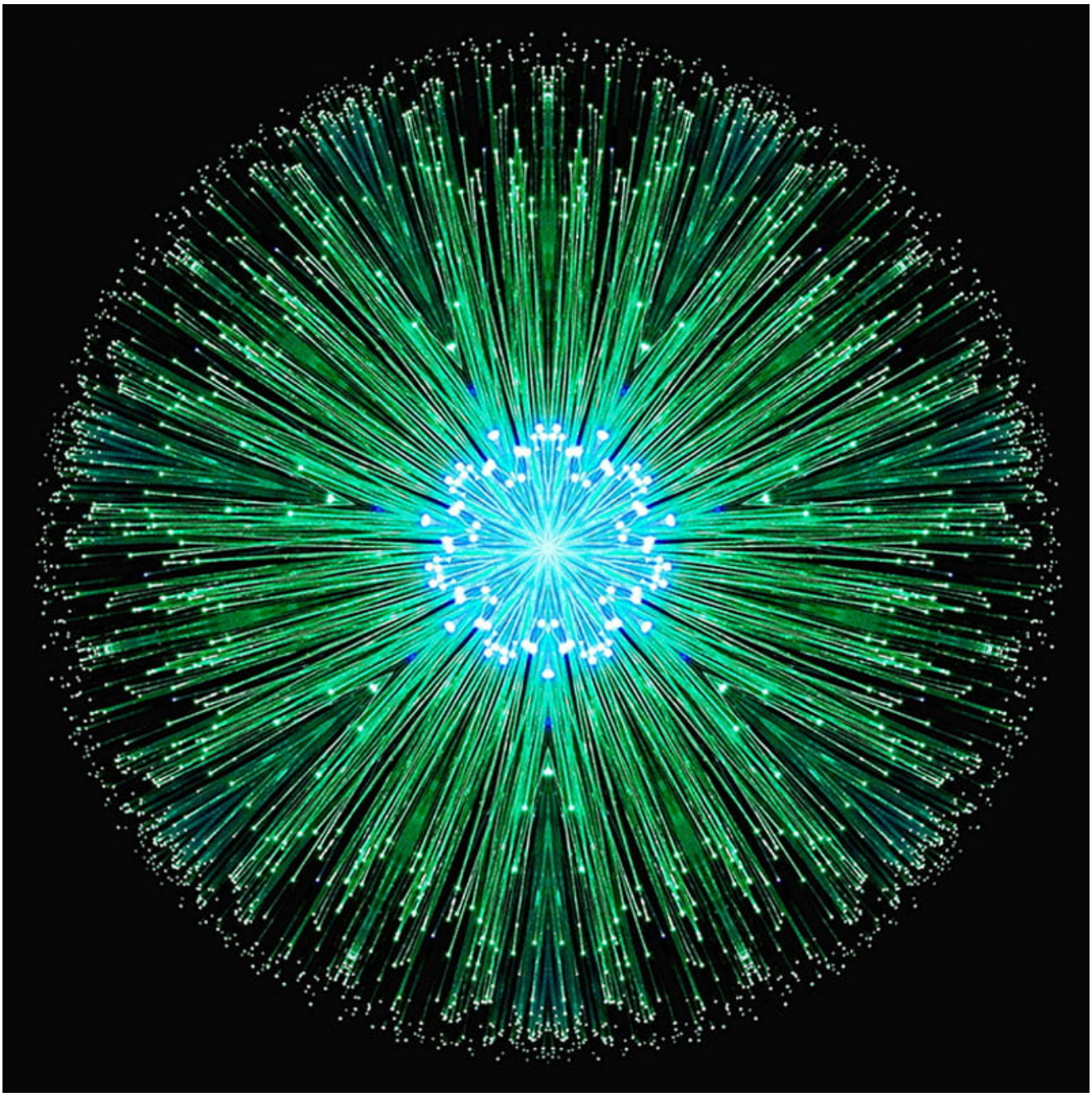
REvil: The GandCrab Connection

secureworks.com/blog/revil-the-gandcrab-connection

Counter Threat Unit Research Team



Technical links between the REvil and GandCrab ransomware families prove that the GandCrab malware authors did not retire in June 2019 as they claimed. Tuesday, September 24, 2019 *By: Counter Threat Unit Research Team*

On May 31, 2019, the developers of the highly profitable GandCrab 'ransomware-as-a-service' announced that they were retiring after earning over $2 billion USD since January 2018. The news was met with interest and skepticism within the security community, as

multiple affiliate groups regularly conducted extremely successful GandCrab campaigns since its inception. After analyzing the threat landscape, Secureworks® Counter Threat Unit™ (CTU) researchers determined that some or all of GandCrab's developers, which the CTU™ research team refers to as GOLD GARDEN, simply shifted their focus to a different ransomware variant.

Enter REvil

The REvil (also known as Sodinokibi) ransomware was first spotted in the wild (ITW) on April 17, when threat actors leveraged an Oracle WebLogic exploit to deliver both REvil and GandCrab. CTU analysis and tracking of REvil samples suggest that the ransomware was in development and testing between April 10 and May 7 and was not intended for public release.

Following the release of version 1.01 on May 7, the REvil developers, which CTU researchers refer to as GOLD SOUTHFIELD, began pushing a new release of the ransomware at the beginning of each month. The features and modifications of each version are listed in the Appendix of this blog post. As of this publication, August is the only skipped month. This cadence and the ransomware's capabilities indicate a structured development process by dedicated and experienced malware authors.

After GOLD GARDEN's retirement announcement, REvil activity increased with expanded delivery methods such as malicious spam campaigns and RDP attacks. This surge suggests that the ransomware operators deemed it ready for public release. On June 20, REvil was leveraged in a strategic web compromise (SWC) against the Italian WinRAR . it website, replacing the WinRAR installation executable with an instance of the malware to infect customers' systems. On the same day, threat actors breached at least three managed service providers (MSPs) and used the access to deploy REvil to the MSPs' customers. Other high-profile supply-chain attacks involving REvil have impacted 22 Texas municipalities and hundreds of dentist offices in the United States. Figure 1 shows a timeline of REvil releases and malicious activity.

