New Anatova Ransomware Supports Modules for Extra Functionality

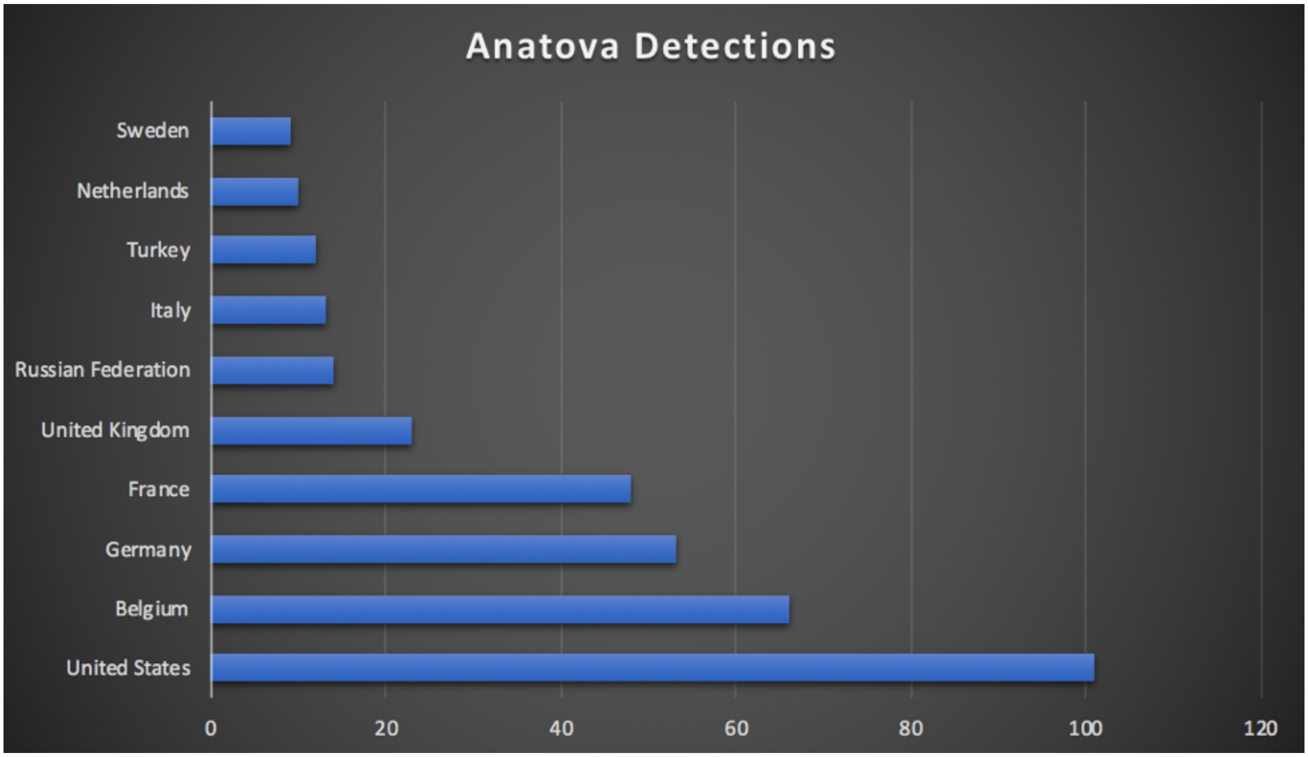
Ionut Ilascu

By
Ionut Ilascu

- January 23, 2019
- 06:02 AM
- 0

A new ransomware family popped on the radar of analysts, who see it as a serious threat created by skilled authors that can turn it into a multifunctional piece of malware.

Infections with Anatova have been reported all over the world, most of them being in the United States, followed by countries in Europe (Belgium, Germany, France, the UK).



