Travelex Hit by an Alleged Ransomware Attack

January 2020

Cyberint

Contents

Executive Summary

On 2 January 2020, Travelex released a statement confirming that a virus attack compromised some of its services on 31 December 2019. The virus has subsequently been identified as a ransomware variant named Sodinokibi, also known as REvil.

REvil is a fairly sophisticated threat that uses various anti-analysis tricks and execution mechanisms to encrypt the victim's machine and common files and have the victim pay ransom to decrypt their data.

Travelex is one of the world's largest foreign exchange service providers with almost 800 retail branches in more than 25 countries, serving large global organizations like Barclays, HSBC, Tesco, Sainsbury's, ASDA, Virgin Money, First Direct, Natwest, RBS, Manchester Airport and London Heathrow Airport.

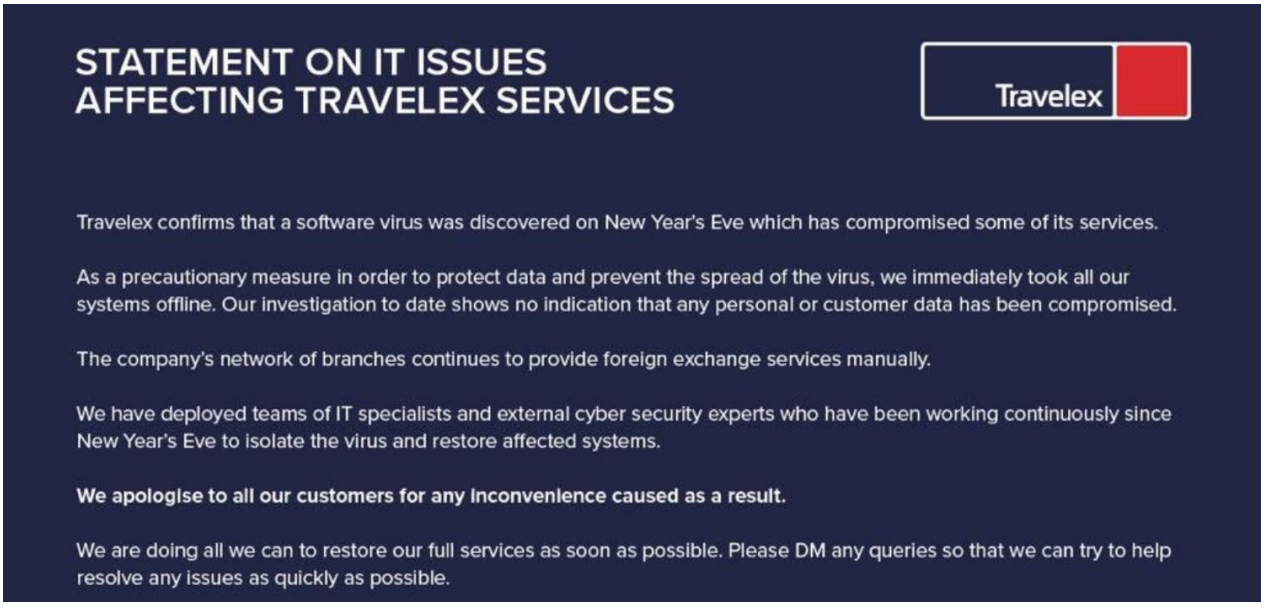


Figure 1 - Travelex Public Statement

CyberInt Research is actively tracking the REvil malware family provided as RaaS (Ransomware-as-a-Service) across various underground marketplaces. In recent months, an increase of what is known as a "big game" ransom was detected – with cybercriminal groups extorting organizations to pay huge ransoms to release their encrypted data.

"Big game" ransom attacks are becoming more frequent and represent a shift from common ransomware attacks that previously targeted small organizations or end users with relatively small ransom demands, typically averaging hundreds of dollars, to targeting large enterprises requesting larger amounts of ransom demands, potentially in the tens and hundreds of thousands of dollars or even millions.

Publicly available information suggests that the REvil ransomware has been delivered by targeting unpatched Pulse Secure VPN services using CVE-2019-11510 [1]and CVE-2019-11539[2], allowing the threat actor to gain access to a victim network and deploy the threat.[3] Public reporting also suggests that Travelex has, or had, at least seven Pulse Secure VPN nodes that could have provided a potential attack vector.[4]

Additional opensource information[5] may also indicate an additional attack vector in the form of a publicly accessible Windows Server, hosted on Amazon Web Services (AWS) with the Remote Desktop Protocol (RDP) enabled and Network Layer Authentication[6] (NLA) disabled. This configuration negates the need for users to authenticate themselves *before* a session is established with the server.

