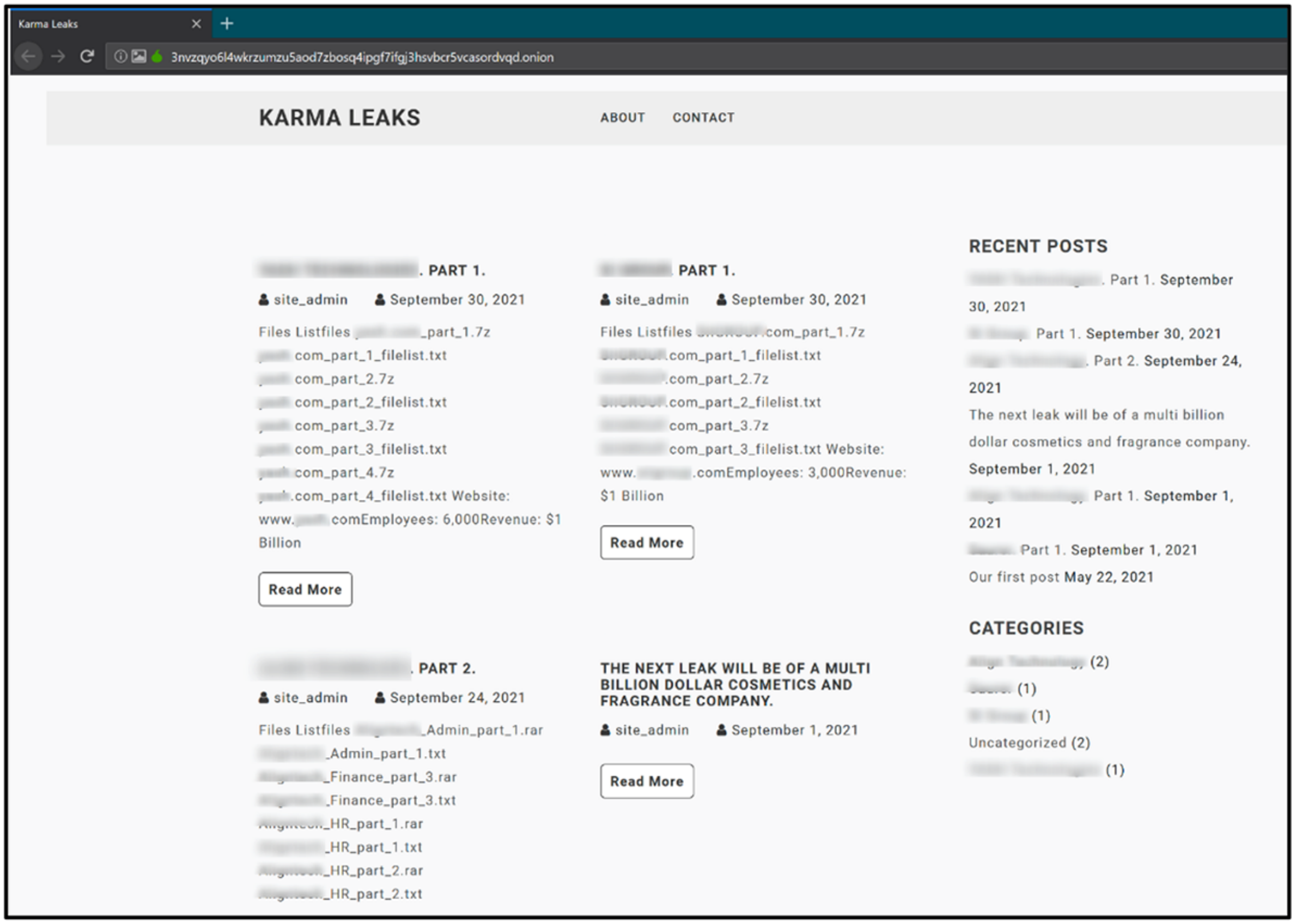
These addresses often follow a pattern of containing at least one of each of the following email services:

- OnionMail
- Tutanota
- ProtonMail

Leak Site

While other prevalent ransomware threats have been observed selling their malicious code to other threat actors as Ransomware-as-a-Service offerings, Karma appears to be used solely by its own creators.

