

Nemty 1.6 Ransomware Released and Pushed via RIG Exploit Kit

By Lawrence Abrams

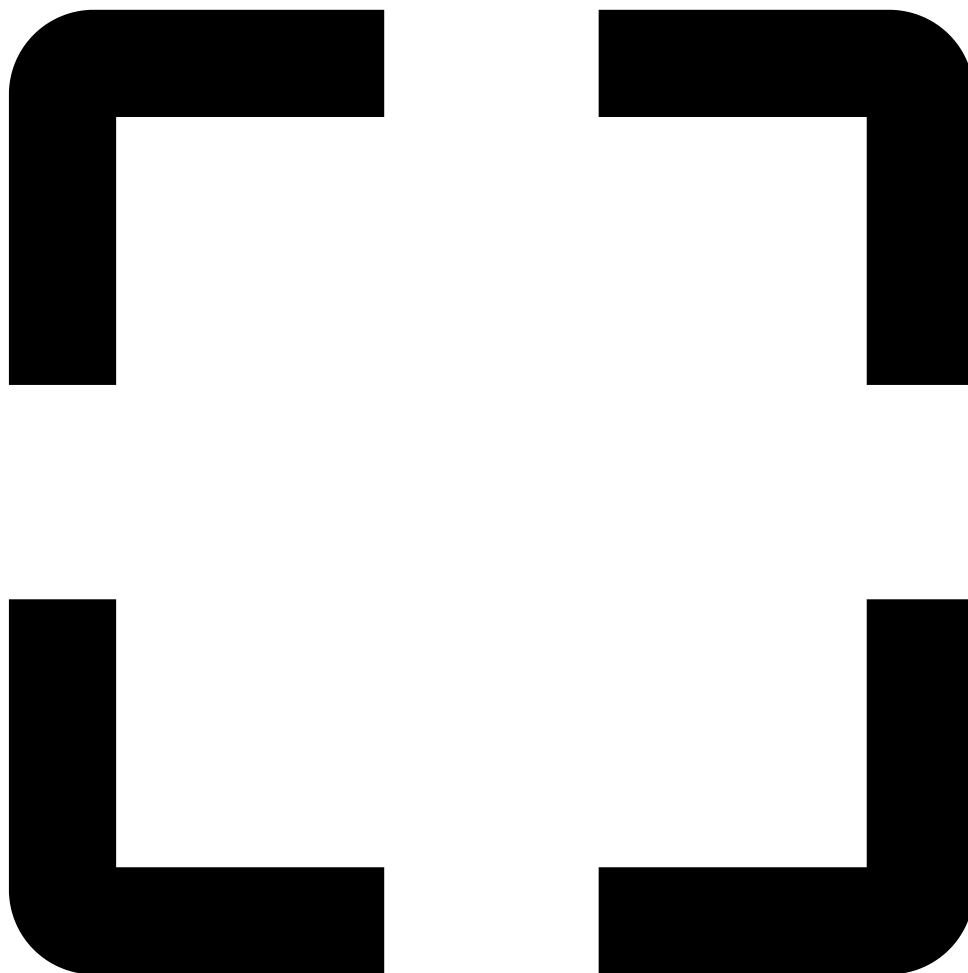
Published: 2019-10-11 · Archived: 2026-05-03 02:41:36 UTC

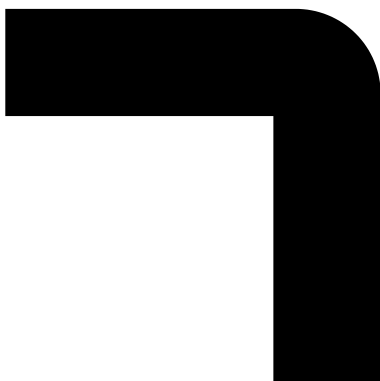
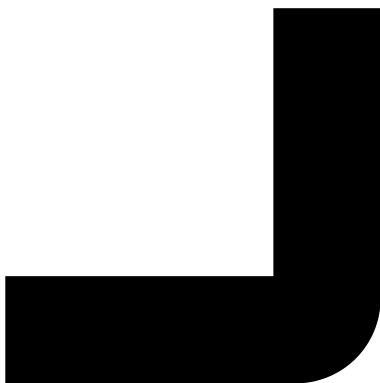


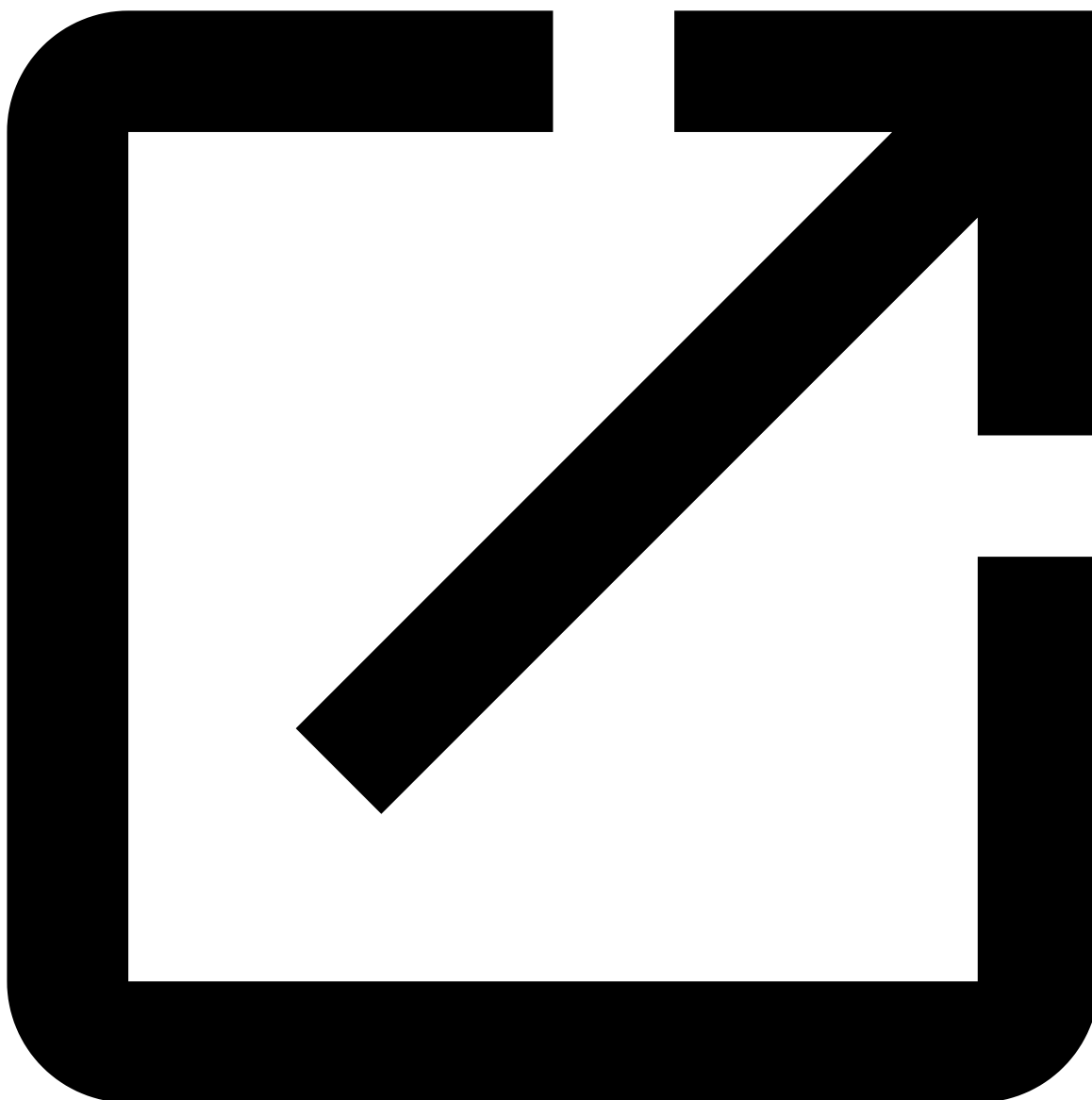
The RIG exploit kit is now pushing a cocktail of malware that includes a new variant of the Nemty Ransomware.

