Priorities in Cyber Security

Dr. Christo Panchev

http://github.com/cpanchev

Complexity

- Black Hat Asia (2017) Locknote
  - https://www.youtube.com/watch?v=aEss6WxSNM8

- You can't solve all the problems in the world
  - You can't even solve a single problem completely
  - Contribute towards the solution

Choosing your project

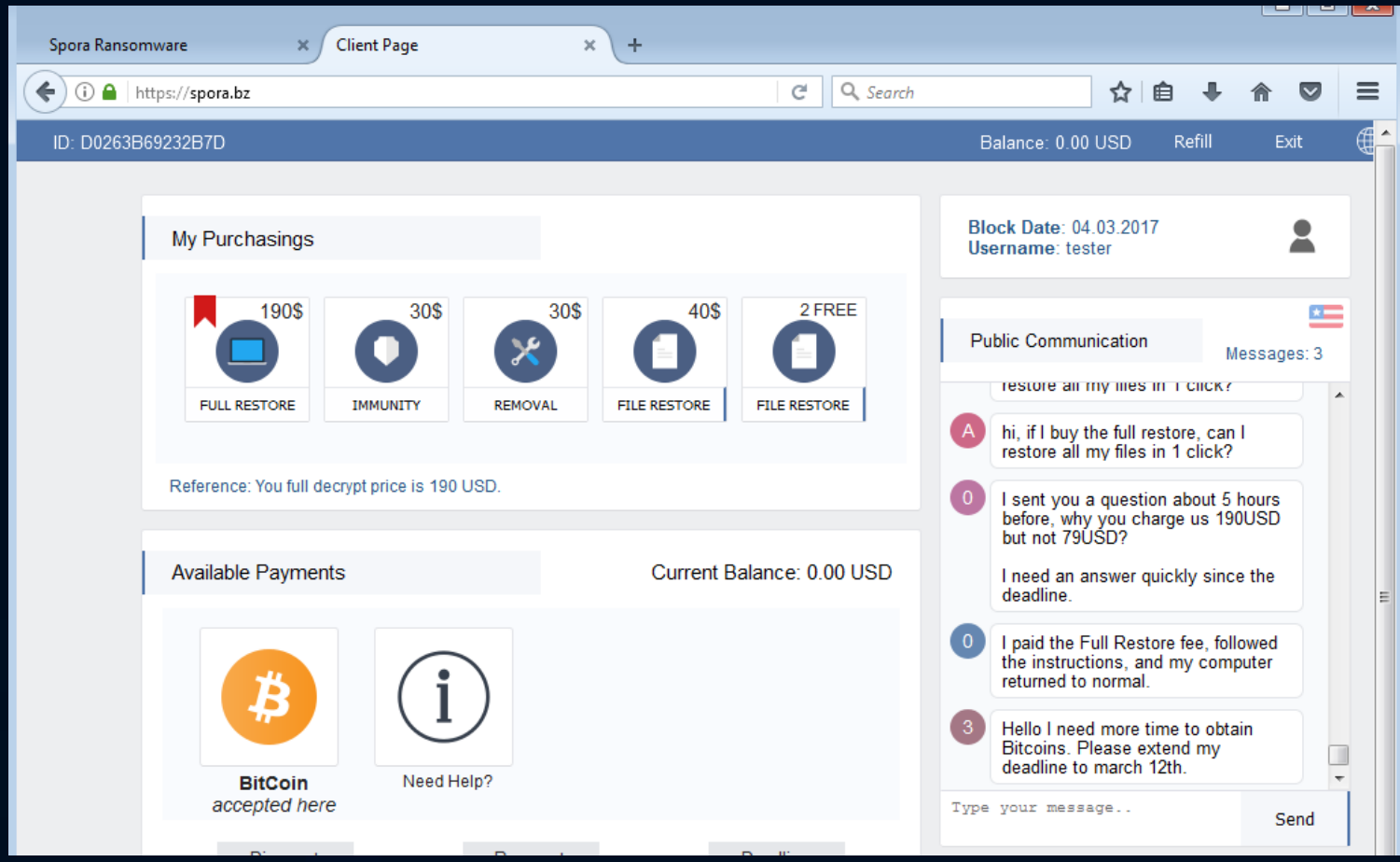
- Interesting enough - love it
- Challenging enough – you can be proud of what you have done
- Simple enough - you already 'know' how to do it

WebApps Security

- We still can’t get this right
- HSTS (and HPKP) have now been broken

Ransomware

- It is now a business model
- Protect
  - Detect and stop an attack
  - Signatures don't work
- Mitigate
  - Recover data after attack



Wireless Networks

- Both popular ones (WiFi and Bluetooth have been broken)
  - BlueBorne – can compromise any Linux/IoT device
  - WPA-2 Key reinstallation attack

- Tools to automatically assess whether a device is vulnerable

Internet of Things (IoT)

- A lot of insecure devices
  - Short development cycle
- Low power devices
- Monitor network/enviroment

Multifactor authentication

- Do we
  - Replace password
  - Compliment passwords
- Optimal combinations

- Automatic identification
  - Face/voice recognition
  - Behavioural analytics (typing, mouse use, apps use, etc.)

Incident Response

- When (not it) we get compromised – are we ready
  - Intrusion Detection/Prevention systems
    - A.I. is becoming a major development method
  - Automated Log Analysis
  - Incident Response Plans
    - Testing
    - Assessment

Open Source Intelligence (OSINT)

- There is a wealth of information out there
- Profile targets (individuals and organisaitons)
- Threat intelligence
- Help in
  - IR investigations
  - Police investigations
- Advanced/automated tools

Closing the weakest link

- User security awareness
  - Training
  - Assessment
  - Mitigation

A system is only as secure as it's weakest link

EU General Data Protection Regulation (GDPR) 2018

- Applies to
  - *controller* says how and why personal data is processed (main legal obligations)
  - *processor* acts on the controller's behalf (has legal obligation for the security of data)
- Applies to
  - organisations operating within the EU
  - organisations outside the EU that offer goods or services to individuals in the EU.
- Applies to
  - Personal data – wide range definition (basically anything that can be used to identify a person)
  - Sensitive personal data – genetic, biometric, etc.
- Penalties of up to £20 million or 4% of annual global turnover – whichever is higher.

GDPR Principles

Personal data shall be:

- (a) processed lawfully, fairly and in a transparent manner
- (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- (d) accurate and, where necessary, kept up to date
- (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
- (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.