Malware Analysis (CS6038)

Week 06.2 Windows Artifacts and Online Analysis

Scott Nusbaum
nusbausa@ucmail.uc.edu

February 21, 2019

University of CINCINNATI

Overview

- Homework 2 Walkthrough
- Walkthrough solution for the in-class problem
- Windows Artifacts
- Online Analysis resources

University of CINCINNATI

Homework

- Homework 2:
  - Due this past Tuesday
  - Fun was not it
- Homework 3:
  - Assigned Feb 14, 2019
  - Due Feb 28, 2019
  - Covers Document Analysis and Windows Artifacts

University of CINCINNATI

Homework

- Walk through my solution of this homework

University of CINCINNATI

In-Class Problem

- Demo 1
  - Walk through the first steps of the malware

University of CINCINNATI

Windows Artifacts

- SANs Poster
- SANs DFIR
- Common Malware Persistence
- Mitre Autoruns

University of CINCINNATI

Online Investigations

- Cymon.io (http://cymon.io)
- Abuseipdb (https://www.abuseipdb.com)
- Shodan.io (https://www.shodan.io)
- Urlscan.io (https://urlscan.io)
- Urlhaus.abuse.ch (https://urlhaus.abuse.ch/)
- AlienVault OTX (https://reputation.alienvault.com/reputation.unix)
- AVCaesar (https://avcaesar.malware.lu/)
- Have I been pwned? (https://haveibeenpwned.com/)
- Hybrid Analysis (https://www.hybrid-analysis.com/)
- Joe Sandbox Cloud (https://www.joesecurity.org/)
- MalShare (https://malshare.com/)
- Maltracker (https://maltracker.net/)
- Malwr (https://malwr.com/)
- Metadefender (https://www.metadefender.com/)
- OpenPhish (https://openphish.com/)
- PDF Examiner (https://www.pdfexaminer.com/)
- PhishTank (http://www.phishtank.com/)
- QuickSand (https://www.quicksand.io/)
- Safe Browsing (https://developers.google.com/safe-browsing/)
- Threat Crowd (https://www.threatcrowd.org/)
- ThreatStream (https://www.anomali.com/platform/threatstream)
- URLVoid (http://www.urlvoid.com/)
- VirusTotal (https://www.virustotal.com/)
- VxStream (https://www.vxstream-sandbox.com/)

University of CINCINNATI