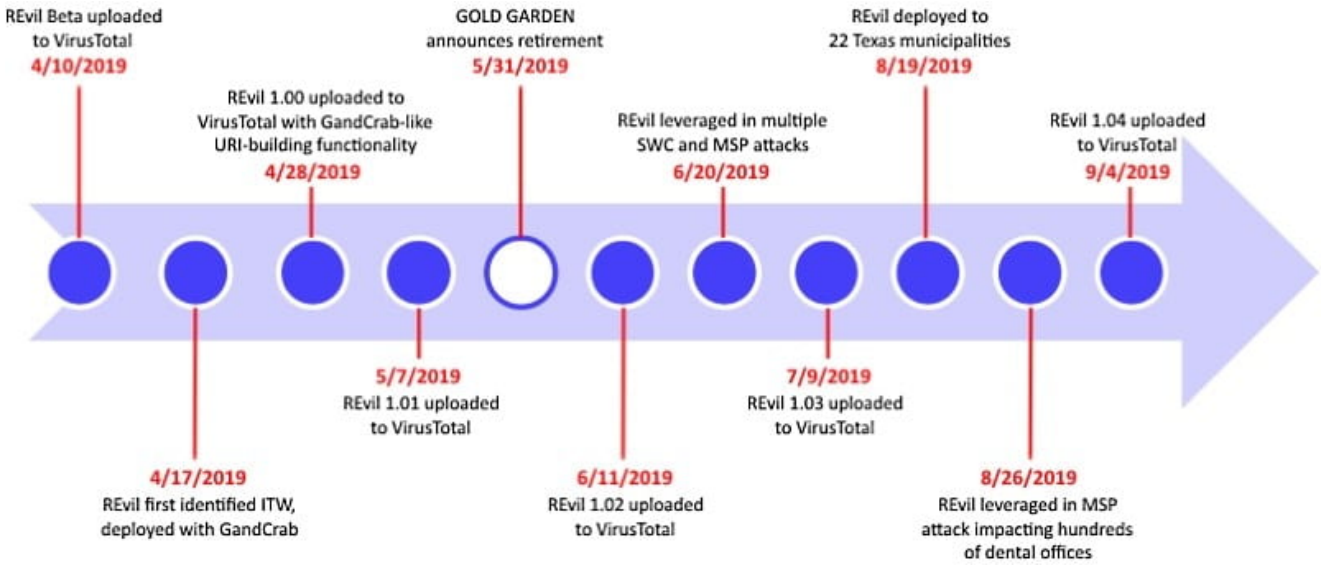


Figure 1. Timeline of REvil activity before and after GOLD GARDEN's retirement announcement. (Source: Secureworks)

Connecting the dots

Numerous characteristics indicate that the same developers were involved in producing GandCrab and REvil, suggesting a connection between members of the GOLD GARDEN and GOLD SOUTHFIELD threat groups. In a technical analysis of REvil version 1.01, CTU researchers identified possible overlap between REvil and GandCrab. Even the earliest identified REvil sample (REvil Beta) included elements that appear to refer to GandCrab.

Nearly identical string decoding function

CTU researchers found that the string decoding functions employed by REvil and GandCrab are nearly identical. Because malware authors typically implement custom encoding/decoding logic in their malware, the code can be used as a fingerprint to identify other samples associated with the malware family. When analyzing REvil, CTU researchers identified and extracted a portion of the opcodes (outlined in red in Figure 2) associated with its string decoding function.

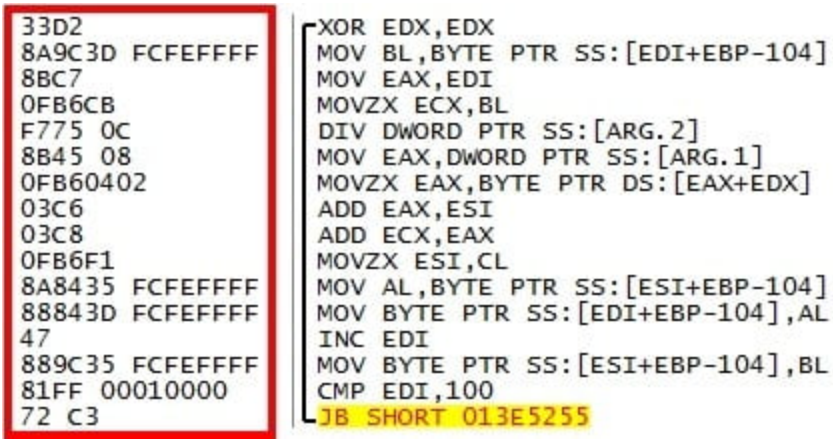


Figure 2. Opcodes for FOR-loop within REvil and GandCrab string decoder function. (Source: Secureworks)

When searching VirusTotal for samples containing this opcode pattern, 286 unique samples were identified. Further analysis of all 286 samples were confirmed to be either GandCrab or REvil (including REvil's decryptor). CTU researchers have not identified other malware families using this opcode pattern as of this publication, supporting the theory that these malware families share code.

Similar URL building logic

REvil 1.00 implements URL building functionality that produces the same command and control (C2) URL pattern as GandCrab. The C2 URLs for both families consist of two URI subpaths followed by a randomly generated resource name and an extension (see Figure 3). The subpath names and extension are retrieved from the hard-coded values listed in Table 1.

```
https://cymru.futbol/wp-content/assets/rjozgsac.gif
https://chorusconsulting.net/static/images/okhmjbkeggsrchqqwv.jpg
https://stagefxinc.com/uploads/pictures/audhents.png
https://kartuindonesia.com/data/temp/shen.jpg
https://craftingalegacy.com/content/pics/pqucnayd.png
https://cleanroomequipment.ie/admin/game/fhskeydbns.gif
```

Figure 3. Example C2 server URLs. (Source: Secureworks)

Values for first subpath	Values for second subpath	Extensions for resource
• wp-content • static • content • include • uploads • news • data • admin	• images • pictures • image • temp • tmp • graphic • assets • pics • game	• .jpg • .png • .gif • .bmp

Table 1. Hard-coded values for REvil and GandCrab C2 URLs.