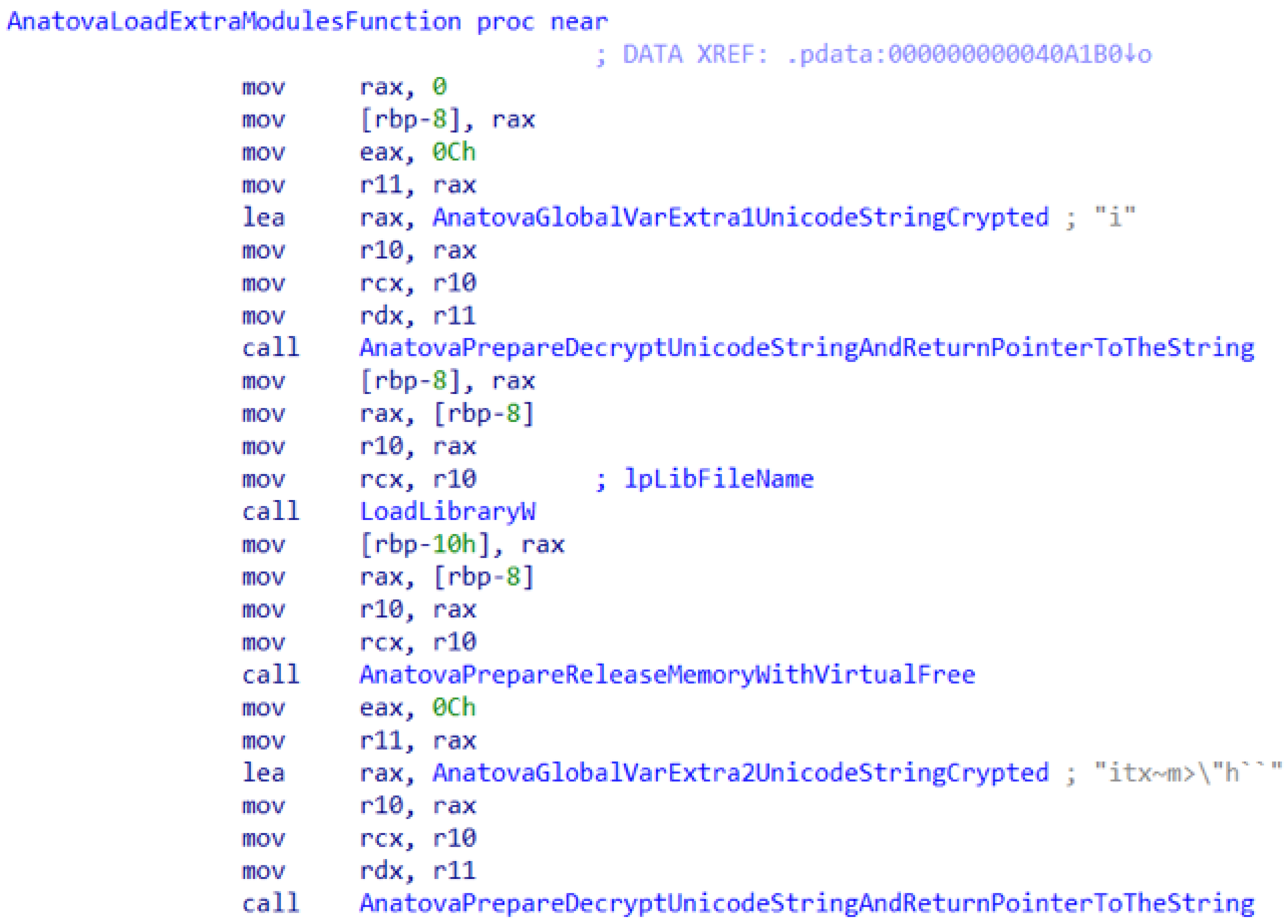
The ransomware includes an anti-analysis routine that gets triggered under certain conditions. Once launched, the ransomware asks for admin privileges, runs a few checks and then encrypts files on the computer and then demands 10 DASH coins, currently valued at $700.

Modular architecture

Malware researchers from McAfee discovered Anatova in a private peer-to-peer network where it uses an icon for a game or an application to lure users into downloading it.

They found that the new ransomware comes with support for additional modules that could extend its capabilities, allowing it to become an all-in-one malware tool.

The clue pointing to this possibility was a flag whose value determined the loading of two DLL files named 'extra1.dll' and 'extra2.dll.' "This might indicate that Anatova is prepared to be modular or to be extended with more functions in the near future," the researchers say in a report.



```
AnatovaLoadExtraModulesFunction proc near
                                        ; DATA XREF: .pdata:000000000040A1B0↓o
                mov     rax, 0
                mov     [rbp-8], rax
                mov     eax, 0Ch
                mov     r11, rax
                lea     rax, AnatovaGlobalVarExtra1UnicodeStringCrypted ; "i"
                mov     r10, rax
                mov     rcx, r10
                mov     rdx, r11
                call    AnatovaPrepareDecryptUnicodeStringAndReturnPointerToTheString
                mov     [rbp-8], rax
                mov     rax, [rbp-8]
                mov     r10, rax
                mov     rcx, r10        ; lpLibFileName
                call    LoadLibraryW
                mov     [rbp-10h], rax
                mov     rax, [rbp-8]
                mov     r10, rax
                mov     rcx, r10
                call    AnatovaPrepareReleaseMemoryWithVirtualFree
                mov     eax, 0Ch
                mov     r11, rax
                lea     rax, AnatovaGlobalVarExtra2UnicodeStringCrypted ; "itx~m>\"h``"
                mov     r10, rax
                mov     rcx, r10
                mov     rdx, r11
                call    AnatovaPrepareDecryptUnicodeStringAndReturnPointerToTheString
```

By making Anatova modular, its authors could use it to include all sorts of capabilities that would take priority before running the file encryption routine. They could collect sensitive information, plant a backdoor, or other types of nasties.

Anti-analysis process

Anatova tried to make the ransomware more resilient to analysis attempts by embedding a memory cleaning procedure that activates in certain situations.

Among the first actions it takes is to check the username of the logged in user. If the name is a match with one on an internal list, the ransomware deploys the cleaning process and exits.

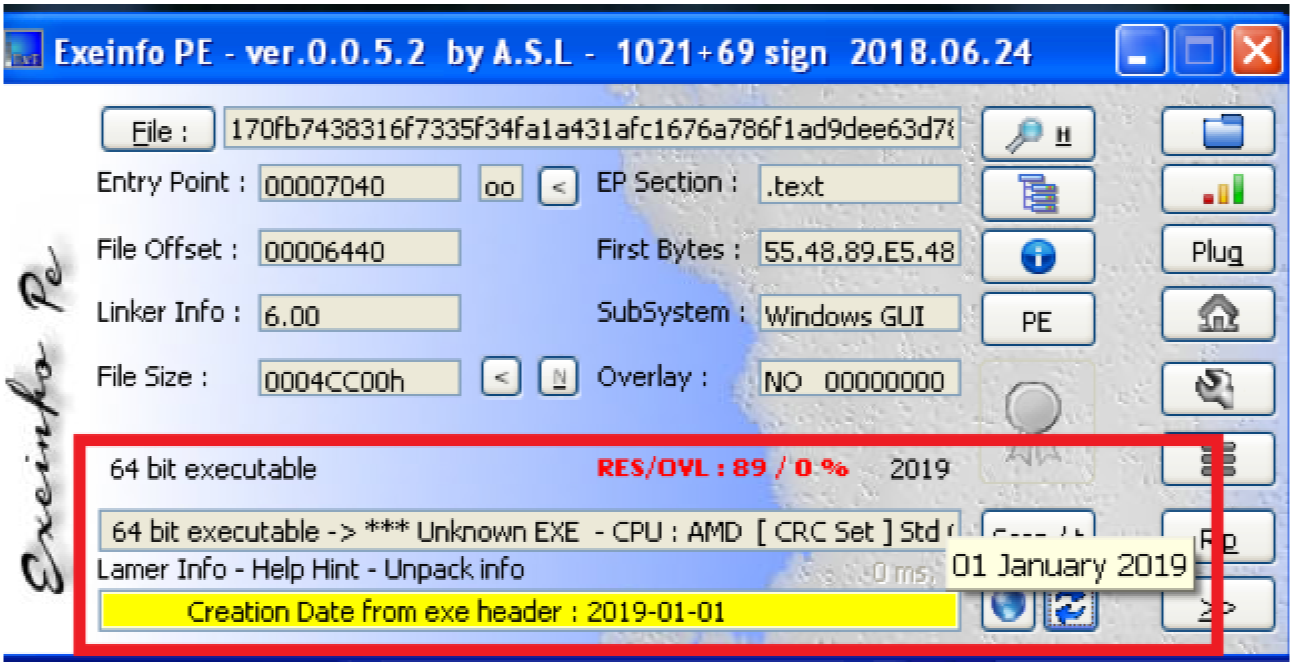
Although the list of names Anatova checks is short, it may protect it from being checked by less careful malware analysts.