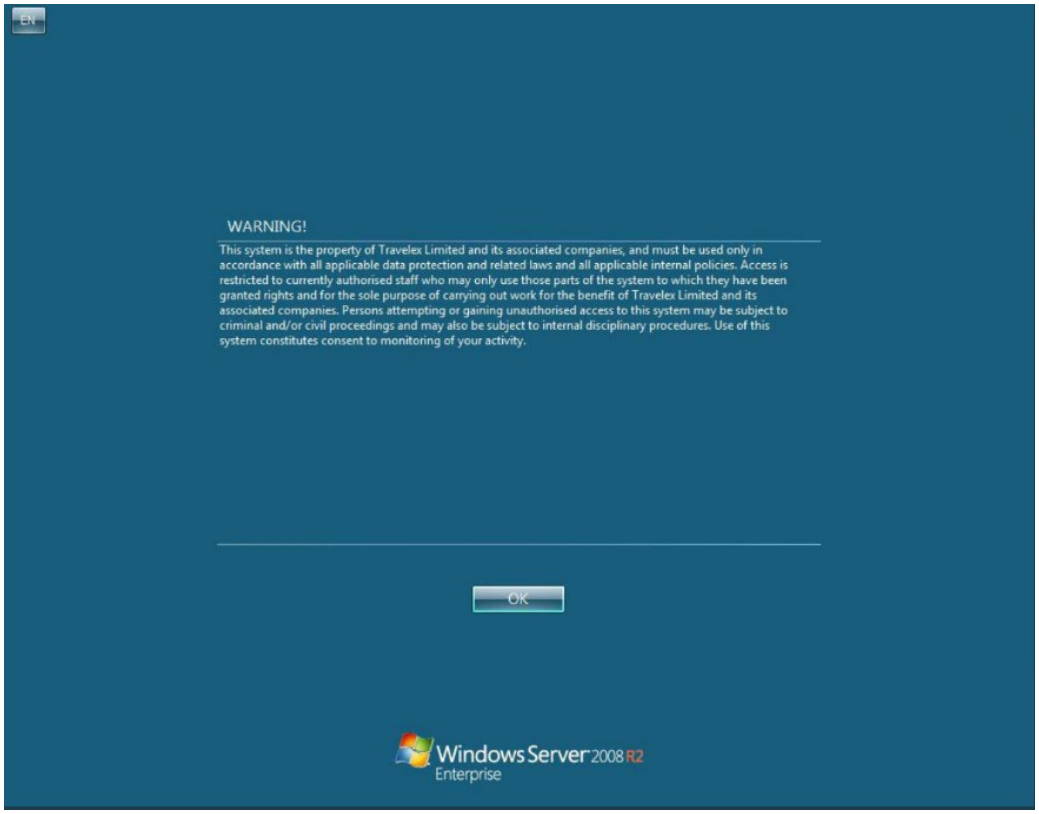


Figure 2 - Publicly Accessible RDP belonging to Travelex

Finally, a third potential attack vector has been suggested[7] with the threat actors behind REvil compromising Managed Service Providers (MSP) to gain access to remote management tools, uninstalling endpoint protection software and deploying their REvil ransomware.

[1] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11510
[2] https://nvd.nist.gov/vuln/detail/CVE-2019-11539
[3] https://www.zdnet.com/article/vpn-warning-revil-ransomware-targets-unpatched-pulse-secure-vpn-servers/
[4] https://twitter.com/GossiTheDog/status/1213532072201084929/photo/1
[5] https://twitter.com/GossiTheDog/status/1212874282596012032/photo/1
[6] https://en.wikipedia.org/wiki/Network_Level_Authentication
[7] https://www.zdnet.com/article/ransomware-gang-hacks-msps-to-deploy-ransomware-on-customer-systems/

Breach Description

On 2 January 2020, Travelex, one of the world's largest foreign exchange service providers with almost 800 retail branches in more than 25 countries and serving large global organizations including Barclays, HSBC, Tesco, Sainsbury's, Natwest, RBS and London's Heathrow Airport, released a statement confirming that a virus attack occurred on 31 December 2019 leading to the compromise of some of its services.

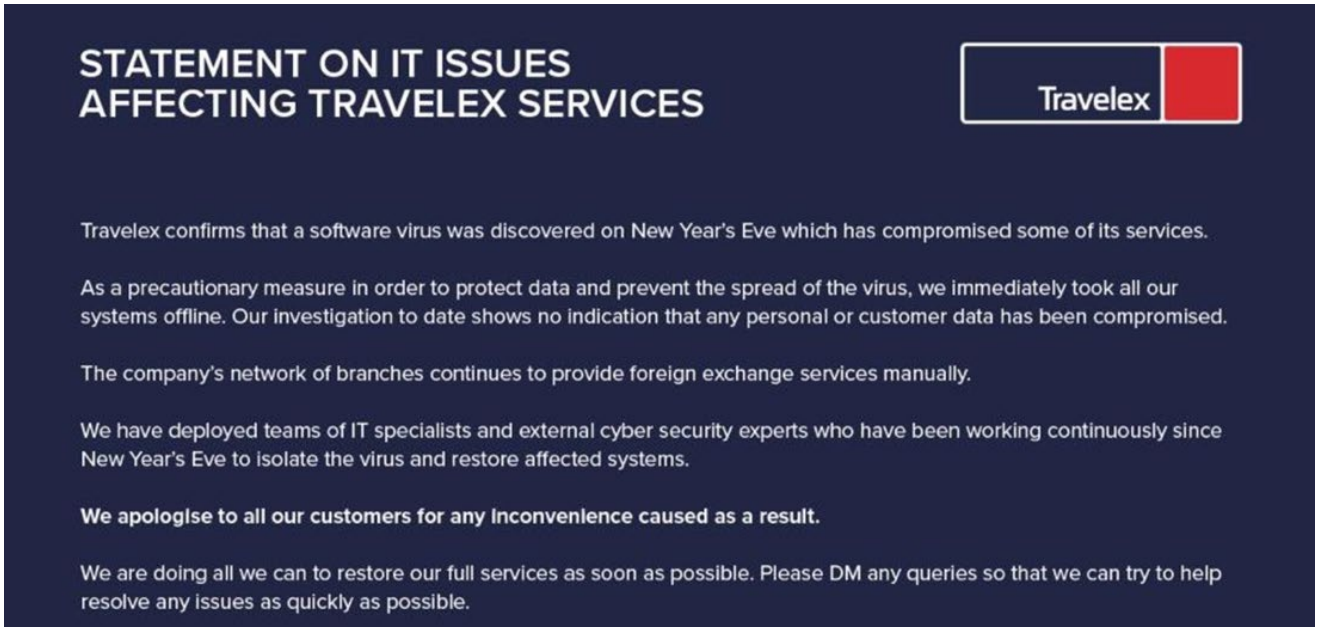


Figure 3 - Travelex Public Disclosure

Early reporting suggests that the virus attack was a ransomware variant named Sodinokibi, also known as REvil. CyberInt Research are actively tracking the REvil malware family that is provided as Ransomware-as-a-Service (RaaS) across various underground marketplaces.

