

MarraCrypt Ransomware actively spreading in the wild

securitynews.sonicwall.com/xmlpost/marracrypt-ransomware-actively-spreading-in-the-wild/



March 5, 2020

The SonicWall Capture Labs Threat Research Team observed reports of a new variant family of **MARRACRYPT** ransomware [**MARRACRYPT.RSM**] actively spreading in the wild.

```
.rdata:00420CD4 ; char FileName[]
.rdata:00420CD4 FileName db 'CONOUT$',0 ; DATA XREF: sub_417E55+E↑o
.rdata:00420CDC a1Qnan db '1#QNaN',0 ; DATA XREF: sub_419384:loc_4194BA↑o
.rdata:00420CE3 align 4
.rdata:00420CE4 a1Inf db '1#INF',0 ; DATA XREF: sub_419384+10A↑o
.rdata:00420CEA align 4
.rdata:00420CEC a1Ind db '1#IND',0 ; DATA XREF: sub_419384+FB↑o
.rdata:00420CF2 align 4
.rdata:00420CF4 a1Snan db '1#SNAN',0 ; DATA XREF: sub_419384+E3↑o
.rdata:00420CFB align 4
.rdata:00420CFC aSunmontuewedth db 'SunMonTueWedThuFriSat',0
.rdata:00420D12 align 4
.rdata:00420D14 aJanFebmaraprma db 'JanFebMarAprMayJunJulAugSepOctNovDec',0
.rdata:00420D39 align 10h
```

The **MARRACRYPT** ransomware encrypts the victim's files with a strong encryption algorithm until the victim pays a fee to get them back.

Infection Cycle:

The ransomware adds the following files to the system:

Malware.exe

- o % App.path%\ **MARRACRYPT_INFORMATION.HTML**
Instruction for recovery
- o %App.path%\ [Name]. **<MARRA>**

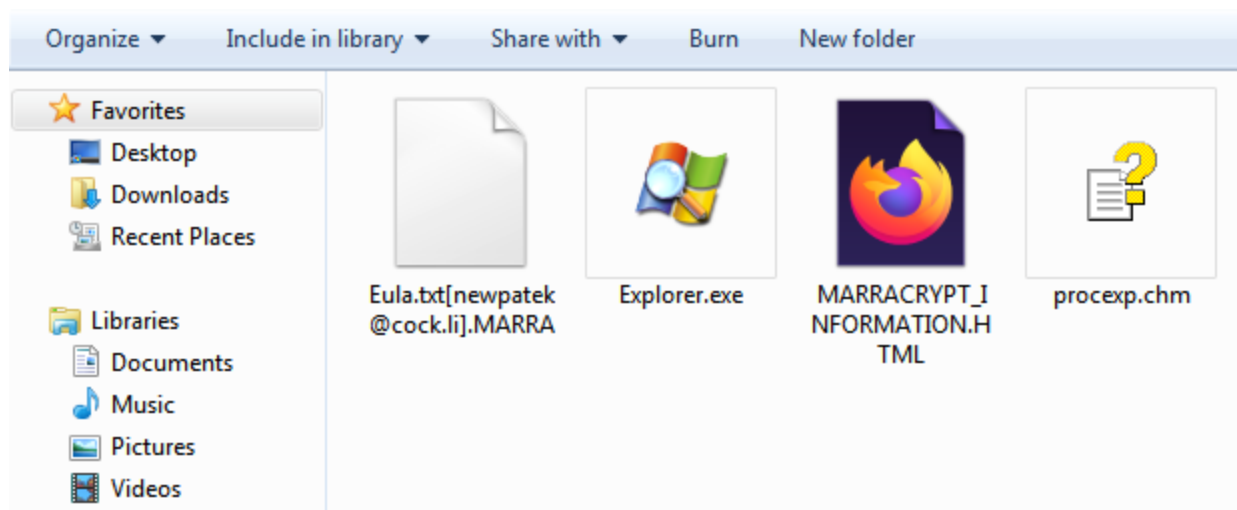
Once the computer is compromised, the ransomware runs the following commands:

Process	Command
Malware.exe (2132)	"C:\Documents and Settings\Administrator\Desktop\Malware.exe"
cmd.exe (2136)	"cmd.exe" /C "C:\Documents And Settings\All Users\sys.bat"
vssadmin.exe (388)	vssadmin Delete Shadows /all /quiet
vssadmin.exe (1644)	
vssadmin.exe (2020)	vssadmin resize shadowstorage /for=c: /on=c: /maxsize=unbounded
vssadmin.exe (1780)	vssadmin resize shadowstorage /for=d: /on=d: /maxsize=401MB
vssadmin.exe (1996)	
vssadmin.exe (1728)	vssadmin resize shadowstorage /for=e: /on=e: /maxsize=401MB
vssadmin.exe (956)	vssadmin resize shadowstorage /for=e: /on=e: /maxsize=unbounded
vssadmin.exe (2016)	vssadmin resize shadowstorage /for=f: /on=f: /maxsize=401MB
vssadmin.exe (2028)	vssadmin resize shadowstorage /for=f: /on=f: /maxsize=unbounded
vssadmin.exe (2100)	vssadmin resize shadowstorage /for=g: /on=g: /maxsize=401MB
vssadmin.exe (324)	vssadmin resize shadowstorage /for=g: /on=g: /maxsize=unbounded
vssadmin.exe (1384)	vssadmin resize shadowstorage /for=h: /on=h: /maxsize=401MB
vssadmin.exe (2828)	vssadmin resize shadowstorage /for=h: /on=h: /maxsize=unbounded
vssadmin.exe (2308)	vssadmin Delete Shadows /all /quiet

Process	Command
vssadmin.exe (2308)	vssadmin Delete Shadows /all /quiet
cmd.exe (328)	cmd /c ""C:\Documents and Settings\All Users\Application Data\newpatek\onmywrist.bat""
cmd.exe (380)	C:\WINDOWS\system32\cmd.exe /c tasklist /NH /FI "IMAGENAME eq Malware.exe"
tasklist.exe (168)	tasklist /NH /FI "IMAGENAME eq Malware.exe"
ping.exe (800)	ping 127.0.0.1 -n 5
cmd.exe (1696)	C:\WINDOWS\system32\cmd.exe /c tasklist /NH /FI "IMAGENAME eq Malware.exe"
tasklist.exe (1904)	tasklist /NH /FI "IMAGENAME eq Malware.exe"
ping.exe (2832)	ping 127.0.0.1 -n 5
cmd.exe (192)	C:\WINDOWS\system32\cmd.exe /c tasklist /NH /FI "IMAGENAME eq Malware.exe"
tasklist.exe (2276)	tasklist /NH /FI "IMAGENAME eq Malware.exe"
ping.exe (2320)	ping 127.0.0.1 -n 5
cmd.exe (2328)	C:\WINDOWS\system32\cmd.exe /c tasklist /NH /FI "IMAGENAME eq Malware.exe"
tasklist.exe (2332)	tasklist /NH /FI "IMAGENAME eq Malware.exe"
ping.exe (2360)	ping 127.0.0.1 -n 5
cmd.exe (2376)	C:\WINDOWS\system32\cmd.exe /c tasklist /NH /FI "IMAGENAME eq Malware.exe"

The ransomware encrypts all the files and appends the **[MARRA]** extension onto each encrypted file's filename.

