SentinelLABS

Karma Ransomware | An Emerging Threat With A Hint of Nemty Pedigree

ANTONIS TEREFOS / OCTOBER 18, 2021

Karma is a relatively new ransomware threat actor, having first been observed in June of 2021. The group has targeted numerous organizations across different industries. Reports of a group with the same name from 2016 are not related to the actors currently using the name. An initial technical analysis of a single sample related to Karma was published by researchers from Cyble in August.

In this post, we take a deeper dive, focusing on the evolution of Karma through multiple versions of the malware appearing through June 2021. In addition, we explore the links between Karma and other well known malware families such as NEMTY and JSWorm and offer an expanded list of technical indicators for threat hunters and defenders.

Initial Sample Analysis

Karma's development has been fairly rapid and regular with updated variants and improvements, oftentimes building multiple versions on the same day. The first few Karma samples our team observed were:

Sample 1: `d9ede4f71e26f4ccd1cb96ae9e7a4f625f8b97c9`

Sample 2: `a9367f36c1d2d0eb179fd27814a7ab2deba70197`

Sample 3: `9c733872f22c79b35c0e12fa93509d0326c3ec7f`

Sample 1 was compiled on 18th, June 2021 and Samples 2 and 3 the following day on the 19th, a few minutes apart. Basic configuration between these samples is similar, though there are some slight differences such as PDB paths.

After Sample 1, we see more of the core features appear, including the writing of the ransom note. Upon execution, these payloads would enumerate all local drives (A to Z) , and encrypt files where possible.

Further hunting revealed a number of other related samples all compiled within a few days of each other. The following table illustrates compilation timestamps and payload size across versions of Karma compiled in a single week. Note how the payload size decreases as the authors' iterate.

Karma Malware	Compilation Timestamp (UTC)	Size (hex-bytes)
Sample 1	18/06/2021, 20:16:46	0x1fc00
Sample 2	19/06/2021, 20:48:52	0x1fbc8
Sample 3	19/06/2021, 20:50:15	0x1dc00
Sample 4	19/06/2021, 20:55:23	0x1dc00
Sample 5	21/06/2021, 18:50:53	0x4200
Sample 6	24/06/2021, 00:08:43	0x4a00
Sample 7	24/06/2021, 00:10:43	0x4a00
Sample 8	25/06/2021, 16:59:29	0x4a00

Ransom Note is not Created in Sample 1.

Also, the list of excluded extensions is somewhat larger in Sample 1 than in both Samples 2 and 3, and the list of extensions is further reduced from Sample 5 onwards to only exclude “.exe”, “.ini”, “.dll”, “.url” and “.lnk”.

Karma Malware	Excluded Extensions	Excluded Folders
Sample 1	'.exe', '.log', '.cab', '.cmd', '.bat', '.com', '.cpl', '.ini', '.dll', '.url', '.ttf', '.mp3', '.pif', '.mp4', '.msi', '.lnk'	'windows', '$recycle.bin', 'all users', 'rsa', 'programdata', 'appdata', 'program files', 'program files (x86)'
Sample 2	'.exe', '.log', '.bat', '.ini', '.dll', '.url', '.pif', '.mp4', '.msi', '.lnk', '.KARMA'	'Windows', 'Program Files (x86)', 'Program Files', 'ProgramData'
Sample 3	'.exe', '.log', '.bat', '.ini', '.dll', '.url', '.pif', '.mp4', '.msi', '.lnk', '.KARMA'	'Windows', 'Program Files (x86)', 'Program Files', 'ProgramData'
Sample 4	'.exe', '.log', '.bat', '.ini', '.dll', '.url', '.pif', '.mp4', '.msi', '.lnk', '.KARMA'	'Windows', 'Program Files (x86)', 'Program Files', 'ProgramData'
Sample 5	'.exe', '.ini', '.dll', '.url', '.lnk', 'KARMA'	'windows', '$recycle.bin', '', 'all users', 'rsa', 'programdata', 'appdata', 'program files', 'program files (x86)'
Sample 6	'.exe', '.ini', '.dll', '.url', '.lnk', 'KARMA'	'windows', '$recycle.bin', 'all users', 'default user', 'public', 'programdata', 'appdata', 'program files', 'program files (x86)', 'default', 'system volume insformation', 'searches'
Sample 7	'.exe', '.ini', '.dll', '.url', '.lnk', 'KARMA'	'windows', '$recycle.bin', 'all users', 'default user', 'public', 'programdata', 'appdata', 'program files', 'program files (x86)', 'default', 'system volume insformation', 'searches'
Sample 8	'.exe', '.ini', '.dll', '.url', '.lnk', 'KARMA	'windows', '$recycle.bin', 'all users', 'default user', 'public', 'programdata', 'appdata', 'program files', 'program files (x86)', 'default', 'system volume insformation', 'searches'

The list of excluded extensions is reduced as the malware authors iterate

Encryption Details

From Sample 2 onwards, the malware calls CreateIoCompletionPort, which is used for communication between the main thread and a sub thread(s) handling the encryption process. This specific call is key in managing efficiency of the encryption process (parallelization in this case).

Individual files are encrypted by way of a random Chacha20 key. Once files are encrypted, the malware will encrypt the random Chacha20 key with the public ECC key and embed it in the encrypted file.

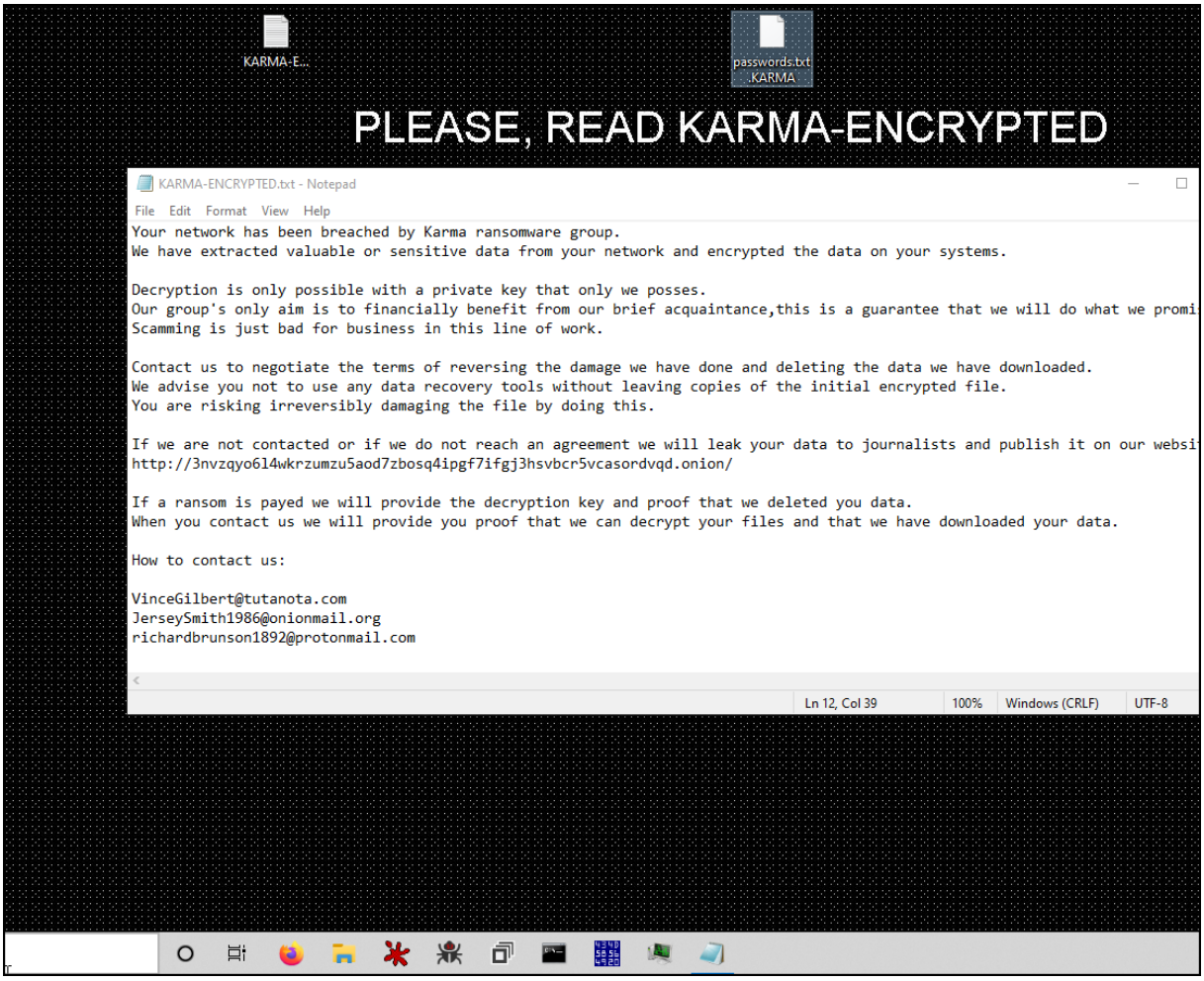
Chacha Encryption

Across Samples 2 to 5, the author removed the `CreateIoCompletionPort` call, instead opting to create a new thread to manage enumeration and encryption per drive. We also note the “KARMA” mutex created to prevent the malware from running more than once. Ransom note names have also been updated to “KARMA-ENCRYPTED.txt”.

