**09 2021**
**TLP: WHITE**

# Dharma/Crysis:

## Overview and adversary tracking

09/2021 - Cyber Intelligence Unit

# Contents

# Executive Summary

This report presents an overview about Dharma/Crysis ransomware. This piece of malware is often observed as late-stage payload in attacks against internet-facing systems, such as RDP. The initial intrusions usually take place via existing vulnerabilities or stolen legitimate credentials. C25 Intelligence finally reports from where Dharma variants have been operated during 2020 and how to defend against this threat.

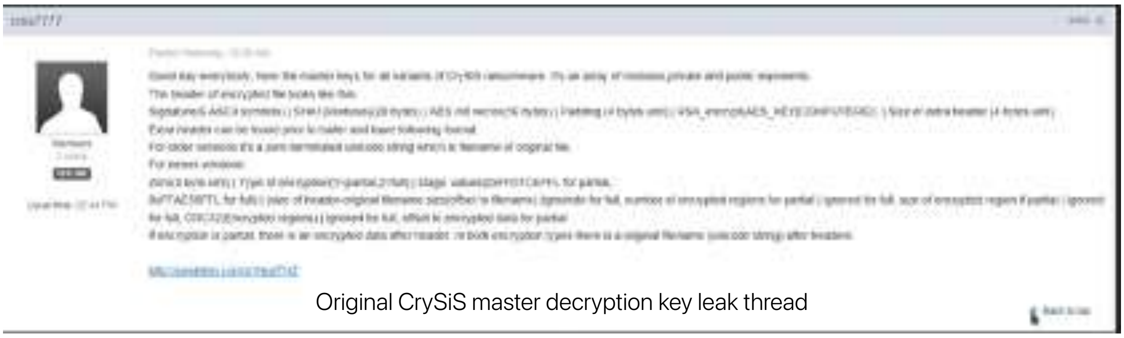
## 01 What is dharma/crysis ransomware

Dharma, a family of ransomware first spotted in 2016, is a malicious program that encrypts a victim's files and takes as hostage the data on demand for the ransom payment to restore the data back. It belongs to a fairly widespread ransomware family that has been successful over time, especially due to the many variants related to it and the fact that it has often represented the basis for R-a-a-S (Ransomware-as-a-Service) programs.

The R-a-a-S Dharma model is often adopted by novice cybercriminals looking for something immediate and easy to use. Indeed, threat actors using this R-a-a-S are equipped with a matrix of predefined scripts and tools that require little skill to work. This toolset greatly increases the attractiveness of this solution for those at the entry-level in ransomware operations. Today we can define Dharma as the basis for Ransomware-as-a-Service (RaaS); it has become one of the most profitable and easy to deploy ransomware especially for those who are new to ransomware attacks.

## 02 Who are they?

Dharma was operated by a cyber gang who managed to remain mostly in the shadows to this day. At the beginning CrySiS (the originator of Dharma) was offered as a R-a-a-S (Ransomware-as-a-Service) meaning that "clients" could use it if they purchased a license from the coders. This means that those who purchase the malware carry out the actual attacks rather than original creators. After the master decryption key leak of CrySiS in November 2016, its R-a-a-S model has been relaunched under the name of Dharma two weeks later.



Good day everybody, here the master keys for all variants of CrySiS ransomware. It's an array of [illegible] private and public exponents.
The header of encrypted file looks like this:
[illegible]
Extra headers can be found prior to header and have following format:
For older versions it's a zero terminated unicode string which is filename of original file.
For newer versions:
[illegible]
[illegible]
[illegible]
If encryption is partial, there is an encrypted data after header. In both encryption types there is a original filename (unicode string) after headers.

