Agenda Ransomware Uses Rust to Target More Vital Industries

trendmicro.com/en_us/research/22/l/agenda-ransomware-uses-rust-to-target-more-vital-industries.html

December 16, 2022

Ransomware

This year, various ransomware-as-a-service groups have developed versions of their ransomware in Rust, including Agenda. Agenda's Rust variant has targeted vital industries like its Go counterpart. In this blog, we will discuss how the Rust variant works.

By: Nathaniel Morales, Ivan Nicole Chavez, Nathaniel Gregory Ragasa, Don Ovid Ladores, Jeffrey Francis Bonaobra, Monte de Jesus December 16, 2022 Read time: (words)

This year, ransomware-as-a-service (RaaS) groups like BlackCat, Hive, and RansomExx have developed versions of their ransomware in Rust, a cross-platform language that makes it easier to tailor malware to different operating systems like Windows and Linux. In this blog entry, we shed light on Agenda (also known as Qilin), another ransomware group that has started using this language.

According to our observations in the past month, the Agenda ransomware's activities included posting numerous companies on its leak site. The threat actors not only claimed that they were able to breach the servers of these companies but also threatened to publish their files. The companies that the ransomware group posts on its leak site are located in different countries and belong mostly in the manufacturing and IT industries, with a combined revenue that surpasses US$550 million.

Recently, we found a sample of the Agenda ransomware written in Rust language and detected as Ransom.Win32.AGENDA.THIAFBB. Notably, the same ransomware, originally written in Go language, was known for targeting healthcare and education sectors in countries like Thailand and Indonesia. The actors customized previous ransomware binaries for the intended victim through the use of confidential information such as leaked accounts and unique company IDs as the appended file extension. The Rust variant has also been seen using intermittent encryption, one of the emerging tactics that threat actors use today for faster encryption and detection evasion.

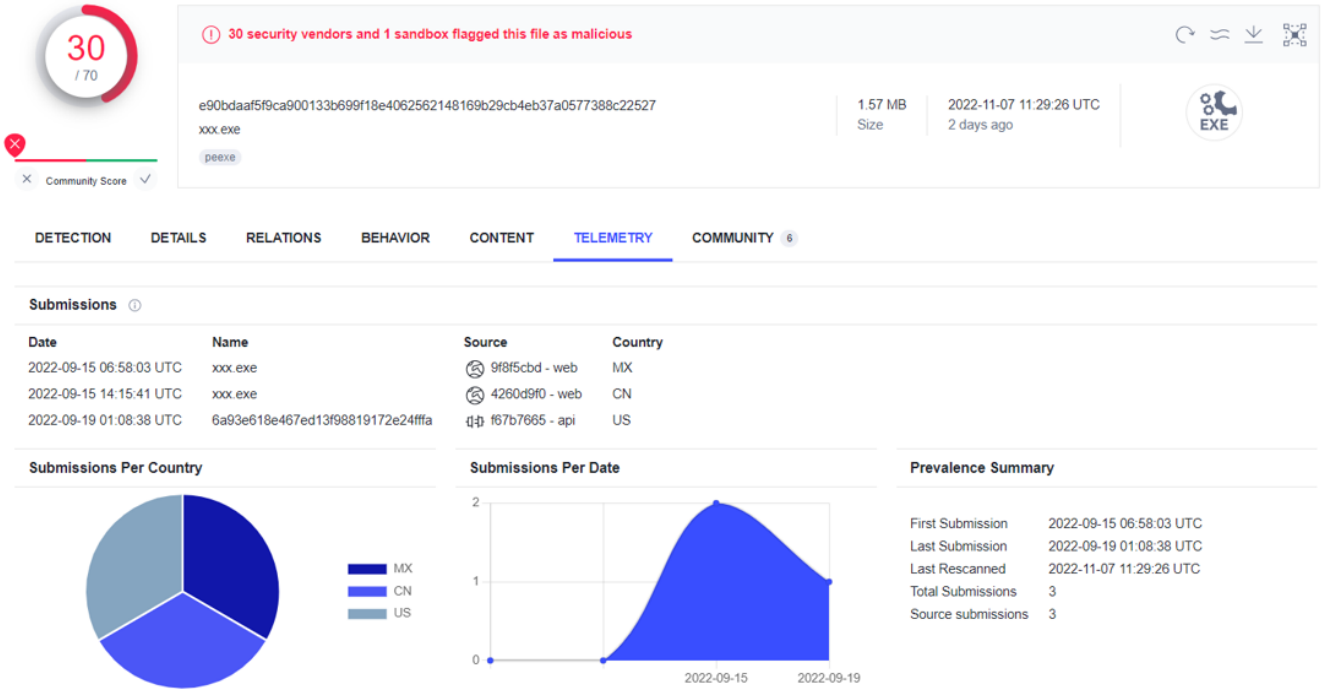

Figure 1. Submission details of the binary in VirusTotal, including the submission date and region it was uploaded.

File pos	Mem pos	ID	Text
A 00166F...	00569590	0	SymGetModuleBase64
A 00166F...	005695...	0	StackWalkEx
A 001671...	00569740	0	/rustc/59e7a308e40fbc6b0901c9a8ee8ed51b17f9e772\library\std\src\io\mod.rs
A 001671...	005697...	0	failed to write whole buffer
A 001671...	005697...	0	formatter error
A 001671...	005697...	0	assertion failed: (*tail).value.is_none()/rustc/59e7a308e40fbc6b0901c9a8ee8ed51b17f9e772\library\std\src\sync\mpsc\mpsc_queue.rs!
A 001672...	00569888	0	assertion failed: (*next).value.is_some()
A 001672...	005698...	0	called
A 001672...	005698...	0	Option::unwrap()
A 001672...	005698...	0	on a
A 001672...	005698...	0	value/rustc/59e7a308e40fbc6b0901c9a8ee8ed51b17f9e772\library\std\src\sync\mpsc\spsc_queue.rs
A 001673...	00569958	0	internal error: entered unreachable code/rustc/59e7a308e40fbc6b0901c9a8ee8ed51b17f9e772\library\std\src\sync\mpsc\mod.rs
A 001674...	00569A...	0	/rustc/59e7a308e40fbc6b0901c9a8ee8ed51b17f9e772\library\std\src\sync\mpsc\sync.rs

Figure 2. Strings viewed on BinText showing Rust modules/functions used by the binary

Blackbox analysis

When executed, the Rust binary prompts the following error requiring a password to be passed as an argument. This command-line feature is similar to the Agenda ransomware binaries written in Golang.

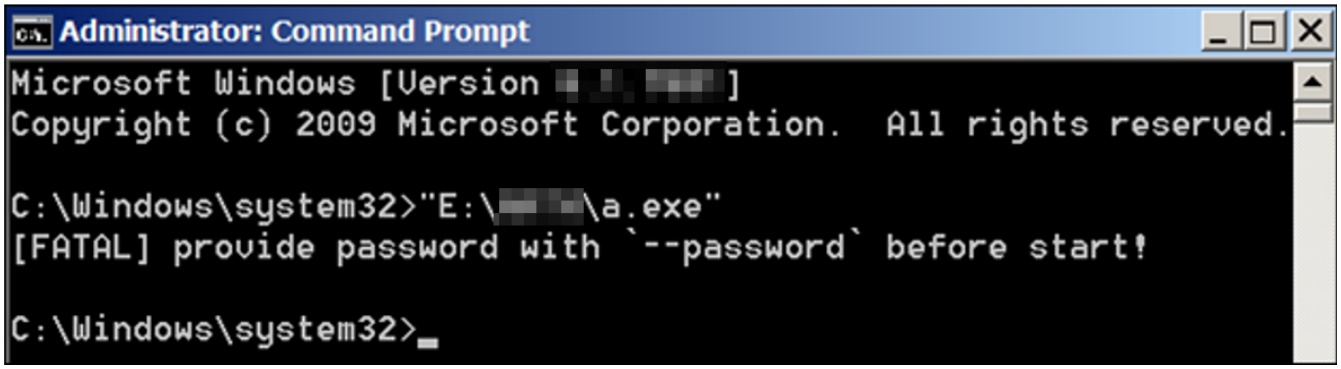

Figure 3. Error prompt when the sample was executed

Upon execution of the sample with "—password" as its parameter in conjunction with a dummy password "AgendaPass," the ransomware sample runs its malicious routine starting with the termination of various processes and services.

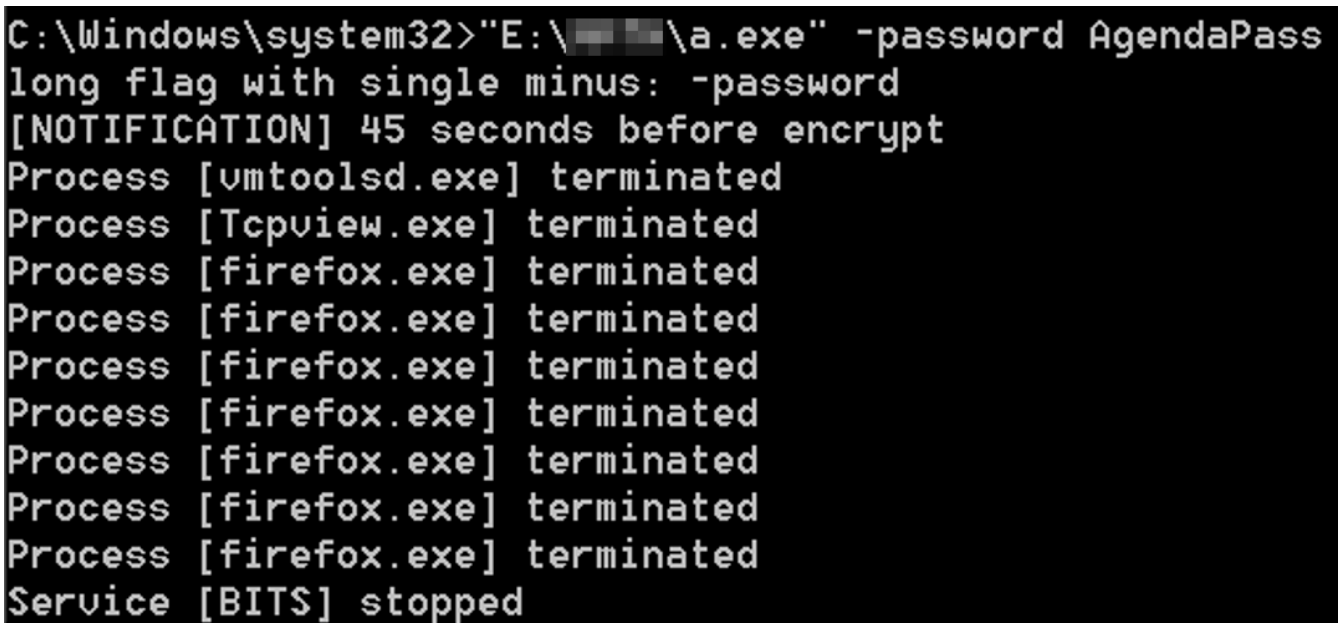

Figure 4. Termination of applications and services

Specific to the sample we analyzed, the ransomware appends the extension "MmXReVIxLV" to encrypted files. It also displays activity logs on the command prompt, including the file it has encrypted and the elapsed time.

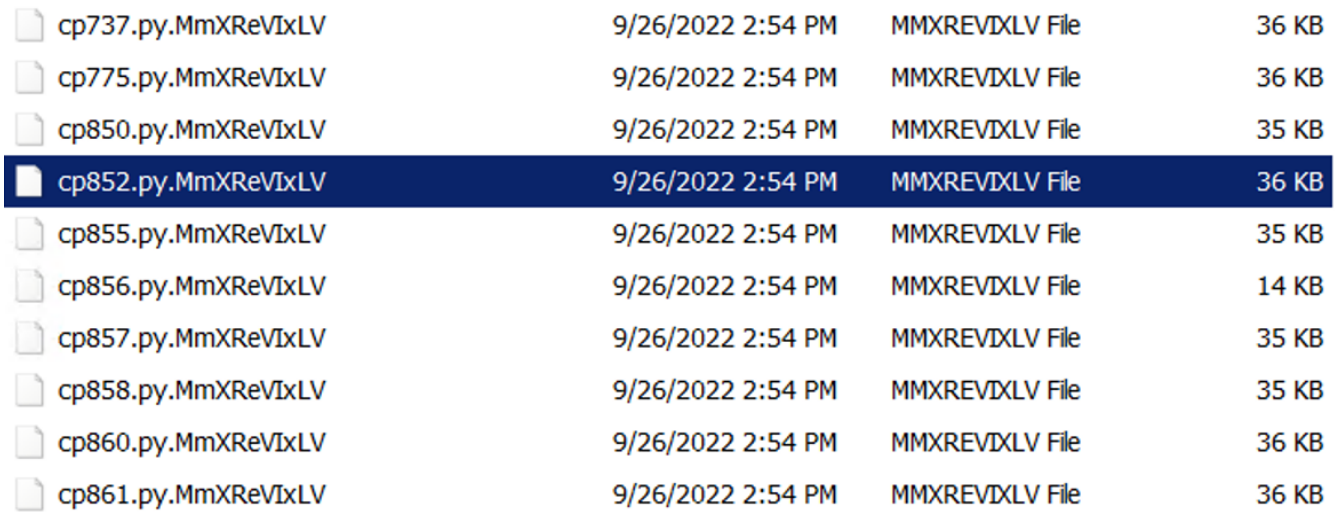

Figure 5. Examples of encrypted files

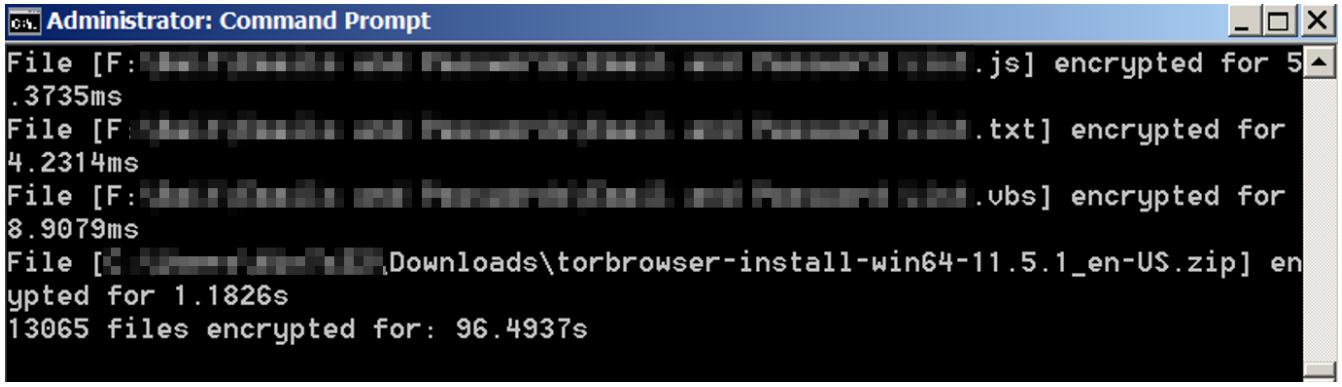

Figure 6. Logs in encrypting files

The ransomware will then proceed to drop its ransom note on every directory it encrypts. As observed in its ransom note, the password used to execute the ransomware will also be used as the password for logging in to the support chat site of the ransomware group.

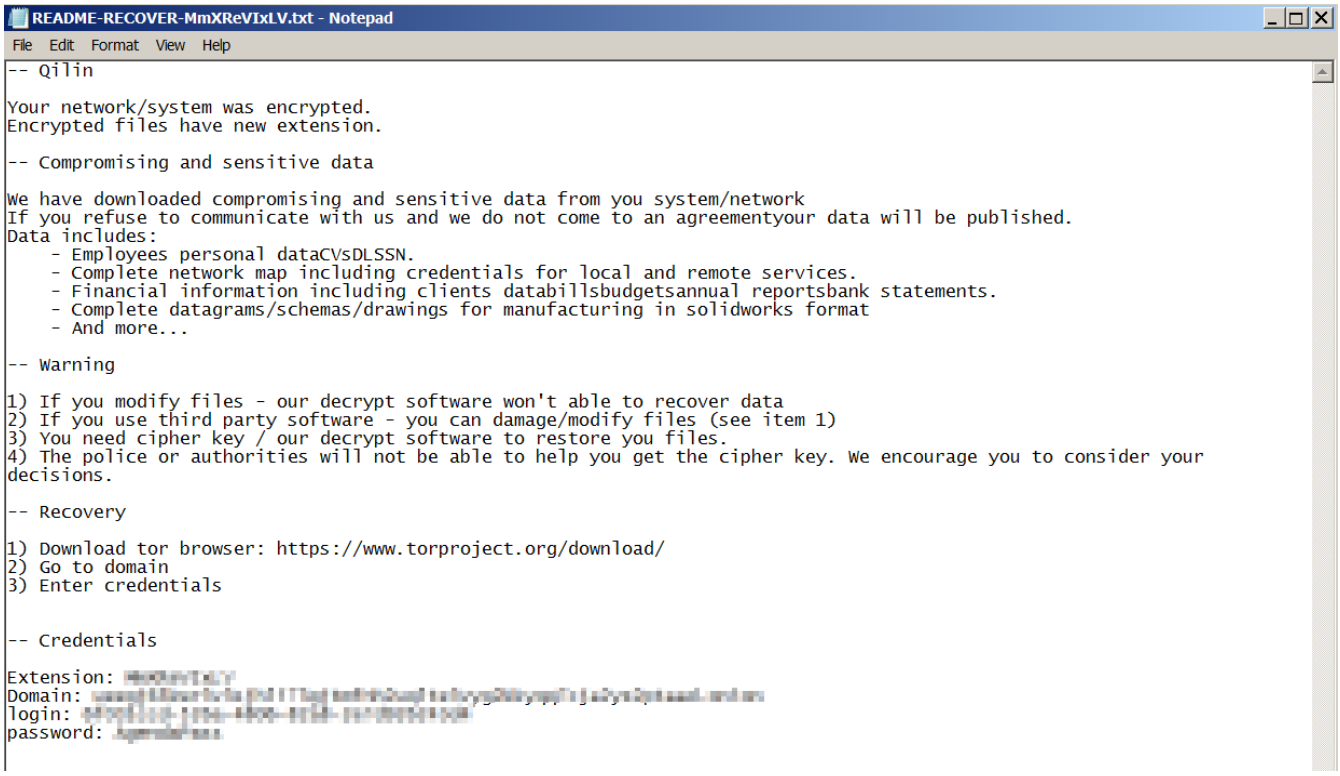

Figure 7. Agenda ransom note

Agenda ransomware analysis

Unlike Agenda's Golang variant, which accepts 10 arguments, its Rust variant only accepts three arguments:

Argument	Description
-password {string}	Defines the password to enter landing
-ips {IP address}	Allows for providing IP addresses
-paths {directory}	Defines the path that parses directories; if this flag is used and left empty, all directories will be scanned

Table 1. Arguments used by the Agenda ransomware's Rust variant

The Rust variant also contains hard-coded configuration inside its binaries like the earlier samples compiled in Golang.

Figure 8. Function inside the binary containing the configuration

```
013C57AD                db ' "public_rsa_pem": "-----BEGIN PUBLIC KEY-----\nMIICIjANBgkqhkiG9'
013C57AD                db 'w0BAQEFAAOCAg8AMIICCgKCAgEA8jT9jTtlea41CPHm9oaK\ns7j93wKJrVIkSF4r'
013C57AD                db 'LqcG8tN60Tg2qpxXlr0VL5Mjmr3cIXL4No/ytOiURXqwJSPO\nIMEKdhbJbU4g87u'
013C57AD                db 'xAg3rYCCt8MuwKgzEi7wrA1+orKls7pQ0YGRCVcKTSyvJhZyE\nXF0BmHpoRLFS+V'
013C57AD                db 'aYZmRG9GGilIZGkBdCNUq6jwUfwCXwd1nolF3ARWeDnOkAHBl1\nn60xF84b/taCx'
013C57AD                db 's1imBZAAKZEVGg4rA08dfwWphSdRqNi843UAIJ54dqX6SqJncz9\nj6IxOHKPS1Ro'
013C57AD                db 'T7PfLrF+MW9DeEZYLlyUS2mvZkvmCq4fF4wEeVrB16kfRbGv7+M9\nvIfHDDVjQ6O'
013C57AD                db '6ASHuX0MiDhOSlC6JpF1TdW/twn9quoLW21E2NipvFODhtk+8ntoW\nPfXt9iaNiy'
013C57AD                db '/c+RHlOA2OjfBg9XrZ++KPpGLONKV/cILtbAvdOgrp9XUGGBXdI9vK\n7EIcpiJY2'
013C57AD                db 'UWUF/XruzVFonxv1r2M08pvpI9BxczpVTZTKi13JW/UNth8KzGW7mf8\nfyZZkyfU'
013C57AD                db 'dLYlq1SB3aPLwucq8spv+vql2RLIQYZhASL5LmxOErHDoF44UgQuDGYP\n44rHo3e'
013C57AD                db 'hGTzrKIauBagY81ahJct+9ixhUdKRjxaocI+A5XZJq0bBmAIB8V6pyLJ7\nnNS1eF'
013C57AD                db 'O8wMpEi3iV4sIJTXUCAwEAAQ==\n-----END PUBLIC KEY-----\n",',0Ah
013C57AD                db ' "private_rsa_pem": "",',0Ah
013C57AD                db ' "directory_black_list": [',0Ah
013C57AD                db ' "windows",',0Ah
013C57AD                db ' "system volume information",',0Ah
013C57AD                db ' "intel",',0Ah
013C57AD                db ' "$windows.~ws",',0Ah
013C57AD                db ' "application data",',0Ah
013C57AD                db ' "$recycle.bin",',0Ah
013C57AD                db ' "mozilla",',0Ah
013C57AD                db ' "program files (x86)",',0Ah
013C57AD                db ' "program files",',0Ah
013C57AD                db ' "$windows.~bt",',0Ah
013C57AD                db ' "public",',0Ah
013C57AD                db ' "msocache",',0Ah
013C57AD                db ' "default",',0Ah
013C57AD                db ' "all users",',0Ah
013C57AD                db ' "tor browser",',0Ah
```

Figure 9. Strings containing the configuration

It also added the -n, -p, fast, skip, and step flags on its configurations, which are not present in the Golang variant configuration and only used via command-line argument. Upon further analysis, we have learned that these flags are used for intermittent encryption. This tactic enables the ransomware to encrypt the victim's files faster by partially encrypting the files depending on the values of the flags. This tactic is becoming more popular among ransomware actors as it lets them encrypt faster and avoid detections that heavily rely on read/write file operations.

Flags	Description
fast	Encrypts the first (N*0x200000h) of the file
skip (N) – step (Y)	Skip encryption for N bytes after encrypting Y bytes of the file
n: {N} p: {P}	Encrypt (N*0x200000h) of the file and skips p bytes (P - percentage of the file size)

Table 2. Flags used for intermittent encryption

```
db ' "company_id": "MmXReVIxLV",',0Ah
db ' "n": 0,',0Ah
db ' "p": 0,',0Ah
db ' "fast": 0,',0Ah
db ' "skip": 0,',0Ah
db ' "step": 0,',0Ah
```

Figure 10. Flags used for intermittent encryption

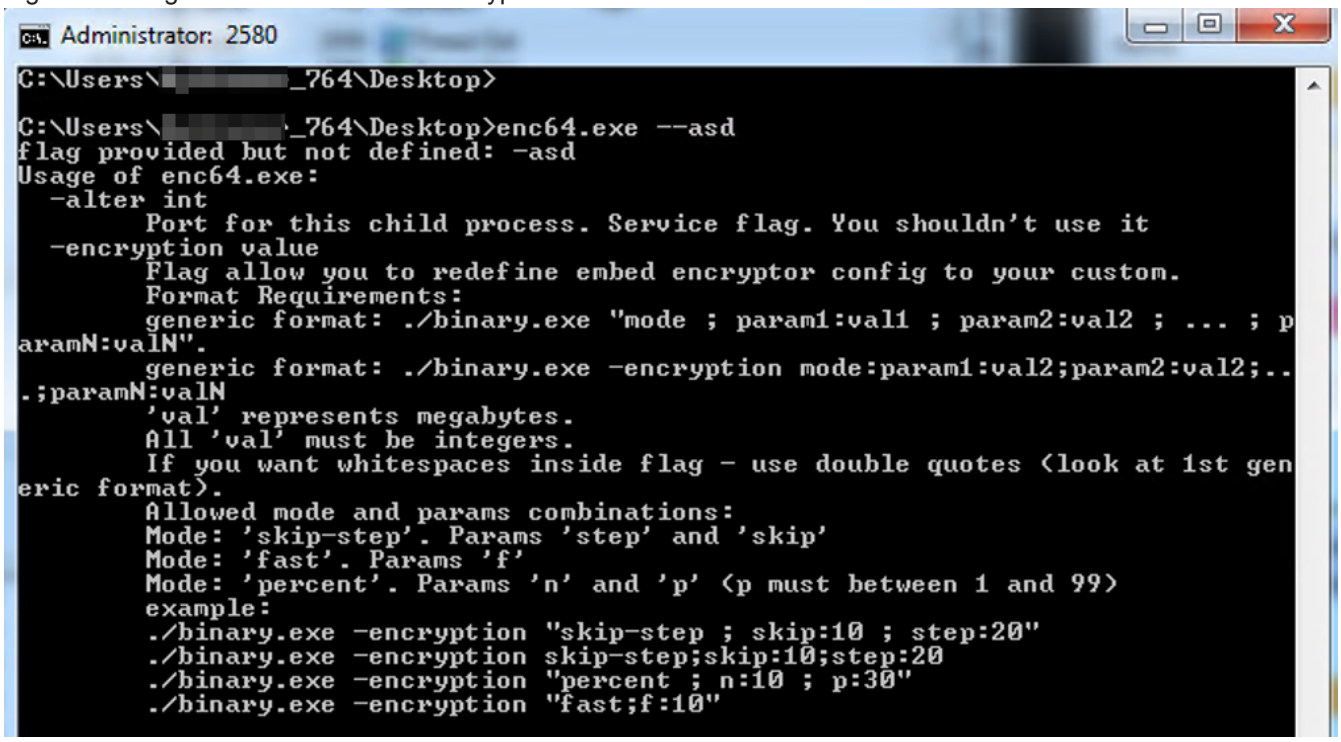

Figure 11. Command-line arguments accepted by the Golang variant of the Agenda ransomware

We tried to mimic its encryption behavior using some of the flags present on its configuration. For this simulation, we used a dummy file filled with "A" as its content.

For fast mode:

Value: 1

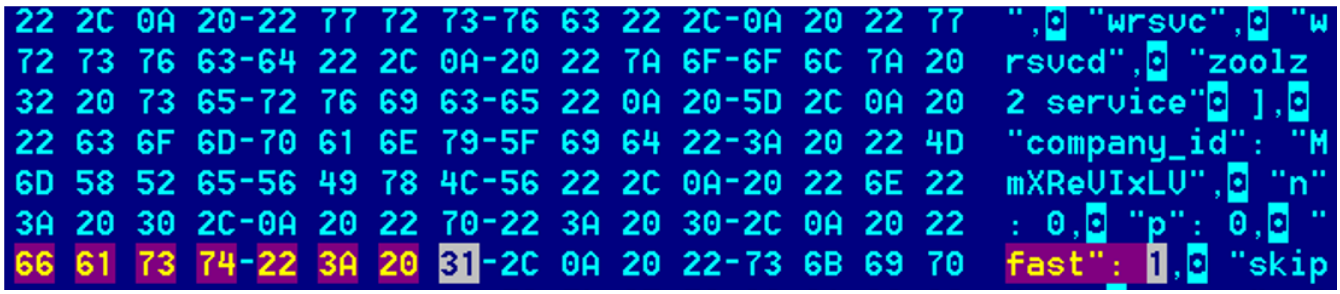

Figure 12. Fast flag set to 1

Encrypted bytes: 1 * 0x200000h, where 1 is the value set in the fast flag

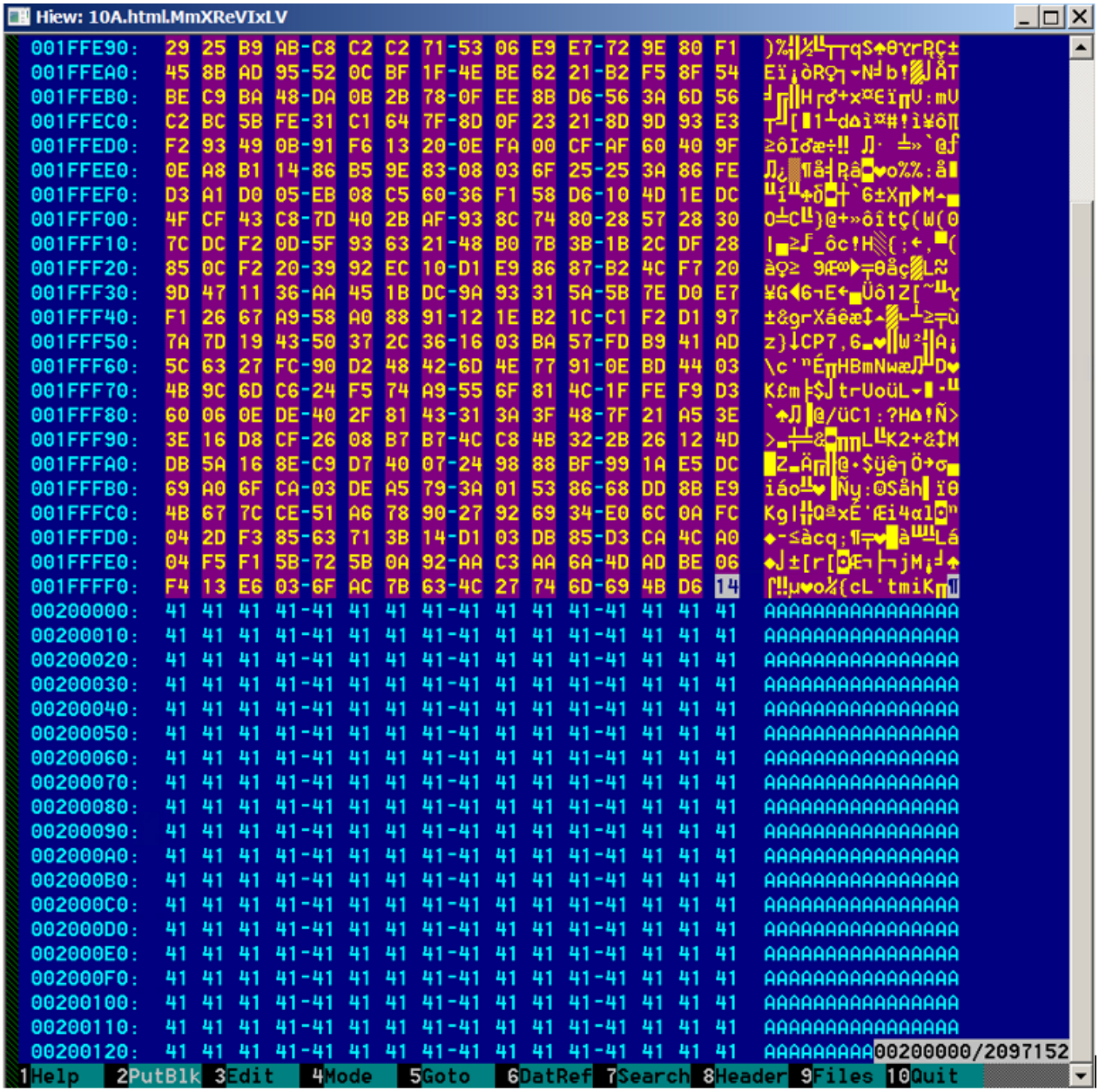

Figure 13. 0x200000h bytes encrypted
For N-P mode:

Figure 14. flags set to n = 1; p = 1
Total size = 88,082,336 bytes

Bytes encrypted = 1 * 0x200000,h where 1 is the value set in the n flag

Bytes skipped = 880,818 bytes (1% of the whole file), where 1 is the value set in the p flag

Figure 15. 0x200000h of bytes encrypted

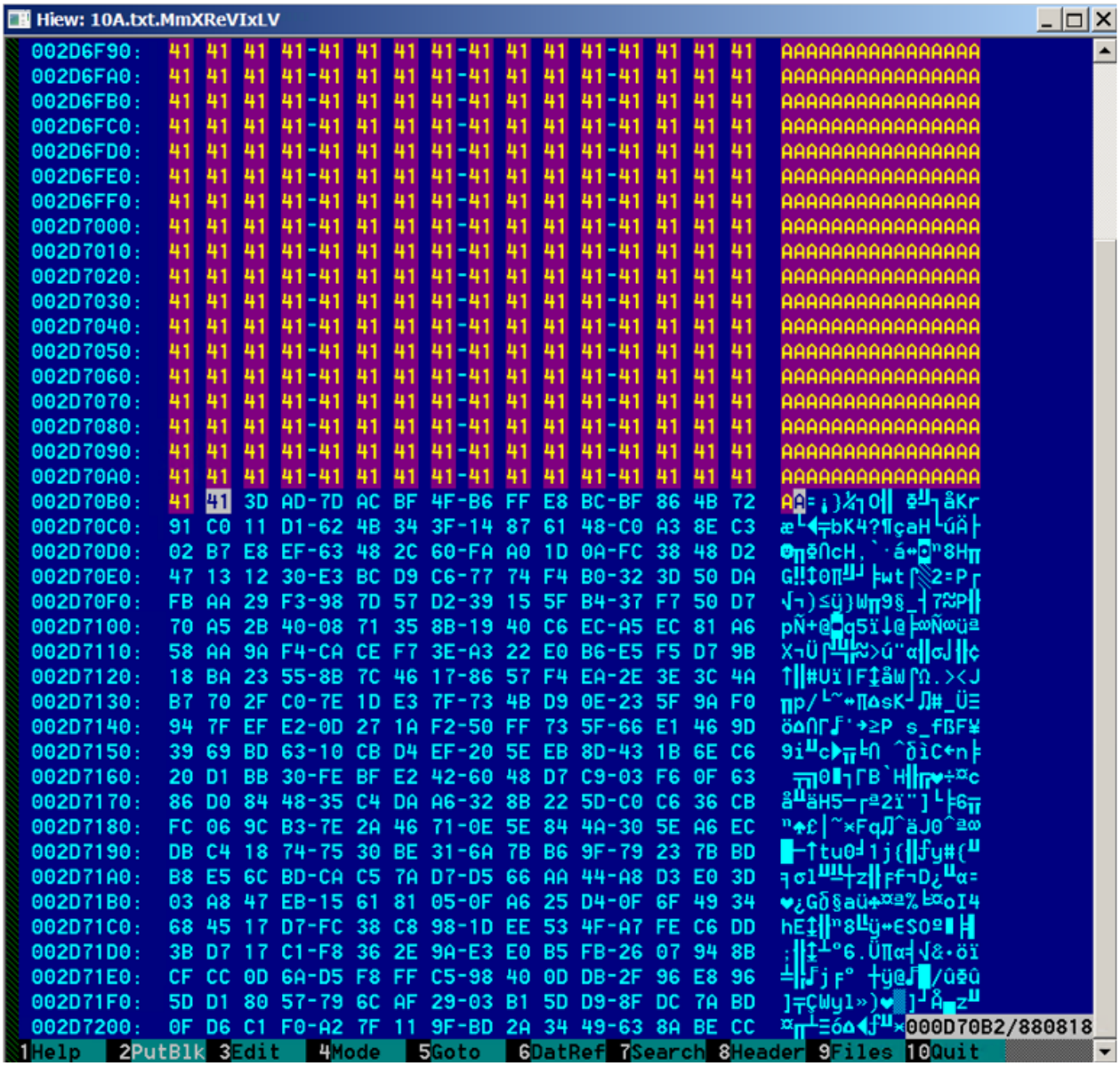

Figure 16. 880,818 bytes (equivalent to 1% of the file) encrypted

Aside from the additional flags used for different encryption modes, the Rust variant has included AppInfo to its roster of services to terminate. It disables User Account Control (UAC), a Windows feature that helps prevent malware from executing with administrative rights, resulting in the inability to run other applications with administrative privileges.

```
LABEL_78:
      if ( v103 )
        HeapFree(hHeap, 0, v115);
      *&lpMem[8] = v109;
      *lpMem = v108;
      Disable_Service_Start(a1, lpMem);
      memset(lpMem, 0, 28);
      if ( ControlService(Service_handle, '\x01', lpMem) )// SERVICE_CONTROL_STOP
      {
        v47 = sub_439FB0();
        v49 = v48;
        v51 = v50;
```

Figure 17. Function used to stop service using parameter 0x01 equivalent to SERVICE_CONTROL_STOP

```
LABEL_133:
              if ( ChangeServiceConfigW(Service_handle, 0xFFFFFFFF, '\x04', 0xFFFFFFFF, 0, 0, 0, 0, 0, 0, 0) )// SERVICE_DISABLED
              {
                v75 = v56;
                LODWORD(v108) = 0;
                if ( !v55 )
                  goto LABEL_167;
                v76 = &v56[v55];
                v77 = v56;
```

Figure 18. Function used for disabling services using parameter 0x04 equivalent to SERVICE_DISABLED

