Bit Paymer Ransomware Hits Scottish Hospitals

By Catalin Cimpanu

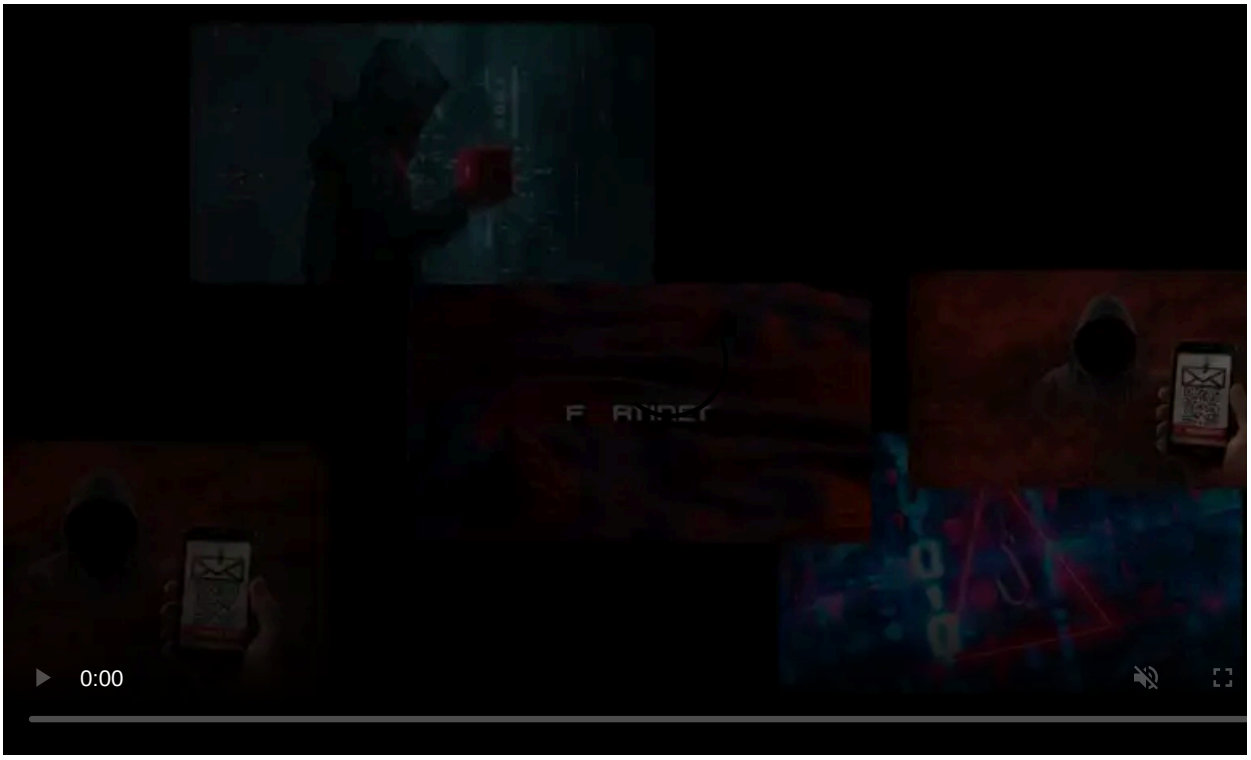
Published: 2017-08-29 · Archived: 2026-04-06 00:40:33 UTC

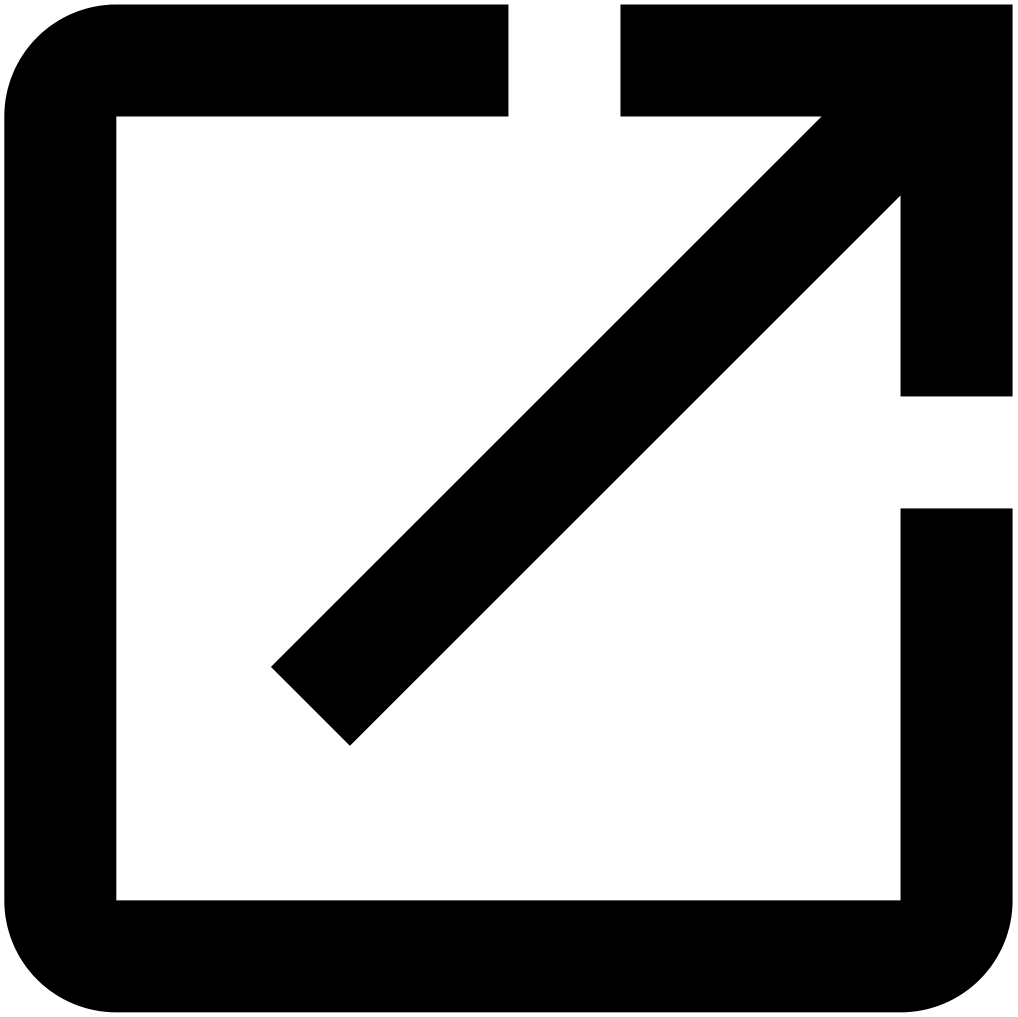
Several hospitals part of the NHS Lanarkshire board were hit on Friday by a version of the Bit Paymer ransomware.

The NHS Lanarkshire board includes hospitals such as Hairmyres Hospital in East Kilbride, Monklands Hospital in Airdrie and Wishaw General Hospital.

Affected systems fixed over the weekend

The infection took root on late Friday, August 25. NHS Lanarkshire officials acknowledged the incident right away.


0:00



The next day, board officials issued a statement revealing they had the situation under control, and they were currently restoring affected systems, an operation they estimated would take until Monday.

"Unfortunately a small number of procedures and appointments have been canceled as a result of the incident," said NHS Lanarkshire chief executive Calum Campbell.

Bit Paymer active since at least June 2017

The Bit Paymer ransomware — sometimes also spelled as Bitpaymer — first came to Bleeping Computer's attention on July 11, when security researcher Michael Gillespie tweeted a link to a sample uploaded on VirusTotal, a web-based file scanning service.

Fellow researcher MalwareHunter told Bleeping Computer today in a private conversation that following the NHS Lanarkshire attacks, more samples were found on VirusTotal going back to June 21, 2017, hinting that more campaigns might have taken place before the NHS Lanarkshire incident.

Unlike most ransomware we see today, Bit Paymer is well coded and appears to be the work of experienced programmers.

Bit Paymer spread via RDP brute-force attacks

An Emsisoft security researcher who goes online by the pseudonym of xXToffeeXx believes the ransomware is installed after attackers performed brute-force attacks on exposed RDP endpoints.

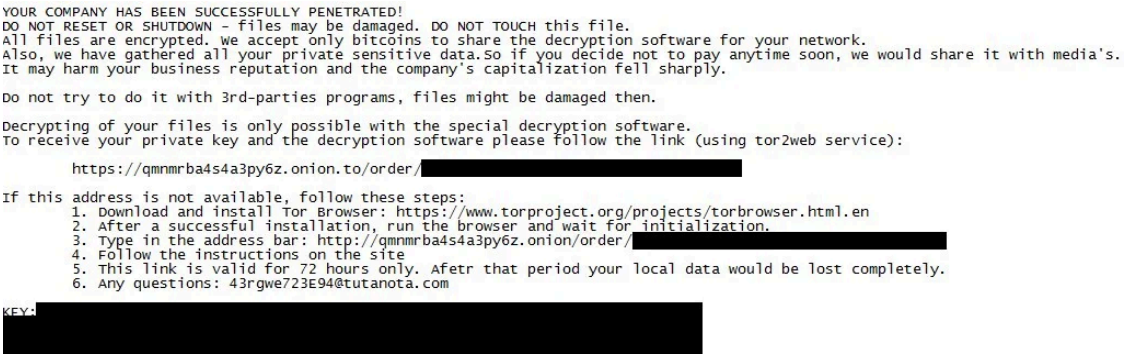
After gaining access to one system, attackers move laterally on the breached network and install Bit Paymer manually on each compromised system.

