## Severity

High

## Analysis Summary

NOKOYAWA is a new emerging ransomware that encrypts data and demands ransom for its decryption. It encrypts files and attaches a ".NOKOYAWA" extention to their filenames. To be more precise, a file named "1.jpg" would become "1.jpg.NOKOYAWA," and the same goes for other files that are impacted by this ransomware. After this process, a ransom note titled "NOKOYAWA_readme.txt" is created on the desktop. This ransomware's ransom message is repeated twice in both English and Chinese. They notifies victims that their files have been encrypted and can only recovered via the attackers' decryption key. Infected email attachments and torrent websites could be the distribution method for this ransomware.

```
Dear usernamme, your files were encrypted, some are compromised.
Be sure, you can't restore it without our help.
You need a private key that only we have.
Contact us to reach an agreement or we will leak your black shit to media:

charlefletcher@onionmail.org
Johnatannielson@protonmail.com

亲爱的用户名，您的文件已加密，有些已被泄露。
请确保，如果没有我们的帮助，您将无法恢复它。
您需要一个只有我们拥有的私钥。
联系我们以达成协议，否则我们会将您的黑屎泄露给媒体：

charlefletcher@onionmail.org
Johnatannielson@protonmail.com
```

Taken from Sentinel One

## Impact

- Information theft
- File encryption

## Indicators Of Compromise

### Email

- Brookslambert@protonmail[.]com
- charlefletcher@onionmail[.]org
- Johnatannielson@protonmail[.]com
- Sheppardarmstrong@tutanota[.]com

### MD5

- 354c0c8c4466f0f8cc508c7813c096f5
- 22a006b6d19558c3cebd708b2b0543bc
- 2e936942613b9ef1a90b5216ef830fbf
- 790e1636821bb83eff48fd8314557817

### SHA-256

- 86953a6ce9fb7bf8b7791b9c6b751120c35ee1df5590ba4ff447e21c29259e51
- fefd1117c2f0ab88d8090bc3bdcb8213daf8065f12de1ee6a6c641e888a27eab
- e097cde0f76df948f039584045acfa6bd7ef863141560815d12c3c6e6452dce4

- 6c98d424ab1b9bfba683eda340fef6540ffe4ec4634f4b95cf9c70fe4ab2de90

SHA-1

- 2904358f825b6eb6b750e13de43da9852c9a9d91
- 2d92468b5982fbbb39776030fab6ac35c4a9b889
- 32c2ecf9703aec725034ab4a8a4c7b2944c1f0b7
- 960fae8b8451399eb80dd7babcc449c0229ee395

# Remediation

- Backup your data. Any damage in case of a successful attack will be mitigated if data is backed up.
- Emails from unknown senders should always be treated with caution.
- Never open links or attachments from unknown senders.
- Disable all threat indicators at your respective controls.
- Look for IOCs in your surroundings.