New DoppelPaymer Ransomware Emerges from BitPaymer's Code

By Ionut Ilascu

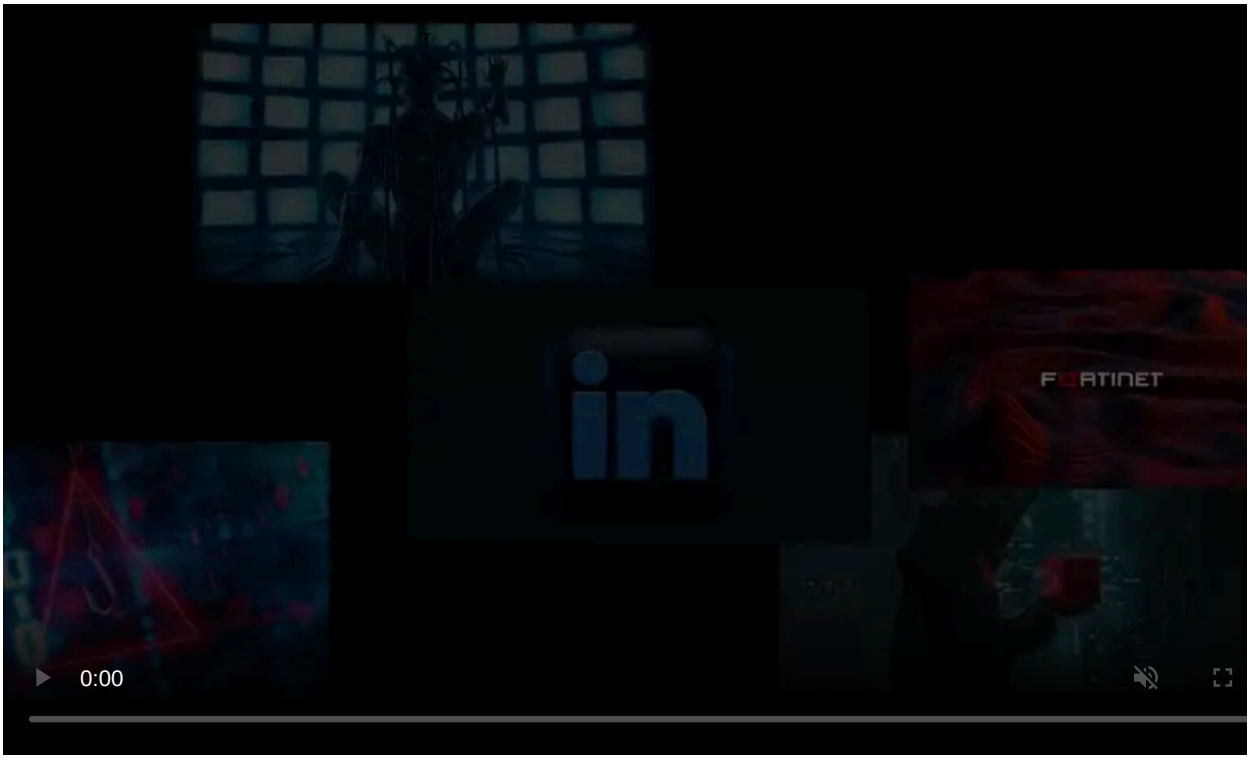
Published: 2019-07-15 · Archived: 2026-04-05 19:15:16 UTC

