REvil Ransomware Reemerges After Shutdown; Universal Decryptor Released

secureworks.com/blog/revil-ransomware-reemerges-after-shutdown-universal-decryptor-released

Counter Threat Unit Research Team

After two months of inactivity following law enforcement actions, GOLD SOUTHFIELD resumed operations and released a new REvil version. The publication of a universal decryptor may help victims compromised prior to the shutdown. Wednesday, September 22, 2021 *By: Counter Threat Unit Research Team*

The ransomware landscape is constantly evolving as threat actors react to law enforcement interest, excessive media scrutiny, or adverse public opinion. 'Retirement' claims or an unexplained and sudden disappearance often indicate that a threat group is rebranding, reorganizing, or tightening operational security. Ransomware campaigns are financially driven, and the potential for profit incentivizes the threat actors to operate as long as possible. As demonstrated by a shutdown of GOLD SOUTHFIELD operations and subsequent reemergence of a new REvil version, threat groups modify their tactics and malware as necessary to address and minimize risks to their operations.

REvil shutdown

On September 7, 2021, Secureworks® Counter Threat Unit™ (CTU) researchers observed that the ransom payment site and victim leak site for the GOLD SOUTHFIELD threat group's REvil ransomware-as-a-service (RaaS) operation had resumed responding to web requests after abruptly going offline on July 13. On September 9, a newly created 'REvil' persona posted messages to the "exploit . in" underground forum explaining that the shutdown occurred because GOLD SOUTHFIELD spokesperson 'UNKN' (also known as Unknown) may have been arrested and the clearnet ransom payment servers were compromised (see Figure 1).

"As Unknown (aka 8800) disappeared, we (the coders) backed up and turned off all the servers. Thought that he was arrested. We tried to search, but to no avail. We waited - he did not show up and we restored everything from backups.

After UNKWN disappeared, the hoster informed us that the Clearnet servers were compromised and they deleted them at once. We shut down the main server with the keys right afterward.

Kaseya decryptor, which was allegedly leaked by the law enforcement, in fact, was leaked by one of our operators during the generation of the decryptor." - REvil

Figure 1. GOLD SOUTHFIELD spokesperson 'REvil' commenting on shutdown (translated from Russian). (Source: Bleeping Computer)

Reemergence with a new version

On September 9, CTU™ researchers identified a REvil sample on the VirusTotal analysis site that appears to be a new version. However, it includes a version value of 2.06. REvil 2.06 was released in April. The latest known version as of the shutdown was REvil 2.08, which was uploaded to VirusTotal on July 10. Despite the 2.06 version value, the September sample has a compilation timestamp of "Sat Sep 04 10:16:49 2021," which is almost two months after the shutdown. While it is possible to timestomp a binary's compilation timestamp, analysis of previous REvil samples indicates that GOLD SOUTHFIELD does not modify this value. It is highly likely that the September sample is a new version.

CTU analysis and the REvil persona's posts suggest that GOLD SOUTHFIELD was forced to restore the REvil codebase from a backup of version 2.06. Changes made in versions 2.07 and 2.08 were reverted in the analyzed September 2021 sample. For example, the original

2.06 version includes a function to terminate prohibited services that stored its strings in an unencoded state (see Figure 2).

```
int __cdecl REvil_WBEM_TerminateService(
        IWbemServices **WMI_ExecMethod,
        IWbemClassObject *WMI_GetObject1)
{
  OLECHAR *str_StopService; // esi
  int v3; // edi
  VARIANTARG Variant_PATH; // [esp+Ch] [ebp-10h] BYREF

  VariantInit(&Variant_PATH);
  str_StopService = SysAllocString(L"StopService");
  v3 = WMI_GetObject1->lpVtbl->Get(WMI_GetObject1, L"__PATH", 0, &Variant_PATH, 0, 0);
  if ( v3 >= 0 )
    v3 = WMI_ExecMethod[3]->lpVtbl->ExecMethod(
           WMI_ExecMethod[3],
           Variant_PATH.Name,
           str_StopService,
           0,
           0,
           0,
           0,
           0);
  VariantClear(&Variant_PATH);
  if ( str_StopService )
    SysFreeString(str_StopService);
  return v3;
}
```

Figure 2. Original REvil 2.06 use of unencoded strings. (Source: Secureworks)

In version 2.07, the malware author updated this and several other functions to store the strings in an encoded state (see Figure 3). However, the September 2021 sample reverted to unencoded strings.

```
int __cdecl REvil_WBEM_TerminateService(
        IWbemServices **WMI_ExecMethod,
        IWbemClassObject *WMI_GetObject1)
{
  OLECHAR *str_StopService; // esi
  int v3; // edi
  OLECHAR str_StopService_1[12]; // [esp+Ch] [ebp-38h] BYREF
  VARIANTARG Variant_PATH; // [esp+24h] [ebp-20h] BYREF
  char str__PATH[12]; // [esp+34h] [ebp-10h] BYREF
  __int16 v8; // [esp+40h] [ebp-4h]

  VariantInit(&Variant_PATH);
  REvil_DecodeString(&encoded_string_array, 639, 8, 22, str_StopService_1);// StopService
  str_StopService_1[11] = 0;
  str_StopService = SysAllocString(str_StopService_1);
  REvil_DecodeString(&encoded_string_array, 1196, 8, 12, str__PATH);// __PATH
  v8 = 0;
  v3 = WMI_GetObject1->lpVtbl->Get(WMI_GetObject1, str__PATH, 0, &Variant_PATH, 0, 0);
  if ( v3 >= 0 )
    v3 = WMI_ExecMethod[3]->lpVtbl->ExecMethod(
           WMI_ExecMethod[3],
           Variant_PATH.Name,
           str_StopService,
           0,
           0,
           0,
           0,
           0);
  VariantClear(&Variant_PATH);
  if ( str_StopService )
    SysFreeString(str_StopService);
  return v3;
}
```

Figure 3. Implementation of encoded strings in REvil 2.07. (Source: Secureworks)

CTU analysis of the September 2021 sample revealed the following modifications that distinguish it from previous versions:

- **Changes encrypted configuration storage location:** Previous REvil binaries contained five sections. The text, rdata, data, and reloc sections were common across all versions. The fifth section was randomly named and contained the RC4-encrypted configuration structure (see Figure 4).

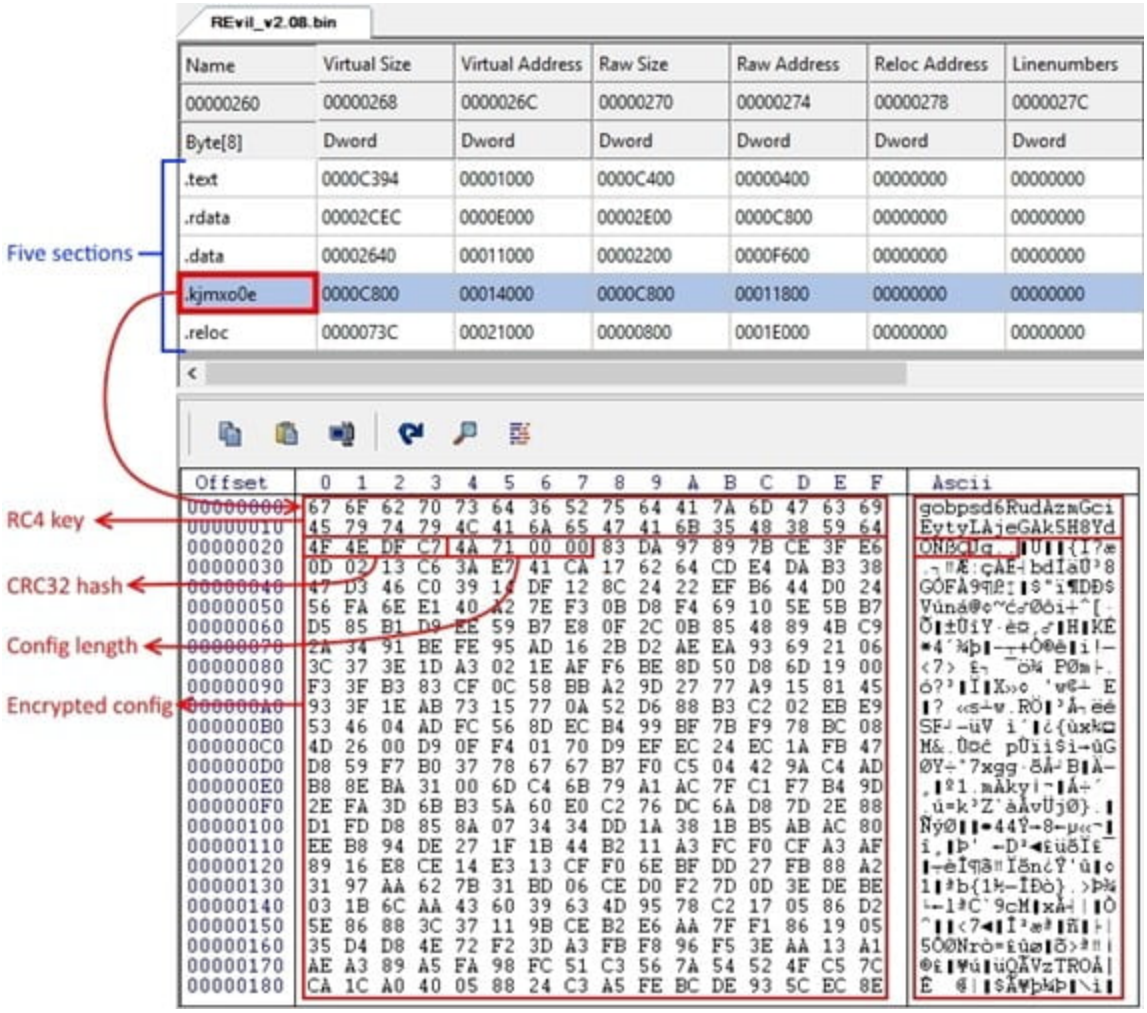


Figure 4. Original configuration storage format with five portable executable sections. (Source: Secureworks)

The September 2021 sample omits the fifth section, and the encrypted configuration was moved to the beginning of the existing data section (see Figure 5). The configuration remains RC4-encrypted, and the data structure still consists of the RC4 key, the CRC32 hash of the encrypted configuration, the length of the configuration, and the encrypted configuration.

