New Redeemer ransomware version promoted on hacker forums

By
Bill Toulas (https://www.bleepingcomputer.com/author/bill-toulas/)

July 21, 2022 02:38 AM **0**

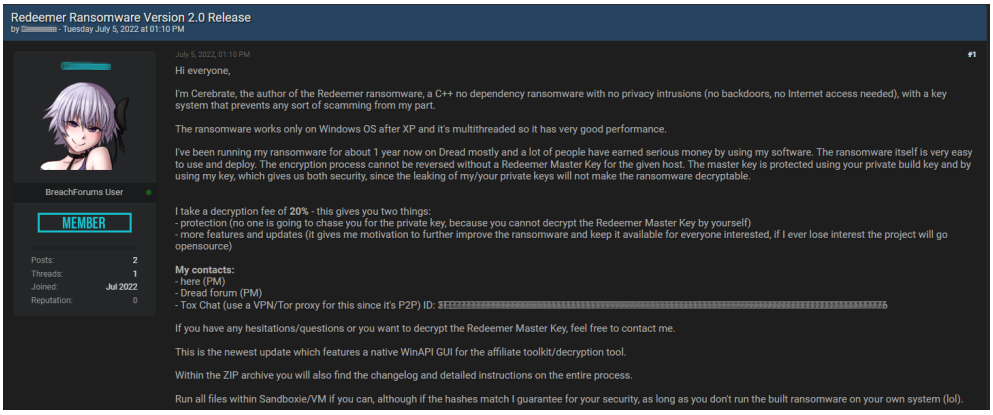
A threat actor is promoting a new version of their free-to-use 'Redeemer' ransomware builder on hacker forums, offering unskilled threat actors an easy entry to the world of encryption-backed extortion attacks.

According to its author, the new version 2.0 release was written entirely in C++ and works on Windows Vista, 7, 8, 10, and 11, featuring multi-threaded performance and a medium AV detection rate.

Unlike many Ransomware-as-a-Service (RaaS) operations, anyone can download and use the Redeemer ransomware builder to launch their own attacks. However, when a victim decides to pay the ransom, the author receives 20% of the fees and shares the master key to be combined with the private build key held by the affiliate for decryption.

Also, the new version features a new graphical user interface for the affiliate to build the ransomware executable and decryption tool, while all instructions on how to use it are enclosed in the ZIP.

The author says the project will go open-source if they lose interest, which is precisely what happened with Redeemer 1.0 back in June 2021, when the threat actor publicly released its source code.



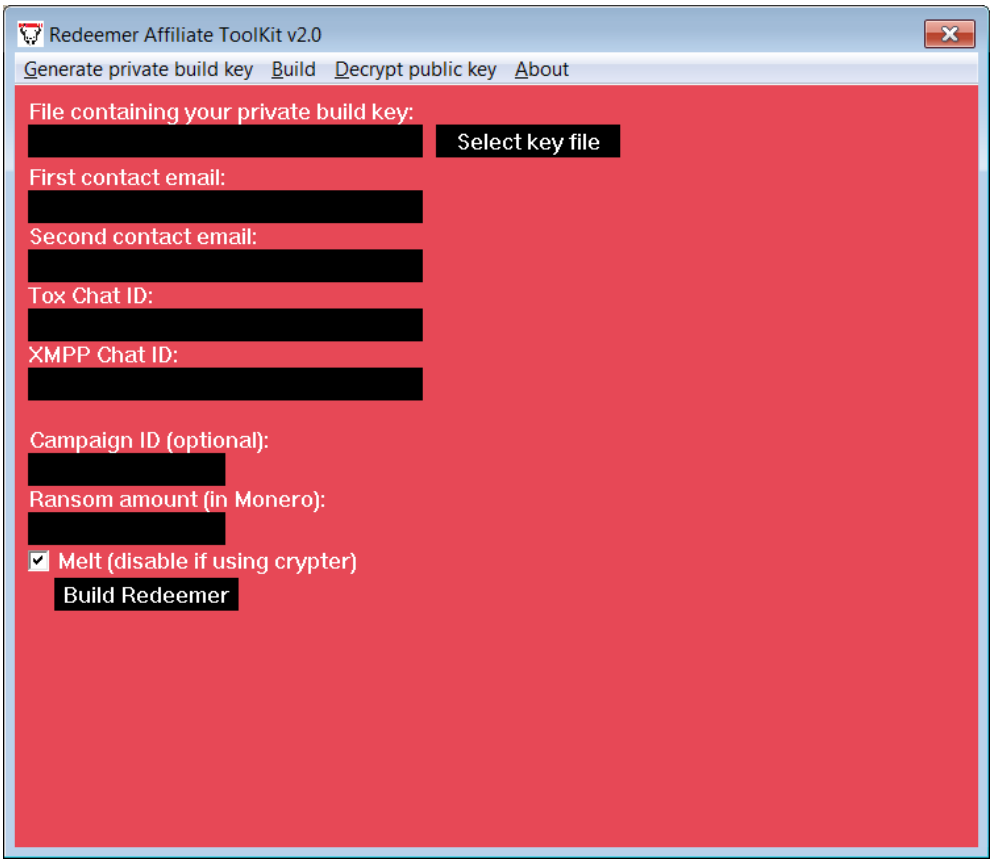
Redeemer's creator promoting the project on hacking forums

