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:

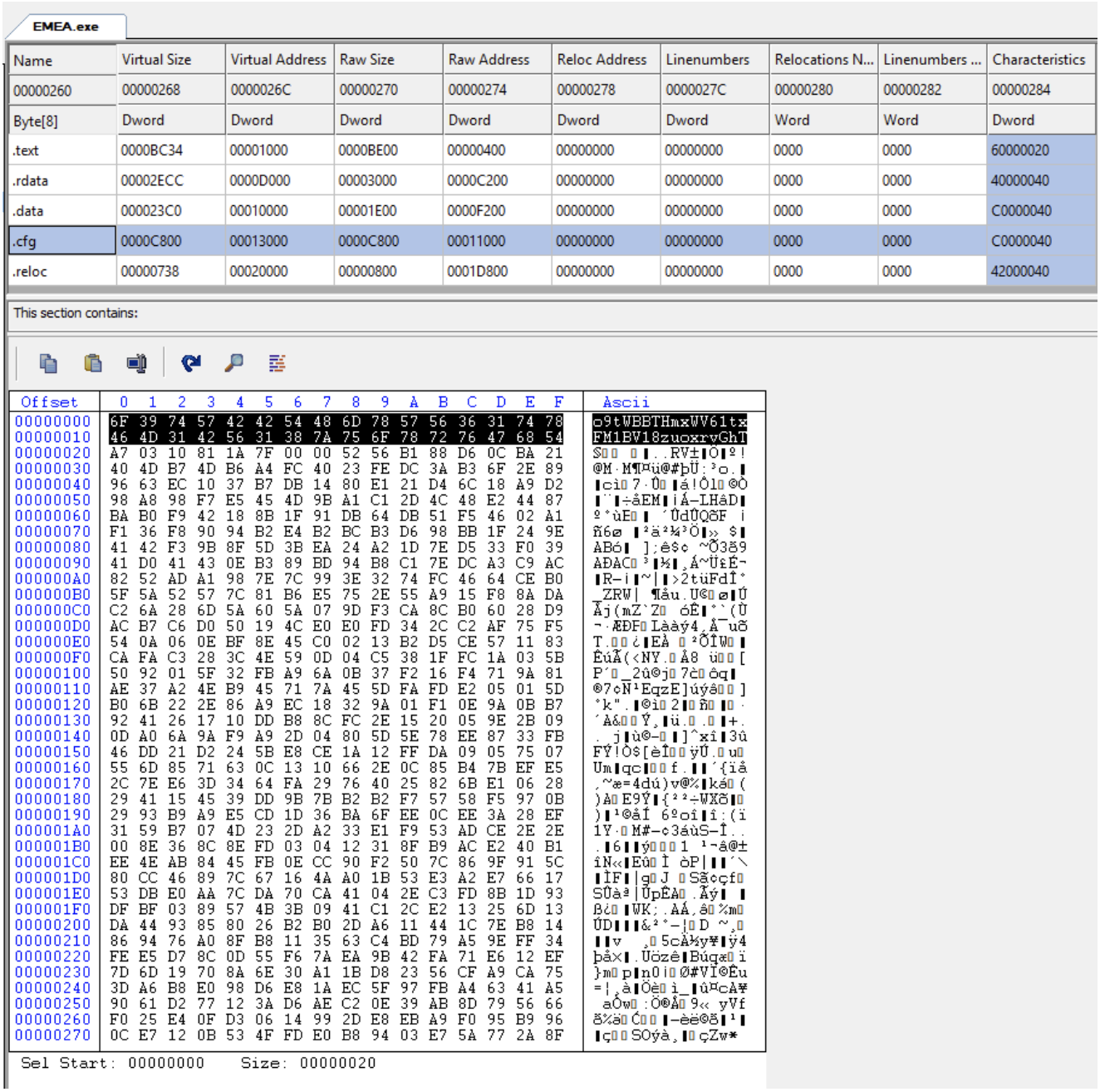

Figure 1: REvil's key is contained in the first 32 bytes.

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\aDTFUAla7j :

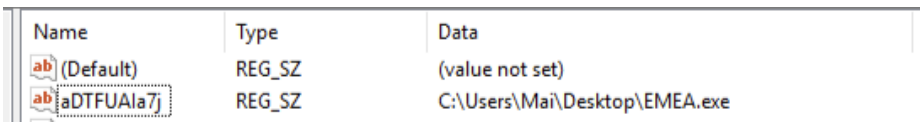

Figure 2: Registry key created.

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

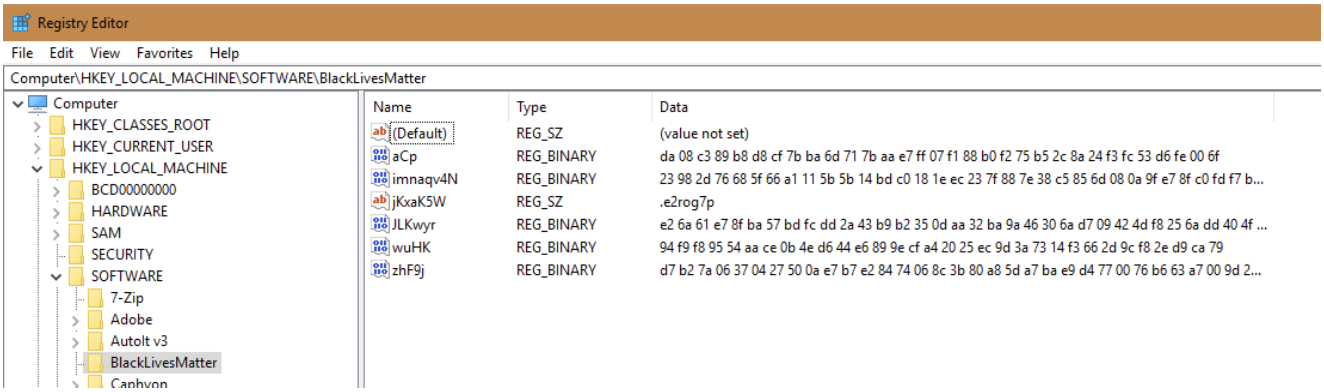

Figure 3: Hex values.

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:

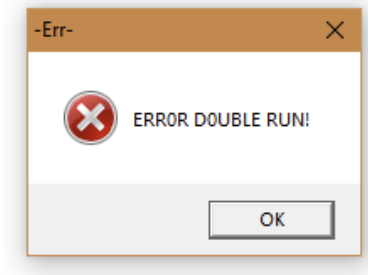

Figure 4: REvil error message.

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**":

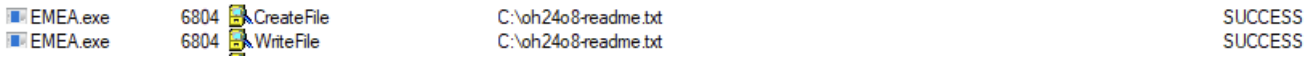

Figure 5: REVil ransom note text file.

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://aplebzu47wgazapdqks6vrcv6zcnjppkbxbr6wketf56nf6aq2nmyoyd.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:

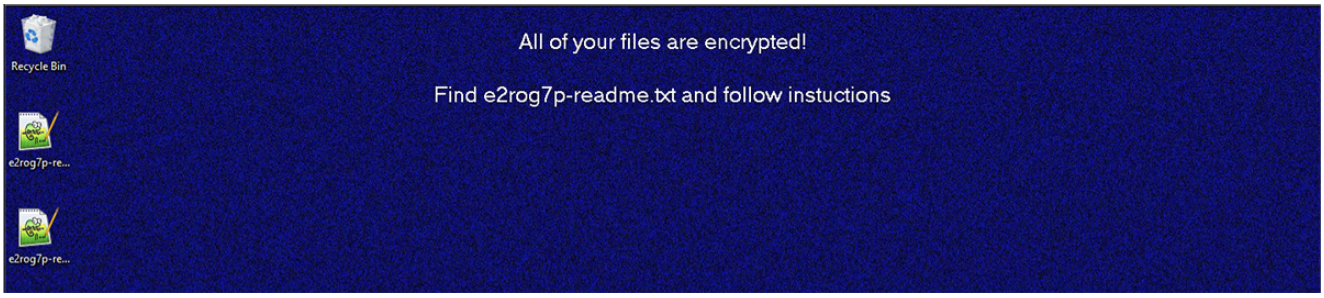

Figure 7: REvil wallpaper ransom note.

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:

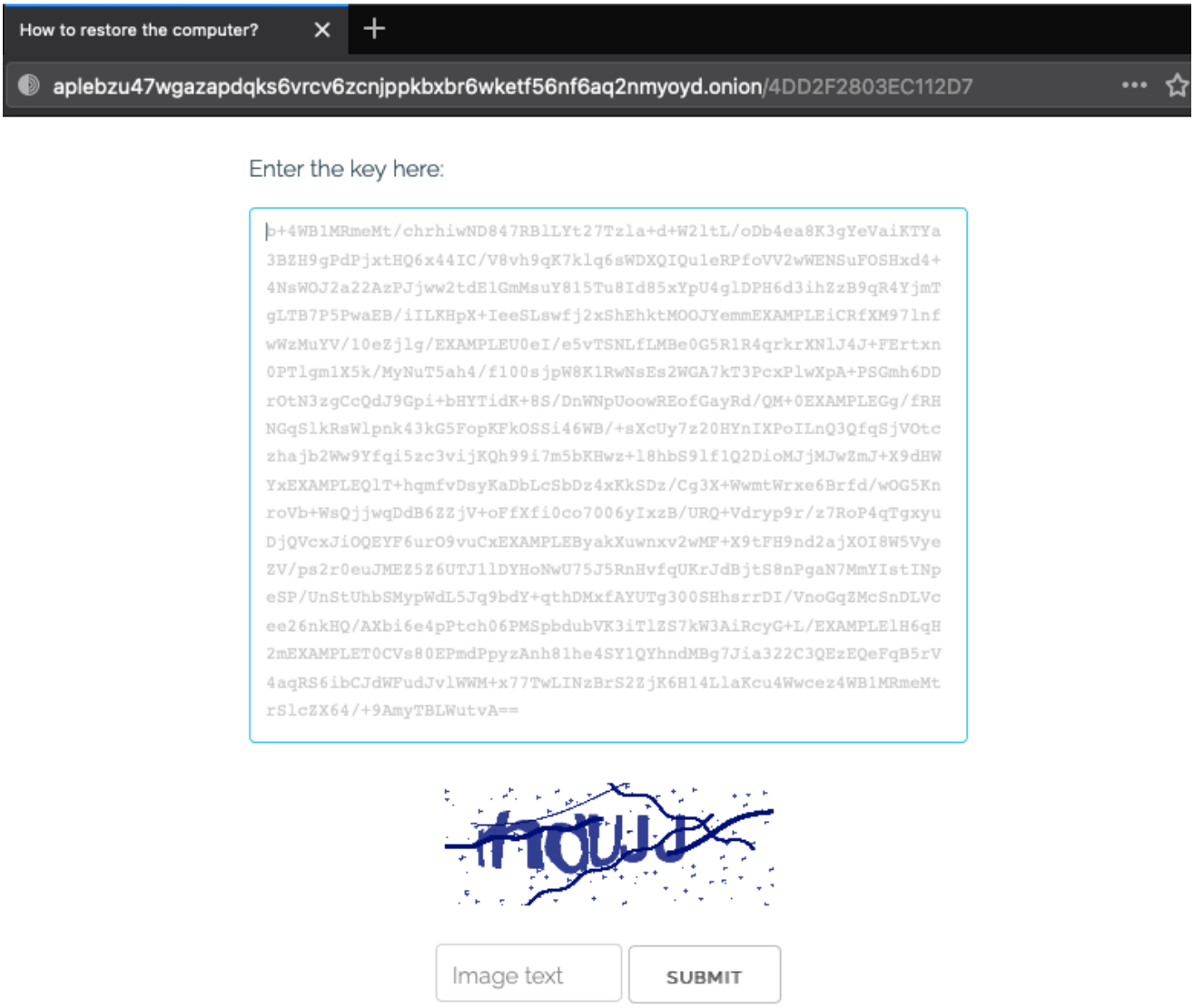

Figure 8: REvil URL for key input.

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%:

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:

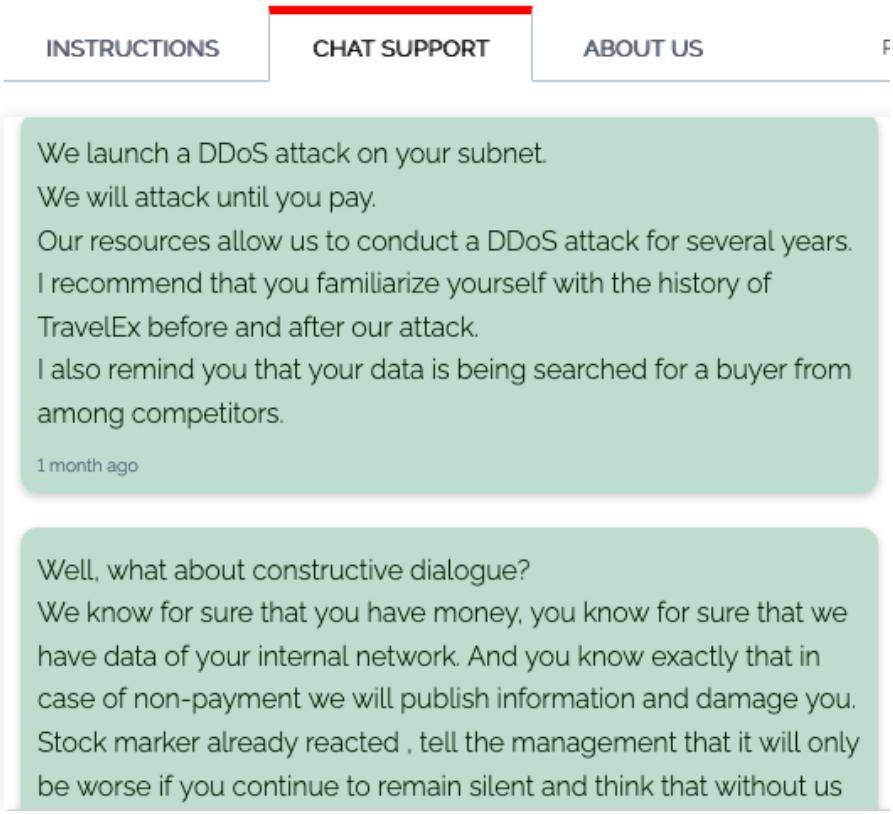

Figure 10: REvil double extortion tactics.

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 = "ERR0R D0UBLE 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\<Username>\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://aplebzu47wgazapdqks6vrcv6zcnjppkbxbr6wketf56nf6aq2nmyoyd[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