Since Karma began posting to its Onion webpage in May 2021, the ransomware threat actors have been busy populating their basic WordPress site with the names and data of victims who have refused to pay their ransom.


Karma Leaks
3nvzqyo6l4wkrzumzu5aod7zbosq4ipgf7ifgj3hsvbcr5vcasordvqd.onion

KARMA LEAKS

ABOUT CONTACT

[redacted]. PART 1.

site_admin September 30, 2021

Files Listfiles [redacted]_part_1.7z
[redacted] com_part_1_filelist.txt
[redacted] com_part_2.7z
[redacted] com_part_2_filelist.txt
[redacted] com_part_3.7z
[redacted] com_part_3_filelist.txt
[redacted] com_part_4.7z
[redacted].com_part_4_filelist.txt Website:
www.[redacted] comEmployees: 6,000Revenue: $1
Billion

Read More

[redacted] PART 1.

site_admin September 30, 2021

Files Listfiles [redacted]com_part_1.7z
[redacted].com_part_1_filelist.txt
[redacted].com_part_2.7z
[redacted].com_part_2_filelist.txt
[redacted] com_part_3.7z
[redacted] com_part_3_filelist.txt Website:
www.[redacted].comEmployees: 3,000Revenue:
$1 Billion

Read More

[redacted]. PART 2.

site_admin September 24, 2021

Files Listfiles [redacted]_Admin_part_1.rar
[redacted]_Admin_part_1.txt
[redacted]_Finance_part_3.rar
[redacted]_Finance_part_3.txt
[redacted]_HR_part_1.rar
[redacted]_HR_part_1.txt
[redacted]_HR_part_2.rar
[redacted]_HR_part_2.txt

THE NEXT LEAK WILL BE OF A MULTI BILLION DOLLAR COSMETICS AND FRAGRANCE COMPANY.

site_admin September 1, 2021

Read More

RECENT POSTS

[redacted]. Part 1. September 30, 2021
[redacted]. Part 1. September 30, 2021
[redacted]. Part 2. September 24, 2021
The next leak will be of a multi billion dollar cosmetics and fragrance company. September 1, 2021
[redacted]. Part 1. September 1, 2021
[redacted]. Part 1. September 1, 2021
Our first post May 22, 2021

