DexCrypt MBRLocker Demands 30 Yuan To Gain Access to Computer

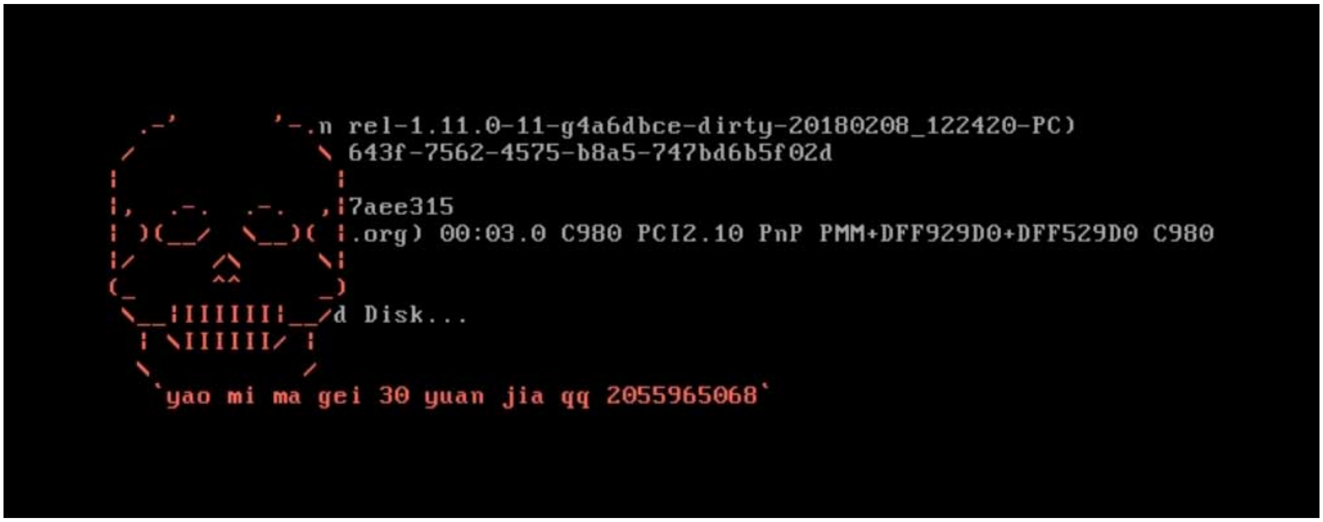
bleepingcomputer.com/news/security/dexcrypt-mbrlocker-demands-30-yuan-to-gain-access-to-computer

By
Lawrence Abrams

- February 9, 2018
- 07:04 PM
- 1

A new Chinese MBRLocker called DexLocker has been discovered that asks for 30 Yuan to get access to a computer. First discovered by security researcher JAMESWT, this ransomware will modify the master boot record of the victim's computer so that it shows a ransom note before Windows starts.

Unfortunately, I was not able to get this sample to run, so I have no first hand analysis of this ransomware. The AnyRun video posted by JAMESWT, though, shows that once you install the ransomware, it immediately reboots the computer and the victim is greeted with an ascii skull and a message to send 30 yaun to the 2055965068 qq address in order to get access to their computer again.



```
   .-'          '-.n rel-1.11.0-11-g4a6dbce-dirty-20180208_122420-PC)
  /                \ 643f-7562-4575-b8a5-747bd6b5f02d
 |                  |
 |,  .-.    .-.   ,|7aee315
 | )(__/    \__)(  |.org) 00:03.0 C980 PCI2.10 PnP PMM+DFF929D0+DFF529D0 C980
 |/      /\       \|
 (_      ^^       _)
  \__|IIIIIII|__/d Disk...
   | \IIIIII/ |
   \          /
    `yao mi ma gei 30 yuan jia qq 2055965068`
```

DexCrypt Lock Screen

Microsoft's Windows Defender Security Team saw Jame's tweet and tweeted that they have labeled the MBRLocker as Ransom:DOS/Dexcrypt.A and that it can be detected by Windows Defender.

> ICYMI: New #ransomware writes code to the Master Boot Record (MBR) and immediately restarts computer to show a note that asks for 30 yuan as ransom. Windows Defender AV detects and blocks this ransomware as Ransom:Win32/Dexcrypt and its MBR-writing code as Ransom:DOS/Dexcrypt.A. https://t.co/wpD0wJeSIu
>
> — Microsoft Security Intelligence (@MsftSecIntel) February 9, 2018

According to kangxiaopao, you can enter the **ssssss** password to gain access. If this password does not work and it does only replace the MBR, it can be fixed by booting up into the Windows Recovery Console and restoring the Master Boot Record using the following commands:

```
bootrec /RebuildBcd
bootrec /fixMbr
bootrec /fixboot
```

Once you enter these commands, you can reboot and get access again to Windows again.

Related Articles:

New ‘Cheers’ Linux ransomware targets VMware ESXi servers

SpiceJet airline passengers stranded after ransomware attack

US Senate: Govt’s ransomware fight hindered by limited reporting

New RansomHouse group sets up extortion market, adds first victims

Ransomware attack exposes data of 500,000 Chicago students

IOCs

Hashes:

```
dfc56a704b5e031f3b0d2d0ea1d06f9157758ad950483b44ac4b77d33293cb38
```

Ransom Note:

```
  .-'      '-.
 /            \
|              |
|,  .-.  .-.  ,|
| )(__/  \__)( |
|/     /\     \|
(_     ^^     _)
 \__|IIIIII|__/
  | \IIIIII/ |
  \          /
   `yao mi ma gei 30 yuan jia qq 2055965068`
```

- DexCrypt
- MBR
- Ransomware

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

Comments

Occasional - 4 years ago

Very interesting - especially the tiny amount asked for in the ransom note.

Why so little? the obvious answer is that many people wouldn't quibble, or try to fix the situation themselves, if they could just make it go away for less than $5.

Perhaps, though, it's that you get more than you bargained for, with your $5 payment - or maybe, you get less than you need.. Smoke and mirrors?

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: