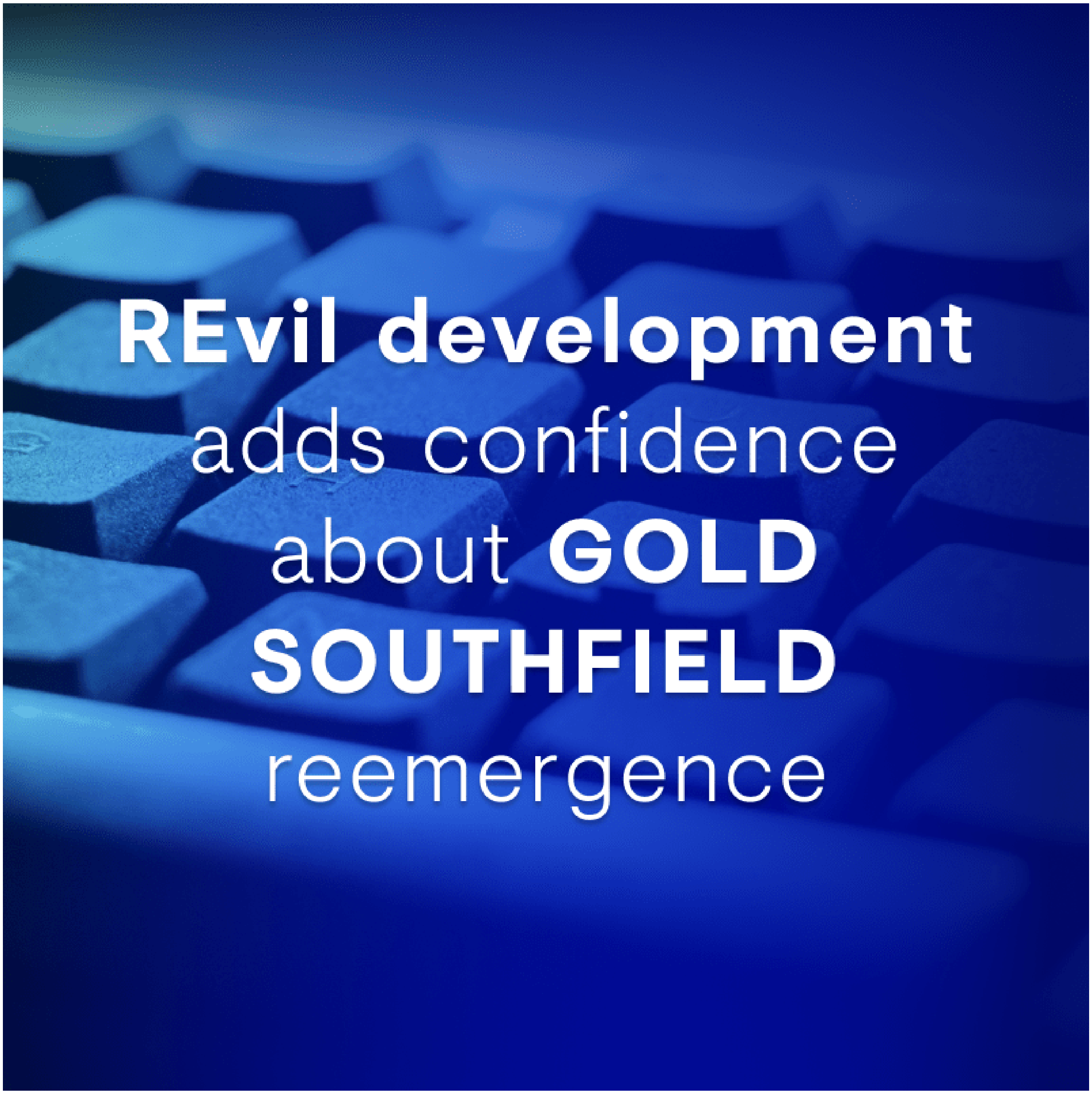
REvil Development Adds Confidence About GOLD SOUTHFIELD Reemergence

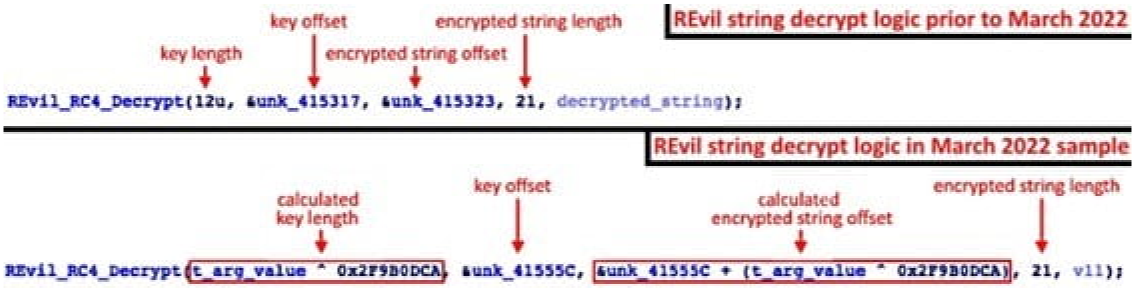
Counter Threat Unit Research Team



Secureworks® Counter Threat Unit™ (CTU) researchers analyzed REvil ransomware samples that were uploaded to the VirusTotal analysis service after the GOLD SOUTHFIELD threat group's infrastructure resumed activity in April 2022. The infrastructure had been shuttered since October 2021. Analysis of these samples indicates that the developer has access to REvil's source code, reinforcing the likelihood that the threat group has reemerged. The identification of multiple samples containing different modifications and the lack of an official new version indicate that REvil is under active development.

The March 22 sample contains artifacts in its configuration that indicate a likely link to a victim published to the REvil leak site in April. Despite a version value of 1.00, the sample has a compile timestamp of 2022-03-11 14:30:49 and includes functionality from a version 2.08 sample identified by CTU™ researchers in October 2021. The March 2022 sample includes the following modifications that distinguish it from the October 2021 sample:

- **Updates string decryption logic to rely on new command-line argument:** A change to the string decryption logic impacts REvil's ability to successfully execute. To run successfully, the threat actor must provide REvil with a pre-determined four-byte integer value between 0 and 4294967295 (0xFFFFFFFF). REvil uses this value during the string decryption process to calculate the RC4 decryption key length and the encrypted string offset. Prior REvil samples used hard-coded lengths and offset references. Figure 1 shows a comparison between the original logic and the logic implemented in the March 2022 sample.


REvil string decrypt logic prior to March 2022
key offset
encrypted string length
key length
encrypted string offset

```
REvil_RC4_Decrypt(12u, &unk_415317, &unk_415323, 21, decrypted_string);
```

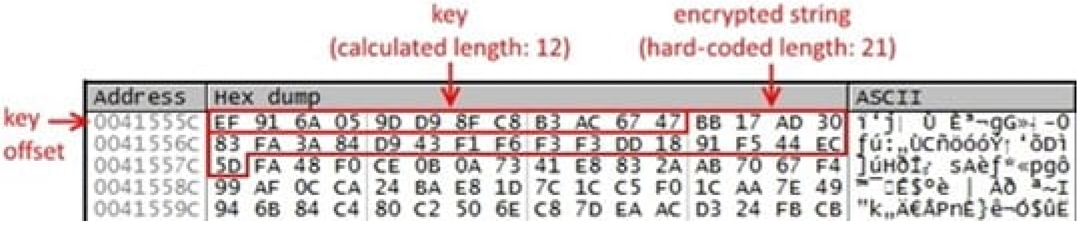
REvil string decrypt logic in March 2022 sample
calculated key length
key offset
calculated encrypted string offset
encrypted string length

```
REvil_RC4_Decrypt(t_arg_value ^ 0x2F9B0DCA, &unk_41555C, &unk_41555C + (t_arg_value ^ 0x2F9B0DCA), 21, v11);
```

Figure 1. String decrypt logic changes in the March 2022 sample. (Source: Secureworks)

This value is passed to the REvil executable via a new "-t" command-line argument. Failure to provide the argument and the correct value results in the executable's termination. Without the correct value, REvil cannot decrypt essential strings such as library and function names that are dynamically resolved at runtime. While this feature prevents network defenders from detonating the REvil sample in a sandbox environment if they do not know the pre-defined value, the unique command-line pattern could make the samples easier to detect and block.

CTU researchers determined that the integer value for the March 2022 sample shown in Figure 1 is 798690758 (e.g., "<*REvil executable filename*> -t=798690758"). The REvil code applies a bitwise XOR operation to the hex equivalent of 798690758 (0x2F9B0DC6) and the hard-coded value 0x2F9B0DCA, resulting in a calculated key length of 12. Because the key offset is known (0x41555C), the RC4 key and encrypted data can be extracted and processed using this calculated key length. Figure 2 shows an encrypted string structure in the March 2022 sample that starts with the RC4 key (EF916A059DD98FC8B3AC6747) followed by an encrypted string at the calculated offset (BB17AD3083FA3A84D943F1F6F3F3DD1891F544EC5D) that decrypts to CreateStreamOnHGlobal.

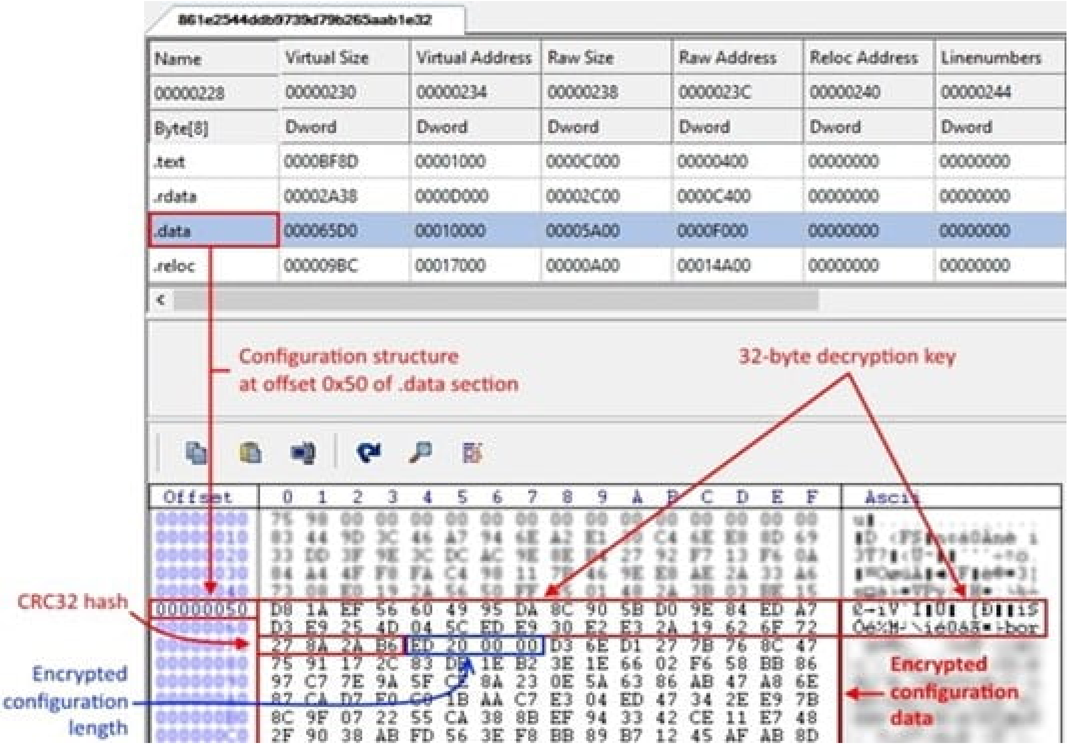


```
Address   Hex dump                                          ASCII
0041555C  EF 91 6A 05 9D D9 8F C8 B3 AC 67 47 BB 17 AD 30  ï'j| Ù È°¬gG»¡-0
0041556C  83 FA 3A 84 D9 43 F1 F6 F3 F3 DD 18 91 F5 44 EC  ƒú:„ÙCñöóóÝ¦'õDì
0041557C  5D FA 48 F0 CE 0B 0A 73 41 E8 83 2A AB 70 67 F4  ]úHðÎ♂ sAèƒ*«pgô
0041558C  99 AF 0C CA 24 BA E8 1D 7C 1C C5 F0 1C AA 7E 49  ™¯♀Ê$ºè | Åð ª~I
0041559C  94 6B 84 C4 80 C2 50 6E C8 7D EA AC D3 24 FB CB  "k„Ä€ÂPnÈ}ê¬Ó$ûË
```

Figure 2. Encrypted string storage structure at calculated offset. (Source: Secureworks)

- **Updates hard-coded public keys:** The malware author changed the two 32-byte hard-coded public keys used to secure artifacts compiled during the encryption session. GOLD SOUTHFIELD may have lost access to the original private key pairs, or those keys may have been exposed. The first key is stored at the start of the sample's .data section at offset 0x10. This key is used to encrypt the session's private key, which is generated at runtime and used to encrypt files. The ASCII representation of this key is 83449D3C46A7946EA2E130C46EE88D6933DD3F9E3CDCAC9E8EB42792F713F60A. The second key is stored in the sample's .data section at offset 0x30. This key is used to encrypt the "stats" JSON data that contains information about the encryption session (e.g., affiliate tracking information, encrypted session private key, victim's username, system's locale, drive details). The ASCII representation of this key is 84A44FF8FAC498117B469EE8AE2A33A67308E0192A5650FF0501482A3B03BE15.

- **Changes the configuration storage location:** The encrypted configuration structure is stored at offset 0x50 relative to the start of the sample's .data section. The decryption key stored at the start of this offset consists of 32 bytes ranging from 0x00 to 0xFF (see Figure 3).



861e2544ddb9739d79b265aab1e32

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers
00000228	00000230	00000234	00000238	0000023C	00000240	00000244
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword
.text	0000BF8D	00001000	0000C000	00000400	00000000	00000000
.rdata	00002A38	0000D000	00002C00	0000C400	00000000	00000000
.data	000065D0	00010000	00005A00	0000F000	00000000	00000000
.reloc	000009BC	00017000	00000A00	00014A00	00000000	00000000

```
Offset    0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   Ascii
00000000  75 98 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000010  83 44 9D 3C 46 A7 94 6E A2 E1 [illegible] C4 6E E8 8D 69
00000020  33 DD 3F 9E 3C DC AC 9E 8E [illegible] 27 92 F7 13 F6 0A
00000030  84 A4 4F F8 FA C4 98 11 [illegible] 46 9E E8 AE 2A 33 A6
00000040  73 08 E0 19 2A 56 50 FF [illegible] 01 48 2A 3B 03 BE 15
00000050  D8 1A EF 56 60 49 95 DA 8C 90 5B D0 9E 84 ED A7
00000060  D3 E9 25 4D 04 5C ED E9 30 E2 E3 2A 19 62 6F 72   Ó6%M-\í60â‚*-bor
00000070  27 8A 2A B6 ED 20 00 00 D3 6E D1 27 7B 76 8C 47
00000080  75 91 17 2C 83 DB 1E B2 3E 1E 66 02 F6 58 BB 86
00000090  97 C7 7E 9A 5F C2 8A 23 0E 5A 63 86 AB 47 A8 6E
000000A0  87 CA D7 F0 C0 1B AA C7 E3 04 ED 47 34 2E E9 7B
000000B0  8C 9F 07 22 55 CA 38 8B EF 94 33 42 CE 11 E7 48
000000C0  2F 90 38 AB FD 56 3E F8 BB 89 B7 12 45 AF AB 8D
```

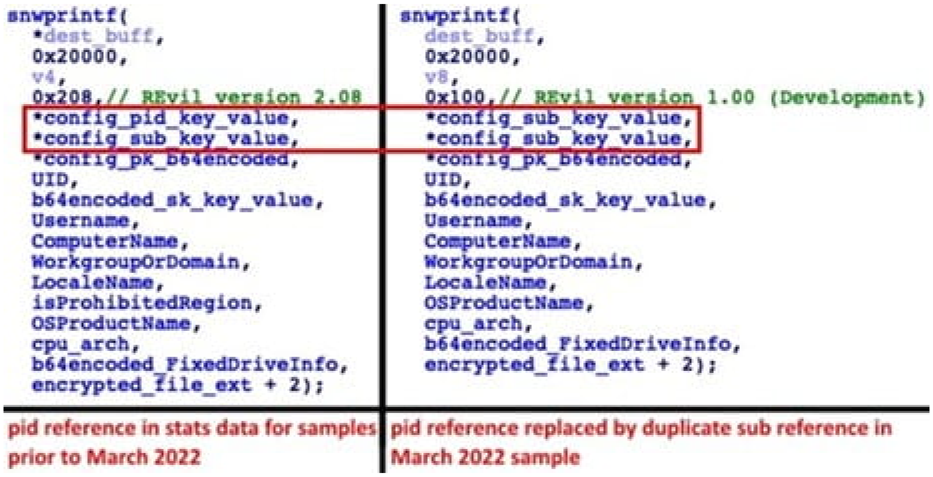
Figure 3. Configuration storage location in the March 2022 REvil sample. (Source: Secureworks)

Prior REvil versions stored the configuration structure at the start of the section (offset 0x00). In most cases, the structure was stored within a non-standard section (e.g., .kjmxo0e). The key in prior versions was limited to alphanumeric characters (e.g., gobpsd6RudAzmGciEytyLAjeGAk5H8Yd) as opposed to any byte value.

The overall configuration structure remains unchanged. It contains the decryption key (32 bytes), the precalculated CRC32 hash of the encrypted configuration (4 bytes), the encrypted configuration data length (4 bytes), and the RC4-encrypted configuration data.

- **Changes affiliate tracking data format:** When first introduced, REvil's affiliate tracking "pid" and "sub" values were stored as integers within the configuration. In February 2020, GOLD SOUTHFIELD started using bcrypt to hash these values to prevent researchers from tracking affiliates. The March 2022 sample changed the pid and sub value format to a globally unique identifier (GUID). The analyzed sample includes the following pid and sub values in its configuration:
    - pid: b78ad33f-32e9-4756-8c7b-83d46f8a0e19
    - sub: bb9ced79-3e79-4649-8fcc-3d4295fabc08

  The pid configuration element is never used, as the function that processed this configuration element was removed from the codebase. The only reference to the pid value was replaced with a duplicate sub reference (see Figure 4).



```
snwprintf(
  *dest_buff,
  0x20000,
  v4,
  0x208,// REvil version 2.08
  *config_pid_key_value,
  *config_sub_key_value,
  *config_pk_b64encoded,
  UID,
  b64encoded_sk_key_value,
  Username,
  ComputerName,
  WorkgroupOrDomain,
  LocaleName,
  isProhibitedRegion,
  OSProductName,
  cpu_arch,
  b64encoded_FixedDriveInfo,
  encrypted_file_ext + 2);
```

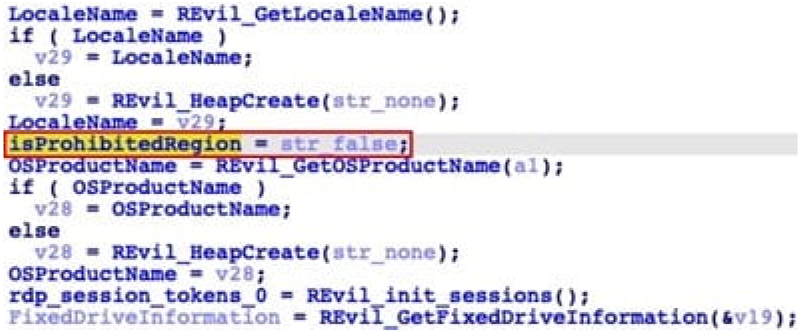
pid reference in stats data for samples prior to March 2022

```
snwprintf(
  dest_buff,
  0x20000,
  v8,
  0x100,// REvil version 1.00 (Development)
  *config_sub_key_value,
  *config_sub_key_value,
  *config_pk_b64encoded,
  UID,
  b64encoded_sk_key_value,
  Username,
  ComputerName,
  WorkgroupOrDomain,
  LocaleName,
  OSProductName,
  cpu_arch,
  b64encoded_FixedDriveInfo,
  encrypted_file_ext + 2);
```

pid reference replaced by duplicate sub reference in March 2022 sample

Figure 4. Comparison of stats data showing replacement of pid variable with duplicate sub variable in March 2022 sample. (Source: Secureworks)

- **Removes prohibited region check:** The October 2021 REvil sample removed code that verified the ransomware was not executing on a system that resided within a prohibited region. This removal enabled REvil to execute on any system regardless of its location. The isProhibitedRegion variable that was assigned the result of this check was still present in the code but was assigned a hard-coded value of "false" (see Figure 5).

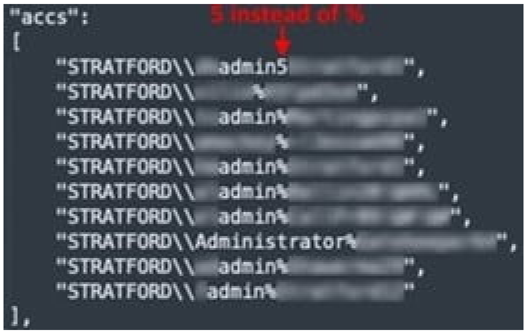
  ```
  LocaleName = REvil_GetLocaleName();
  if ( LocaleName )
    v29 = LocaleName;
  else
    v29 = REvil_HeapCreate(str_none);
  LocaleName = v29;
  isProhibitedRegion = str_false;
  OSProductName = REvil_GetOSProductName(a1);
  if ( OSProductName )
    v28 = OSProductName;
  else
    v28 = REvil_HeapCreate(str_none);
  OSProductName = v28;
  rdp_session_tokens_0 = REvil_init_sessions();
  FixedDriveInformation = REvil_GetFixedDriveInformation(&v19);
  ```

  Figure 5. Prohibited region variable assigned hard-coded value of false in October 2021 sample. (Source: Secureworks)

  The March 2022 sample removes this variable and no longer includes it in the stats data.

- **Leverages "accs" configuration element:** The accs configuration element introduced in the October 2021 sample did not contain a value, but CTU researchers determined that it should contain a list of strings that represent username and password combinations separated by the percent ("%") sign. If this value is defined, the ransomware uses the credentials to attempt authentication to protected network resources prior to encrypting their contents. However, it was unclear if the threat actor intended to list common username and password combinations or include credentials extracted from the targeted environment.

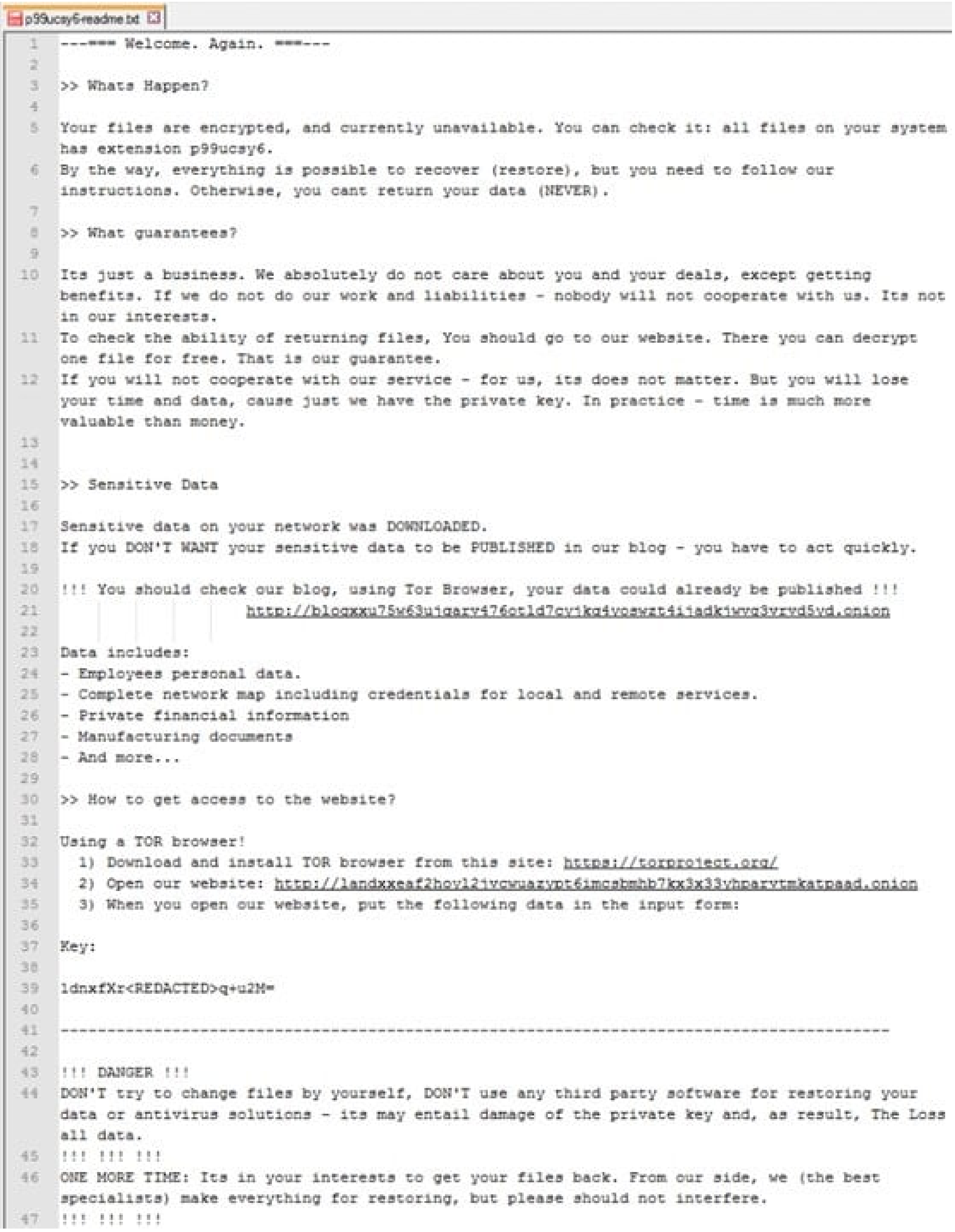
  The March 2022 sample includes values in the accs configuration element, and the credentials appear to be targeted. Most of the credentials were for specific administrative accounts (see Figure 6). A typo in one of the credentials ("5" instead of "%") suggests that the threat actors may manually format the values before including them in the configuration.

  ```
  "accs":
  [
      "STRATFORD\\[redacted]admin5[redacted]",
      "STRATFORD\\[redacted]%[redacted]",
      "STRATFORD\\[redacted]admin%[redacted]",
      "STRATFORD\\[redacted]%[redacted]",
      "STRATFORD\\[redacted]admin%[redacted]",
      "STRATFORD\\[redacted]admin%[redacted]",
      "STRATFORD\\[redacted]admin%[redacted]",
      "STRATFORD\\Administrator%[redacted]",
      "STRATFORD\\[redacted]admin%[redacted]",
      "STRATFORD\\[redacted]admin%[redacted]"
  ],
  ```

  Figure 6. Targeted credentials listed in the accs configuration element of the March 2022 sample. (Source: Secureworks)

