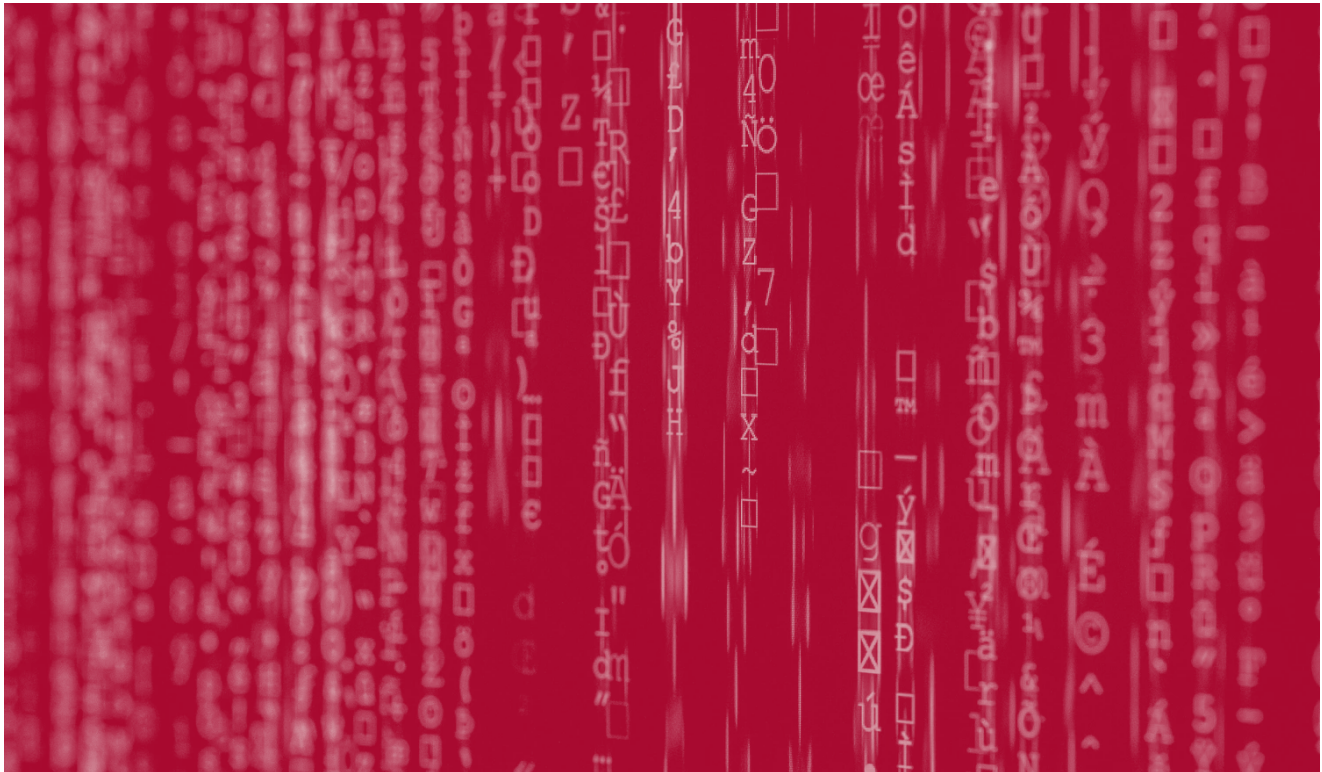


Source code for Paradise ransomware leaked on hacking forums

R. therecord.media/source-code-for-paradise-ransomware-leaked-on-hacking-forums/

June 15, 2021




The source code of the .NET version of the Paradise ransomware was leaked on hacking forums over the weekend, [Tom Malka](#), a senior threat intelligence analyst for security firm Security Joes, has told *The Record* today.

