DDoS Ransom Attack: No Honor Among Thieves

RED BUTTON
DDoS Experts

BACKGROUND

The customer is one of several online gambling companies in the Caribbean islands. Gambling is a very large industry in the region, with both online and casino gambling operations regulated by law in the customer's country.

THE CHALLENGE

The customer was suddenly hit with an aggressive volumetric attack on its main website. Their ISP data center - which included a DDoS mitigation appliance, a firewall and a local traffic manager -was overwhelmed. Pipe saturation was reached and the site went down.

Every hour the site was down cost the company tens of thousands of US dollars, adding up to one million dollars or more during peak hours. The immediate losses are compounded by the reputational impact on continuing business, with customers driven to the competitors and possibly not returning.

THE SOLUTION

Once the successful DDoS attack was underway, the company launched an urgent search for incident response (IR) experts. An IT consultant provided them with a contact who recommended Red Button.

The company reached out to Red Button in Israel by phone on Friday morning. IR began immediately with mitigation guidance and by midnight, a Red Button team was in the air to the Caribbean.

A Costly Cat-and-Mouse Game

It was clearly more than a one-off DDoS attack. A sophisticated "cat-and-mouse-game" began between the attacker and the company, with every mitigation move met by a new attack vector, followed by a new defense, and so on.

In response to the initial volumetric attack on their website, the company purchased a cloud-based web application firewall (WAF) with the capability and mitigation technology to handle whatever level of traffic is thrown at it in DDoS attacks. This additional layer of protection relieved pressure on the data center, with incoming DNS traffic diverted to the WAF first.

The attacker was apparently expecting that and began a direct-to-origin attack, bypassing the diversion mechanism and targeting the company's IP address directly. Pipe saturation was reached again, with the same impact as the original attack.

Identifying the new tactic, the company requested a different IP address for their website from their internet service provider (ISP). The hacker may have known the previous IP, but this one would be hidden from their view.

No such luck. The website's new address came under another volumetric attack. And it hit hard, taking down the entire Caribbean-based ISP and affecting many other companies as well. The Red Button team shared with the customer the hacking techniques possibly

used to discover the new IP. However, company leadership believed it was simpler than that – the hacker probably bribed someone for it.

The next step was to change ISPs. The customer selected a larger service provider, based in the United States and offering much better default DDoS protection. That quickly put an end to the volumetric attacks.

But not to the entire DDoS campaign. The attacker moved on to application attacks, which even very good ISPs cannot block.

The first target was the website's homepage. The company reacted with a geo-protection measure, instructing their cloud WAF vendor to selectively block traffic from outside the country. The DDoS traffic, originating from around the world, would be very effectively neutralized by this restriction without harming business, because local regulations limit online gambling to national residents alone.

Within a short amount of time, the homepage once again came under attack. The hacker switched to a totally local botnet, bypassing the geo-protection roadblock. Red Button noted that this was very, very rare and indicated the attacker's skills, capabilities and persistence.

The solution was applying a transparent redirect rule within the cloud WAF, sending traffic to the server after a detour to a new URL. This requires a behind-the-scenes interaction with the visitor's browser, which DDoS bots cannot generally emulate. Again, the attack was mitigated.

So, the attacker tried one more application-level vector and targeted a different page on the company's website. The company then established a new firewall rule and all hostile requests to that URL were blocked before reaching the server.

Turncoat: The DDoS Ransom Letter

Throughout the DDoS campaign, the hacker was clearly paying close attention to attack effectiveness and reacting quickly. Then, out of the blue, came a novel and unexpected twist.

The attacker contacted the company directly.

"I am the one responsible for taking down your business," the communication said, claiming that two competitors hired the hacker as a DDoS mercenary. However, they did not pay as agreed and the hacker is willing to halt the attack – in exchange for a ransom of 400,000 US dollars. The hacker even offered a "package deal": to not only stop the attack, but also attack the company's competitors and provide defense against any future DDoS attacks.

Lesson Learned: Don't Gamble on DDoS Protection

The attacks continued, but without any impact thanks to the mitigation measures taken.

The volumetric attacks were identified, analyzed and addressed over a couple of days, with mitigation dependent on the responsiveness of the ISP and the cloud WAF vendor as well. Each of the application attacks were identified and handled within around an hour.

While the incident response was key to getting the customer's business back up and running, it had longer-term implications as well. Red Button guided the customer in configuring their cloud WAF in line with the capabilities of the specific vendor and how to optimize their defensive architecture. In addition, three active protective measures were implemented immediately and three others were prepared for emergency deployment in the event of renewed DDoS attacks.

Thanks to Red Button, the customer was no longer taking any chances.