While technically it would be possible for an unaffiliated threat actor to reproduce this logic within a separate malware family, doing so with such accuracy would require the threat actor to reverse engineer a GandCrab sample. Given the level of effort requires and the insignificant nature of the URI pattern, it is more likely that code originally created for GandCrab was repurposed in REvil.

Hints at GandCrab version 6

CTU analysis of the REvil Beta sample revealed two findings that are significant in proving a link between GandCrab and this first-identified version of REvil:

- **gcfin and gc6 debug paths** — A debug path is typically created by the integrated development environment (IDE) used by the malware author. Competent malware authors remove this information prior to distribution, as it could reveal the malware's name or details about the malware author's environment. The REvil Beta sample includes the d:\code\csrc\!1\new_a\gcfin\bin\debug\rwenc_exe_x86_debug.pdb debug path. gcfin is the malware author's name for the development project, and in context with other evidence appears to refer to “GandCrab Final”. Similarly, a discovered REvil file decryptor executable specifies the D:\\gc6\\core\\src\\common\\debug.c debug path. The reference to gc6 in the debug path could be a reference to GandCrab 6, which suggests that REvil was originally intended as GandCrab version 6.

- **REvil version 6.00?** — REvil populates a stat JSON data structure with information about the malware and the compromised host. Starting with REvil 1.00, the stat JSON is encrypted and sent to the attacker's C2 server. CTU researchers determined that the integer value assigned to the ver key located within the stat JSON represents the malware version. REvil interprets the value as hexadecimal. The REvil Beta sample includes the hard-coded value 1536, which converts to hexadecimal is 0x600 and indicates version 6.00. This version does not align with REvil's incremental numbering pattern as the next release is version 1.00, but it would align with the GandCrab numbering pattern given that the last observed version of GandCrab was 5.2.

Region whitelisting

Both REvil and GandCrab whitelist similar keyboard locales to prevent infection of Russia-based hosts. Malware authors commonly whitelist regions where they reside to prevent scrutiny from local law enforcement. This similarity does not establish a direct connection between REvil and GandCrab but does indicate that the malware authors likely reside in the same region.

Conclusion

GandCrab's 'ransomware-as-a-service model' proved to be a highly lucrative endeavor for GOLD GARDEN, so it is unlikely that the threat actors abandoned all malicious activity. Characteristics of REvil that appear to be operational security mistakes by the malware authors enabled CTU researchers to technically link the REvil and GandCrab ransomware families. This link indicates that the malware authors have shifted their focus from GandCrab to REvil.

Appendix — REvil version features and modifications

REvil Beta

MD5: bed6fc04aeb785815744706239a1f243
SHA1: 3d0649b5f76dbbff9f86b926afbd18ae028946bf
SHA256: 3641b09bf6eae22579d4fd5aae420476a134f5948966944189a70afd8032cb45

- Privilege escalation via CVE-2018-8453 (64-bit only)
- Rerun with RunAs to elevate privileges
- Implements a requirement that if “exp” is set, privilege escalation must be successful for full execution to occur
- Implements target whitelisting using GetKetboardLayoutList
- Contains debug console logging functionality
- Defines the REvil registry root key as SOFTWARE\!test
- Includes two variable placeholders in the ransom note: UID & KEY
- Terminates processes specified in the “prc” configuration key prior to encryption
- Deletes shadow copies and disables recovery
- Wipes contents of folders specified in the "wfld" configuration key prior to encryption
- Encrypts all non-whitelisted files on fixed drives
- Encrypts all non-whitelisted files on network mapped drives if it is running with System-level privileges or can impersonate the security context of explorer.exe
- Partially implements a background image setting to display a basic "Image text" message
- Sends encrypted system data to a C2 domain via an HTTPS POST request (URI path building is not implemented.)

REvil 1.00

MD5: 65aa793c000762174b2f86077bdafaea
SHA1: 95a21e764ad0c98ea3d034d293aee5511e7c8457
SHA256: f0c60f62ef9ffc044d0b4aeb8cc26b971236f24a2611cb1be09ff4845c3841bc

- Adds 32-bit implementation of CVE-2018-8453 exploit
- Removes console debug logging
- Changes the REvil registry root key to SOFTWARE\recfg
- Removes the System/Impersonation success requirement for encrypting network mapped drives
- Adds a "wipe" key to the configuration for optional folder wiping
- Fully implements the background image setting and leverages values defined in the “img” configuration key
- Adds an EXT variable placeholder to the ransom note to support UID, KEY, and EXT
- Implements URI path building so encrypted system data is sent to a C2 pseudo-random URL
- Fixes the function that returns the victim's username so the correct value is placed in the stats JSON data

REvil 1.01

MD5: 2abff29b4d87f30f011874b6e98959e9
SHA1: 9d1b61b1cba411ee6d4664ba2561fa59cdb0732c
SHA256: a88e2857a2f3922b44247316642f08ba8665185297e3cd958bbd22a83f380feb

- Removes the exp/privilege escalation requirement for full execution and encrypts data regardless of privilege level
- Makes encryption of network mapped drives optional by adding the “-nolan” argument

REvil 1.02

MD5: 4af953b20f3a1f165e7cf31d6156c035
SHA1: b859de5ffcb90e4ca8e304d81a4f81e8785bb299
SHA256: 89d80016ff4c6600e8dd8cfad1fa6912af4d21c5457b4e9866d1796939b48dc4

- Enhances whitelisting validation by adding inspection of GetUserDefaultUILanguage and GetSystemDefaultUILanguage
- Partially implements “lock file” logic by generating a lock filename based on the first four bytes of the Base64-decoded pk key, appending a .lock file extension, and adding the filename to
  the list of whitelisted files in the REvil configuration (It does not appear that this value is referenced after it is created and stored in memory. There is no evidence that a lock file is dropped to disk.)
- Enhances folder whitelisting logic that take special considerations if the folder is associated with "program files" directories
  - Hard-codes whitelisting of all direct content within the Program Files or Program Files x86 directories
  - Hard-codes whitelisting of "sql" subfolders within program files
  - Encrypts program files sub-folders that does not contain "sql" in the path
  - Compares other folders to the list of whitelisted folders specified in the REvil configuration to determine if they are whitelisted
- Encodes stored strings used for URI building within the binary and decodes them in memory right before use
- Introduces a REvil registry root key "sub_key" registry value containing the attacker's public key

REvil 1.03

MD5: 3cae02306a95564b1fff4ea45a7dfc00
SHA1: 0ce2cae5287a64138d273007b34933362901783d
SHA256: 78fa32f179224c46ae81252c841e75ee4e80b57e6b026d0a05bb07d34ec37bbf

- Removes lock file logic that was partially implemented in 1.02
- Leverages WMI to continuously monitor for and kill newly launched processes whose names are listed in the prc configuration key (Previous versions performed this action once.)
- Encodes stored shellcode
- Adds the -path argument:
  - Does not wipe folders (even if wipe == true)
  - Does not set desktop background
  - Does not contact the C2 server (even if net == true)
  - Encrypts files in the specified folder and drops the ransom note
- Changes the REvil registry root key to SOFTWARE\QtProject\OrganizationDefaults
- Changes the registry key value names

REvil 1.04

MD5: 6e3efb83299d800edf1624ecbc0665e7
SHA1: 0bd22f204c5373f1a22d9a02c59f69f354a2cc0d
SHA256: 2ca64feaaf5ab6cf96677fbc2bc0e1995b3bc93472d7af884139aa757240e3f6

- Leverages PowerShell and WMI to delete shadow copies if the victim's operating system is newer than Windows XP (For Windows XP or older, it uses the original command that was executed in all previous REvil versions.)
- Removes the folder wipe capability
- Changes the REvil registry root key to SOFTWARE\GitForWindows
- Changes the registry key value names