

Analiza automată a comportamentului dinamic al virușilor

Conducători științifici
C. d. asociat Topan Vlad
Conf. Dr. Boian Rareș

Absolvent
Oancea Alin-Andrei

Cuprins

- Malware
- Analiza de malware
- Lucrări relevante
- Analiza automată a comportamentului dinamic al virușilor (aplicația)
- Proiectare, implementare și tehnologii folosite
- Concluzii
- Extinderi posibile
- Demo & Întrebări

Malware

- Tipuri de malware
- Măsuri siguranță

Analiza de malware

- Analiza statică
- Analiza dinamică
- Analiza automată

Lucrări relevante

- VirusTotal
- Hybrid Analysis
- Cuckoo Sandbox

Analiza automată a comportamentului dinamic al virușilor

- Metoda abordată
 - Fișiere
 - Chei de regiștri
- Utilitatea

Proiectare și implementare

- Fișiere de configurare
- Interfața web - python/bottle
- Interfața de tip consolă

Tehnologii folosite

- Python3
- VirtualBox
- Python-VirtualBox

Concluzii

- Utilitatea aplicației

Extinderi posibile

- Monitorizarea traficului de rețea
- Suport pentru mai multe hypervizoare
- Ascunderea utilităților de analiză

Demo & Întrebări