[illegible]

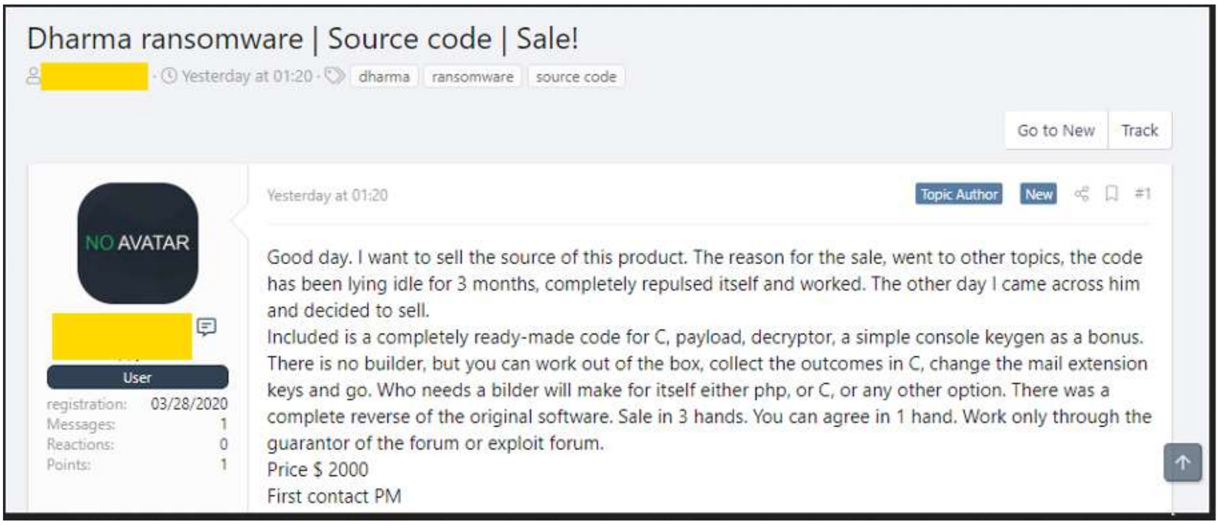
Original CrySiS master decryption key leak thread

Since then, the malware developers have released a constant flow of new Dharma variants utilizing many differently named extensions. The FBI has ranked Dharma the second most lucrative ransomware operation in recent years.

C25 Intelligence traces the origin of the first CrySiS variants to Ukraine, a country in which it places its original developers with high confidence. Dharma, instead, is not centrally administrated and its variants come from different sources. In 2020, for example, C25 Intelligence observed variants to be controlled from the following cities/Countries:

[+] Johannesburg, South Africa
[+] Tel Aviv, Israel
[+] Ahvaz, Iran
[+] Tabriz, Iran
[+] Kazan, Russia
[+] Kiev, Ukraine

In March 2020 the source code for ransomware-as-a-service (RaaS) strain of Dharma was observed being put for sale on a top-tier deep web forum for 2,000 USD.



Dharma ransomware | Source code | Sale!

[redacted] · Yesterday at 01:20 · dharma ransomware source code

[redacted]

User

registration: 03/28/2020
Messages: 1
Reactions: 0
Points: 1

Yesterday at 01:20 Topic Author New #1

Good day. I want to sell the source of this product. The reason for the sale, went to other topics, the code has been lying idle for 3 months, completely repulsed itself and worked. The other day I came across him and decided to sell.
Included is a completely ready-made code for C, payload, decryptor, a simple console keygen as a bonus. There is no builder, but you can work out of the box, collect the outcomes in C, change the mail extension keys and go. Who needs a bilder will make for itself either php, or C, or any other option. There was a complete reverse of the original software. Sale in 3 hands. You can agree in 1 hand. Work only through the guarantor of the forum or exploit forum.
Price $ 2000
First contact PM

# 03 Who do they target?

Victimology of Dharma ransomware does not differ much from distinct Ransomware as a Service (RaaS) gangs, Dharma ransomware affiliates do not appear to discriminate among industries.

Victims have been identified in the following sectors:

Academic
Automotive
Energy
Extractive
Financial Services
Government
Healthcare
Hospitality
Legal
Logistics
Manufacturing
Media
Retail
Technology
Telecommunications
Transportation

These intrusions have shown consistent techniques that include gaining initial access over Remote Desktop Protocol (RDP), brute forcing or password spraying, using publicly available utilities to attempt to identify and uninstall security software, harvesting credentials and mapping network shares.