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.

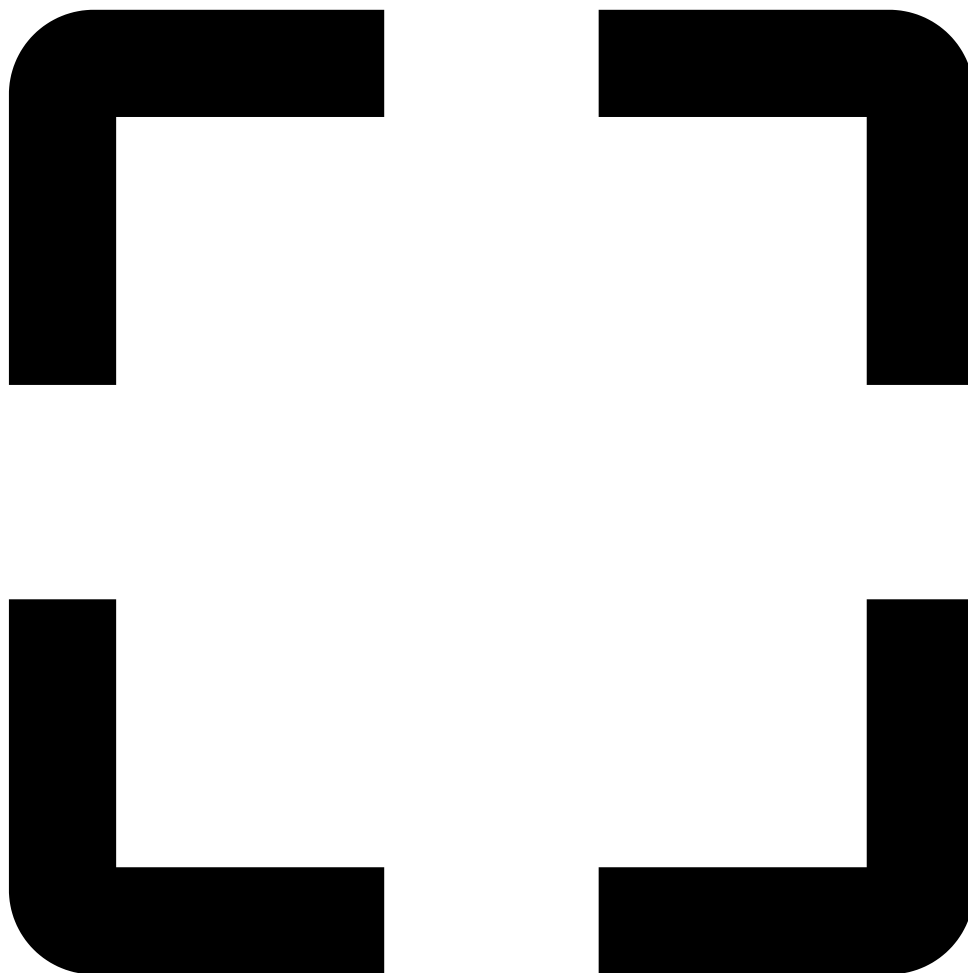
If a user running these outdated programs are redirected to the exploit kit landing page, the malicious scripts will attempt to exploit vulnerabilities in the browser to install a variety of malware including the Nemty 1.6 ransomware.