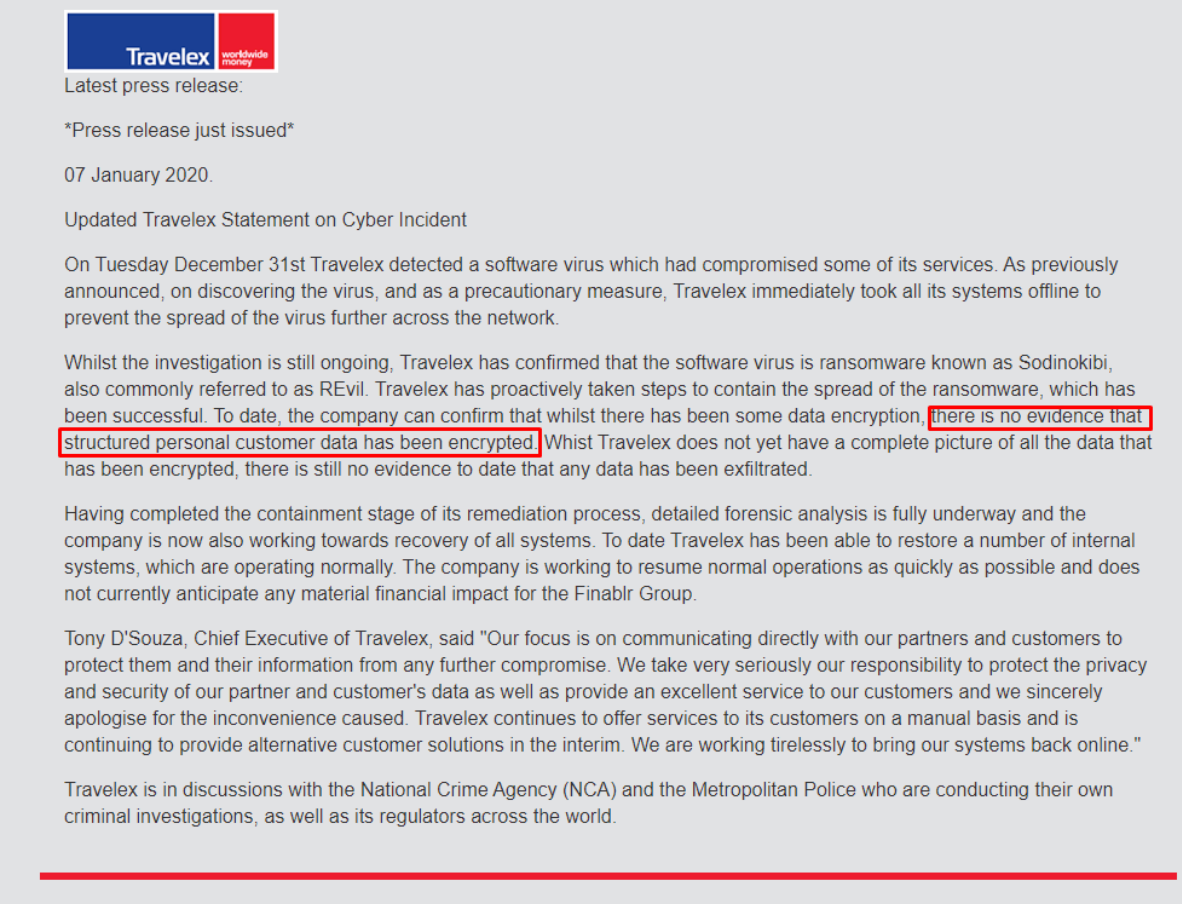
REvil is a fairly sophisticated threat that uses various anti-analysis tricks and execution mechanisms to encrypt the victim's machine and common files, forcing the victim to pay a sizable ransom to decrypt their data.

In recent months, CyberInt Research has observed an increase of what is known as a "big game" ransom where cybercriminal groups are extorting organizations to pay huge ransoms to release their encrypted data. "Big game" ransom attacks are becoming more frequent and represent a shift from common ransomware attacks that previously targeted small organizations or end users with relatively small ransom demands, typically averaging hundreds of dollars, to targeting large enterprises requesting larger amounts of ransom demands, potentially in the tens and hundreds of thousands of dollars or even millions.

Publicly available information suggests that the REvil ransomware has been delivered by targeting unpatched Pulse Secure VPN services using CVE-2019-11510 and CVE-2019-11539, allowing the threat actor to gain access to a

victim network and deploy the threat. In this incident, it is also claimed that the threat actors hold 5GB of Travelex' sensitive customer data, in addition to the encrypted information, and have demanded a ransom of US$6m.

This threat actor statement contrasts with the official Travelex public announcement that states that no customer data has been leaked. The potential exposure of customer information might cause Travelex to face serious regulatory consequences, such as GDPR fines, on top of either paying the ransom demand to release the encrypted data or suffering the costs of remediation along with indirect collateral damage of brand reputation loss, potential customer churn, legal actions, etc.



Travelex worldwide money

Latest press release:

Press release just issued

07 January 2020.

Updated Travelex Statement on Cyber Incident

On Tuesday December 31st Travelex detected a software virus which had compromised some of its services. As previously announced, on discovering the virus, and as a precautionary measure, Travelex immediately took all its systems offline to prevent the spread of the virus further across the network.

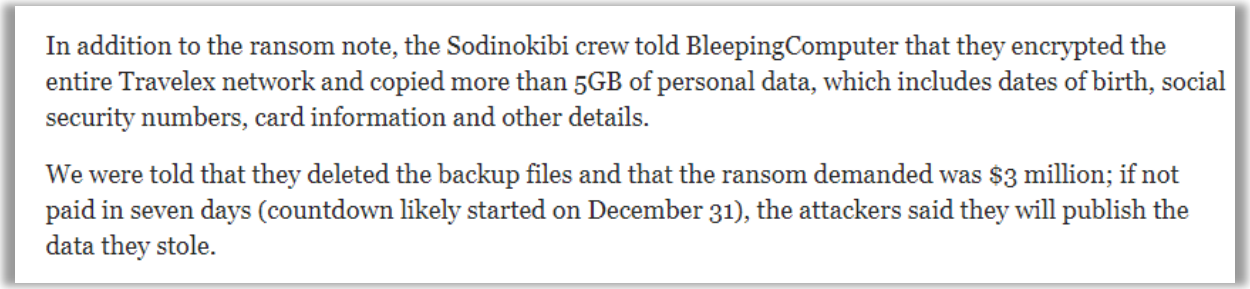
Whilst the investigation is still ongoing, Travelex has confirmed that the software virus is ransomware known as Sodinokibi, also commonly referred to as REvil. Travelex has proactively taken steps to contain the spread of the ransomware, which has been successful. To date, the company can confirm that whilst there has been some data encryption, there is no evidence that structured personal customer data has been encrypted. Whist Travelex does not yet have a complete picture of all the data that has been encrypted, there is still no evidence to date that any data has been exfiltrated.

Having completed the containment stage of its remediation process, detailed forensic analysis is fully underway and the company is now also working towards recovery of all systems. To date Travelex has been able to restore a number of internal systems, which are operating normally. The company is working to resume normal operations as quickly as possible and does not currently anticipate any material financial impact for the Finablr Group.

Tony D'Souza, Chief Executive of Travelex, said "Our focus is on communicating directly with our partners and customers to protect them and their information from any further compromise. We take very seriously our responsibility to protect the privacy and security of our partner and customer's data as well as provide an excellent service to our customers and we sincerely apologise for the inconvenience caused. Travelex continues to offer services to its customers on a manual basis and is continuing to provide alternative customer solutions in the interim. We are working tirelessly to bring our systems back online."

