SunCrypt Ransomware sheds light on the Maze ransomware cartel

bleepingcomputer.com/news/security/suncrypt-ransomware-sheds-light-on-the-maze-ransomware-cartel/

Lawrence Abrams

By Lawrence Abrams

- August 26, 2020
- 11:47 AM
- 1



A ransomware named SunCrypt has joined the 'Maze cartel,' and with their membership, we get insight into how these groups are working together.

In June, we broke the story that the Maze threat actors <u>created a cartel of ransomware</u> <u>operations</u> to share information and techniques to help each other extort their victims.

When first started, this cartel included Maze and <u>LockBit</u>, but soon <u>expanded to include</u> <u>Ragnar Locker</u>.

When Maze first formed this group, they refused to answer our questions on how members of their cartel benefited, and if there was a monetary benefit to Maze.

SunCrypt joins the Maze ransomware cartel

In an email sent to BleepingComputer, the operators of a ransomware named SunCrypt stated that they are a new member of the Maze Ransomware cartel.

Based on submissions statistics to <u>ID-Ransomware</u>, this ransomware family began operating in October 2019, but was not very active.

SunCrypt told BleepingComputer that they are an independently run ransomware operation from Maze, but as part of the cartel, they have "two-way communication channels with them,"

When asked why they joined this 'cartel,' we were told that Maze could not handle the volume and needed outside help.

"They just can't handle all the available field of operations. Our main specialization is ransomware attacks," - SunCrypt ransomware operators.

After further questions, they eventually told us that they "share revenue from the successful operation," but did not provide any details about what Maze provided to earn that revenue share.

Based on their statement that they were brought in because Maze can't handle all of the potential attacks, Maze may provide compromised network access to cartel members in exchange for a revenue share.

From a ransomware sample seen by BleepingComputer, it looks like cartel members get more for their money.

Maze shares its resources with cartel members

Yesterday, GrujaRS was finally able to <u>find a sample</u> of the SunCrypt ransomware so we can get a better glimpse into how the ransomware works.

The SunCrypt Ransomware sample is installed via a heavily obfuscated PowerShell script, shown below.

📕 želoveni prizvidel (prostij zkol	eth de arthur sind service arthur s	☆ 物液体0.ps1 - Notepad2	- 🗆	×
<u>File E</u> dit <u>V</u> iew <u>S</u> ettings <u>?</u>				
🗋 😂 🛱 🛃 🔊 🛯 🕹 🗈 🛍 🗛 🎭	u 🔍 🔍 🖃 🖬 📭			
1 Add-Type -TypeDefinition	@.'			/
<pre>2 using System;</pre>				
³ using System.Diagnostics				
4 using System.Runtime.Int				
spublic static class SczD			8	
<pre>6 [D]]Import("kernel32.d]]</pre>				
	IT VORUXYWTVFZJTZIW	BtHIL,uint AqocDvPgGYAcPi	JpRrzxc,uint	
<pre>TEQOIZJktLeneVZqwAmaG); 7 [DllImport("user32.dll")</pre>	public static auto	no IntEta EnumbertoneW(I	o+D+a	
		pCNReLX,IntPtr iZTzialERG		
8 }	FCI DOWWYWKCSDDIIEL	penkeen, increi 12121aieko	qrotarebhile),	
9 '@				
10				
11				
12 Function nSZkQPmkPfdWCnl	idAsKn() {			
13 return ((-1084 + 1695)	- (12622 - 9614))			
14				
15 }				
16 \$SOMktntsZhpaaSnopvuHr =	nSZkQPmkPfdWCnRidA	sKn		
17	1 () f			
18 Function RGacawknYmxytp 19 return (\$SOMktntsZhpaaSh				
20	оруингу			
20 21 }				
22 \$dpYwyTWCLgTIrdiFqLMpt =	RGacawknYmxytndlns	cra		
23	Kdacamarininy cparps			
24 Function OwAcSxjrDIBVPp)	NOcneiO {			
25 return 12141				
26				
27 }				
<pre>28 \$KrFbS0ZPbpkkJbicuTYXD =</pre>	OwAcSxjrDIBVPpXNOc	nej		
29				
30 Function NgCrmWDpWoPFK0	LcFnPq() {			`
.n 1,100 : 123,883 Col 1 Sel 0	1.38 MB ANSI	CR+LF INS PowerShell Scrip	t	

Obfuscated PowerShell script

When the ransomware is executed, it will connect to the URL http://91.218.114[.]31 and transmit information about the attack and its victim.

The use of this IP address provides another big clue as to what services the Maze threat actors provide their cartel members.

For months, Maze has been hosting a data leak site and launching attacks from known public IP addresses. Yet in all this time, their services remain intact and have not been taken down by law enforcement.

The 91.218.114.31 address is one of the addresses that the Maze operation <u>uses as part of its campaign</u>. Even more similar, Maze infections also transmit information to this IP address during an attack.

This shared IP address means one of the two things; Maze is sharing their infrastructure or white-labeling their ransomware technology to other groups.

This sharing of resources would also explain why they would earn a revenue share for each ransom payment.

Update 8/31/2020: The Maze threat actors have told BleepingComputer that they are not affiliated with the SunCrypt ransomware operators.

"We do not have any connections with SunCrypt, it is a lie."

"We do not know why SunCrypt does it, but we believe it is a PR strategy, to send links to companies in chat that they are working with us as a pressure," Maze told BleepingComputer.

Advanced Intel's Vitali Kremez has told BleepingComputer that in addition to connecting to http://91.218.114[.]31, the SunCrypt ransomware will also connect to http://91.218.114[.]30.

Both of these IP addresses are on the same address space.

As previously stated, 91.218.114[.]31 has been used by Maze in the past.

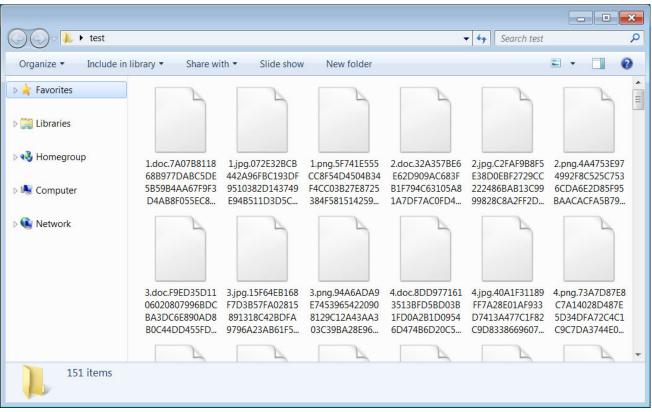
SunCrypt is no longer responding to our queries with follow up questions.

The SunCrypt Ransomware

The SunCrypt ransomware itself is still being analyzed, but we can provide a basic overview of the ransomware.

The ransomware is currently being distributed as a DLL that, when executed, will encrypt a computer's files.

When encrypting files, it will append a hexadecimal hash to the end of each file name. It is not known what this hash represents.



SunCrypt encrypted files

In every folder a ransom note named **YOUR_FILES_ARE_ENCRYPTED.HTML** is created that contains information on what happened to a victim's files and a link to the Tor payment site.

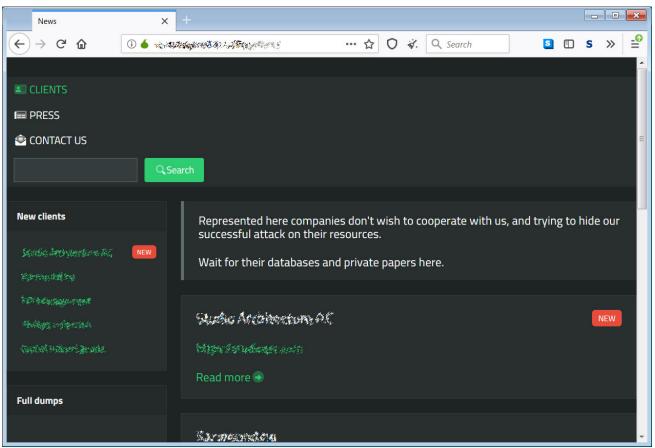
♦ YOUR_FILES_ARE_ENCRYPTED.HT × +		
← → C (①) File C:/Users/User/AppData/Local/Temp/YOUR_FILES_ARE_ENCRYPTED.HTML		9:
EN DE FR ES JP		
Whats Happen?		
We got your documents and files encrypted and you cannot access them. To make sure we are not bluffing just check out your files. Want to rea them? Just do what we instruct you to. If you fail to follow our recommendations, you will never see your files again. During each attack, we co valuable commercial data. If the user doesn't pay to us, we will either send those data to rivals, or publish them. GDPR. Don't want to pay to us more to the government.	ру	x
What Guarantees?		
We're doing our own business and never care about what you do. All we need is to earn. Should we be unfair guys, no one would work with us. drop our offer we won't take any offense but you'll lose all of your data and files. How much time would it take to recover losses? You only ma		
How do I access the website?		
<u>Get TOR browser here</u> <u>Go to our website</u>		
In case you decide not to cooperate, your private data will be published here or sold.		
Offline how-to Copy & Paste this secret message to <u>this page</u> textarea field		
LIGHTING SERVICESSING SERVICESSING SERVICESSING STATES STATES STATES STATES STATES STATES SERVICESSING SERVICES		

SunCrypt ransom note

The Tor link enclosed in a ransom note is hardcoded into the ransomware executable. This means that every victim encrypted by a particular SunCrypt executable will have the same Tor payment site link.

The Tor payment site does not have automated features and simply contains a chat screen where a victim can negotiate a ransom with the SunCrypt threat actors.

Furthermore, every ransom note contains a link to the SunCrypt data leak site that the threat actors warn will be used to publish the victim's data.



SunCrypt data leak site

At this time, there are approximately five victims listed on the SunCrypt data leak site.

Other ransomware operations that run <u>data leak sites</u> or have stolen unencrypted files to extort their victims include Ako, Avaddon, Clop, Conti, CryLock, DoppelPaymer, Maze, MountLocker, Nemty, Nephilim, Netwalker, Pysa/Mespinoza, Ragnar Locker, REvil, Sekhmet, Snatch, and Snake.

SunCrypt is currently being analyzed for weaknesses, and it is not known if it is possible to recover files for free.

Update 8/31/20: The Maze operators deny having any affiliation with SunCrypt.

Related Articles:

Industrial Spy data extortion market gets into the ransomware game

Quantum ransomware seen deployed in rapid network attacks

Snap-on discloses data breach claimed by Conti ransomware gang

Shutterfly discloses data breach after Conti ransomware attack

SunCrypt ransomware is still alive and kicking in 2022

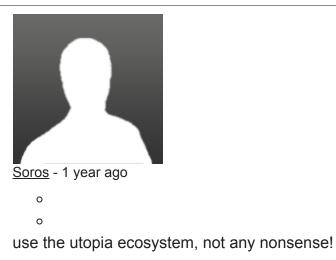
- <u>Cartel</u>
- Data Exfiltration
- Data Leak
- <u>Maze</u>
- Ransomware
- <u>SunCrypt</u>

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

Comments



Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: