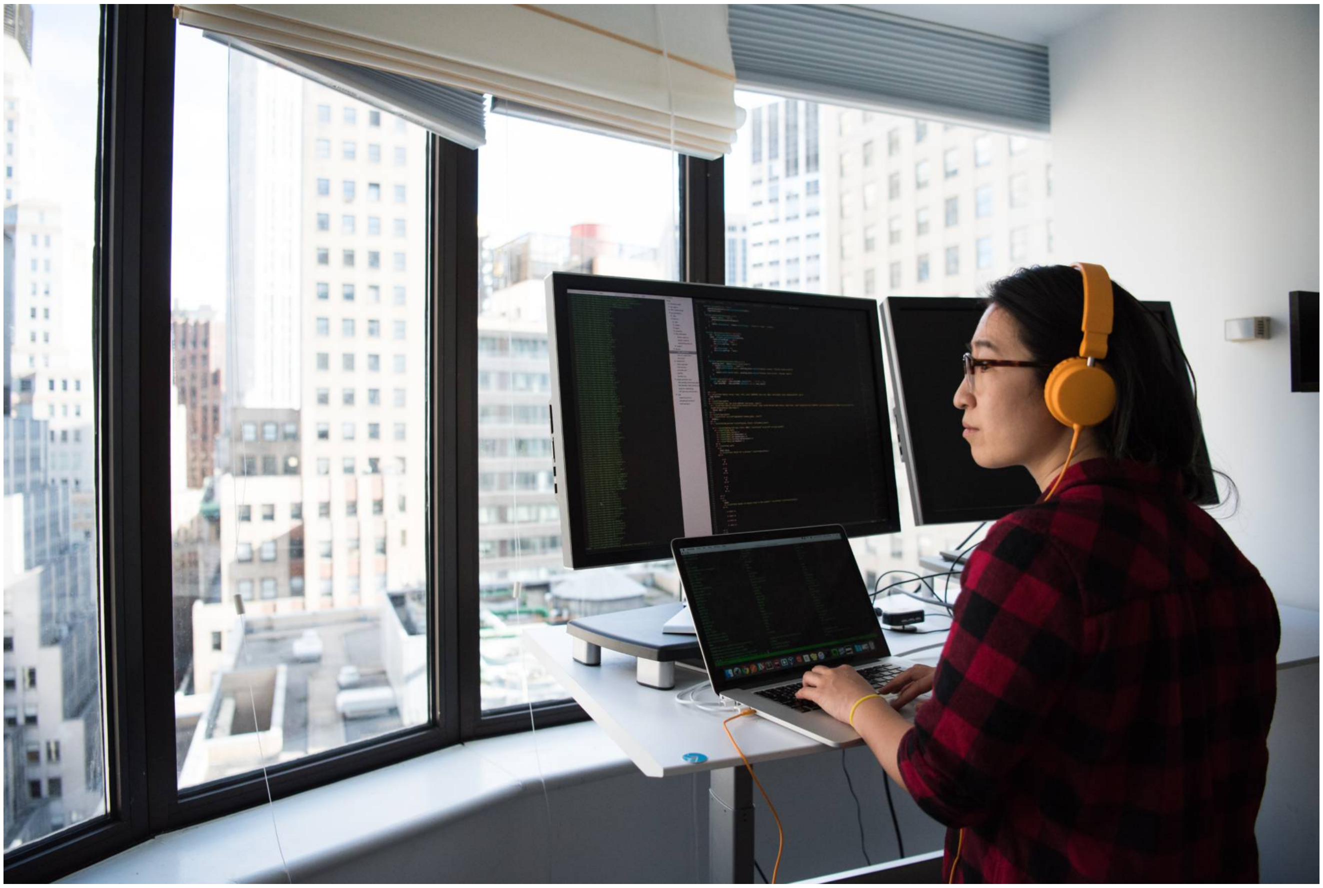
Analysis of NoCry: A variant of the Judge ransomware

tesorion.nl/en/posts/analysis-of-nocry-a-variant-of-the-judge-ransomware/

By Gijs Rijnders

May 16, 2021



In January this year, we published a blog post on our analysis of the Judge ransomware. We announced a free decryptor for Judge victims in this blog post, which is available through the NoMoreRansom initiative. Our decryptor has been helping victims to recover their files for free since its release.

After a few months, BleepingComputer wrote about a new variant of the Stupid ransomware, called NoCry. This variant was found by GrujaRS. When we first analyzed the Judge ransomware, we also found the alias: NoCry in the binary. As such, we went ahead to analyze NoCry and determined that it is a variant of Judge as well.

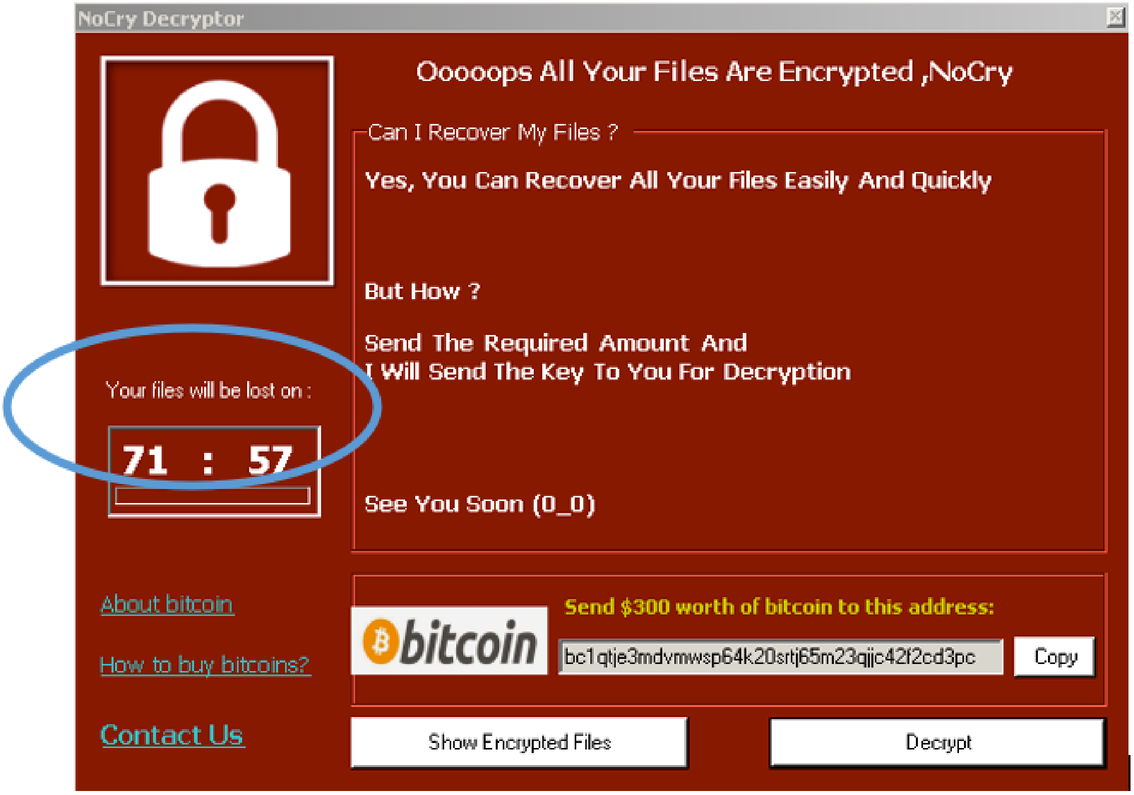
Fortunately, our decryptor for Judge also decrypts files encrypted by the NoCry/Stupid ransomware. In this blog post, we discuss some differences between Judge and NoCry. Furthermore, we confirm that our decryptor also decrypts files affected by NoCry.

Overview

The NoCry ransomware we analyzed is very similar to Judge, the one we previously looked at. It creates a mutex to prevent multiple instances from running in parallel, provides sandbox detection and deletes system restore points. When those tasks are completed, the ransomware starts encrypting the victim's files. The file encryption process is the same, and therefore, our decryptor can also be used for NoCry.

Some slight differences

Looking closely, there are a couple of interesting differences between NoCry and the Judge ransomware we previously analyzed. For example, the mutex this time is: "rGoB8VnbP6W42hW5". Furthermore, the screen displayed to the user after file encryption is completed is different.



NoCry Decryptor

Ooooops All Your Files Are Encrypted ,NoCry

Can I Recover My Files ?

Yes, You Can Recover All Your Files Easily And Quickly

But How ?

Send The Required Amount And
I Will Send The Key To You For Decryption

See You Soon (0_0)

Your files will be lost on :

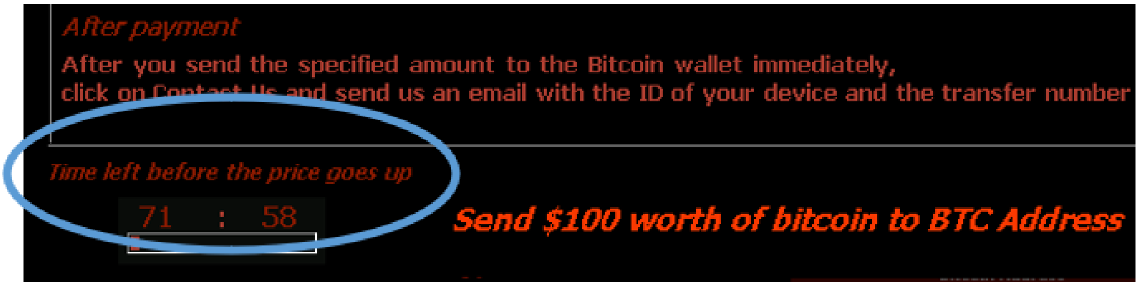
71 : 57

Send $300 worth of bitcoin to this address:

bc1qtje3mdvmwsp64k20srtj65m23qjjc42f2cd3pc

The screen displayed above is very similar to the one displayed by the WannaCry ransomware. The structure and colors of the screen are similar, and the countdown WannaCry presents is also 72 hours.

We found that the countdown in NoCry is a little bit different from the one presented by Judge. The ransom note screen of the previously analyzed Judge ransomware is displayed below. As we can see, the text above the countdown is: "Time left before the price goes up". In the NoCry ransomware, the text changed to: "Your files will be lost on", making the threat more serious.



After payment

After you send the specified amount to the Bitcoin wallet immediately,
click on Contact Us and send us an email with the ID of your device and the transfer number

Time left before the price goes up

71 : 58

Send $100 worth of bitcoin to BTC Address

When these 72 hours pass, the ransomware deletes itself from the infected system. The “Decrypt” button on the ransom note screen is the only way for a victim to restore its files via the intended route. Therefore, once the 72 hours pass, the victim can no longer perform decryption. Using our decryptor however, decryption is still possible.

A free decryptor

The file encryption process did not change, so the decryptor only requires some minor adjustments. Therefore, our current decryptor also decrypts (non-corrupted) files affected by this NoCry/Stupid variant. The decryptor remains free of charge and will be available via the NoMoreRansom initiative soon.

Indicators of Compromise (IoC)

Indicator	Value
SHA256 of ransomware	f2a842eb78e2be3cd1d638a3dabcf21f8fbc35dcd768bb772f5e6080d1f246cc
Command & control hostname	niddle-noddle-eyes[.]000webhostapp[.]com

| RSS NL | RSS EN