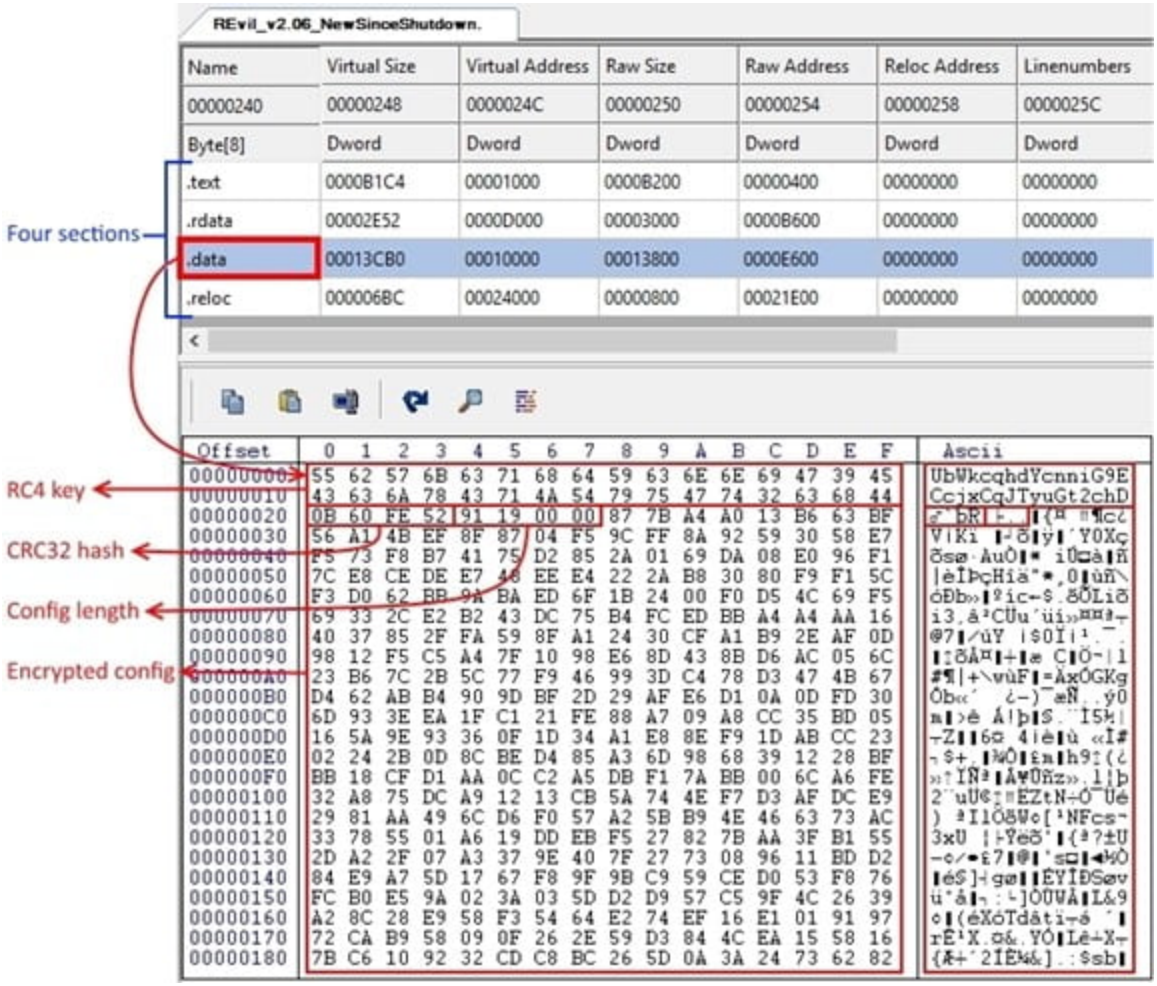


Figure 5. Analyzed September 2021 sample's configuration storage format with four portable executable sections. (Source: Secureworks)

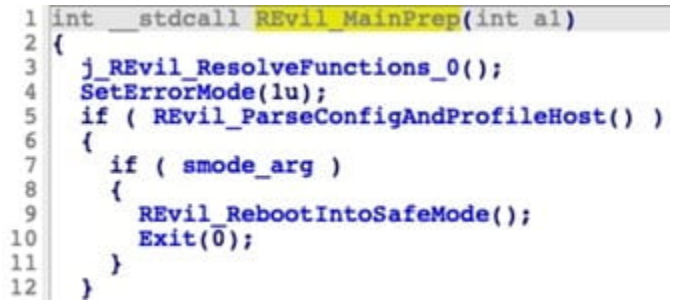
- **Removes debug and prohibited region checks:** Since its inception, REvil performed a pre-infection check to ensure that the compromised system did not reside within the Commonwealth of Independent States (CIS). This validation was controlled by a 'dbg' element contained within the REvil configuration. If the malware detected a CIS region and the dbg configuration element was set to false, REvil did not infect the system (see Figure 6). This behavior was one of several characteristics that suggested the threat actors likely reside within a CIS region.

```
int __stdcall REvil_MainPrep(int a1)
{
  void *v2; // [esp-8h] [ebp-8h]
  ULONG v3; // [esp-4h] [ebp-4h]

  j_REvil_ResolveFunctions_0();
  SetErrorMode(1u);
  if ( REvil_ParseConfigAndProfileHost() )
  {
    if ( !config_dbg_key_value && REvil_isProhibitedRegion() )
      Exit(0);
    if ( smode_arg )
    {
      REvil_RebootIntoSafeMode();
      Exit(0);
    }
  }
```