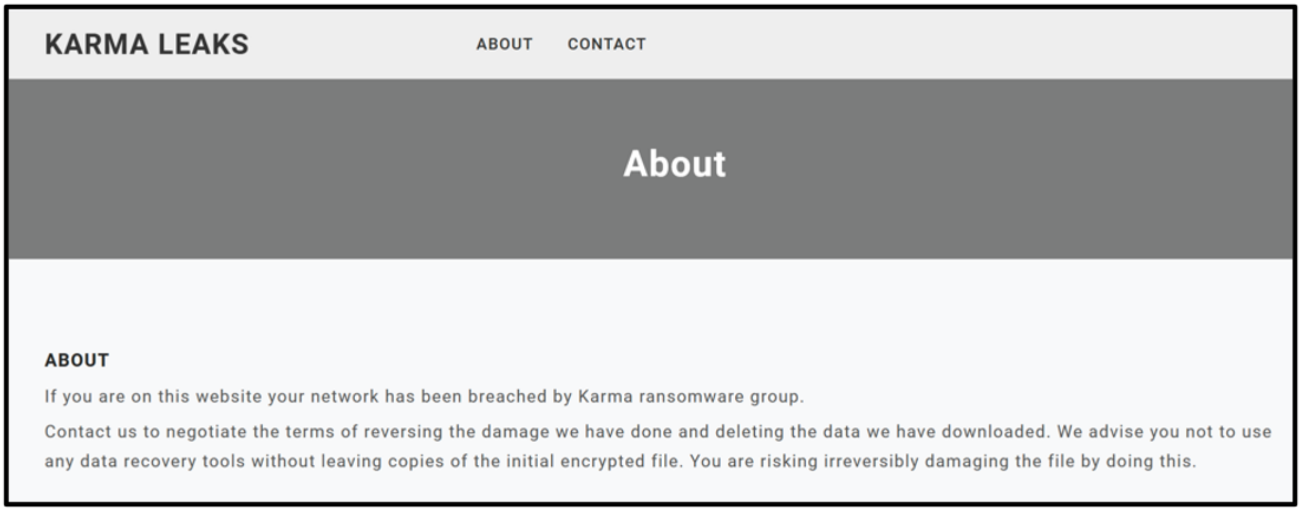
CATEGORIES

[redacted] (2)
[redacted] (1)
[redacted] (1)
Uncategorized (2)
[redacted] (1)

Figure 12: Current content of “Karma Leaks” website (redacted)

As of November 2021, the site hosts the data of four victims who have not engaged or contacted the group and therefore have had their data publicly leaked. Each post shown in Figure 12 contains multiple links to download confidential information stolen by the threat actors. The site suggests that these “double-extortion” posts would be removed if a fee is paid, which means that the true number of victims who have fallen to Karma may extend beyond this initial tally.

It appears that the Karma ransomware gang tends to target large multinational organizations; in particular, those with more than 1,000 employees and around $1 billion in revenue.



KARMA LEAKS

ABOUT CONTACT

About

ABOUT

If you are on this website your network has been breached by Karma ransomware group.

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.

Figure 13: Karma leak site’s “About” page text

Karma’s website has a few blog-like posts about potential victims they intend to leak data from soon, and further ways to contact the gang. The “About" page shares a few additional pieces of information, as seen in Figure 13.

Neither the ransom note nor the website publicly discloses a specific ransom amount. Typically, ransomware would immediately demand a victim-specific fee or a flat-rate fee for the decryption of files.

As the Karma ransomware gang likely infiltrates organizations directly, as opposed to an RaaS model, fees could vary based on not just on the damage caused by the ransomware, but on the victim’s ability to pay and criticality of the affected data.

Conclusion

Karma ransomware is a quickly evolving and ruthless operation. Though Karma shares a lot of similarities with other known ransomware families, its rapid development and advancement in techniques makes both the malware and the threat actor behind it extremely dangerous. The use of “Karma Leaks” as a double-extortion ploy shows the threat group’s willingness to expose victims who do not pay.

With both the activity on “Karma Leaks” and the development of KARMA_V2, it appears this threat actor is spinning up its operations, and that it is actively looking for large organizations to target next.

YARA Rule

The following YARA rule was authored by the BlackBerry Research & Intelligence Team to catch the threat described in this document:

```
import "pe"

rule Mal_Ransom_Win32_Karma_2021
{
    meta:
        description = "Detects Karma Ransomware 2021"
        author = "Blackberry Threat Research Team "
        date = "2021-10"
license = "This Yara rule is provided under the Apache License 2.0
(https://www.apache.org/licenses/LICENSE-2.0) and open to any user or organization, as long as
you use it under this license and ensure originator credit in any derivative to The BlackBerry
Research & Intelligence Team"

    strings:
                        $s1 =
"WW91ciBuZXR3b3JrIGhhcyBiZWVuIGJyZWFjaGVkIGJ5IEthcm1hIHJhbnNvbXdhcmUgZ3JvdXAu"
ascii wide
                        $x2 = "crypt32.dll" nocase
                        $x3 = "KARMA" ascii wide
                        $x4 = "Sleep" nocase

      condition:

        //PE File
        uint16(0) == 0x5a4d and

        //Base64 Karma Note
        all of ($s*) and

        //All Strings
                        all of ($x*)
}
```

Indicators of Compromise (IoCs)