The code, which was shared on a Russian-speaking forum called XSS, represents the second major ransomware strain whose source code was leaked in recent years after the [Dharma code leaked in early 2020](#).

malware Paradise Ransomware - Source code

Суббота в 00:05 · paradise ransomware sourcecodemalware




Пользователь

Регистрация: 14.07.2020
Сообщения: 115
Реакции: 76

Суббота в 00:05 #1

Исходный код Paradise Ransomware.



Mega:

Для просмотра содержимого вам необходимо войти.

Malware.

Image: The Record

The authenticity of the leaked files was verified and confirmed by malware analysts [Bart Blaze](#) and [MalwareHunterTeam](#), which previously analyzed several Paradise ransomware campaigns.

A short history of the Paradise ransomware

First spotted in [September 2017](#), the Paradise ransomware was rented online to cybercrime gangs via a classic Ransomware-as-a-Service (RaaS) offering.

Paradise ransomware advertised as a RaaS pic.twitter.com/17hXePXnbn

— Catalin Cimpanu (@campuscodi) [September 23, 2017](#)

Threat actors would sign up for the Paradise RaaS, and they'd receive a specialized app, called a builder, which they'd use to build custom versions of the Paradise ransomware that they would later spread to victims via email spam and other methods.

While in recent years, we have gone accustomed to ransomware gangs going after high-profile companies, chasing large payments, the Paradise ransomware was primarily used to target home consumers and smaller companies.

Seeking small ransom payments, the Paradise RaaS was considered an entry point into the ransomware scene for criminal gangs, which would begin their career targeting end consumers and small businesses, and then move to the more professional RaaS offerings that targeted large corporations.

ransomware **Paradise**

All your files have been encrypted!

All your files have been encrypted due to a security problem with your pc. If you want to restore them, write us to the e-mail: info@decrypt.ws
Write this ID in the title of your message: RYfoCqiN
You have to pay for decryption in Bitcoins. The price depends on how fast you write us.
After payment we will send you the decryption tool that will decrypt all your files.

Free decryption as guarantee

Before paying you can send us up to 1 file for free decryption. The total size of file must be less than 10Mb(non archived), and file should not contain valuable information.(databases, backups, large excel sheets, etc.)

How to obtain Bitcoins

The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy Bitcoins', and select the seller by payment method and price.

https://localbitcoins.com/buy_bitcoins

Also you can find other places to buy Bitcoins and beginners guide here:

<http://www.coindesk.com/information/how-can-i-buy-bitcoins/>

Attention!

Do not rename encrypted files

Do not try to decrypt your data using third party software, it may cause permanent data loss

If you not write on e-mail in 36 hours - your key has been deleted and you cant decrypt your files

Image: [Andrey Ivanov](#)

The Paradise RaaS operated for years, constantly releasing new versions, including a .NET version, which saw limited use in 2019 and 2020.

The RaaS hit its first major snag in October 2019 when security firm [Emsisoft released a free decryption utility](#) that allowed victims to decrypt files encrypted by the Paradise ransomware without paying the ransom demand.

The Paradise operators released new versions, but security firm [Bitdefender released a second decrypter](#) a few months later, in January 2020.

Since then, the RaaS' operations have lost some of their stamina, with fewer campaigns being spotted by security researchers on a weekly basis.

One of the Paradise affiliates drew some attention to itself in March 2020 when they utilized a [novel spam campaign](#) that used IQY files to spread the ransomware, but since then, Paradise payloads have been rare, with the last public sample being seen in January this year.

[#Paradise](#) [#Ransomware](#)

mail:

[\[email protected\]](#)

[\[email protected\]](#)

ext:Cukiesi

sample:https://t.co/9ltw4clA85@Amigo_A_@demonslay335

pic.twitter.com/wBEC30GPbG

— xiaopao (@Kangxiaopao) [January 29, 2021](#)

Security firm SonicWall also reported spotting a new ransomware version named Cukiesi, which they concluded was an offshoot of the old Paradise, but this variant didn't survive for long either.

Today, the native version of the Paradise ransomware is still making a handful of victims on a weekly basis. According to MalwareHunterTeam, the ID-Ransomware service has only seen two submissions in the last 30 days, suggesting the project has been abandoned or is seeing lesser use in favor of its native version – with natively-coded ransomware being known to be faster at encrypting files compared to .NET alternatives.

Paradise ransomware builder leaked

The Paradise code that was leaked over the weekend is the source code for the .NET version of the Paradise ransomware, and more precisely for its builder and decryption utility, Malka and Blaze told *The Record* today.

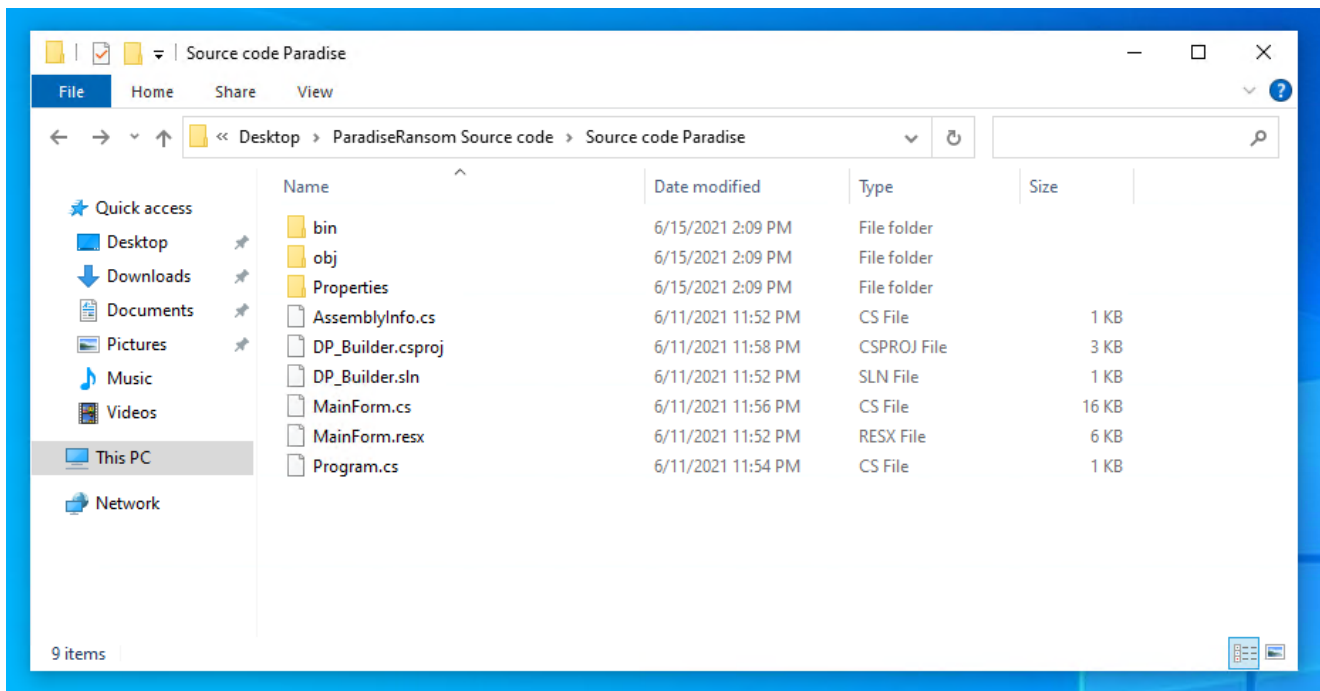


Image: The Record

Source code Paradise > bin > Debug > 4 build myid [test@therecord.media]

Name	Type	Size
DP_Main.exe	Application	28 KB
DP_Keygen.exe	Application	10 KB
DP_Decrypter.exe	Application	13 KB

Image: Bart Blaze (supplied)

