SEQURETEK

RansomEXX

OVERVIEW

Human Operated ransomware RansomEXX's Operators developed new ELF executable to infect Linux based operating systems.

KNOWLEDGE BASE REGISTER

- Version Control

Issue Date	Version	Prepared by	Approved by
11th Nov 2020	v 1.0	Vidhi Patel	Cdr. Subhash Dutta

OVERVIEW

- Kaspersky researchers discovered Linux version of windows human operated ransomware RansomEXX's.
- RansomEXX operators created new ELF executable, designed to encrypt data on computers controlled by Linux-based operating systems.
- RansomEXX is known for targeted attacks. Each sample includes hard coded name of victim organization.
- Ransom note also includes name of organization. Encrypted file extension and the email address for contacting the extortionists also make use of the victim organization's name.

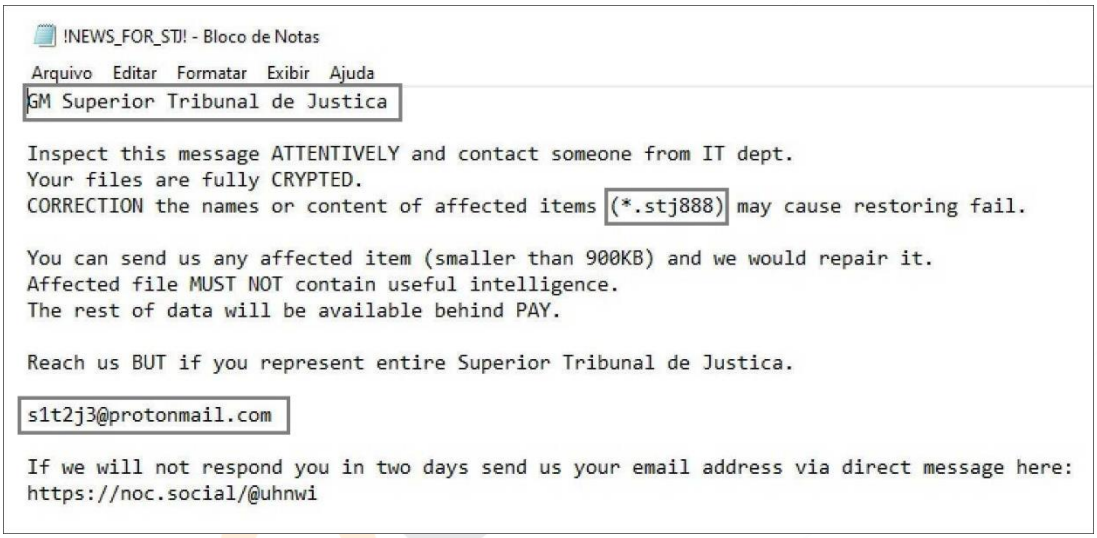

Figure 1: RansomEXX RansomNote

TECHNICAL DETAILS

- Linux version of RansomEXX deploys an ELF executable named 'svc-new' to encrypt a victim's server.
- Ransomware generates a 256-bit key and uses it to encrypt all the files belonging to the victim that it can reach using the AES block cipher in ECB mode.
- The AES key is encrypted by a public RSA-4096 key embedded in the Trojan's body and appended to each encrypted file.
- Ransomware generate regenerate and re-encrypt the AES in every 0.18 seconds.
- Linux and Windows version of ransomware are using some same function of open-source library **mbedtls**.

INDICATORS OF COMPROMISE

FILE HASHES (MD5)

Linux: AA1DDF0C8312349BE614FF43E80A262F

Windows: FCD21C6FCA3B9378961AA1865BEE7ECB

PREVENTIVE AND CORRECTIVE DEFENCE ACTIONS

- **Preventive Actions**
  - Block the IoCs in the corresponding security devices.
  - All these IoCs are combined in our Threat Intelligence Feed that is integrated with our SOC to provide proactive threat protection to our clients.
  - Employ content scanning and filtering on the organization mail servers. Inbound e-mails should be scanned for known threats and should block any attachment types that could pose a threat.
  - Update your Operating system and software to latest version.
  - Ensure anti-virus and anti-malware solutions are set to automatically update and regular scans are conducted.
  - Do not trust emails from untrusted source.
  - Do not open links and attachments from untrusted sources.
  - Back-up data, store it outside of network connection.
  - Use strong password and change it at regular interval. Don't use the old password again.
  - Disable the unwanted services and close the ports that are not needed.
- **Corrective Actions**
  - If infected, disconnect the affected system from the Network.
  - Inform the Information Security Team.
  - Use antivirus or anti-malware software to clean the malware.