Severity

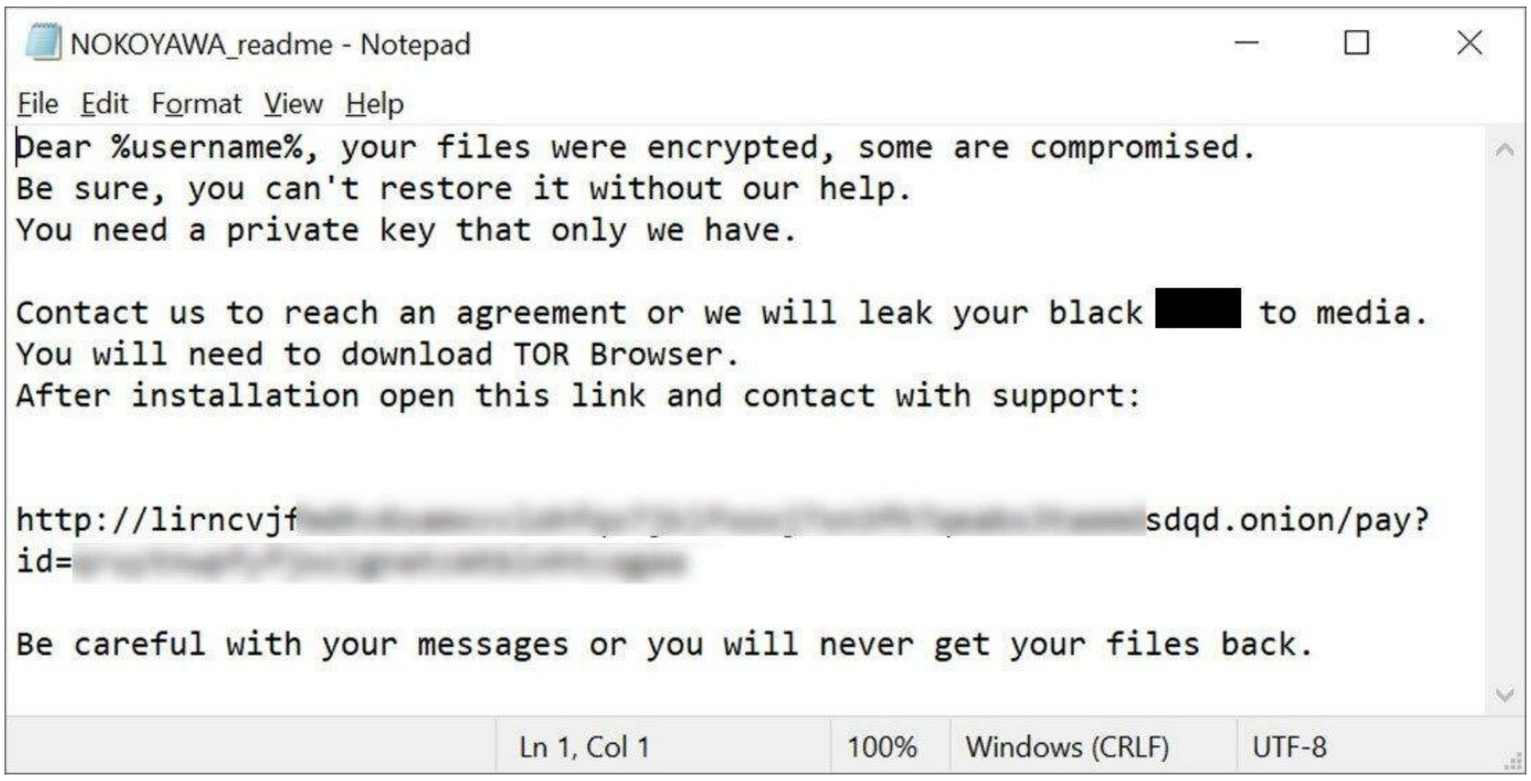
High

Analysis Summary

Nokoyawa is a new malware for Windows that first appeared this year. Researchers' samples revealed coding similarities with Karma, another ransomware that traces its lineage to Nemty via a long string of variants. Researchers have discovered a new strain of the Nemty ransomware campaign that has been improving by reusing code from publicly available sources. Nokoyawa offers many command line options for customized executions:

- —help (Print the list of command line options)
- -network (Encrypt files on all drives and volumes for both local and networked)
- -file filePath (Encrypt a single file)
- -dir dirPath (Encrypt all files in specified directory and sub-directories)

Nokoyawa encrypts all local drives and volumes by default if no argument is provided. The "-help" parameter implies that the developers are not the same as the operators who distribute and execute the ransomware. A .NOKOYAWA extension is attached to files encrypted by ransomware. The ransom message is written into NOKOYAWA_readme.txt in each encrypted directory



```
Dear %username%, 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 [redacted] to media.
You will need to download TOR Browser.
After installation open this link and contact with support:


http://lirncvjf[redacted]sdqd.onion/pay?
id=[redacted]

Be careful with your messages or you will never get your files back.
```

Impact

- File Encryption
- Password Theft

Indicators of Compromise

MD5

- c159afb7d2111690326cad610776db34
- feb7b1e0161df136c3d385bfd2d4b247

SHA-256

- a32b7e40fc353fd2f13307d8bfe1c7c634c8c897b80e72a9872baa9a1da08c46
- 304e01db6da020fc1e0e02fdaccd60467a9e01579f246a8846dcfc33c1a959f8

SHA-1

- 228239d1bf7020ecdc4021f3c20a14041b210d78
- 93027bd81e608b3bd88a608fe3f6826c96656864

Remediation

Block all threat indicators at your respective controls. Search for IOCs in your environment.