Product Solutions Resources Open Source Enterprise Pricing Sign in Sign up

albertzsigovits / malware-notes Public

Notifications Fork 8 Star 58

Code Issues Pull requests Actions Projects Security Insights

Files

c820c7f

Go to file

- Ransomware-Linux-Lockbit
- Ransomware-Windows-LockBit-v3
- Ransomware-Windows-Yanluowa...
- Ransomware
  - Afrodita.md
  - Antefrigus.md
  - Clop.md
  - DeathRansom.md
  - Lockbit.md
  - Mamo434376.md
  - Maze.md
  - Nemty.md
  - Ouroboros.md
  - PureLocker.md
  - Robbinhood.md
  - Snake.md
  - Snatch.md
  - _ransom_cmd.md
  - _ransom_notes.md
  - _ransomware.yara
- Stealer-Windows-Krown
- .DS_Store
- .gitignore

malware-notes / Ransomware / Maze.md

albertzsigovits Merge branch 'master' of https://github.com/albe... 26657b3 · 4 years ago History

Preview Code Blame 98 lines (93 loc) · 4.69 KB Raw

Maze ransomware

SHA256 hashes

04e22ab46a8d5dc5fea6c41ea6fdc913b793a4e33df8f0bc1868b72b180c0e6e
067f1b8f1e0b2bfe286f5169e17834e8cf7f4266b8d97f28ea78995dc81b0e7b
153defee225de889d2ac66605f391f4aeaa8b867b4093c686941e64d0d245a57
195ef8cfabc2e877ebb1a60a19850c714fb0a477592b0a8d61d88f0f96be5de9
19713e7ae529091a995effe4e7271f2c23487c594af0a39cd4335d95e0abc99d
58fe9776f33628fd965d1bcc442ec8dc5bfae0c648dcaec400f6090633484806
5c9b7224ffd2029b6ce7b82ea40d63b9d4e4f502169bc91de88b4ea577f52353
6a22220c0fe5f578da11ce22945b63d93172b75452996defdc2ff48756bde6af
7c03b49d24c948f838b737fb476d57849a1fd6b205f94214bf2a5a3b7a36f17a
806fc33650b7ec35dd01a06be3037674ae3cc0db6ba1e3f690ee9ba9403c0627
822a264191230f753546407a823c6993e1a83a83a75fa36071a874318893afb8
91514e6be3f581a77daa79e2a4905dcbdf6bdcc32ee0f713599a94d453a26fc1
9e88e833d1309fe1417628519851f74cffafa51ea8a65bbd7f0433c9d9be196a
a9da834206c24147866c3281c0ba898fb0d162fd9f87453df4c1674aaed45df7
c040defb9c90074b489857f328d3e0040ac0ddab26cde132f17cccae7f1309cc
e8a091a84dd2ea7ee429135ff48e9f48f7787637ccb79f6c3eb42f34588bc684
ebbb5ac2be538edff5560ef74b996a3fbc3589b3063074c5037da05acd6374d2
fc611f9d09f645f31c4a77a27b6e6b1aec74db916d0712bef5bce052d12c971f

References

https://twitter.com/VK_Intel/status/1189431136398794752
https://twitter.com/VK_Intel/status/1186346215388131333
https://twitter.com/VK_Intel/status/1185255932474904576
https://twitter.com/MalwareTechBlog/status/1184926173861572608
http://mazenews.top

Notes

- Maze Team maintains a site: `mazenews.top`
- Ransom note file: `DECRYPT-FILES.txt`
- Checks AV software: `Select * From AntiVirusProduct` via `root\SecurityCenter2`
- Check shadow copies: `select * from Win32_ShadowCopy` via `ROOT\cimv2`
- Used User-Agent in C2 traffic: `User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; AS; rv:11.0) like Gecko`
- Seen pdbs:
- `C:\random\fucking\path\to\fucking\idiotic\nonexisting\file\with\pdb\extension.pdb`
- `C:\vc5\Release\Zeroaccess.pdb`

- `C:\shit\gavno.pdb`
- `C:\demonslay335\emsisoft_work\ransomware\hutchins.pdb`
- Mutex is randomly generated: `Global\c35e0a1a78e8cdbc`
- Same string used as `c35e0a1a78e8cdbc.tmp` on the file system
- Shadow copy deletion: wmic `"%s" shadowcopy delete` via `Win32_ShadowCopy.ID='%s'`

VT searches

- imphash:"4c3d146415a27e5b2b768097598f2851"
- imphash:"a0667aaff29d40b151e423bcd42d1e15"
- imphash:"e6c2e529c8b3c790ab91901a5172e552"
- resource:"0cad26ce9da0bb3e380866e27c5f5ad17bb2f363352105f42b3dc1e9086c9366"
- resource:"884d4eddb1c544532c4225419e319749700b5503503e707f86b1cae740bc4c18"
- resource:"a4d658476e4693a873db1a349aa5ca0238c1df1708d5e67ed0f0187784d7336d"

Yara rules

```
rule maze_caro
{
  condition:
    new_file and signatures matches /.*Ransom.*Maze.*/
}
```

Ransom note

```
Attention!
----------------------------
| What happened?
----------------------------
All your files, documents, photos, databases, and other important data a
You cannot access the files right now. But do not worry. You have a chan
----------------------------
| How to get my files back?
----------------------------
The only method to restore your files is to purchase a unique for you pr
To contact us and purchase the key you have to visit our website in a hi
There are general 2 ways to reach us:
1) [Recommended] Using hidden TOR network.
  a) Download a special TOR browser: https://www.torproject.org/
  b) Install the TOR Browser.
  c) Open the TOR Browser.
  d) Open our website in the TOR browser: http://aoacugmutagkwctu.onion/
  e) Follow the instructions on this page.
2) If you have any problems connecting or using TOR network
  a) Open our website: https://mazedecrypt.top/%USERID%
  b) Follow the instructions on this page.
Warning: the second (2) method can be blocked in some countries. That is
On this page, you will see instructions on how to make a free decryption
Also it has a live chat with our operators and support team.
----------------------------
| What about guarantees?
----------------------------
We understand your stress and worry.
So you have a FREE opportunity to test a service by instantly decrypting
If you have any problems our friendly support team is always here to ass
-------------------------------------------------------------------------
THIS IS A SPECIAL BLOCK WITH A PERSONAL AND CONFIDENTIAL INFORMATION! DO
---BEGIN MAZE KEY---
%base64key%
---END MAZE KEY---
```