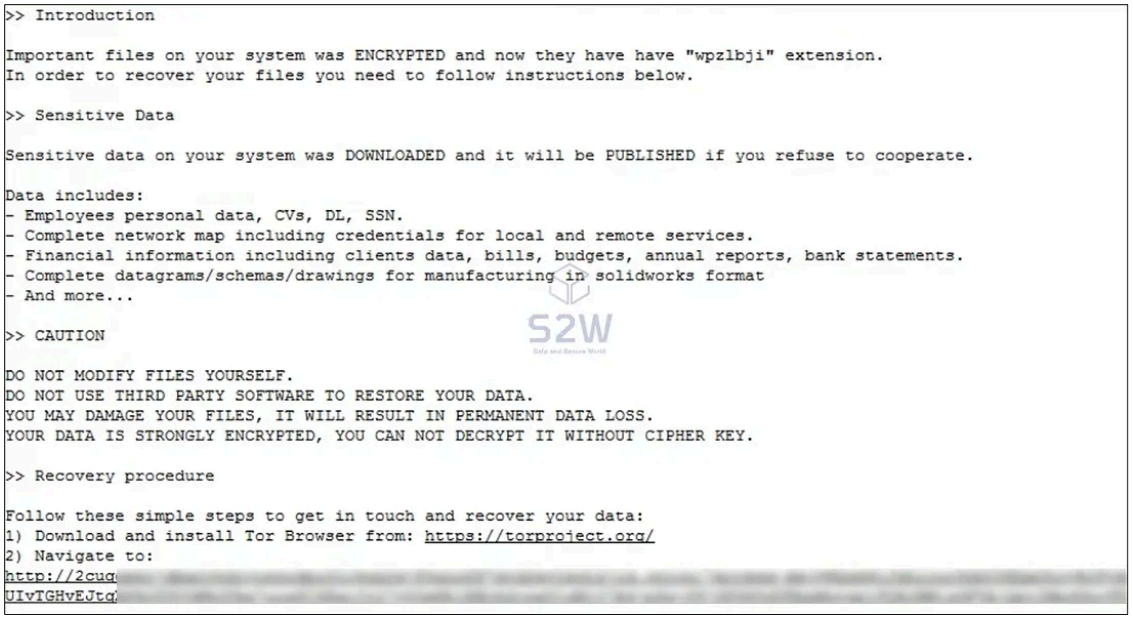
BlackCat : New Rust based ransomware borrowing BlackMatter's configuration

By S2W

Published: 2021-12-10 · Archived: 2026-04-05 23:41:24 UTC

Press enter or click to view image in full size



- Why Rust?

Rust is a multi-paradigm programming language, developed by Mozilla in 2010, which is aimed at achieving higher performance and **better safety levels** in comparison to C++. Rust has been Stack Overflow's most loved language for five years in a row. For this reason, malware developers are also probably trying to develop malware using Rust.

In fact, Rust-based MaaS(Malware-as-a-service) such as RustyBuer and FickerStealer has been appearing on the Deep and Dark web.

1.2. Borrow BlackMatter's configuration

BlackCat ransomware performs malicious actions by referring to the internal configuration like other RaaS ransomware.

Press enter or click to view image in full size

Num	Field	Description
1	config_id	configuration id
2	public_key	RSA Public key
3	extension	encrypted file extension
4	note_file_name	ransom note filename
5	note_full_text	ransom note text
6	note_short_text	short notice text
7	default_file_mode	[not yet confirmed]
8	default_file_cipher	[not yet confirmed]
9	credentials	domain credentials
10	kill_services	list of services to kill
11	kill_processes	list of processes to kill
12	exclude_directory_names	list of directories to exclude
13	exclude_file_names	list of files to exclude
14	exclude_file_extensions	list of extensions to exclude
15	exclude_file_path_wildcard	list of specific paths to exclude
16	enable_network_discovery	flag for network encryption
17	enable_self_propagation	flag for propagation
18	enable_set_wallpaper	flag for changing wallpaper
19	enable_esxi_vm_kill	[not yet confirmed]
20	enable_esxi_vm_snapshot_kill	[not yet confirmed]
21	strict_include_paths	list of specific paths to include always

However, we have confirmed the values of the following BlackCat's configuration fields completely match BlackMatter's.

- kill_services
- kill_processes
- exclude_directory_names
- exclude_file_names
- exclude_file_extensions

and the configuration field like "credentials" is also used by BlackMatter V1 and Darkside. In this field, it includes the victim's domain credentials.

1.3. Different from BlackMatter

After comparing BlackCat and BlackMatter, we found it difficult to conclude that they are the same group.

1) Too similar

When Darkside, known to be used by the FIN7 group, was rebranded to BlackMatter, it did not use the same configuration.

Press enter or click to view image in full size

Darkside

List of services to kill	vss	sql	svc$
	memtas	mepocs	sophos
	veeam	backup	GxVss
	GxBlr	GxFWD	GxCVD
	GxCliMgr		
List of processes to kill	sql	mydesktopservice	sqbcoreservice	steam
	oracle	ocautoupds	excel	thebat
	ocssd	encsvc	infopath	thunderbird
	dbsnmp	firefox	msaccess	visio
	synctime	tbirdconfig	mspub	winword
	agntsvc	mydesktopqos	onenote	wordpad
	isqlplussvc	ocomm	outlook	notepad
	xfssvccon	dbeng50	powerpnt	
List of directories to exclude	$recycle.bin	appdata	program files	windows.old	public
	config.msi	application data	program files (x86)	intel	all users
	$windows.~bt	boot	programdata	msocache	default
	$windows.~ws	google	system volume information	perflogs	
	windows	mozilla	tor browser	x64dbg	
List of files to exclude	autorun.inf	boot.ini	bootfont.bin	bootsect.bak	desktop.ini	iconcache.db
	ntldr	ntuser.dat	ntuser.dat.log	ntuser.ini	thumbs.db	
List of extensions to exclude	386	cab	deskthemepack	drv	ico	mod	msu	ps1	spl	lock
	adv	cmd	diagcab	exe	ics	mpa	nls	rom	sys	key
	ani	com	diagcfg	hlp	idx	msc	nomedia	rtp	theme	hta
	bat	cpl	diagpkg	icl	ldf	msp	ocx	scr	themepack	msi
	bin	cur	dll	icns	lnk	msstyles	prf	shs	wpx	pdb

BlackMatter

mepocs	memtas	veeam		
svc$	backup	sql		
vss	msexchange			
encsvc	thebat	mydesktopqos	xfssvccon	firefox
infopath	winword	steam	synctime	notepad
ocomm	onenote	mspub	thunderbird	agntsvc
sql	excel	powerpnt	outlook	wordpad
dbeng50	isqlplussvc	sqbcoreservice	oracle	ocautoupds
dbsnmp	msaccess	tbirdconfig	ocssd	mydesktopservice
visio				
system volume information	intel	$windows.~ws	application data	
mozilla	program files (x86)	program files	$windows.~bt	
public	msocache	windows	default	
all users	tor browser	programdata	boot	
config.msi	google	perflogs	appdata	
windows.old	$recycle.bin			
desktop.ini	autorun.inf	ntldr	bootsect.bak	
thumbs.db	boot.ini	ntuser.dat	iconcache.db	
bootfont.bin	ntuser.ini	ntuser.dat.log		
themepack	nls	diagpkg	msi	wpx
lnk	exe	cab	scr	hlp
bat	drv	rtp	msp	icns
prf	msc	ico	key	rom
ocx	diagcab	diagcfg	pdb	dll
msstyles	mod	ps1	ics	hta
bin	cmd	ani	386	lock
cur	idx	sys	com	deskthemepack
shs	ldf	theme	mpa	nomedia
spl	cpl	adv	icl	msu

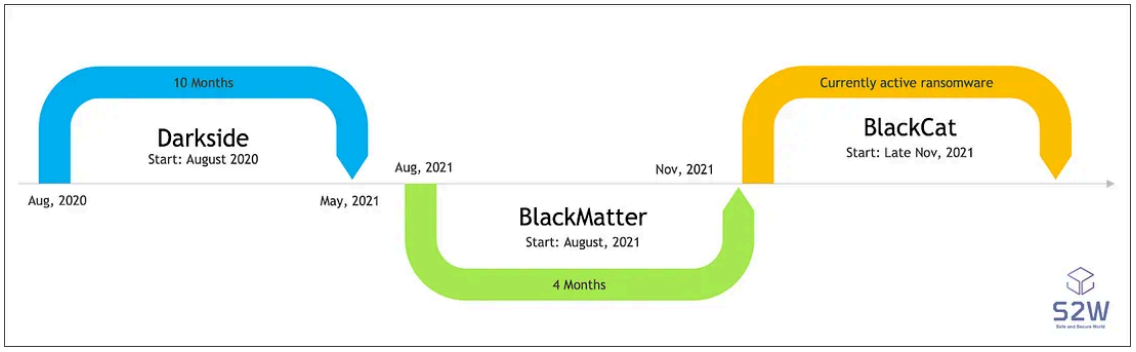
2) Based on Rust

The BlackCat ransomware is based on Rust programming language. However, both DarkSide ransomware and BlackMatter were written in C/C++.

3) Too soon

It’s too soon for BlackMatter to have rebranded as BlackCat ransomware using a different programming language, Rust.

Press enter or click to view image in full size



- Darkside: from **August 2020** to **May 2021**
- BlackMatter: from **August 2021** to **November 2021**
- BlackCat: from **Late November** (PE timestamp based)

4) Lots of execution options

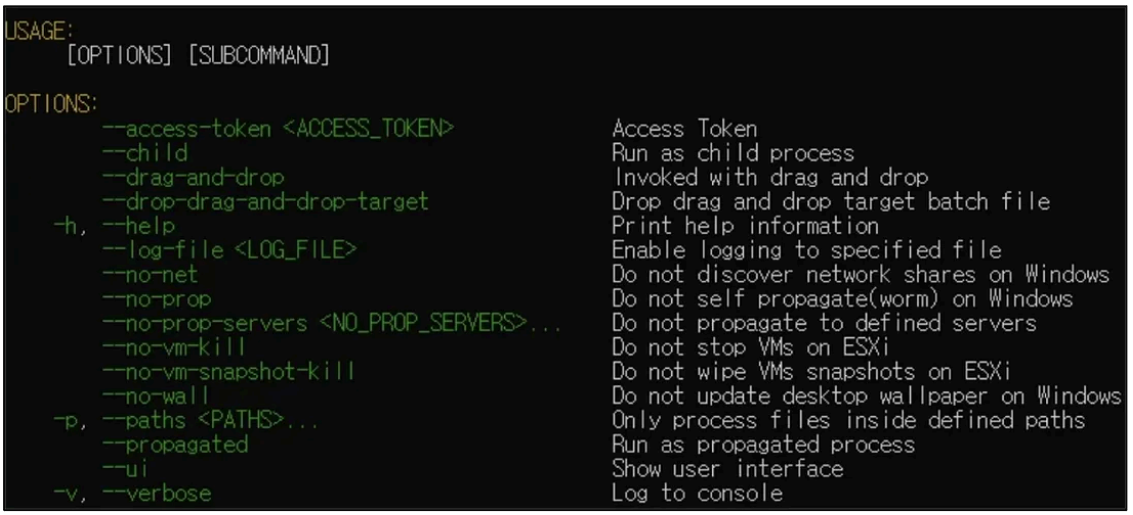
Get S2W’s stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

Unlike Darkside and BlackMatter, which used two or three options, BlackCat ransomware supports various options.

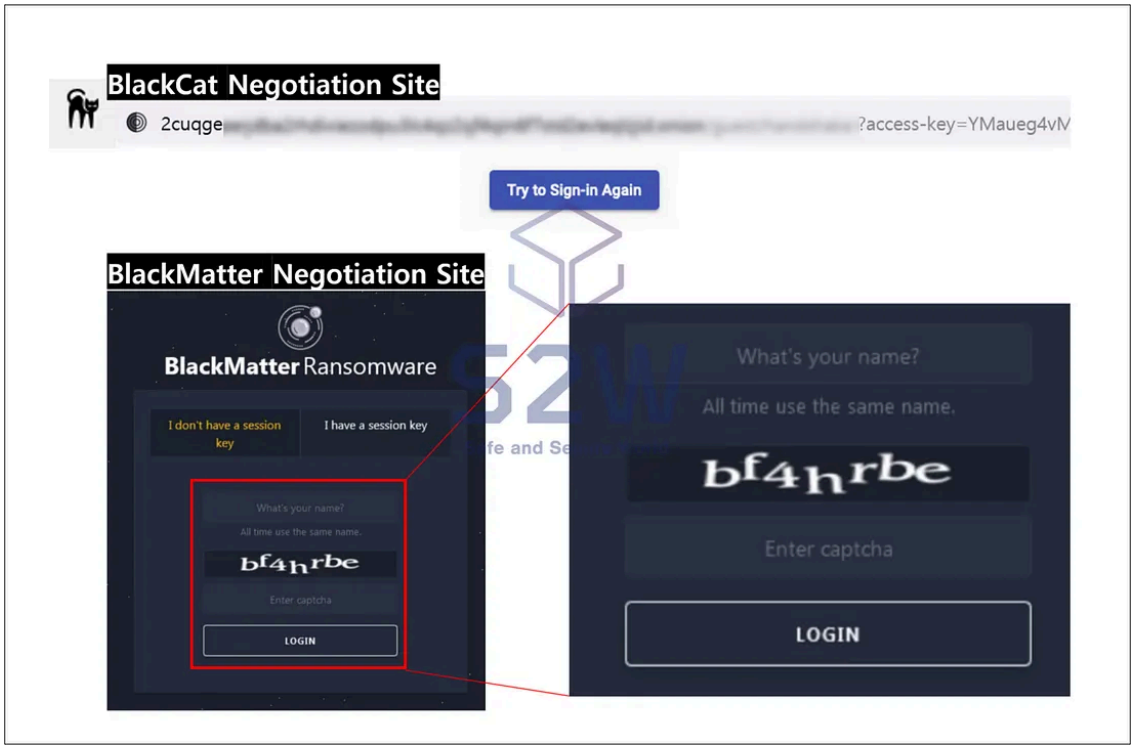
Press enter or click to view image in full size



5) Leak site

When accessing the DarkSide and BlackMatter ransomware negotiation sites, the key was needed to enter in the negotiation page, but in the case of BlackCat, the access key is used as a GET parameter and no input box is displayed on the page. In addition, BlackCat has added a private leak site, probably a pre-published leak site.

Press enter or click to view image in full size



2. The negotiation site and leak sites

Five onion domains used by BlackCat have been identified so far. They are currently categorized as the negotiation site, public leak site, private leak site, and seem to use favicons on the same site. It seems that they initially operated a private preview page, and then moved it to the Alphv leak site. (Unfortunately, private leak site was not accessible at the time)

Press enter or click to view image in full size

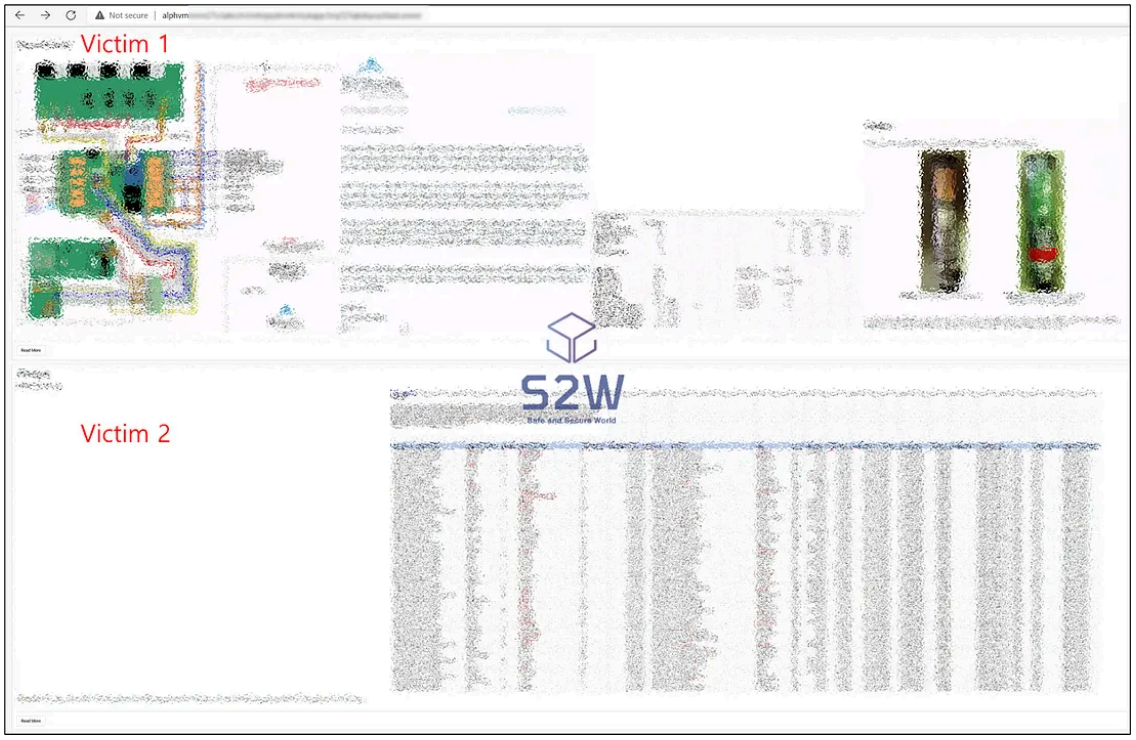
Press enter or click to view image in full size

	BlackCat negotiation site (1)	BlackCat negotiation site (2)	BlackCat negotiation site (3)	Alphv public leak site (Now)	Alphv private leak site (Past)
Domain	mu75lt*****.onion	2cuqge*****.onion	sty5r4*****.onion	alphv*****.onion	zujgzb*****.onion
Web title	(Blank)	(Blank)	(Blank)	(Blank)	*Connection unavailable*
Icon	black-cat	black-cat	black-cat	horror	

2.1. Alphv leak site

Two victims were posted on the Alphv leak site recently.

Press enter or click to view image in full size



2.2. Two victims on the Alphv leak site seems to be attacked by the BlackCat ransomware

We have confirmed that the configuration within the BlackCat ransomware contains the victim’s credentials.

Press enter or click to view image in full size

We also have confirmed that the victim was included in the filename of the BlackCat ransomware posted to the leak site during the analysis.

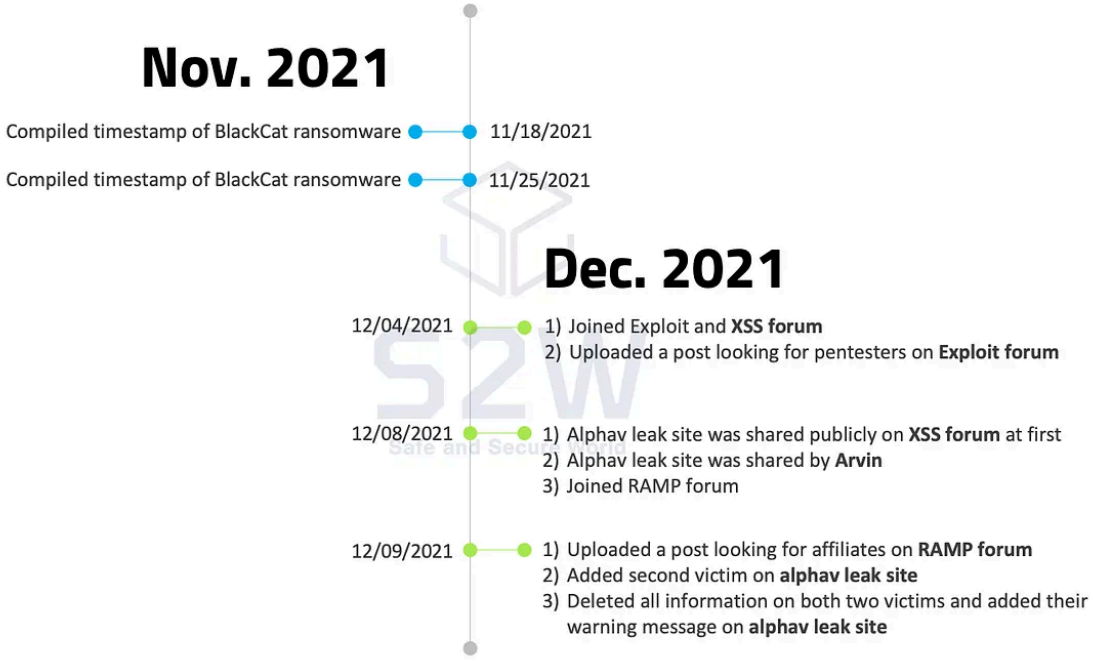
Press enter or click to view image in full size

3. Activities

We have analyzed their recent activities and it seems to have been active since November.

3.1. Timeline

Press enter or click to view image in full size



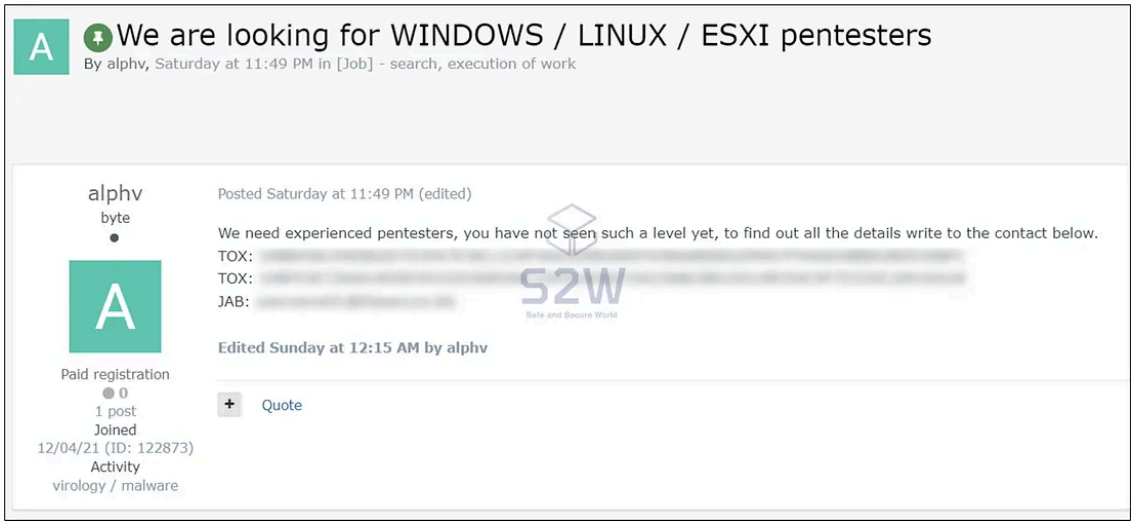
3.2. Looking for pentesters and affiliates

The BlackCat ransomware operator has been using the “alphv” as a username in XSS and Exploit, but using “ransom” as a username in RAMP forum.

