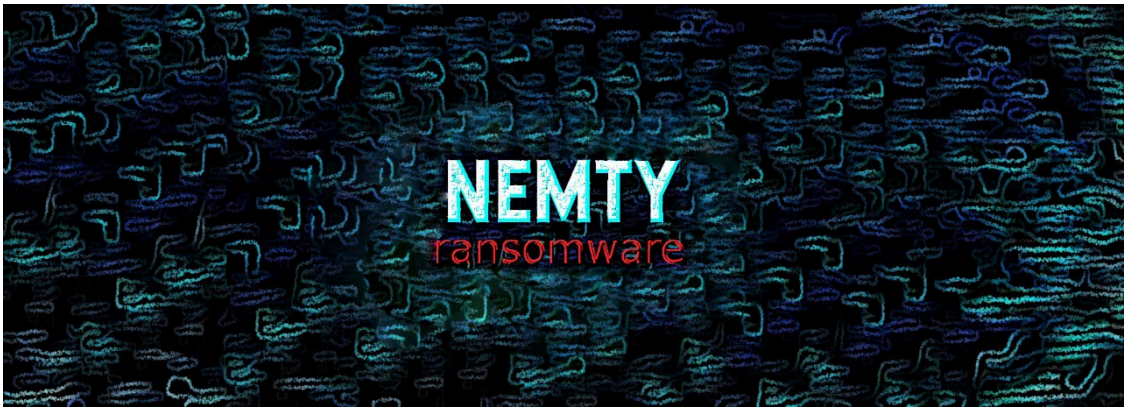
Nemty 1.6 Ransomware Released and Pushed via RIG Exploit Kit

By Lawrence Abrams

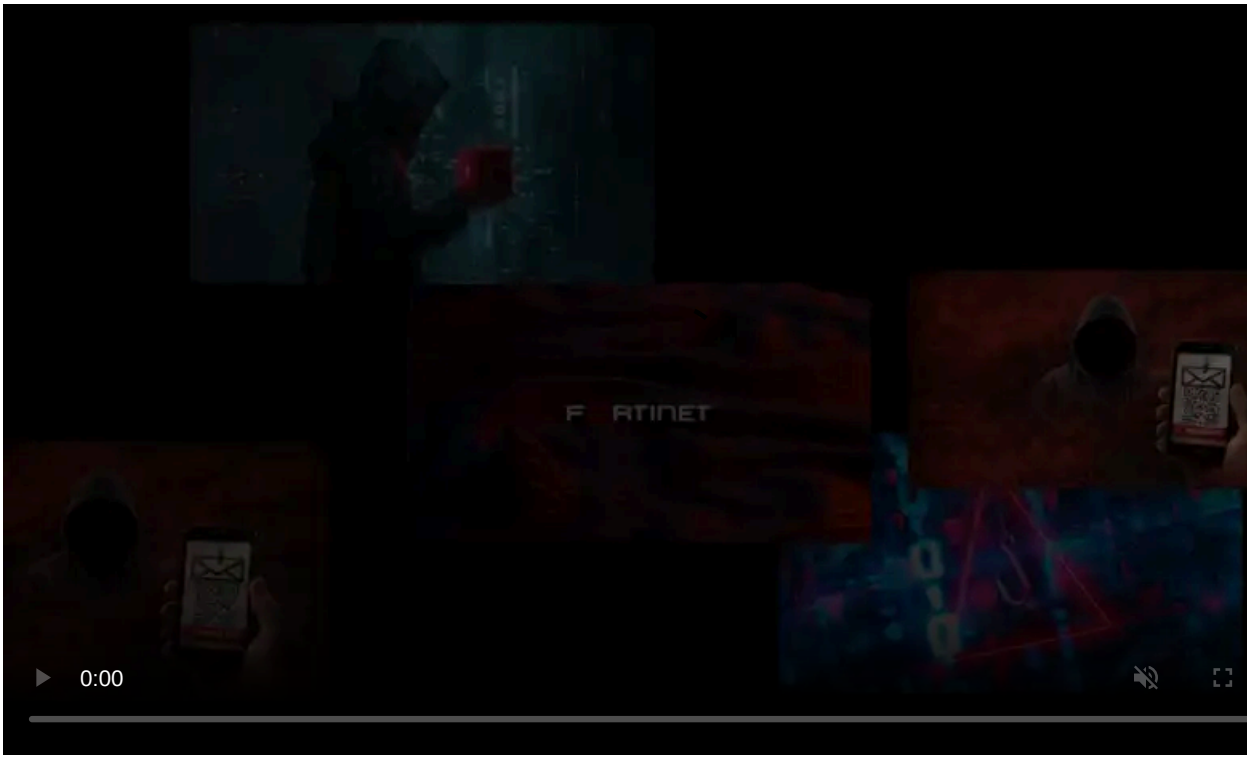
Published: 2019-10-11 · Archived: 2026-04-05 20:24:58 UTC

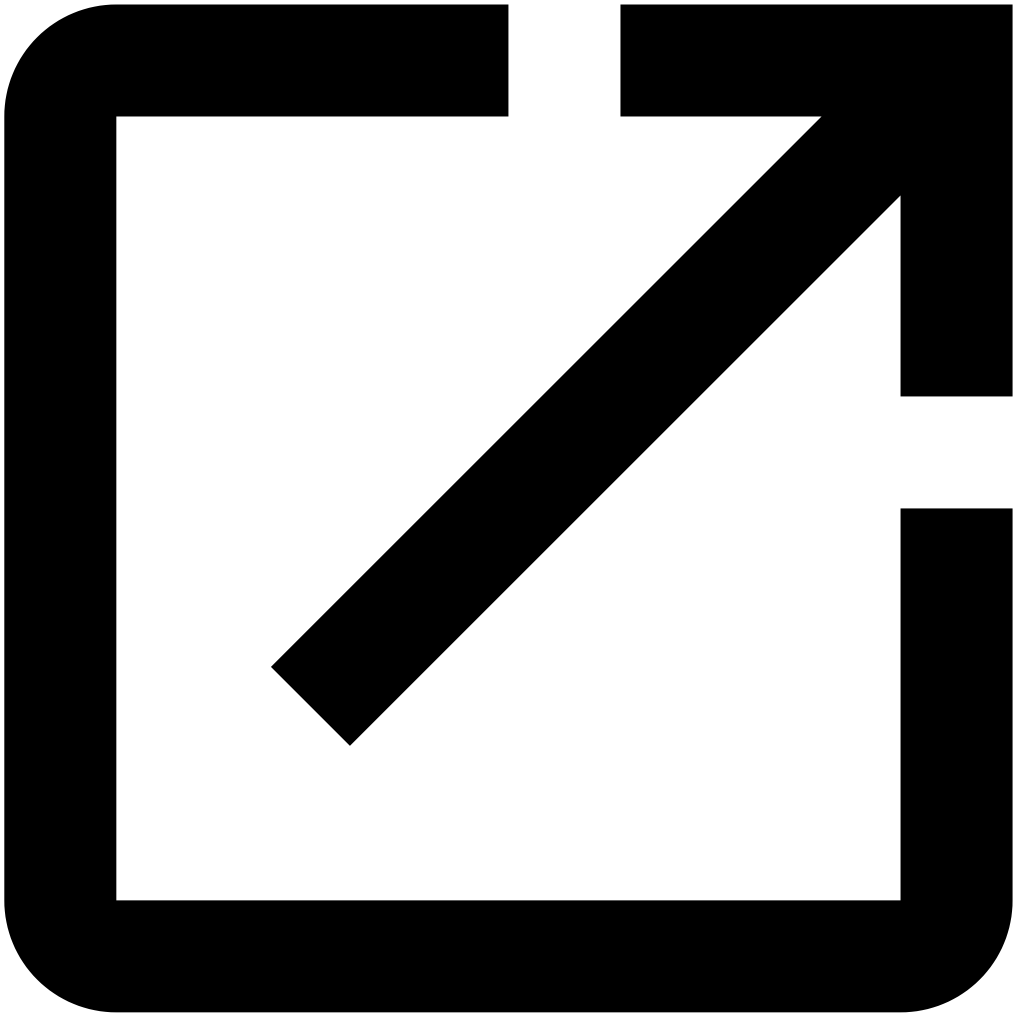


The RIG exploit kit is now pushing a cocktail of malware that includes a new variant of the Nemty Ransomware.

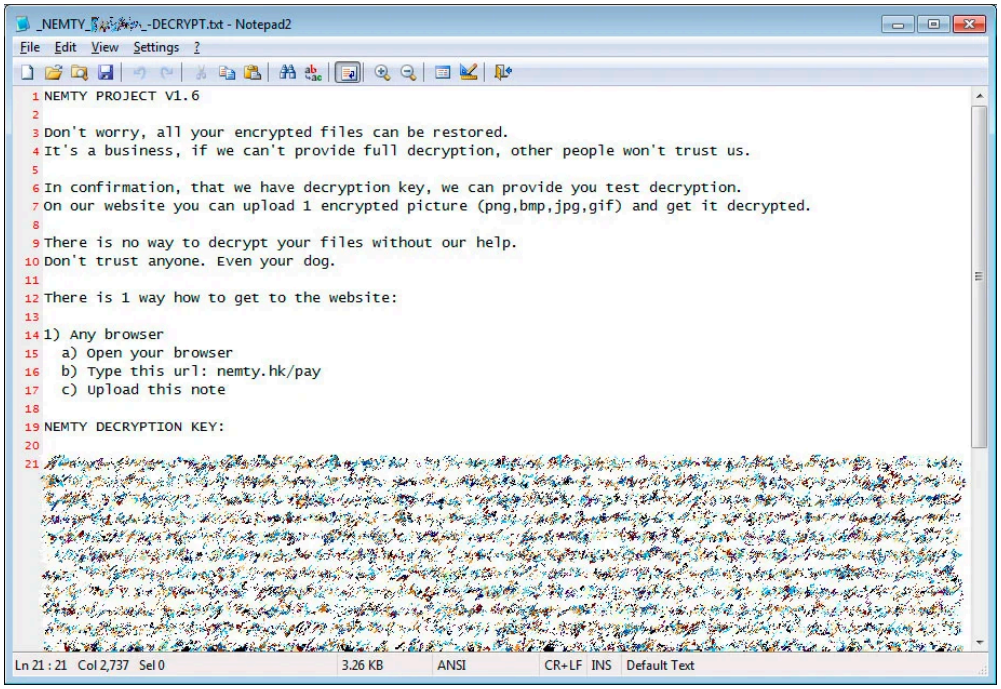
First spotted by exploit kit researcher mol69, a malvertising campaign is redirecting users to the RIG exploit kit to target enterprise users who are still utilizing Internet Explorer and Flash Player.

If a user running these outdated programs are redirected to the exploit kit landing page, the malicious scripts will attempt to exploit vulnerabilities in the browser to install a variety of malware including the Nemty 1.6 ransomware.


F RTINET
0:00



The most obvious change in this version is the ransom note that now shows a version number of 1.6 as seen below.



Nemty 1.6 Ransom Note

According to security firm Tesorion, Nemty 1.6 also modified their encryption algorithm to use the Windows cryptographic libraries instead of their own custom AES implementation.

This was most likely done to break the decryptor created by Tesorion, which didn't go as plan as Tesorion's decryptor can still decrypt Nemty 1.6 victims for free.
