DefendAgainst: Ransomware ‘STOP’/DJVU

By Vishal Thakur

Published: 2021-12-23 · Archived: 2026-04-05 20:28:17 UTC

aka DJVU

Originally published here.

In recent weeks, we have observed a spike in infections involving the STOP ransomware variant. STOP is also known as DJVU by other vendors in the industry. In this article, we’ve looked at the latest version circulating in the wild. We will look at some of the main characteristics of this malware variant, along with detections that can be used to prevent infection and IOCs that we were able to extract during analysis.

Introduction

The STOP ransomware has been around for some time, dating back to 2019. The latest version has been found to be distributed broadly in the past few weeks. Like the ones in the past, this variant is a portable executable that uses a public key to encrypt data on the victim’s machine and drops a ransom note in folder directories as it goes through the entire file system encrypting files using the Salsa20 encryption algorithm. The threat actors behind STOP have gone for a flat rate of USD 980 to provide the decryption keys to victims and have also offered a ‘discounted’ rate of USD 490 if the victims contact them within 72 hours of the attack occurring. This tactic is consistent with what has been observed in the past for this ransomware group.

Based on the tactics and techniques used by the malware, it indicates that the threat actors behind it are likely from the Russian region. The malware avoids encryption explicitly on systems geo-located in or near Russia.

Press enter or click to view image in full size

Quick Snapshot:
Class: DOS
Type: PE32
Machine: X86-64
OS: Windows
Entry Point: 0009D410
MD5: a2f33095ef25b4d5b061eb53a7fe6548

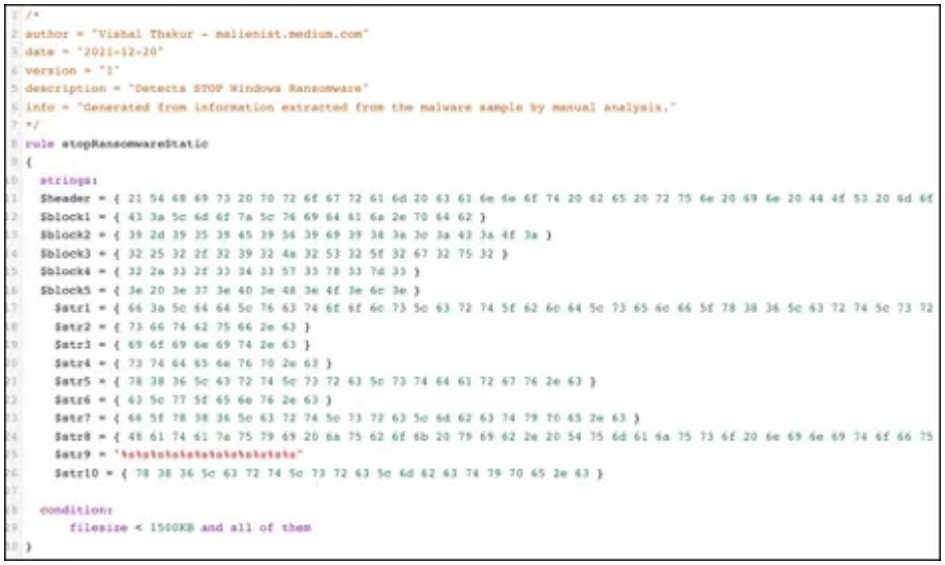
Figure 1: Quick Snapshot of STOP Ransomware

Mitigation

This section provides information that can be used to prevent infection by the STOP ransomware. We have included detections, IOC list and YARA Rules that can be used to defend against this threat.

