Applications of Deep Learning for Cyber security

Vinayakumar R
https://vinayakumarr.github.io/
https://vinayakumarr.github.io/Cybersecurity-Lab-at-CEN/
https://vinayakumarr.github.io/ComputationalThinking-Lab-at-CEN/

Center for Computational Engineering and Networking (CEN)

Amrita School of Engineering, Coimbatore

Amrita Vishwa Vidyapeetham

18th December, 2018

Upcoming Shared tasks

The following shared tasks are organized by Mr. Akarsh M (MTech student), Mr. Vinayakumar R, Prof. Vijay Krishnan Menon, Prof. Prabaharan poornachandran, Prof. Soman KP and Prof. Mamoun Alazab

1. IOT Malware Classification
2. Windows Malware Classification
3. Ransomware Classification

Problem Statement

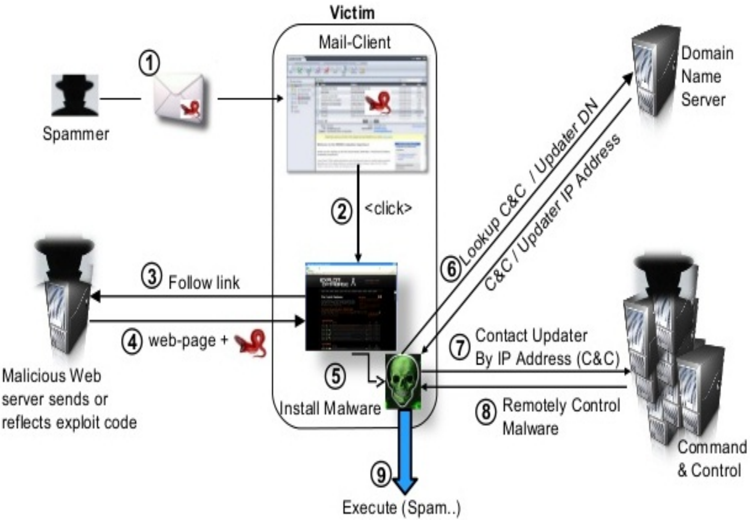

Figure 1: A Typical Threat Example

Problem Statement Contd...

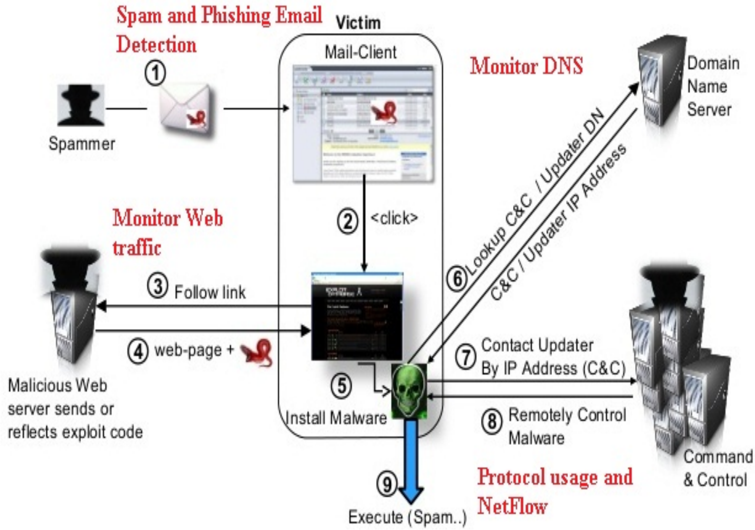
Spam and Phishing Email Detection
Victim
Mail-Client
Monitor DNS
Domain Name Server
①
Spammer
② <click>
Monitor Web traffic
③ Follow link
④ web-page +
Malicious Web server sends or reflects exploit code
⑤ Install Malware
⑥ Lookup C&C / Updater DN
C&C / Updater IP Address
⑦ Contact Updater By IP Address (C&C)
⑧ Remotely Control Malware
Command & Control
⑨ Execute (Spam..)
Protocol usage and NetFlow

Figure 2: A Typical Threat Example and its various levels of Cyber security solution

Problem Statement Contd... I

1. With an increasing amount of people getting connected to Internet, the malicious activities that cause massive harm are increasing also.
2. Most commonly an attacker use malware to conduct malicious activities.
3. Cyber attack is a type of malicious activity which can be detected using firewall and intrusion detection system. However, Both firewall and IDS can be considered as an initial shelter for attack detection rather than malware detection.
4. Malwares are efficiently spreaded through Email, URL and DGA.
5. Malware can be detected using malware binary analysis. This provides detailed information on the structure and behaviour of the malware.
6. Malware binary analysis requires more time to reverse engineer the binaries to create signatures. By the time the Anti-Malware signature is available, there is a chance that a significant amount of damage might have happened.

Problem Statement Contd... II

7. However, it may be detected faster through cyber threat situational awareness events such as Email, URL, DGA and information of malware and security events in social media resource, Twitter.

Aim

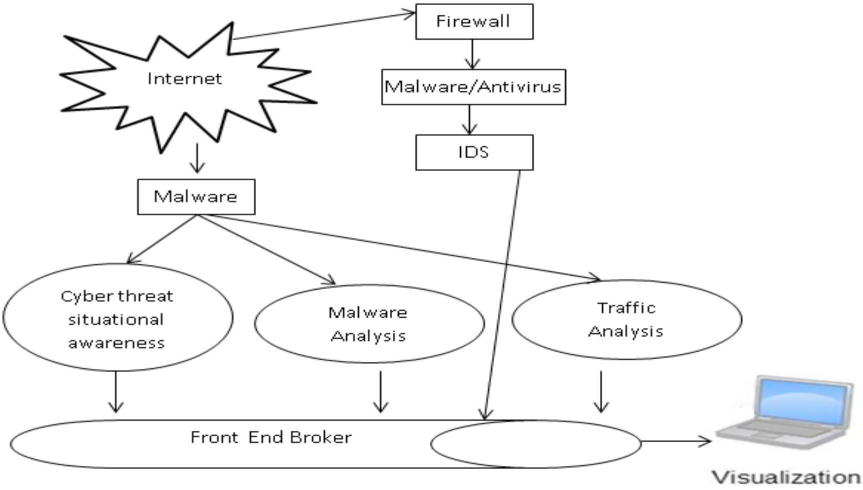

Figure 3: Scalable and Hybrid Framework. All components are not shown

cyber security use cases

1. Domain name system Data Analysis
2. Network Intrusion Detection
3. Malicious URL Detection
4. Spam Email Detection
5. Image Spam Detection
6. Malware Analysis