From: "[redacted]>
To: "[redacted]>
Subject: Re: timeline
Date: Tue, 14 Feb 2023 02:27:31 +0000
Importance: Normal

Copy. Thanks.

[redacted]
FBI NY Violent Crime Threat
Cell: [redacted]

From: [redacted]>
Sent: Monday, February 13, 2023 9:27:06 PM
To: [redacted]>
Subject: Re: timeline

Desktop

[redacted]
FBI NY Child Exploitation & Human Trafficking Task Force
[redacted]
C [redacted]
D [redacted]

From: [redacted]>
Sent: Monday, February 13, 2023 9:18:30 PM
To: [redacted]>
Subject: Re: timeline

Thanks.

Is a Talino computer a laptop or desktop?

[redacted]
FBI NY Violent Crime Threat
Cell: [redacted]

From: [redacted]>
Sent: Monday, February 13, 2023 9:17:40 PM
To: [redacted]>
Subject: Fwd: timeline

[redacted]
FBI NY Child Exploitation & Human Trafficking Task Force
[redacted]
C [redacted]
D [redacted]

From: [redacted]>
Sent: Monday, February 13, 2023 9:13:47 PM
To: [redacted]>
Subject: timeline

[redacted], below is a timeline of what transpired today, noting that we had no idea this was a potential hack until late this afternoon. Given the potential that someone accessed our lab to do this, and that the issue may have been with the way we setup our network, below is also a little insight to the many attempts we've made to get the FBI to assist in both physical security to the lab and to help with networking:

Today's events (approx times)
-7:30am - I arrived at the office and noticed my Talino computer had restarted.
-7:40am - I logged in to my Talino and a txt file popped up that said in part my network has been compromised and provided an email address to contact. This file was in the "startup" folder so when logging in it opened automatically. I ran my computers anti-virus software, which was up to date and active, and it identified one potential threat which I attempted to remove. While this is not common, it is also not unusual given the data we recover from 305 subject devices.
-I attempted to remove the potential threat, but my administrative privliges had been removed, and despite many attempts to gain access, I could not
-8:30am - I reached out to [redacted] at CART for help, but he was going to be tied up for a couple of hours
-9:00am, I reached out to Talino for help and they walked me through some steps, but nothing worked. They then advised me of a process to take to run antivirus software against my Talinos Operating System hard drive, which took some time but identified the likely source of the threat, which was attributed to a forensic program we use called Axiom. The threat was determined to possibly be a "booby-trap" left by a subject (who is a hacker) that was tripped when the Axiom forensic program ran across it. After this discussion it was believed that was the reason for the issues and we then began working on a solution, which seemed likely to fix my issue.
-Around this time I also noticed our main server was down, but I didn't think too much of it since we just added a new switch and tried to configure some ports to run at different settings to increase our bandwidth. I assumed at the time the lack of access was a result of incorrectly applying the settings to the "LAG" and "BOND" configurations of the switch. I was able to see that according to the switch, the server seemed to be connected just fine, so I spent some time troubleshooting it.
-Around 11:00am or so I was finally on instant message chat with the makers of the server, Synology, who had us conduct some tests and they ultimately concluded that a possible issue was a defective hard drive in the server. This was a problem sine the server is "raided" and finding the defective hard drive was a time-consuming and difficult task, but several of us began our attempts.
-3:00pm - Is when [redacted] and [redacted] from CART came over to help. After a bunch of triage and testing we could not figure out why we could not connect to the server, since by all accounts it was working.
-We then noticed that our other servers (NAS1 and NAS2) were also not working properly, although we were able to access their control windows, unlike with the Synology server. After some digging around we noticed the folders that contain our data was missing. Initially we thought this was due to a firmware issue since Christian and I had dealt with that in the past and resembled the same issue.
-Around 3:30pm or so we located the log files and began combing though, which is when we noticed strange IP activity that took place yesterday from two IP addresses. The activity included combing through certain files pertaining to the Epstein investigation. I reached out to one of the case agents to see if they were in the office yesterday, thinking that maybe they inadvertently changed a setting on the NAS or if they noticed anything strange about them.
-Around 4/4:30pm we dove into the IPs and checked all of our computers to see which had the IPs in question. One computer, our discovery computer, matched one of them and is located in a room next to the lab. The

other IP is one we don't recognize, but is the same address as the IPs on our network, leading us to believe it was a computer that accessed our network somehow. We were not able to identify the computer, but it had to have accessed our network either by being plugged into the network, or possibly by telnetting in virtually.
-5:00pm - we realized we were hacked and discussed what we needed to do to ensure its contained.
-5:15pm, we immediately saved our logs and shut everything down. We disconnected the Internet and ensured anything containing a log file was preserved.
-5:30pm - I began calling my SSA, [redacted] in Security, [redacted] at CART, [redacted] in Cyber.

Physical Security
-Dec, 2021 - Moved into the 10th floor lab
-Dec, 2021 - made numerous requests for an electronic keypad lock on the door only to be told by the locksmith there is no funding for a lock. These requests have been made numerous times from Dec, 2021 until a couple months ago, when the response was to make numerous copies of the key we have to the lab

Networking/Network Security
-Since approx 2017 we have elicited help from CART and Cyber in networking our lab, all to no avail. Some CART and Cyber folks have come over on their good graces, but they were not network savvy and just tired to do what they could. Some months ago (I can look up the exact date) we again requested help from CART, but were told their networking person was too busy to help. This mean no one with any networking experience or ability was willing to help, so we had to figure it out on own own.

[redacted]
FBI - New York Office
Child Exploitation and Human Trafficking Task Force
[redacted]