

勒索病毒肆虐, 防范和应对措施必不可少

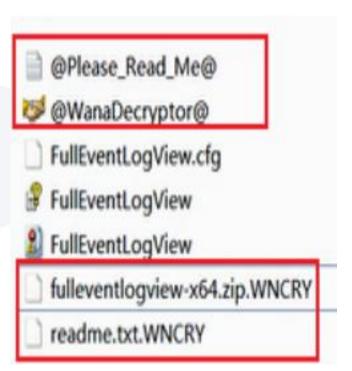
# 目录

- 一、勒索病毒介绍
- 二、勒索病毒种类



## 一、勒索病毒介绍

- (1) 勒索病毒是伴随数字货币兴起的一种新型病毒木马。
- (2)一旦遭受勒索病毒攻击,介绍系统绝大多数文件被加密,并添加一个特殊的后缀。
- (3)黑客向受害用户勒索高昂的赎金,赎金通常通过数字货币支付。
- (4)大家知道最早的勒索病毒是什么时候出现的吗?





## 二、勒索病毒种类

## (1)、加密类勒索病毒

WannaCry





## (2)、系统锁定类勒索病毒

#### petya

Repairing file system on C:

The type of the file system is NTFS. One of your disks contains errors and needs to be repaired. This process may take several hours to complete. It is strongly recommended to let it complete.

WARNING: DO NOT TURN OFF YOUR PC! IF YOU ABORT THIS PROCESS, YOU COULD DESTROY ALL OF YOUR DATA! PLEASE ENSURE THAT YOUR POWER CABLE IS PLUGGED IN!

CHKDSK is repairing sector 19282 of 94720 (20%)

You became victim of the PETYA RANSOMWARE!

The harddisks of your computer have been encrypted with an military grade encryption algorithm. There is no way to restore your data without a special key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy steps:

- 1. Download the Tor Browser at "https://ыны.torproject.org/". If you need help, please google for "access onion page".
- 2. Visit one of the following pages with the Tor Browser:

http://petya37h5tbhyvki.onion/72Shng http://petya5koahtsf7sv.onion/72Shng

3. Enter your personal decryption code there:



If you already purchased your key, please enter it below.

key: \_



## (3)、数据窃取类勒索病毒

### Conti REvil

Happy Blog Auction (new)

Blog search

#### Acer Inc.



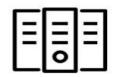
Acer.com - is a Taiwanese multinational hardware and electronics corporation specializing in advanced electronics technic headquartered in Xirhi, New Taipei City. Its products include desktop PCs, laptop PCs tablets, servers, storage devices, via reality devices, displays, smartphones and peripherals, as well as gaming PCs and accessories under its Predator brand. As the world's 6th-largest PC vendor by unit sales as of January 2021

| ELATIONIS JONE   | the State of Parties | Cire continents with<br>multiple Constant<br>(1976) | Topic Service | State From STS Research |   | DUTCHER LOCAL NAME   |
|--|----------------------|---|---------------|-------------------------|---|--|
|  |                      |   | Doors         |                         |   |  |
| MINISTER STORYNGS  | RESOURCE             |   | 1000          |                         | Mill State .                              | V 200  |
| ubmout 75/4/67   | DOMESTIC:            | No.   | 1855          |                         | ADDITION OF THE PERSON                    | Africanaet Buginhout   |
| ubmotts tolepide   | DOMESTIC             | An .  | and .         |                         | age wydydddiddina                         | TENTRE DOM   |
| debicate 57 Style 6  | INDEPENDENCE.        | No.   | 1050          | 9.0                     | APPALANTAL APPEARANCE                     | action representation of the plant   |
| Committee of the Commit | 100000037            | in.   | stre          |                         | arthursto                                 | Highlight in   |
| commo Hypes.   | 1000000XX            | 99  | 1150          |                         | artificial Charles (Autor)                | NAMES OF THE PARTY |
| committee of the latest  | 0000000              | M.  | 100           |                         | and the first program of the state of the | Superintent transfer of the year of the  |
|  |                      |   |               |                         |   |  |



## 勒索赎金攻击者索要214151个门罗币(XMR),高达5000万

#### Your network has been infected!



Your documents, photos,
databases and other important files
encrypted



To decrypt your files you need to buy our special software - General-Decryptor



Follow the instructions below. But remember that you do not have much time

#### General-Decryptor price

the price is for all PCs of your infected network

You have 8 days, 19:07:29

- \* If you do not pay on time, the price will be doubled
- \* Time ends on Mar 28, 16:30:11

Current price

After time ends

214151 XMR ≈ 50,000,000 USD

428302 XMR ≈ 100,000,000 USD



## (4)、屏幕锁定类勒索病毒

#### winlock







# 谢谢