

Threat Thursday: Dr. REvil Ransomware Strikes Again, Employs Double Extortion Tactics

 blogs.blackberry.com/en/2021/05/threat-thursday-dr-revil-ransomware-strikes-again-employs-double-extortion-tactics

The BlackBerry Research & Intelligence Team

1. [BlackBerry ThreatVector Blog](#)
2. Threat Thursday: Dr. REvil Ransomware Strikes Again, Employs Double Extortion Tactics



Summary

The FBI has named the Russia-affiliated Ransomware-as-a-Service (RaaS) group REvil (also known as Sodin or Sodinokibi) as the culprits behind attacks on the world's largest meat supplier, JBS. These attacks threatened the global food supply chain and serve as a reminder of the vulnerable state of critical infrastructure worldwide.

Given the success of the REvil attacks and other similar malware, it is crucial for organizations to learn how to prevent ransomware threats. This blog offers a brief overview of how REvil operates and offers effective solutions for stopping these kinds of attacks in the future.

The malware acts as a Ransomware-as-a-Service (RaaS) and became prolific after another RaaS group, GandCrab, shut down their operations. Security researchers have identified many similarities and code reuse between REvil and GandCrab. REvil was first advertised on Russian language cybercrime forums and is associated with the threat actor "Unknown" or "UNKN".

REvil is most famously associated with recent attacks on [Travelex](#), [Acer](#), and Apple supplier [Quanta Computer](#). Acting as a RaaS, REvil relies on affiliates or partners to perform its attacks. The REvil developers receive a percentage of all proceeds from ransom payments. Because the ransomware is distributed by different entities, the initial infection vector can vary; typically, this is either via phishing campaigns, brute force attacks to compromise RDP, or through software vulnerabilities. REvil is also known to be distributed by other malware such as [IcedID](#).

[Read our previous deep dive on Sodinokibi.](#)

Operating System

Windows	MacOS	Linux	Android
✓	✗	✗	✗

Risk and Impact

Impact	High
Risk	High

Technical Analysis

REvil stores its configuration as an encoded resource. The first 32 bytes are the key used to decode the configuration, which is contained in the remaining bytes:

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...	Characteristics
00000260	00000268	0000026C	00000270	00000274	00000278	0000027C	00000280	00000282	00000284
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
.text	0000BC34	00001000	0000BE00	00000400	00000000	00000000	0000	0000	60000020
.rdata	00002ECC	0000D000	00003000	0000C200	00000000	00000000	0000	0000	40000040
.data	000023C0	00010000	00001E00	0000F200	00000000	00000000	0000	0000	C0000040
.cfg	0000C800	00013000	0000C800	00011000	00000000	00000000	0000	0000	C0000040
.reloc	00000738	00020000	00000800	0001D800	00000000	00000000	0000	0000	42000040

This section contains:

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000000	6F	39	74	57	42	42	54	48	6D	78	57	56	36	31	74	78	c9tWBETHmxWV61tz
00000010	46	4D	31	42	56	31	38	7A	75	6F	78	72	76	47	68	54	EM1BV18zucxrvGhI
00000020	A7	03	10	81	1A	7F	00	00	52	56	B1	88	D6	0C	BA	21	S00 0 . RV± O!@!
00000030	40	4D	B7	4D	B6	A4	FC	40	23	FE	DC	3A	B3	6F	2E	89	@M.M!P!u@#bU.°c.!
00000040	96	63	EC	10	37	B7	DB	14	80	E1	21	D4	6C	18	A9	D2	!cin 7·0n !á!Ó!n@O
00000050	98	A8	98	F7	E5	45	4D	9B	A1	C1	2D	4C	48	E2	44	87	! !-±EM!iÁ-LHÁD!
00000060	BA	B0	F9	42	18	8B	1F	91	DB	64	DB	51	F5	46	02	A1	±·úE0! !·úDÚ0±F i
00000070	F1	36	F8	90	94	B2	E4	B2	BC	B3	D6	98	BB	1F	24	9E	ñ6ø !²á²k²Ó!; \$!
00000080	41	42	F3	9B	8F	5D	3B	EA	24	A2	1D	7E	D5	33	F0	39	AB0!]:é±c·°Ó3±9
00000090	41	D0	41	43	0E	B3	89	BD	94	B8	C1	7E	DC	A3	C9	AC	ADÁC0²!±!Á~Ú!E-
000000A0	82	52	AD	A1	98	7E	7C	99	3E	32	74	FC	46	64	CE	B0	!R-i!~ !>2túFdi*
000000B0	5F	5A	52	57	7C	81	B6	E5	75	2E	55	A9	15	F8	8A	DA	_ZRW! !áu.U0ø!Ú
000000C0	C2	6A	28	6D	5A	60	5A	07	9D	F3	CA	8C	B0	60	28	D9	Áj(mZ!Zn óE!^(Ú
000000D0	AC	B7	C6	D0	50	19	4C	E0	E0	FD	34	2C	C2	AF	75	F5	-·ÆBF0!ààý4.Á-uš
000000E0	54	0A	06	0E	BF	8E	45	C0	02	13	B2	D5	CE	57	11	83	T.00 c!EÁ 0²Ó!W0!
000000F0	CA	FA	C3	28	3C	4E	59	0D	04	C5	38	1F	FC	1A	03	5B	EúÁ(<<NY.0.Á8 ú00[
00000100	50	92	01	5F	32	FB	A9	6A	0B	37	F2	16	F4	71	9A	81	P'0_2ú@j07c0 óq!
00000110	AE	37	A2	4E	B9	45	71	7A	45	5D	FA	FD	E2	05	01	5D	@7cN!EqzE!úý00]
00000120	B0	6B	22	2E	86	A9	EC	18	32	9A	01	F1	0E	9A	0B	B7	*k. !@in 2!0ñ0!0·
00000130	92	41	26	17	10	DD	B8	8C	FC	2E	15	20	05	9E	2B	09	·Á&00Ý, !ü.0.0!+.
00000140	0D	A0	6A	9A	F9	A9	2D	04	80	5D	5E	78	EE	87	33	FB	. j!ú@-0!]^xi!3ú
00000150	46	DD	21	D2	24	5B	E8	CE	1A	12	FF	DA	09	05	75	07	FÝ!Os!@!0n ýÜ.0.ú0
00000160	55	6D	85	71	63	0C	13	10	66	2E	0C	85	B4	7B	EF	E5	Um!qc!00 f.!!'!iá
00000170	2C	7E	E6	3D	34	64	FA	29	76	40	25	82	6B	E1	06	28	·~±=4dú)v@%!k&0(
00000180	29	41	15	45	39	DD	9B	7B	B2	B2	F7	57	58	F5	97	0B)Á0E9Ý!(!²±-NXš!0
00000190	29	93	B9	A9	E5	CD	1D	36	BA	6F	EE	0C	EE	3A	28	EF)!¹@á! 6±oi!i:(i
000001A0	31	59	B7	07	4D	23	2D	A2	33	E1	F9	53	AD	CE	2E	2E	1Y·0M#-c3áúS-!..
000001B0	00	8E	36	8C	8E	FD	03	04	12	31	8F	B9	AC	E2	40	B1	.!6! ý000 1²-á@±
000001C0	EE	4E	AB	84	45	FB	0E	CC	90	F2	50	7C	86	9F	91	5C	iN<<!E00! 0P! !'\
000001D0	80	CC	46	89	7C	67	16	4A	A0	1B	53	E3	A2	E7	66	17	!IF! q0J 0S±c0f0
000001E0	53	DB	E0	AA	7C	DA	70	CA	41	04	2E	C3	FD	8B	1D	93	SÚà±!ÚpEÁ0.Áý! !
000001F0	DF	BF	03	89	57	48	3B	09	41	C1	2C	E2	13	25	6D	13	Bc0!WK:ÁÁ.80%00
00000200	DA	44	93	85	80	26	B2	B0	2D	A6	11	44	1C	7E	B8	14	ÚD! ! ²²-!0D ~.0
00000210	86	94	76	A0	8F	B8	11	35	63	C4	BD	79	A5	9E	FF	34	! !v .05cÁkY#!ý4
00000220	FE	E5	D7	8C	0D	55	F6	7A	EA	9B	42	FA	71	E6	12	EF	bá×! .ÚcZé!Búq0!i
00000230	7D	6D	19	70	8A	6E	30	A1	1B	D8	23	56	CF	A9	CA	75	}m0 p!n0!0#V!0Eu
00000240	3D	A6	B8	E0	98	D6	E8	1A	EC	5F	97	FB	A4	63	41	A5	=! á!0èn i !úPcÁ#
00000250	90	61	D2	77	12	3A	D6	AE	C2	0E	39	AB	8D	79	56	66	a0w0:00Á0 9<< yVf
00000260	F0	25	E4	0F	D3	06	14	99	2D	E8	EB	A9	F0	95	B9	96	±%00 C00! -èè0±!!
00000270	0C	E7	12	0B	53	4F	FD	E0	B8	94	03	E7	5A	77	2A	8F	!c00 SOyà, !0 cZw*

Sel Start: 00000000 Size: 00000020

Figure 1: REvil's key is contained in the first 32 bytes.

Initially, REvil will fingerprint the target machine and gather system information. Before beginning the encryption routine, REvil will kill certain processes such as email clients, SQL or other database servers, browsers and Microsoft® Office applications to ensure it can encrypt important files belonging to the victim. It will also remove shadow copies to prevent easy recovery.

For persistence, the ransomware creates a registry key to execute with Windows startup under:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\!aDTFUAla7!

Name	Type	Data
(Default)	REG_SZ	(value not set)
!aDTFUAla7!	REG_SZ	C:\Users\Mai\Desktop\EMEA.exe

Figure 2: Registry key created.

The sample analyzed also creates registry entries under **HKLM\BlackLivesMatter** containing hex values:

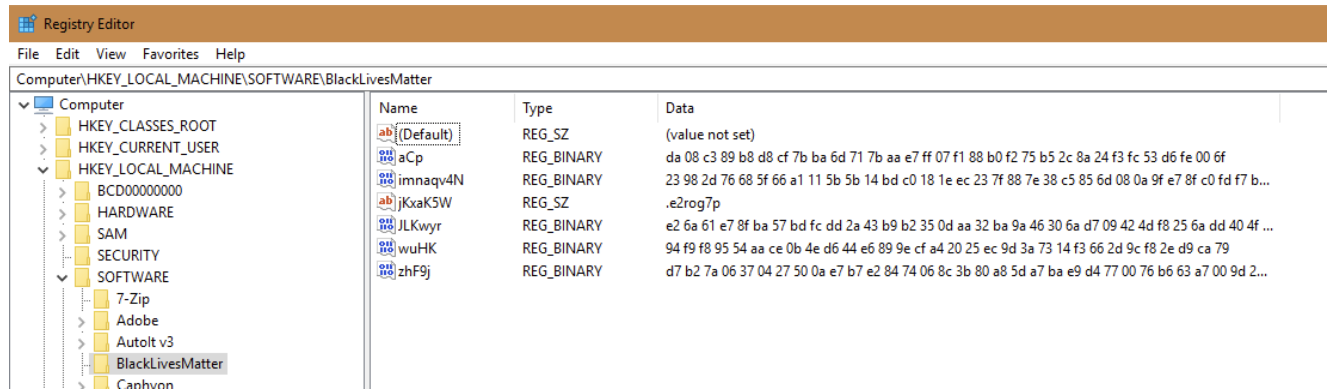


Figure 3: Hex values.

The malware creates a mutex: "**Global\8C39F091-3A8D-46F4-DBC5-DDA17B3C63C2**", to ensure it is the only running instance. If another instance is executed, it will prompt an error message:

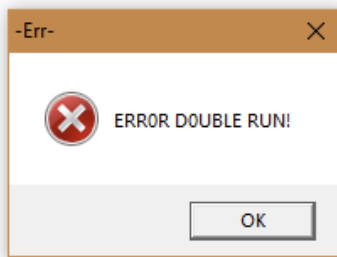


Figure 4: REvil error message.

REvil will enumerate files on the system and during the encryption process appends a random alpha numeric extension between 5 and 10 characters in length, E.G.: **“.oh24o8”**.

A ransom note, with the same alpha-numeric name as that used for the file extensions, followed by **“readme.txt”**, is dropped in all affected directories, E.G.: **“oh24o8-readme.txt”**:

EMEA.exe	6804	CreateFile	C:\oh24o8-readme.txt	SUCCESS
EMEA.exe	6804	WriteFile	C:\oh24o8-readme.txt	SUCCESS

Figure 5: REvil ransom note text file.

Screenshot of the ransom note belonging to REvil:

```

----- Welcome. Again. -----

[+] Whats Happen? [+]

Your files are encrypted, and currently unavailable. You can check it: all files on your system has extension 0ytly968.
By the way, everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).

=====Attention!!!=====
Also your private data was downloaded. We will publish it in case you will not get in touch with us asap.
=====

[+] What guarantees? [+]

Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody
will not cooperate with us. Its not in our interests.
To check the ability of returning files, You should go to our website. There you can decrypt one file for free. That is our guarantee.
If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data, cause just we have the private key.
In practise - time is much more valuable than money.

[+] How to get access on website? [+]

You have two ways:

1) [Recommended] Using a TOR browser!
  a) Download and install TOR browser from this site: https://torproject.org/
  b) Open our website: http://aplebzu47wgazapdqks6vrcv6zcn1ppkxbr6wketf56nf6ag2nmvovd.onion/4DD2F2803EC112D7

2) If TOR blocked in your country, try to use VPN! But you can use our secondary website. For this:
  a) Open your any browser (Chrome, Firefox, Opera, IE, Edge)
  b) Open our secondary website: http://decoder.re/4DD2F2803EC112D7

Warning: secondary website can be blocked, thats why first variant much better and more available.

When you open our website, put the following data in the input form:
Key:

```

Figure 6: REvil ransom note.

For file encryption, REvil uses **curve25519/Salsa20**; key encryption utilizes **curve25519/AES-256-CTR**. The developers of REvil pride themselves as having created the best data encryption and decryption system currently available.

A custom .bmp image is dropped to the **%Temp%** directory and this is set as the desktop wallpaper via a registry setting. The wallpaper image informs the user that their files have been encrypted:

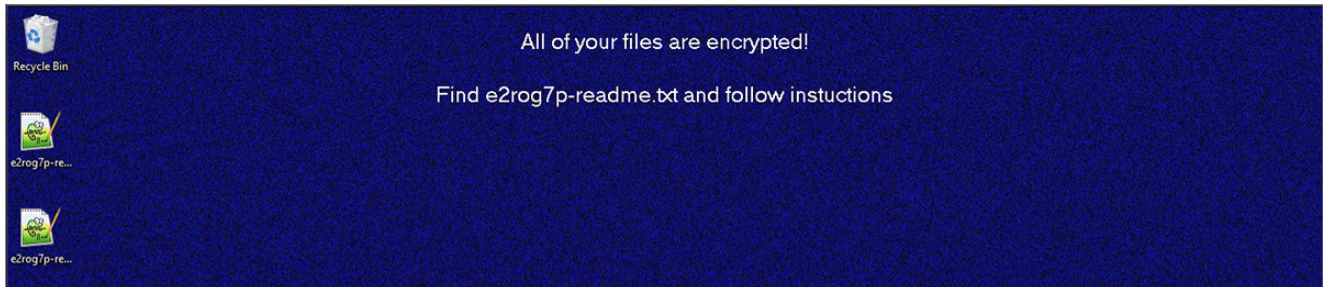


Figure 7: REvil wallpaper ransom note.

To pay the ransom, two URLs are provided, one accessible with the TOR browser and a secondary site which can be used if TOR is blocked in the user's location:

Enter the key here:

```
p+4WB1MRmeMt/chrhiwND847RB1LYt27Tzla+d+W21tL/oDb4ea8K3gYeVaiKTYa  
3BZH9gPdPjxtHQ6x44IC/V8vh9qK7klq6sWDXQIQuleRPfoVV2wWENSuFOSHxd4+  
4NsWOJ2a22AzPJjww2tdE1GmMsuY815Tu8Id85xYpU4glDPH6d3ihZzB9qR4YjmT  
gLTB7P5PwaEB/iILKHpX+IeeSLwfj2xShEhktMOOJYemmEXAMPLEiCRfXM97lnf  
wWzMuYV/10eZjlg/EXAMPLEU0eI/e5vTSNLFMBE0G5R1R4qrkrXNlJ4J+FErtxn  
0PTlgmlX5k/MyNuT5ah4/f100sjpW8K1RwNsEs2WGA7kT3PcxPlwXpA+PSGmh6DD  
rOtN3zgcCqDj9Gpi+bHYTidK+8S/DnWNPuooWREofGayRd/QM+0EXAMPLEGg/fRH  
NGqS1kRsWlpnk43kG5PopKFkOSSi46WB/+sXcUy7z20HYnIXPoILnQ3QfqSjV0tc  
zhaJb2Ww9Yfqi5zc3vijKQh99i7m5bKBWz+l8hs91f1Q2DioMJjMjWzZmJ+X9dHW  
YxEXAMPLEQLT+hqmfVdsyKaDbLcSbDz4xKkSDz/Cg3X+WwmtWrxe6Brfd/wOG5Kn  
roVb+WsqjJwqDdB6ZZjV+oFfXfi0co7006yIxB/URQ+Vdryp9r/z7RoP4qTgxyu  
DjQVcxJiOQEYF6urO9vuCxEXAMPLEByakXuwnxv2wMF+X9tFH9nd2ajXOI8W5Vye  
ZV/ps2r0euJMEZ5Z6UTJ1lDYHoNwU75J5RnHvfqUKrJdBjtS8nPgan7MmYIstINp  
eSP/UnStUhbSMypWdL5Jq9bdY+qthDMxfAYUTg300SHhsrrDI/VnoGqZMcSnDLVc  
ee26nkHQ/AXbi6e4pPtch06PMSpbdubVK3iTlZS7kw3AiRcyG+L/EXAMPLElH6qH  
2mEXAMPLET0Cvs80EPmdPpyzAnh8lhe4SY1QYhndMBg7Jia322C3QEzEQeFqB5rV  
4aqRS6ibCJdWFudJv1WWM+x77TwLINzBrS2ZjK6H14LlLaKcu4WwceZ4WB1MRmeMt  
rSlcZX64/+9AmyTBLWutvA==
```



Figure 8: REvil URL for key input.

The ransom note provides the key to enter after navigating to either website. The ransom can be paid in either Monero or Bitcoin, although if the user chooses to pay in Bitcoin, this increases the cost by 10%:

Your network has been infected!



Your documents, photos, databases and other important files **encrypted**



To **decrypt your files** you need to buy our special software - **General-Decryptor**



Follow the instructions below. But remember that you do not have much time

General-Decryptor price
the price is for all PCs of your infected network

Time is over

* You didn't pay on time, the price was doubled

Current price

259289 XMR
≈ 100,000,000 USD

Monero address: 86u2HFPhvXt5PycXDh1zSKJ3xa6dmRu9FCH;

* XMR will be recalculated in 2 hours with an actual rate.

Figure 9: REvil warning re. price increase.

REvil also benefits from employing the effective tactic of double extortion. To encourage the victim to pay the ransom in a timely manner, the attacker threatens to publicly disclose or sell confidential stolen information on the dark web:

We launch a DDoS attack on your subnet.
We will attack until you pay.
Our resources allow us to conduct a DDoS attack for several years.
I recommend that you familiarize yourself with the history of TravelEx before and after our attack.
I also remind you that your data is being searched for a buyer from among competitors.

1 month ago

Well, what about constructive dialogue?
We know for sure that you have money, you know for sure that we have data of your internal network. And you know exactly that in case of non-payment we will publish information and damage you. Stock market already reacted, tell the management that it will only be worse if you continue to remain silent and think that without us

Figure 10: REvil double extortion tactics.

The following Yara rule was authored by the BlackBerry Threat Research Team to catch the threat described in this document:

Yara Rule:

```

import "pe"

rule Mal_Win_Ransom_REvil
{
    meta:
    description = "REvil sample April 2021"
    author = "Blackberry Threat Research"
    date = "2021-04"

    strings:
    $s1 = "bootcfg /raw /a /safeboot:network /id 1" nocase ascii
    $s2 = "bcdedit /set" nocase ascii
    $s3 = "safeboot network" nocase ascii
    $s4 = "Domain" nocase wide
    $s5 = "StopService" nocase wide
    $s6 = "GetOwner" nocase wide
    $s7 = "ERROR DOUBLE RUN!" nocase wide
    $s8 = "k-Err-" nocase wide
    $s9 = "Win32_Service" nocase wide

    condition:
    //PE File
    uint16(0) == 0x5A4D and
    // Filesize
    filesize < 130KB and
    // Import Hash
    pe.imphash() == "031931d2f2d921a9d906454d42f21be0" and
    // Five PE Sections
    pe.number_of_sections == 5 and
    // All Strings
    all of them
}

```

Indicators of Compromise (IoCs):

At BlackBerry, we take a prevention-first and AI-driven approach to cybersecurity. Putting prevention first neutralizes malware before the exploitation stage of the kill-chain. By stopping malware at this stage, BlackBerry solutions help organizations increase their resilience. It also helps reduce infrastructure complexity and streamline security management to ensure business, people, and endpoints are secure.

Registry Keys:

HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\BlackLivesMatter\[a-zA-Z0-9]{3}
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\BlackLivesMatter\[a-zA-Z0-9]{4}
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\BlackLivesMatter\[a-zA-Z0-9]{5}
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\BlackLivesMatter\[a-zA-Z0-9]{6}
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\BlackLivesMatter\[a-zA-Z0-9]{7}
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\BlackLivesMatter\[a-zA-Z0-9]{8}

AutoRun Registry Key:

HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Windows\CurrentVersion\Run\[a-zA-Z0-9]{10}

Custom Wallpaper Image:

C:\User\\AppData\Local\Temp\[a-zA-Z0-9]{13}.bmp

Encrypted Files:

<file_name>.<alpha-numeric_extension>

Ransom Note:

<alpha-numeric_extension>-readme.txt

URLs for Ransom Payment:

hxxp://aplebzu47wgazapdqks6vrcv6zcnjppkxbxr6wketf56nf6aq2nmyoyd[dot]onion/4DD2F2803EC112D7
hxxp://decoder[dot]re/4DD2F2803EC112D7

BlackBerry Assistance

If you're battling this 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 such as REvil 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>.

**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](#)