YARA Rule

This YARA Rule can be used to detect STOP Ransomware. Download the entire ruleset here.



```
/*
author = "Vishal Thakur - malienist.medium.com"
date = "2021-12-20"
version = "1"
description = "Detecta STOP Windows Ransomware"
info = "Generated from information extracted from the malware sample by manual analysis."
*/
rule stopRansomwareStatic
{
  strings:
  $header = { 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f
  $block1 = { 43 3a 5c 6d 6f 7a 5c 76 69 64 61 6a 2e 70 64 62 }
  $block2 = { 39 2d 39 35 39 45 39 56 39 69 39 34 3a 3o 3a 43 3a 4f 3a }
  $block3 = { 32 25 32 2f 32 39 32 4a 32 53 32 5f 32 67 32 75 32 }
  $block4 = { 32 2a 33 2f 33 34 33 57 33 78 33 7d 33 }
  $block5 = { 3e 20 3e 37 3e 40 3e 48 3e 4f 3e 6c 3e }
    $str1 = { 66 3a 5c 64 64 5c 76 63 74 6f 6f 6c 73 5c 63 72 74 5f 62 6o 64 5c 73 65 6c 66 5f 78 38 36 5c 63 72 74 5c 73 72
    $str2 = { 73 66 74 62 75 66 2e 63 }
    $str3 = { 69 6f 69 6e 69 74 2e 63 }
    $str4 = { 73 74 64 65 6e 76 70 2e 63 }
    $str5 = { 78 38 36 5c 63 72 74 5c 73 72 63 5c 73 74 64 61 72 67 76 2e 63 }
    $str6 = { 63 5c 77 5f 65 6e 76 2e 63 }
    $str7 = { 66 5f 78 38 36 5c 63 72 74 5c 73 72 63 5c 6d 62 63 74 79 70 65 2e 63 }
    $str8 = { 48 61 74 61 7a 75 79 69 20 6a 75 62 6f 6b 20 79 69 62 2e 20 54 75 6d 61 6a 75 73 6f 20 6e 69 6e 69 74 6f 66 75
    $str9 = "hahahahahahahahahaha"
    $str10 = { 78 38 36 5c 63 72 74 5c 73 72 63 5c 6d 62 63 74 79 70 65 2e 63 }

  condition:
      filesize < 1500KB and all of them
}
```

Figure 2: YARA Ruleset for STOP Ransomware

Detections

The following figure has the information that can be used to create detections for this malware. Download the entire list here.

Get Vishal Thakur’s stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

The following strings are from the unpacked malware, and these can be found in memory during and after the malware has been fully executed. This information can be used to create detections for EDR tools that can access and read memory and take actions based on detection rules applied.

Press enter or click to view image in full size

Figure 3: Detections

IOC List

Download the entire list here.

Press enter or click to view image in full size

Figure 4: IOC list

Execution

Once the STOP ransomware executes, it attempts to make a few network connections over the Internet for various purposes, such as; geo-checking, key retrieval, and further infection by downloading different malware. First, let's look at the start of the execution of this malware.

Figure 5: Malware Entry-point

Upon execution, the malware copies itself to the ‘C:\Users\[username]\AppData\Local\[GUID]’ directory on disk and tries to execute with escalated privileges, as shown in the figures below.

Figure 6: Malware copies itself to a different location

Press enter or click to view image in full size

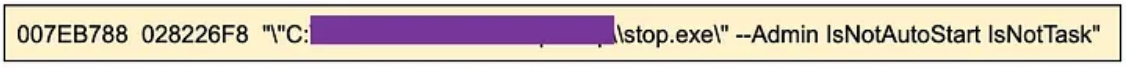


Figure 7: Spawning new process with elevated privileges

The malware then attempts to connect over the Internet to “https://api.2ip.ua/geo.json” to verify the victim’s geolocation. This link leads to a Russian site (screenshot below) that provides geolocation services based on public Internet IP addresses which the malware uses to ascertain the location of its victims. The malware has a hard-coded country codes list that is checked before it continues executing on the victim’s system and will avoid encrypting victims within these countries.

Press enter or click to view image in full size

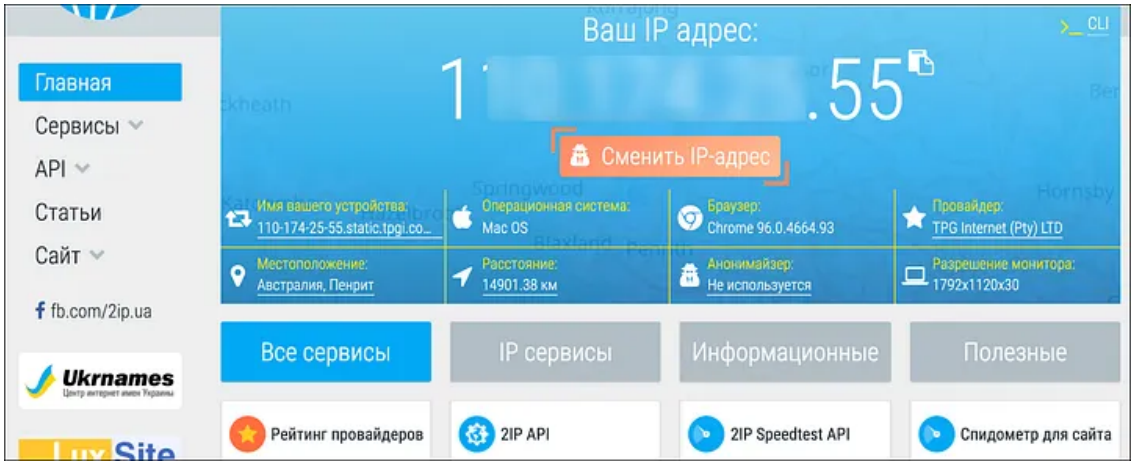


Figure 8: Geo-location service used by the malware

The site also offers an API-based service that the malware uses to determine the geolocation of the victim machines.

Press enter or click to view image in full size

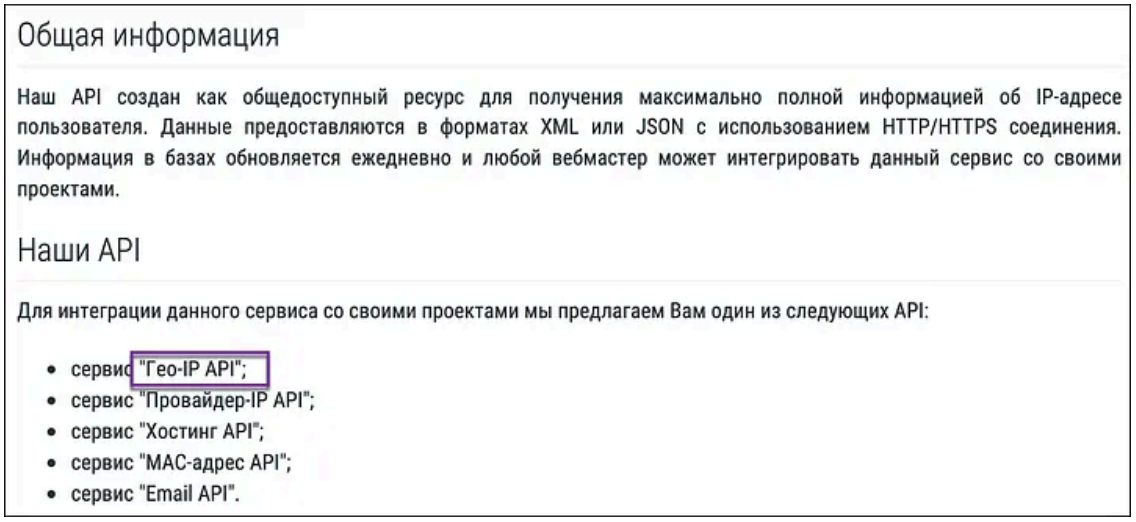


Figure 9: The specific API-based service the malware uses

The country code list can be seen in the figure below, showing the codes in memory during execution.

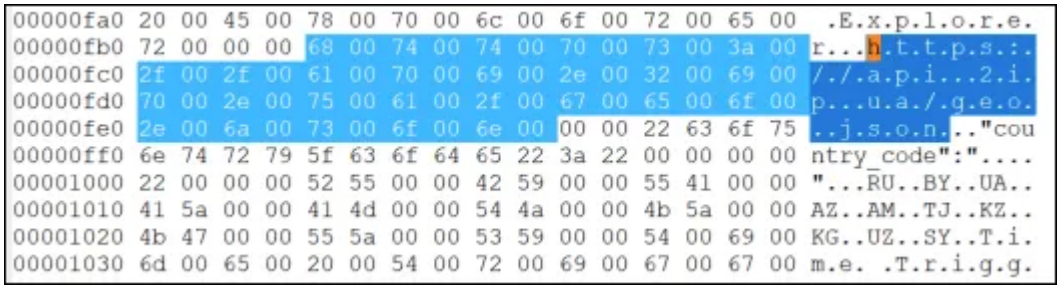


Figure 10: Country codes of locations this malware avoids

Next, the malware tries to connect to a command and control URI to get the public key for encryption. As we can see in the figure below, it sends a request to this URI with a PID created for the victim.

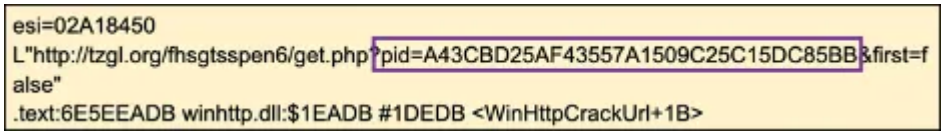


Figure 11: URI loaded into the stack for processing

Press enter or click to view image in full size

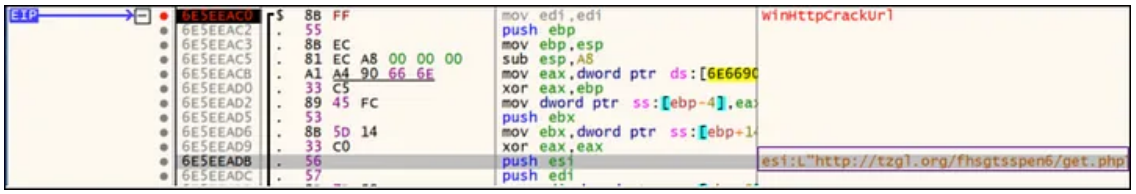


Figure 12: Connection to the C2 for public key

Once the request is successful, the malware uses the public key with the ID to encrypt the victim's data.

Press enter or click to view image in full size

Figure 13: Public Key for encryption served by the C2

The malware uses a standard encryption sequence, calling in the functions required to encrypt data from start to finish. The complete sequence can be seen in the figure below, in the order of called functions.

Press enter or click to view image in full size

Figure 14: Encryption Sequence of function calls

CSP — Cryptography Service Provider

The malware queries the Registry on the victim machine to set the CSP and CSP type. Note that type shown in the figure below is 'Type 001' which is the 'RSA Full' provider.

Press enter or click to view image in full size

```
007EE8D8  029EBD90  "SOFTWARE\\Microsoft\\Cryptography\\Defaults\\Provider Types\\Type 001"
```

Figure 15: Malware query to Registry for the Type of CSP

The malware uses the Registry to set the provider type and subsequently the actual provider, which in this case happens to be RSA Full.

RegOpenKey

Press enter or click to view image in full size

```
74BC9490    8B FF           mov edi,edi
74BC9492    55              push ebp
74BC9493    8B EC           mov ebp,esp
74BC9495    51              push ecx
74BC9496    6A 00           push 0
74BC9498    FF 75 18        push dword ptr ss:[ebp+18]
74BC949B    FF 75 14        push dword ptr ss:[ebp+14]
74BC949E    FF 75 10        push dword ptr ss:[ebp+10]
74BC94A1    FF 75 0C        push dword ptr ss:[ebp+C]
74BC94A4    FF 75 08        push dword ptr ss:[ebp+8]
74BC94A7    E8 14 00 00 00  call <kernelbase.RegOpenKeyExInternalA>
74BC94AC    59              pop ecx
74BC94AD    5D              pop ebp
74BC94AE    C2 14 00        ret 14
```

Figure 16: Registry functions used to determine the CSP

RegOpenKeyExA

Next, the malware queries the Registry to determine the actual CSP as can be seen in the figure below.

Press enter or click to view image in full size

```
EBX   029D0B98   "SOFTWARE\\Microsoft\\Cryptography\\Defaults\\Provider\\Microsoft Strong Cryptographic Provider"
```

Figure 17: The absolute Registry path passing through the Registers

Name	Type	Data
(Default)	REG_SZ	(value not set)
Name	REG_SZ	Microsoft Strong Cryptographic Provider
TypeName	REG_SZ	RSA Full (Signature and Key Exchange)

Figure 18: The CSP highlighted in the Registry

Name	Type	Data
(Default)	REG_SZ	(value not set)
Image Path	REG_SZ	%SystemRoot%\system32\rsaenh.dll
SigInFile	REG_DWORD	0x00000000 (0)
Type	REG_DWORD	0x00000001 (1)

