DDoS: Evolving Threats, Solutions

Carlos Morales of Arbor Networks Offers New Strategies

FEATUREING:

• Characteristics of recent attacks;
• Gaps in organizations' defenses;
• How to best prepare for and respond to DDoS.
DoS attacks on banks have returned, and the attackers are changing their tactics and expanding their attack toolsets. How must organizations change the way they defend against DDoS? Carlos Morales of Arbor Networks shares strategies.

Morales, vice president of global sales engineering and consulting at Arbor Networks, says the attackers so far have demonstrated great resiliency in their distributed denial of service attacks.

“They’ve gotten more complex, they’re exploiting holes in the defenses of some of the financial institutions that have been attacked - they’ve essentially become intelligent,” Morales says.

So, the challenge is: How do organizations evolve their defensive strategies?

In an interview about evolving DDoS attacks and how to respond, Morales discusses:
• Characteristics of recent attacks;
• Gaps in organizations' defenses;
• How to best prepare for and respond to DDoS.

Carlos Morales, Vice President of Global Sales Engineering and Consulting, Arbor Networks
Morales is responsible for all aspects of pre-sales engineering, consulting and sales operations worldwide. He works closely with Arbor’s customers and strategic and integration partners to ensure ongoing product interoperability and to set the direction for new product features. He has more than 15 years of experience implementing security, routing and access solutions in service provider, cloud and enterprise networks. Morales' background includes management positions at Nortel Networks, where he served as the director of systems engineering for Nortel's access products. Formerly, he was systems engineering director for Tiburon Networks and held systems engineering roles at Shiva Corporation, Crescent Networks and Hayes Microcomputer.
“A lot of the perimeter defenses that most enterprises have put out there, government and others, are really based on technologies that are 10-15 years old.”

- Carlos Morales
Characteristics of Recent Attacks

TOM FIELD: I know you’ve watched these attacks closely. What can you tell us? Have the tools that have been used in the attack characteristics changed over time?

CARLOS MORALES: Yes; in fact, more so than we’ve seen with any other attack to date before this. Clearly, the group behind this is well-organized, well-funded and very capable. They’ve been using a base set of tools, which we’ve called the “Brobot,” KamiKaze, and AMOS, based on some aspects of the tools and a text within the tools.

However, those tools have changed significantly over the course of roughly six months that these attacks have been going on. They’ve gotten more complex. They’re exploiting holes in the defenses of some of the financial institutions that are being attacked. They have essentially become intelligent. Traditional botnet-based attacks tend to be a little bit more brute-force to see if they cause damage -- and if not, “oh well.” These attacks have been shown to actually probe for weaknesses on different networks that they’re exploiting and then attacking based on those weaknesses. “We’ve seen multi-vector -- lots of different attacks that combine both volumetric, as well as application attacks -- on different applications simultaneously. We’ve seen a high volume of attacks against simultaneous companies at once, which stresses the infrastructure, and we’ve seen attacks that are far more subtle in affecting SSL-encrypted traffic and other application-layer exploits that they’re able to manipulate and take sites down. Frankly, the attacks have been ever-changing, which is very unusual for one wave of attacks from a particular miscreant.

How to Best Detect Attacks

FIELD: Given those characteristics, how would you say organizations can best detect these attacks, particularly at the application level as you mentioned?

MORALES: That’s a great question. [While] these attacks are becoming more popular over the last couple of years, application-layer attacks have proven that a one-tool-fits-all approach doesn’t necessarily work. Traditional volumetric attacks were easily detected through statistical anomaly-based means in ISP networks and carrier networks, as well as in enterprise networks looking for changes in network behavior and network traffic that were indicative of threats.

That’s not the case for a lot of these application-layer threats. You actually have to look down deeper into the packet themselves and look for patterns that are deviant from not protocol standards, but deviant from a behaviorist standpoint - maybe doing things over and over that they shouldn’t be doing, or maybe taking and exploiting some limitations or some bottlenecks in protocols and applications. You have to actually look at packet-layer data and apply some fairly comprehensive mechanisms to detect the subtle behaviors that are application-layer threats.

Gaps in Perimeter Defenses

FIELD: You get to see lots of different organizations and lots of different defenses. What gaps do you see in how organizations currently defend their perimeters?

MORALES: A lot of the perimeter defenses that most enterprises have put out there, government and others, are really based on technologies that are 10-15 years old. Firewall technologies, even repackaged as next generation, are still firewalls. They’re still policy-based systems that are trying to detect when something deviates from the normal of a spec of a particular application. Something malicious might hide itself in the application and fundamentally change how that works, so therefore it can get through the block by these policy-based systems.

Similarly, IPS equipment that has been deployed for sometime is also looking at policy-based threats - deviations that have deviated from the specs of the applications themselves. DDoS is something that actually falls within the spec of the application. For instance, many DDoS attacks are just simply connections for the TCP protocol. That’s normal. It may be web

“Clearly, the group behind this is well-organized, well-funded and very capable.”
“We’ve seen attacks that are far more subtle in affecting SSL-encrypted traffic and other application-layer exploits that they’re able to manipulate and take sites down.”
connections. That’s also normal. That’s in fact desirable for a web server.

However, they’re doing something maybe in a malicious way, like asking for the same thing over and over in a connection to the web server. It’s a normal activity done multiple times, which creates an abnormal strain on the system. You have to have a different set of techniques to detect and mitigate those types of attacks. That’s why the intelligent DDoS mitigation devices were invented, to specifically look for and track those types of behaviors that are maybe normal from an application sense, but abnormal from a behavioral sense.

Strategies, Solutions against DDoS

FIELD: If we’ve learned anything from the past six months, it’s that the DDoS problem is clearly growing in complexity. Given that, what strategies and solutions do you recommend to customers to defend themselves?

MORALES: First of all, it’s two-fold. One is they have to take into account the fact that attacks can be volumetric - very large - as well as complex and application-layer-based. Don’t assume that a single solution that says, “I solve DDoS,” is going to solve the problem. You have to look for solutions that are focused on this problem so they’ll change over time as the problems change, and that the types of attacks change.

You also have to look for an ecosystem. Most networks don’t have infinite capacity to the Internet, which means that eventually somebody can come in and attack them and take more bandwidth than is available to them, taking them down. In that case, you really need to have already relationships and agreements in place with your upstream providers to have them aid with the mitigation of it. Taking into account both an ecosystem approach, having upstream and on-premise mitigation, and choosing vendors in the solutions that are dedicated to that job, as opposed to doing it as an offshoot, are really the best practices in this.

Arbor’s DDoS Detection & Response

FIELD: You’ve worked in a number of organizations. Tell us how Arbor has helped these organizations to improve their DDoS detection and response?

MORALES: Arbor has been doing DDoS basically since it was founded in the year 2000. We’re a pioneer in using NetFlow technology to detect those statistical deviations I mentioned earlier as a means of detecting DOS events on your network. We’ve been at this for a long time and we’re very micro-focused on this as a solution.

Fast-forward to today. Arbor has a portfolio of solutions where we’re the only provider that actually has the entire ecosystem of provider-based cloud solutions and premise-based solutions that can both actively mitigate using similar techniques, our own proven techniques, but also talk amongst each other to create a more cohesive solution and ecosystem. In fact, according to a recent Infonetics report, Arbor owns 61 percent of the global DDoS market. We’re very much a proven player in this space and we have the right solution for different types of organizational needs.

Advice on Preparing for DDoS

FIELD: What advice would you give organizations at risk of DDoS? As you and I both know, any organization can be at risk. How should they assess and bolster their preparedness?

MORALES: Preparedness I think is the key word in that. First of all, there are a lot of industry best practices outside of intelligent DDoS mitigation that you can use to limit the attack surface that’s available on your network. That could be everything from dropping any types of services that you’re not actively running right at your network perimeters using ACLs. It could be hardening and maintaining antivirus and latest version control on your services. There are a lot of things that will hopefully reduce the attack surface to more of,
“Application-layer attacks have proven that a one-tool-fits-all approach doesn’t necessarily work.”

“Here are the only services that I’m actually actively providing to the Internet.”

Then, choose a solution based on the tenets that I mentioned before, a solution that’s going to be focused and solve your problem not only today, but in the future, and is able to span the full breadth of the different types of DDoS attacks that are out there and be equipped to handle new attacks as they go forward.

Finally, have the experienced people behind it to be able to help you in the time of need, because not only having the right tools is important but having the know-how and having the right people to call is equally important. I encourage doing some research into what solutions are out there and who can provide that solution. I think you’ll find that Arbor is very clearly the right solution for you.

LISTEN TO THE INTERVIEW

http://www.bankinfosecurity.com/interviews/ddos-evolving-threats-solutions-i-1840
About ISMG

Headquartered in Princeton, New Jersey, Information Security Media Group, Corp. (ISMG) is a media company focusing on Information Technology Risk Management for vertical industries. The company provides news, training, education and other related content for risk management professionals in their respective industries.

This information is used by ISMG’s subscribers in a variety of ways—researching for a specific information security compliance issue, learning from their peers in the industry, gaining insights into compliance related regulatory guidance and simply keeping up with the Information Technology Risk Management landscape.

Contact

(800) 944-0401
editor@ismgcorp.com