Process Name	PID	Operation	Path
Malware.exe	2132	WriteFile	C:\Program Files\Messenger\newalert.wav[newpatek@cock.li].MARRA
Malware.exe	2132	WriteFile	C:\Program Files\Messenger\newalert.wav[newpatek@cock.li].MARRA
Malware.exe	2132	SetRename...	C:\Program Files\Messenger\newemail.wav
Malware.exe	2132	WriteFile	C:\Program Files\Messenger\newemail.wav[newpatek@cock.li].MARRA
Malware.exe	2132	WriteFile	C:\Program Files\Messenger\newemail.wav[newpatek@cock.li].MARRA
Malware.exe	2132	SetRename...	C:\Program Files\Messenger\online.wav
Malware.exe	2132	WriteFile	C:\Program Files\Messenger\online.wav[newpatek@cock.li].MARRA
Malware.exe	2132	WriteFile	C:\Program Files\Messenger\online.wav[newpatek@cock.li].MARRA
Malware.exe	2132	SetRename...	C:\Program Files\Messenger\type.wav
Malware.exe	2132	WriteFile	C:\Program Files\Messenger\type.wav[newpatek@cock.li].MARRA
Malware.exe	2132	WriteFile	C:\Program Files\Messenger\type.wav[newpatek@cock.li].MARRA
Malware.exe	2132	CreateFile	C:\Program Files\microsoft frontpage\version3.0\bin\MARRACRYPT_INFORMATION.HTML
Malware.exe	2132	WriteFile	C:\Program Files\microsoft frontpage\version3.0\bin\MARRACRYPT_INFORMATION.HTML
Malware.exe	2132	WriteFile	C:\Program Files\microsoft frontpage\version3.0\bin\MARRACRYPT_INFORMATION.HTML
Malware.exe	2132	CreateFile	C:\Program Files\microsoft frontpage\version3.0\MARRACRYPT_INFORMATION.HTML
Malware.exe	2132	WriteFile	C:\Program Files\microsoft frontpage\version3.0\MARRACRYPT_INFORMATION.HTML
Malware.exe	2132	WriteFile	C:\Program Files\microsoft frontpage\version3.0\MARRACRYPT_INFORMATION.HTML
Malware.exe	2132	CreateFile	C:\Program Files\microsoft frontpage\MARRACRYPT_INFORMATION.HTML
Malware.exe	2132	WriteFile	C:\Program Files\microsoft frontpage\MARRACRYPT_INFORMATION.HTML
Malware.exe	2132	WriteFile	C:\Program Files\microsoft frontpage\MARRACRYPT_INFORMATION.HTML



After encrypting all personal documents, the ransomware shows the following HTML file containing a message reporting that the computer has been encrypted and to contact its developer for unlock instructions.

MARRACRYPT 1.0 RANSOMWARE

Your files has been encrypted using RSA-4096 algorithm with unique public-key stored on your PC.

There is only one way to get your files back: contact with us, pay, and get **decryptor software**.

We accept Bitcoin, and other cryptocurrencies, you can find exchangers on bestbitcoinexchange.io

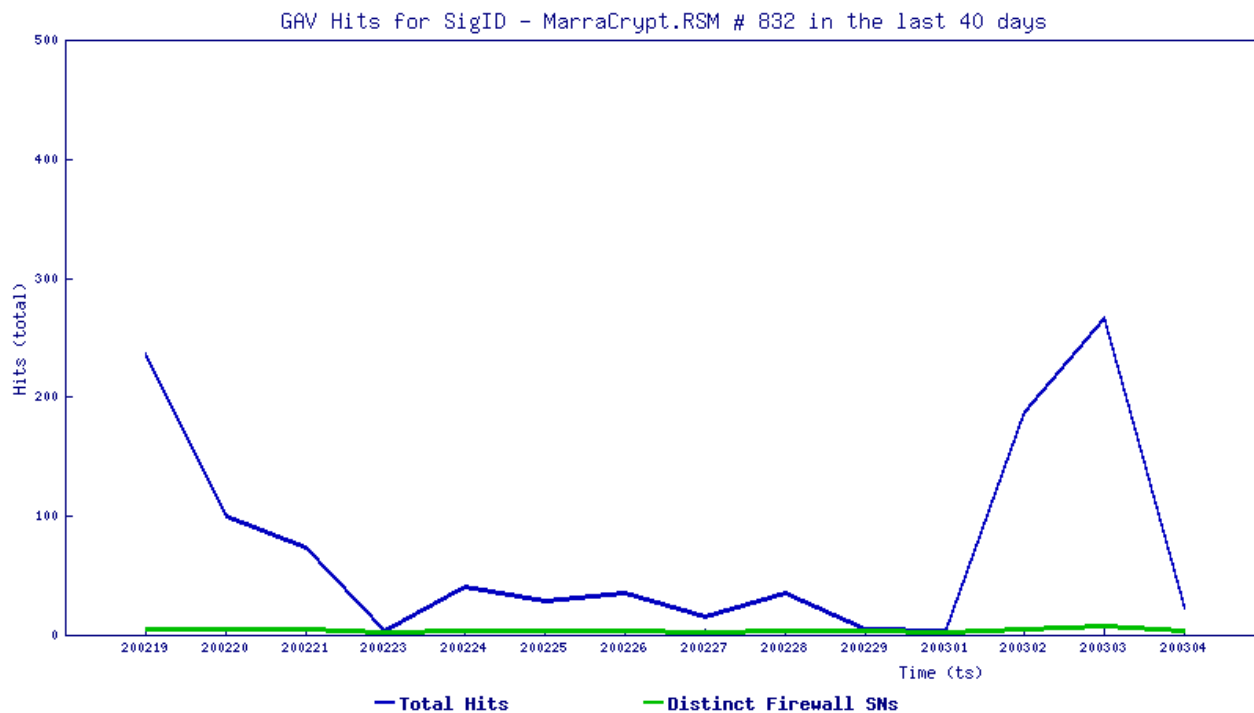
You have unique idkey (in a yellow frame), write it in letter when contact with us.

