COMPUTER SECURITY BULLETIN

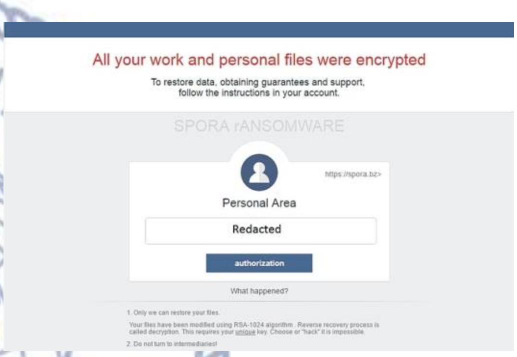
Risk/Impact Rating: SERIOUS

< SPORA >

CSB17-013

Description:

Spora is written in C and is packed using the UPX executable packer. It doesn't rename files it encrypts.



All your work and personal files were encrypted

To restore data, obtaining guarantees and support,
follow the instructions in your account.

SPORA rANSOMWARE

https://spora.bz>

Personal Area

Redacted

What happened?

1. Only we can restore your files.

Your files have been modified using RSA-1024 algorithm . Reverse recovery process is called decryption. This requires your unique key. Choose or "hack" it is impossible.

2. Do not turn to intermediaries!

It can cause problems for the solutions that are designed to protect against the ransomware.

Features:

- Solid encryption routine
- Ability to work offline
- A very well put together ransom payment site

Spora offers several packages such as victim can choose only to recover encrypted data or opt for recovering data and gain immunity from future ransomware attacks.

Currently, the Spora ransomware only targets Russian users and is distributed via spam emails that pretend to be invoices. These emails come with attachments in the form of ZIP files that contain HTA files.

These HTA (HTML Application) files use a double extension, as PDF.HTA or DOC.HTA. On Windows computers where the file extension is hidden, users will see only the first extension and might be tricked into opening the file. Launching any of these files starts the Spora ransomware process.

Recommendations / Solutions / How To's:

For PNP Personnel

- Regular Data Back-up;
- Use strong passwords;

- Don’t open attachments or click on links unless you’re certain they’re safe;
- Keep your software up-to-date;
- Maintain up-to-date anti-virus software, and scan all software downloaded from the internet prior to executing;
- Use a reputable security suite;
- Do not follow unsolicited Web links in emails;
- Show hidden file extensions;
- Disconnect from WiFi or unplug from the network immediately.

For Key officers and Technical Staff

- Restrict users’ ability (permissions) to install and run unwanted software applications;
- Avoid enabling macros from email attachments;
- Filter EXEs in email;
- Disable files running from AppData/LocalAppData folders and RDP (Remote Desktop Protocol);
- Check to see if a decryptor is available;
- Use system Restore to get back to a known-clean state;
- Set the BIOS clock back;
- Enable and properly configure Firewall;
- Secure web browser; and
- Disable macros in Office documents.

References:

http://www.welivesecurity.com/2016/10/10/ransomware-expert-advice-keep-safe-secure/

https://www.hackread.com/spora-ransomware-infects-users-with-good-faith/

http://www.pymnts.com/news/security-and-risk/2017/spora-ransomware-cybersecurity-problems/

http://bestsecuritysearch.com/spora-ransomware-virus-removal-steps-protection-updates/

https://www.bleepingcomputer.com/news/security/spora-ransomware-works-offline-has-the-most-sophisticated-payment-site-as-of-yet/

http://virusguides.com/spora-ransomware-working-offline-proficient-payment-website/

http://www.pcauthority.com.au/News/447366,spora-ransomware-encrypts-offline-and-offers-unique-payment-options.aspx