SEI Cyber Talk (Episode 4)

Defending Your Computer Network from DNS Hijacking
by Eliezer Kanal and Daniel Ruef

Eliezer Kanal: Hello. This is Eli Kanal. I'm here today with Dan Ruef, and we're going to talk today a little bit about some of the recent interesting warnings that have come out <music fades> of the Department of Homeland Security.

So DHS recently released an interesting warning, which I think many people might not know what it means. They were giving a warning to website owners, particularly government website owners, about this thing called DNS hijacking and different ways to protect yourself against it. Could you help us understand a little bit, what is DNS hijacking?

Daniel Ruef: Yeah. DNS is like the phone book for websites. So when you go to a browser you don't go directly to the website, you send what's called a DNS request that says, "Where does ESPN.com live?" for example, and it tells you, and then your computer sends information there. So if someone can change the phone book, the information won't go directly to the website, it might go to a malicious actor first, who could forward your call to the website after that and you might not know any different.

Eliezer Kanal: So let's say I'm the owner of some store. I have an online store, right, and I want people to come to my store and buy my stuff. When they type in, you know, Eliesstore.com, I have a server somewhere and their request goes to my server. What you're saying is instead of going directly to my server it'll go somewhere else first. So what kind of bad things could happen if my traffic gets redirected like that?

Daniel Ruef: Someone could see all of the--see all the things that the user wanted to read about your website. They could find out what they're interested in. If you're selling things, they could see their buying preferences. Depending on how any payment information is transmitted, it might get sent to an adversary first, who could still forward it to your website so the user wouldn't know any better, but they might have just grabbed some credit card information or some login information, because it goes to the malicious actor first, potentially malicious actor first, and then to your website, because the actor changed where the world thinks your server lives, and they told them to point to them instead by changing the phone book entry.

Eliezer Kanal: So do you know, how would you go about? I mean, how does someone go about registering the phone book at the first time? You know, we have this DNS thing. How do I update my phone book entry?

Daniel Ruef: You can register with the domain registrar's service. It's an international body that governs the internet and things of that nature, and so you create an account and you keep your password and you keep it updated, and then they know it's you registering a site, and they say Eliesshop.com should be--all traffic should be sent to your server. But if someone gets a hold of your account, they can say, "Hey, I changed my IP address. I have a new server. Use this one instead," and the domain says, "Well, that was a legit login, so we will accept your changes."

Eliezer Kanal: Cool, and I know last time we were talking we actually had a whole conversation with another gentleman here, Matt Butkovic, about how to keep proper hygiene, proper data hygiene, proper security, and I guess this all falls in that also, if you have logins on the internet and if you have just general information that's relevant to this sort of stuff. Keep that stuff secure. Don't click phishing emails, and I guess that's part of--if you're going to keep this stuff secure, you really need to protect all your information related to these, this phone book entry.

Daniel Ruef: Yeah, and especially things that you do once. Because realistically, if you're a small company, you bought one server and it's not going to change much, and you might register your domain one time without any updates, and you might let that password get old. You might not have done it well in the first place because you knew you were only doing it once. It's not something you login to every day, and so yes. Keeping it up-to-date and secure, maintaining all of these types of accounts, is very important.

Eliezer Kanal: Cool. All right. So let's take a step back for a second because I know, you know, we're talking about this DNS thing, but, you know, the work that you do on a regular day is looking at internet traffic. I don't think people really appreciate what this is. So can you describe a little bit just when you're visiting websites and then you're saying here I can look at that traffic, what is that traffic?

Daniel Ruef: Well, to go back to the initial example with the phone book is you type something into your browser, a particular website you want to go to, and you hit Enter so it kicks off. It first sends what we call packets to that domain registrar service and those packets contain the address you want to go to and the registrar service replies with the IP address that you are to send the remaining requests to.

So in our example, you send a message that says, "Hey, where is Eliesshop.com?" and it replies with the IP address of your server, and then all of the webpage-related requests go to your server. It might say, "Hey, what is your webpage?" or, "Let me see info on this particular product," and then your server sends all, a whole bunch of information back, and it gets displayed in your browser, and so those are in the form of packets containing a number of bytes of information.

Eliezer Kanal: And to be fair, I mean, we're talking about web, but if you're on your local network at home or if you're in your office and you say, "I want to print a document," that kind of falls into traffic as well, doesn't it?

Daniel Ruef: Yeah. Anything that goes over, well, over a network and is communication between a number of different computers is--are formatted in terms of packets, and so that would be called network traffic. Typically referring to IP traffic, so there are computers with internet

protocol addresses of the form of maybe 1.2.3.4. You might've heard the dot notation before, and so communication between IP addresses would be called network traffic.

Eliezer Kanal: Cool. You mentioned that, you know, the guys who are doing this DNS hijacking, that sort of thing DHS saw that some people are doing this hijacking. So how would you be able to detect that some hijacking is going on? What would you be able to see that would allow that?

Daniel Ruef: Well, if you were collecting the network traffic from your own network, and you sent a request, your own request to find your, say, your website, and then you looked at the response that you got and if the IP that was in there isn't your IP address, then you can tell that someone has hijacked your DNS.

Eliezer Kanal: So to go little bit back with that, so if I, when I send a request to another server and that sends its packet along this network, it's actually possible to capture that packet and someone can, like, hold it and look at it, so to speak?

Daniel Ruef: Yes. There are a number of we would call network sensing programs or network collection programs. We've created a few here at CERT, and you can get--it essentially makes a copy. It can make a copy of all the packets, everything it sees, and can categorize it, describe it, come up with maybe summary statistics, and can look at all of the contents. So if you know what you want to look for, what you are interested in, you might be able to focus on a particular type of traffic and either detect differences or anomalies or things like that.

Eliezer Kanal: So you were talking about capturing or making a copy of some of these packets. Is it feasible to make a copy of all the traffic going in and out of a business, for example?

Daniel Ruef: Maybe a very small business. Maybe Elie's Shop, that has one small web server and maybe an email address. That's probably doable. But if you--if that website is CNN.com, with millions of people hitting it all day and a number of redirects and adds that have to load, you can't store every bit and byte that makes it in and out to that--into that network. So you would like, you would prefer, initially, to summarize it, and part of the reason you can't store it all is you--storage can be expensive at certain scales, but also you have to process it, and there's no point in collecting a bunch of data if you cannot query it later. So you can write down everything that ever happens, but if someone says, "Hey, what did you write down?" and it takes three days for a response, it's kind of useless.

Eliezer Kanal: And you--actually, when you said "adds," you made me think. I mean, so this isn't only, you know, if I go to the site and I say, "Give me back your homepage," then I get back the homepage. But if I'm, let's say, watching a video or if there's some movie running, I'm doing a lot of traffic. Isn't--I mean, there's a lot of requests going back and forth.

Daniel Ruef: Yeah, and especially as you mention a movie, I mean, it seems very simple to go to, say, a YouTube video and watch it for an hour. You did very little from a user perspective in your browser that says, "Go to this video. Hit Start." But everything that you see came from the server, so that is all network traffic. That would all have to be collected if you were trying to collect everything, and those videos can be very dense, and there's lots of information that you also might not want to store. Storing the contents of each packet of a YouTube video might not tell you anything, but storing that you went to YouTube for an hour and exchanged this much traffic with the server, or more, note, in this case, received this much traffic, that could tell you something interesting, and so we would wrap that up in what we call a flow.

Eliezer Kanal: Okay. I was going to get to that. So instead of then capturing every packet, we have this flow, I guess. So what is--how do you use a flow?

Daniel Ruef: You would use a flow to get more higher-level information. So those are, for everyone listening, they're, you all, are hearing the words that Eli and I are saying. That is the details or the packet contents, if we were exchanging packets. But someone could describe this as Eli and Dan talked for some amount of time, maybe 15 minutes, said some number of words to each other. We started at a particular time and we ended at a particular time, and we spoke in English. That is a description of what we said. But we don't have to hear all of the words.

So you can do that with network traffic. Elie's computer went to YouTube for an hour at noon, exchanged a megabyte of traffic, and that's it. So you can track where you went or the IP addresses you communicated with without having to store everything that ever crossed the network.

Eliezer Kanal: And going back to our DNS hijacking, I could still see though that it came from here and went to there and I could see if the here and there, so to speak, are what I expect it to be, and I would be able to detect different kinds of attacks.

Daniel Ruef: Yes. If you have a sense of what IP addresses are linked to certain websites, so certain ones you think are very important and you want to keep track of what the domain registrar has for each website, if you start seeing traffic that you expect to go to, say, Eliesshop.com but it's going to a different IP, well, that would come out in the flow, because the IP is tracked there. So just like if I--if everyone has a pretty good sense of what you look like, if someone walks in that doesn't look like you and says, "Hi, I'm Eli Kanal. We're supposed to meet this morning to talk," I would say, "You're not Eli," because I know what you look like.

Eliezer Kanal: Right.

Daniel Ruef: But if I hadn't met you before because I hadn't been tracking, from a computer standpoint, tracking what IPs are connected to what domains, from a person standpoint, I didn't know what you look like, I could believe anything.

Eliezer Kanal: So we were talking last time about personal hygiene and how to keep yourself safe on the internet. It sounds like if you're running a business, there's an entire separate set of hygiene for keeping your network secure. You know, I need--whereas I need to just know what my passwords are and make sure I'm not logging into phishing sites, not plugging in random USBs into my computer, you know, in this context who do I usually talk to, what does it look like, who are my usual users? I mean, is that kind of what I'm hearing?

Daniel Ruef: Yeah, those are things you can do. There's a wide variety of things you can do, and that can usually be a scary amount of things or something that can create anxiety, because there's so many things you could watch, there's so many things you could look for, there's so many things you can hear about.

So what's important is figuring out what's actually interesting or what's important to you. So if it's very important for you to know that your website is all--is coming to your IP address, then you can have maybe a host on your network send periodic requests to your web address and monitor the response, where if you're collecting the traffic and you're looking for that particular thing, you can make sure that those responses always have your IP address. You can't solve all the problems at once, but you can solve individual problems if you know what you would <outro music begins> want to solve.

Eliezer Kanal: Cool. Thank you. Thank you very much, Dan. If any of you have any more questions about this, how to keep your network secure, feel free to get in touch with us at info@sei.cmu.edu or visit our website.

Related Resources

DNS Infrastructure Hijacking Campaign

FloCon 2020: Using Data to Defend

SEI Cyber Talk: What is Cyber Hygiene?

Network Traffic Analysis with SiLK