Rewterz Threat Alert – Evilnum APT Group - Active IOCs - Rewterz

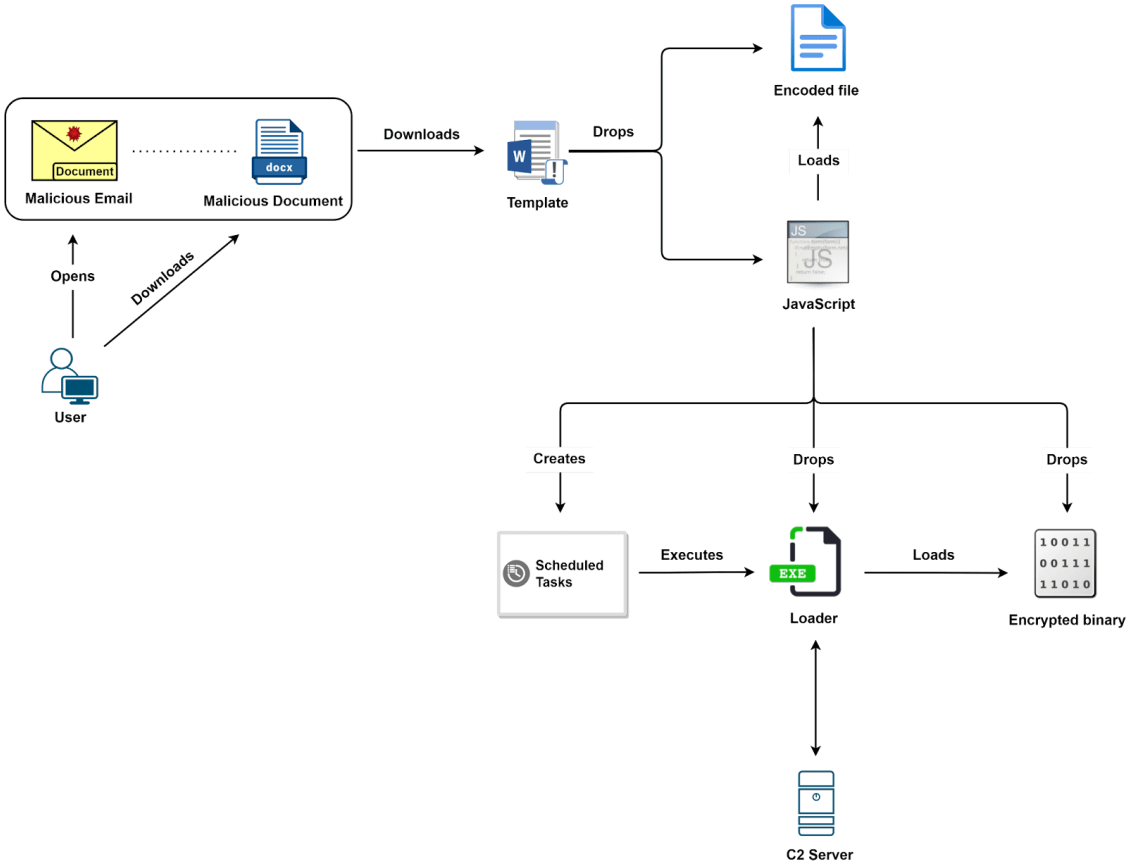
Published: 2022-06-30 · Archived: 2026-04-05 18:13:50 UTC

Severity

High

Analysis Summary

APT group Evilnum aka Jointworm has been seen targeting the financial sector with malicious emails. The group first seen in 2018 with the motivation of information theft and espionage has been active recently in an attempt to rob users of their credentials and gaining sensitive information for their gain. The Evilnum APT group has mostly targeted FinTech (financial services) sector, particularly those in the UK and Europe that deal with trading and compliance. However, in March, 2022, the group targets Intergovernmental organizations that offer assistance related to international migration.
EVILNUM is a JavaScript-based malware family. A heavily obfuscated JavaScript was used in recent campaigns for dropping the payloads and decryption. Compared to previous versions used by EvilNum APT, this JavaScript has significant improvements in the obfuscation technique.



Impact

- Exposure of Sensitive Data
- Information Theft and Espionage

Indicators of Compromise

Domain Name

- travinfor[.]com
- webinfors[.]com
- khnga[.]com
- netwebsoc[.]com
- infcloudnet[.]com
- bgamifieder[.]com
- bunflun[.]com
- refinance-ltd[.]com
- book-advp[.]com

MD5

- 0b4f0ead0482582f7a98362dbf18c219
- 4406d7271b00328218723b0a89fb953b
- 61776b209b01d62565e148585fda1954
- 6d329140fb53a3078666e17c249ce112
- db0866289dfded1174941880af94296f
- f0d3cff26b419aff4acfede637f6d3a2
- 79157a3117b8d64571f60fe62c19bf17

SHA-256

- f0e89639e3796a7b7d5ced50e84d770753e72885df7413cd5204a41b1fd6cfbe
- 4ad43986f7130d8d1a40f0377e0c1ada1115fae3e972b339f728d0e794b4a20f
- 531e1e4e076fc0e5a792b60bd138209105f22b2e7b9818aff5efc0ff9f616917
- 78c6c33ebb8d5311c85c58817a1cce7bd126aa9457155962e7d5d2ffcc74c805
- c4cedf78bf239c28e49e43a21c723ec66ffaca48a7b2c4767f73437325c7cc0d
- bb975fed53a9fa18a4234b90ffbd489429ea03a91245dad030fe4053f465ec28
- 29f5aba55197172be28be0fabe2bd9d89ccff73393dc10fd8f2f6bd74287af7e

SHA-1

- 75c0a948fc341177d0da16da19407bd41da183a5
- 9172ef18ad1d0e5aa0e947321dbd2ed38bd7755d
- 49b65b553ad506ce6fb20b84468a543208aa0691

- 7ebcc05d39ff25ad7814ed2ad081b7e8ec5a5003
- 9d692fc1ee6ea146d70d6bb307e3c0fed6c5bd24
- af6ee983a8e085fec67b19bfa3a0a042658a3740
- 038dae3c3d738a5a2da3650cbf1dbfac8655f004

Remediation

- Search for IOCs in your environment.
- Block all threat indications at their respective controls.