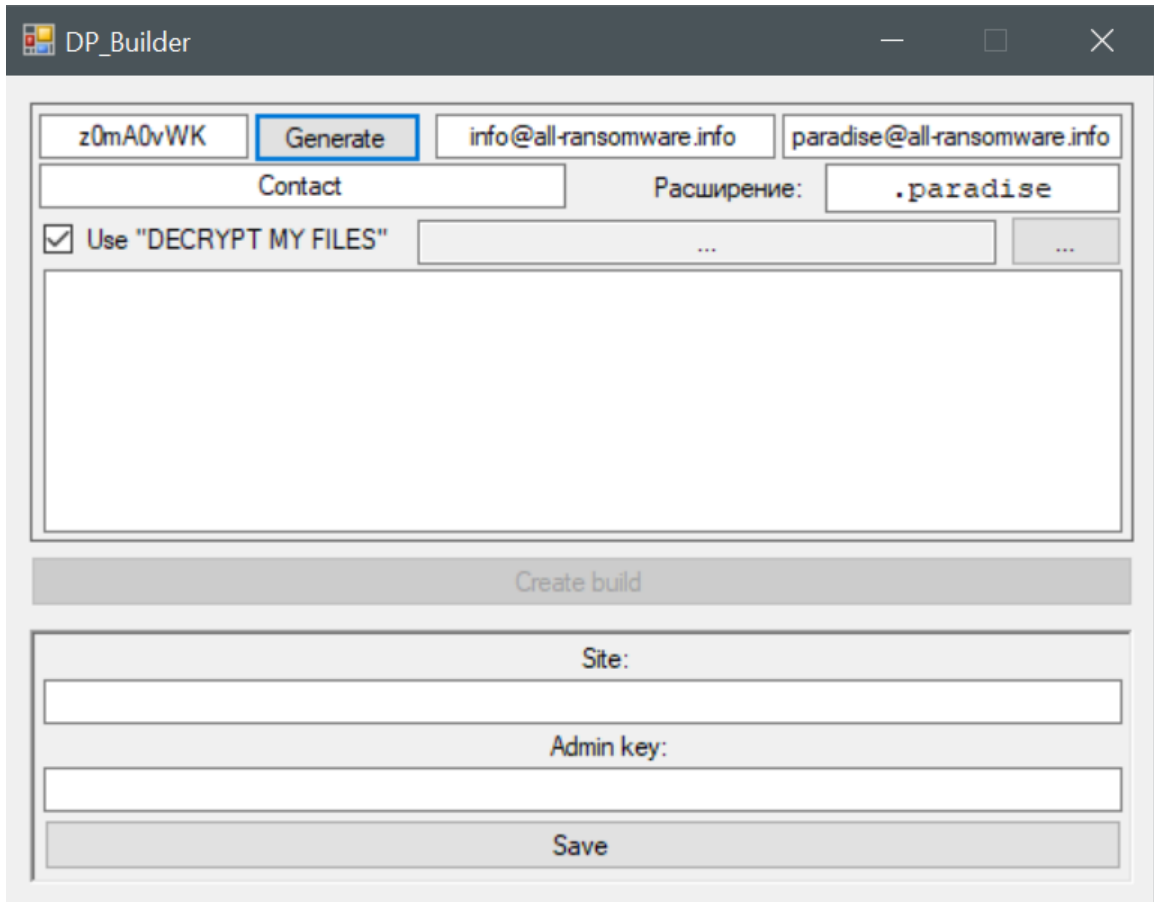


Image:

Bart Blaze (supplied)

