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

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

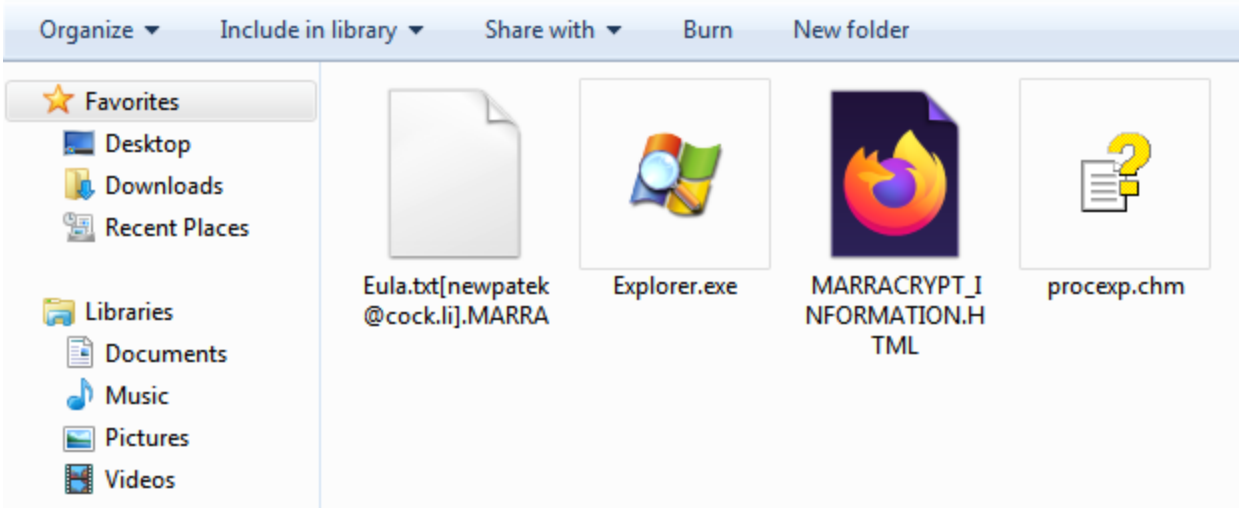
Once the computer is compromised, the ransomware runs the following commands:

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"

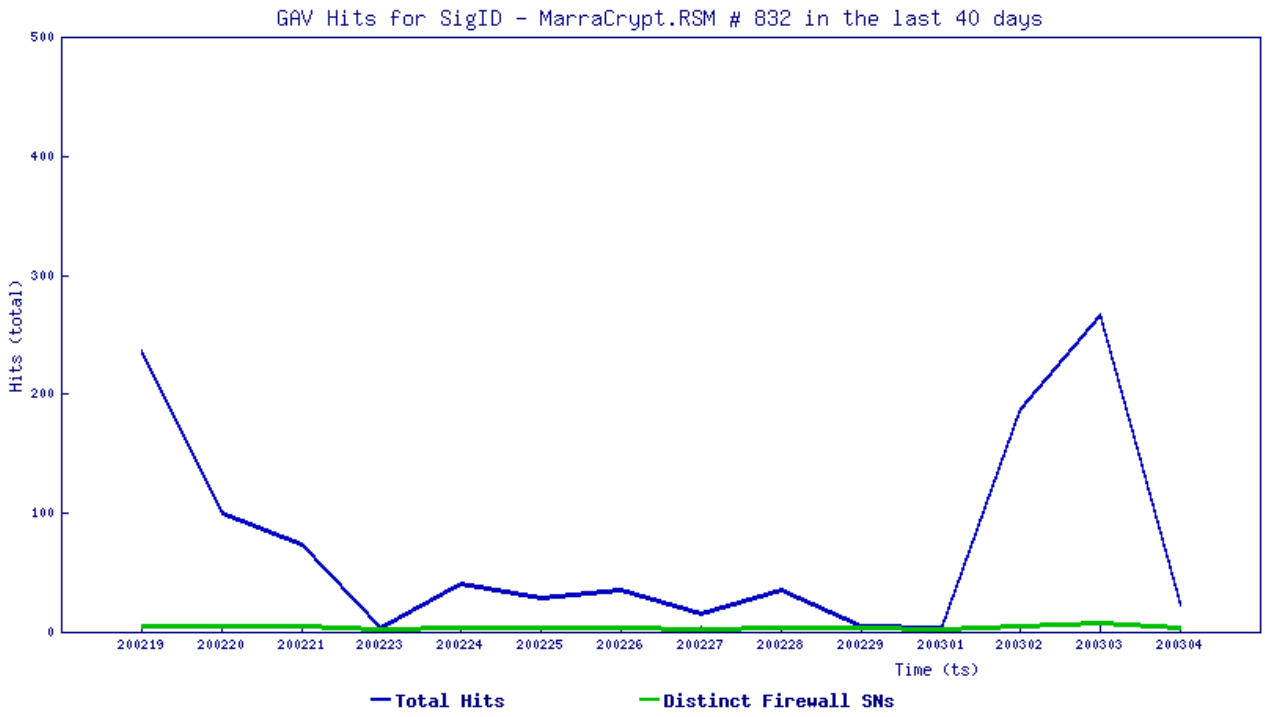
The ransomware encrypts all the files and appends the **[MARRA]** extension onto each encrypted file's filename.

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	SetRenamel...	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	SetRenamel...	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	SetRenamel...	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.

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.