Redeemer 2.0 details

The new ransomware builder version features several additions like support for Windows 11, GUI tools, and more communication options such as XMPP and Tox Chat.

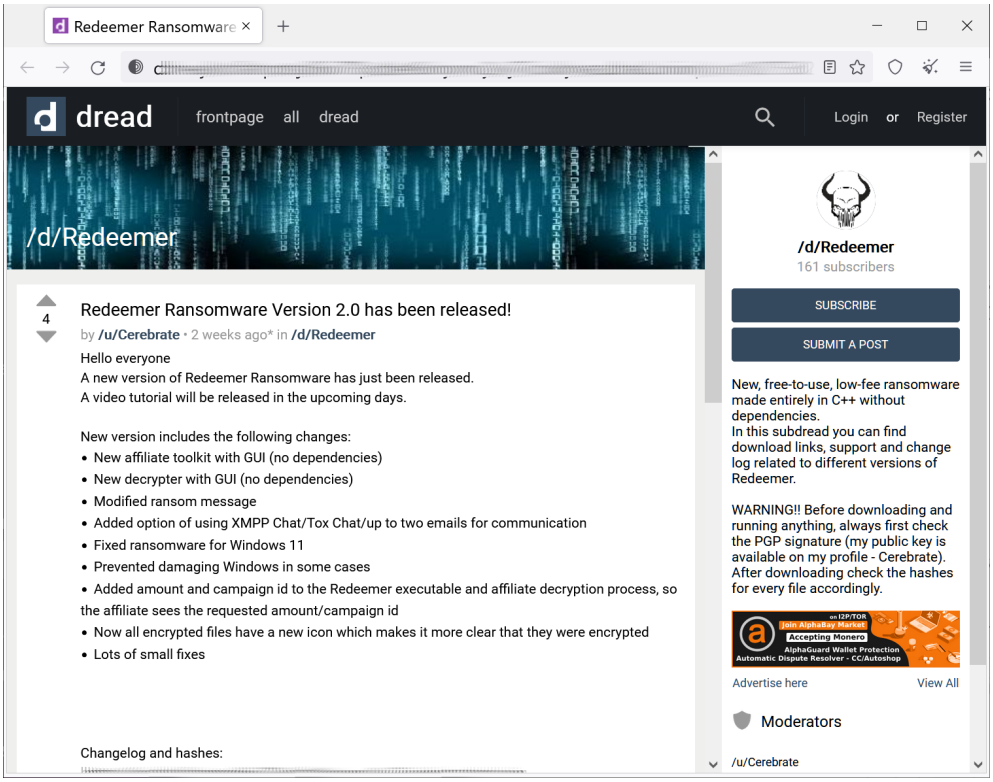
Moreover, there's now a campaign ID tracking system, adding the data into the executable, allowing threat actors to track various campaigns they may be conducting.

Because the ransom amount is set during the building of the executable and corresponds to a specific ID, the affiliate cannot make arbitrary claims to the author, so the latter's 20% cut is guaranteed.



Redeemer ransomware GUI builder
Source: BleepingComputer

The author has created a page on the dark web site Dread for the affiliates to acquire the kit, establish communication, access instructions, and receive support.



