RansomExx Ransomware upgrades to Rust programming language

By Pierluigi Paganini

Published: 2022-11-24 · Archived: 2026-04-02 12:32:11 UTC

Pierluigi Paganini November 24, 2022

```
Hello!

First of all it is just a business and the only thing we are interested in is
money.

All your data was encrypted.
Please don't try to modify or rename any of encrypted files, because it can result
in serious data loss and decryption failure.

Here is your personal link with full information regarding this accident (use Tor
browser):
http://rnsm777cdsjrsdlbs4v5qoeppu3px6sb2igmh53jzrx7ipcrbjz5b2ad.onion/<victim_id>/
```

RansomExx ransomware is the last ransomware in order of time to have a version totally written in the Rust programming language.

The operators of the RansomExx ransomware (aka Defray777 and Ransom X) have developed a new variant of their malware, tracked as RansomExx2, that was ported into the Rust programming language.

The move follows the decision of other ransomware gangs, like Hive, Blackcat, and Luna, of rewriting their ransomware into Rust programming language.

The main reason to rewrite malware in Rust is to have lower AV detection rates, compared to malware written in more common languages.

RansomExx2 was developed to target Linux operating system, but experts believe that ransomware operators are already working on a Windows version.

RansomExx operation has been active since 2018, the list of its victims includes government agencies, the computer manufacturer and distributor GIGABYTE, and the Italian luxury brand Zegna. RansomExx is operated by the DefrayX threat actor group (Hive0091), the group also developed the PyXie RAT, Vatet loader, and Defray ransomware strains.

The functionality implemented in RansomExx2 is very similar to previous RansomExx Linux variants.

"RansomExx2 has been completely rewritten using Rust, but otherwise, its functionality is similar to its C++ predecessor. It requires a list of target directories to encrypt to be passed as command line parameters and then encrypts files using AES-256, with RSA used to protect the encryption keys." reads the analysis published by IBM Security X-Force.

The ransomware iterates through the specified directories, enumerating and encrypting files. The malware encrypts any file greater than or equal to 40 bytes and gives a new file extension to each file.

The RansomExx2 encrypts files using the AES-256 algorithm, it drops a ransom note in each encrypted directory.

```
Hello!

First of all it is just a business and the only thing we are interested in is
money.

All your data was encrypted.
Please don't try to modify or rename any of encrypted files, because it can result
in serious data loss and decryption failure.

Here is your personal link with full information regarding this accident (use Tor
browser):
http://rnsm777cdsjrsdlbs4v5qoeppu3px6sb2igmh53jzrx7ipcrbjz5b2ad.onion/<victim_id>/
```

"RansomExx is yet another major ransomware family to switch to Rust in 2022 (following similar efforts with Hive and Blackcat)." concludes the report. "While these latest changes by RansomExx may not represent a significant upgrade in functionality, the switch to Rust suggests a continued focus on the development and innovation of the ransomware by the group, and continued attempts to evade detection."

Follow me on Twitter: **@securityaffairs** and **Facebook** and **Mastodon**

[adrotate banner="9"]	[adrotate banner="12"]

Pierluigi Paganini

(SecurityAffairs – hacking, RansomExx ransomware)

[adrotate banner="5"]

[adrotate banner="13"]

Source: https://securityaffairs.co/wordpress/138933/malware/ransomexx-ransomware-rust-language.html