Nemty update: decryptors for Nemty 1.5 and 1.6

tesorion.nl/en/posts/nemty-update-decryptors-for-nemty-1-5-and-1-6/

By Frank van den Hurk October 10, 2019

Summary

Last week, we published a blog post on our decryptor for the Nemty ransomware. Since we performed our analysis, two new versions of Nemty have appeared: version 1.5 and 1.6. We have analyzed both and have been working on decryptors for them. As 1.6 is the most recent version of the two, we have been focussing our efforts on this version first. We now have a working decryptor for version 1.6. Please contact Tesorion CSIRT to obtain our decryptor for free if you are a victim of Nemty 1.6. We are also finishing our decryptor for Nemty 1.5 and expect to release it soon as well. Finally, we are working with Europol to get our decryptors included in their NoMoreRansom project.

Update: Our universal decryptor for Nemty versions up to and including 1.6 is available for download at the NoMoreRansom website.

Introduction

In our blog post last week, we described some peculiarities of the cryptography used by the Nemty ransomware up to version 1.4. These peculiarities involved bugs in the AES-256 key scheduling, and the implementation of the CBC block mode. Furthermore, we announced the availability of a free decryptor for Nemty victims through our CSIRT team. In this blog we announce the availability of a free decryptor for Nemty 1.6, and the expected availability of a free decryptor for Nemty 1.5 next week.

Recovering files for Nemty 1.4 and below

Since our previous blog post, our CSIRT team has been very busy assisting numerous victims of Nemty 1.4 and below with recovering their files for free. Furthermore, we have been improving our decryptor based on feedback from the victims who contacted us, and it should by now be able to successfully decrypt a lot of files. We are working on automating this process and expect to be able to release a decryptor soon that will no longer involve our CSIRT team. However, instead of waiting for the availability of our automated decryptor, we decided last week to make our CSIRT team available to assist victims at no cost in the meantime.

Nemty 1.5: stuck in the middle

After finishing our research on Nemty 1.4 and below, a newer 1.5 version was spotted in the wild. The AES bugs of the 1.4 version are still present in this version, but there are some other minor differences that require some changes to our 1.4 decryption process. We have analyzed Nemty 1.5 and have a proof-of-concept decryptor working for this version. Our teams are working on a solution that should enable 1.5 victims to recover many of their files for free as well and hope to include this functionality in our free decryptor somewhere next week.

Update: Nemty 1.5 is also suppored in our decryptor.

Nemty 1.6: a challenger appears

As discussed in our previous blog post, writing about the workings of a ransomware family while announcing a decryptor is bound to trigger some response by the malware authors. And as expected a new version of Nemty has appeared after we published our blog post that described some peculiarities in the AES implementation of Nemty 1.4 and below. In the 1.6 version, the authors even acknowledge our work: the malware binary contains the literal string “tesorion thanks for your article”!

We are glad they took our advice to heart and have moved away from their own AES implementation and now simply use the default Windows cryptographic libraries instead. This made our analysis of the cryptography in the 1.6 version a lot easier. We now no longer had to compare all the individual calculations in their AES implementation to the standard to find out why initially we could not decrypt any Nemty 1.4 encrypted files. Our analysis indeed

confirms that Nemty 1.6 now uses a proper default AES-128-CBC implementation. Good work guys, if everybody would just adhere to these standards, we'd all have more time for the really fun things in life!

By the way, the mutex used in Nemty 1.6 also seems to indicate a certain light-hearted nature in the authors of the ransomware. The mutex in Nemty 1.6 is named "just_a_game".

The best things in life are free: a free decryptor for Nemty 1.6

After analyzing Nemty 1.6, we have constructed a decryptor that is able to decrypt many files encrypted by the Nemty 1.6 ransomware for free. And just like our previous decryptor for Nemty 1.4 and below, we will make this one available for free to victims of the Nemty ransomware.

Short and to the point: If you are a victim of the Nemty ransomware version 1.6 or below, Tesorion can probably help you recover many of your files for free.

Update: Our decryptor is available for download at the NoMoreRansom website.

Indicators of Compromise

SHA256 of the Nemty 1.6 binary used in this research:
98f260b52586edd447eaab38f113fc98b9ff6014e291c59c9cd639df48556e12