Heather:

Welcome to the Hurricane Labs Podcast. I'm Heather. Today we're going to be talking about Distributed Denial of Service attacks, or D-D-O-S. Here to help with this talk. I have Roxy our vulnerability management and compliance specialist. And Joe, one of our, SOC analysts. Joe, Roxy thanks for joining me today. First things first, what exactly is a DDoS attack?

Joe:

DDoS is a distributed denial of service attack. What it means it's preventing communication to your web server or external facing servers by bogging down the bandwidth to the point they can no longer communicate. And thus crash or remove themselves and you're no longer traffic is going, in essence.

Roxy:

Right? The goal of these DDoS attacks is mostly to make your website or your service unavailable. If it's unavailable, then the company that they're targeting, or the person they're targeting is losing income. And banks especially get hit hard with this. Sometimes they will get ransom notes that say things like, "Hey, if you don't send us X amount of Bitcoin, we're going to launch a DDoS attack on your website." It can be a source of revenue loss. It's very important to prepare for.

Heather:

All right. What about identifying that you are in fact having a DDoS attack situation? Well, what sort of things can you do if you think that's what's happening?

Joe:

Generally, if you have a network traffic monitoring. A spike of traffic out of nowhere, specifically in, I mean, including like at like 1:00 AM or 2:00 AM sometimes odd hours, you'll find these spikes. Or if the spikes will happen every five to 10 minutes or so. Or from a specific IP range or a single address. That should let you know there's something strange going on. Generally, if a huge spike of traffic happens and it's not expected, there's a good chance you're under a DDoS.

Roxy:

Also, it's important to try to identify these attacks before they hit you. Because once they hit the website, that's when the revenue loss can start. A lot of times what I would do when I was in the SOC, I would subscribe to mailing lists that people would share, how to identify certain attacks or what the trends are. One of the most popular mailing lists is called ISAC. Which is Information Sharing and Analysis Center. Every industry will have a different mailing list. When I was working for banks. I would join the FS-ISAC, which was a financial sector. Also you have your cloud provider or your MSP that should be able to set up alerts and identify these attacks for you. If you're not able to.

Joe:

Sometimes, the ISP will do their own mitigation. Or they'll be, oh, this is too much and they'll start doing their own little mitigation. Whether, I don't know if they'll contact you, they should, but that's possibility they'll do their own mitigation to prevent the traffic.

Roxy:

Right. That's true. Also, there's different types of DDoS attacks.

Joe:

Yep.

Roxy:

Becoming familiar with the different types and then setting up alerts to identify those. That way you're not taken by surprise, because it could be something like DNS requests. Or it could be something very specific that specific protocol that they are using to flood your servers. Make sure you have a variety of different types of alerts to cover different types of DDoS attacks.

Joe:

Yeah. There's the HTTP Flood, which attacks on the OSI application layer seven. That can be mitigated with a WAF, a web application firewall. Actually that's the flavor of the month. That's that attack level seems to be going up with because back in the day it used to be a SYN Flood. They would just send spoof SYN packets. And your server would keep on sending SYN-ACK's and they would never get responded because the IP were spoofed and then that would overwhelm it. But lately the HTTP requesting to be the method of choice now for hackers and such.

Roxy:

Right. Also I forgot to mention the typical attack that we're used to. The typical denial of service attack would come from one IP address. What we used to do is just as soon as that one IP was attacking and sending a lot of requests, we would block that IP. When it comes to distributed attacks though, you're getting them from a variety of IP addresses. You have to find what is the common denominator? What are they all doing? Then what you're doing instead of blocking those IPs, which I'm sure eventually you will. But instead of focusing on blocking IPs, you're focusing on blocking a particular type of traffic, for example. Blocking it in a way that does not disrupt business. You have to find out how to do that from different IP addresses, and not affect business.

Heather:

Well, what things can you do or what resources or tools can you lean on to prevent or mitigate this attack?

Joe:

Like I mentioned before, a web application firewall is pretty good with helping with an HTTP Flood. It filters those out and allows traffic to continue. One of the best things is defense in depth. Have multiple layers of different types of defenses, firewalls, WAF firewalls. Actually, this is one of the few things where you can throw money at. The more bandwidth you have, the harder it is to process, I mean, to be stopped by DDoS in essence. If you have more processing, more bandwidth than they have botnets to throw at you, then the DDoS can be mitigated and it just keeps on and they just usually give up at that point.

Roxy:

What you can do is make sure that your alerts are set to the appropriate thresholds. So that you can identify a DDoS attack early enough, but also you can tune it so that it's not too low. So, it doesn't interrupt business or prevents average users from visiting the website. Also, you can figure out which pages are being attacked the most and focus your resources on those pages more than others. For

example, if your sign in page is the one that's getting attacked the most. That might be more important than the contact page. Doing some analysis and there's tools that you can use. There's Splunk dashboards, and you can do some analysis to figure out where you're not only what types of attacks you're receiving, but what the targets are for the attacks. There's also services like GreyNoise. And GreyNoise will, what it says on their website, is we collect, analyze, and label data on IPs that saturates security tools with noise. GreyNoise and other similar services can help you preemptively block malicious IPs.