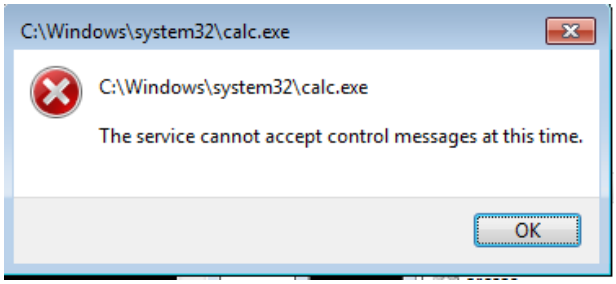

Figure 19. Unable to run an application with administrative rights after disabling AppInfo service

The Agenda ransomware is also known to deploy customized ransomware for each victim, and we have seen that its Rust variants have an allocated space for adding accounts in their configuration to be used mostly for privilege escalation.

```
db ' "accounts": [],',0Ah
db ' "note": "-- Qilin\r\n\r\nYour network/system was encrypted.\r\nE'
db 'ncrypted files have new extension.\r\n\r\n-- Compromising and sen'
db 'sitive data\r\n\r\nWe have downloaded compromising and sensitive '
db 'data from you system/network\r\nIf you refuse to communicate with'
db ' us and we do not come to an agreementyour data will be published'
db '.\r\nData includes:\r\n    - Employees personal dataCVsDLSSN.\r\n'
db '    - Complete network map including credentials for local and re'
db 'mote services.\r\n    - Financial information including clients d'
db 'atabillsbudgetsannual reportsbank statements.\r\n    - Complete d'
db 'atagrams/schemas/drawings for manufacturing in solidworks format\'
```

Figure 20. Allocated accounts in the Rust variant configuration of the Agenda ransomware

The file extension to be appended on the encrypted files is hard-coded in its configuration.

```
db ' "company_id": "MmXReVIxLV",',0Ah
```

Figure 21. File extension to be appended

Unlike the previous Golang variant, however, the threat actors did not include the credentials of the victim in the configuration of the Rust variant. This feature of the latter prevents other researchers not only from visiting the ransomware's chat support site but also accessing the threat actors' conversations when a sample becomes available externally. It also prevents unsolicited messages from other people besides the victim.

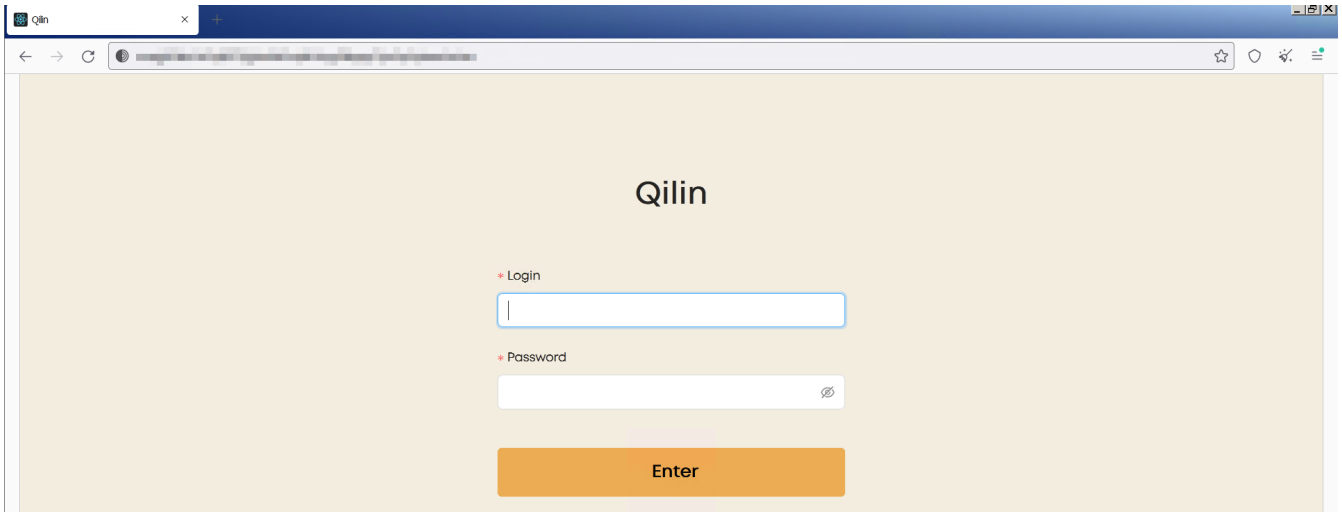

Figure 22. The Agenda ransomware chat support site

Conclusion

An emerging ransomware family, Agenda has recently been targeting critical sectors such as healthcare and education industries. At present, its threat actors appear to be migrating their ransomware code to Rust as recent samples still lack some features seen in the original binaries written in the Golang variant of the ransomware. Rust language is becoming more popular among threat actors as it is more difficult to analyze and has a lower detection rate by antivirus engines.

Threat actors continue to favor ransomware as their tool of choice for conducting their operations, reiterating the call for enterprises and organizations to rely on a multilayered solution to secure data. Trend Micro Vision One™ provides visibility, correlated detection, and behavior monitoring across multiple layers: email, endpoints, servers, cloud workloads to help enterprises and organizations protect their systems from different threats, including ransomware.

Indicators of Compromise (IOCs)

SHA256	Detection
e90bdaaf5f9ca900133b699f18e4062562148169b29cb4eb37a0577388c22527	Ransom.Win32.AGENDA.THIAFBB
55e070a86b3ef2488d0e58f945f432aca494bfe65c9c4363d739649225efbbd1	Ransom.Win32.AGENDA.THIAHBB
37546b811e369547c8bd631fa4399730d3bdaff635e744d83632b74f44f56cf6	Ransom.Win32.AGENDA.THIAHBB