Nemty Ransomware Expands Its Reach, Also Delivered by Trik Botnet

By About the Author

The Nemty ransomware (Ransom.Nemty), initially detected in August 2019, has increased its reach by partnering up with the Trik botnet (Trojan.Wortrik), which now delivers Nemty to compromised computers.

Trik, also known as Phorpiex, has been around for approximately 10 years. In its early days, the malware self-propagated via removable USB drives, Windows Live Messenger, or Skype private messages. The criminals behind the botnet use the infected computers to send email spam and have been observed pushing out a wide range of malware families, with Nemty being the latest to join the list.

Nemty, meanwhile, first appeared on the scene in mid-August 2019. While the malware first appeared to be a run-of-the-mill ransomware, a constant series of changes to the threat made it apparent that it was very much a work in progress and something to be taken seriously.

In the past, Nemty has been observed being spread via the RIG exploit kit, as well as via malicious spam campaigns targeting users in Korea and China, where the malware is attached inside an archive.

Our data shows that most Nemty infections are found in Korea and China.

In early October, we noticed that Trik had begun distributing Nemty as a payload, adding another channel for the ransomware's delivery.

How Trik spreads Nemty using the SMB protocol

We observed a recent version of Trik delivering a tiny component that uses the Server Message Block (SMB) protocol and a list of hardcoded credentials to try to connect to remote computers with port 139 open.

First, the SMB component creates the following registry entry:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApp
[PATH OF THE ORIGINAL FILE]" = "[PATH OF THE ORIGINAL FILE]:*:Enabled: Windows NetBIOS Driver"

Trik then checks if the file **winsvcs.txt** is present or not in the **%AppData%** directory on the compromised computer. This file is present if the computer has previously been infected with Trik.

- If **winsvcs.txt** is not present, the Nemty ransomware is downloaded and executed. This check prevents Trik from being hindered by files on the computer being encrypted by Nemty.
- If **winsvcs.txt** is present, the SMB component checks if it is running as a service or not.
    - If it is not running as a service, the component tries to spread itself through the SMB protocol.

To find targets, the SMB component generates random IP addresses then tries to connect to them on port 139.

From analysing the malware's code, we can see that it skips the routine if the created IP address is a local one (Figure 4). The malware can infect public IP addresses with port 139 open that are using any of the common administrator usernames and passwords on its list.

Usernames: Administrator, administrator, Admin, admin

Passwords: 123, 1234, 12345, 123456, 1234567, 12345678, 123456789, 1234567890, 123123, 12321, 123321, 123abc, 123qwe, 123asd, 1234abcd, 1234qwer, 1q2w3e, a1b2c3, administrator, Administrator, admin, Admin, admin123, Admin123, admin12345, Admin12345, administrator123, Ad ministrator123, nimda, qwewq, qweewq, qwerty, qweasd, asdsa, asddsa, asdzxc, asdfgh, qweasdzxc, q1w2e3, qazwsx, qazwsxedc, zxcxz, zxccxz, zxcvb, zxcvbn, passwd, password, Password, login, Login, pass, mypass, mypassword, adminadmin, root, rootroot, test, testtest, temp, temptemp, foofoo, foobar, default, password1, password12, password123, admin1, admin12, admin123, pass1, pass12, pass123, root123, abc123, abcde, abcabc, qwe123, test123, temp123, sample, example, internet, Internet

If access is granted, the malware uses the SMB protocol to copy itself to the remote machine. It then uses the Windows Service Control Manager to start the SMB component's process on the remote machine. The sample running on the remote machine also checks for the presence of winsvcs.txt, which again determines whether or not Nemty is downloaded and executed.

Ransom.Nemty technical analysis

Other researchers have provided a detailed analysis of Nemty 1.0. However, during our analysis of Nemty 1.6, we noted some key updates compared to 1.0, which are listed here:

- Nemty 1.6 closes certain applications and stops services which may be using files which the ransomware would not be able to encrypt otherwise.
- Nemty 1.6 gains persistence by adding a scheduled task using the following command:

cmd.exe /c schtasks.exe /create /sc onstart /tn "NEMTY_<FILEID>_" /tr "C:\Users\user\AdobeUpdate.exe"

- It deletes shadow copies and backups before, rather than after (as 1.0 does), encryption.
- It adds two new exclusion folders: $RECYCLE.BIN and %AppData%.
- Version 1.6 stores its configuration file, file ID, and public key (RSA-2048) in the registry entry HKEY_CURRENT_USER/Software/NEMTY with the subkeys "cfg", "fid", and "pbkey" respectively.
- Finally, for 1.6, the malware authors decided to use Windows CryptoAPI instead of their custom AES-256 implementation which, as other researchers found, was non-standard and buggy. We also observed some discrepancy in the encryption algorithm while testing Nemty 1.0 (see Figure 9). The same issue was found in 1.6 (see Figure 10). We were unable to test the decryption because the URL the attackers listed for decryption verification was inaccessible.

The developers behind the Nemty ransomware are constantly updating and improving its code, as well as its delivery methods, in an attempt to reach more victims. The Trik botnet, itself known for adapting to the latest trends in order to stay relevant, makes a perfect partner in crime for Nemty.

Protection/Mitigation

Symantec has the following protection in place to protect customers against these attacks:

File-based protection

- Ransom.Nemty
- Trojan.Wortrik

Network-based protection (Intrusion Prevention System)

- System Infected: Ransom.Nemty Activity

Symantec Email Security.cloud technology blocks email spreading this threat using advanced heuristics.

Indicators of Compromise

Nemty

- 62c3b52b5310393dbf0590bc246161249632a1d2f21c3aa7fb779dc8018a0edf
- 5078a0940abc31a7fa271483ac345044a91a0e21c517bceb85091cd3fca310f7

Trik

- 0c77b260ee3fdd2754cd4f289efce709519aad34fa3cb84663655a6240e45973
- 1ab8feefd67f3706a42f996a3291d24a7ab2c5eb67d98236eb73995d587576ad
- 3ecb650c471d7c8291d084fffd634da0eddc9a473d29792d5033fe5fdcbf4ddd
- 64d187bed40d023e14d41b1a80d528f5c12dcf743fcb4de91530567d3244e09e
- 77689e7752470501d26cf8a5e2eb9b4e1ac372b27b2151268e0acf024e355f99
- 81dab2787f72997afb09fb98ada159f78c3e93f9d3fa83f844e580620d08322a
- 87fb207ae29baa300c2377625b745667a516e2243e1904ef81b4f7b97b5da1b0

- 9875c102bbe89ad636096efca6b04d6b843529eb9717d822f7b0b42a087c7332
- a0170a01e656cf7089a0d68a1803c3e2ba64ba8996c8eb5ffa8098940cb4c0ec
- b9b4511065cb56bd162e143c22cf2afe32e3ee6617ba5a4852182cb0781f18f1
- c6f43bedad8b0c3f60d71a2a6c1fab297e144483f17deeb5150bdbe6c73755a4
- d746e41e18bb637062881aca207186dc3d005e79c857e025f89ce2a1b3e52ecf
- d9edee0541b9a5baf2cb2b1915aef1d034efd4edd4b3c030b508669da1e2aaf2
- db627ff946ff64910cf909c81ae51294c4bb6477ee2c620aae1d0f7a7208b6b5
- f4909c420e208e4728116e8b0f4254c9f741d864f9618cddbe3f51b71f602066
- fa2993f2455971244350178008cc671fb739b53d79b594c80e69047421ce1666

Trik SMB component

- bf480a5862210b9e033f270379bb95c1d1fadd16bf0d21db5bfbc9268ae595ac

---