Figure 6. Original code with debug and prohibited region checks. (Source: Secureworks)

This validation was removed in the September 2021 sample (see Figure 7) although the dbg configuration element is still present in the configuration.



```
int __stdcall REvil_MainPrep(int a1)
{
  j_REvil_ResolveFunctions_0();
  SetErrorMode(1u);
  if ( REvil_ParseConfigAndProfileHost() )
  {
    if ( smode_arg )
    {
      REvil_RebootIntoSafeMode();
      Exit(0);
    }
  }
```

Figure 7. Analyzed September 2021 sample without debug and prohibited region checks. (Source: Secureworks)

As of this publication, it is unclear why this validation was removed. The validation likely protected the malware author, as infected systems within the CIS region could result in unwanted attention from local authorities. It is possible that the malware author removed this check in response to public reports that describe how organizations can leverage this feature to prevent ransomware infections. While the threat actors removed this check from the code, they instituted restrictions on which types of organizations affiliates could target to accomplish the same goal of avoiding organizations in the CIS region.

- **Changes password and registry values for safe mode option**: REvil 2.05 introduced a safe mode option. This reboot feature set the current user's password, configured automatic logon, created RunOnce registry values to handle post-reboot operations, and then rebooted the system. In the September 2021 sample, the current user's password was changed from 'DTrump4ever' to 'U1k$NEIq3c6Q'. The RunOnce registry values used for post-reboot operations were changed from '*AstraZeneca' to '*Ponyaz' and from '*MarineLePen' to '*b2l0uo' (see Figure 8).

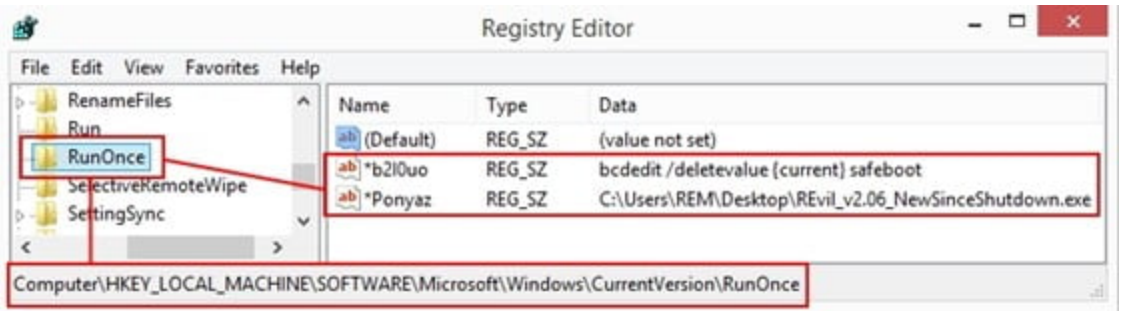


Figure 8. Updated safe mode registry values. (Source: Secureworks)

- **Removes persistence:** The persistence logic that resumes encryption if a victim reboots the system during the encryption process was removed in the September 2021 sample. The presence of persistence logic has been inconsistent across REvil versions.

- **Removes Network Discovery enablement:** REvil 2.07 introduced functionality that attempted to enable Network Discovery by executing the following command via the WinExec function: netsh advfirewall firewall set rule group="Network Discovery" new enable=Yes. It is possible that this functionality was not intentionally removed. If GOLD SOUTHFIELD restored the code from a version 2.06 backup, this feature had not yet been implemented.

- **Removes duplicate process termination functionality:** Starting with version 1.03, REvil implemented two redundant functions for process termination: a thread that continuously monitored for the creation of new “prohibited” processes, and an initial one-time scan for running processes considered to be prohibited (see Figure 9). Prohibited processes are defined in the ‘prc’ configuration element and are typically processes that could result in resource conflicts during the encryption process (e.g., sql, firefox, winword). Both functions attempted to terminate detected prohibited processes.

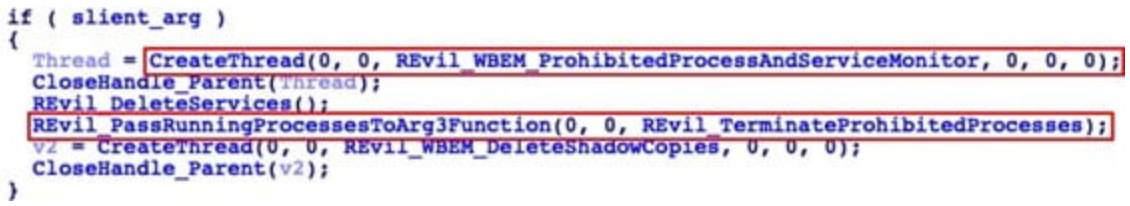


Figure 9. Redundant process termination functions included in the original code. (Source: Secureworks)

The September 2021 sample does not contain the initial scan for prohibited process termination. It only contains the more robust thread that continuously monitors for prohibited processes.

- **Removes C2 functionality:** After REvil successfully encrypts a system, it has an option to communicate basic details to one or more GOLD SOUTHFIELD command and control (C2) servers. If the 'net' configuration element is set to true, REvil sends encrypted data about the infected system, the malware's encryption, and the malware instance. CTU researchers refer to the encrypted data sent to the C2 servers as 'stats'. Figure 10 shows an example of the stats data structure in its unencrypted form.


```
{
    "bit": 86,
    "bro": false,
    "dsk": "QwADAAAAAPDf/xgAAAAA0LxsFQAAAA==",
    "grp": "WORKGROUP",
    "lng": "en-US",
    "net": "VICTIM-HOSTNAME",
    "os": "Windows 8.1 Pro",
    "pid": "7",
    "pk": "nAjfiPcoIyeIwwCkM1hLhXo5HUQMtrAB+7m8eHzerho=",
    "sk":
    "ww8h065kK3Tm7Thg/Y0nT3tSLReYMJUoaVVIkkDq8/L/5k1IcaoVF
    KkDtKcrdap6Q1mzZd+B6oAD2McVjLnWu6F/w0VVVHvGr/RJWfwH5cn
    Tppruevrgog==",
    "sub": "3",
    "uid": "F3FD1FCFF284306B",
    "unm": "VICTIM-USERNAME",
    "ver": 257
}
```


Figure 10. Example of the stats data structure in its unencrypted form. (Source: Secureworks)

While the 'net' configuration element is present in the September 2021 sample, the C2 logic was removed. The 'dmn' configuration element that stored approximately 1,200 C2 domains was also removed.

In the September 2021 sample, the stats data is only located within the ransom note dropped to disk during the file encryption process. The ransom note instructs the victim to submit the encrypted stats string to the ransom payment site to begin the ransom payment and data restoration process.

- **Discontinues clearnet ransom payment site:** GOLD SOUTHFIELD traditionally included both clearnet and Tor-based ransom payment domains in its ransom notes. The first REvil clearnet domain was decryptor . top, which was suspended by its registrar on January 20, 2020. GOLD SOUTHFIELD switched to decryptor . cc for approximately a year before switching to decoder . re on January 23, 2021. As of this publication, the decoder . re domain does not resolve to an IP address even though GOLD SOUTHFIELD's infrastructure is online. The ransom note references a 'secondary website' and does not include a clearnet domain (see Figure 11).

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

Using a TOR browser!
  1) Download and install TOR browser from this site: https://torproject.org/
  2) Open our website:
  http://aplebzu47wgazapdqks6vrcv6zcnjppkbxbr6wketf56nf6aq2nmyoyd.onion/8321BD91F284306B

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

Figure 11. Ransom note without the clearnet ransom payment domain. (Source: Secureworks)

- **Updates registry key and values:** The registry key that stores encryption-related information was changed from SOFTWARE\BlackLivesMatter, which was introduced in a beta version of REvil 2.04, to SOFTWARE\XMT0qpW. The value names stored within this key also changed, which is consistent with the author's pattern of renaming registry values in each version. The value used to store the encrypted session private key was removed, possibly to prevent unauthorized decryption of a victim's files if the threat actor's private keys are compromised. Table 1 defines the registry values in the September 2021 sample.

Registry Value	Purpose
JgC	Threat actor's public key in REvil's configuration
CsUQ	Session public key
5XB29	Session private key encrypted with the threat actor's public key in REvil's configuration
6mna6tT	Random extension generated at runtime and appended to encrypted files
OKDigiPr	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 September 2021 sample.

Universal decryptor

On September 16, Bitdefender announced a universal decryption tool for REvil infections that occurred prior to July 13. During CTU analysis, the tool successfully decrypted files encrypted by multiple REvil versions released prior to that date. This tool is not an offline decryptor. The infected system must connect to the internet to download the appropriate decryption key from Bitdefender's servers. Connecting to the internet could expose the compromised organization to unintended consequences such as new infections or data loss if additional malware is running on the infected system. Additionally, as of this publication Bitdefender has not disclosed if telemetry is collected from the network traffic to the decryption key server and how the vendor and law enforcement might use that information. CTU researchers highly recommend that organizations perform their own risk assessment before using this decryption tool.

Bitdefender's collaboration with law enforcement on the universal decryptor and the REvil spokesperson's claims that GOLD SOUTHFIELD's infrastructure was compromised suggest that law enforcement compromised the infrastructure and confiscated the threat group's private keys. In response, GOLD SOUTHFIELD appears to be reducing its attack surface by eliminating clearnet infrastructure and removing unnecessary features.

Conclusion

CTU researchers had hypothesized that GOLD SOUTHFIELD proactively shut down operations in response to the U.S. government's commitment to address the ransomware threat following high-profile attacks on Colonial Pipeline, JBS, and Kaseya. However, the REvil spokesperson's claims suggest that the shutdown was due to law enforcement actions against the threat group and its infrastructure. The reactivation of the group's infrastructure, the emergence of a new underground forum spokesperson, and evidence of active malware development indicate that GOLD SOUTHFIELD has resumed operations.

Ransomware attacks are often opportunistic. Threat actors search for systems that have lax security and exposed vulnerabilities. Organizations should implement good security practices and controls to secure their environments. Removing initial access vectors can minimize the risk of a ransomware attack. It is critical that organizations implement and routinely test a 3-2-1 backup strategy to ensure speedy recovery in the event of a successful ransomware attack.

Contact us to learn more about proactive steps. Our emergency incident response services can help ransomware victims.

Threat indicators

To mitigate exposure to this malware, 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
21d01fa87dfcaf971ff7b63a1a6fda94	MD5 hash	September 2021 REvil sample
f3caa9831fc715af4f47cd98803549902dffe30a	SHA1 hash	September 2021 REvil sample
ab0aa003d7238940cbdf7393677f968c4a252516de7f0699cd4654abd2e7ae83	SHA256 hash	September 2021 REvil sample
9ca7e337b99bfbb826b4f7f3b8b15589	MD5 hash	September 2021 REvil sample
7d79e62de12d81b1547217c01d70b5fdbf5a9658	SHA1 hash	September 2021 REvil sample
1780b5affc8c38d17ed35c4a6716d8a5a2f5d3a699f6a4c8a2f3e1e643324152	SHA256 hash	September 2021 REvil sample
aplebzu47wgazapdqks6vrcv6zcnjppkbxbr6wketf56nf6aq2nmyoyd.onion	Domain name	REvil ransom payment site
dnpscnbaix6nkwvystl3yxglz7nteicqrou3t75tpcc5532cztc46qyd.onion	Domain name	REvil leak site

Table 2. Indicators for this threat.