Joe:

Preempting those IP's is pretty good to make sure that you don't get overwhelmed. You can also, if you have a any cast network set up. You can take the traffic and just scatter it all across your network. In essence, it just gets absorbed and the DDoS is pretty much nullified at that point. You can do that as well.

Roxy:

Right. You also have load balancers that can switch back and forth as well.

Joe:

Yeah. I mean the hardest DDoS is to mitigate are the ones that do a multi-prong attack. Like one that does a HTTP and a SYN Flood at the same time. Then you got to figure out, okay, which one's legitimate? Which one is fake? Then you got to say, okay, how much of our mitigation defenses can handle this? Can we process it? Can we just, diffuse it over the network? Can we shut it down? Do we need to call in the heavy hitters? What are the alerts? Stuff like that.The multi-pronged DDoS are the ones that are very dangerous.

Heather:

What are some of those other mitigation tactics that you can use?

Joe:

Well, if you want to, you can create a black hole and just drop all the traffic in there and call it a day. The only problem with that is that you'll probably drop some legitimate traffic in there too. And in the end, it does make the network inaccessible. So, it's a way to mitigate it, but it doesn't mitigate it at the same time. But pretty much a WAF as I mentioned, a web application firewall is your best bet for any of those layer seven DDoS attacks. It can do reverse proxy and protect the server from the traffic and just mitigate it and lay and get rid of it in essence, to make sure it doesn't stop. I mean, make sure it stops. You use custom rules to help mitigate it on the WAF.

Roxy:

There are some times that some attacks will come through that just cannot be identified, or maybe they're a new type of attack. Maybe they're coming from a different source or something that, somewhere that you don't expect. What you'll have to do is find out what is, what you want your analyst to do is inspect the raw data and find out what is the common factor in all of these attacks. So that you can use that to block and block that type of traffic. For example, I was working at a bank. A very big bank that had a lot of resources. And we received a distributed DDoS attack, that we just could not figure out how to block. None of our tools were blocking it. Nothing was working. And it was on the sign in page.

We also didn't want to block potential users from being able to sign into our page because we couldn't find out how to block this traffic without blocking users as well. We found that when we inspected the raw data. There was a string of numbers in there. That string was a unix timestamp. And a unix timestamp is the number of seconds that have happened since, I forget what exactly the date is, I think it's January 1st, 1970, but I [crosstalk 00:10:35] can't remember.

Joe:

Frist day Unix was launched.

Roxy:

Yeah, it was the first day that unix was launched. It's the number of seconds that have elapsed since that time. All of those had a similar format. Those numbers were all formatted similarly. We simply blocked all traffic that had a unix timestamp using regular expressions to match that in the data. Sometimes, you just have to figure out what is the common data that is connecting all of these bad requests together. You can also block it based on the type of protocol that is being flooded. Like we were talking about earlier. You can do that as well. There's some protocol that we don't use anymore or it's deprecated, or it simply might be something that you don't use. Like maybe in one company you might use FTP for whatever reason. At another company you don't use FTP. I can't tell you to block all FTP. But if your company is not using certain protocols, you can block those because there might be attacks that are, what you're basically doing is reducing your attack surface by doing that.

Joe:

Yeah. As a general rule on your firewalls, you should pretty much block all ports, except the ones that you want to allow traffic in. Otherwise, you're just open surface and just open season on you at that point.

Roxy:

Right? You could have some obscure protocol be responsible for her bringing down your website. You don't want that to happen.

Joe:

There's no way to determine what protocol that you decide not to close today could be effective DDoS in the future. It's better to be proactive than reactive. In this instance.

Heather:

Do you have any other like tips or resources to offer when it comes to DDoS?

Joe:

If you are in the cloud. Contact your cloud provider. A lot of them, Microsoft, Amazon, and Google have their own in-house DDoS teams that can respond and block the traffic and go about preventing it for you. That should be part of the package depending on what package you select. Definitely, if you're in the cloud look into contacting your cloud provider, if you're under attack.

Roxy:

Or your managed service provider, like Hurricane Labs.

Joe:

There you go.

Roxy:

We can certainly help identify, block, alert. We're very familiar with blocking and identifying this type of activity. Not to toot our own horn or anything. It's kind of what we do.

Heather:

No, No. Toot away. All right. Well, thank you very much for taking the time to chat with me.

Joe:

Thank you.

Roxy:

Yes. Thank you for inviting us. This is a great topic.

Heather:

All Right. That's all for today. Thanks for joining us. Be sure to check out our links to see tools and resources that we talked about today, and until next time stay safe.