Incident Response Report #2

This assignment is similar to the last incident response report. You will take the framework you developed for your report, with corrections that I suggested as feedback, then develop a new report for this incident. The grading rubrics will be the same, but the grading will be stricter being this is your 2nd time developing an incident response report.

The incident scenario this time is that an employee was installing a new computer. They were in the process of installing software when they noticed abnormal mouse activity on the computer. At that point, they walked away from the computer and called you for help. Treat this like an incident at a corporation, although the computer is not joined to a domain.

I am expecting that at a minimum you are able to tell the story of what happened during the incident. What was the initial infection vector, what happened next? Are there any persistence mechanisms in play? Are there any IP addresses associated with the attacker? And if so, what are they?

Instead of a 22 page document with evidence, you will be working with evidence that has been extracted from the computer in its raw form just like an incident responder would see if they were working on the workstation. The evidence totals about 7 gigs with the memory image. Some of the evidence collected may overlap evidence that was collected in another method. Some of the included evidence is from:

- Netstat
- Complete directory / file structure listing for the entire C drive
- Services
- Several Kape collections – These will provide a rich set of evidence but take a little bit to get used to the way Kape provides the collected evidence
- Browser information
- Prefetch
- Scheduled Tasks
- Users
- Windows Event Logs
- Forensic RAM image

The evidence can be downloaded from a Google Drive link I'll post on D2L.

Not every piece of evidence collected will yield results. It is your job to comb through the evidence to put together the pieces of what happened to develop your report. You can successfully respond to the incident without doing the memory forensics, but it may provide some easier insights if you want to give it a shot. The memory image is around 5.4 gigs in size. I split the evidence into different folders to make it easier to download and work with if you don't have the full 7 gigs of free space on your drive.

Start by forming your investigative questions, then going searching for evidence that proves your questions. Your IOCs this time will be generated based on actual evidence you find that can be used to search other computers to determine if they are in scope of the incident as well.

I will be providing the VM as an optional way to investigate the incident. The VM is provided as is without any additional support from me. It is a VMWare image. Some of the evidence will still be in the VM, but it will be provided post attack after that attacker is already gone.

To produce your report, analyze the evidence, then summarize and present it using the guidelines from the chapter 16 lecture, chapter 16 from the textbook, and guidance from the "ICS-487 incident report what to include" in the sticky section of D2L.

The report should be at least 5 not counting any pictures utilized and the mandatory coverpage. There will be a point penalty if the report is less than 5 pages. Do not turn in a 50-page report for this assignment. The objective is to be concise as you tell the who what when where and how story.

As previously stated, the raw evidence for this report has already been collected for you. You will need to comb through it to find useful artifacts to fill in the pieces for the report. This means making up a company that was hacked, the name of your company that is responding, etc. Basic remediation steps will also need to be described as partof this assignment. For the lessons learned section, describe in a paragraph or two items that you learned about incident response that you will apply to future investigations based on theevidence that was provided to you this time.

You should list 5 Indicators of Compromise that you gleaned from the evidence that are worth searching for enterprise wide to make sure no other systems are infected. These will be best displayed in a table for the IOC section. These IOCs will be developed when you find artifacts related to the investigation. A timeline should also be put into the report like last time.

You will also need to develop 10 investigative questions that you would ask during the course of this investigation.

Keep in mind that for this project this evidence is manually collected from a single computer. This is a normal amount of evidence one would collect in the course of Incident Response. This is why we are teaching the method of developing investigative leads, turning those leads into IOCs, then searching for those IOCs. This type of manual collection does not scale across more than one or two systems in an incident. The next Incident Response report will involve you collecting the evidence, and then reporting on that evidence you collect.

Make sure you start this assignment early. This is a 400-level class and will require some critical thought to complete this assignment along with utilizing the skills that have been taught up to this point. A quality report will take time to produce especially when it comes to selecting which pieces of evidence to use that will tell the story but not provide unnecessary detail. Also keep in mind the responses I provided to your previous report.

A common mistake is making the executive summary and findings section too technical. This should be written in language that an 80 year old grandma who doesn't have an IT background can understand.

Because this is an academic environment, anytime you use someone else's ideas you must cite it in IEEE format. It is assumed that most of your content will be coming from the provided evidence document. You don't have to cite general information you take from that document. Make sure that you are re-telling the story. It is ok to use a sentence or two once in a while. Do not just copy an entire paragraph from the evidence document and turn that in as your work.

Grading Rubric

Requirement	Possible Score
Coversheet meets specifications including affected organization, incident number or name, date published, name of the organization that performed the investigation, and "Privileged and Confidential"	2
Table of contents	2
Report is at least 5 pages long not including cover sheet and any pictures used as part of the report	3
Good grammar, style, and use of IEEE citations if applicable	10
Formatted according to specifications and style suggestions in Chapter 16 and reporting lecture	10
10 quality investigative questions based on evidence provided	10
5 Indicators of Compromise based on evidence provided	5
1 - 2 paragraphs of lessons learned describing items that you learned from this investigation that you will apply to future investigations	7
Remediation describes exact steps taken to expel malicious actors from the network	5
Who what where when why is told to the best of the author's ability with the evidence provided throughout the documents without making the reader piece any parts of the puzzle together	8
Executive summary containing how the incident was discovered, the type of incident this is what the response was, the goal of the investigation, duration of the work, start and stop date, and who sponsored the work	10

Findings section addresses the goals of the investigation by summarizing the information found in the investigative questions, systems involved, IOC, evidence collected and remediation sections in a manner that is written with nontechnical executives in mind. No more than a page long.	5

Systems involved are described and information that is known based on the limited evidence provided is recorded.	3
Evidence collected section contains detailed account of the evidence that was utilized for the report, how it was collected, what facts it is providing to back up the rest of the report. Any procedures have to be documented in such a way that a third party could replicate the results of the analysis. You may have to do a little googling here to come up with any missing parts of the analysis and collection.	15
Recommendations section describes fixing the holes that caused this incident and any larger suggestions for the company as a whole to improve their overall security posture	5

This report has a total of 25 grading points available. Each individual item will be scored as a percentage adding to a total of 100% for the assignment. Your total percentage will be what percent of the 25 points you get on the assignment. For example, I produce a report that scores a total of 85 of the 100 available percentage points. 85% of 25 is 21.25 so I will get 21.25 points on the assignment.