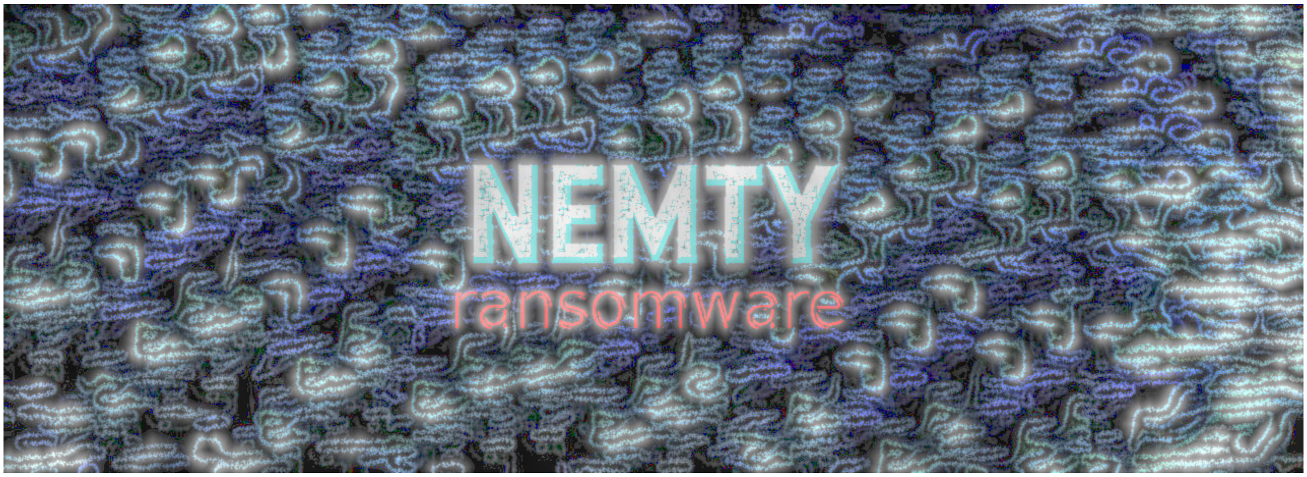
Nemty Ransomware Gets Distribution from RIG Exploit Kit

bleepingcomputer.com/news/security/nemty-ransomware-gets-distribution-from-rig-exploit-kit/

Ionut Ilascu

By
Ionut Ilascu

- September 3, 2019
- 04:48 AM
- 0



The operators of Nemty ransomware appear to have struck a distribution deal to target systems with outdated technology that can still be infected by exploit kits.

Exploit kits are not as commonly used since they typically thrive on vulnerabilities in Internet Explorer and Flash Player, two products that used to dominate the web a few years ago but are now with one foot out in the grave.

Even so, many companies still depend on them and Microsoft's web browser continues to be used in many countries, turning them into targets for web threats to which most of the world is immune.

Nemty is all RIGged up

Nemty appeared on the radar towards the end of August, although the malware administrators made it known on cybercriminal forums long before this date.

It drew attention through its code, which in version 1.0 contains references to the Russian president and to antivirus software.

BleepingComputer saw that the post-encryption ransom demand was around $1,000 in bitcoin. Unfortunately, there is no free decryption tool available at the moment and the malware makes sure to remove the file shadows created by Windows.

Security researcher Mol69 noticed that the file-encrypting malware is now a payload in malvertising campaigns from RIG exploit kit (EK).

The malware used the .nemty extension for the encrypted files but the variant observed by Mol69 adds '._NEMTY_Lct5F3C_' at the end of the processed files.

> #Malvertising -> #RIGEK -> #NEMTY (#Ransomware)
>
> [Extention]
> ._NEMTY_Lct5F3C_
>
> Example Payloadhttps://t.co/eZk2oFZ1t9@anyrun_app @EKFiddle @adrian__luca @jeromesegura @nao_sec @david_jursa pic.twitter.com/HJngPRBKBW
>
> — mol69 (@tkanalyst) August 31, 2019

In the ransom note shown after encrypting the files, Nemty provides instructions on how to pay to recover the data.

In the ransom note is also an encrypted version of the key that unlocks the files on the infected computer, and decrypting it is controlled by the malware administrators.

Suspicious community

Mol69 rolled the infection chain in an AnyRun test environment that documents all of the steps leading to the file encryption process. The entire activity took over 10 minutes to finish.

Nemty is new on the scene and on at least one underground forum it was received with skepticism. This is not unusual with new ransomware, BleepingComputer learned from Yelisey Boguslavskiy, director of security research at Advanced Intelligence (AdvIntel).

This was not the case of Sodinokibi, though, whose administrators are suspected to be from the old GandCrab gang. Sodinokibi ransomware received immediate support from high-profile members of the forum.

Furthermore, its profitability only enticed spirits and prompted malware distributors to jump at the opportunity of partnering up. However, Sodinokibi operators are very selective and associated only with individuals considered veterans in the field.

Nemty, on the other hand, did not enjoy a warm welcome in the community.

Related Articles:

BlackCat/ALPHV ransomware asks $5 million to unlock Austrian state

Windows 11 KB5014019 breaks Trend Micro ransomware protection

Industrial Spy data extortion market gets into the ransomware game

New ‘Cheers’ Linux ransomware targets VMware ESXi servers

SpiceJet airline passengers stranded after ransomware attack

- Encryption Keys
- Nemty Ransomware
- Ransomware
- RIG

Ionut Ilascu

Ionut Ilascu is a technology writer with a focus on all things cybersecurity. The topics he writes about include malware, vulnerabilities, exploits and security defenses, as well as research and innovation in information security. His work has been published by Bitdefender, Netgear, The Security Ledger and Softpedia.

- Previous Article
- Next Article

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: