## Agenda Ransomware Uses Rust to Target More Vital Industries

b 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, <u>ransomware-as-a-service (RaaS)</u> groups like <u>BlackCat</u>, <u>Hive</u>, and <u>RansomExx</u> 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 <u>Agenda</u> (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 <u>numerous</u> <u>companies</u> 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 <u>ransomware</u> group posts on its leak site are located in different countries and belong mostly in the manufacturing and IT industries, with a <u>combined</u> <u>revenue</u> that surpasses US\$550 million.

Recently, we found a sample of the Agenda ransomware written in Rust language and detected as <u>Ransom.Win32.AGENDA.THIAFBB</u>. 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.

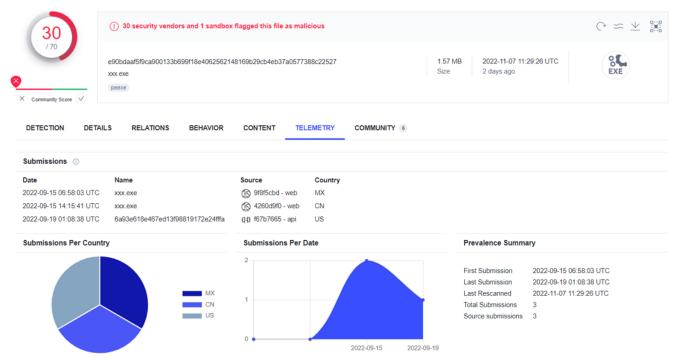


Figure 1. Submission details of the binary in VirusTotal, including the submission date and region it was uploaded.

File pos	Mem pos	ID	Text	-
A 00166F	00569590	0	SymGetModuleBase64	
A 00166F	005695	0	StackWalkEx	
<b>A</b> 001671	00569740	0	/rustc/59e7a308e40fbc6b0901c9a8ee8ed51b17f9e772\library\std\src\io\mod.rs	
<b>A</b> 001671	005697	0	failed to write whole buffer	
<b>A</b> 001671	005697	0	formatter error	
<b>A</b> 001671	005697	0	assertion failed: ("tail).value.is_none()/rustc/59e7a308e40fbc6b0901c9a8ee8ed51b17f9e772\library\std\src\sync\mpsc\mpsc_queue.rs!	
<b>A</b> 001672	00569888	0	assertion failed: (*next).value.is_some()	
<b>A</b> 001672	005698	0	called	
<b>A</b> 001672	005698	0	Option::unwrap()	
<b>A</b> 001672	005698	0	ona	
A 001672	005698	0	value/rustc/59e7a308e40fbc6b0901c9a8ee8ed51b17f9e772\library\std\src\sync\mpsc\spsc_queue.rs	
<b>4</b> 001673	00569958	0	internal error: entered unreachable code/rustc/59e7a308e40fbc6b0901c9a8ee8ed51b17f9e772\library\std\src\sync\mpsc\mod.rs	
<b>A</b> 001674	00569A	0	/rustc/59e7a308e40fbc6b0901c9a8ee8ed51b17f9e772\library\std\src\sync\mpsc\sync.rs	-
4				

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.

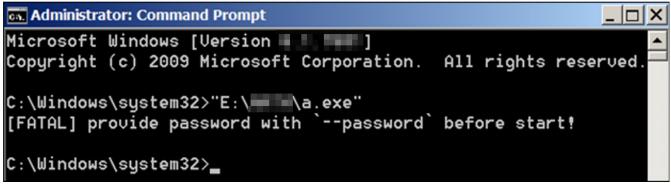


Figure 3. Error prompt when the sample was executed

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.

C:\Windows\system32>"E:\\a.exe" -password AgendaPass
long flag with single minus: -password
[NOTIFICATION] 45 seconds before encrypt
Process [vmtoolsd.exe] terminated
Process [Tcpview.exe] terminated
Process [firefox.exe] terminated
Service [BITS] stopped

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.

cp737.py.MmXReVIxLV	9/26/2022 2:54 PM	MMXREVIXLV File	36 KB
cp775.py.MmXReVIxLV	9/26/2022 2:54 PM	MMXREVIXLV File	36 KB
cp850.py.MmXReVIxLV	9/26/2022 2:54 PM	MMXREVIXLV File	35 KB
cp852.py.MmXReVIxLV	9/26/2022 2:54 PM	MMXREVIXLV File	36 KB
cp855.py.MmXReVIxLV	9/26/2022 2:54 PM	MMXREVIXLV File	35 KB
cp856.py.MmXReVIxLV	9/26/2022 2:54 PM	MMXREVIXLV File	14 KB
cp857.py.MmXReVIxLV	9/26/2022 2:54 PM	MMXREVIXLV File	35 KB
cp858.py.MmXReVIxLV	9/26/2022 2:54 PM	MMXREVIXLV File	35 KB
cp860.py.MmXReVIxLV	9/26/2022 2:54 PM	MMXREVIXLV File	36 KB
cp861.py.MmXReVIxLV	9/26/2022 2:54 PM	MMXREVIXLV File	36 KB

Figure 5. Examples of encrypted files

. 🗆 🗙

File [F: \_\_\_\_\_\_.js] encrypted for 5 .3735ms File [F: \_\_\_\_\_\_.txt] encrypted for 4.2314ms File [F: \_\_\_\_\_\_.ubs] encrypted for 8.9079ms File [ \_\_\_\_\_\_.Downloads\torbrowser-install-win64-11.5.1\_en-US.zip] en ypted for 1.1826s 13065 files encrypted for: 96.4937s

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.

README-RECOVER-MmXReVIxLV.txt - Notepad	<u>_   X</u>
File Edit Format View Help	
Qilin	<b></b>
Your network/system was encrypted. Encrypted files have new extension.	
Compromising and sensitive data	
We have downloaded compromising and sensitive data from you system/network If you refuse to communicate with us and we do not come to an agreementyour data will be published. Data includes: - Employees personal dataCVsDLSSN. - Complete network map including credentials for local and remote services. - Financial information including clients databillsbudgetsannual reportsbank statements. - Complete datagrams/schemas/drawings for manufacturing in solidworks format - And more	
Warning	
<ol> <li>If you modify files - our decrypt software won't able to recover data</li> <li>If you use third party software - you can damage/modify files (see item 1)</li> <li>You need cipher key / our decrypt software to restore you files.</li> <li>The police or authorities will not be able to help you get the cipher key. We encourage you to consider your decisions.</li> </ol>	
Recovery	
1) Download tor browser: https://www.torproject.org/download/ 2) Go to domain 3) Enter credentials	
Credentials	
Extension: Province For The International In	
Eigure 7. Agonda ransom poto	

# Figure 7. Agenda ransom note **Agenda ransomware analysis**

Unlike <u>Agenda's Golang variant</u>, 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.

012CCD3D	68 C27D0000	PUSH 7DC2	
012CCD42	68 AD573C01	PUSH a.013C57AD	ASCII "{",LF," ""public_rsa_pem"": ""BEGIN PUBLIC KEY
012CCD47		PUSH EAX	
012CCD48	E8 53C4FFFF	CALL a.012C91A0	

Figure 8. Function inside the binary containing the configuration

013C57AD	db ' "public_rsa_pem": "BEGIN PUBLIC KEY\nMIICIjANBgkqhkiG9'
013C57AD	<pre>db 'w0BAQEFAAOCAg8AMIICCgKCAgEA8jT9jTtlea41CPHm9oaK\ns7j93wKJrVIkSF4r'</pre>
013C57AD	db 'LqcG8tN60Tg2qpxXlr0VL5Mjmr3cIXL4No/ytOiURXqwJSPO\nIMEKdhbJbU4g87u'
013C57AD	<pre>db 'xAg3rYCCt8MuwKgzEi7wrA1+orKls7pQ0YGRCVcKTSyvJhZyE\nXF0BmHpoRLFS+V'</pre>
013C57AD	<pre>db 'aYZmRG9GGillZGkBdCNUq6jwUfwCXwd1nolF3ARWeDnOkAHBl1\nn60xF84b/taCx'</pre>
013C57AD	db 's1imBZAAKZEVGg4rA08dfwWphSdRqNi843UAIJ54dqX6SqJncz9\nj6IxOHKPS1Ro'
013C57AD	db 'T7PfLrF+MW9DeEZYLlyUS2mvZkvmCq4fF4wEeVrB16kfRbGv7+M9\nvIfHDDVjQ60'
013C57AD	<pre>db '6ASHuX0MiDhOSlC6JpF1TdW/twn9quoLW21E2NipvF0Dhtk+8ntoW\nPfXt9iaNiy'</pre>
013C57AD	db '/c+RH10A20jfBg9XrZ++KPpGL0NKV/cILtbAvd0grp9XUGGBXdI9vK\n7EIcpiJY2'
013C57AD	db 'UWUF/XruzVFonxv1r2M08pvpI9BxczpVTZTKi13JW/UNth8KzGW7mf8\nfyZZkyfU'
013C57AD	db 'dLYlq1SB3aPLwucq8spv+vql2RLIQYZhASL5LmxOErHDoF44UgQuDGYP\n44rHo3e'
013C57AD	db 'hGTzrKIauBagY81ahJct+9ixhUdKRjxaocI+A5XZJq0bBmAIB8V6pyLJ7\nnNS1eF'
013C57AD	db '08wMpEi3iV4sIJTXUCAwEAAQ==\nEND 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",',OAh
013C57AD	db ' "program files (x86)",',0Ah
013C57AD	db ' "program files",',0Ah
013C57AD	db ' "\$windows.~bt",',0Ah
013C57AD	db ' "public",',OAh
013C57AD	db ' "msocache",',OAh
013C57AD	db ' "default",',OAh
013C57AD	db ' "all users",',OAh
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	•	<pre>"company_id": "MmXReVIxLV",',0Ah</pre>
db	1	"n": 0,',0Ah
db	1	"p": 0,',0Ah
db	1	"fast": 0,',0Ah
db	1	"skip": 0,',0Ah
db	1	"step": 0,',0Ah

Figure 10. Flags used for intermittent encryption

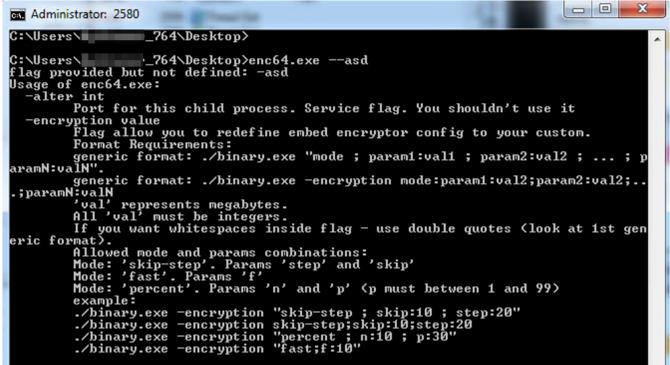


Figure 11. Command-line arguments accepted by the Golang variant of the Agenda ransomware We tried to mimic its encryption behavior using some of the flags present on its configuration. For this simulation, we used a dummy file filled with "A" as its content.

For fast mode:

Value: 1

22	20	0A	20-22	77	72	73-76	63	22	2C-0A	20	22	77	", <mark>0</mark> "wrsvc", <mark>0</mark> "w
72	73	76	63-64	22	20	0A-20	22	7A	6F-6F	60	7A	20	rsucd", <mark>0</mark> "zoolz
32	20	73	65-72	76	69	63-65	22	0A	20-5D	20	0A	20	2 service" <mark>0</mark> ],0
													"company_id": "M
6D	58	52	65-56	49	78	40-56	22	20	0A-20	22	6E	22	mXReUIxLV", <mark>0</mark> "n"
3A	20	30	2C-0A	20	22	70-22	3A	20	30-20	0A	20	22	: 0, <mark>0</mark> "p": 0, <mark>0</mark> "
66	61	73	74-22	3A	20	31 <mark>-2C</mark>	0A	20	22-73	6B	69	70	fast": [, <mark>0</mark> "skip