Also you can decrypt 2 files as a test, its a guarantee we can decrypt your files.

!!! IDKEY !!!

```
>>>a13add8c1c3466fbced929e72a2c1410b623edcc269e633d8697d62bdd02ccc987951f87250c330580c685796
4bfa5ae2f00d590f084e2ae906c83efcc01120f13955787a65f3ae6d1cb99aee293be3304b7842f92cebbf5f0d3a2e
36f13285f9768c8690c53df92fa44d5aed3fd58389c713eb4a3840cfe09b2c84403fe62fa647b690f401789bf72740
aeb0e5f93479d2b7021e9bb5b9fcd54589d6654d485011726d3c39b399028b9a32f4f0a89eaccda801ea4926d
53b42af28c45c91e252e88d5ac06881bf2d2f37f0a663bfdfca270e82ef0c73987a8af0f42220ee15afac3e8ac3bf
a4c6d42e0c2d22cab457004e1a8a757f168258a7c694fac8efe7a910a56c8b1f4daf7ffd250abb2658e3ffff12555b
0f6c4cc69899e271fa8bbbc5093e4ba390a5a069e57abe1b841c1d01519d7a1090b1447e481f6e6acd18844cc3bf1
ee4703cf5580eb9a002013ce1c3cd9f5cb78bfdcc0af7f7bbabc2cca0881980e7cd7d7ed6faf053ac6a1804985e0c136
a6bbab99647cc543bed9c9100f53b6ccaa22906f3e8ad98261e5f2f615140d72c37b5e4f786bc491ebce0630bdc9b8f
61d29e50b1d5be23ccf32bd2bc0f9bc383f06e19523d881e1b3b131ed89e9e1da3fd23fc509ddc97f3b6266bbeb8ac
5761a905d22d9e2eb57bf24d664bcbac4ba1ac718051885c8b8e0d77967de5ee1512ba7fa5a9344804b322b3e2fd
6a5f18c959765c169050120ae990942bfd20c3fb90d655312c774e08ed7008db96e690bd02835152aeb31603
e8f2491dc44a21280ff8923c56952bcc5b5405de47e6c57310810322917a92706cda17dd9d8a8eebe17612e2c121
473bf5179cc70cb838f27e668996a534ce87e5224a6bd02645b7f0c627e25fb59975d6edf56b614f90a28379e149
```

We have been monitoring varying hits over the past few days for the signature that blocks this threat:



SonicWall Capture Labs provides protection against this threat via the following signature:

GAV: MARRACRYPT.RSM (Trojan)

This threat is also detected by SonicWALL Capture ATP w/RTDMI and the Capture Client endpoint solutions.