Inspire, Transform and Create (ITC) XXIV – 2020 Digital Forensics
Written by: Brock Bell, Digital Forensics Certification Board

Background Information

Due to the recent outbreak of CoronaVirus, small medical practice owner, Janet Hart, has been working from home more frequently and conducting appointments virtually through Zoom. A couple days ago, she noticed a few weird movements of her mouse, among other "weird things." Out of frustration and confusion Janet has called her IT provider for assistance in checking out the problem.

Daniel Cherry, a managed service provider for IT support has been helping Janet get her practice going for the last few months. After some poking around, Daniel notices a remote access program running that he doesn't remember using recently. Daniel informs Janet that her desktop might be compromised and immediately removes the desktop from Janet for an inspection. Although Daniel is computer savvy, he does not have the technical knowledge to complete this digital forensics examination and hires DigiDiscover to complete the task.

Consultant Task

You are the newest members of DigiDiscover and have been tasked to work with Daniel and Janet in conducting a digital forensic investigation into unusual activity on Janet's desktop. As part of your investigation, you should analyze all available evidence to determine if an intrusion occurred, if there is an insider threat, and if there are any other investigations that should be conducted.

The evidence is provided on a virtual disk file. The hash for the provided 7zip container should match `08DAE7D8488018F368DBFBF9006AEB1C`.

Deliverable 1: Expert Witness Report

Teams will be expected to provide a narrative examination report documenting their methodologies, analysis, and findings. The **Final Expert Witness Report** is due no later than **11:59 PM Pacific, April 5, 2020 via Google Form.**

If you do not turn in a report, you will not be allowed to move to the following Presentation Phase. Furthermore, you are not permitted to have anyone other than the members of your team actively play a role in examining the evidence, writing the examination report, or presenting your findings. The following items, at a minimum, should be included in your report:

1) Introduction
    a) A quick description of the compelling event
    b) A description of the services requested
    c) Team Members and the roles they played
2) Summary
    a) Synopsis of findings

3) Methodologies
    a) A description of the evidence you reviewed for the case
    b) Evidence Validation and Verification
    c) What tools were used to review the evidence during the course of the exam
4) Analysis and Findings
    a) Detailed Explanation of any probative or exculpatory findings and the analysis conducted to reach that finding
        i) What was the point of entry into the environment?
        ii) What account(s) were compromised?
        iii) Was there any data ex filtration? If so, exactly what data was exfiltrated?
        iv) Did the attacker successfully access any other machines? If so, how many machines did the attacker access?
    b) Include References to Exhibits
    c) Include definitions of technical terminology
5) Conclusion
    a) Mitigation and Remediation Actions
    b) Were any exceptions noted during the exam
    c) Disposition of all evidence and case materials
    d) Description of all exhibits

NOTE: Teams should be prepared to receive and analyze digital evidence from multiple sources. As with any Digital Forensics / Incident Response case, the provided evidence may hold malicious files. Teams should be careful handling potentially malicious files and take steps to prevent infection of the examination machine or loss of data.

Deliverable 2: Live Presentation

The Presentation powerpoint is due no later than **5:00 PM Pacific, April 10, 2020 via Google Form.** The Live Video Presentation will take place on **Saturday, April 11th, 2020.**

Each team will be expected to present their findings during the ITC Virtual Event in front of the panel of Judges. Your team should be prepared to provide a verbal testimony as to your team's methodologies and findings. The ability of your team to present your findings and accurately represent the evidence will be scored. Each team will have no more than 20 minutes to present their findings, followed by 10 minutes of Question and Answer from the Judges Panel. During the Q & A portion of this phase, you and your team should be able to attest to the findings of your report, provide further meaning as asked, and be able to defend your methodologies.