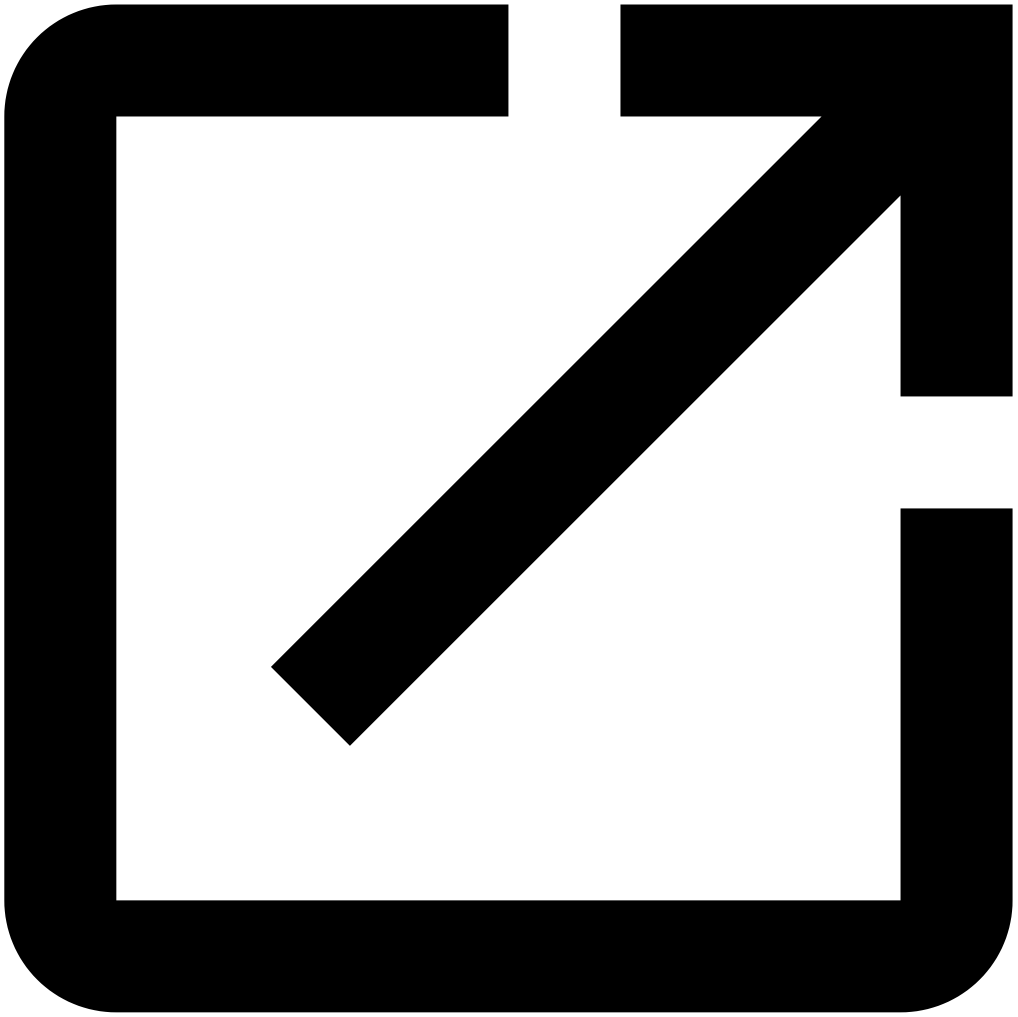
Malware researchers have discovered a new file-encrypting malware they dubbed DoppelPaymer that has been making victims since at least mid-June, asking hundreds of thousands of US dollars in ransom.

