Automated and Ad-Hoc Malware Analysis

Jason Yohanan, Paul Benoit, Yaqi He, Rahat Kamal, Lorenzo Testagrossa

Sponsor: INOVA

Subject Matter Expert: Mark Jenkins

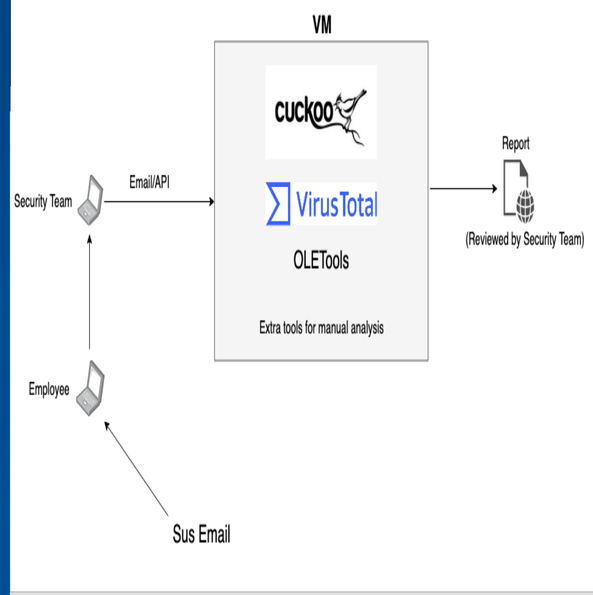
Background

- Ensuring a users data is digitally guarded from a variety of malware attacks.
- Working with INOVA to design an automated and ad-hoc malware analysis solution to can analyze files submitted via email and API to see if they potentially contain malware
- Automate this malware recognition process of files that traverse the network and give them an optimal solution protect their clients and employees.

Objectives/Purpose

- Configure an environment that automates the process of recognizing malicious email or API files.
- Cuckoo automates the recognition process and ejects a malware analysis report to see if inputted files contain malware.
- Connected Cuckoo to VirusTotal and OleTools to encapsulate their registries.
- Cuckoo uses these registries to complete it's outputted report to the end-user.
- Reduces time in the analysis and validates Cuckoo reports.

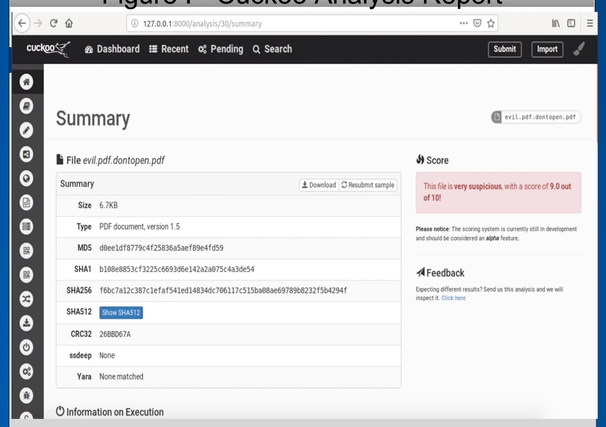
Approach/Tools



- Our Virtual Machine uses:
  - Cuckoo, VirusTotal, and Oletools.
- An Email or API file is inputted to the VM and the three programs will analyze it.
- Report any anomalies or infections, and detection of malicious files.
- A user-friendly report will be outputted.
- VirusTotal is used to analyzes suspicious files and URLs to detect types of malware from a community collected list.
- OLEtools used to analyze Microsoft OLE2 files.

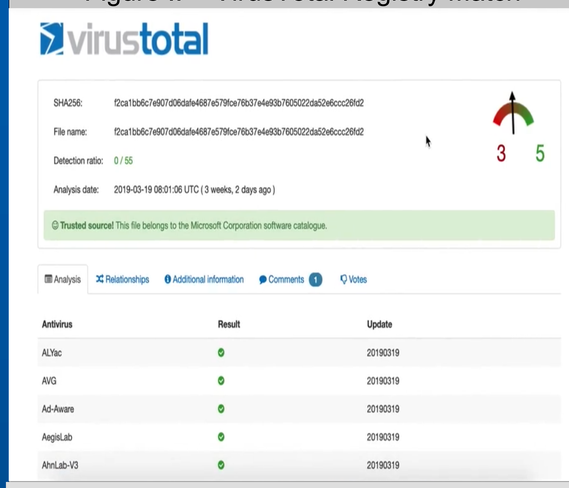
Verification/Results

Figure I - Cuckoo Analysis Report



- Cuckoo report detecting a banking Trojan (malware)

Figure II - VirusTotal Registry Match



- Above is a VirusTotal report verifying that a common utility is not malware

Conclusions

- Our solution is an integrated framework that contains both local malware analysis system and remote virus database reference.
- Our solution guarantees these tools can detect various malware sources and notify INOVA security team members.
- A concise report will be generated and sent to the cybersecurity team to help them quickly identify the malware and resolve vulnerabilities.
- Our framework is scalable to allow for additional malware detection or prevention functionalities according future customer desires.

Acknowledgments

- It was a privilege to work alongside INOVA and create such a meaningful product for them to implement into their network architecture.
- We would like to express our sincerest form of gratitude and gratefulness to Mark Jenkins, Marty Baron, Scott Larsen, and Matthew Wilkes.
- Thank you to Professor Gino Manzo, Professor Rock Sabetto, Dr. Brouse, and the CYSE department for their continued support through CYSE 492/493 and the degree as a whole.

References

Cuckoo. "Reporting Results." *Reporting Results - Cuckoo Sandbox v0.3.2 Book*, cuckoo.readthedocs.io/en/0.3.2/customization/reporting/

VirusTotal. "VirusTotal." *VirusTotal*, www.virustotal.com/#/home/upload.

George Mason University. "Downloads." *The George Mason University Brand Profile*, brand.gmu.edu/downloads/.

Mindgrub. "Work." *Mindgrub*, www.mindgrub.com/work.

May 2nd, 2019