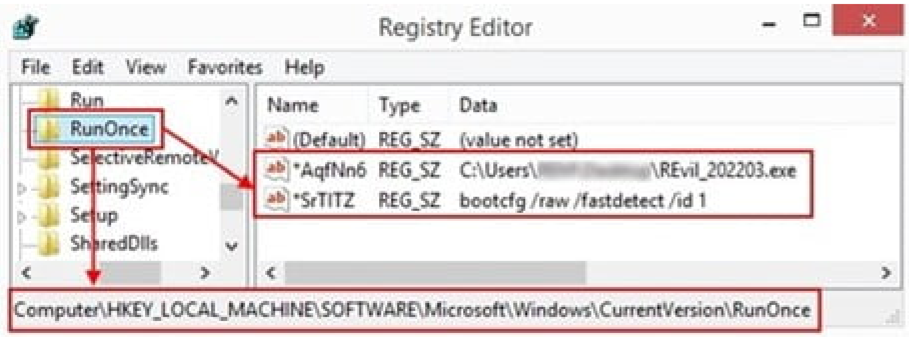
- **Includes new Tor domains in ransom note:** The ransom note dropped on a victim's system (see Figure 7) was updated to reference Tor domains that became active on April 19, 2022 when GOLD SOUTHFIELD's infrastructure resumed activity:
    - REvil leak site: blogxxu75w63ujqarv476otld7cyjkq4yoswzt4ijadkjwvg3vrvd5yd . onion
    - REvil ransom payment site: landxxeaf2hoyl2jvcwuazypt6imcsbmhb7kx3x33yhparvtmkatpaad . onion



```
---=== Welcome. Again. ===---

>> Whats Happen?

Your files are encrypted, and currently unavailable. You can check it: all files on your system
has extension p99ucsy6.
By the way, everything is possible to recover (restore), but you need to follow our
instructions. Otherwise, you cant return your data (NEVER).

>> 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 practice - time is much more
valuable than money.


>> Sensitive Data

Sensitive data on your network was DOWNLOADED.
If you DON'T WANT your sensitive data to be PUBLISHED in our blog - you have to act quickly.

!!! You should check our blog, using Tor Browser, your data could already be published !!!
                      http://blogxxu75w63ujqarv476otld7cyjkq4yoswzt4ijadkjwvg3vrvd5yd.onion

Data includes:
- Employees personal data.
- Complete network map including credentials for local and remote services.
- Private financial information
- Manufacturing documents
- And more...

>> How to get access to the website?

Using a TOR browser!
  1) Download and install TOR browser from this site: https://torproject.org/
  2) Open our website: http://landxxeaf2hoyl2jvcwuazypt6imcsbmhb7kx3x33yhparvtmkatpaad.onion
  3) When you open our website, put the following data in the input form:

Key:

1dnxfXr<REDACTED>q+u2M=

-----------------------------------------------------------------------------------------------

!!! DANGER !!!
DON'T try to change files by yourself, DON'T use any third party software for restoring your
data or antivirus solutions - its may entail damage of the private key and, as result, The Loss
all data.
!!! !!! !!!
ONE MORE TIME: Its in your interests to get your files back. From our side, we (the best
specialists) make everything for restoring, but please should not interfere.
!!! !!! !!!
```

Figure 7. REvil ransom note containing updated Tor domains for payment and leak sites. (Source: Secureworks)

- **Changes safe-mode option values:** The March 2022 sample modified safe-mode reboot details:
    - The password for the current user was set to "k$UqZy9zIC".
    - The RunOnce registry values used for post-reboot operations were set to "*AqfNn6" and "*SrTITZ" (see Figure 8).



Name	Type	Data
(Default)	REG_SZ	(value not set)
*AqfNn6	REG_SZ	C:\Users\[redacted]\REvil_202203.exe
*SrTITZ	REG_SZ	bootcfg /raw /fastdetect /id 1

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

Figure 8. Updated RunOnce registry values associated with REvil's safe-mode reboot. (Source: Secureworks)

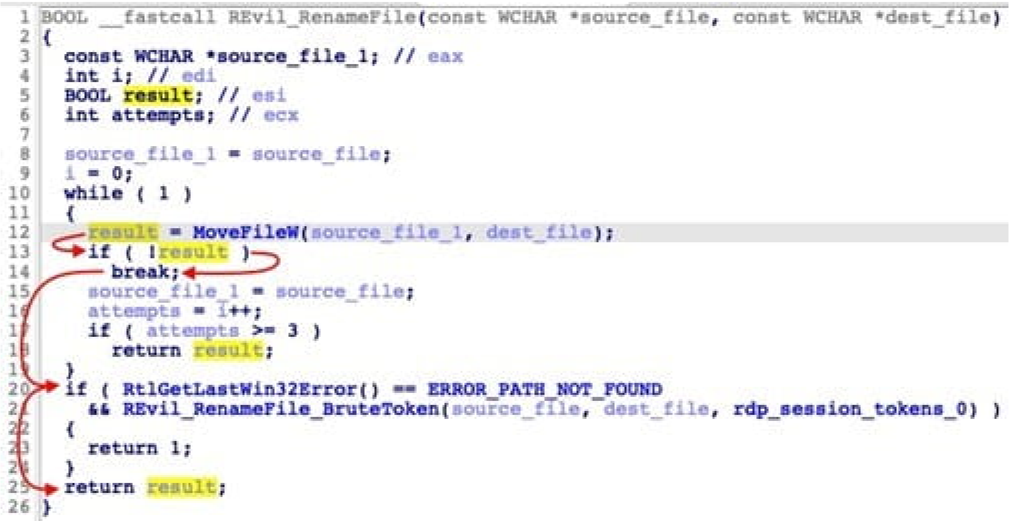
- **Updates registry key and values:** The registry key that stores encryption-related information was set to SOFTWARE\JnX5ywJ. The value names stored within this key also changed, which is consistent with the author's pattern of renaming registry values in each version. Table 1 lists the registry values in the March 2022 sample.