Travelex is in discussions with the National Crime Agency (NCA) and the Metropolitan Police who are conducting their own criminal investigations, as well as its regulators across the world.

Figure 4 - Travelex announcement about the incident



In addition to the ransom note, the Sodinokibi crew told BleepingComputer that they encrypted the entire Travelex network and copied more than 5GB of personal data, which includes dates of birth, social security numbers, card information and other details.

We were told that they deleted the backup files and that the ransom demanded was $3 million; if not paid in seven days (countdown likely started on December 31), the attackers said they will publish the data they stole.

Figure 5 - Public reporting indicating the threat actor has access to the entire Travelex network

Pulse Secure VPN as a Potential Attack Vector

Evidence of the actual attack vector is still unavailable, but our research as well as publicly available information might suggest several vectors that could have been used by the threat actor to gain access to Travelex' network and deploy the REvil ransomware.

On 2 October 2019 the UK Government's National Cyber Security Centre (NCSC) published[8] a warning regarding Advanced Persistent Threat (APT) actors exploiting vulnerabilities in various VPN products including:

Pulse Secure VPN

- CVE-2019-11510: pre-auth arbitrary file reading;
- CVE-2019-11539: post-auth command injection;

Fortinet

- CVE-2018-13379: Pre-auth arbitrary file reading;
- CVE-2018-13382: Allows an unauthenticated attacker to change the password of an SSL VPN web portal user;
- CVE-2018-13383: Post-auth heap overflow. This allows an attacker to gain a shell running on the router;

Palo Alto

- CVE-2019-1579: Palo Alto Networks GlobalProtect Portal;

Publicly available information *verified by CyberInt Research* indicates that Travelex was using a vulnerable version of the Secure Pulse VPN gateway for remote access.

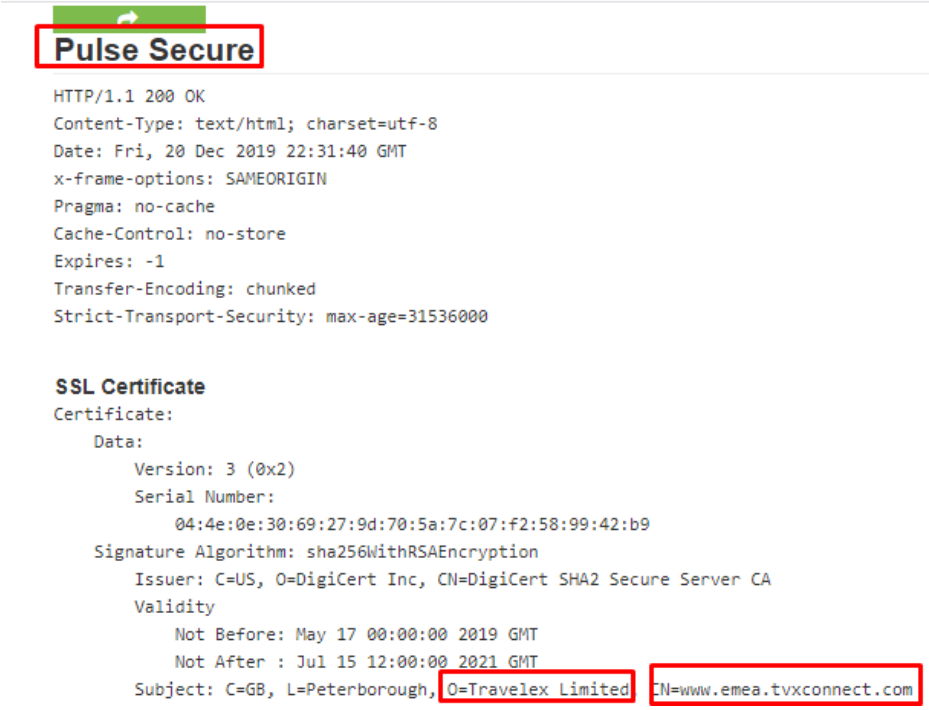


Figure 6 - Travelex vulnerable Pulse Secure VPN SSL Certificate

[8] https://www.ncsc.gov.uk/news/alert-vpn-vulnerabilities

Information on both Pulse Secure VPN vulnerabilities were made publicly available on 24 April 2019, subsequently opensource information suggests that Travelex was notified by Badpackets[9] of vulnerabilities in their configuration on 13 September 2019 and they failed to react or patch the vulnerable software versions.

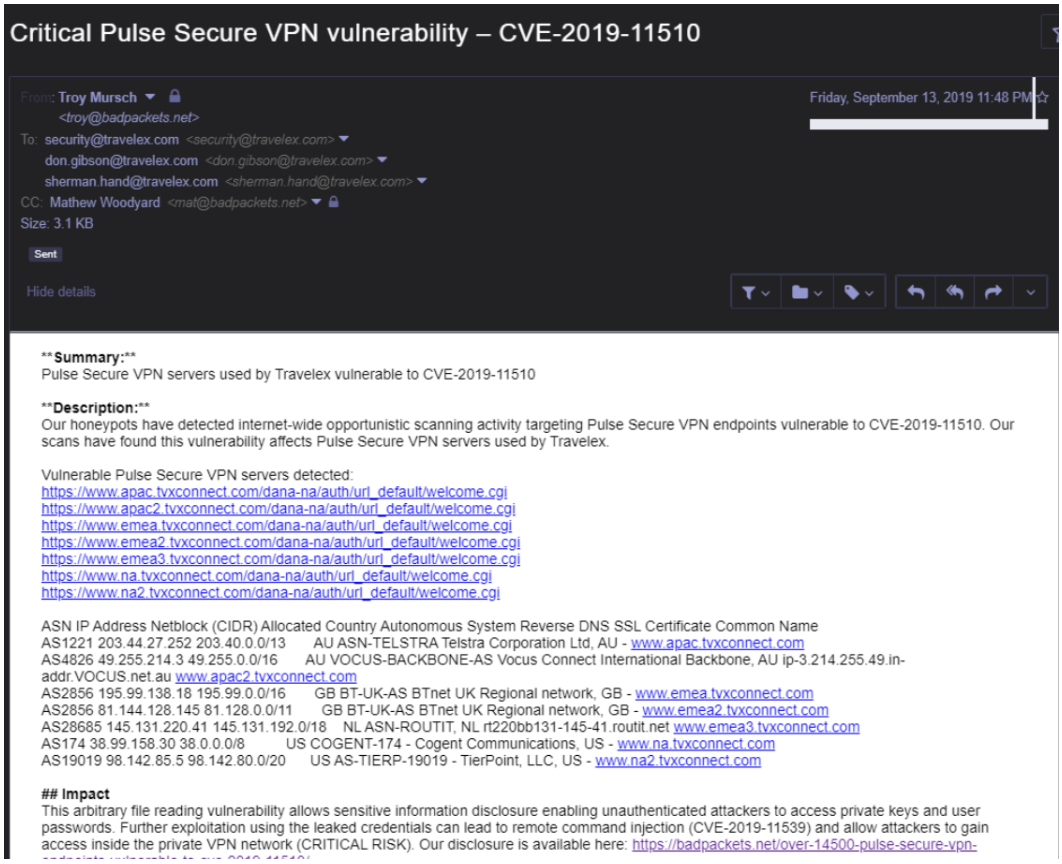


Figure 7 - Badpackets notification to Travelex about the vulnerability

On 4 January 2020, security researcher Kevin Beaumont published an article[10] suggesting that threat actors were exploiting this Secure Pulse VPN vulnerability to deploy the REvil ransomware; publicly available exploits were available from the "Packet Storm Security" website since 21 August 2019[11].

Given this, the evidence suggests that Travelex may have fallen victim to a REvil campaign that leveraged the Secure Pulse VPN vulnerability to deploy the ransomware across their network.

[9] https://badpackets.net/
[10] https://doublepulsar.com/big-game-ransomware-being-delivered-to-organisations-via-pulse-secure-vpn-bd01b791aad9
[11] https://packetstormsecurity.com/files/154176/Pulse-Secure-SSL-VPN-8.1R15.1-8.2-8.3-9.0-Arbitrary-File-Disclosure.html

Exposed RDP Server as a Potential Attack Vector

Additional opensource information may also indicate an additional attack vector in the form of a publicly accessible Windows Server, hosted on Amazon Web Services (AWS) with the Remote Desktop Protocol (RDP) enabled and Network Layer Authentication (NLA) disabled. This configuration negates the need for users to authenticate themselves *before* a session is established with the server.

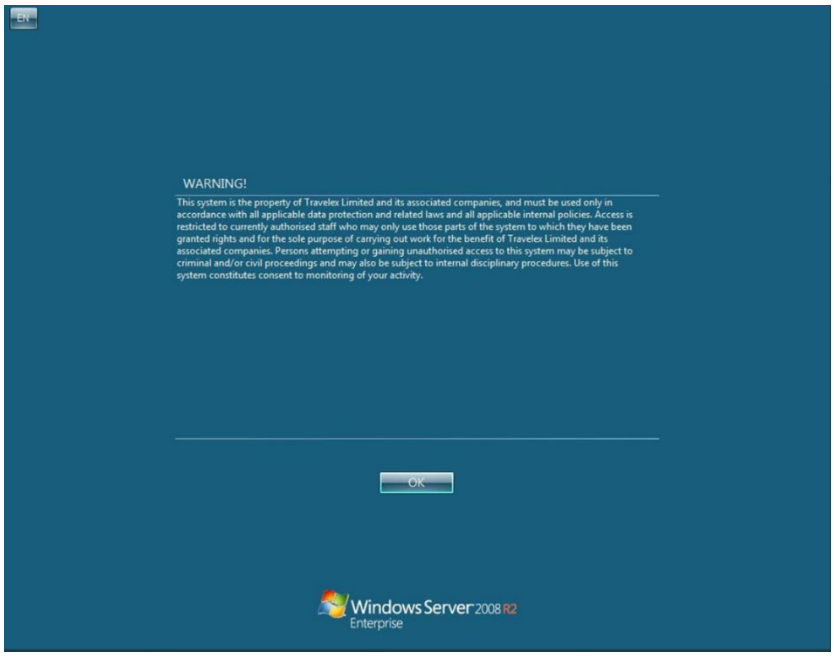


Figure 8 - Exposed Travelex RDP

Finally, a third potential attack vector has been suggested with the threat actors behind REvil compromising Managed Service Providers (MSP) to gain access to remote management tools, uninstalling endpoint protection software and deploying their REvil ransomware. CyberInt Research have seen evidence of an earlier campaign in May 2018 targeting Italian financial organizations using this attack vector to distribute the REvil ransomware[12].

Whatever the attack vector was, the evidence suggests that Travelex' IT practices may have contributed to their exposure to attacks such as the one they are currently dealing with. As a UK-based financial organization Travelex are subject to the Financial Conduct Authority's (FCA)[13] regulatory requirements. The FCA regulates some 59,000 financial service companies in the UK and on 17 August 2018 Travelex released information about their new FCA Regulated B2C payment platform hosted on AWS[14]. Given that the Travelex RDP server identified as exposed and hosted on AWS may suggest that the organization may also fall foul of FCA regulatory requirements.

[12] https://twitter.com/VirITeXplorer/status/1133302287491842049
[13] https://www.fca.org.uk/about/the-fca
[14] https://hostingjournalist.com/video/travelex-a-secure-fca-regulated-b2c-payment-platform-on-ecs/

REvil Technical Analysis

REvil ransomware was first observed on 17 April 2019 and was considered a new strain of ransomware that was provided as Ransomware-as-a-Service (RaaS). Although not as popular as some of the other ransomware malware families like Ryuk or Lockergoka, REvil ransomware is considered to be somewhat sophisticated with multiple anti-analysis mechanisms.

Common delivery methods have included exploit kits, exposed RDP servers, and backdoor software installers in addition to exploiting vulnerable hosts to download and install the ransomware payload.
Like most malware today, REvil is packed by either commercial packers like VMProtect or custom packers provided by the authors. The goal of packing the malware is to avoid detection and inhibit analysis efforts.

Once unpacked, and based on malware analysis conducted by SecureWorks[15], REvil can perform the following tasks:

- Exploit CVE-2018-8453 to elevate privileges
- Terminate blacklisted processes prior to encryption to eliminate resource conflicts
- Wipe the contents of blacklisted folders
- Encrypt non-whitelisted files and folders on local storage devices and network shares
- Exfiltrate basic host information

[15] https://www.secureworks.com/research/revil-sodinokibi-ransomware

Malware Configuration

The REvil malware contains a resource named '.m69' in the unpacked binary. The resource contains encoded data, the first 32 bytes of which is a key used to decode the remaining data, an encoded JSON configuration resource.