Diving in deeper, some samples show that the ChaCha20 algorithm has been swapped out for Salsa20. The asymmetric algorithm (for ECC) has

been swapped from Secp256k1 to Sect233r1. Some updates around execution began to appear during this time as well, such as support for command line parameters.

A few changes were noted in Samples 6 and 7. The main difference is the newly included background image. The file “background.jpg” is written to %TEMP% and set as the Desktop image/wallpaper for the logged in user.



Desktop image change and message

Malware Similarity Analysis

From our analysis, we see similarities between JSWorm and the associated permutations of that ransomware family such as NEMTY, Nefilim, and GangBang. Specifically, the Karma code analyzed bears close similarity to the GangBang or Milihpen variants that appeared around January 2021.

	Gangbang, Milihpen	Karma Malware
Excluded Extensions	.bat, .cab, .cmd, .dll, .exe, .ini, .lnk, .log, .mp3, .mp4, .msi, .pif, .url	.bat, .cab, .cmd, .dll, .exe, .ini, .lnk, .log, .mp3, .mp4, .msi, .pif, .url, .com, .cpl, .ttf
Excluded Folders	"$recycle.bin", "all users", "appdata", "program files (x86)", "program files", "programdata", "rsa", "windows"	"$recycle.bin", "all users", "appdata", "program files (x86)", "program files", "programdata", "rsa", "windows"
Debug Messages	'[+] Getting all settings...' '[-] Failed to get ttructure...' '[+] Checking mutex...' '[+] Importing pub...' '[+] Getting argument list...' '[+] Searching in: %S' '[+] Encrypting: %S' '[+] Starting all threads...' '[-] Failed to import RSA public key...'	'[+] Checking if already started...' '[+] Getting argument list...' ' [-] Argument: ' '[+] Encrypting directory: ' '[+] Encrypting file: ' '[+] Starting all threads...' '[+] Trying to import ECC public key...'

Some high-level similarities are visible in the configurations.

We can see deeper relationships when we conduct a **bindiff** on Karma and GangBang samples. The following image shows how similar the `main()` functions are:

The `main()` function & argument processing in Gangbang (left) and Karma

Victim Communication

The main body of the ransom note text hasn't changed since the first sample and still contains mistakes. The ransom notes are base64-encoded in the binary and dropped on the victim machine with the filename "KARMA-AGREE.txt" or, in later samples, "KARMA-ENCRYPTED.txt".

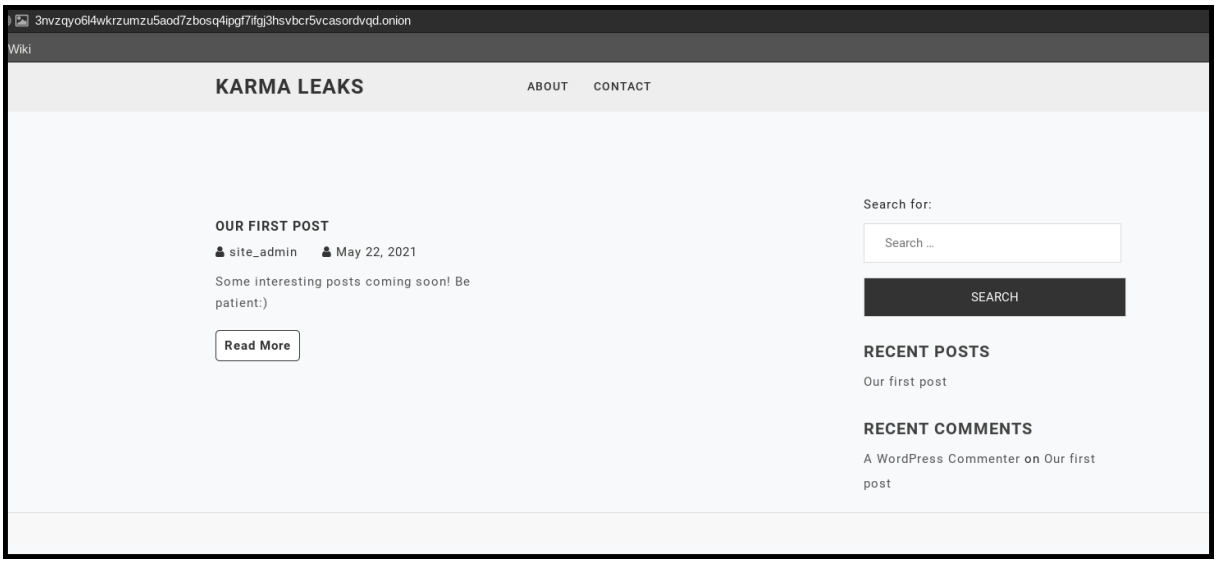
```
Your network has been breached by Karma ransomware group.

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:



{email1@onionmail.org}

{email2@tutanota.com}

{email3@protonmail.com}
```