Registry Value	Purpose
3OG	Threat actor's public key in REvil's configuration
b2vr	Session public key
Elnzo	Session private key encrypted with the threat actor's public key in REvil's configuration
16uKrF7	Random extension generated at runtime and appended to encrypted files
E7w3RRdi	Encrypted 'stat' JSON data structure that contains information about the system and the malware

Table 1. REvil registry values used to store encryption data in the analyzed March 2022 sample.

On April 29, 2022, Twitter user @JakubKroustek detected a REvil sample with a compile timestamp of 2022-04-26 19:39:04 and a version value of 1.00. CTU analysis of the April 2022 sample revealed that its functionality is nearly identical to the March 2022 sample. However, the April 2022 sample does not contain the string decryption changes implemented in the March 2022 sample.

Third-party reporting claimed that the April 2022 sample did not encrypt files but instead renamed them to a random extension. CTU researchers determined that a bug caused this behavior. The malware author modified the functionality that renames files being encrypted. The bug resides within a test that determines if the file rename operation was successful (see Figure 9, line 13).



```
 1 BOOL __fastcall REvil_RenameFile(const WCHAR *source_file, const WCHAR *dest_file)
 2 {
 3   const WCHAR *source_file_1; // eax
 4   int i; // edi
 5   BOOL result; // esi
 6   int attempts; // ecx
 7
 8   source_file_1 = source_file;
 9   i = 0;
10   while ( 1 )
11   {
12     result = MoveFileW(source_file_1, dest_file);
13     if ( !result )
14       break;
15     source_file_1 = source_file;
16     attempts = i++;
17     if ( attempts >= 3 )
18       return result;
19   }
20   if ( RtlGetLastWin32Error() == ERROR_PATH_NOT_FOUND
21     && REvil_RenameFile_BruteToken(source_file, dest_file, rdp_session_tokens_0) )
22   {
23     return 1;
24   }
25   return result;
26 }
```

Figure 9. Code associated with file rename bug preventing file encryption in April 2022 sample. (Source: Secureworks)

Because the malware author used "if (!result)" instead of "if (result)", the file is successfully renamed on the first loop iteration but never breaks out of the loop. On the second loop iteration, the source file is missing because it has been renamed. As a result, the second file rename attempt fails and the file is never encrypted.

To mitigate exposure to this threat, CTU researchers recommend that organizations use available controls to review and restrict access using the indicators listed in Table 2. The domains may contain malicious content, so consider the risks before opening them in a browser.

Indicator	Type	Context
db2401798c8b41b0d5728e5b6bbb94cf	MD5 hash	March 2022 REvil sample
6620f5647a14e543d14d447ee2bd7fecc03be882	SHA1 hash	March 2022 REvil sample
861e2544ddb9739d79b265aab1e327d11617bc9d9c94bc5b35282c33fcb419bc	SHA256 hash	March 2022 REvil sample
ad49374e3c72613023fe420f0d6010d9	MD5 hash	April 2022 REvil sample

Indicator	Type	Context
eb563ab4caca7e19bdeee807b025ab2d54e23624	SHA1 hash	April 2022 REvil sample
0c10cf1b1640c9c845080f460ee69392bfaac981a4407b607e8e30d2ddf903e8	SHA256 hash	April 2022 REvil sample
blogxxu75w63ujqarv476otld7cyjkq4yoswzt4ijadkjwvg3vrvd5yd.onion	Domain name	REvil leak site in April 2022
landxxeaf2hoyl2jvcwuazypt6imcsbmhb7kx3x33yhparvtmkatpaad.onion	Domain name	REvil ransom payment site in April 2022

Table 2. Indicators for this threat.

To learn more about how ransomware groups adapt, read our Ransomware Evolution analysis and watch our Ransomware Trends: The Evolution of Threat webinar.

If you need urgent assistance with an incident, contact the Secureworks Incident Response team.