Phobos Ransomware, A Combo of CrySiS and Dharma

coveware.com/blog/phobos-ransomware-distributed-dharma-crew

January 18, 2019

Updated 01/29/2019

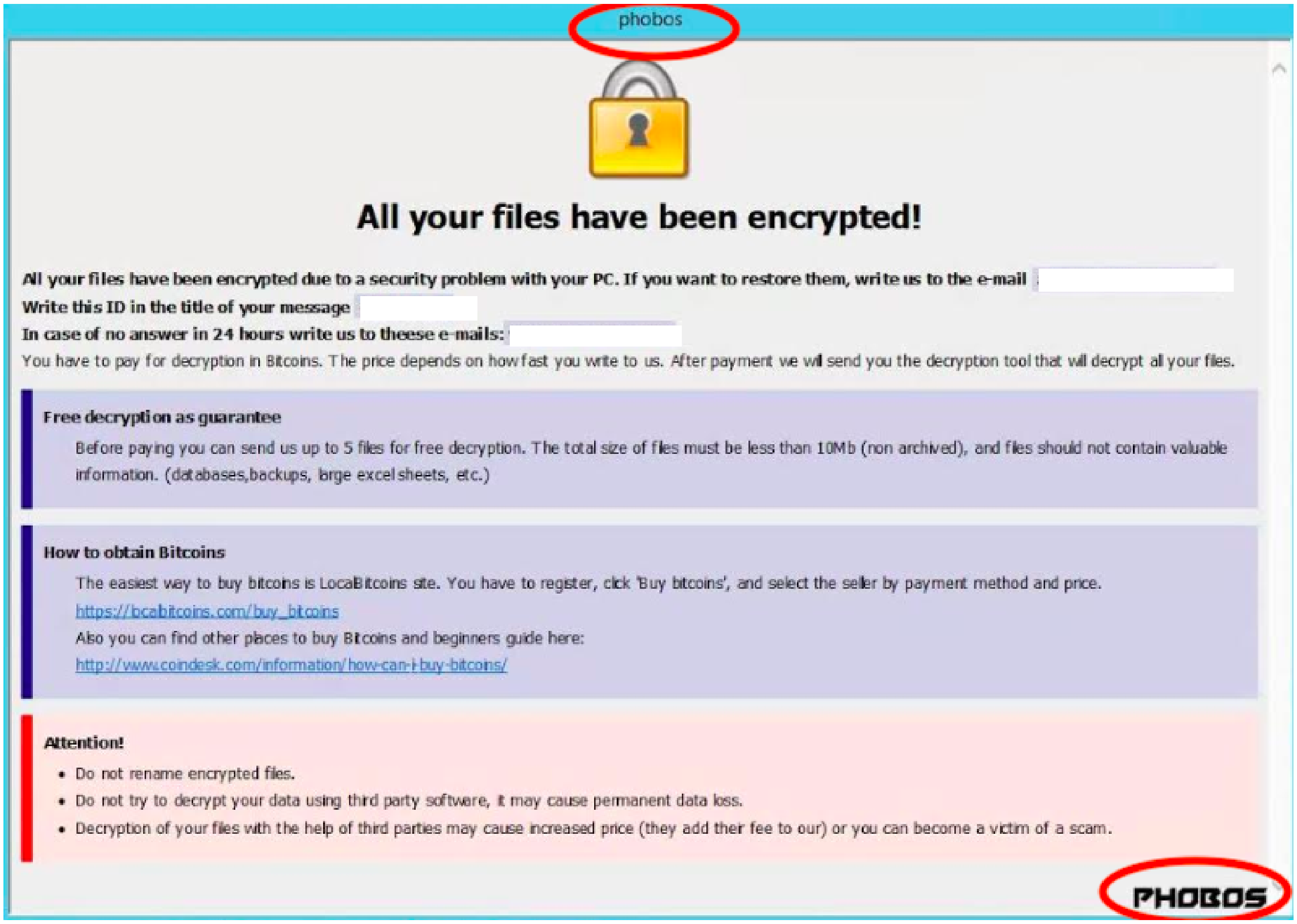
We are researching the possibility that the primary distribution group behind Phobos may have been disrupted by the recent xDedic takedown. At approximately the same time that xDedic was taken down, all known email addresses associated with Phobos attacks became disabled and inbound emails bounced. We are unsure at this time if the ransomware distributors themselves disabled their accounts, or if their email hosting provider disabled the accounts as part of the law enforcement action. We will further update this post as we learn more.

Original Phobos Post below:

A new strain of ransomware has been impacting businesses globally since mid December. The ransomware, dubbed Phobos by the distributors (possibly after the greek god of fear), shares both technical and operational similarities to several recent Dharma variants. The attack vectors being leveraged by Phobos distributors are well worn, open or weakly secured RDP ports. As usual, the attacks are exacerbated when companies either have no backups, or have not properly partitioned them from the network with strong administrative controls.

Rebranded Dharma Ransom Note and Same Encrypted File Extension Format

Most ransomware leaves behind an obvious ransom note so that the victim can find it and contact the hacker. Typically, these notes vary significantly depending upon the ransomware strain. However, both Dharma and Phobos use the same ransom note. The only observable difference is that Phobos added a bit of branding to the top and bottom as seen in the below image.



All your files have been encrypted!

All your files have been encrypted due to a security problem with your PC. If you want to restore them, write us to the e-mail [redacted]
Write this ID in the title of your message [redacted]
In case of no answer in 24 hours write us to theese e-mails: [redacted]
You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the decryption tool that will decrypt all your files.

Free decryption as guarantee
Before paying you can send us up to 5 files for free decryption. The total size of files must be less than 10Mb (non archived), and files should not contain valuable information. (databases,backups, large excel sheets, etc.)

How to obtain Bitcoins
The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', and select the seller by payment method and price.
https://localbitcoins.com/buy_bitcoins
Also you can find other places to buy Bitcoins and beginners guide here:
http://www.coindesk.com/information/how-can-i-buy-bitcoins/

Attention!
- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, it may cause permanent data loss.
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

Phobos Ransomware Note is similar to a Dharma Note

Other than that, the text and composition is identical. The encrypted file name format is also the same as Dharma variants. It is constructed by concatenating the original file name, a unique ID number, hacker email, and the .phobos file extension.

Emails Offer Security Advice when Paying for Decryption Keys

When a victim of ransomware contacts the email address in the ransom notice to negotiate, the first response elicited is often a cut and paste standard response. The first response from Phobos is a verbatim match to first responses of several Dharma variants including .bip, .gamma, and .adobe. This group's first responses are unique in that they offer a friendly 'upsell', in addition to extorting the victim for safe decryption of data.

> ***"we also offer service to you. full of advice for protecting against attacks? - the price of 0.1 BTC, and remember our work is very hard. and it requires a lot of time and costs."***

The above phrase is at the end of the first response email, and offers security advice for the low low price of 0.1 BTC. This phrase has been consistent across Dharma variants and Phobos. To our knowledge, no one has taken them up on this *generous* offer.

Technically, Phobos Ransomware is only Slightly Different from Dharma

Topically, Phobos appears to a largely cut+paste variant of Dharma.. However, from a technical perspective, Phobos carries some subtle differences from active Dharma variants. Both type of ransomware draw their lines from the CySis ransomware family and commonly used AV software will identify a Phobos executable sample as CrySis. The differences observed in a recent analysis by @Demonslay335 note that the file marker structure of Phobos is significantly different from Dharma variants. What is clear is that while the ransomware type may be different, the group distributing Phobos, the exploit methods, ransom notes and communications remain the nearly identical to Dharma.