[Exploit forum] We are looking for WINDOWS / LINUX / ESXI pentesters

- Posted on 12/04/2021

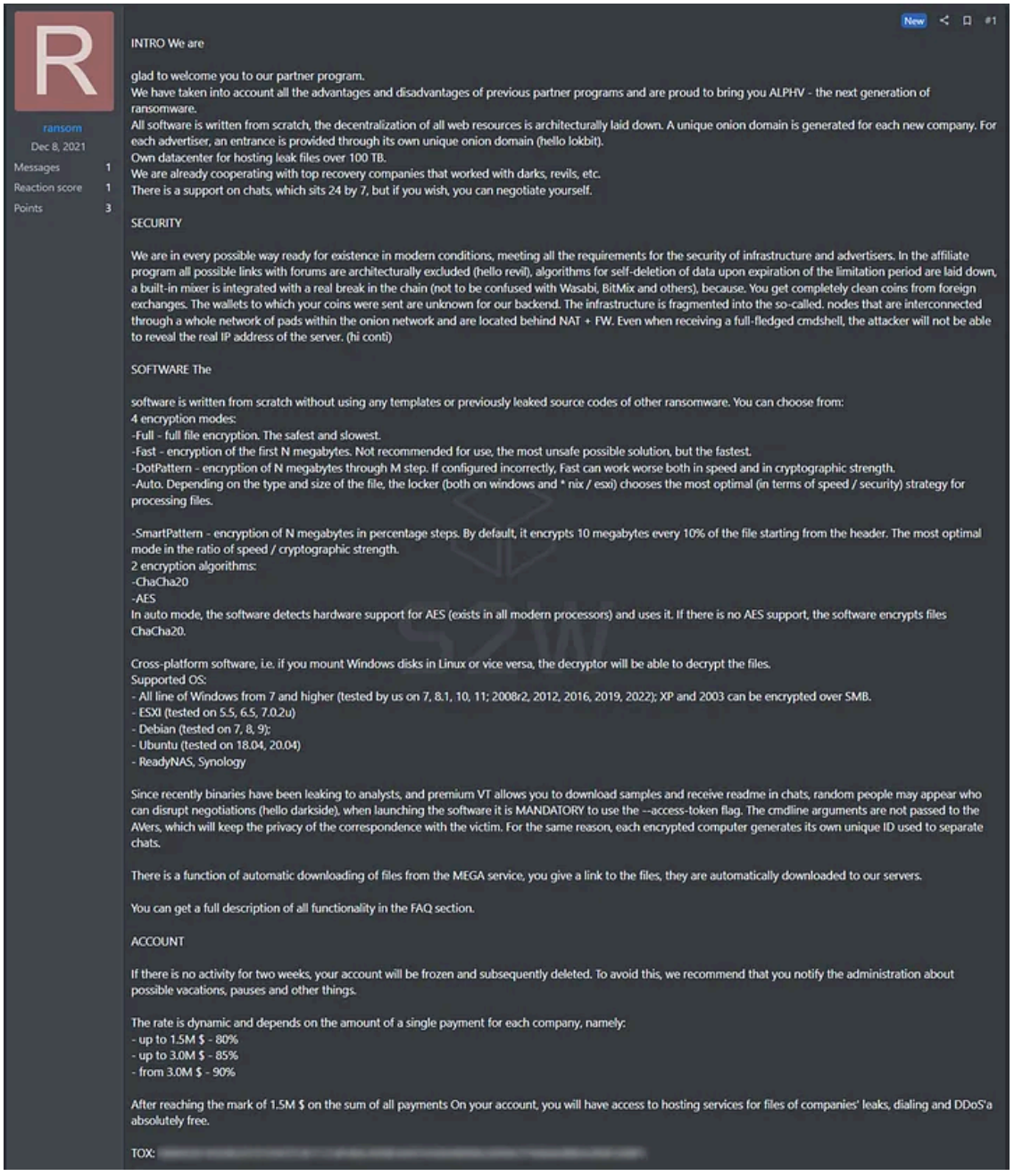
  Press enter or click to view image in full size



[RAMP forum] ALPHV-ng RaaS new generation.

- Posted on 12/09/2021

  Press enter or click to view image in full size



3.3. Warning messages posted on Alphv

- After information about the BlackCat ransomware and Alphv leak site was revealed on Twitter, they deleted all information of both two victims and added their warning message on Alphv leak site.

  Press enter or click to view image in full size

Source: https://medium.com/s2wblog/blackcat-new-rust-based-ransomware-borrowing-blackmatters-configuration-31c8d330a809