Nemty Ransomware Loves You

Author: James Barnett

Overview

Last week, Nemty ransomware made its first attempt to target English-speaking victims with a malicious spam (malspam) campaign.[1] Nemty only recently started using malspam as a distribution method, and until now its malspam campaigns have been restricted to targets in the Asia-Pacific region (APAC).[2,3]

Customer Impact

Nemty is a ransomware that finds and deletes shadow copies of files before it encrypts them, making it more difficult for users to restore files without paying the ransom.

Earlier this year, the threat actors behind Nemty announced their intention to begin leaking the confidential data of victims who refuse to pay their ransom.[4] This strategy has become increasingly popular amongst ransomware operators because it allows them to extort victims regardless of whether or not the victim can restore their files from a backup.

Campaign Analysis

The campaign in this report used a classic "secret admirer" lure reminiscent of the ILOVEYOU worm of 2000.[5] All of the email subjects we observed in last week's campaign used phrases such as "I love you," "Loveletter for you," and "Can't forget you" to entice recipients into opening a malicious attachment. The message body contained only the ;) winking emoticon.

Unlike the Nemty campaigns Infoblox has previously reported,[6,7] this campaign had no apparent geographic targeting aside from the fact that its emails and files were written in English.

Attack Chain

When the victim extracts and executes the malicious JavaScript file contained within the ZIP file attachment, it launches a PowerShell command that retrieves and executes the Nemty ransomware payload from a remote server. Before Nemty begins encrypting the victim's files, it uses the Windows vssadmin command to delete any existing shadow copies of files to prevent the victim from easily restoring them.

It then uses the taskkill command to stop processes and services that may prevent it from successfully encrypting files. Compared to previous samples of Nemty that we have examined, these sought to terminate an expanded list of specific processes, adding node, QBW32, WBGX, Teams, and Flow to the previously known list that included sql, winword, wordpad, outlook, thunderbird, oracle, excel, onenote, and virtualboxvm.

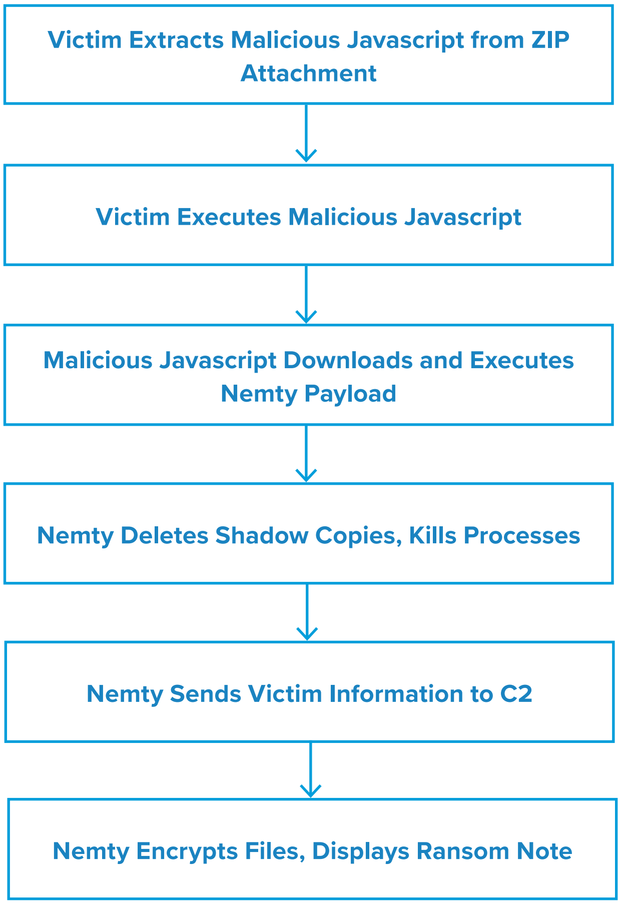
Nemty then transmits information about the infected system to its command and control (C2) server. Afterwards, it proceeds to encrypt the victim's files and change their file extensions to: _NEMTY_{seven random characters}.

Once Nemty completes the encryption process, it displays a ransom note informing victims that their files are encrypted and instructing them to visit the attacker's payment website.

Vulnerabilities & Mitigation

Infoblox recommends the following actions for combatting malspam:

- Be cautious of emails from unfamiliar senders and inspect unexpected attachments before opening them.
- Always be suspicious of vague or empty emails, especially if there is a prompt to open an attachment or click on a link.
- Implement attachment filtering to reduce the likelihood of malicious content reaching a user's workstation.
- Be aware of any attachment's file type, and never open files that could be a script (.js, .vbs, .cmd, .bat), an internet shortcut file, or compression file. Using the latter is a known method for evading detection methods based on file hashes and signatures. Threat actors use them to mask the real malicious file due to email service restrictions on attachment file types.
- Back up data and systems regularly to minimize the potential impact of ransomware in general.
- Ideally, store backup data off the network.



Victim Extracts Malicious Javascript from ZIP Attachment

Victim Executes Malicious Javascript

Malicious Javascript Downloads and Executes Nemty Payload

Nemty Deletes Shadow Copies, Kills Processes

Nemty Sends Victim Information to C2

Nemty Encrypts Files, Displays Ransom Note

Endnotes

1. https://twitter.com/MBThreatIntel/status/1232828557040029696
2. https://www.lastline.com/labsblog/nemty-ransomware-scaling-up-apac-mailboxes-swarmed-dual-downloaders/
3. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--60
4. https://www.bleepingcomputer.com/news/security/nemty-ransomware-to-start-leaking-non-paying-victims-data/
5. https://en.wikipedia.org/wiki/ILOVEYOU
6. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--41
7. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--60

Infoblox enables next-level network experiences with its Secure Cloud-Managed Network Services. As the pioneer in providing the world's most reliable, secure and automated networks, we are relentless in our pursuit of network simplicity. A recognized industry leader, Infoblox has 50 percent market share comprised of 8,000 customers, including 350 of the Fortune 500.

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com