

JUGAAD: Comprehensive Malware Behavior-as-a-Service

¥

Sareena K P, Nikhilesh Singh, Chester Rebeiro, Kamakoti V. Indian Institute of Technology Madras, India

15th Cyber Security Experimentation and Test (CSET) 2022.

Cyber Attacks – A Harsh Reality \widehat{X}

Accenture Hit By Ransomware Attack, Latest Victim Of 'Cyber-Pandemic'

'If a \$45 billion company like Accenture is vulnerable then everyone is vulnerable,' says Michael Goldstein, CEO of



Cyber Attacks – A Harsh Reality \widehat{X}

Accenture Hit By Ransomware Attack, Latest Victim Of 'Cyber-Pandemic' 'If a \$45 billion company like Accenture is vulnerable then everyone is vulnerable,' says Michael Goldstein, CEO of Florida-based solution A New Wave of Malware Attack Targeting Organizations in South By Joseph F. Kovar America September 20, 2021 • Ravie Experts Uncover Spyware Attacks Against Catalan Politicians and Activists Money & Banking MALWARE 🛗 April 19, 2022 🛛 🛔 Ravie Lakshmanan Beware of trojan malware attack, 27 major banks Debangana Ghosh | Mumbai | Updated on Septembe **Despite having state-of-the-art Antivirus software!!**



Confronting Cyber Attacks





Confronting Cyber Attacks



In-depth understanding of Ground-truth of malware behavior

Objectives, functionalities, and consequences



Run-time Behavioral Analysis

3



Malware



Access to Malware Samples





Access

Access to LIVE samples Monopolized by Enterprises High-Cost 12K samples @ 82K\$

2 Older malware samples (Stale)







Capturing Behavior









Multiple Pain Points



Precise collection: Timely execution of live malware in real-world connected conditions



Malware Behavior-as-a-Service



Alternate Model: Malware Behavior-as-a-Service

X2

JUGAAD: Malware Behavior-as-a-Service





For Malware Researchers



Users: Malware researchers from academia and industry







Access to malware samples **7** K7 SECURITY

2.7 TB of data, 22M behavioral snapshots

- Facilitates **precise**, **unbiased** view of diverse **perspectives** of malware activity
- **Offloads** time, efforts, and cost, while alleviating risk.
- Enables a fair platform for comparison of detection mechanisms
- Opens up the field for researchers in **non-security domains (data science)**
- Quickly explore and build novel solutions
- Future work: Include other **perspectives** (memory, instruction traces)

Ministry of Electronics & Information Technology. overnment of India

3

versus

