Warning - you have received a subpoena email - blueAPACHE

Canonical: https://www.blueapache.com/blog/warning-you-have-received-a-subpoena-email

Details:

Historical warning: 8 March 2016, concerning the fake AFP email campaign described below.

Further to our recent warning about fake Australia Post emails , a new ransomware email pretending to be from the Australian Federal Police (AFP) is now circulating. Branded with the AFP logo and the subject “AFP You have been issued”, the email claims you have been subpoenaed to appear in court due to a “law violation”. The email includes a case number and date. We have seen several of these over recent days. An example received is: The AFP have recently advised that they were aware of the fake email, and made a statement advising they do not issue subpoenas via email. There were a few giveaway signs that this email was suspicious. The from address (tom@padeldanmark.dk) is from Denmark – not from the AFP, and the email includes an unsubscribe option, which seems strange considering this is supposedly a subpoena. As always, when in doubt – phone the issuing body for clarification before clicking on links. If identified as fake or if you remain concerned, delete the email (and permanently delete the email from your deleted items folder or bin). Do not click on links contained in the email or reply to the email. This latest ransomware email provides links (a text link and a button) that take you to a fake AFP website that requires completion of a captcha form to access your case details (see below). Completing the captcha form will result in downloading a zip file that appears to contain your court details, but is in fact the TorrentLocker ransomware. Once opened, TorrentLocker will usually attempt to delete volume shadow copies (to remove the chance of file recovery), copy itself to the windows directory and contact the command and control server. An encryption key is then generated and all accessible files on the network are encrypted. Upon encryption, the ransom message is displayed and details of the encrypted files are sent to the command and control server. TorrentLocker then harvests email accounts from your email programs (including online email accounts) and sends them to the command and control server to further spread the malware. As with most ransomware, payment is made with bitcoins. TorrentLocker accepts a reduced fee if payment is made within a short period of time (usually four days), after which the price doubles. It is claimed that after one month the decryption key will be destroyed and encrypted files will be unrecoverable. The decryption file is typically priced between $500 and $1000. Even when paying, there is no guarantee that you will receive the key to decrypt your files, or that the key will work. If you have concerns about your security posture, would like staff security training, or would like to better understand how to protect your business, contact our account team .

Has the AFP confirmed whether it sends subpoenas via email?

Yes. The AFP advised that it was aware of the fake email and made a statement confirming that it does not issue subpoenas via email.

What were the warning signs that the AFP subpoena email was fake?

The email's "from" address (tom@padeldanmark.dk) originated from Denmark rather than the AFP, and the email included an unsubscribe option, which is unusual for a supposed legal subpoena.

What happens if you click the links in the fake AFP subpoena email?

The links (a text link and a button) take you to a fake AFP website requiring completion of a captcha form to access supposed case details. Completing the captcha results in downloading a zip file that appears to contain court details but actually contains the TorrentLocker ransomware.

What does the TorrentLocker ransomware do once it is opened?

TorrentLocker typically attempts to delete volume shadow copies to prevent file recovery, copies itself to the Windows directory, and contacts a command and control server. It then generates an encryption key, encrypts all accessible files on the network, displays a ransom message, and sends details of the encrypted files to the command and control server. It also harvests email accounts from email programs (including online accounts) and sends them to the command and control server to further spread the malware.

How is ransom typically paid for TorrentLocker, and what happens if payment is delayed?

Payment is made with bitcoins. TorrentLocker offers a reduced fee if payment is made within a short period (usually four days), after which the price doubles. It is claimed that after one month the decryption key is destroyed and encrypted files become unrecoverable.

How much does the TorrentLocker decryption typically cost, and is payment guaranteed to work?

The decryption file is typically priced between $500 and $1000. Even after paying, there is no guarantee of receiving a working decryption key.

What should you do if you receive a suspicious subpoena-style email?

According to us, you should phone the issuing body for clarification before clicking on any links. If the email is identified as fake or you remain concerned, delete it (and permanently delete it from your deleted items folder or bin), and do not click on links or reply to the email.

How does the article advise checking a suspicious subpoena-style email?

It advises phoning the purported issuing body to clarify the message before clicking links or replying. As a practical precaution, obtain the contact details independently from the body's official website rather than from the suspicious email.

What contractual notification duties may apply to a notice concerning Customer Data?

Check the actual notice and the agreement that applies to your service. Clause 14.2 of the published General Terms requires prompt notice to blueAPACHE and compliance with specified regulatory take-down, service-cessation and link-deletion notices or Telecommunications Industry Ombudsman directions relating to Customer Data. It does not state a universal immediate-notification duty for every subpoena or legal demand.

Who can businesses contact for help with security concerns or staff security training related to this type of threat?

Businesses with concerns about their security posture, who want staff security training, or who want to better understand how to protect their business can contact our account team.

When was your warning about the fake AFP subpoena email published?

The article was published on March 8, 2016, and is written by us.