Ransom Note:
KARMA-AGREE.txt
KARMA-ENCRYPTED.txt

Encrypted Files:
*.KARMA
*.KARMA_V2

Mutex:
Global\KARMA

Malware Digital Cert:
Serial: {00 C4 CD EE EB 36 88 DA 08 1F 95 D6 AA 33 7E 93 D1}

Payment Email IoC's:
JamesHoopkins1988[@]onionmail[.]com
Leslydown1988[@]tutanota[.]com
ollivergreen1977[@]protomail[.]com
IndiAdams[@]onionmail[.]org
Jimmyhendricks[@]tutanota[.]com
karlironsterson122[@]protomail[.]com

Leak Site:
hxxp://3nvzqyo6l4wkrzumzu5aod7zbosq4ipgf7ifgj3hsvbcr5vcasordvqd[.]onion/
SHA256:
KARMA_V2
1c41acdc2e9d8b89522ebb51d65b4c41d7fd130a14ce9d449edb05f53bbb8d59
6c98d424ab1b9bfba683eda340fef6540ffe4ec4634f4b95cf9c70fe4ab2de90

KARMA
0d037ee0252e4f26800bcf7c750f61d0c549b7ba0a522c75e8d96dcf4f689e27
84d24a16949b5a89162411ab98ab2230128d8f01a3d3695874394733ac2a1dbd
124f3a5caf6eb464027f2865225a6a1238c3639e5b4a399f0f7f2dda7bd75aec
3ff1b90dbad5d78397fdc731c3a3c080d91fc488ac9152793b538b74a1e2d8f3
ad841882052c3f9d856ad9a393232e0a59d28e17c240d23258f1dac62f903ab8
19417c0a38a1206007a0cc82c0fc2e19db897214d27d0998bc4dbac53cc2788d
a63937d94b4d0576c083398497f35abc2ed116138bd22fad4aec5714f83371b0
34629751d8202be456dcf149b516afefc980a9128dd6096fd6286fee530a0d20

BlackBerry Assistance

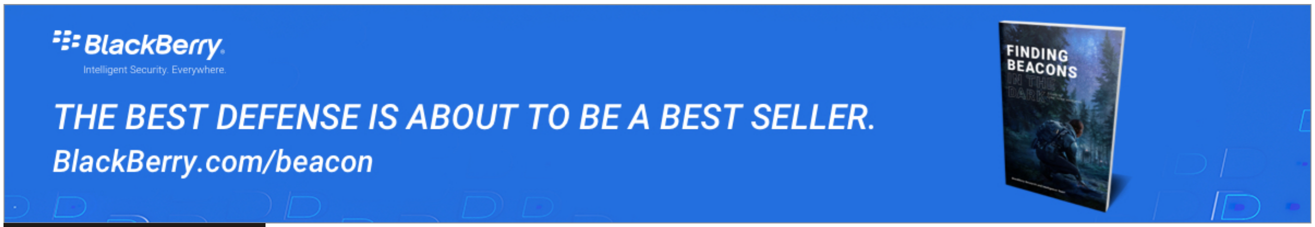
If you're battling this malware or a similar threat, you've come to the right place, regardless of your existing BlackBerry relationship.

The BlackBerry Incident Response team is made up of world-class consultants dedicated to handling response and containment services for a wide range of incidents, including ransomware and Advanced Persistent Threat (APT) cases.

We have a global consulting team standing by to assist you providing around-the-clock support, where required, as well as local assistance. Please contact us here:

https://www.blackberry.com/us/en/forms/cylance/handraiser/emergency-incident-response-containment

Want to learn more about cyber threat hunting? Check out the BlackBerry Research & Intelligence Team's new book, Finding Beacons in the Dark: A Guide to Cyber Threat Intelligence, now available for pre-order ***here.***


BlackBerry
Intelligent Security. Everywhere.
THE BEST DEFENSE IS ABOUT TO BE A BEST SELLER.
BlackBerry.com/beacon
FINDING BEACONS

About The BlackBerry Research & Intelligence Team

The BlackBerry Research & Intelligence team examines emerging and persistent threats, providing intelligence analysis for the benefit of defenders and the organizations they serve.

Back