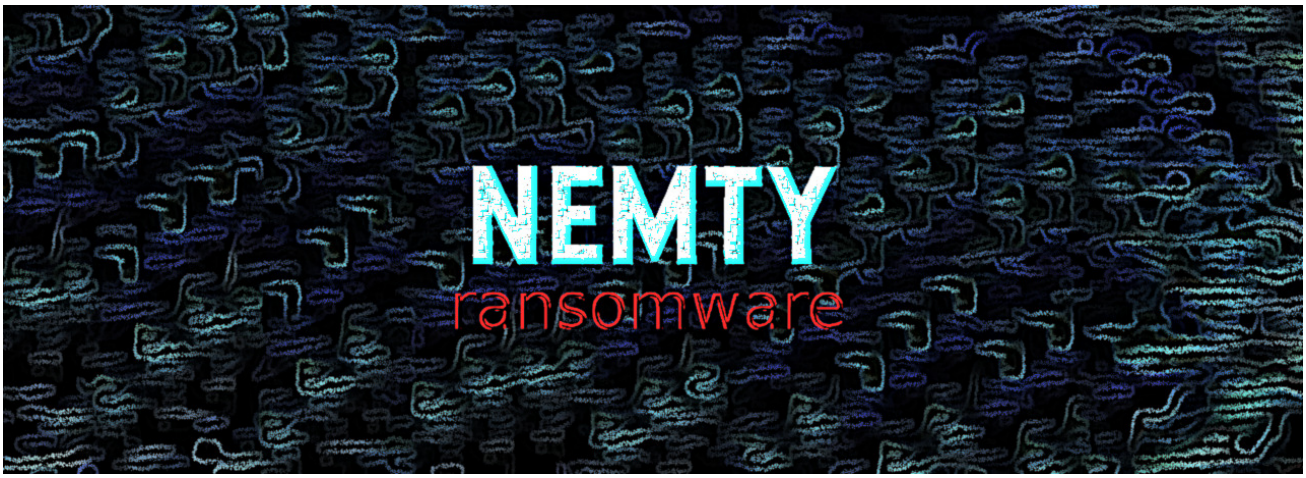
New Nemty Ransomware May Spread via Compromised RDP Connections

bleepingcomputer.com/news/security/new-nemty-ransomware-may-spread-via-compromised-rdp-connections/

Ionut Ilascu

By
Ionut Ilascu

- August 26, 2019
- 03:29 AM
- 0



A new ransomware has been spotted over the weekend, carrying references to the Russian president and antivirus software. The researchers call it Nemty.

This is the first version of Nemty ransomware, named so after the extension it adds to the files following the encryption process.

The ransom demand

Like any proper file-encrypting malware, Nemty will delete the shadow copies for the files it processes, taking away from the victim the possibility to recover versions of the data as created by the Windows operating system.

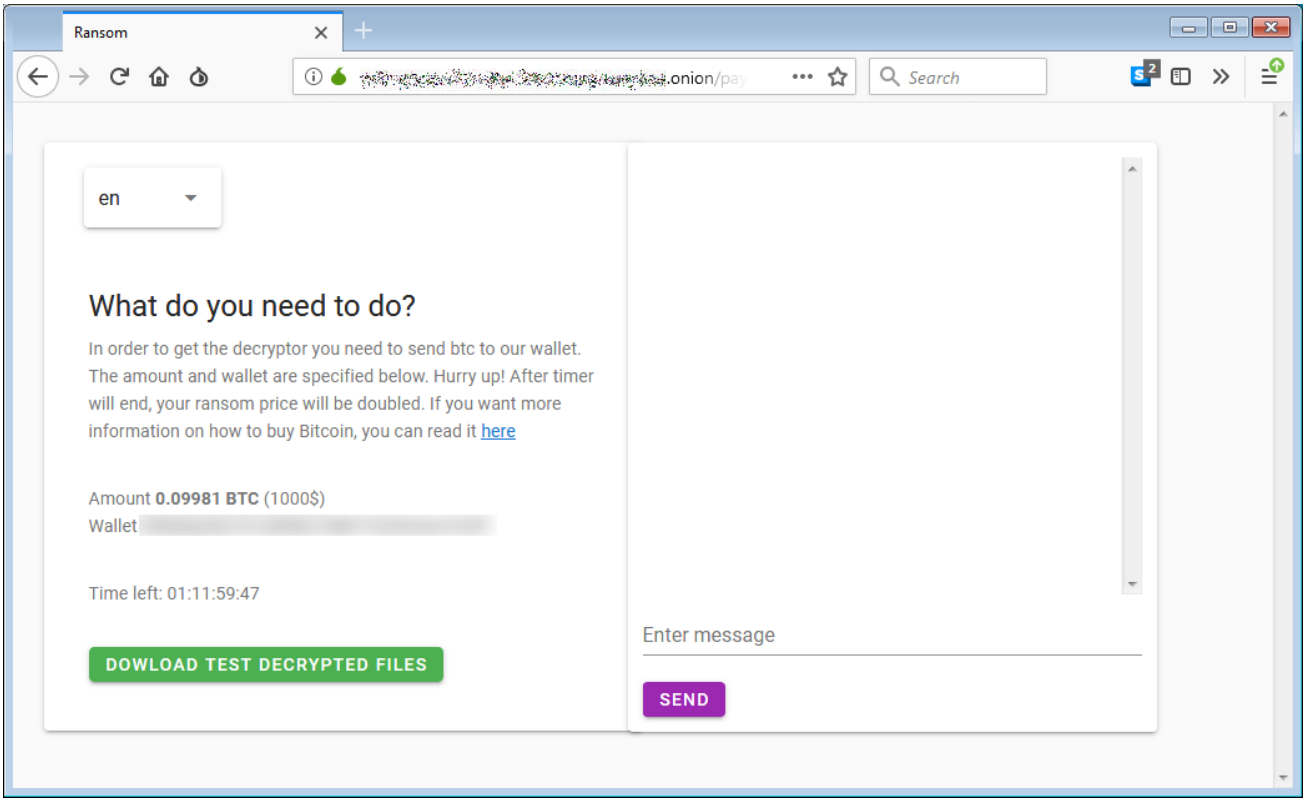
Victims will see a ransom note informing that the attackers hold the decryption key and that data is recoverable for a price.

```
 ---=== NEMTY PROJECT ===---

[+] Whats Happen? [+]

Your files are encrypted, and currently unavailable. You can check it: all files on you computer has extension .nemty
By the way, everything is possible to restore, but you need to follow our instructions. Otherwise, you cant return your data (NEVER).

[+] What guarantees? [+]

It's just a business. We absolutely do not care about you and your deals, except getting benefits.
If we do not do our work and liabilities - nobody will not cooperate with us.
It's not in our interests.
If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data, cause just we have the private key.
In practise - time is much more valuable than money.

[+] How to get access on website? [+]

  1) Download and install TOR browser from this site: https://torproject.org/
  2) Open our website: zjoxyw5mkacojk5ptn2iprkivg5clow72mjkyk5ttubzxprjjnwapkad.onion/pay

When you open our website, follow the instructions and you will get your files back.
```

In BleepingComputer's tests, the ransom demand was 0.09981 BTC, which converts to around $1,000 at the moment.

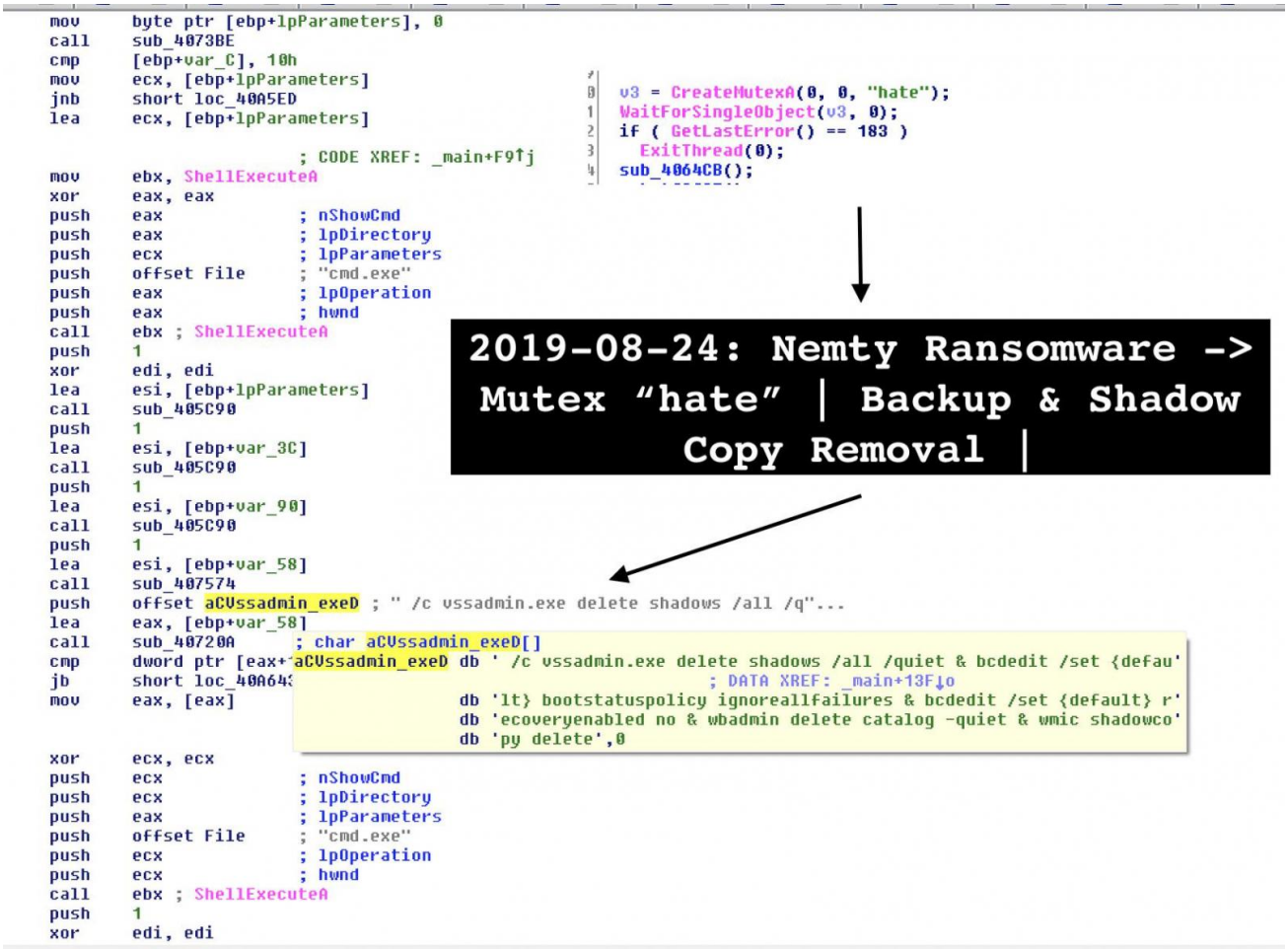
The payment portal is hosted on the Tor network for anonymity, and users have to upload their configuration file.

Based on this, they are provided with the link to another website that comes with a chat function and more information on the demands.



Messages in the code

Security researcher Vitali Kremez took a closer look at the malware and noticed that it comes with an unusual name for the mutex object. The author called it "hate," as visible in the image below.



A mutually exclusive (mutex) object is a flag that allows programs to control resources by allowing access to them to one execution thread at a time.

Another weird thing Kremez noticed in Nemty's code is a link to this picture of Vladimir Putin, with a caption saying "I added you to the list of [insult], but only with pencil for now."

The list of peculiarities does not stop at this. A straight message to the antivirus industry was spotted by the researcher.

At first, the reference seemed an odd thing in the code but a second look at how Nemty worked revealed that it was the key for decoding base64 strings and create URLs is a straight message to the antivirus industry.

```
  v19 = *(_DWORD *)"fuckav";
  v20 = *(_WORD *)"av";
  v7 = 0;
  v21 = aFuckav[6];
  memset(&v22, 0, 0x79u);
  v8 = pszString;
  pcbBinary = 0;
  if ( (unsigned int)a7 < 0x10 )
    v8 = (const CHAR *)&pszString;
  if ( !CryptStringToBinaryA(v8, cchString, 1u, 0, &pcbBinary, 0, 0) )
    goto LABEL_16;
  v9 = (BYTE *)malloc(pcbBinary);
  if ( !v9 )
    goto LABEL_16;
  v10 = pszString;
  if ( (unsigned int)a7 < 0x10 )
    v10 = (const CHAR *)&pszString;
  if ( !CryptStringToBinaryA(v10, cchString, 1u, v9, &pcbBinary, 0, 0) )
LABEL_16:
    ExitThread(0);
  v11 = malloc(0x408u);
  v12 = v11;
  v13 = sub_40A72C((int)v11, (int)&v19);
  sub_40A787(v13, (int)v9, pcbBinary);
  *(_DWORD *)(a1 + 20) = 15;
  *(_DWORD *)(a1 + 16) = 0;
  *(_BYTE *)a1 = 0;
  sub_40720A((int)&v17, (char *)v9);
  free(v12);
  free(v9);
  if ( pcbBinary > 0 )
  {
    do
    {
      v14 = v17;
      if ( v18 < 0x10 )
        v14 = (int *)&v17;
      sub_40A493(*((_BYTE *)v14 + v7++));
    }
    while ( v7 < pcbBinary );
  }
  sub_405C90(0, (int)&v17, 1);
  sub_405C90(0, (int)&pszString, 1);
```

Another interesting thing is a verification Nemty makes to identify computers in Russia, Belarus, Kazakhstan, Tajikistan, and Ukraine. This is not to exempt the hosts from the file encryption routine, though, Kremez told BleepingComputer.

The "isRU" check in the malware code simply marks the systems as being in one of the five countries and then sends to the attacker data that includes the computer name, username, operating system, and computer ID.

```
int sub_408958()
{
  const char *v0; // esi@5

  if ( (unsigned __int8)sub_407FDB("Russia")
    || (unsigned __int8)sub_407FDB("Belarus")
    || (unsigned __int8)sub_407FDB("Kazakhstan")
    || (unsigned __int8)sub_407FDB("Tajikistan")
    || (v0 = "false", (unsigned __int8)sub_407FDB("Ukraine")) )
  {
    v0 = "true";
  }
  strlen(v0);
  return sub_4075B4((void *)v0);
}
```

2019-08-24: Nemty Ransomware -> 'isRu' check true/false set

It's unclear how Nemty is distributed but Kremez heard from a reliable source that the operators deploy it via compromised remote desktop connections.

Compared to phishing email, which is currently the common distribution method, leveraging a RDP connection puts the attacker in control as they no longer have to wait for the victim to take the phishing bait.

Kremez published his research notes on Nemty where he includes the list of folders (anything needed for booting the OS) and the file extensions (binaries, shortcuts, and log data) the malware does not touch.

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

- Nemty Ransomware
- Ransomware

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

You may also like: