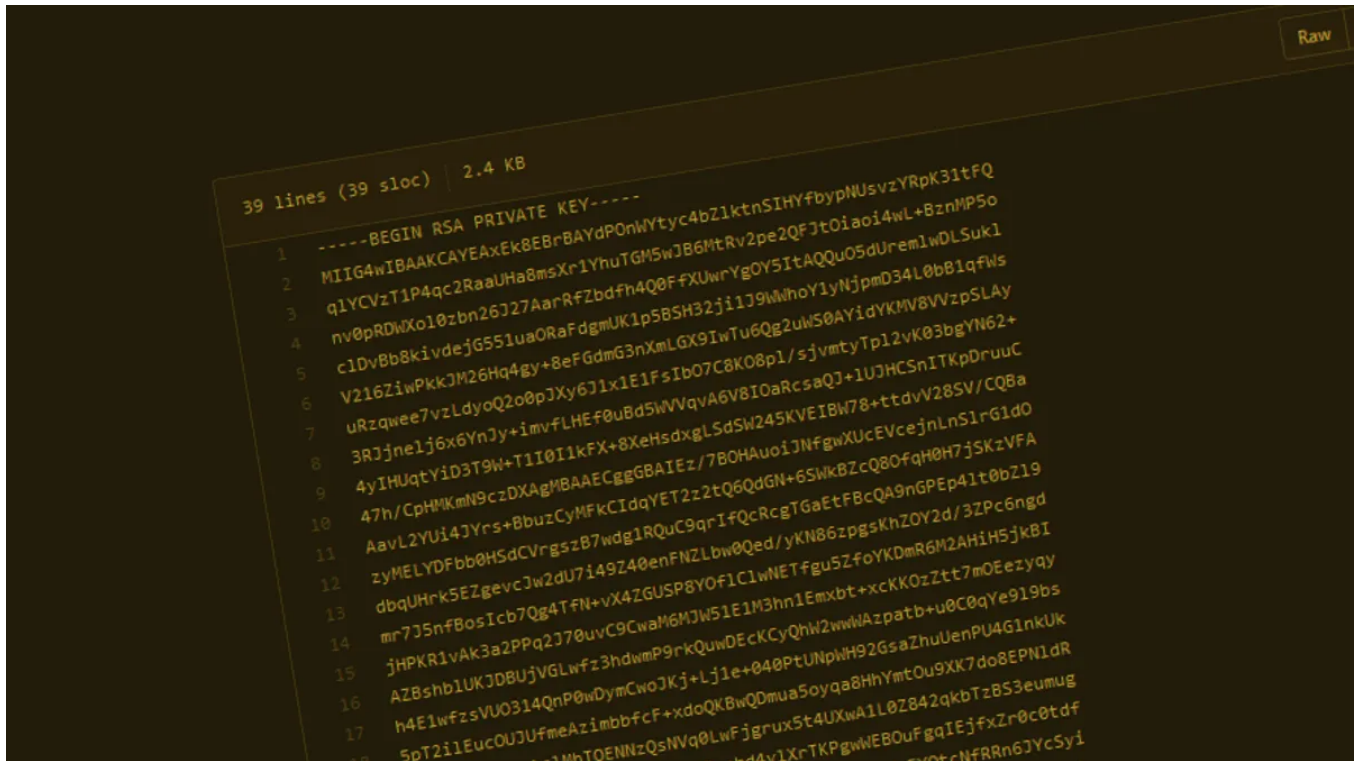


Shade (Troidesh) ransomware shuts down and releases decryption keys

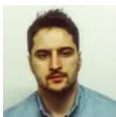
zdnet.com/article/shade-troidesh-ransomware-shuts-down-and-releases-all-decryption-keys/



```
39 lines (39 sloc) | 2.4 KB
-----BEGIN RSA PRIVATE KEY-----
1  MIIG4wIBAAKCAYEAXEk8EBRBAyDPOhWYtyc4bZ1ktnSIHYfbyPNUsvzYRpK31tFQ
2  q1YCVzT1P4qc2RaaUHa8msXr1YhuTGM5wJB6MtRv2pe2QFJtOiaoi4wL+BznMP5o
3  nv0pRDwXo10zbn26J27AarRfZbdfn4Q0FfXUwrYgOY5ItAQQu05dUrem1wDLSuk1
4  c1DvBb8kiVdeJG551uaORaFdgMUK1p5B5H32ji1J9wWhoY1yNjpmD34L0bB1qfws
5  V216ZiWpkkJM26Hq4gy+8eFGdmG3nXmLGX9IwTu6Qg2uW50AYidYKMW8VzpsLAY
6  uRzqwee7vzLdYoQ2o8pJXy6J1x1E1FsIb07C8K08pl/sjvmtYTp12vK03bgYN62+
7  3RjJne1j6x6YnJy+imvFLHEf0uBd5WVvQVA6V8IOaRcsaQJ+1UJHCSnITKpDruuC
8  4yIHUqtYiD3T9W+T1I0I1kFX+8XeHsdXgLSdSW245KVEIBW78+ttDvV28SV/CQ8a
9  47h/CpHMkMn9czDXAgMBAACEggGBAIEz/7BOHAuoijNfgwXUCeVcejnLnS1rG1d0
10 AavL2YU14JYrs+8buzCyMfKCIIdqYET2z2tQ6QdGN+6SWkBZcQ80FqH0H7jSKzVFA
11 zyMELYDFbb0HSdCVrgszB7wdg1RQuC9qrIfQcRcgTGaEtFBcQA9nGPEp41t0bZ19
12 dbqUhrk5EZgevcJw2dU7i49Z40enFNZLbw0Qed/yKN86zpgsKhZOY2d/3ZPc6ngd
13 mr7J5nfBosIcb7Qg4TFN+vX4ZGUSP8YOf1ClwNETfgu5ZfoYKDMR6M2AHiH5jkbI
14 jHPKR1vAk3a2PPq2J70uvC9CwaM6MJW51E1M3hn1Emxht+xcKK0zZtt7m0Ezyqy
15 AZBshb1UKJDBUjVGLwFz3hdwmP9rkQuwDEcKCyQhW2wwWAZpatb+u0C0qYe919bs
16 h4E1wFzsVU0314QnP0wDymCwoJKj+Lj1e+040PtUNpWH92GsaZhuUenPU4G1nkUk
17 5pT2i1EucOUJUfmeAzimbbfcF+xdoQKBwQDmua5oyqa8HhYmtOu9XK7do8EPN1dR
  ...
```

Home Innovation Security

The Shade ransomware gang have published more than 750,000 decryption keys on GitHub. Kaspersky is working on a decryption app.



Written by [Catalin Cimpanu](#), Contributor on April 27, 2020

-
-
-
-
-

shade-keys.png

Image: ZDNet

The operators of the [Shade \(Troldeh\) ransomware](#) have shut down over the weekend and, as a sign of goodwill, have released more than 750,000 decryption keys that past victims can now use to decrypt their files.

Security researchers from Kaspersky Lab have [confirmed](#) the validity of the leaked keys and have released a [free decryption tool](#).

In a short message posted in a [GitHub repository](#), the Shade team explained what led to their decision.

We are the team which created a trojan-encryptor mostly known as Shade, Troldeh or Encoder.858. In fact, we stopped its distribution in the end of 2019. Now we made a decision to put the last point in this story and to publish all the decryption keys we have (over 750 thousands at all). We are also publishing our decryption soft; we also hope that, having the keys, antivirus companies will issue their own more user-friendly decryption tools. All other data related to our activity (including the source codes of the trojan) was irrevocably destroyed. We apologize to all the victims of the trojan and hope that the keys we published will help them to recover their data.

While the Shade gang explained why they released the decryption keys, they did not explain why they shut down. Several theories have started to form among ransomware experts, yet none are based on actual tangible threat intelligence.

Prior to shutting down at the end of 2019, the Shade ransomware has been one of the oldest ransomware strains, being first spotted in 2014 and operating almost non-stop until it shut down last year.

It was also one of the most most active ransomware operations [1, 2], being distributed via a combination of email spam campaigns and exploit kits.

The ransomware wasn't perfect, though, and during its lifetime, security researchers from Kaspersky and Intel Security (now McAfee) have released [multiple decryption apps](#) that could help victims recover files. However, the decrypters only worked against a small number of Shade versions, and the last of these tools was released in 2017.

The decryption keys released today will help all users who had files encrypted by the Shade ransomware. The keys are believed to account for all versions of the ransomware and all users who ever got infected.

The only condition is that users still have the encrypted files laying around, so they can be decrypted.

While security experts often recommend saving ransomware-encrypted files on an offline hard drive, most victims simply reinstall their computer from scratch, deleting the encrypted data. Those who saved their encrypted files can now recover data they once considered lost.

Updated on May 1 with a link to Kaspersky's free decryption tool.

The FBI's most wanted cybercriminals
