Tutorial

on

Evolution of Malware and their Detection Techniques

by

Ashu Sharma
Senior Malware Analyst,
Panda Securities, WatchGuard Technologies Inc, India /
Founder, CyberSecSociety (NGO), India
ashu.abviiitm@gmail.com

1 Abstract:

Often computer/mobile users call everything that disturbs/corrupts their system a virus without being aware of what it means or accomplishes. This tutorial systematically gives an introduction to the different varieties of samples that come under the broad umbrella known as malware, their distinctive properties, different methods of analysing the malware and their detection techniques. We will also cover evolution of the complexity of malware and propagation methods for the malware. Furthermore, we will discuss the techniques used by the defence team to detect such malware and the challenges they are facing to create 100% secure environment.

2 Objectives:

This workshop will cover fundamental techniques, limitations, open research problems and future directions in the field of malware analysis and detection. Following are the three specific learning outcomes:

1. Audiences will get familiarity with different types of malware and their detection techniques.
2. Applications of classification and clustering based frameworks, tools and techniques for malware detection.
3. Overview of significant research problems in the area of malware analysis and detection, results and conclusions from the recent research papers.

3 Target Audiences:

Senior undergraduate students (B.E.), postgraduate students (M.E./M.Tech./M.S.), PhD. students, faculty members and researchers working or interested in the area of malware analysis and detection.

4 Duration:

1.5 Hours

5 Pre-requisite

1. Basic knowledge of the operating system (windows)
2. Understanding of assembly codes & C programming language
3. Familiarity with classification and clustering techniques (Desirable)

6 Topics to be covered:

1. Introduction of malware
2. Traditional Malware Detection Systems
3. Types of Malware Signatures used
4. Signature generations
5. Static Malware Analysis
6. 2nd Generation Malware
7. Dynamic Malware Analysis
8. Non Signature-based techniques
9. Challenges in Malware Detection

7 Hands-on session:

Laboratory activities will involve analyzing and handling malicious code on a test system. Virtual machines can be used but it is not recommended to use the organization's laptop in laboratory activity.

8 Similar Tutorial @ other conference and workshops by speakers:

1. A Tutorial on Malware Analysis @*IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridCom) 2021, Aachen, Germany*
2. A Tutorial on Malware Analysis @*IEEE International Conference on High Performance Switching and Routing (ComSoc) 2021, Paris, France*
3. A Tutorial on Malware Analysis @*2021 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom) 2021, Bucharest, Romania*
4. A Tutorial on Malware Analysis @*FDP (2021) on "Cryptography for Network Security", CSE department, NITTTR Chandigarh, India*
5. A Tutorial on Malware Analysis @*Short Term Training Program on "Cyber Security Threats and Safeguards" (2021) under Information Security Education and Awareness (ISEA) - Project (Phase-II), GTU-GSET,Gujrat, India"*
6. A Tutorial on "Advanced Malware Analysis" @*Best Of The World In Security" by CISO Platform and SACON (2020), Banglore, India*
7. Advanced Malware and their Detection Technique @*SPACE 2019, IIT Kanpur, India*
8. Malware Analysis @*TENCON 2019, Kochi, India*

9 More details:

1. The tutorial is designed and delivered by specialist from industry and academics.
2. The tutorial will also cover hands-on session for practical engagement.

References

[1] Michael Ligh, Blake Hartstein, and Steven Adair. *Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code*. John Wiley & Sons Inc, 2010.

[2] Ashu Sharma and Sanjay Kumar Sahay. Evolution and detection of polymorphic and metamorphic malwares: A survey. *arXiv preprint arXiv:1406.7061*, 2014.

[3] Michael Sikorski and Andrew Honig. *Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software*. No Starch Press, 2012.

[4] Carsten Willems, Thorsten Holz, and Felix Freiling. Toward automated dynamic malware analysis using cwsandbox. *IEEE Security & Privacy*, 5(2):32–39, 2007.

[5] Yanfang Ye, Tao Li, Donald Adjeroh, and S Sitharama Iyengar. A survey on malware detection using data mining techniques. *ACM Computing Surveys (CSUR)*, 50(3):1–40, 2017.

10 Biography

I am Dr Ashu Sharma. My area of interest is to study new Malware and to provide protection for them. I am currently working as a Senior Malware Researcher at WatchGuard Technologies, Noida, India. I have more than 3 years of Industry experience in Malware Analysis and more than 2 years of teaching experience in Academics. I am a speaker for many reputed conferences and workshops. I earned an M.Tech degree in Information Security from the Indian Institute of Information Technology, Gwalior, India. I did my PhD in Static malware analysis from BITS Pilani and worked with Prof. S. K. Sahay (Prof. at BITS Pilani). I worked in "Malware identification via dynamic analysis" with Prof. Sandeep Shukla (Prof. at IIT Kanpur) during my post-doctoral research at IIT Kanpur. I have many publications in Malware detection in reputed Conferences and Journals