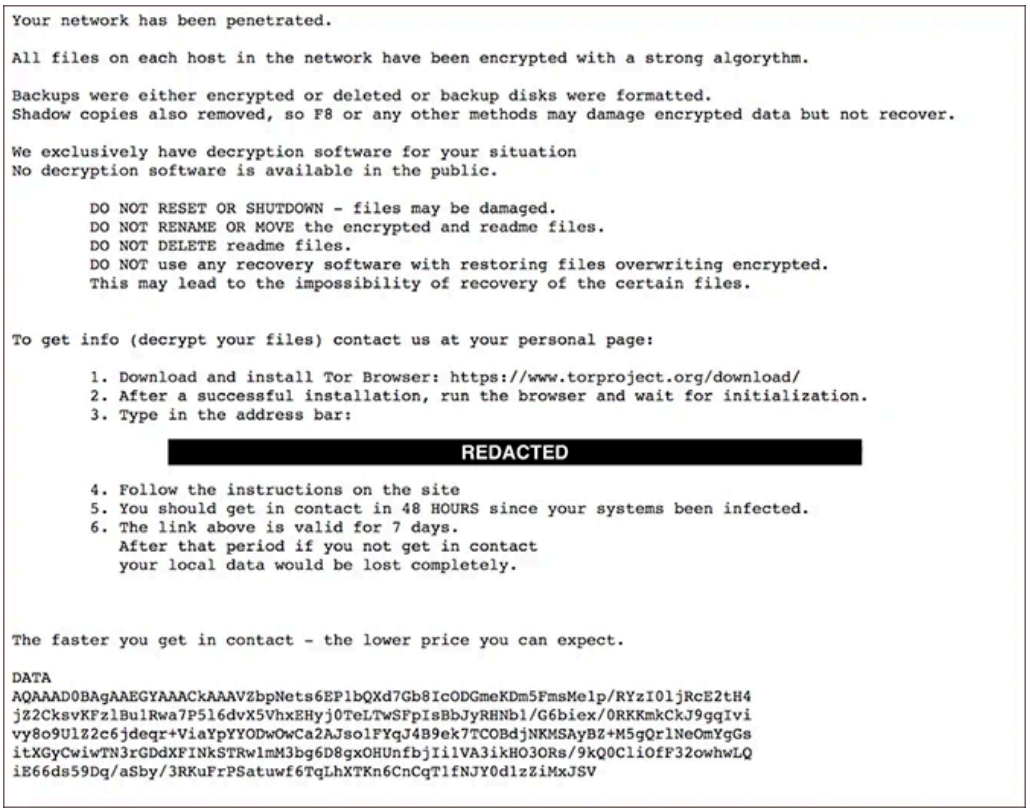
The ransomware strain has at least eight variants that extended their feature set gradually, with the earliest one dating since April.

Victims in the public service sector

DoppelPaymer takes its name from BitPaymer, with which it shares more than large portions of code. There are three confirmed victims of this ransomware strain, which priced its decryption keys between 2 BTC and 100 BTC, say researchers from CrowdStrike.


0:00





```
Your network has been penetrated.

All files on each host in the network have been encrypted with a strong algorythm.

Backups were either encrypted or deleted or backup disks were formatted.
Shadow copies also removed, so F8 or any other methods may damage encrypted data but not recover.

We exclusively have decryption software for your situation
No decryption software is available in the public.

        DO NOT RESET OR SHUTDOWN - files may be damaged.
        DO NOT RENAME OR MOVE the encrypted and readme files.
        DO NOT DELETE readme files.
        DO NOT use any recovery software with restoring files overwriting encrypted.
        This may lead to the impossibility of recovery of the certain files.


To get info (decrypt your files) contact us at your personal page:

        1. Download and install Tor Browser: https://www.torproject.org/download/
        2. After a successful installation, run the browser and wait for initialization.
        3. Type in the address bar:

                              REDACTED

        4. Follow the instructions on the site
        5. You should get in contact in 48 HOURS since your systems been infected.
        6. The link above is valid for 7 days.
           After that period if you not get in contact
           your local data would be lost completely.


The faster you get in contact - the lower price you can expect.

DATA
AQAAAD0BAgAAEGYAAACkAAAVZbpNets6EPlbQXd7Gb8IcODGmeKDm5FmsMelp/RYzI0ljRcE2tH4
jZ2CksvKFzlBu1Rwa7P5l6dvX5VhxEHyj0TeLTwSFpIsBbJyRHNbl/G6biex/0RKKmkCkJ9gqIvi
vy8o9Ulz2c6jdeqr+ViaYpYYODwOwCa2AJsolFYqJ4B9ek7TCOBdjNKMSAyBZ+M5gQrlNeOmYgGs
itXGyCwiwTN3rGDdXFINkSTRwlmM3bg6D8gxOHUnfbjIilVA3ikHO3ORs/9kQ0CliOfF32owhwLQ
iE66ds59Dq/aSby/3RKuFrPSatuwf6TqLhXTKn6CnCqTlfNJY0d1zZiMxJSV
```

Bitcoin price in late April was around $5,150 and kept rising ever since, with lows well above the $7,000 mark and peaking above $12,000 in late June and early July.

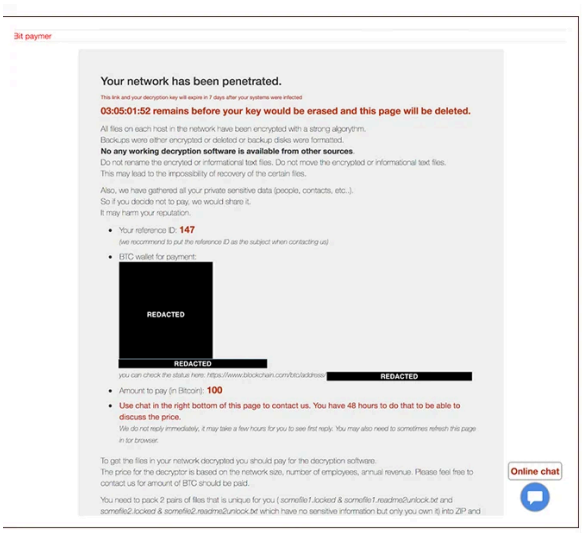
One of the victims is the City of Edcouch, Texas, which was left with a ransom note demanding 8 BTC to decrypt the data on the affected computers.

It is unclear when the Edcouch administration was attacked, but city officials said that the amount converted to about $40,000. This makes it likely that the compromise happened in early May or before when bitcoin price stooped below $5,500.

Another victim was the Chilean Ministry of Agriculture, the researchers said in a report last week. The country's Computer Security Incident Response Team (CSIRT) confirmed on July 1 that a ransomware attack hit servers from a public service connected to the Ministry of Agriculture.

Parallel extortion activity

CrowdStrike researchers observed some striking similarities between DoppelPaymer's payment portal and the original one for BitPaymer. One striking hint linking the two ransomware threats is the "Bit paymer" title at the top of the page but they're similar all over.



DoppelPaymer payment portal

Older BitPaymer payment portal

Another clue pointing to a connection between the two pieces of malware is that they "share significant amounts of code." However, they have different encryption schemes.

Where DoppelPaymer combines 2048-bit RSA keys with 256-bit AES, the latest BitPaymer versions use 4096-bit RSA with the same specification for symmetric encryption.

Also, there is standard AES encryption padding (PKCS#7) in DoppelPaymer while BitPaymer uses random bytes specified in a field called 'TAIL.'

By analyzing differences and similarities between the two, Brett Stone-Gross, Sergei Frankoff and Bex Hartley of CrowdStrike's research and threat intel team believe that the new ransomware strain may be the work of a BitPaymer group member that started their own ransomware business.

"Both BitPaymer and DoppelPaymer continue to be operated in parallel and new victims of both ransomware families have been identified in June and July 2019. The parallel operations, coupled with the significant code overlap between BitPaymer and DoppelPaymer, indicate not only a fork of the BitPaymer code base, but an entirely separate operation." - CrowdStrike

The new ransomware includes modifications that make it superior to BitPaymer, such as threaded encryption process for a quicker operation.

The operators of BitPaymer are the same individuals behind the Dridex banking trojan, collectively known as the INDRIK SPIDER. They are former affiliates of the cybercriminal gang calling itself "The Business Club."

The group is responsible for using the GameOver Zeus botnet (disrupted in 2014), believed to have infected over one million computers, and causing damages in excess of $100 million from business and financial institutions across the world.

Source: https://www.bleepingcomputer.com/news/security/new-doppelpaymer-ransomware-emerges-from-bitpaymers-code/