PNP Computer Security Bulletin CSB17-015

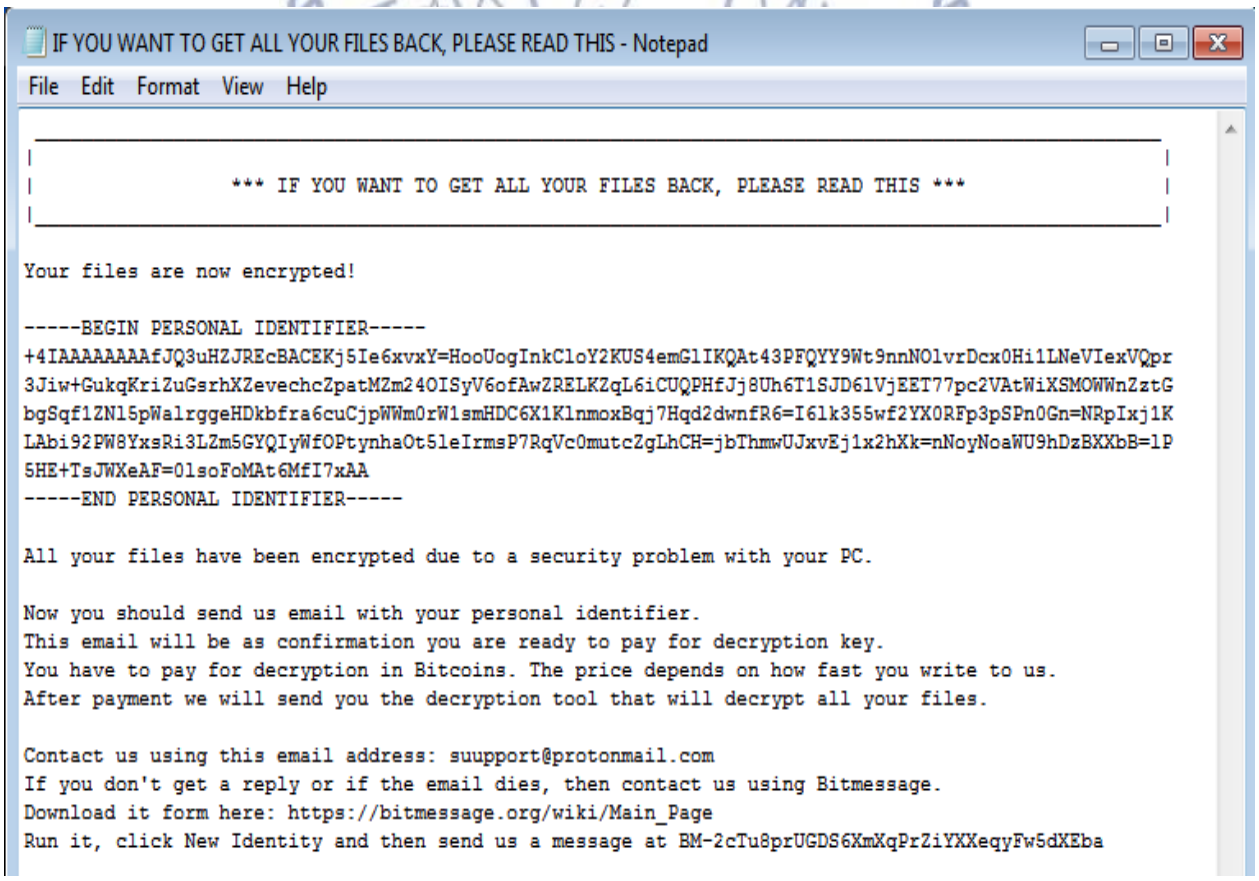
Scarab Ransomware

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".

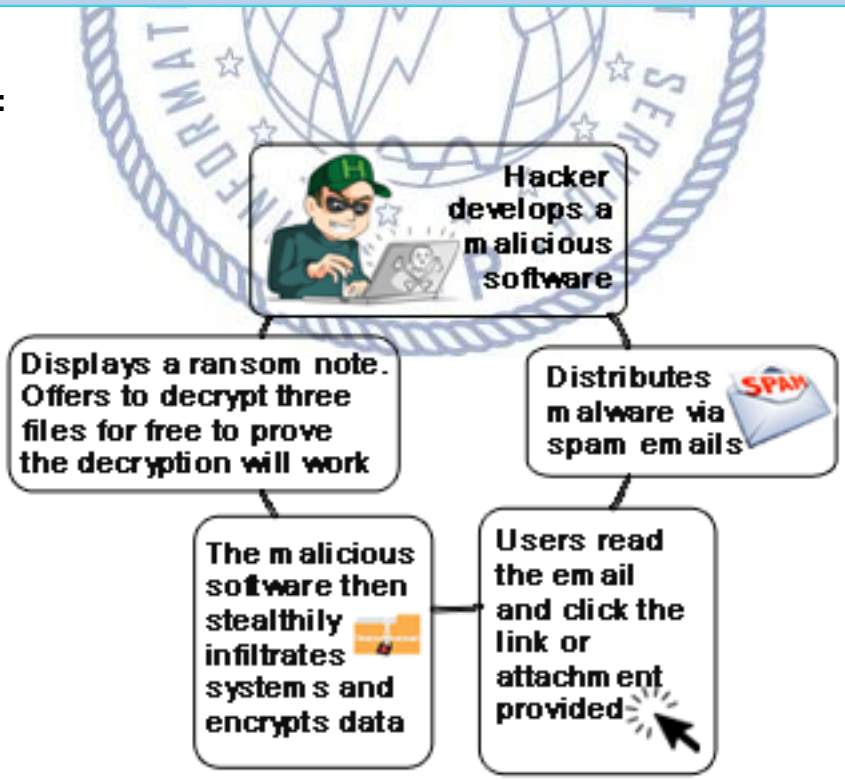


```
Free decryption as guarantee!
Before paying you can send us up to 3 files for free decryption.
The total size of files must be less than 10Mb (non archived), and files should not contain
valuable information (databases, backups, large excel sheets, etc.).

 _____________________________________________________________________________
|                                                                             |
|  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
| * 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: **wscsditms@pnp.gov.ph**; and
- Chat Service: **www.itms.pnp.gov.ph**.