Figure 12. Fast flag set to 1

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

🖪 Hiew: 10A.html.MmXReVIxLV										
001FFE90:	29 25 B	9 AB-C8 C2 C2	2 71-53 06 E9 E7-72 9	E 80 F1 )%	rqS+8yrRDZ					
001FFEA0:	45 8B AI				-N <sup>l</sup> b !∭ÅT					
001FFEB0:	BE C9 B				פ∈ïπÜ:mU					
001FFEC0:	C2 BC 5	B FE-31 C1 64	+ 7F-8D 0F 23 21-8D 9		loì¤#!ì¥ôπ					
001FFED0:	F2 93 4		3 20-0E FA 00 CF-AF 6		! Л· ±»`@f					
001FFEE0:	0E A8 B	1 14-86 B5 9F	E 83-08 03 6F 25-25 3	A 86 FE J; 184	ξâ <mark>-</mark> ψo%% : å∎					
001FFEF0:	D3 A1 D	0 05-EB 08 C	5 60-36 F1 58 D6-10 4	D 1E DC <sup>Π</sup> ĭΠ <sub>Φ</sub> δ	È <sup>°</sup> 6±Xπ▶M≁ <mark>_</mark>					
001FFF00:	4F CF 4:	3 C8-7D 40 2	3 AF-93 8C 74 80-28 5	7 28 30 0±CL)@-	×ôîtÇ(W(0					
001FFF10:	7C DC F	2 0D-5F 93 63	3 21-48 B0 7B 3B-1B 2	C DF 28   <u></u> _≥,[_ô(	≥!H∭(;+, <mark>=</mark> (					
001FFF20:	85 0C F	2 20-39 92 E	C 10-D1 E9 86 87-B2 4	C F7 20 àQ≥ 968	•▶ <del>∓</del> θåç <mark>∭</mark> L%					
001FFF30:	9D 47 1	1 36-AA 45 1E	3 DC-9A 93 31 5A-5B 7	E D0 E7 ¥G46-1E4	-Ûô1Ζ[ <sup>~μ</sup> γ					
001FFF40:	F1 26 6	7 A9-58 A0 88	3 91-12 1E B2 1C-C1 F		êæ‡ <mark>≁</mark> ∭⊢⊥≥ <del>⊤</del> ù					
001FFF50:	7A 7D 1	9 43 <mark>-</mark> 50 37 20	C 36-16 03 BA 57-FD B		,6 <b>_♥</b>  ₩² <b> </b> A;					
001FFF60:	5C 63 2	7 FC-90 D2 48	3 42-6D 4E 77 91-0E E		IBmNwæ <b>∬<sup>⊔</sup>D</b> ⊌					
001FFF70:	4B 9C 6I		4 A9-55 6F 81 4C-1F F	E F9 D3 K£m [\$]	trUoüL <b>≁∎</b> • <sup>Щ</sup>					
001FFF80:	60 06 01			1 A5 3E `♠Л @/(	iC1:?Ho!N>					
001FFF90:	3E 16 D			6 12 4D > + &	IIIL <sup>L</sup> K2+&1M					
001FFFA0:	DB 5A 1				ē•\$ÿê <sub>l</sub> Ö <b>≯σ</b>					
001FFFB0:	69 A0 6			D 8B E9 iáo 🗣	ly:@Såh <mark>i</mark> ï0					
001FFFC0:	4B 67 7				¢É'Æi4αl <mark>o</mark> n					
001FFFD0:	04 2D F				¶ <b>∓v</b> a <sup>lu⊥</sup> Lá					
001FFFE0:	04 F5 F				Æn hnjM;d ↔					
001FFFF0:	F4 13 E				[cL'tmiKm <sup>II</sup>					
00200000:	41 41 4				AAAAAAAAA					
00200010:	41 41 4									
00200020:	41 41 4									
00200030:	41 41 4				AAAAAAAAA					
00200040:	41 41 4									
00200050:	41 41 4				000000000000000000000000000000000000000					
00200070:	41 41 4									
00200080:	41 41 4									
00200090:	41 41 4									
002000A0:	41 41 4				000000000000000000000000000000000000000					
002000B0:	41 41 4				000000000000000000000000000000000000000					
002000C0:	41 41 4				000000000000000000000000000000000000000					
002000D0:	41 41 4				000000000000000000000000000000000000000					
002000E0:	41 41 4				000000000000000000000000000000000000000					
002000F0:	41 41 4				000000000000000000000000000000000000000					
00200100:	41 41 4				000000000000000000000000000000000000000					
00200110:	41 41 4	1 41-41 41 41	41-41 41 41 41-41 4		19999999999					
00200120:	41 41 4	1 41-41 41 41	41-41 41 41 41-41 4	1 41 41 888888	AA00200000/2097152					
1Help 2Pu	tB1k <mark>3</mark> Ed	it <mark>4</mark> Mode	5 <mark>Goto 6</mark> DatRef 7Sea	rch <mark>8</mark> Header 9Fil						
E. 10 0 0										

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

20 0	9A 2	20	22-63	6F	6D	70-61	6E	79	5F-69	64	22	3A	<pre>, o "company_id":</pre>
													"MmXReVIxLV", <mark>0</mark>
22 🤅	6E 2	22	3A <mark>-</mark> 20	31	20	0A-20	22	70	22-3A	20	31	2C	"n": 1, <mark>0</mark> "p" <u>:</u> 1,

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

Hiew: 10A.txt.MmXReVIxLV										
001FFEE0:			D5 58-E2 2D B	4 FF-98 00 0E E7	1F0¥FtF[F-1 ¢ JY					
001FFEF0:			D4 3F-5B 25 F		‼v↓i+â=?[%2H.29â					
001FFF00:			20 51-E6 CE 1		0úc≈ç~ Qµ <mark>∥</mark> _S!+(»					
001FFF10:				C 76-22 33 67 82	Nk.N4ARŇZBIU"3gé					
001FFF20:			58 D1-62 1F F		S§πOx©X∓b-JJmYI					
001FFF30:			93 A2-C8 C5 5		ر عال <sub>ع</sub> د المُؤلك بي المال					
001FFF40:			7B 91-F1 EB E		½÷ÅaΓ`(æ±δ∞∽በq <b>n</b> U					
001FFF50:			3C 17-A2 E2 5		H!ù°dH<‡6FRRΩGHÆ					
001FFF60:	CB 7C 2	20 FB-8D 24	A5 BE-DA 52 F		<b>π</b> ∣ √ì\$Ñ <sup>j</sup> [R[+ <sub>1</sub> .♥ì					
001FFF70:	07 OF F	F4 37-A8 D5	A0 57-89 7A 9	7 7F-89 E5 C2 EA	•¤ [7¿ FáWëzùΔëστΩ					
001FFF80:		4B 7B-B0 B2	38 20-05 9D 0	8 51-88 E7 AD C4	‡ëK{∭8 +¥ <mark>−</mark> Ω <sub>7</sub> γ;−					
001FFF90:	94 4E i	76 92-DD 48	E6 DD-25 07 F	C 20-59 DD 7E 33	öΝυÆ Ĥμ %•" Υ΄ ~3					
001FFFA0:	BF B2 S	97 85 <mark>-</mark> A3 49	C5 2A-C5 87 9	8 52-1C 60 84 A8	j∰ùàúI†×†ç¢R⊢`ä¿					
001FFFB0:	07 24 F	F2 3B-8E AE	12 B7-FB 03 9	9 9F-CF 1D 5D 5A	•\$≥;Ä«‡π√₩Ƀ±+]Z					
001FFFC0:	39 A7 8	84 F6-BE DB	35 3A-43 DE F	E BA-1D 9A AC F8	9ºä÷ <b>4 5</b> ∶C ∎ +ܼ°					
001FFFD0:	5A 98 E	E7 A8-98 2B	30 85-24 B2 2	F 85-26 A7 15 22	Zÿv¿ÿ+0à\$ <b>》</b> /₹&º§"					
001FFFE0:	5D 94 i	77 E2-62 C1	A7 82-3C 60 0		]öwГb <sup>⊥</sup> ≌é<` <b>÷</b> II÷£ď					
001FFFF0:	32 C3 i	71 64 <mark>-</mark> D7 1A	7C 18-E7 F4 4	5 98-94 1E DD D2	2 -qd → I ← Υ ſEÿö → 📊					
00200000:	41 41 4	41 41-41 41	41 41-41 41 4	1 41-41 41 41 41	AAAAAAAAAAAAAAA					
00200010:	41 41 4	41 41-41 41	41 41-41 41 4	1 41-41 41 41 41	AAAAAAAAAAAAAAA					
00200020:	41 41 4	41 41-41 41	41 41-41 41 4	1 41-41 41 41 41	AAAAAAAAAAAAAAA	Figure				
00200030:	41 41 4	41 41-41 41	41 41-41 41 4	1 41-41 41 41 41	AAAAAAAAAAAAAAA	Ű				
00200040:	41 41 4	41 41-41 41	41 41-41 41 4		AAAAAAAAAAAAAAAA					
00200050:			41 41-41 41 4		AAAAAAAAAAAAAAAA					
00200060:			41 41-41 41 4		AAAAAAAAAAAAAAAAA					
00200070:	41 41 4		41 41-41 41 4		AAAAAAAAAAAAAAAAA					
00200080:	41 41 4		41 41-41 41 4		AAAAAAAAAAAAAAAAA					
00200090:			41 41-41 41 4		AAAAAAAAAAAAAAAAA					
002000A0:			41 41-41 41 4		<u>AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA</u>					
002000B0:			41 41-41 41 4		<u>AAAAAAAAAAAAAAAAA</u>					
002000C0:	41 41 4		41 41-41 41 4		AAAAAAAAAAAAAAAAA					
002000D0:	41 41 4		41 41-41 41 4		AAAAAAAAAAAAAAAAA					
002000E0:			41 41-41 41 4		AAAAAAAAAAAAAAAAA					
002000F0: 00200100:	41 41 4		41 41-41 41 4		AAAAAAAAAAAAAAAAAA					
			41 41-41 41 4		AAAAAAAAAAAAAAAAAA					
00200110: 00200120:	41 41 4		41 41-41 41 4 41 41-41 41 4		AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA					
00200120:	41 41 4		41 41-41 41 4 41 41-41 41 4							
00200140:			41 41-41 41 4		AAAAAAAAAAAAAAAAAAA					
00200150:			41 41-41 41 4		AAAAAAAAAAAAAAAAAAA					
00200160:			$41 \ 41 \ 41 \ 41 \ 41 \ 41$							
00200170:				1 41-41 41 41 41	AAAAAAAAAA 00200000/20971	52				
1Help 2Pu		dit <mark>4</mark> Mode			der 9 <mark>Files 10</mark> Quit	<b>v</b>				
	5 0x200000h of bytes encrypted									

15. 0x200000h of bytes encrypted

Hiew: 10A.txt	.MmX	(ReV	/IxL\	v										
002D6F90:	41	41	41	41-41	41	41	41-41	41	41	41-41	41	41	41	000000000000000000000000000000000000000
002D6FA0:	41	41	41	41-41	41	41	41-41	41	41	41-41	41	41	41	8888888888888888888
002D6FB0:	41	41	41	41-41	41	41	41-41	41	41	41-41	41	41	41	888888888888888888
002D6FC0:	41	41	41	41-41	41	41	41-41	41	41	41-41	41	41	41	888888888888888888
002D6FD0:	41	41	41	41-41	41	41	41-41	41	41	41-41	41	41	41	8888888888888888888
002D6FE0:	41	41	41	41-41	41	41	41-41	41	41	41-41	41	41	41	888888888888888888
002D6FF0:	41	41	41	41-41	41	41	41-41	41	41	41-41	41	41	41	<u>AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA</u>
002D7000:	41	41	41	41-41	41	41	41-41	41	41	41-41	41	41	41	<u>AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA</u>
002D7010:	41	41	41	41-41	41	41	41-41	41	41	41-41	41	41	41	AAAAAAAAAAAAAAAA
002D7020:	41	41	41	41-41	41	41	41-41	41	41	41-41	41	41	41	<u>AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA</u>
002D7030:	41	41	41	41-41	41	41	41-41	41	41	41-41	41	41	41	<u>AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA</u>
002D7040:	41	41	41	41-41	41	41	41-41	41	41	41-41	41	41	41	AAAAAAAAAAAAAAAA
002D7050:	41	41	41	41-41	41	41	41-41	41	41	41-41	41	41	41	AAAAAAAAAAAAAAAAA
002D7060:	41	41	41	41-41	41	41	41-41	41	41	41-41	41	41	41	AAAAAAAAAAAAAAAA
002D7070:	41	41	41	41-41	41	41	41-41	41	41	41-41	41	41	41	AAAAAAAAAAAAAAAA
002D7080:	41	41	41	41-41	41	41	41-41	41	41	41-41	41	41	41	AAAAAAAAAAAAAAAA
002D7090:	41	41	41	41-41	41	41	41-41	41	41	41-41	41	41	41	AAAAAAAAAAAAAAAA
002D70A0:	41	41	41	41-41	41	41	41-41	41	41	41-41	41	41	41	AAAAAAAAAAAAAAAA
002D70B0:	41	41	3D	AD-7D	AC	BF	4F-B6	FF	E8	BC-BF	86	4B	72	<mark>፼፼</mark> =;} <mark>∦</mark> ገዐ∥ ፸ <sup>⊔</sup> ገåKr
002D70C0:	91	CO	11	D1-62	4B	34	3F-14	87	61	48-00	A3	8E	C3	æ <sup>L</sup> ¶ <del>∓</del> bK4?¶çaH <sup>L</sup> úÄ
002D70D0:	02	<b>B</b> 7	E8	EF-63	48	20	60-FA	A0	1D	0A-FC	38	48	D2	©η⊉ĤcH,`·á+ <mark>o</mark> n8H <mark>n</mark>
002D70E0:	47	13	12	30-E3	BC	D9	C6-77	74	F4	B0-32	3D	50	DA	G‼‡0Π╝╘wt ſ͡2=PŢ
002D70F0:	FB	AA	29	F3-98	7D	57	D2-39	15	5F	B4-37	F7	50	D7	√¬)≤ÿ}₩π9§_17%P