Figure 19: DLL image path to be called for the CSP

The malware uses the public key obtained from the command and control server to start the process of encryption on the victim's system.

```
7429FB50    8B FF           mov edi,edi
7429FB52    55              push ebp
7429FB53    8B EC           mov ebp,esp
7429FB55    5D              pop ebp
7429FB56  ^ FF 25 44 10 2F 74  jmp dword ptr ds:[<&CryptCreateHash> ]
7429FB5C    CC              int3
7429FB5D    CC              int3
7429FB5E    CC              int3
7429FB5F    CC              int3
7429FB60    8B FF           mov edi,edi
7429FB62    55              push ebp
7429FB63    8B EC           mov ebp,esp
7429FB65    83 EC 34        sub esp,34
7429FB68    A1 30 74 2E 74  mov eax,dword ptr ds:[742E7430]
7429FB6D    33 C5           xor eax,ebp
7429FB6F    89 45 FC        mov dword ptr ss:[ebp-4],eax
7429FB72    8B 4D 08        mov ecx,dword ptr ss:[ebp+8]
7429FB75    56              push esi
7429FB76    33 F6           xor esi,esi
7429FB78    89 75 CC        mov dword ptr ss:[ebp-34],esi
7429FB7B    85 C9           test ecx,ecx
7429FB7D  v 0F 85 6D 05 01 00  jne advapi32.742B00F0
```

Figure 20: Second function to be called in the Encryption Sequence

Press enter or click to view image in full size

```
04FDF9FC  0040EB07  return to stop.0040EB07 from ???
04FDFA00  04FDFA48
04FDFA04  00000000
04FDFA08  00000000
04FDFA0C  00000001
04FDFA10  F0000000
04FDFA14  00540000  stop.00540000
04FDFA18  000005E4
04FDFA1C  00162588  "-----BEGIN PUBLIC KEY-----\\\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA8
04FDFA20  000001D9
04FDFA24  000001D9
04FDFA28  04FDFA48
04FDFA2C  00420CAB  return to stop.00420CAB from ???
```

Figure 21: Public key loaded

Once the entire encryption sequence is completed for a directory, the final step is to write a ransom note to the directory with instructions on how to pay the ransom.

```
753DE250  ^ FF 25 C0 0E 3E 75  jmp dword ptr ds:[<&WriteFile> ]
753DE256    CC              int3
753DE257    CC              int3
753DE258    CC              int3
753DE259    CC              int3
753DE25A    CC              int3
753DE25B    CC              int3
753DE25C    CC              int3
753DE25D    CC              int3
753DE25E    CC              int3
753DE25F    CC              int3
753DE260  ^ FF 25 C4 0E 3E 75  jmp dword ptr ds:[<&WriteFileEx> ]
753DE266    CC              int3
753DE267    CC              int3
```

Figure 22: Ransom note 'write' initiated

The figure below shows the ransom note as strings being passed onto the stack before it is written to the disk.

Press enter or click to view image in full size

Figure 23: Ransom note loaded into the Stack

Finally, the ransom note is written as a ‘txt’ file to the disk. This process is repeated for all directories in which the malware encrypts data. The figure below shows the newly created ransom note “_readme.txt”.

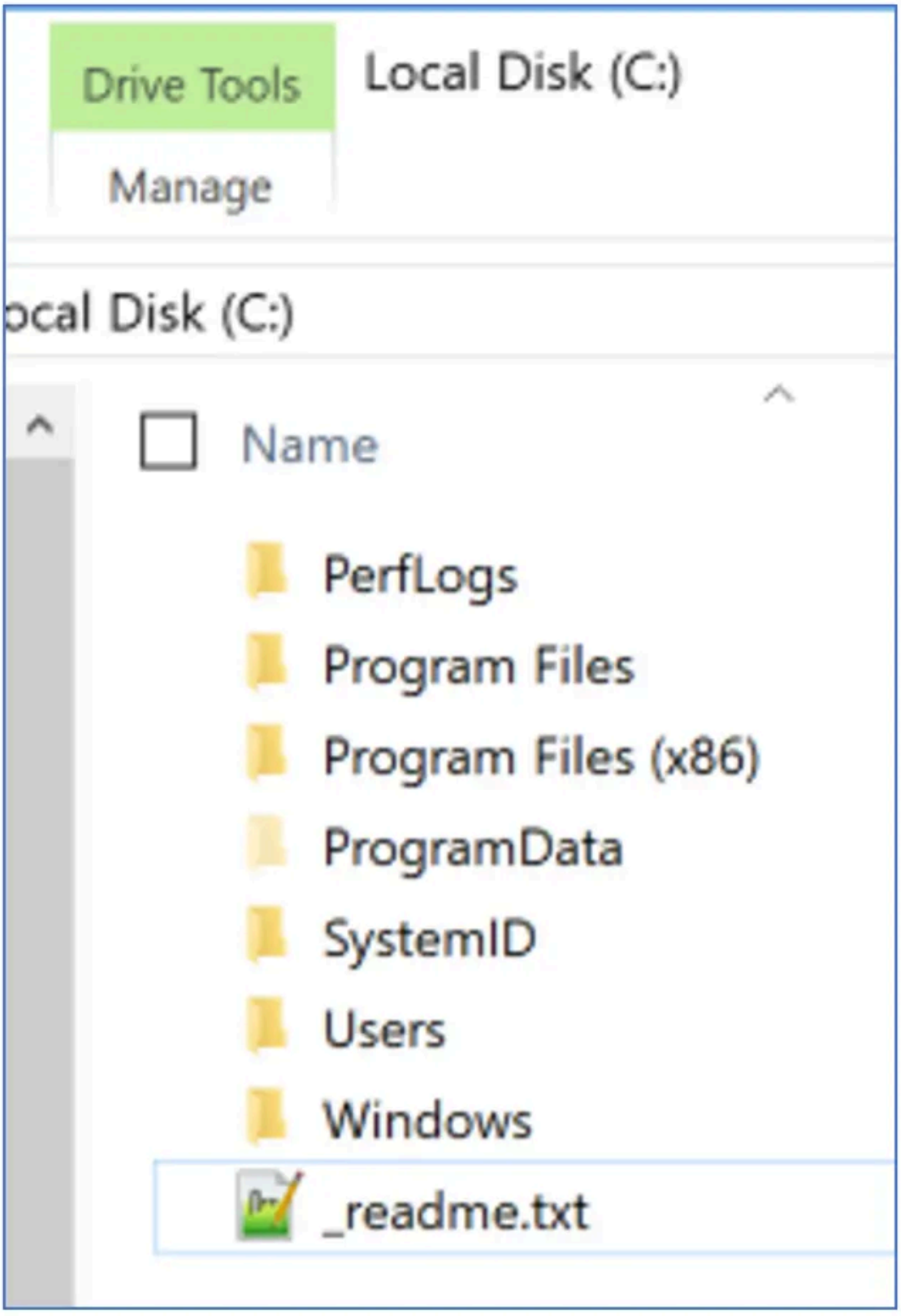


Figure 24: Ransom note file written to the current directory

The ransom note has the instructions on how the victims can pay to get the decryption key and provides a unique ID that the victim needs to use to get the decryption key for their machine. There is also a link to a demo video showing how the decryption tool works. The note also provides a couple of email addresses for the victims to contact the ransomware group if needed.

Press enter or click to view image in full size

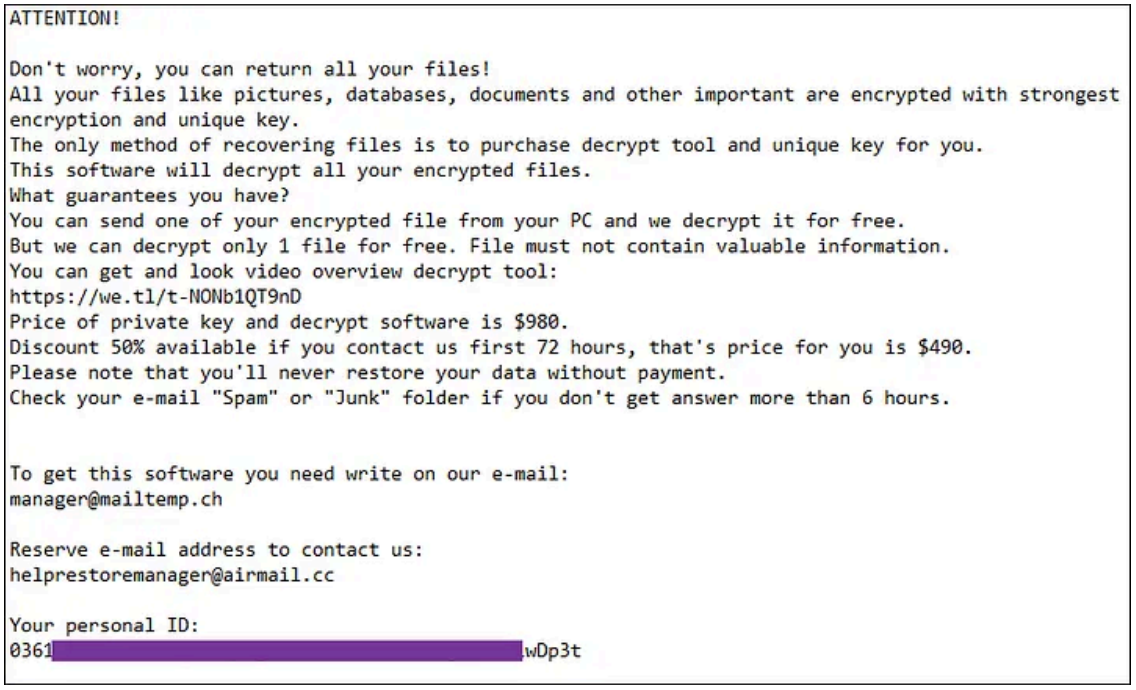


Figure 25: Ransom note with instructions on next steps

This version of the STOP ransomware variant encrypts the file and replaces the file-extensions to ".shgv", as seen in the figure below.

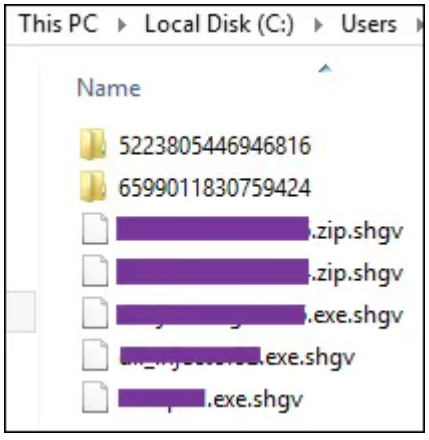


Figure 26: Files successfully encrypted

Downloader Module

Aside from performing common ransomware activities, this malware also tries to download and execute other malware:

Press enter or click to view image in full size

Figure 27: Downloaded malware — Vidar Stealer

This downloaded PE is a variant of the Vidar malware family.
Vidar Stealer is malware designed to steal information, mainly distributed as spam mail or cracked versions of commercial software and keygen programs. When installed, data such as infected device information, account, and history recorded in the browser is collected and sent to a command and control server.

The group behind the development or distribution (or both) of STOP ransomware may be working with the group responsible for developing the Vidar malware.

Conclusion

STOP ransomware has been around for quite some time now. Early occurrences of infections by this ransomware can be traced back to 2019.

Compared to some other ransomware families, the execution standard is low and it's clear that this ransomware model is affiliation-leaning (working with other malware groups). We were able to link this malware to a different malware, the Vidar Stealer, which has been the case for quite some time.

The encryption is straightforward, with the threat actors not bothering to create their encryption algorithm or deploying any additional modules other than a downloader for a separate malware. The malware uses the Salsa20 algorithm for encryption. It is capable of both online and offline encryption.

This ransomware avoids infecting victims in and near Russia.

The ransomware seems to be targeted towards individuals or small businesses at best, as the asking price for the decryption key is not that high. They even offer an 'early bird' discount to top it all off.

References

Deep Analysis of Vidar Stealer — Sojun Ryu
YAYA ruleset for STOP Ransomware — Vishal Thakur
Detections list for STOP Ransomware — Vishal Thakur
IOC list of STOP Ransomware — Vishal Thakur

Intezer Analysis