## 04 Kill-chain

Cluster25 managed to map all the infection chain used by Dharma Ransomware affiliates. Dharma Ransomware targets Windows systems, and this family primarily targets businesses. It uses several methods of distribution:

- Dharma Ransomware is distributed as malicious attachments in spam emails.

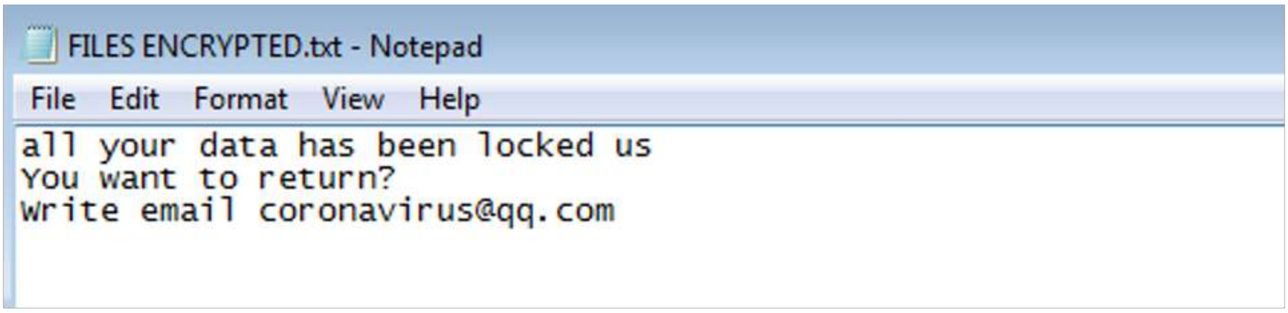
- Dharma Ransomware can also arrive disguised as installation files for legitimate software, including AV vendors. Dharma operators will offer up these harmless looking installers for various legitimate applications as downloadable executables, which they have been distributing through various online locations and shared networks.

- Most of the time, Dharma Ransomware is delivered manually in targeted attacks by exploiting leaked or weak RDP credentials. This means an attacker is accessing the victim machines prior to the infection by brute-forcing the Windows RDP protocol on port 3389 or by RDP credentials acquired in dark / deep web channels.

Dharma does not stop the affected system from working properly after the encryption is finished, but every time a file is added to the targeted directories, it will be encrypted unless the Dharma Ransomware infection is removed. Once the Ransomware has completed the encryption routing it drops a ransomware note on the desktop of the victim providing usually 2 email addresses which the victim can use to contact the threat actor in order to pay the ransom.

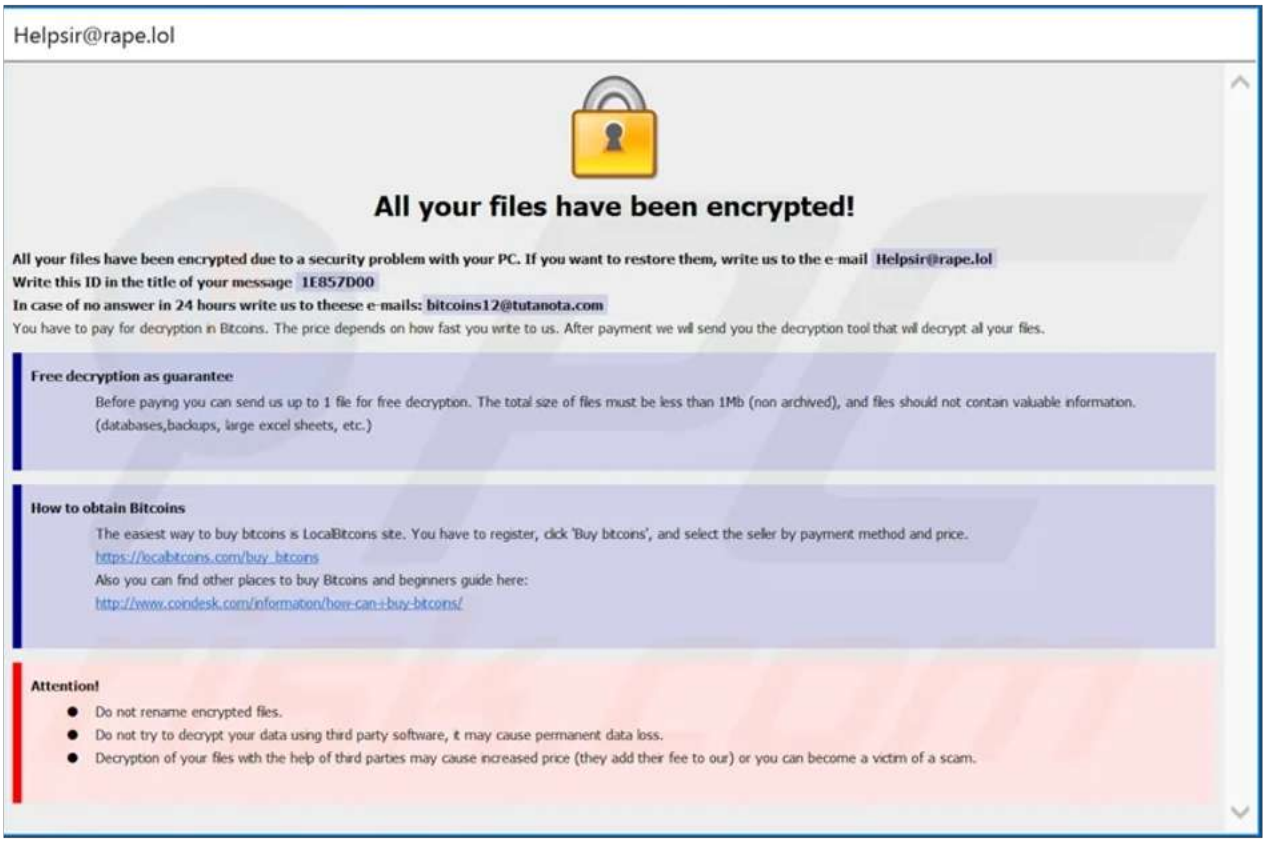
Dharma encrypts user data with **AES-256** (CBC mode) or **DES + RSA**. The file decryption key, along with random bytes, is encrypted using the **RSA-1024** algorithm and stored at the end of the encrypted file. On other malicious sample that we have analyzed some ransomware notes contain only one email address. The ransomware can be different in relation to variants and affiliates.

Some of them will not have a ransom note. During the outbreak of coronavirus pandemic, we have seen that also Dharma Ransomware took part into this cybercrime ecosystem pushing their malicious payload into tricking the victims to download harmless looking installers for various legitimate applications to watch for Coronavirus infection



```
all your data has been locked us
You want to return?
write email coronavirus@qq.com
```

Another example of the ransomware note that the victims see on their desktop once they are infected/ encrypted are shown below from .lol and .biden variants:



**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 Helpsir@rape.lol**

**Write this ID in the title of your message 1E857D00**

**In case of no answer in 24 hours write us to theese e-mails: bitcoins12@tutanota.com**

You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the decryption tool that will decrypt all your files.

**Free decryption as guarantee**

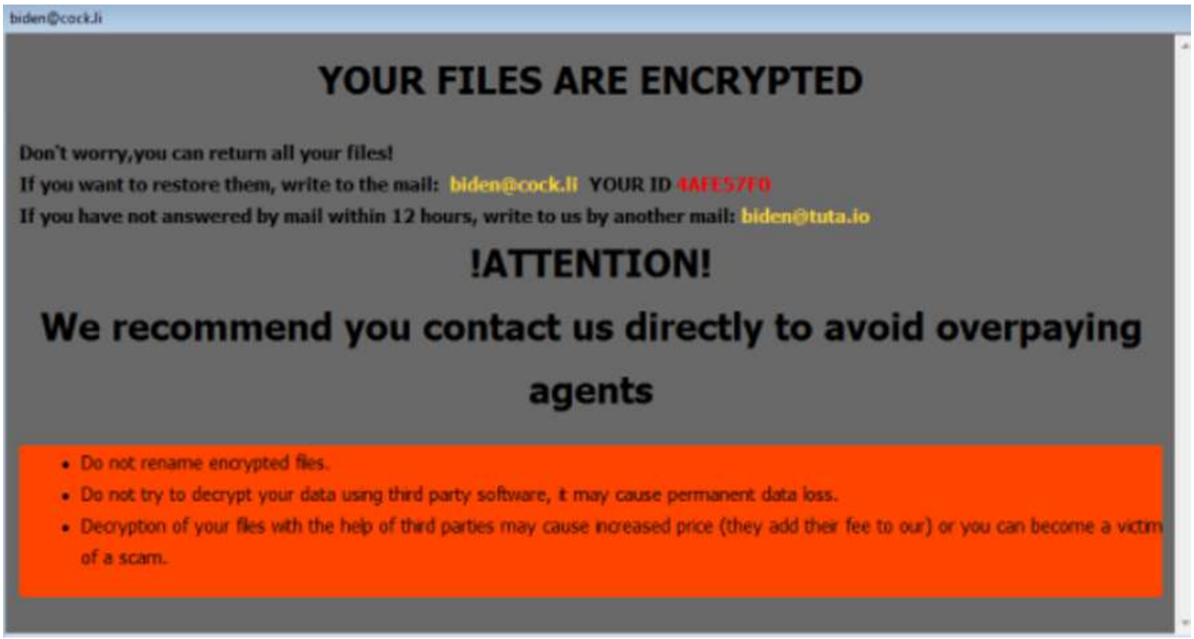
Before paying you can send us up to 1 file for free decryption. The total size of files must be less than 1Mb (non archived), and files should not contain valuable information. (databases,backups, large excel sheets, etc.)

**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.
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.



biden@cock.li

YOUR FILES ARE ENCRYPTED

Don't worry,you can return all your files!
If you want to restore them, write to the mail: biden@cock.li YOUR ID 4AFE57F0
If you have not answered by mail within 12 hours, write to us by another mail: biden@tuta.io

!ATTENTION!

We recommend you contact us directly to avoid overpaying agents

- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, it may cause permanent data loss.
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

## 05 Att&ck Matrix

| TACTICS | TECHNIQUES | DESCRIPTION |
|---|---|---|
| Initial Access | T1133<br>T1078 | External Remote Services<br>Valid Accounts |
| Persistence | T1133<br>T1108<br>T1078 | External Remote Services<br>Redundant Access<br>Valid Accounts |
| Privilege Escalation | T1078 | Valid Accounts |
| Defense Evasion | T1108<br>T1078 | Redundant Access<br>Valid Accounts |
| Discovery | T1046 | Network Share Discovery |
| Lateral Movement | T1076<br>T1077 | Remote Desktop Protocol<br>Windows Admin Shares |
| Command and Control | T1043<br>T1065<br>T1008 | Commonly Used Ports<br>Uncommonly Used Port<br>Fallback Channels |
| Exfiltration | T1048 | Exfiltration Over Alternative Protocol |

# About Cluster25

Cluster25 is a Cyber Intelligence Research an Adversary Hunting Unit. Cluster25 experts are specialized in hunting and collecting cyber threats, analysis, reverse-engineering and adversary hunting practices.

Cluster25 internally develops technologies and capabilities for classification and categorization of malicious artifacts often before being used in real operations.

Visit us at **cluster25.io**

Given the inherent nature of threat intelligence, the content contained in this report is based on information gathered and understood at the time of its creation. The information in this report is general in nature and does not take into account the specific needs of your IT ecosystem and network, which may vary and require unique action. As such, Cluster25 provides the information and content on an "as-is" basis without representation or warranty and accepts no liability for any action or failure to act taken in response to the information contained or referenced in this report. The reader is responsible for determining whether or not to follow any of the suggestions, recommendations or potential mitigations set out in this report, entirely at their own discretion.