002D7100:	70	A5	2B	40-08	71	35	8B-19	40	C6	EC-A5	EC	81	A6	pÑ+@ <mark>=</mark> q5ï↓@ ⊨∞Ñ∞üª
002D7110:	-58	AA	9A	F4-CA	CE	F7	3E-A3	22	E0	B6-E5	F5	D7	9B	X¬Ü┞Щ¦╦>ú¨α┨σͿ∦¢
002D7120:	18	BA	23	55-8B	70	46	17-86	57	F4	EA-2E	3E	30	46	1 #Uï F‡åω[Ω.> <j< td=""></j<>
002D7130:	B7	70	2F	C0-7E	1D	E3	7F-73	4B	D9	0E-23	5F	9A	F0	πp/ <sup>L~</sup> +ΠΔsK <sup>J</sup> ∬#_ÜΞ
002D7140:	94	7F	EF	E2-0D	27	18	F2-50	FF	73	5F-66	E1	46	9D	ö∆∩ГҐ'+≥P s_fBF¥
002D7150:	- 39	69	BD	63-10	СВ		EF-20							9i <sup>⊔</sup> c∳π⊧∩_δìC∻n⊧
002D7160:	20	D1	BB	30-FE	BF	E2	42-60	48	D7	C9-03	F6	ΘF	63	<u></u> ∏0∎₁ՐВ`Н <mark>⊪</mark> ү÷¤c
002D7170:				48-35			A6-32							å <sup>∐</sup> äH5−Γª2ï¨]└╞6π
002D7180:							71-0E							<u>"</u> ♠£   ~×FqЛ^äJ0 <sup>^</sup> ª∞
002D7190:						BE	31-6A	7B						-1tu0≤1j( fy#("
002D71A0:	B8	E5	60	BD-CA	C5		D7-D5			44-A8				ησ1""+z  Ff¬D¿"α=
002D71B0:	03			EB-15			05-0F							♥¿Gϧaü+∞ª% E∞oI4
002D71C0:	68						98-1D							hE⊈∥™8Ľÿ+ESO≏∎Ħ
002D71D0:		D7		C1-F8			9A-E3							;l‡ <sup>Ľ</sup> °6.Űπα╡√&∙öï ≟lĴjF° †ÿ@Ĵ
002D71E0:		CC					C5-98			DB-2F			96	≐ ¦JjF° †ÿ@J∎∕ûēû
002D71F0:	5D						29-03			D9-8F				]∓ÇWy1»)♥ ] <sup>J</sup> Å <sub>■</sub> z <sup>⊔</sup>
002D7200:							9F-BD							×π <sup>⊥</sup> ΞόΔ∢Ĵ <sup>⊥</sup> ×000D70B2/880818_
Eigure 16, 880												ch	8Hea	ader 9 <mark>Files 10</mark> Quit ▼

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

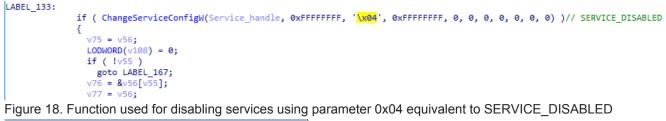




Figure 19. Unable to run an application with administrative

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 ' " <mark>accounts</mark> ": [],',0Ah
db ' "note": " Qilin\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\'
variant configuration of the Agenda ransomware

Figure 20. Allocated accounts in the Rust

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.

L	🙀 Qiin		× +						<u>s</u> x
	$\leftarrow \rightarrow$	C		a desired of the later of the second s		☆	0	х.	-
					Qilin				
				* Login					
				* Password					
					ø				
					Enter				

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. <u>Trend Micro Vision One™</u> 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