Months to Milliseconds: A Dedicated Team Defending Cyber

On Screen Text: [Months to Milliseconds, a Dedicated Team Defending Cyber]

[Arial view of Washington D.C. in the daylight]

On Screen Text: [Wed/3 Jun//6:04 pm. Program Management Office Government Administration Building.]

[Benjamin is at his desk working and speaking on the phone, jotting down notes in a folder. Clock shows 6:04pm.]

Benjamin: Uh, actually I'm finishing up right now. Yeah, I know, I know. Okay... see you then. See you then.

[Benjamin's computer shows an email alert from HR. E-mail fills the screen, partially covering up an application that was running. Benjamin sighs impatiently as it opens. Benjamin clicks the attachment labeled agenda. His mouse pointer shows a loading icon—nothing else appears to happen. He clicks his mouse repeatedly.]

Benjamin: Oh, you've got to be kidding me. I thought I was gonna be out of here on time for once this week. I'll deal with this tomorrow.

And... I am gone.

[Benjamin turns of his computer, grabs his coat, and leaves.]

[Hackers, vaguely silhouetted in a dark room, type at their computers.]

[Benjamin's office, now empty for the night, the clock reads 2:06 AM. The power light on Benjamin's computer flickers to life and ominous code crawls across his monitor.]

[The hackers continue working.]

[Benjamin knocks on the door of Andy Greenwood, System Administrator. Andy turns from his computer to look at Benjamin.]

Benjamin: Yo bud! You, oh sage, of all things IT, can you help me? My computer is running painfully slow. I put in a ticket, but I need it done right now... 9 a.m. presentation I cannot be late for.

Andy Greenwood: You? You're lucky I like you. Let me see what I can do for you.

Benjamin: Thanks.

[Andy works for a moment at his computer while Benjamin looks on.]

Andy: What are you doing sending me emails at 2 a.m.?

Benjamin: What? I wasn't sending you any emails. I was in bed dreaming of vacation at 2 a.m.

Andy: Let me remote into your box. Looks like we have some unusual processes going on right now. And... unless you can be in two places at once it looks like you're logging in all over the place. As we speak. With admin privileges?

Benjamin: Uh...

[Andy gives Benjamin a quick and grim look before turning to his phone.]

[The hackers continue their attack.]

On Screen Text: [Thu/4 Jun//9:41 AM. DHS Employee Orientation, DHS Headquarters.]

[John stands on a stage before a group of well-dressed professionals. NCCIC briefing slides are on display.]

John: Good morning I'm John O' Neil, a member of the Department of Homeland Security's National Cybersecurity and Communications Integration Center, probably better known as DHS NCCIC. We are an operations center that runs around the clock twenty-four-by-seven. Our mission is to reduce the likelihood and severity of any incident that may significantly compromise the security of our nation's critical IT and communications networks. Today, I'm going to be talking to you about three key capabilities: Einstein Reputation Scoring System and Continuous Diagnostics and Mitigation. Now, before I get into the meaty st--

[John's Deputy appears off of the stage and to the right. She briefly confers with two figures watching from the side, before briskly walking to John and handing him a note.]

[Note reads: NCCIC Director called. She needs you back at the NCCIC immediately.]

John: Excuse me. Excuse me, I have to run, my Deputy will be taking over.

[Distracted, John leaves the stage.]

[John drives urgently back to NCCIC. As he does so the hackers continue to attack.]

On Screen Text: [Thu/4 Jun//10:56 AM. National Cybersecurity and Communications Integration Center.]

[John moves through dark hallways towards the NCCIC Director's office. He stops at her door and knocks. Glancing up, Director Phyllis puts her phone down and gestures for John to come in.]

Director Phyllis: Sorry to pull you out of you briefing, but this has the potential to be high impact. I just had another agency report an incident and request assistance. It's looking like the same campaign as the one from yesterday and I don't think it's a coincidence. It's probably happening at multiple agencies.

Time is not on our side John. I need you to get a response team in place, and use all of our capabilities to stop this attack.

John: I'm on it.

Director Phyllis: Fix this thing, okay?

On Screen Text: [Thu/ 4 Jun//11:31 AM. National Cybersecurity and Communications Integration Center.]

[John stands at the head of a table with his newly assembled team before him and two other Directors, Jeff and Randi on VTC, behind him. The team John, Robinson, Jamey, Pete, Alex and Monica sit around a table awaiting the briefing.]

John: Team, this is Jeff Williams and Randi Jennings, Chief Information Security Officers of the two agencies that were hit. My incident response team is en route to your site to assist in the examination.

Here's what we know so far: One of Jeff's Sys Admins escalated a concern through a security operation control center this morning when he discovered an unauthorized process running on a desktop computer in the middle of the night. The Ops center's investigation points to a spear-phishing attack but there's no indication of any disruption to their network.

[John approaches a whiteboard and gestures to a diagram depicting the attack's path and NCCIC's efforts to thwart it.]

John: Whoever this is they apparently know what they're doing. They had enough info to craft a tailored email to their targets and now it looks like they're mapping the network.

Robinson: They?

John: At this point we don't know who they are or what their goal is, but whether it is to steal, manipulate, or destroy, our job is to find out as much as we can and stop them.

Pete: I've already pulled in our liaison from Secret Service Homeland Security Investigations and interagency partners.

John: Absolutely, we need to attack this from all sides.

Pete: I'm on it.

[Pete grabs his notes and leaves to meet with NCCIC liaisons.]

John: Between what's happening now at your agency Jeff, and what you both discovered yesterday there are too many parallels for these attacks to not come from the same point of origin.

Monica: What about Einstein? Doesn't it screen this kind of traffic?

[John returns to the whiteboard and points to a depiction of Einstein.]

John: Einstein is doing its job. We verified. It continues to stop hundreds of events every day. This one got through because it didn't present any known signatures. The privacy offices of both agencies have agreed to share their logs through the privacy protections we have in place.

John: All right, we all know what to do now let's do it.

On Screen Text: [Sat/ 6 Jun//6:21 PM. National Cybersecurity and Communications Integration Center.]

[On the NCCIC Watch floor, dozens of analysts are focused on the task at hand--stopping the attack. John, Robinson, Jamey, and Monica are among them.]

Robinson: Somebody put a lot of effort into this.

[Jamey points to his screen.]

Jamey: Look here the phishing attempts are very targeted, but not limited.

John: We're talking about more than a couple of employees here. Look at this: here's the traffic from Einstein. At least a dozen people took the bait from both agencies.

Robinson: Look here though, Einstein has been blocking attacks using similar attacking patterns.

John: And then they busted through. Something had to change. They've clearly altered their attack pattern.

Jamey: It looks like when one of the targets clicked on the spear-phishing attachment, it installed malware in a hidden directory. Traffic in the infected box is shown calling out to the same location. I cross-referenced them with the attacks over the last eighteen months there are similarities all over the place.

[Monica stands up and leans over her computer towards John, Jamey, and Robinson.]

Monica: The actor's been moving laterally through the network but no data has been stolen or manipulated ...yet. They seem to be trying to gain access to more sensitive networks before they strike. If they get there, game over.

[Unhindered, the hackers continue their attack on NCCIC and the U.S.]

John: There is no doubt in my mind these are nation state actors, highly sophisticated, highly motivated, and persistent.

Jamey: How could something like this get through?

John: It's a Zero Day.

Jamey: What?

John: They burned a Zero Day. They did their research, exploited vulnerability, spent a lot of dough, and launched an extremely targeted spear-phishing campaign to infiltrate the network.

Jamey: Well, which application had a Zero Day?

John: Yeah, exactly.

On Screen Text: [Sat/ 6 Jun// 9:44 PM. National Cybersecurity and Communications Integration Center.]

[Back in the conference room the team is working late into the night as they look for the Zero Day. They continue for hours without success. Then John slowly raises his head in sudden comprehension.]

Jamey: Well, which application had a Zero Day, Zero Day, Zero Day…

John: Yeah, exactly.

John: Monica, do you have the software logs for the agencies?

[John quickly flips though the logs and smiles.]

John: I'll be right back.

[He then turns and rushes from the room.]

[Elsewhere, Randi Jennings is speaking over the phone in her office.]

Randi: Yeah, John, I can confirm that. We just installed that software a few weeks back.

John: Thanks, Randi. We'll be in touch.

[John, hangs up his phone and quietly chuckles to himself.]

On Screen Text: [Mon/ 8 Jun// 7:26 PM. National Cybersecurity and Communications Integration Center.]

[In the fading light of dusk, NCCIC appears asleep, but inside the team has once more assembled in the conference room.]

John: So we reached out to the software company, and they're on it. They've got a team to create a patch to eliminate the vulnerability and a process for rolling out patches very quickly.

[John points to the whiteboard diagram.]

Here's how we worked it: We tasked Einstein to block any traffic that resembles the signatures that we created. We are also going to add the IP address of the source of the phishing attack to dynamically adjust the threat's grade if you will. Using the reputation scoring system this will protect against any other IP addresses that are associated with this attack. Even as this evolves, we'll no longer have to rely on signatures. Any similar spear-phishing attacks on our networks will be stopped.

[John looks to Robinson.]

Robinson, make sure this information is shared using our information sharing system so that our government and private sector partners are protected.

Robinson: Roger. Already working on that John.

[Robinson continues to enter data to his laptop and John goes back to the whiteboard.]

John: To heal the ecosystem the departments and the agencies can monitor the implementation and status of the patch using continuous diagnostics and mitigation. We're lucky that the CDM program provides implementation monitoring and tools for the agencies.

[The team slowly walks though the halls after a long struggle.]

Robinson: I 'll bet whoever launched that attack is fuming.

John: Well, It's ok to do the happy dance, for a minute, but don't celebrate for too long.

[The hackers are agitated. One hacker slams his fist onto his computer.]

John: They're going to notice real quickly that their access is dwindling away so they'll identify other options… find other ways.

Jamey: You know a year ago this attack could have been catastrophic… a year from now these kind of threats might be altogether ineffective.

Monica: The harder we make it, the higher we raise the cost to the adversary. That's where they'll feel the most pain and it just might make our networks too expensive to tackle. Who knows… maybe we even put 'em out of business.

[A hacker turns in rage to shove another.]

John: That is the goal right now, I'd be happy to identify the threat in milliseconds. It would put us ahead of the adversary… That'll be a good day.

Robinson: What's next?

John: Let's get out of here. We've earned our keep for the day but we're not done. And believe me they're not either. I want to see you all in the morning. Early OK?

All: Goodnight John!

[The picture fades to black. Then slowly, scenes of the hackers return. Once again they are at work.]

On Screen Text: [This video is a representation of DHS National Cybersecurity and Communications Integration Center (NCCIC) capabilities. It should be noted that the events and characters portrayed in this video are fictional.]