Malware Analysis (CS6038)

Week 09.1 Communication

Scott Nusbaum
nusbausa@ucmail.uc.edu

March 12, 2019

University of CINCINNATI

Overview

- Homework
- Communication
  - Consulting
  - Release (Write Ups)
  - Internal

University of CINCINNATI

Homework

- Homework 4:
  - Due March 14, 2019
  - Reverse Engineering (Use Ghidra) and PCAP analysis
- Homework 5:
  - Assigned March 28, 2019
  - Subject: Reverse Engineering (3 Shellcode Samples)

University of CINCINNATI

Communication

- Consulting
  - Statement of Work (SOW)
  - Kick off Meetings
  - Engagement Notes
  - Status Updates
  - Report Draft
  - Final Report
  - Review

University of CINCINNATI

SOW

- Legally binding document to ensure that both parties understand and agree to the work that is to be completed, deliverables and time frame.
- Contains
  - The scope of the engagement
    - What is in and out of scope
    - Expectations of both parties
  - The responsible parties
    - Set up points of contact
  - The responsibility for deliverables
    - Updates
    - Reports
    - Investigation artifacts
    - Background information
  - The hours to be performed
  - Price of the service and payment details
  - Signatures of all parties

University of CINCINNATI

Kick Off Meetings

- First call between the project lead and the effected company.
- Information Gathering
  - Understanding of the issue
  - Ask about the companies network and systems
  - Ask about logging and resources
  - Ask about timeline and current understanding of the events
- Discuss expectations of the engagement on a lower level
- Setup regular communications
- Setup for of secure data transfers

University of CINCINNATI

Engagement Notes

- Log all events and actions taken during the engagement when they happen
- This begins during the Kick Off meeting(s)
  - Stories evolve and grow as the investigation continues and the story changes as well. Having documentation of the story helps draft a complete story during the report phase
  - Reduces the risk of the consultant misinterpreting or misunderstanding
    - Very useful when providing summaries of meeting notes. This is used to verify understanding of events
- As the investigation continues these notes become the foundation of the client updates and the report.
  - These notes will contain what when and the outcome of each action taken.
    - Normally beginning with steps used to acquire the sample, steps used to verify the samples chain of custody, steps used to determine the type of malware and the steps used to investigate the malware

University of CINCINNATI

Status Updates

- Updates are sometimes required in the SOW but if not it is a good practice to set up reoccurring updates with the client during the Kick Off meeting.
- Updates should meet exactly that agreed upon in the SOW (this is a legal document) however if during the investigation it is determined that more frequent updates or a different form of updates are need this is normal.
- Status updates can include conference calls, individual calls, emails, TXT, or in person meetings. The normal method used to provide updates is through email or in-person.

University of CINCINNATI

Update Contents

- Information provided during the updates
  - Current major finding or actions that needed immediate attention
  - Indicators of Compromise (IOC)
  - Actions performed since the last update
  - Actions planned for the immediate future
  - Overall actions plans
  - Time left in the investigation

University of CINCINNATI

Reports and Reviews

- Review the TrustedSec Report Template
- First Draft Deliverable
  - Provides the customer to review the document for understanding and validity.
  - Clients and or their Lawyers review from a legal perspective and might want more clarification or rewording of findings as to better line up with legal constraints
- Review with the customers
  - Occurs with review of the first draft or shortly after the first draft was delivered
  - Allows the client to speak directly with the analyst and ask questions clarify meanings or wording
- Final Report Deliverable
  - If required by the SOW is a legally required document
    - Depending on the SOW the client might not be required to submit payment until the delivery of the report

University of CINCINNATI

Internal to Company

- Generally less formal.
- Communication normally through email, incident tracking system, and standup meetings
- Task assigned to an analyst
  - Assignment should include expected results.
    - Discover Indicator of Compromise (IOC)
    - General overview of malware activities
    - Complete Analysis including potential downloaded modules
    - Number of hours to work on task
- Analyst provides the following
  - Status emails with new IOCs
  - Potential Verbal reports to management
  - Final Report
    - Contains high level of IOCs
    - Contains information on the infection vectors, persistence methods, modules, methods used to spread …

University of CINCINNATI

External Write Ups

- Used to showcase the malware or a new feature
- Goal is to provide information to others about ways to detect, isolate, and remove the malware.
- Must have permission before releasing writeups. Some malware is targeted and if released the attackers then know they have been compromised.
- Types of Write Up Release methods
  - Blog posts
  - News Journals
  - Pod casts
  - Github

University of CINCINNATI