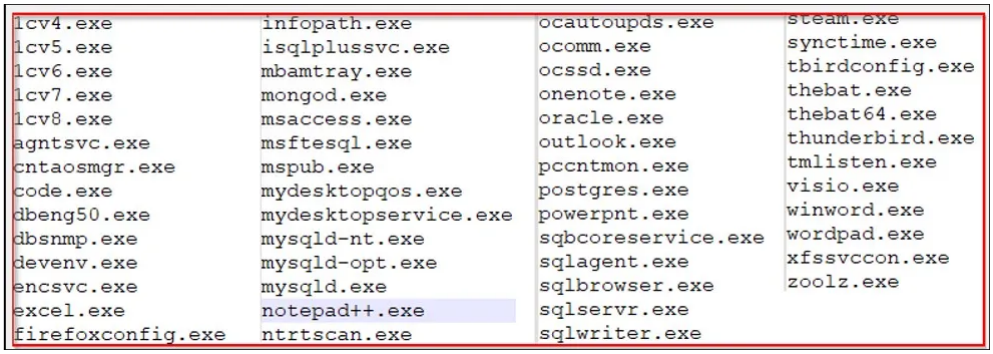
Announcement of version 2.0 on the author's Dread page

Site: BleepingComputer

Researchers at Cyble (https://blog.cyble.com/2022/07/20/redeemer-ransomware-back-action/), who have analyzed the new version, report that the ransomware creates a mutex upon launch to avoid multiple running instances on the victim's system and abuses Windows APIs to execute itself with admin privileges.

Before encryption, the malware abuses Windows commands to clear the event logs and delete shadow copies and any system state backups, preventing easy/free restoration.

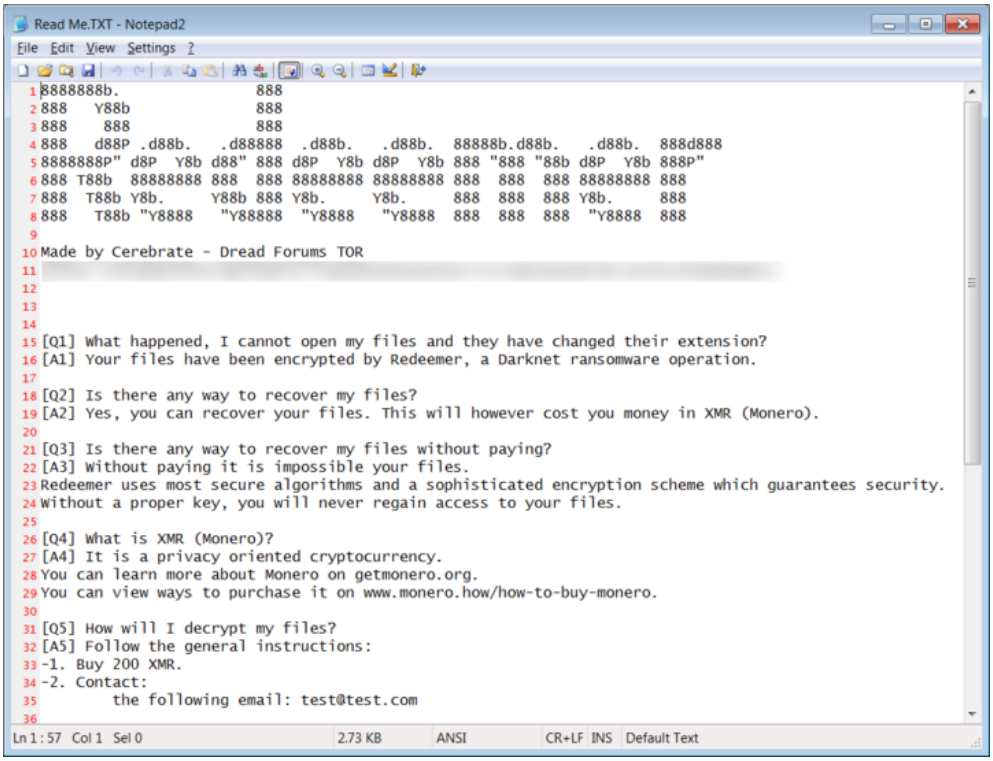
Next, the processes shown below are terminated to prevent jeopardizing the encryption process and to free up all target files and data to make them encryptable.



1cv4.exe	infopath.exe	ocautoupds.exe	steam.exe
1cv5.exe	isqlplussvc.exe	ocomm.exe	synctime.exe
1cv6.exe	mbamtray.exe	ocssd.exe	tbirdconfig.exe
1cv7.exe	mongod.exe	onenote.exe	thebat.exe
1cv8.exe	msaccess.exe	oracle.exe	thebat64.exe
agntsvc.exe	msftesql.exe	outlook.exe	thunderbird.exe
cntaosmgr.exe	mspub.exe	pccntmon.exe	tmlisten.exe
code.exe	mydesktopqos.exe	postgres.exe	visio.exe
dbeng50.exe	mydesktopservice.exe	powerpnt.exe	winword.exe
dbsnmp.exe	mysqld-nt.exe	sqbcoreservice.exe	wordpad.exe
devenv.exe	mysqld-opt.exe	sqlagent.exe	xfssvccon.exe
encsvc.exe	mysqld.exe	sqlbrowser.exe	zoolz.exe
excel.exe	notepad++.exe	sqlservr.exe	
firefoxconfig.exe	ntrtscan.exe	sqlwriter.exe	

Processes terminated prior to encryption *(Cyble)*

After that, the ransomware drops a custom icon for Windows to use for the encrypted files extension (redeem), generates the ransom notes, and enumerates all files and directories.



Read Me.TXT - Notepad2

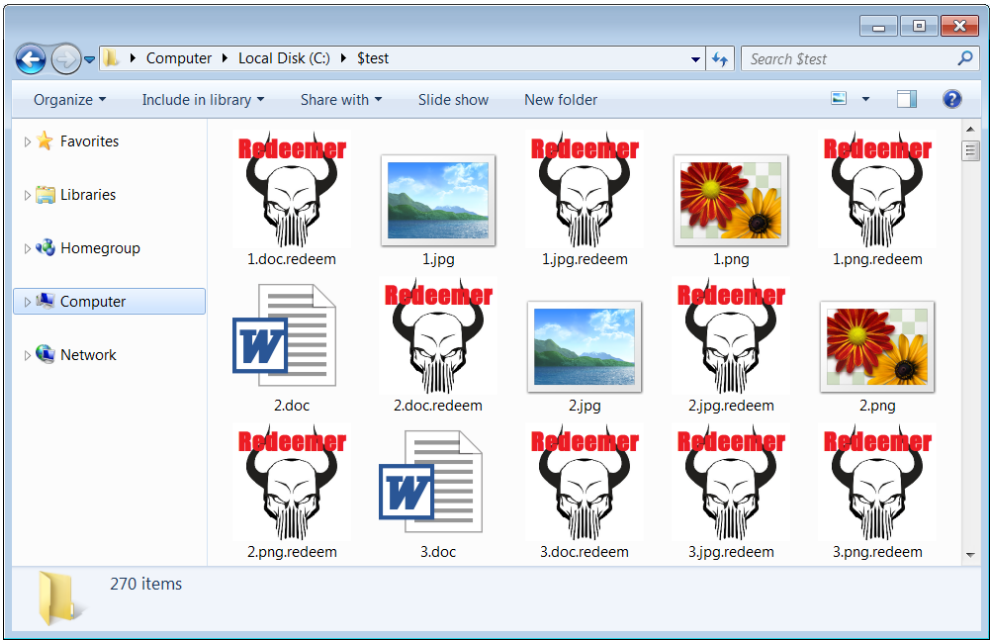
File Edit View Settings ?

```
8888888b.               888
888   Y88b              888
888    888              888
888   d88P .d88b.   .d88888  .d88b.   .d88b.  88888b.d88b.   .d88b.  888d888
8888888P" d8P  Y8b d88" 888 d8P  Y8b d8P  Y8b 888 "888 "88b d8P  Y8b 888P"
888 T88b  88888888 888  888 88888888 88888888 888  888  888 88888888 888
888  T88b Y8b.     Y88b 888 Y8b.     Y8b.     888  888  888 Y8b.     888
888   T88b "Y8888   "Y88888  "Y8888   "Y8888  888  888  888  "Y8888  888

Made by Cerebrate - Dread Forums TOR
[redacted]



[Q1] What happened, I cannot open my files and they have changed their extension?
[A1] Your files have been encrypted by Redeemer, a Darknet ransomware operation.

[Q2] Is there any way to recover my files?
[A2] Yes, you can recover your files. This will however cost you money in XMR (Monero).

[Q3] Is there any way to recover my files without paying?
[A3] Without paying it is impossible your files.
Redeemer uses most secure algorithms and a sophisticated encryption scheme which guarantees security.
Without a proper key, you will never regain access to your files.

[Q4] What is XMR (Monero)?
[A4] It is a privacy oriented cryptocurrency.
You can learn more about Monero on getmonero.org.
You can view ways to purchase it on www.monero.how/how-to-buy-monero.

[Q5] How will I decrypt my files?
[A5] Follow the general instructions:
-1. Buy 200 XMR.
-2. Contact:
        the following email: test@test.com
```

Ln 1 : 57 Col 1 Sel 0 | 2.73 KB | ANSI | CR+LF | INS | Default Text

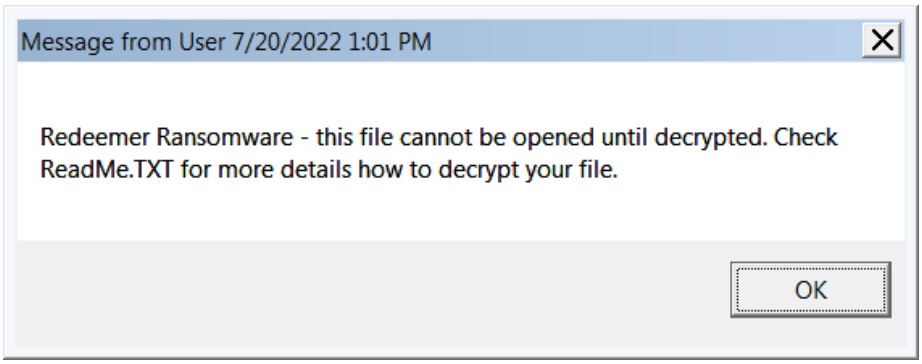
Redeemer's ransom note

Bleeping Computer tested the ransomware independently and found that it didn't delete all files after encrypting them, so its operation appears unreliable now.



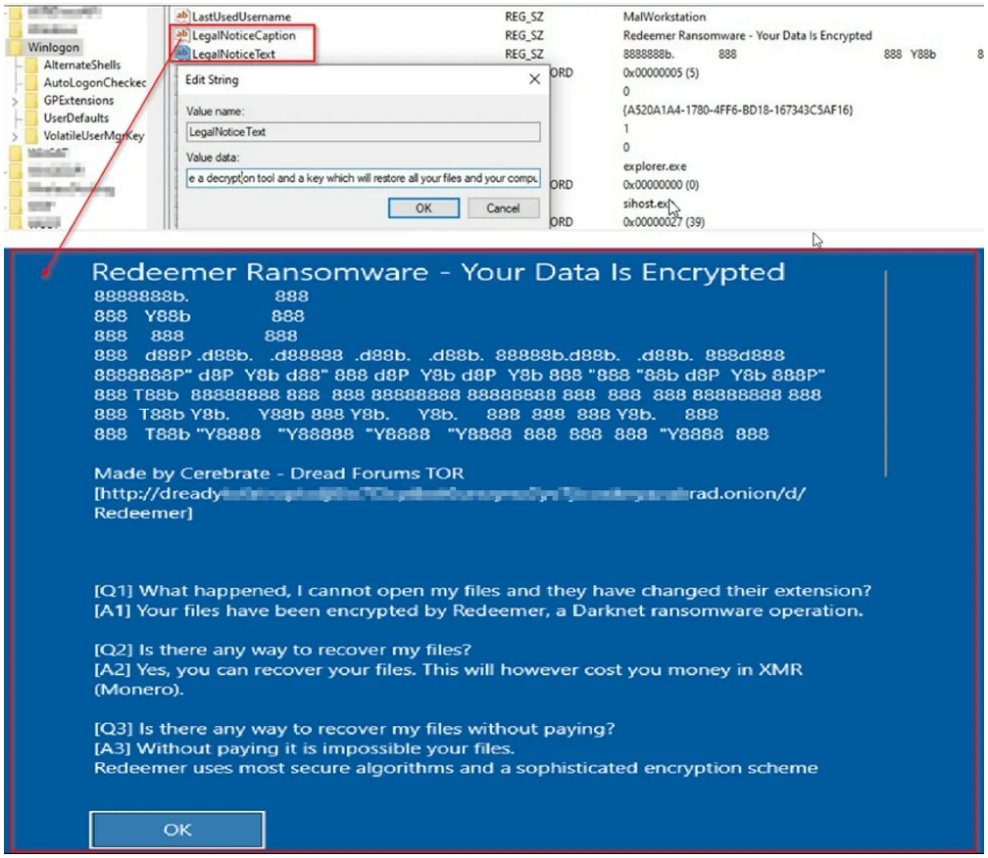
Encrypted files along with some of the originals

When attempting to open one of the encrypted copies, the victim receives a message that points them to open the ransom note for instructions on what to do.



Error message when opening encrypted file

The ransomware also adds a ransom note in the Winlogon registry key to warn the user about what has happened upon system restart.



Ransom note displayed during system restart *(Cyble)*

Should you be worried?

The problem with projects like Redeemer is that they offer a dramatically lower bar of entry to the ransomware space for many cybercriminals, including low-skilled threat actors.

While these lower-tier hackers usually lack the skills to find initial access points on valuable corporate networks, they can still cause significant damage to many vital but inadequately protected entities, like healthcare and small businesses.

However, the adoption of this new ransomware doesn't appear very high, but even if the project fails, the promise of releasing the source code creates the gloomy prospect of new projects based on the Redeemer source code.