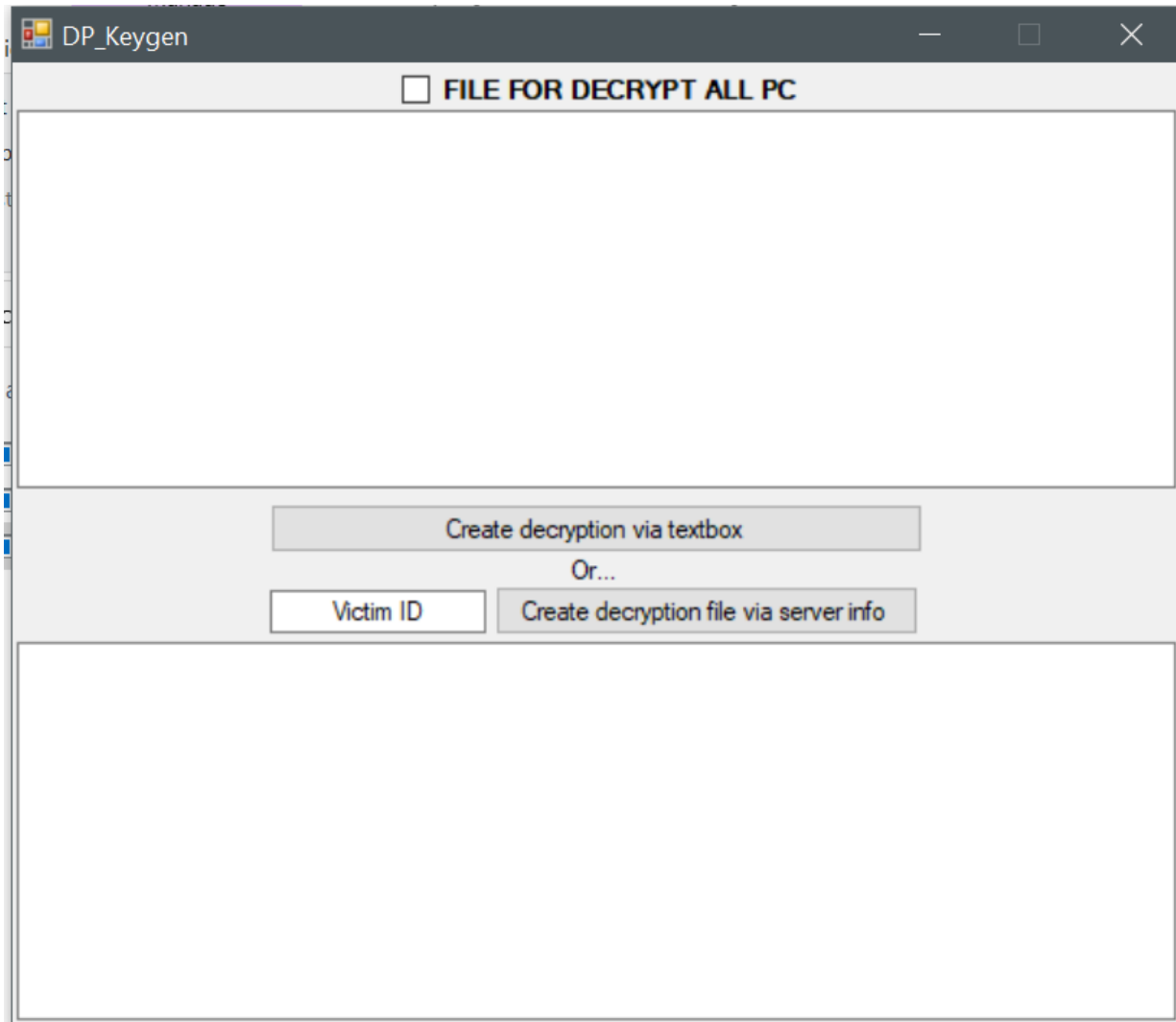


Image: Bart Blaze (supplied)

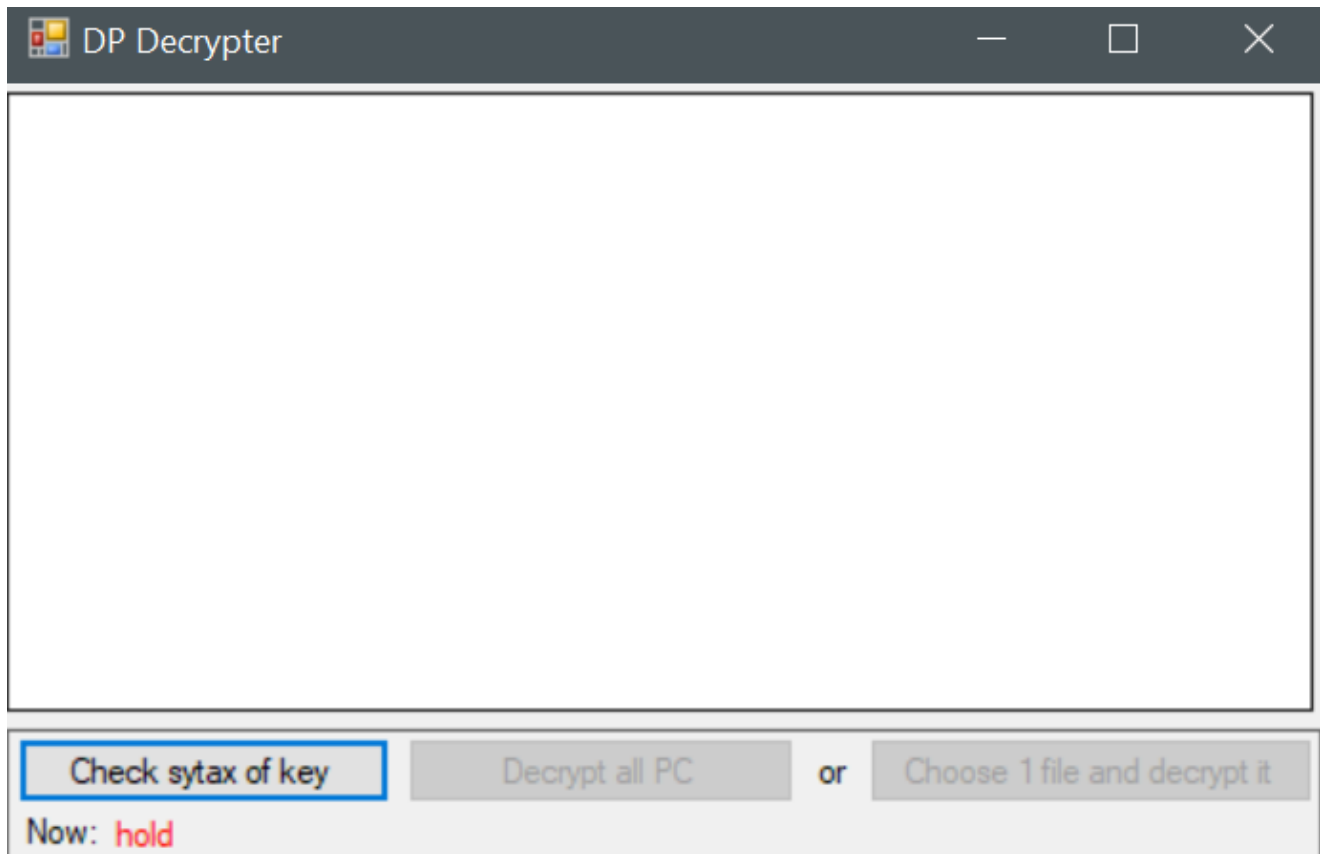


Image: Bart Blaze (supplied)

The leak of the Paradise ransomware builder is a legitimate cause for concern, even if it's for the lesser-used .NET version.

Sample Paradise ransomware strains built by Blaze earlier today were classified as undecryptable when uploaded and verified via the ID-Ransomware service.

With the source code readily available in the public domain, and known to be undecryptable, we cannot exclude that some threat actors will jump on the opportunity to use it, even if it's not as refined as the native version of the Paradise RaaS.

Tags

- [hacking forum](#)
- [leak](#)
- [malware](#)
- [Paradise](#)
- [RaaS](#)
- [Ransomware](#)
- [source code](#)
- [XSS](#)

Catalin Cimpanu is a cybersecurity reporter for The Record. He previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.