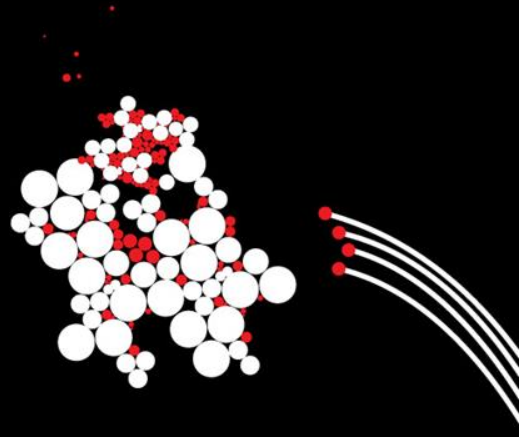
UNIVERSITY OF TWENTE.

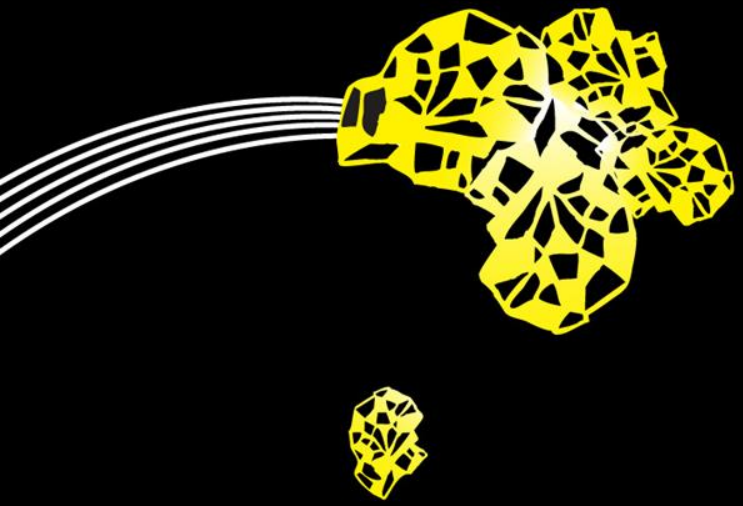


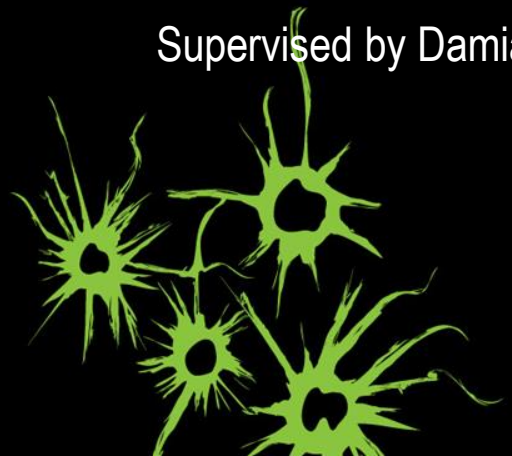
C&C Botnet Detection over SSL

Author: Riccardo Bortolameotti

Contact: r.bortolameotti@utwente.nl

Supervised by Damiano Bolzoni





Agenda

- Problem
- Our Method
- Results
- Conclusions

Problem – Are botnet using SSL?

Our Method - How did we face the problem?

Assumptions:

- Encrypted part cannot be attacked due to capability reasons, we focus on the plaintext part (i.e. handshake)
- SSL is not “controlled” in background application as it is in browsers

Results – Potential Botnet

- 34 connections over 14 different countries (from May to July)
- 10 IP identified as malicious by ThreatStop
- They authenticate themselves with an expired SSL certificate of Amazon
- Amazon has investigated the problem

Results - Others

- Detected 5338 broken SSL connections (some of them vulnerable to mitm attacks)
- Other malicious connections running on TOR
- TOR traffic identification among HTTPS traffic
- Detection of infected IP before professional services (e.g. ThreatStop)

Conclusions

- **First SSL-based malware detection system**
- **Lightweight and privacy-preserving solution**
- Rule to identify TOR among HTTPS traffic
- Confirmed the presence of many vulnerable SSL application to mitm
- Detected an infected IP before professional services (i.e. ThreatStop)
- Detected malicious connections over TOR
- Detected, for what we believe, a **botnet**
- Proven that a preventive-approach can work

Thank you – Any Question?

Our Method - Selected Features

- Certificate x509 Validity (chain validation)
- Certificate x509 Generation Date
- Certificate is valid for the Domain requested (i.e TLS server name)
- Request for Mutual Authentication
- Domain requested randomly generated
- Self-signed certificate similar to famous websites (Levenshtein distance)