PNP Computer Security Bulletin CSB17-016

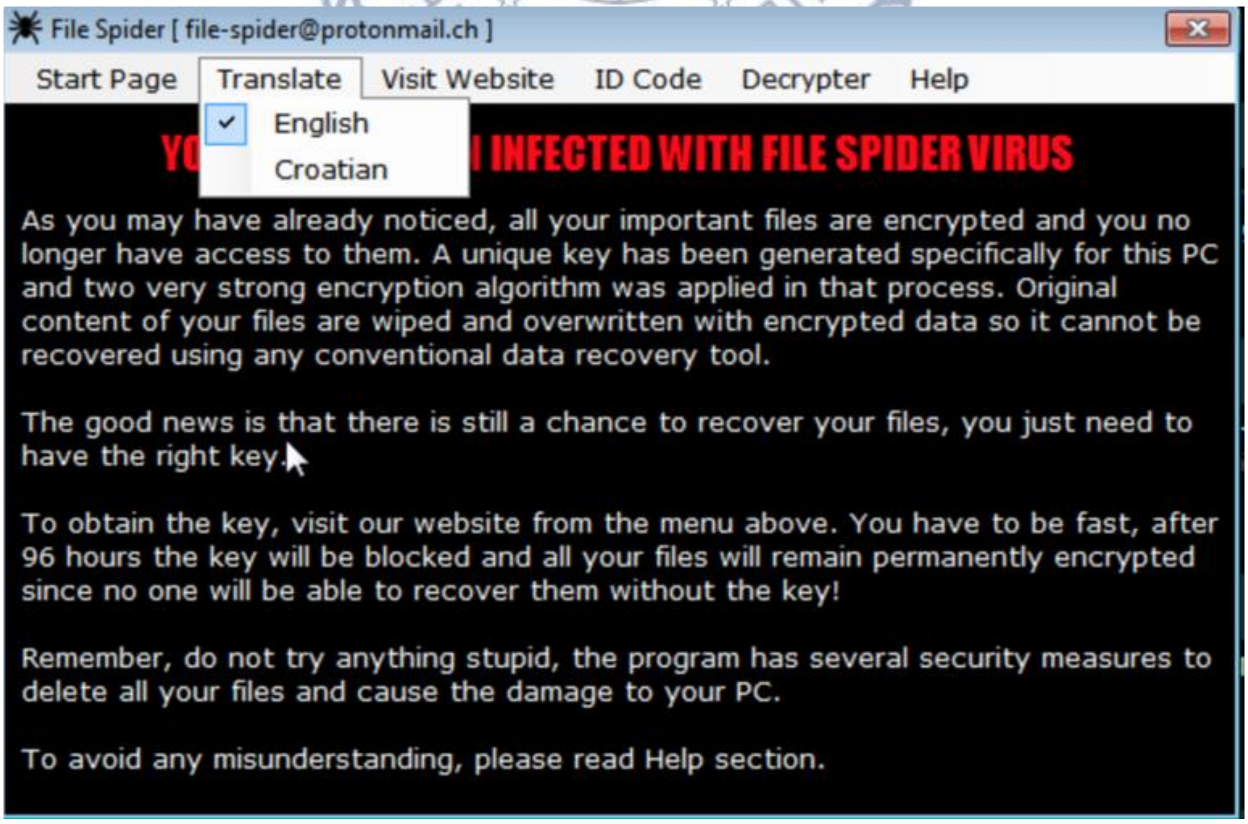
Spider Ransomware

Risk/Impact Rating: **SERIOUS**

Created: December 13, 2017

Description:

- Spider Ransomware is targeting victims in Balkans;
- Distributed using spam emails with malicious attachments that are written in the Bosnian language which contain obfuscated macro code;
- Spam emails were sent to victms with malicious Office documents with the subject line “Debt Collection”, according to Google Translate of the Bosnian-language phrase “Potrazivanje dugovanja”;
- These attachments are auto-synced to the enterprise cloud storage and collaborations apps;
- Decoy document: ‘VB:Trojan.VBA.Agent.QP’
- Downloaded payload: ‘Trojan.GenerickD.12668779’ and ‘Trojan.GenericKD.6290916’;
- A ransom note tells the victim they’ve been infected with the Spider Virus and that they need to make a bitcoin payment for the right key in order to get their files back;
- Victims are given a 96-hour deadline to pay;
- Attackers assure victims that the ransom payment and file recovery process will be “really easy”;
- Attackers provided a link to a video tutorial on how the Spider ransomware payment and file recovery process works.



YO

I INFECTED WITH FILE SPIDER VIRUS

As you may have already noticed, all your important files are encrypted and you no longer have access to them. A unique key has been generated specifically for this PC and two very strong encryption algorithm was applied in that process. Original content of your files are wiped and overwritten with encrypted data so it cannot be recovered using any conventional data recovery tool.

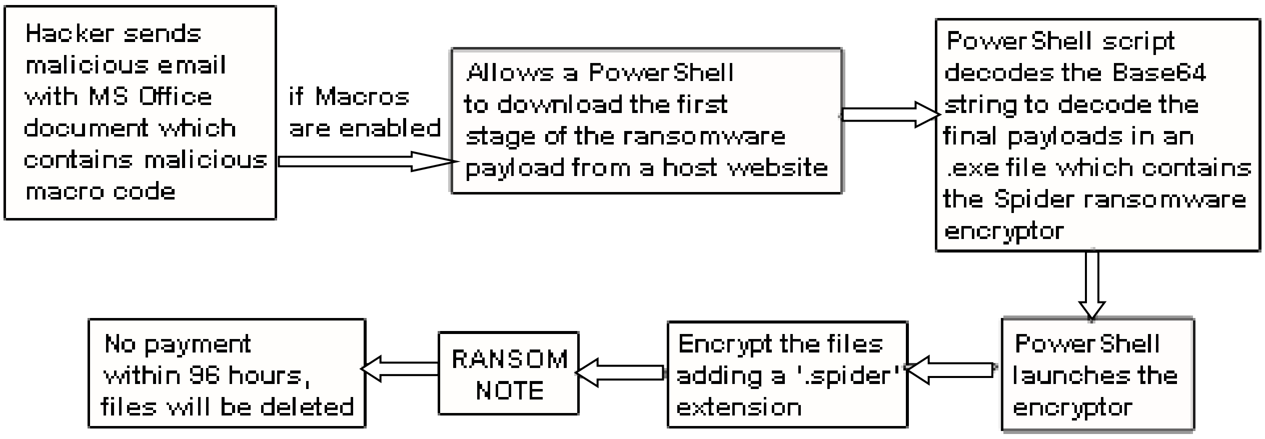
The good news is that there is still a chance to recover your files, you just need to have the right key.

To obtain the key, visit our website from the menu above. You have to be fast, after 96 hours the key will be blocked and all your files will remain permanently encrypted since no one will be able to recover them without the key!

Remember, do not try anything stupid, the program has several security measures to delete all your files and cause the damage to your PC.

To avoid any misunderstanding, please read Help section.

How it works:


Hacker sends malicious email with MS Office document which contains malicious macro code
if Macros are enabled
Allows a PowerShell to download the first stage of the ransomware payload from a host website
PowerShell script decodes the Base64 string to decode the final payloads in an .exe file which contains the Spider ransomware encryptor
PowerShell launches the encryptor
Encrypt the files adding a '.spider' extension
RANSOM NOTE
No payment within 96 hours, files will be deleted

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

Modus Operandi:

- Via email with subject line “Debt Collection” which contains malicious macros

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;
- Disabled Macro setting;
- Avoid opening e-mails from unverified or questionable sources;
- 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**.