



## PNP Computer Security Bulletin CSB17-015

# Scarab Ransomware

Risk/Impact Rating: **SERIOUS**

Created: November 29, 2017

### Description:

- Ransomware-type virus that stealthily infiltrates systems and encrypts various data;
- Distributed using spam emails with malicious attachments by Necurs botnet – the internet’s largest email spam botnet;
- Emails disguised as archives carrying scanned images and have subject line “Scanned from(printer company name)”;
- Emails carried a 7 zip archive that contained a Visual Basic Script that will download and run an exe file;
- A ransom note with the filename ‘IF YOU WANT TO GET ALL YOUR FILES BACK, PLEASE READ THIS.TXT’ dropped within each affected directory; and
- The note doesn’t specify how much is the ransom, but it states “the price depends on how fast you write to us”.

A screenshot of a Notepad window titled "IF YOU WANT TO GET ALL YOUR FILES BACK, PLEASE READ THIS - Notepad". The window contains a ransom note with the following text:

```
*** IF YOU WANT TO GET ALL YOUR FILES BACK, PLEASE READ THIS ***

Your files are now encrypted!

-----BEGIN PERSONAL IDENTIFIER-----
+4IAAAAAAAAAfJQ3uHZJREcBACEKj5Ie6xvxY=HooUogInkCloY2KUS4emG1IKQAt43PFQYY9Wt9nnNO1vrDcx0Hi1LLNeVIexVQpr
3Jiw+GukqKriZuGsrhXZevechc2patM2m240ISyV6ofAwZRELKZqL6iCUQPHfJj8Uh6T1SJD61VjEET77pc2VAtWiXSMOWWn2ztG
bgSqf1Zn1SpWalrggeHDKbfra6cuCjpWmOrW1smHDC6X1KlnmoxBqj7Hqd2dwnfR6=I6lk355wf2YXORFp3pSPn0Gn=NRpIxj1K
LAbi92PW8YxsRi3LZm5GYQIyWfOPtynhaOt5leIrmsP7RqVc0mutc2ZgLhCH=jbThmwUJxvEj1x2hXk=nNoyNoaWU9hDzBXXbB=1P
5HE+TsJWKeAF=0lsoFoMat6MfI7xAA
-----END PERSONAL IDENTIFIER-----

All your files have been encrypted due to a security problem with your PC.

Now you should send us email with your personal identifier.
This email will be as confirmation you are ready to pay for decryption key.
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.

Contact us using this email address: suupport@protonmail.com
If you don't get a reply or if the email dies, then contact us using Bitmessage.
Download it form here: https://bitmessage.org/wiki/Main_Page
Run it, click New Identity and then send us a message at BM-2cTu8prUGDS6XmXqPrZiYXXeqyFw5dXEba
```

Free decryption as guarantee!

Before paying you can send us up to 3 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.).

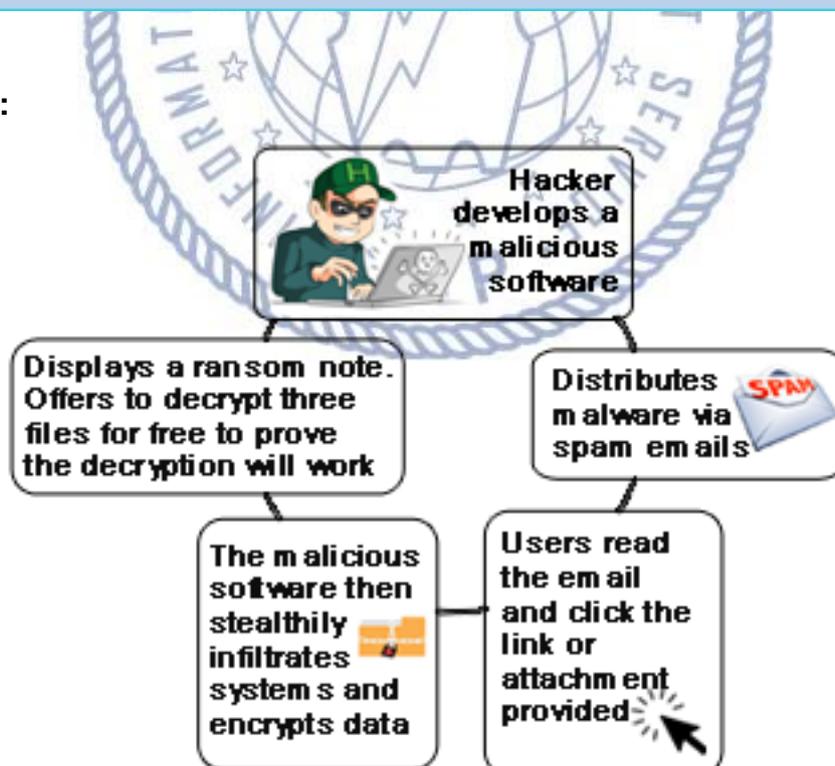
How to obtain Bitcoins?

- \* 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](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.

How it works:



*Note: Payment of ransom is no guarantee that hacker will send a key to decrypt the infected data.*

## Modus Operandi:

- Via email with subject lines “Scanned from Lexmark”, “Scanned from Epson”, “Scanned from HP”, and “Scanned from Canon” which contains 7zip attachment with a VBScript downloader.

## Security Risks to PNP Computer Systems and Data:

- Data can be altered, damaged, deleted, and infused with additional computer viruses.
- Risk profile such as data breach, possible espionage and cyber terror; and
- Interfere with the normal functioning of the computer system or prevent its utilization.

## Mitigation Measures:

- Back up and test your data regularly;
- Avoid opening e-mails from unverified or questionable sources;
- Avoid illegal websites or torrent sites;
- Use genuine software and patch/update;
- Scan your computer regularly using antivirus software;
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching the end users; and
- Run regular penetration tests as often as possible and practical.

## If infected:

- Reformat the computer and restore back-up; and
- Contact ITMS WSCSD for technical support assistance.

*Warning: Once infected by Ransomware there is a high risk that the computer system cannot be restored to its working condition or recover the infected files.*



## For further inquiries, contact ITMS WSCSD:

- Telephone Number: **(02) 723-0401 local 4225**;
- E-mail address: **wcsditms@pnp.gov.ph**; and
- Chat Service: **www.itms.pnp.gov.ph**.