**Hidings Report**

**Project Scenario**

Xavier Midnight, having studied for the past 4 years at a university learning Cybersecurity, was ready to put his newfound tech skills to work. At this point in time, the market was hot for this career field, but Xavier did not want to find himself in a 9-5 career working his way to the top. With a bank account that was barely getting him by, Xavier needed quick money. Fortunately for him, he found himself in the height of the crypto era. 2020 was the year newly created crypto millionaires were springing up and he envisioned himself as a Bitcoin Baron and owning the Internet. “Why am I going to purchase this coin myself? I’m just going to take it,” he thought to himself.

In recent news, Xavier observed that Greenan Blusk, had just bought the company myCoin for far more than it is worth and had started disrupting the typical security operations for the organization, obliterating all employee morale, and causing uncertainty within the organization. With the layoff of more than half of all security personnel and the IT team, Xavier noted that this would be the prime time to get into the building and cause even more havoc. With the removal of the “work-from-home” policy, Xavier knew he may be able pass off as a remote employee who was forced to come back into the office. Little did Greenan Blusk know, that this temper tantrum was soon to result in the theft of his cryptocurrency under the cover of Midnight darkness.

Xavier decided that the most effective way to obtain the crypto keys that this organization possessed would be to get directly into the building. All Xavier needed was the call directory to make a few phone calls, do some LinkedIn searches and acquire a fire evacuation plan to get familiar with the building, your basic OSINT. “Man, these things are too easy to get” he thought to himself as he analyzed the evacuation plan. A google street view of the building was also sufficient in giving Xavier a clue on where the entrances and employee parking was located.

In preparation, Xavier purchased a textbook titled “Social Engineering – The Science of Human Hacking" and many others due to his understanding that the human aspect is the weakest link in security. After preparing, Xavier finally mustered up the courage to call the Security Operations Chief, Itel Soks, who was already on his way out and could not care less about the fate of myCoin.

“Itel Soks, this is Bruffer Overlid the new security personnel officer, how are you today?” Xavier says.

“Good afternoon Bruffer, I’m doing well, thank you. How can I help you?” Itel asks. “Glad to hear that sir. I will not take much of your time. My boss is out today, and I unfortunately do not have a copy of the security key to open our floor plan drawer. My job tonight is to build a monitoring path for myself around the building and I am calling up personnel for any relevant information on the office layout. Are you able to help me out?” Xavier confidently asks.

“Sure thing, Bruffer. There’s not much to write home about the office, but oh there is one thing. Please make sure to keep an extra eyelid out for our Administrator suite, will ya. All our admin terminals and monitoring hardware are in that office, and it would be a shame if something were to go missing or a foot. I trust you will keep the company security and livelihood in mind.” Itel says.

“Yes sir you got it, and thank you for the information. I’ll make sure to drink an extra cup of coffee for the patrol. Goodbye now.” Xavier says.

After acquiring this information, Xavier felt confident that he knew how to navigate around the building and get to the crypto keys that he saw as his ticket to the good life. Xavier envisioned himself inside the building, but what would he do once he found himself at the terminal? “I need a script.” he thought. Xavier began preparing his little pet duck for business.

The day arrived when Xavier would finally make his move. Equipped with knowledge of the building layout, confidence, and his rubber ducky in his pocket, he arrives at the building ready to execute. Xavier meticulously parked a few blocks away from the building to avoid cameras picking his car up. With a confident strut, Xavier plunged into the building headfirst and right through the front door. Ready to be questioned on his reasoning for being there, Xavier is surprised there is no receptionist at the front. With quick thinking he begins to calmly look around for the first set of stairs to the second floor. Xavier purposely avoided an elevator to mitigate possible encounters with personnel he might have talked to and because he knew there is always a possibility the elevator could fail. Skipping up the steps and trying to remember the fire evacuation plan layout Xavier comes around a corner and finds himself in an exceptionally long hallway with office suites on either side. He begins to slowly walk down the hallway while also reading each office door plate quickly. “Second floor, seventh door facing north. Found ya!” Xavier thinks to himself. He then opens the SOC door and is surprised when he is met by no one. Computers are beeping and sounds are in the air but not a single soul is in the office. To Xavier’s left is the Administrator sub-suite. Xavier darts for the first terminal he sees and quickly plugs in the rubber ducky that he pulled out of his pocket. Now he must wait the longest 15 seconds of his career, no..., his life.

“No way, I'm actually in!”. Xavier had never felt such an adrenaline rush. He quickly took a screengrab of the crypto codes and placed it on the USB. He got what he came here for and slipped out of the building as undetected as he had come in.

Once at home, Xavier still could not believe he had performed such a heist. He was concerned that the feds would be alerted the moment that he took possession of the crypto. “Worst case scenario...,” he thought, “I need to make sure they don’t find all this evidence. Admit what you can, deny what you will.” Xavier finally made use of the code and found himself as the owner of $10,652,054 in cryptocurrency.

Meanwhile, while Xavier was celebrating, myCoin had detected the large loss of currency from its system, and immediately sent a notification to the authorities. As a newly joined detective, you have been assigned as primary. The audit on the Windows Registry revealed that a USB drive was connected to the company system shortly after Xavier was seen entering the room on the security cameras, and is now the primary suspect in this investigation. Before taking action against Xavier, you draft a warrant detailing the items to be seized which specified interests in laptops, USB drives, hard drives, and their related peripherals. The day arrives when you perform a raid on Xavier’s residence....

“Where’s the money Lebowski?”, you say as you drown Xavier in the toilet.

“It’s down there somewhere, let me take another look”, Xavier says as you dunk him once more into the white throne.

Realizing that Xavier is not going to disclose any information, you decide to book him into the county jail, and resume your examination of the camera footage. “Hmm..”, you think, “he was out of there pretty quickly.” You start having a deeper interest in the USB you stored in the evidence bag. “Who does he think he is, hiding stuff in the cyber realm. Time to get to work.”

**Xavier Midnight Hidings Technique Summary**

1. Delete Evidence (Autopsy)

|  |  |
| --- | --- |
| **sudo\_wrapper.sh** | Just deleted. Should be quickly recoverable. |
| **server.sh** | Just deleted. Should be quickly recoverable. |
| **password\_grabber.ducky** | Just deleted. Should be quickly recoverable. |
| **Ducky\_PSWD\_Grabber\_Instructions.txt** | Just deleted. Should be quickly recoverable. |

2. Change Extension and Misdirection (Hex Workshop & File Explorer)

|  |  |
| --- | --- |
| Social\_engineering\_script.txt -> **Houston Skyline.PNG** | Hidden Attribute selected; PNG extension instead of txt |
| MyCoin Building.PNG **-> myCoin Building.txt** | A txt extension instead of the actual PNG; Investigator will attempt to open it and should observe quickly that it is a PNG. |

3. Steganography (Use S-Tools)

|  |  |
| --- | --- |
| **Green Ape.gif** | Contains steganography that holds the Crypto codes  **Passphrase:** Chunky Monkey  **Base64 Encoding of passphrase:** Q2h1bmt5IE1vbmtleQ==  **File Hidden Within:** Crypto Keys SS.png (File which contains the main evidence, the crypto codes) |

4. Bit Shifted (Use Hex Workshop)

|  |  |
| --- | --- |
| **Orange Ape.png** | Block shifted to the left. Needs to be Block Shifted to the right to correct. |
| **MyCoin Fire Evacuation Plan.png** | Block shifted to the left. Needs to be Block Shifted to the right to correct. |

5. Misdirection

|  |  |
| --- | --- |
| **Crypto Codes.pdf** | Serves as misdirection and is password protected. Is not actually able to be opened. |
| **Blue Ape.png** | Just deleted. Meant to also provide misdirection. |

6. Altered File Header (Hex Workshop)

|  |  |
| --- | --- |
| **Employment\_Letter.pdf** | Extension is left clearly visible, but cannot be opened because the file header’s first 4 bytes has been altered from “25 50 44 46” to “7A 7A 7A 7A”. Investigator will need to correct this file header to view this PDF. The correct file header can be found in Banana Passphrase.txt |

**Question and Answer Summary**

***Q. Is there any type of evidence in the USB drive that shows ownership of the USB, or anything that shows the USB has been in use by Xavier Midnight?***

A. Xavier’s Aperture Laboratories offer letter as a Cybersecurity Analyst shows ownership of the USB.

In the document, Xavier’s name is clearly present and that this offer letter was meant for him. It may have kicked off his desire for wanting “quick money” rather than working this full-time position.

***Q. What method was used by Xavier to extract passwords and locate the crypto codes ?***

A. Xavier used a script on a rubber ducky USB to extract the codes.

Deleted within the USB are scripts that were used to target the terminals. These are sudo\_wrapper.sh, server.sh, password\_grabber.ducky, and Ducky\_PSWD\_Grabber\_Instructions.txt.

***Q. Is there any evidence showing that Xavier took a pre-meditated course of action towards the company myCoin?***

A. Disguised as a PNG image is some practice social engineering scripts that helped Xavier in getting information about navigating through the building and identifying the location of the codes. There is also a picture of the outside of the building showing the exits, and the room in which the crypto codes are stored.

The existence of these scripts proves the intent that Xavier meant to talk his way into receiving access.

**Q. *What did the base64 encoding located in the USB translate to? What did this allow you to access?***

A. The Base64 encoding located in the text file translates to ‘Chunky Monkey’.

This is the passphrase that needs to be used on the green ape, which has a screengrab hidden within it.