According to Gillespie, the ransomware encrypts files with a combination of RC4 and RSA-1024 encryption algorithms. The researcher says there's currently no way to decrypt files locked by the Bit Paymer ransomware.

Ransomware asks for a whopping $230,000 ransom payment

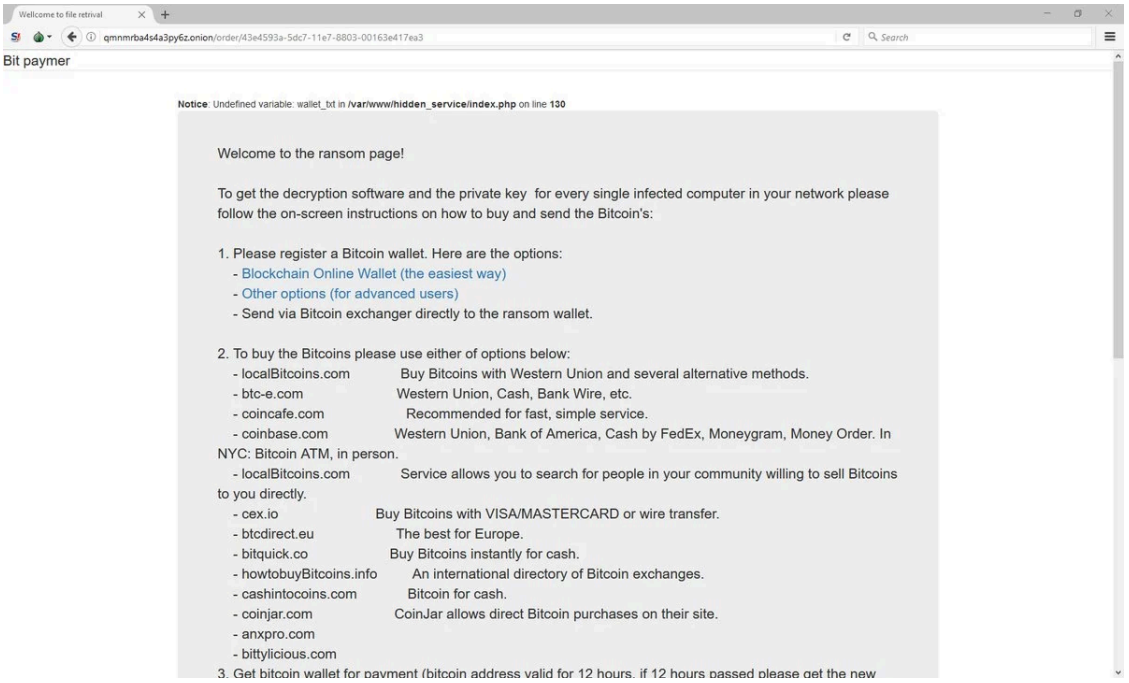
The ransomware appends the ".locked" string at the end of each encrypted file name. A file named "image.png" will become "image.png.locked".

Bit Paymer also generates text files holding the ransom note and drops them all over the filesystem, where it encrypted files.



```
YOUR COMPANY HAS BEEN SUCCESSFULLY PENETRATED!
DO NOT RESET OR SHUTDOWN - files may be damaged. DO NOT TOUCH this file.
All files are encrypted. We accept only bitcoins to share the decryption software for your network.
Also, we have gathered all your private sensitive data.So if you decide not to pay anytime soon, we would share it with media's.
It may harm your business reputation and the company's capitalization fell sharply.

Do not try to do it with 3rd-parties programs, files might be damaged then.

Decrypting of your files is only possible with the special decryption software.
To receive your private key and the decryption software please follow the link (using tor2web service):

        https://qmnmrba4s4a3py6z.onion.to/order/[redacted]

If this address is not available, follow these steps:
        1. Download and install Tor Browser: https://www.torproject.org/projects/torbrowser.html.en
        2. After a successful installation, run the browser and wait for initialization.
        3. Type in the address bar: http://qmnmrba4s4a3py6z.onion/order/[redacted]
        4. Follow the instructions on the site
        5. This link is valid for 72 hours only. Afetr that period your local data would be lost completely.
        6. Any questions: 43rgwe723E94@tutanota.com

KEY:[redacted]
```

The ransom note instructs victims to connect to a Tor-based portal where victims can pay to recover their files.



This site also holds the ransom demand. Just like similar ransomware strains installed via targeted attacks, Bit Paymer asks for astronomical ransom demands. In samples observed in the past, this was of 53 Bitcoin, which is $230,000 at today's exchange rate. In other cases observed by xXToffeeXx, the ransom was smaller, of only 20 Bitcoin. "They do change the ransom amount depending on the victims," the researcher said.

Bit Paymer is also very strange in the way it handles ransom payments. The group behind this ransomware wants victims to send three 1 Bitcoin "confirmation" transactions before sending the full payment. This is most likely to prevent victims from sending the bulk of the sum to the wrong Bitcoin address.

A focus on large companies

Other ransomware families that we've seen in the past manually installed on targets' systems after RDP brute-force attacks include RSAUtil, Xpan, Crysis, Samas (SamSam), LowLevel, DMA Locker, Apocalypse, Smrss32, Bucbi, Aura/BandarChor, ACCDFISA, or Globe.

"The interesting thing about Bitpaymer is that they are specifically targeting companies, and not just any companies, quite big companies," xXToffeeXx explains. "This is quite different to most other RDP company targeting ransomware. Reminds me of SamSam."

Bit Paymer should not be confused with the Defray ransomware, which Proofpoint researchers discovered last week targeting healthcare organizations. According to a Proofpoint report, Defray is spread via email spam, not RDP brute-force attacks.

Two weeks ago, Malwarebytes researcher Hasherezade uploaded a video on YouTube detailing the process of unpacking the BitPaymer ransomware payload. The video can prove helpful for researchers looking to analyze the threat.

IOCs:

SHA256 Hashes:

```
 1c0ffdaddec1eca9a9a5ef5192151dbce8ccd8e31a84c51d70f5a5c64f07a363
d693c33dd550529f3634e3c7e53d82df70c9d4fbd0c339dbc1849ada9e539ea2
```

Ransom note:

```
 YOUR COMPANY HAS BEEN SUCCESSFULLY PENETRATED!
All files are encrypted. We accept only bitcoins to share the decryption software for your network.
Also, we have gathered all your private sensitive data.So if you decide not to pay anytime soon, we would share it with me
It may harm your business reputation and the company's capitalization fell sharply.

Do not try to do it with 3rd-parties programs, files might be damaged then.

Decrypting of your files is only possible with the special decryption software.
To receive your private key and the decryption software please follow the link (using tor2web service):

[REDACTED URL]

If this address is not available, follow these steps:
1. Download and install Tor Browser: hxxps://www.torproject.org/projects/torbrowser.html.en
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: [REDACTED URL]
4. Follow the instructions on the site
5. This link is valid for 72 hours only. Afetr that period your local data would be lost completely.
6. Any questions: [REDACTED EMAIL]
```

Bit Paymer payment site:

```
 Bit paymer
Welcome to the ransom page!

To get the decryption software and the private key for every single infected computer in your network please follow the or

1. Please register a Bitcoin wallet. Here are the options:
- Blockchain Online Wallet (the easiest way)
- Other options (for advanced users)
- Send via Bitcoin exchanger directly to the ransom wallet.

2. To buy the Bitcoins please use either of options below:
- localBitcoins.com Buy Bitcoins with Western Union and several alternative methods.
- btc-e.com Western Union, Cash, Bank Wire, etc.
- coincafe.com Recommended for fast, simple service.
- coinbase.com Western Union, Bank of America, Cash by FedEx, Moneygram, Money Order. In NYC: Bitcoin ATM, in person.
- localBitcoins.com Service allows you to search for people in your community willing to sell Bitcoins to you directly.
- cex.io Buy Bitcoins with VISA/MASTERCARD or wire transfer.
- btcdirect.eu The best for Europe.
- bitquick.co Buy Bitcoins instantly for cash.
- howtobuyBitcoins.info An international directory of Bitcoin exchanges.
- cashintocoins.com Bitcoin for cash.
- coinjar.com CoinJar allows direct Bitcoin purchases on their site.
- anxpro.com
- bittylicious.com
3. Get bitcoin wallet for payment (bitcoin address valid for 12 hours, if 12 hours passed please get the new wallet)
4. Send 50 BTC to the bitcoin address
[REDACTED WALLET] (must be sent in 1 transaction!)
```

```
Please note that we require 3 Bitcoin transaction confirmations.
- To view the current status of your transaction please follow the link: hxxps://blockchain.info/address/[REDACTED WALLET]
- Once the transaction passed 3 confirmations please refresh the page and you will be granted to download the decryption s
- If something goes wrong please contact us via email: [REDACTED EMAIL]
- We can decrypt 2-3 non-important light-weight files before you pay, send'em to email: [REDACTED EMAIL]

4. Please be advised that the ransom amount may be raised after 48 hours since your first visit if no payment received. In

Your company is secure enough, but we may tell you what is wrong after payment being processed. Good Luck!
```

Source: https://www.bleepingcomputer.com/news/security/bit-paymer-ransomware-hits-scottish-hospitals/