Laptop maker Compal hit by ransomware, $17 million demanded

bleepingcomputer.com/news/security/laptop-maker-compal-hit-by-ransomware-17-million-demanded/

Lawrence Abrams

By
Lawrence Abrams

- November 9, 2020
- 01:33 PM
- 0

Taiwanese laptop maker Compal Electronics suffered a DoppelPaymer ransomware attack over the weekend, with the attackers demanding an almost $17 million ransom.

Compal is the second-largest original design manufacturer (ODM) of laptops globally, with well-known companies rebranding their devices or designs, including Apple, HP, Dell, Lenovo, and Acer.

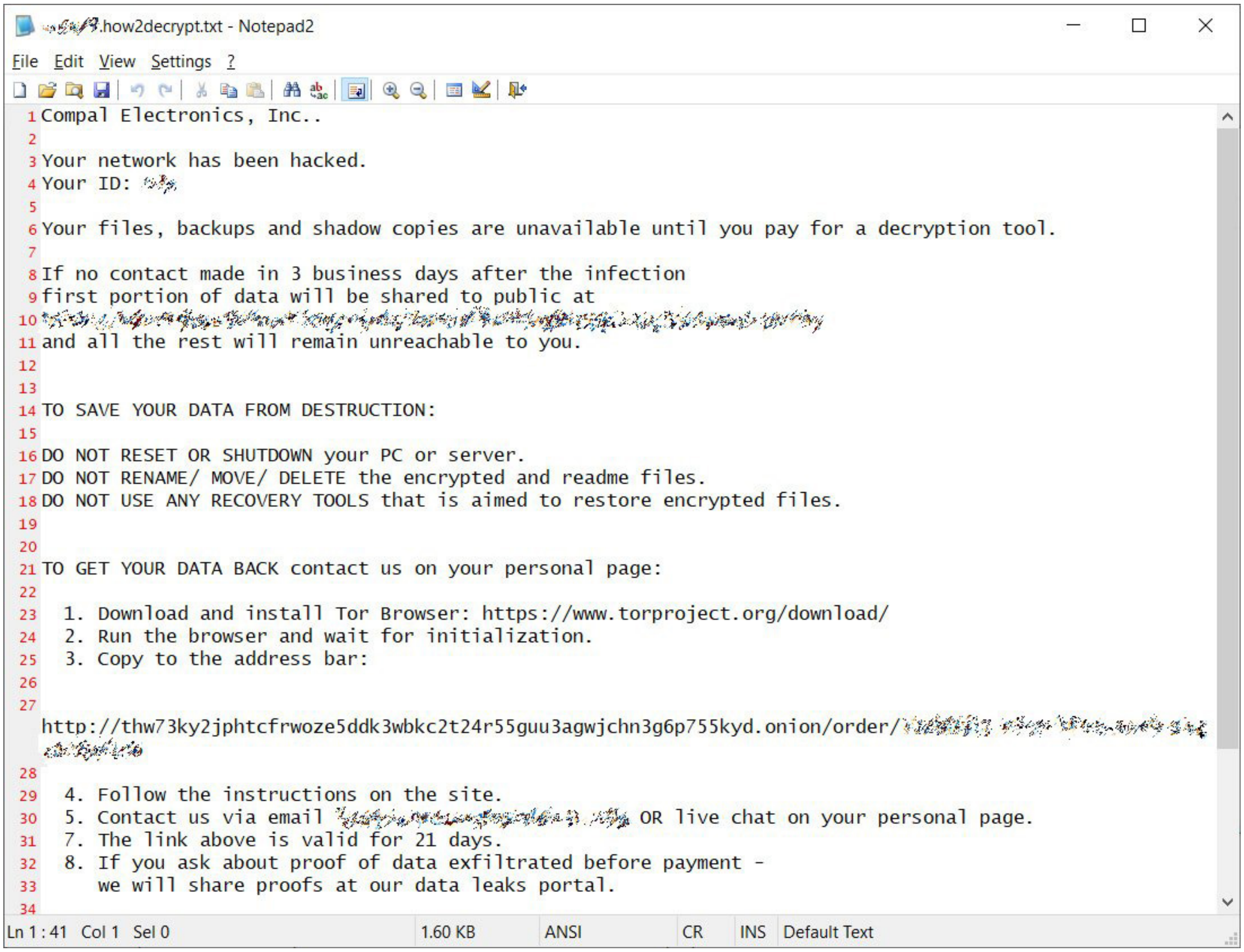
$16.7 million ransom demanded

Over the weekend, Taiwanese media reported that Compal suffered a cyberattack, but the laptop maker claimed it was just an "abnormality" in their office automation system.

"Lu Qingxiong said that the main reason was an abnormality in the office automation system. The company suspected of being invaded by hackers. It has urgently repaired most of it and is expected to return to normal today,"

"Lu Qingxiong emphasized that Compal is not being blackmailed by hackers, as is reported by the outside world, and everything is currently normal in production," UDN reported.

Since then, BleepingComputer has confirmed that Compal suffered a DoppelPaymer ransomware attack after we obtained a ransom note used in the attack.

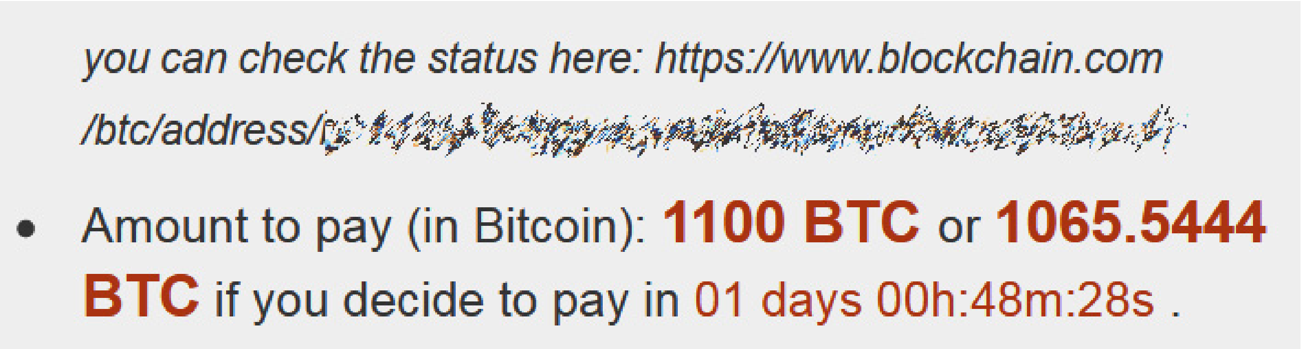

[redacted].how2decrypt.txt - Notepad2
File Edit View Settings ?
Ln 1 : 41 Col 1 Sel 0
1.60 KB
ANSI
CR
INS
Default Text

```
Compal Electronics, Inc..

Your network has been hacked.
Your ID: [redacted]

Your files, backups and shadow copies are unavailable until you pay for a decryption tool.

If no contact made in 3 business days after the infection
first portion of data will be shared to public at
[redacted]
and all the rest will remain unreachable to you.


TO SAVE YOUR DATA FROM DESTRUCTION:

DO NOT RESET OR SHUTDOWN your PC or server.
DO NOT RENAME/ MOVE/ DELETE the encrypted and readme files.
DO NOT USE ANY RECOVERY TOOLS that is aimed to restore encrypted files.


TO GET YOUR DATA BACK contact us on your personal page:

  1. Download and install Tor Browser: https://www.torproject.org/download/
  2. Run the browser and wait for initialization.
  3. Copy to the address bar:

http://thw73ky2jphtcfrwoze5ddk3wbkc2t24r55guu3agwjchn3g6p755kyd.onion/order/[redacted]

  4. Follow the instructions on the site.
  5. Contact us via email [redacted] OR live chat on your personal page.
  7. The link above is valid for 21 days.
  8. If you ask about proof of data exfiltrated before payment -
     we will share proofs at our data leaks portal.
```

Compal ransom note

DoppelPaymer is a ransomware operation known for attacking enterprise targets by gaining access to admin credentials and using them to spread throughout a Windows network. Once they gain access to a Windows domain controller, they deploy the ransomware payloads to all devices on the network.

According to the DoppelPaymer Tor payment site linked to in the ransom note, the ransomware gang is demanding 1,100 Bitcoins, or $16,725,500.00 at today's prices, to receive a decryptor.



you can check the status here: https://www.blockchain.com /btc/address/[redacted]

- Amount to pay (in Bitcoin): **1100 BTC** or **1065.5444 BTC** if you decide to pay in 01 days 00h:48m:28s .

DoppelPaymer ransom demand

According to the ransom note and DoppelPaymer's past history, the attackers likely stole unencrypted data as part of their attack.

This stolen data is then used as a double-extortion strategy where the ransomware gangs threaten to release the files on data leak sites if a ransom is not paid.

It should be noted that the initial ransom demands are a "starting" price and are commonly negotiated to a significantly lower amount for victims who decide to pay the ransom.

Other victims attacked by DoppelPaymer in the past include PEMEX (Petróleos Mexicanos), the City of Torrance in California, Newcastle University, Hall County in Georgia, and Bretagne Télécom.

Related Articles:

Windows 11 KB5014019 breaks Trend Micro ransomware protection

Industrial Spy data extortion market gets into the ransomware game

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

- Compal
- DoppelPaymer
- Laptop
- 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

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: