Nemty Ransomware Actively Distributed via 'Love Letter' Spam

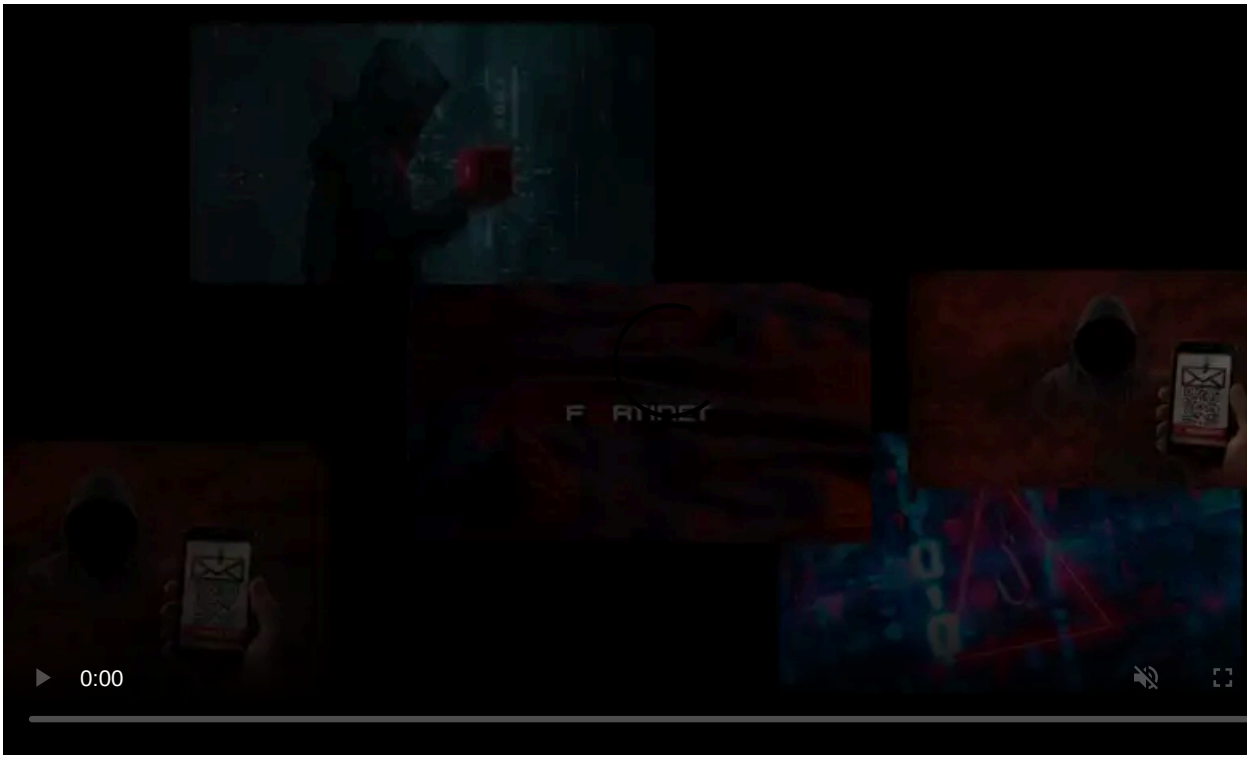
By Sergiu Gatlan

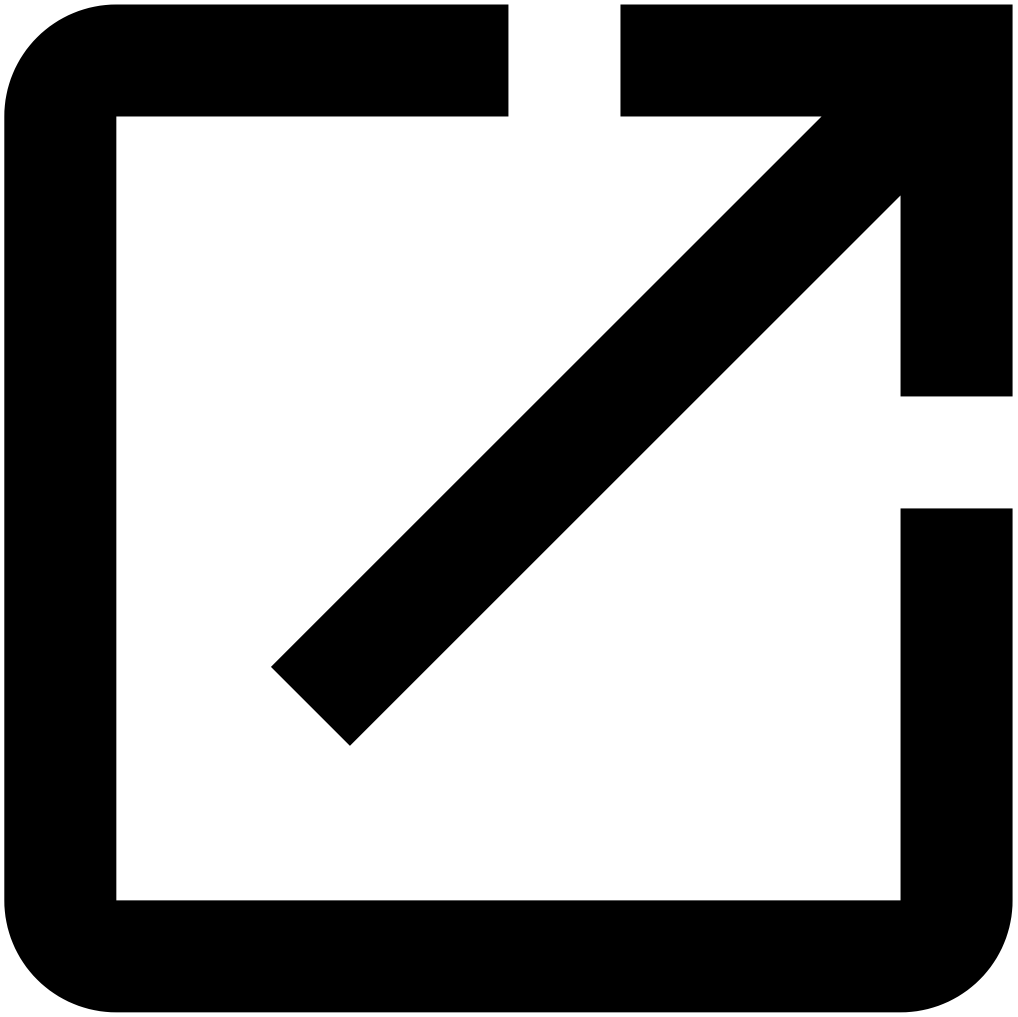
Published: 2020-02-27 · Archived: 2026-04-05 23:40:46 UTC

Security researchers have spotted an ongoing malspam campaign using emails disguised as messages from secret lovers to deliver Nemty Ransomware payloads on the computers of potential victims.

The spam campaign was identified by both Malwarebytes and X-Force IRIS researchers and has started distributing malicious messages yesterday via a persistent stream of emails.

The attackers use several subject lines that hint at the contents of the email being sent by someone the recipient already knows and are built using a love letter template with statements such as "Don't tell anyone," "I love you," "Letter for you," "Will be our secret," and "Can't forget you."

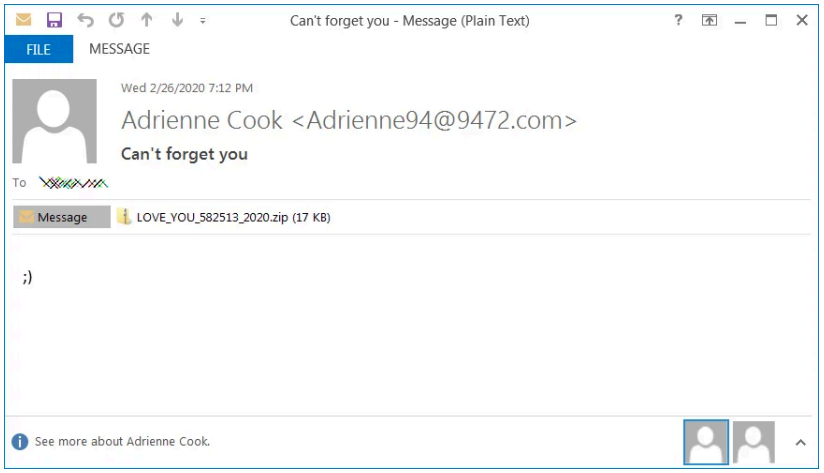

0:00



Visit Advertiser website[GO TO PAGE]

What sets this campaign apart from others is that the operators didn't bother composing an enticing email since all these spam messages only contain a wink `;)` text emoticon.

This might be a hint at the attackers thinking that the 'secret lover' bait — as it was dubbed by Malwarebytes — is effective enough on its own.

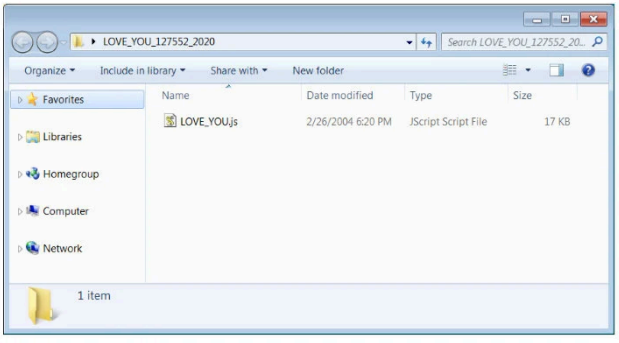


Sample spam email

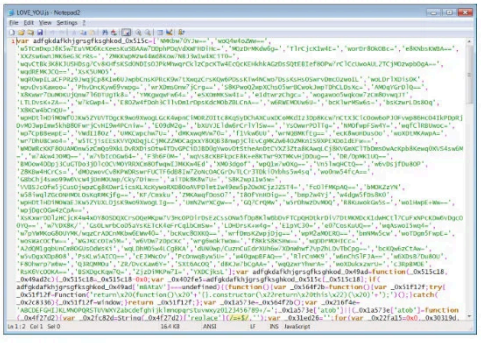
"Attached to each email is a ZIP archive with a name formatted as 'LOVE_YOU_######_2020.zip' with only the #s changing," researchers at X-Force IRIS found.

"The hash of the file contained within each of these archives remains the same and is associated with a highly obfuscated JavaScript file named LOVE_YOU.js,"

This malicious JavaScript file has a very low VirusTotal detection rate at the moment which might lead to an increased number of infections until other security solutions add it to their definitions.



The ZIP attachment contents

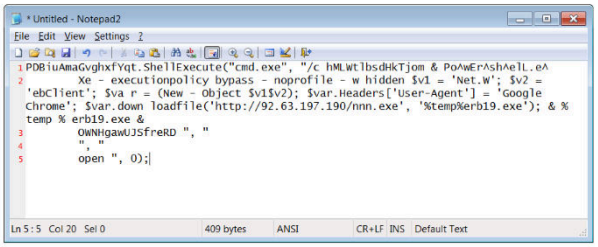


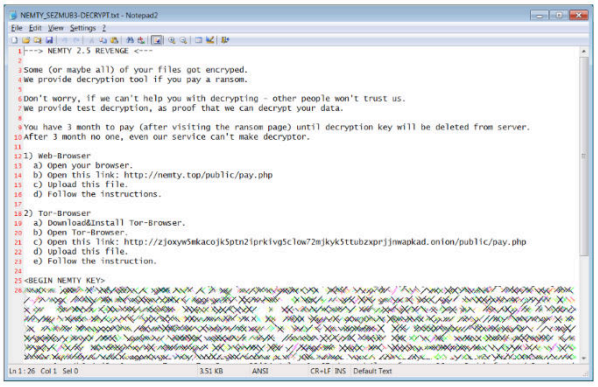
Obfuscated JavaScript file

The attackers use it to drop a Nemty ransomware executable on the victims' computers when executed by downloading the malicious payload from a remote server and launching it.

"The downloaded executable was identified to be the Nemty ransomware and performs encryption of system files upon execution, leaving behind a ransom note demanding payment in exchange for the decryption key," the researchers discovered.

Script deobfuscated by BleepingComputer





Ransom note

Nemty ransomware was first spotted in August 2019 and is known for deleting the shadow copies of all the files it encrypts, making it impossible for victims who don't have separate backups to recover their data.

Researchers discovered one month later that the malware's developers upgraded it to include code for killing Windows services and processes to allow it to encrypt files that are currently in use.

Security firm Tesorion created a free Nemty ransomware decryptor in October 2019 for Nemty versions 1.4 and 1.6, and working for a limited number of document types including images, videos, office docs, and archives.

Last month the operators behind the Nemty ransomware said that they're planning to create a leak blog to be used to publish information stolen for ransomware victims who refused to pay the ransoms.

This trend was started by Maze Ransomware in November 2019, with Sodinokibi, BitPyLock, and Nemty following on their tracks and saying that they'll adopt the same tactic (1, 2, 3).

Source: https://www.bleepingcomputer.com/news/security/nemty-ransomware-actively-distributed-via-love-letter-spam/