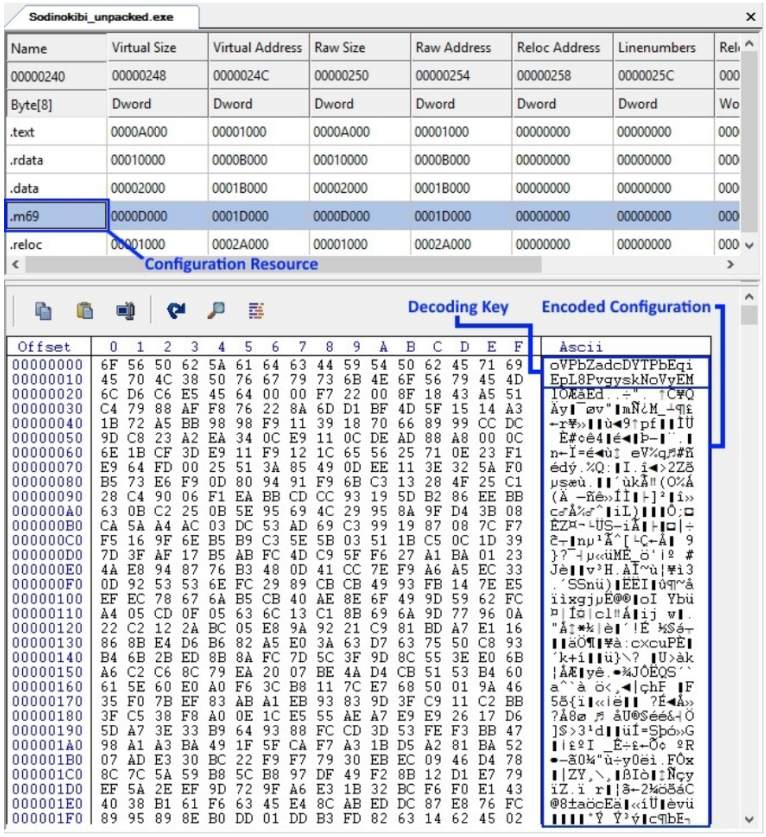


Figure 9 - REvil encrypted Resource

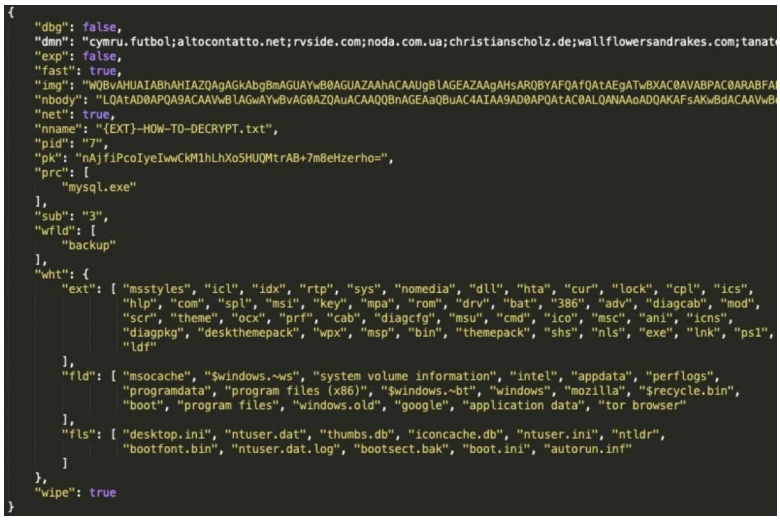


Figure 10 - JSON formatted REvil config file

Once decoded, this JSON-formatted text contains configurable REvil options including numerous key-value elements used during execution, such as the following whitelist exclusions, files and directories that won't encrypted, presumably to ensure the system remains stable:

- "ext": Whitelisted file extensions including scripts and executables;
- "fld": Whitelisted directories including core application and operating system locations;
- "fls": Whitelists filenames such as boot configuration files;

Another notable setting is the 'wipe' key instructing the ransomware to wipe or delete original files after encryption.

The table below shows further detail of the observed configuration settings:

Key	Definition
dbg	True/false value used by the malware author during development (referenced only when determining if the victim is Russian)
dmn	A 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	An 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	An 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 — Explicitly whitelisted filenames

Delivery

When REvil was first discovered, it was delivered to targets via the exploitation of Oracle WebLogic vulnerabilities. Since then, the threat actors have expanded the delivery method to include malicious spam campaigns[16], RDP attacks[17], and other attack vectors. There are reports[18] that the threat actors have also leveraged a Strategic Web Compromise (SWC) to deliver REvil by compromising the Italian version of the popular compression utility 'WinRAR', replacing the WinRAR installation executable on the website with an instance of the malware. This SWC resulted in the infection of unsuspecting WinRAR customers' systems. In other reports[19], threat actors have breached at least three Managed Service Providers (MSPs) and used their illicit 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.

Encryption Routine

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

- Obtains the volume serial number for the system drive;
- Generates a CRC32 hash of the volume serial number using the hard-coded seed value of 0x539;
- Generates a CRC32 hash of the value returned by the CPUID[20] assembly instruction using the CRC32 hash for the volume serial number as a seed value;
- 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".

REvil determines if it has already generated and stores the session encryption keys in the host's registry, by default the HKLM registry hive and falling back to HKCU in the event of failure, likely due to inadequate permissions. REvil samples use the hard-coded "Software\recfg" registry subkey. The presence of this key or the associated values could indicate a REvil infection.

[16] https://www.gdatasoftware.com/blog/2019/06/31724-strange-bits-sodinokibi-spam-cinarat-and-fake-g-data
[17] https://twitter.com/VirITeXplorer/status/1133302287491842049
[18] https://www.drcommodore.it/2019/06/20/hackerato-winrar-it-malware-al-posto-del-programma/
[19] https://www.reddit.com/r/msp/comments/c2wls0/kaseya_weaponized_to_deliver_sodinokibi_ransomware/
[20] https://c9x.me/x86/html/file_module_x86_id_45.html

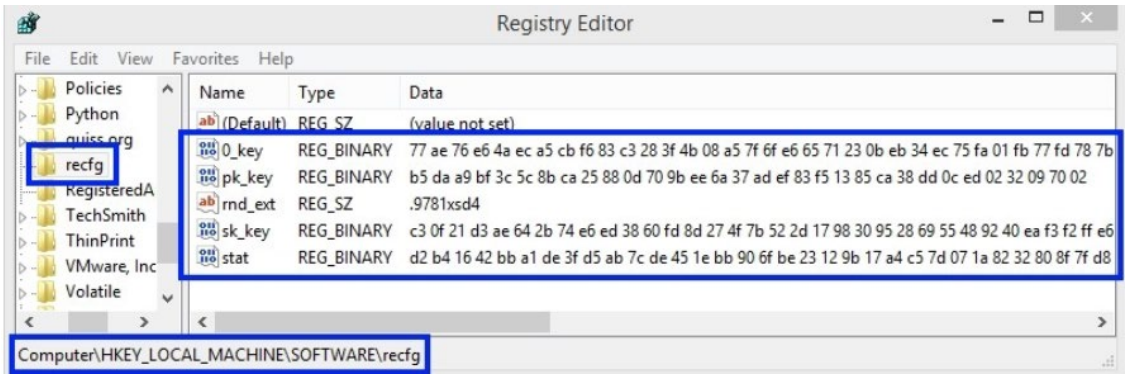


Figure 11 - REvil Registry Settings

Ransom Note

Below is a 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.

```
1  ---=== Welcome. Again. ===---
2
3  [+] Whats Happen? [+]
4
5  Your files are encrypted, and currently unavailable. You can check it: all files on
   you computer has expansion {EXT}.
6  By the way, everything is possible to recover (restore), but you need to follow our
   instructions. Otherwise, you cant return your data (NEVER).
7
8  [+] What guarantees? [+]
9
10 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.
11 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.
12 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.
13
14 [+] How to get access on website? [+]
15
16 You have two ways:
17
18 1) [Recommended] Using a TOR browser!
19   a) Download and install TOR browser from this site: https://torproject.org/
20   b) Open our website:
     http://aplebzu47wgazapdqks6vrcv6zcnjppkbxbr6wketf56nf6aq2nmyoyd.onion/{UID}
21
22 2) If TOR blocked in your country, try to use VPN! But you can use our secondary
   website. For this:
23   a) Open your any browser (Chrome, Firefox, Opera, IE, Edge)
24   b) Open our secondary website: http://decryptor.top/{UID}
25
26 Warning: secondary website can be blocked, thats why first variant much better and
   more available.
27
28 When you open our website, put the following data in the input form:
29 Key:
30
31 {KEY}
32
33
34 Extension name:
35
36 {EXT}
37
38 ---------------------------------------------------------------------------------
   -----
39
40 !!! DANGER !!!
41 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.
42 !!! !!! !!!
43 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.
44 !!! !!! !!!
```

Figure 12 - REvil Ransom note example

REvil generates the ransom note's filename using a similar process. It obtains the value stored within the "nname" key in its configuration and replaces the {EXT} variable placeholder with its corresponding value. In the analyzed sample, the nname key value "{EXT}-HOW-TO-DECRYPT.txt" led to the ransom note filename 9781xsd4-HOW-TO-DECRYPT.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!".

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.

Delete Shadow Copy

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

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".

