# Serianu Cyber Security Advisory

## RansomEXX Ransomware Attacks Linux Systems.

**Serianu SOC Advisory Number:**

TA – 2020/021

**Date(s) issued:**

24th November, 2020

## Systems Affected

- Linux Systems

**OVERVIEW:**

RansomEXX is a new human-operated ransomware variant which was first detected in June 2020. This ransomware is notorious for attacking large companies, firms and corporates that have the means to pay and are heavily reliant on their data and systems. With downtime costing the companies millions, payment of the ransom seems to be an easier fix than attempting to recover files from backups. RansomEXX spreads to your computer and encrypts the user data. According to our research, the files will be permanently lost if the user does not pay the ransom.

The ransomware has attracted a lot of attention in recent weeks after being used in attacks on government departments and many large enterprises This advisory provides an in-depth research on the impact, execution and recommendation of the RansomEXX.

## Technical Details

Serianu threat intelligence research team discovered a Linux version of RansomEXX ransomware aka Defray777. This is one of the first times that a Windows ransomware has been adapted to attack Linux systems, with the new variant able to be used in targeted attacks on organizations that have both Windows and Linux systems to cause greater disruption.

Like other similar ransomware targeting enterprises, RansomEXX is manually controlled.First,the attackers penetrate the network of the victims company, gradually spread the attack to various devices and wait until they receive the

administrator's credentials. Then through the domain controller, the attackers spread the malware to the entire Corporate network, encrypting all the files on all available devices.

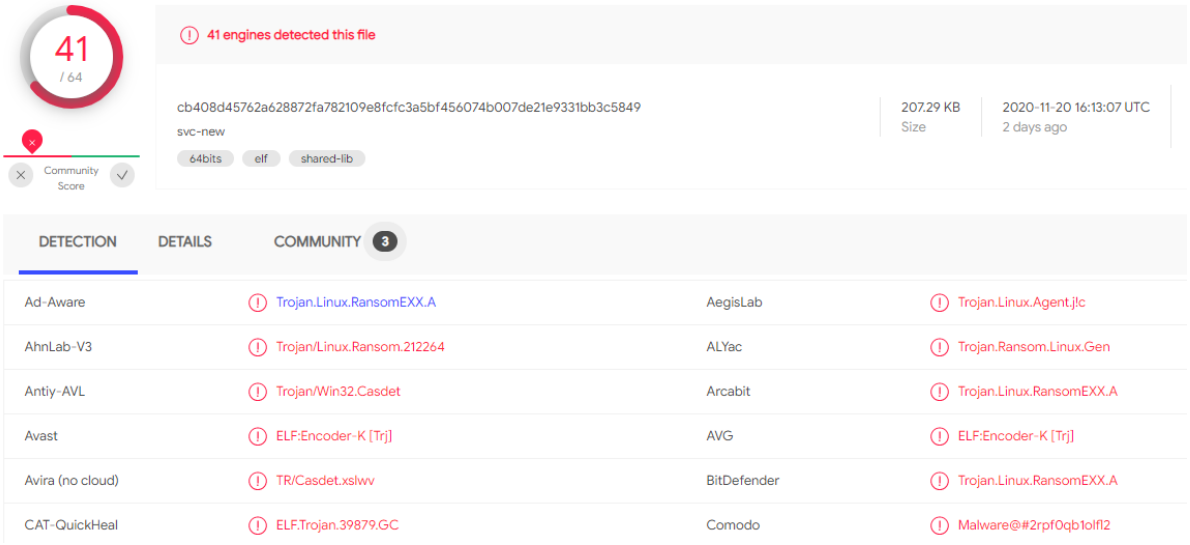
## How RansomEXX Works

When targeting Linux servers, the RansomExx operators will deploy an ELF executable named 'svc-new' used to encrypt a victim's server. When launched, the Trojan generates a 256-bit key and uses it to encrypt all the files belonging to the victim that it can reach. The ransomware then encrypts the AES (Advanced Encryption Standard, used to encrypt sensitive data) key using a public RSA-4096 key appended to each encrypted file.

The malware launches a thread that regenerates and re-encrypts the AES key every 0.18 seconds. However, based on an analysis of the implementation, the keys actually only differ every second. Apart from encrypting the files and leaving ransom notes, the sample has none of the additional functionality that other threat actors tend to use in their Trojans. Unlike the windows version, the Linux version does not contain any Command and Control communication, no termination of running processes and no anti-analysis tricks. Each sample of the malware contains a hardcoded name of the victim organization. If a victim pays the ransom, they will receive both a Linux and Windows decryptor with the corresponding RSA-4096 private key and encrypted file extension embedded in the executable.

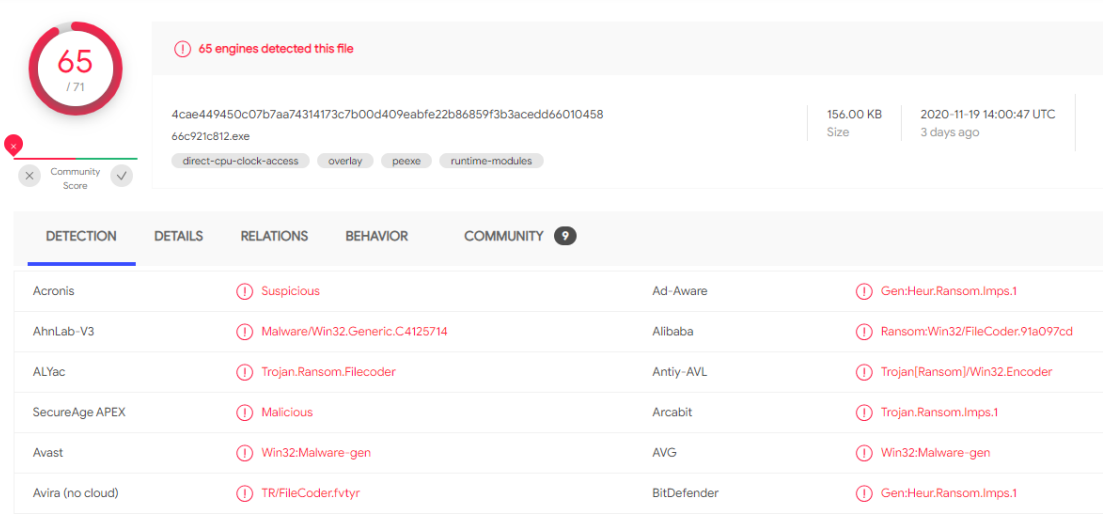
**Sample Hashes – Linux Version**

- **MD5** - aa1ddf0c8312349be614ff43e80a262f
- **SHA-256** - cb408d45762a628872fa782109e8fcfc3a5bf456074b007de21e9331bb3c5849



**Sample Hashes – Windows Version**

- **MD5** - fcd21c6fca3b9378961aa1865bee7ecb
- **SHA-256** - 4cae449450c07b7aa74314173c7b00d409eabfe22b86859f3b3acedd66010458




## Delivery Methods

RansomEXX, spreads to a machine through:

1. Unprotected network settings.
2. An attachment in a spam e-mail.
3. A false update for a program or utility installed on your system.

## Impact

The impact of a Ransomware includes the following:

- Loss or destruction of critical information and data.
- Shutdown of  the organisations operations.
- Business disruption in the post-attack period.
- Damage of hostage systems, data and files.
- Loss of reputation of the victimized company.
- Financial loss associated with remediation efforts.
- Damaged to your company's reputation.

## Recommendations:

- Backup your critical data offline. Make sure to keep everything copied on an external hard drive but be sure not to leave it connected to your computer when not in use. If the hard drive is plugged in when you become a victim of a ransomware attack, this data will also be encrypted. Additionally, cloud storage solutions allow you to revert to previous versions of your files. Therefore, if they become encrypted by ransomware, you should be able to return to an unencrypted version via cloud storage.
- Never click on unverified links.
- Do not open an untrusted email attachment.
- Only download attachments from trusted sites.
- Avoid giving out personal data.
- Use mail server content scanning and filtering. Using content scanning and filtering on your mail servers is a smart way to prevent ransomware. This software reduces the likelihood of a spam email containing malware-infected attachments or links from reaching your inbox.
- Never use unfamiliar USBs.
- Keep your software and operating systems updated.
- Use antivirus and other software that can protect your system against such threats.
- General user awareness training to the staff. Security training can teach team members what to look for in an email before they click on a link or download an attachment.

## Conclusion

The ransomware operators continue to use stolen or brute-forced remote desktop protocol credentials to gain remote access to victims' networks.

Serianu does not encourage victims to pay the ransom, which might insight cybercriminals to target additional organizations or encourage other hackers to leverage ransomware. Paying the ransom demand also does not guarantee the hackers will unlock the files.

## Information Sharing

As a means of preventing such attacks from occurring, we encourage any organization or individual that has access to ransomware related attacks to share it with us through our email info@serianu.com to allow us to analyze any indicators of compromise (IOC).