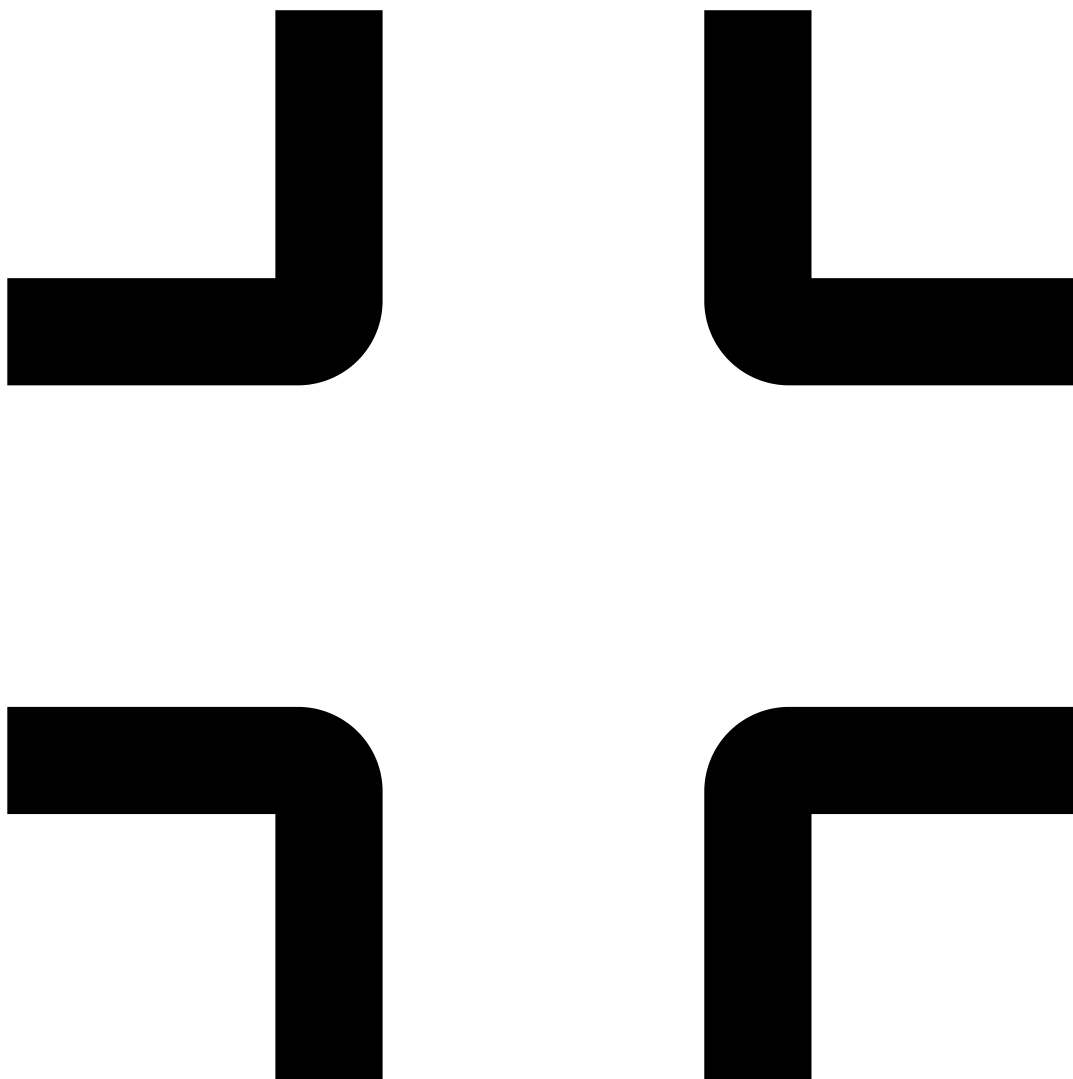




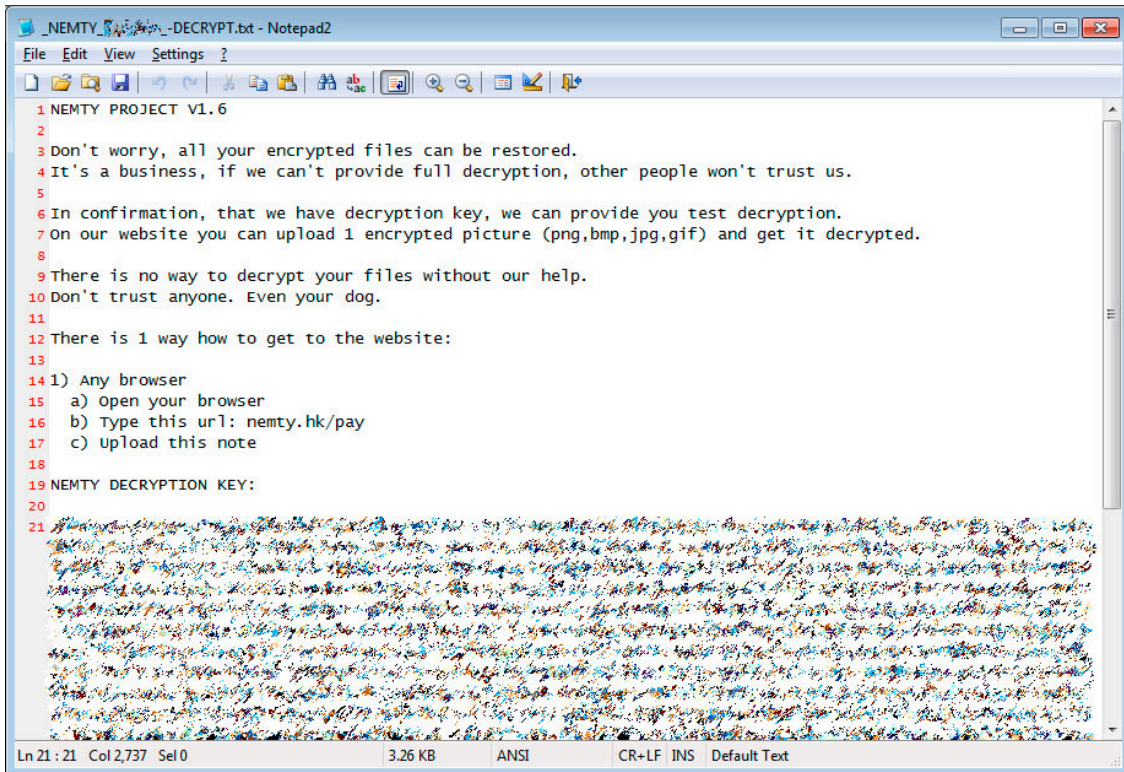


Visit Advertiser website [GO TO PAGE](#)





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



```
1 NEMTY PROJECT V1.6
2
3 Don't worry, all your encrypted files can be restored.
4 It's a business, if we can't provide full decryption, other people won't trust us.
5
6 In confirmation, that we have decryption key, we can provide you test decryption.
7 On our website you can upload 1 encrypted picture (png,bmp,jpg,gif) and get it decrypted.
8
9 There is no way to decrypt your files without our help.
10 Don't trust anyone. Even your dog.
11
12 There is 1 way how to get to the website:
13
14 1) Any browser
15   a) open your browser
16   b) Type this url: nemty.hk/pay
17   c) upload this note
18
19 NEMTY DECRYPTION KEY:
20
21 [Large block of encrypted text]
```

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.

The image is a promotional poster for the PICUS 2026 Summit. At the top, the word "PICUS" is written in a large, white, sans-serif font. Below it, "2026 SUMMIT" is written in a smaller, white font inside a dark red rectangular box. The main title, "AUTONOMOUS VALIDATION", is written in a very large, bold, pink font with a slight shadow effect. Below the title, the dates and times are listed: "12th May 1:00 PM EST | 14th May 10:00 AM BST". A prominent dark red button with the text "REGISTER NOW" in white is centered below the dates. At the bottom of the poster, there are six headshots of speakers, each with a logo underneath: Kraft Heinz, PICUS, Frost & Sullivan, Glow, Atlassian, and Hacker Valley.

[99% of What Mythos Found Is Still Unpatched.](#)

AI chained four zero-days into one exploit that bypassed both renderer and OS sandboxes. A wave of new exploits is coming.

At the Autonomous Validation Summit (May 12 & 14), see how autonomous, context-rich validation finds what's exploitable, proves controls hold, and closes the remediation loop.

[Claim Your Spot](#)

Source: <https://www.bleepingcomputer.com/news/security/nemty-16-ransomware-released-and-pushed-via-rig-exploit-kit/>