It includes the following strings: 'LaVirulera,' 'tester,' 'Tester,' 'analyst,' 'Analyst,' 'lab,' 'Lab,' 'Malware,' and 'malware.'

According to McAfee, these names are the default choices when setting up a virtual machine or a sandbox environment or they are regularly used by some malware analysts.

Additional protection techniques are encrypting most of the strings and using different keys for decrypting them and heavy reliance on dynamic calls.

Anatova seems to be a new player on the ransomware market, as the analyzed sample came with a compilation date of January 1, 2019.



Exeinfo PE - ver.0.0.5.2 by A.S.L - 1021+69 sign 2018.06.24

File : 170fb7438316f7335f34fa1a431afc1676a786f1ad9dee63d7

Entry Point : 00007040 oo < EP Section : .text

File Offset : 00006440 First Bytes : 55.48.89.E5.48

Linker Info : 6.00 SubSystem : Windows GUI

File Size : 0004CC00h < N Overlay : NO 00000000

64 bit executable RES/OVL : 89 / 0 % 2019

64 bit executable -> *** Unknown EXE - CPU : AMD [CRC Set] Std (

Lamer Info - Help Hint - Unpack info 0 ms.

Creation Date from exe header : 2019-01-01

01 January 2019

The ransomware packs quite a punch for a package of just 32KB, excluding resources. It encrypts files using the Salsa20 algorithm and extends this process to available network-shares.

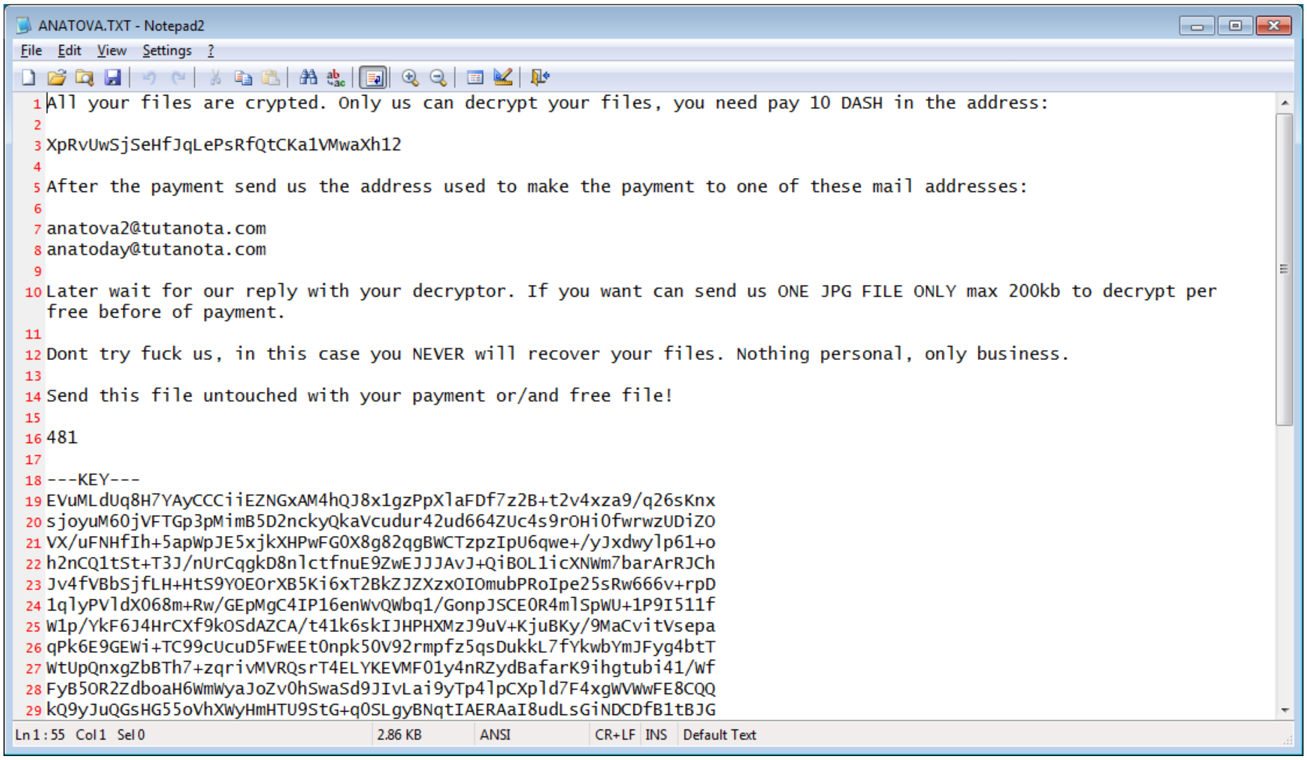
To eliminate file recovery possibilities from the infected machine, Anatova destroys the Volume Shadow copies ten times in a row. For this, it uses the 'vssadmin' utility, which needs admin rights.

Encrypted files get no special extension

To make the encryption process quick, Anatova targets files that are 1MB in size or smaller. This procedure avoids critical directories and files and does not result in files with a different extension.

"By setting pointers at the end of the encrypted files, Anatova makes sure that it does not encrypt files that are already encrypted," explain the researchers.

Unlike other ransomware pieces, this one adds the ransom note only to folders where it encrypted at least one file. Also, it will not overwrite an existing note, most likely to save time.



```
All your files are crypted. Only us can decrypt your files, you need pay 10 DASH in the address:

XpRvUwSjSeHfJqLePsRfQtCKa1VMwaXh12

After the payment send us the address used to make the payment to one of these mail addresses:

anatova2@tutanota.com
anatoday@tutanota.com

Later wait for our reply with your decryptor. If you want can send us ONE JPG FILE ONLY max 200kb to decrypt per
free before of payment.

Dont try fuck us, in this case you NEVER will recover your files. Nothing personal, only business.

Send this file untouched with your payment or/and free file!

481

---KEY---
EVuMLdUq8H7YAyCCCiiEZNGxAM4hQJ8x1gzPpXlaFDf7z2B+t2v4xza9/q26sKnx
sjoyuM60jVFTGp3pMimB5D2nckyQkaVcudur42ud664ZUc4s9rOHiOfwrwzUDiZO
VX/uFNHfIh+5apWpJE5xjkXHPwFGOX8g82qgBWCTzpzIpU6qwe+/yJxdwylp61+o
h2nCQ1tSt+T3J/nUrCqgkD8nlctfnuE9ZwEJJJAvJ+QiBOL1icXNWm7barArRJCh
Jv4fVBbSjfLH+HtS9YOEOrXB5Ki6xT2BkZJZXzxOIOmubPRoIpe25sRw666v+rpD
1qlyPVldX068m+Rw/GEpMgC4IP16enWvQWbq1/GonpJSCE0R4mlSpWU+1P9I511f
W1p/YkF6J4HrCXf9kOSdAZCA/t41k6skIJHPHXMzJ9uV+KjuBKy/9MaCvitVsepa
qPk6E9GEWi+TC99cUcuD5FwEEt0npk50V92rmpfz5qsDukkL7fYkwbYmJFyg4btT
WtUpQnxgZbBTh7+zqrivMVRQsrT4ELYKEVMF01y4nRZydBafarK9ihgtubi41/Wf
FyB5OR2ZdboaH6WmWyaJoZv0hSwaSd9JIvLai9yTp4lpCXpld7F4xgWVWwFE8CQQ
kQ9yJuQGsHG55oVhXWyHmHTU9StG+q0SLgyBNqtIAERAaI8udLsGiNDCDfB1tBJG
```

One peculiarity Lawrence Abrams of BleepingComputer observed while testing the ransomware multiple times was that it crashed Windows File Explorer.

Anatova could prove to be a next step in the evolution of the ransomware threat by incorporating functions that take advantage of the full spectrum of monetization possibilities. This way, even if the victim does not pay the ransom, the criminals will still be able to make some money by stealing private and sensitive information, or selling access to the compromised station.

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: