Arthur Liou
CS373

Week 1 Writeup

Prompt: Submitting a write-up of your thoughts, impressions, and any conclusions based on the material from the week. Each week will have its own assignment in the grades page.

Write-Up: I'll be writing a paragraph's length of my write-up. If that is "not enough", I've also included my notes from watching the lectures. Unfortunately in Lataex/overleaf, they do not recognize the bullet points and smashed everything into paragraphs, so I apologize for that. Also first time using Latex, so I'll have to keep learning and improving my Latex structure/formatting.

This week's topic and material was a good intro the course. I liked the professor's style of lecturing since I personally like it when the professor ties in real-world events, history, and "how it impacts" type of content. (Side note: Many of my past professors failed to do this or have failed in attempting to do this, so I'm very much looking forward to the other lectures in the course.) Going through the VM instructions and lab was confusing; the VM instructions page was duplicated and seemed put together at the last minute. Similarly for the instructions, it wasn't very clear, although I can see why the professor, TAs, and staff would think it is, what a student should be doing at each particular step. This can be reflected in the questions and uncertainty that students asked in Piazza. I'd suggest, that in the next quarter, the staff sit down with a student or TA and approach the instructions with fresh eyes, so that the steps can be updated (with specific steps, tools, and screenshots) for students who have never used the tools and VMware before to be able to follow along and understand what they are trying to do. Keep in mind that most students have had no experience in any cybersecurity tools (even Windows for that matter), are not on campus (for this class at least), and that having a strong first lab where they can walk through understanding the material and labs will help set them up well for the rest of the quarter. Students have to learn how to walk before they can run. But, overall, my impression of this week is positive; I liked the lab and the professor's lecturing style, so I'm looking forward to the rest of the quarter!

PS: It would help a lot if students had an example of a good lab / writeup. I have no idea what style or format I should be using (hence big paragraph block) and would prefer it the professor/TA specified some sort of template. That way it's not only easier for students to follow along in understanding what the professor/TAs is looking for, but also easier on grading/reading (structured vs unstructured reading).

Lecture Notes

W1L1 – Basics of Malware

- Today is Malware / Theory, will use mainly industry tech terms
- Sony hack. Forensics and malware analysis
- Guesses on where malware was first started

- Started by two brothers in Pakistan who worked for IBM trying to prevent pirated floppies
- Fake AV, Fake Mac Malware
- Malware infection – US is pretty impacted
- Why Malware exists? Pushing limits, OC, fire/break things, advertising, research reasons, weapon, government, Anonymous,
- Motivation: Recon, Political, Financial, Destruction
- Honeypot to catch malware
- Checksum/hash of the file
- Driver in the malware
- Understand and describe the threat, author countermeasures, approach design and dev from an anti-attacker perspective
- DGA – domain generating algo
- Malware industry basics – 25 years
- Malware – Malicious software
- Viruses – parasitic, polymorphic, worms
- Trojans
- Potentially unwanted program (PUP, PUA, PUS) – adware, spyware, tools
- Various exploits / vectors
- Goats to analyze malware – machine you sacrifice for malware. Today for VMs
- Honeypot – catching. Goat – on purpose to infect
- Hash – calculating of a file
- IMPhash
- AEP functions
- Infection stats
- Handling Malware: Transport in an inactive state, Exchange of malware and logging it, lock down dev environment, be ready to disconnect at a drop of a hat
- Also renaming file extension from exe to bin
- Malware replication – basic static analysis
- Use the information gathered to write countermeasures.
- Measuring successful replication. Snapshots, what changes occurred

Lesson 2

- Review: Naming Conventions, basics of replication, sample execution, tools,
- XOR
- Agenda: APTs, analyses, continue replication
- APTs = Advanced Persistent Threats
    - Term created by Air Force in 2006
    - Advanced – Attacker is fluent in cyber-intrusion
    - Persistent – Objective and works to achieve their goals without / mission
    - Threat – Organized, receives instructions, is sufficiently funded to perform operations, and is motivated

- Characteristics: Actors, motives, targets, goals
- Patient Zero – first infected machine
- OSINTs – open source intelligence, passive intelligence
- Job hiring posts, scrap website for PPTs / metadata (words, excel, PDFs)
- APT-Kill-Chain
- Step 1: Recon
- Step 2: Weaponization
- Step 3: Delivery
- Step 4: Exploitation
- Step 5: Installation
- Step 6: Command and control
- Step 7: Action on Objectives
- Critical asset
- Forensic analysis: contextual metadata leading researcher to this point
- Static analysis, dynamic analysis
- Stories and lab lectures
- XOR encryption
- Base64 – never call encryption
- FileInsight tool
- Packer – compressed compiled code
- UPX – basic packers
- High entropy – very dense
- Source analysis
- Delphi code, compress / decompress
- String analysis lab