Trends through CERT-EE eyes

Klaid Mägi
CERT-EE

Tallinn - September 2015
24/7 “attacks”
Phishing campaigns

Amount increased

Better language

Smart content

Evolving frameworks
Defacement waves

By hosting provider

By ASN

By country
Example
Example (2)

Hacked By Islamic State

@isis_cyberarmy

My.Email

isis-cyberarmy@mail.ru
Drive by attacks

Smart acting

More sophisticated

Erasing evidence
“Hit and Run” is getting boring

Better preparation

Focused targets

...
B2B fraud

Invoice hijack

Manual conversation

Very good background info

Usually attack lifecycle is long (> 2 months)
Media is not helping

They are fast

They don’t think

Amplifying the damage
Law issues

- DPI & IPS/IDS
- Logs
- Personal private data
- Information sharing
- Scanning
- Honeypots
- Hackback ... Active defense
Problems

• Missing cooperation
• Incomplete monitoring
• Non-existent experience
• No emergency plan
• Very low awareness
Thank You!

Klaid Mägi
klaid@cert.ee