File Encryption

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)

```
"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 13 - REvil JSON Config describing file encryption

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:

- Reads the file contents into a buffer
- Encrypts the contents of the buffer
- Writes the encrypted contents of the buffer to the original file, overwriting the original file content
- Renames the original file with the previously generated random extension

When encrypting files, REvil uses I/O completion ports (IOCPs[21]) to efficiently manage simultaneous asynchronous activities such as file reading, encrypting, and writing. This implementation results in extremely fast encryption, as IOCPs and multi-threaded processing let REvil fully leverage all of the host's available processing resources.
The malware appears to encrypt files with the Salsa20 stream cipher[22]. The encryption uses a unique key for each file based on the session public key in the Software\recfg\pk_key registry key/value. The only way to decrypt files encrypted by REvil is to obtain one of the following keys from the threat actor:

- The unencrypted session private key that was generated, encrypted, and stored within the sk_key and 0_key registry values
- The attacker's private key associated with the public key stored in the REvil configuration (The public key was used to encrypt the private session key.)

Once encrypting all applicable files in a folder, the malware drops the ransom note in that folder and moves to another folder. After REvil encrypts of all eligible files on local fixed drives, it checks if the -nolan switch was passed to the binary when launched. If so, REvil does not encrypt mapped network shares. If not, REvil encrypts all non-whitelisted files on mapped network shares.

[21] https://docs.microsoft.com/en-us/windows/desktop/fileio/i-o-completion-ports
[22] https://en.wikipedia.org/wiki/Salsa20

REvil Changes the Desktop Background

If the encryption process is successful, REvil changes the desktop background to make the victim aware of the compromise. The malware generates a bitmap image one pixel at a time using semi-random integer values for pixel color that results in a grainy blue background that is unique for each infection. The previously generated message (e.g., You are infected! Read 9781xsd4-HOW-TO-DECRYPT.txt!) is placed at the top center of the image in white text.

REvil saves the finished image to the host's %Temp% directory using a random filename consisting of lowercase letters and numbers between 3 and 13 characters in length appended with the ".bmp" extension (e.g., C:\Users\<user>\AppData\Local\Temp\cd2sxy.bmp). REvil calls the user32.dll SystemParametersInfoW function to set the image as the desktop background

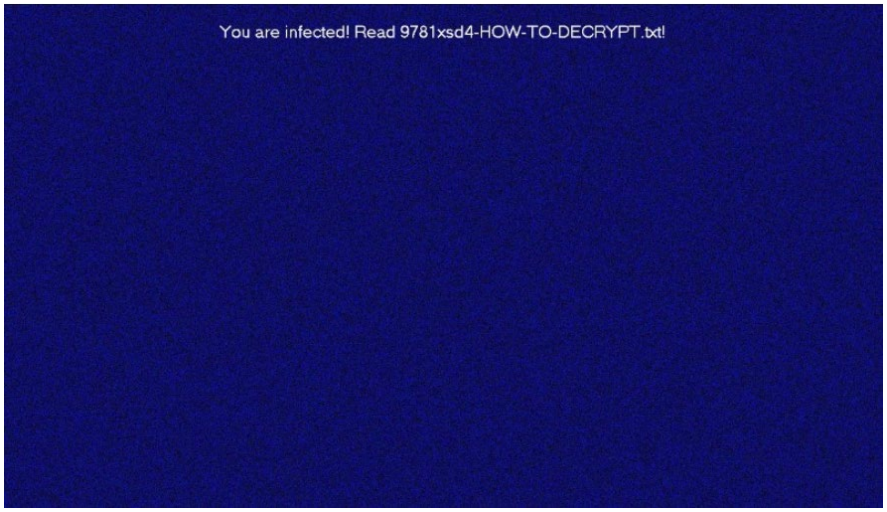


Figure 14 - Desktop background displayed on the victim machine after encryption

Command and Control Communication

REvil can send the victim's stat information to one or more C2 servers. The malware queries the net configuration key value to determine if C2 communication should take place. If the value is true, REvil iterates through all of the C2 domains specified within the dmn configuration key and builds a semi-random URL for each C2 server using the following pattern, in which the protocol is hard-coded as "https":
https://<c2_domain>/<URI_sub1>/<URI_sub2>/<random_resource_name>.<ext>

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"].

REvil sends the encrypted stat data containing the host profile and malware information to the C2 URL via the HTTP POST method. Detection of the associated network traffic is challenging because REvil uses the HTTPS protocol, which encrypts the network communication. The malware reads the subsequent C2 server response but implements no logic to act on the received data. This deficit eliminates the possibility of remote access trojan (RAT) functionality. Finally, REvil terminates execution.

Decryption Website

The ransom note instructs the victim to use a unique URL to decrypt their files. The URL leads to an attacker-controlled website that displays the form.

Victims must provide the key and extension names included in the ransom note. The key specified in the ransom note is the Base64-encoded representation of the encrypted stat data stored in the registry.

Figure 15 - REvil Decryption Site Example

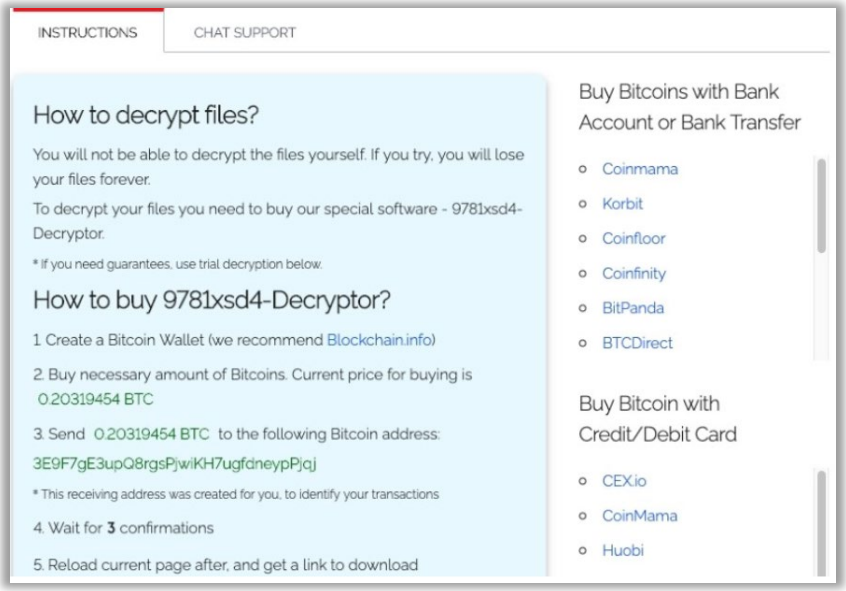


Figure 16 - REvil Ransom Payment Instructions

Possible Connection to GandCrab Ransomware

On 24 June 2019 the Authors behind the GandCrab Ransomware one of the most prolific Ransomware-as-a-Service (RaaS) announced their retirement after claiming profit of more than 2 Billion USD. This announcement was unusual in the cybercriminal underground. Though evidence suggests that the actor behind GandCrab shifted to a different malware.

And when looking at the REvil and GandCrab code a lot of similarities between the malware family is shown.

Almost Identical Decoding Function

The strongest characteristic linking the REvil and GandCrab malware families is the nearly identical functions used for decoding strings at runtime. The screen below 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 17 - Decompiled Pseudocode of the decoder function in REvil (left) and GandCrab (Right)

Circumstantial Evidence

Circumstantial evidence also suggests that the same threat actors could be responsible for REvil and GandCrab:

- The REvil file decryptor executable reportedly[23] contains a "D:\\gc6\\core\\src\\common\\debug.c" debug path that reflects the folder structure created by the malware author during development. Some researchers view "gc6" to be a reference to GandCrab v6, which could indicate that REvil is GandCrab v6;
- REvil was dropped on hosts in conjunction with GandCrab on April 17, 2019. The GandCrab threat actors announced [24]their retirement on May 31. After May 31, REvil activity increased and the delivery methods expanded and became more sophisticated;
- Both REvil and GandCrab whitelisted 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, so the REvil and GandCrab malware authors likely reside in the same region;

[23] https://twitter.com/noblebarstool/status/1146079158096687105
[24] https://www.zdnet.com/article/gandcrab-ransomware-operation-says-its-shutting-down/

Recommendations

The Travelex breach is yet another reminder of the risk and dangers organizations face by cybercriminal threat actors.

- Evidence suggests that Travelex' IT practices may have increased their exposure to threats of this nature as well as increasing the potential impact to the organization. Both reputational and financial damage can mount-up tremendously, not just the inability to operate during the time of a breach but also managing customers and partners, providing business continuity, replacing IT assets and more.
- Conducting sound IT security practices and solid detection and response practices could reduce the risk of materializing such threats.
- Additionally, consideration should be given to the impact on Travelex partners; Travelex provides foreign exchange services to some of the largest financial organizations in the world that are now also at risk from the breach, be that reputational damage and loss of customer confidence or potential threats through the compromise of infrastructure and connectivity links between the organizations.

Contact Information

www.cyberint.com | sales@cyberint.com | blog.cyberint.com

USA
Tel: +1-646-568-7813
W 29th Street, Suite 06A-104, New York, NY, 10001 214

Israel
Tel: +972-3-7286777 17
Ha-Mefalsim St, 4951447, Kiriat Arie, Petah Tikva 17

United Kingdom
Tel: +44-203-514-1515
Grays Inn Rd Fox Court, Suite 2068, Holborn, London, WC1X 8HN 14

Singapore
Tel:+65-3163-5760
Cecil St. #10-01 MYP PLAZA 069536 135

LATAM
Tel: +507-395-1553
Edificio Corporativo Cable Onda/TeleCarrier, Panama City

Cyberint.