**Final Project**

**and**

**Report**

**Scareware Beware**

**Prepared by: Madelyn Speers**

**UID: 11803339**

**University of South Florida**

**Foundations of Cybersecurity**

**Table of Contents**

**Page**

1. Introduction…………………………………………………………3

1.1 Abstract……………………………………………………3

1.2 Scenario…………………………………………………...3

1.3 Threat Actor……………………………………………….4

1.4 Target………………………………………………………4

1.5 Campaign………………………………………………….4

1.6 The Exploit…………………………………………………4

2. Stages of the Attack………………………………………………..5

2.1 Renaissance……………………………………………….5

2.2 Weaponizing……………………………………………….5

2.3 Delivery……………………………………………………..5

2.4 Exploit……………………………………………………….5

2.4.1 STIX Viz Representation………………………..6

2.4.2 Soltra Edge Representation…………………….6

2.5 Install…………………………………………………………7

2.6 Command and Control……………………………………..7

2.7 Actions on Objectives………………………………………7

3. Incident Handling Process…………………………………………..7

3.1 Identification Phase…………………………………………7

3.2 Eradication & Recovery Phase…………………………….8

3.3 Lessons Learned…………………………………………….8

4. Exploit References…………………………………………………….8

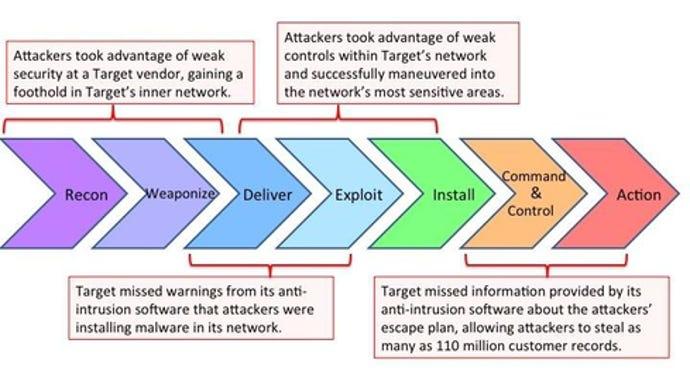
5. References……………………………………………………………..8

1. **Introduction**

**1.1 Abstract**

This report is going to demonstrate the phases of the attack “Scareware” and “NightMare” a malware cyberattack that uses a social engineering tactic to scare people into buying or downloading a malicious software to remove a virus from their computer. This attack is a multi-prong attack and uses spoofing and a sense of urgency to invoke the user to download the malware. A scareware attack is often launched through pop-ups that appear on a user’s screen, warning them that their computer or files have been infected and then offering a solution.[[1]](#footnote-0)

This report will demonstrate the phases of attack using a DHS “Kill Chain”, represented below:



**1.2 Scenario**

For this scenario, I will be defining key actors for the scenario and organize the actors into their respective STIX representation.

**1.3 Threat Actor**

A young computer science major student is currently running low on money while attending University of South Florida, and plans to earn some money by using scareware against other students at the University via ads from a third-party advertising website and sending the ad to students’ emails.

**1.4 Target**

The target for this scenario is the University of South Florida network (WiFi) that thousands of students who attend the university are connected to. This young student plans to use ads through email to get students to download a fake antivirus software as a ploy to earn some quick cash.

**1.5 Campaign**

The student plans to use the scareware “NightMare” as it seemed to have the best effect of social engineering using fear and a sense of urgency. The screen would quickly display a digital illustration of a skull facing right with its jaws open, its teeth covered in blood, and a bleeding bullet hole in its side.[[2]](#footnote-1) It runs in the background of one’s computer and shows the image every 5 minutes and eventually corrupts one’s computer over time. This student plans to use this NightMare scareware and include that it will be removed if they download antivirus software for a price of $50 after the image is displayed. The student plans to use this in the form of an ad advertising Microsoft software from a legitimate looking fake USF email.

**1.6 The Exploit**

“NightMare” is the perfect plan to use on college students. It inflicts a sense of fear and confusion as to why it's happening on their computer. The student hopes someone will fall for this illicit plan and they can earn some cash quickly.

**2. Stages of the Attack**

**2.1 Renaissance**

The student uses a third-party advertising service to deploy the fake Microsoft software advertisement. This was very easy to use due to the site Genius Monkey, which creates the ads for the student. Now the student will add a virus to this ad. He makes it so the ad will redirect the person who clicks on it to several different URLs, then infecting the computer with the scareware.

**2.2 Weaponizing**

The student embeds the ad with malicious malware and when a person clicks on it, the virus “NightMare” will be installed on their computer which will then prompt them to download antivirus software to their computer for $50 to get rid of the image. Since the ad is posing as Microsoft software, students will be more inclined to view it.

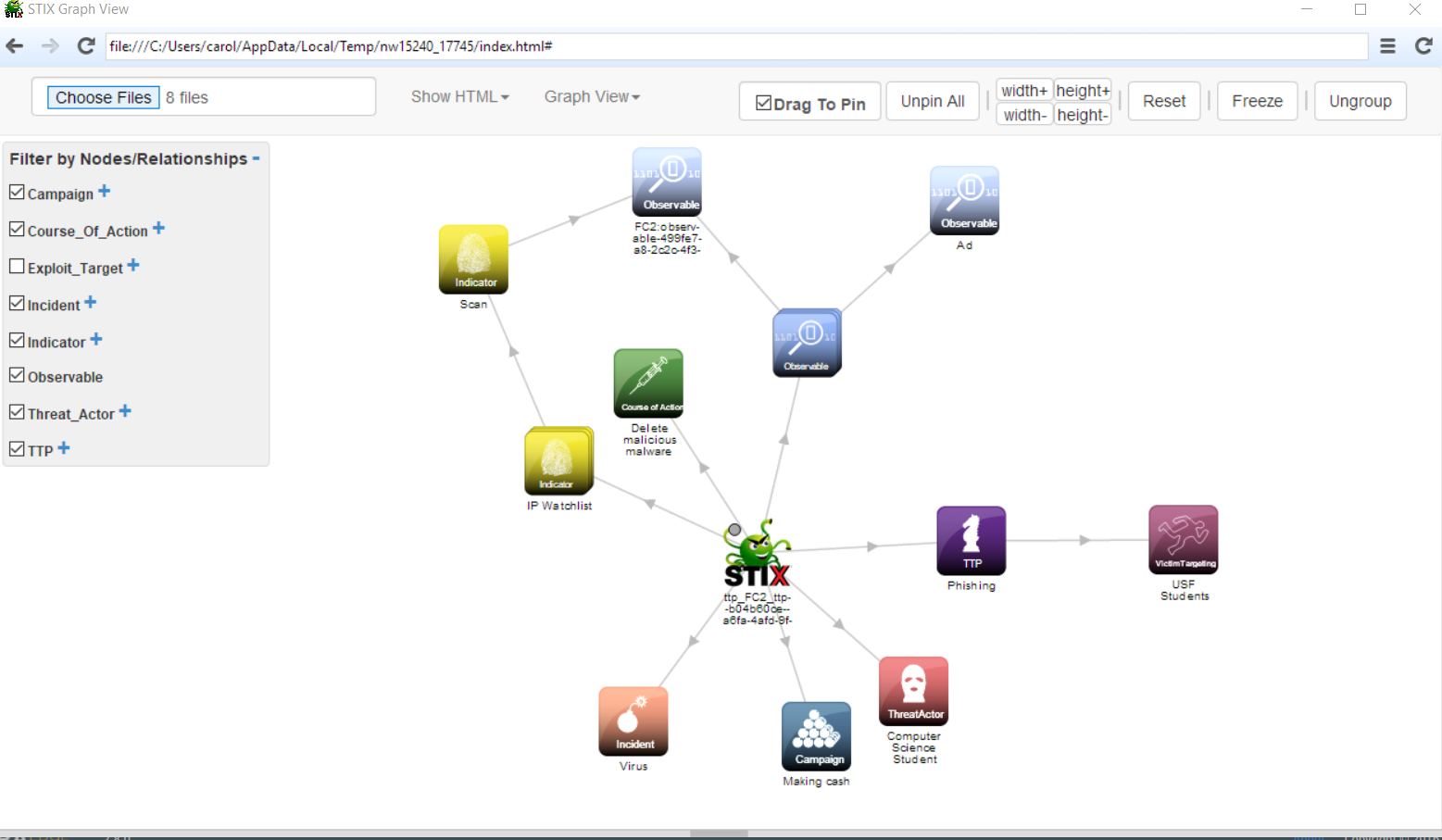
**2.3 Delivery**

The scareware will be sent through email using a phishing attack. Students will receive an email from a fake USF account and the student is hoping at least one person will fall for the pop up ad scam.

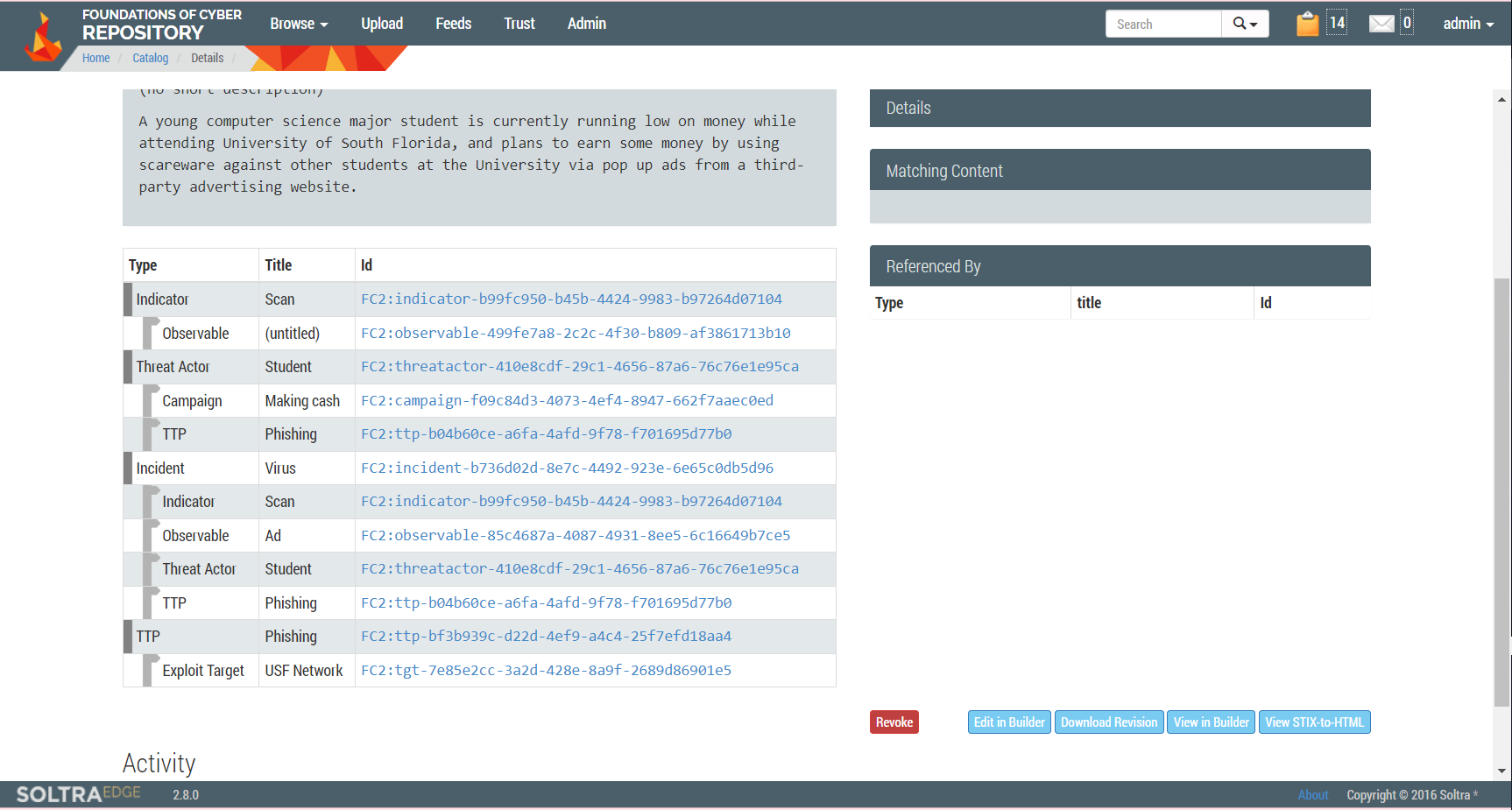
**2.4 Exploit**

Since the scareware is being sent via email, the student just has to sit back and wait for someone to click on the ad and then the fun begins. The person who opens the ad will be prompted to send money to a bitcoin account which is owned by the student.

**2.5 StixViz Representation**

****

**2.6 Soltra Edge Representation**

****

**2.5 Install**

After the user clicks on the ad, the software begins installing onto the computer without the user knowing. The user will begin to notice the computer being slow and may check a process monitor to view what program is taking up so much CPU. Before the user can do that, the “NightMare” image appears on the screen with a pop up window which will reappear every 5 minutes. The pop up window contains information about installing antivirus software for money.

**2.6 Command and Control**

Before the user can uninstall the scareware, the student then installs a backdoor to keep the scareware running as long as possible to get them to pay for the fake antivirus software.

**2.7 Actions on Objectives**

After the backdoor is installed, the student then installs a rootkit onto the backdoor to ensure the user does not know he is there on his computer. After some time keeping control over the user’s computer, the student receives the money and erases all traces he was ever there. The student repeats this with multiple people until he has enough money to be satisfied.

**3. Incident Handling Process**

**3.1 Identification Phase**

After some time of NightMare being run on a person’s computer, it starts to corrupt and lose all files and the computer is deemed unusable after some time. This is only if the user decides to not send money and does nothing to try and restore the computer to a clean state.

**3.2 Eradication & Recovery Phase**

The recovery process of removing scareware is so easy anyone could do it. That is why the student decided to use scareware, only for a profit of money and so most people wouldn’t lose their data or files:

1. Go to the Control Panel or list of programs or apps on your computer.
2. Search for the name of the sketchy software. If you don’t know what the name is, look for any unusual program or app names and run a Google search.
3. Once you’ve identified the program, right-click on its name and select **Remove** or **Uninstall**.

Extreme scareware infections might require you to do the following:

* Reinstall your antivirus software (in case the malware disabled it).
* Cut off your internet connection to minimize leaked information.
* Turn off your computer and consult an IT expert.
* Change your passwords through another, uninfected device.[[3]](#footnote-2)

**3.3 Lessons Learned**

Since the student was looking for quick cash and not planning to induce much harm on a person’s computer, the results could have been worse if he used a more harmful APT.

This attack could easily be stopped by spam filters in the USF emails. If the student had more time and experience, this attack would have worked if he was a professional.

**4. Exploit References**

STIX “Documentation” URL: <https://stixproject.github.io/documentation/>

Soltra Edge

**5. References**

Fortinet. (2023). *What is Scareware? defined and explained*. Fortinet. Retrieved April 23, 2023, from https://www.fortinet.com/resources/cyberglossary/scareware#:~:text=Scareware%20Meaning,spread%20through%20spam%20email%20attacks.

Screamer Wiki. (2023, February 16). *Nightmare*. Screamer Wiki. Retrieved from https://screamer.wiki/NightMare

Buxton, O. (2022, December 19). *What Is Scareware? Detection, Prevention, and Removal*. What is Scareware? detection, prevention, and removal. Retrieved from https://www.avast.com/c-scareware

1. Fortinet. (2023). *What is Scareware? defined and explained*. Fortinet. Retrieved April 23, 2023, from https://www.fortinet.com/resources/cyberglossary/scareware#:~:text=Scareware%20Meaning,spread%20through%20spam%20email%20attacks. [↑](#footnote-ref-0)
2. Screamer Wiki. (2023, February 16). *Nightmare*. Screamer Wiki. Retrieved from https://screamer.wiki/NightMare [↑](#footnote-ref-1)
3. Buxton, O. (2022, December 19). *What Is Scareware? Detection, Prevention, and Removal*. What is Scareware? detection, prevention, and removal. Retrieved from https://www.avast.com/c-scareware [↑](#footnote-ref-2)