Each sample observed offers three contact emails, one for each of the mail providers onionmail, tutanota, and protonmail. In each sample, the contact emails are unique, suggesting they are specific communication channels per victim. The notes contain no other unique ID or victim identifier as sometimes seen in notes used by other ransomware groups.

In common with other operators, however, the Karma ransom demand threatens to leak victim data if the victim does not pay. The address of a common leaks site where the data will be published is also given in the

note. This website page appears to have been authored in May 2021 using WordPress.



The Karma Ransomware Group's Onion Page

Conclusion

Karma is a young and hungry ransomware operation. They are aggressive in their targeting, and show no reluctance in following through with their threats. The apparent similarities to the JSWorm family are also highly notable as it could be an indicator of the group being more than they appear. The rapid iteration over recent months suggests the actor is investing in development and aims to be around for the foreseeable future. SentinelLabs continues to follow and analyze the development of Karma ransomware.

Indicators of Compromise

SHA1s

Karma Ransomware

Sample 1: d9ede4f71e26f4ccd1cb96ae9e7a4f625f8b97c9

Sample 2: a9367f36c1d2d0eb179fd27814a7ab2deba70197

Sample 3: 9c733872f22c79b35c0e12fa93509d0326c3ec7f

Sample 4: c4cd4da94a2a1130c0b9b1bf05552e06312fbd14

Sample 5: bb088c5bcd5001554d28442bbdb144b90b163cc5

Sample 6: 5ff1cd5b07e6c78ed7311b9c43ffaa589208c60b

Sample 7: 08f1ef785d59b4822811efbc06a94df16b72fea3

Sample 8: b396affd40f38c5be6ec2fc18550bbfc913fc7ea

Gangbang Sample

ac091ce1281a16f9d7766a7853108c612f058c09

Karma Desktop image

%TEMP%/background.jpg

7b8c45769981344668ce09d48ace78fae50d71bc

Victim Blog (TOR)

http[:]//3nvzqyo6l4wkrzumzu5aod7zbosq4ipgf7ifgj3hsvbcr5vcasordvqd[.]

onion/

Ransom Note Email Addresses

alabacoman@tutanota.com

alberttconner2021@protonmail.com

AndryCooper1988@tutanota.com

CharlesSLewis1987@onionmail.org

DavidSchmidt1977@protonmail.com

DorothyFBrennan1992@tutanota.com

dwaynehogan33@onionmail.org

ElizabethAntone1961@protonmail.com

EndryuRidus@tutanota.com

fionahammers1995@onionmail.org

JamesHoopkins1988@onionmail.org

jasonchow30@onionmail.org

JerseySmith1986@onionmail.org

Kirklord1967@tutanota.com

leonardred1989@protonmail.com

Leslydown1988@tutanota.com

leticiaparkinson1983@onionmail.org

MarkHuntigton1977@tutanota.com

Mikedillov1986@onionmail.org

noreywaterson1988@protonmail.com

ollivergreen1977@protonmail.com

richardbrunson1892@protonmail.com

rickysmithson1975@protonmail.com

VinceGilbert@tutanota.com

MITRE ATT&CK

T1485 Data Destruction

T1486 Data Encrypted for Impact

T1012 Query Registry

T1082 System Information Discovery

T1120 Peripheral Device Discovery

T1204 User Execution

T1204.002 User Execution: Malicious File