DDoS

Today's attackers can corral millions of systems infected with malware to launch focused botnet attacks that can easily bring down targeted servers.

ebook

An SC Magazine publication

Sponsored by

Waiting for DDoS

There are modern defensive measures organizations can employ to protect themselves from relatively inexpensive and easily exploitable DDoS attacks. Larry Jaffee reports.

In American football, many offensive plays are designed to trick the defense into thinking something else is about to unfold. In the world of cybersecurity, DoS (denial-of-service) or DDoS (distributed denial-of-service) attacks often serve as a similar smokescreen to a far more sinister plot – with the ulterior motive to mount a computer network breach that results in the loss of data or intellectual property.

A DoS attack typically uses one computer and one internet connection to flood a targeted system or resource, whereas DDoS uses multiple computers and internet connections to flood the targeted resource.

It was a DDoS attack that woke up Sony Pictures a year ago (watch the video emailed to Sony employees on the morning of the incursion: http://for.tn/1HgzKb5), even though attackers had infiltrated the company's networks undetected months before – and eventually obliterated its computer systems. According to Fortune, half of Sony's global network was wiped out, erasing everything stored on 3,262 of the company's 6,797 personal computers and 837 of its 1,555 servers.

Hackers calling themselves "#GOP" (Guardians of Peace) threatened to release Sony Pictures' internal data if their demands, including "monetary compensation," were not met. They weren't bluffing.

#GOP's demands, other than halting the release of the movie The Interview, which lampooned North Korea's president, were never clearly stated. But when the attack became public, it was revealed that #GOP emailed Sony's top management warning of a damaging cyberattack three days before studio employees could not use their computers. Sony executives reportedly dismissed the emails as spam and didn't open them.

While perhaps not as monumental as the assault on Sony, another method, ransomware, is often tied to a DDoS attack, followed by demands of being paid in Bitcoins. Often the attackers make relatively modest requests of the equivalent of thousands of dollars. Pay up or your site won't function again, the attackers threaten. (Sound advice: Don't! Attackers almost always are going to act on their threats whether or not you meet their financial demands, experts say. You are better off seeking immediate law enforcement help.)

DDoS attacks are wielded on companies and organizations of all sizes and all industries. In the past few months, email companies in Europe and Australia were crippled with a flurry of highly publicized ransomware-driven attacks.

OUR EXPERTS: DDoS

JJ Cummings, managing principal, Security Incident Response Team, Cisco
Ondrej Krehel, digital forensics lead & CEO, LIFARS
Larry Ponemon, chairman & founder, Ponemon Institute
Charles Renert, VP of cybersecurity, ViaSat
Mark Tonnesen, CIO, CSO and VP operations, Neustar
Mike Weber, VP of labs, Coalfire

Sobering DDoS statistics

Recent studies show DDoS attacks growing exponentially in the past few years, launched through rentable, relatively inexpensive anonymous botnets that cost as little as $1,000 and can render an e-commerce website completely inoperable.

The average denial-of-service (DoS) attack costs the victim $1.5 million, according to a separate Ponemon Institute survey sponsored

>20%

of the DDoS attack vectors in Q1 2015 were Simple Service Discovery Protocol attacks.

– Akamai State of the Internet [security] report

by Akamai and published in March 2015. The 682 responding companies reported four attacks a year.

AT&T also reported that companies across its network were hit four times a year with DDoS attacks and experienced 62 percent growth in DDoS attacks over the past two years.

Once an organization is on the receiving end of a DDoS attack, the chances of it subsequently being the object of a data breach are better than 70 percent, reported Neustar, a Sterling, Va.-based provider of cloud-based information services, including conducting research on cloud metrics and managing various top-level internet domains.

Further, the second quarter of 2015 set a record for the number of DDoS attacks recorded on Akamai's Prolexic Routed network – more than double what was reported in 2014's second quarter. The worst DDoS attack on the Akamai network peaked at 214 million packets per second (Mpps), a volume capable of taking out tier 1 routers, such as those used by internet service providers (ISPs).

Corero Networks, a Hudson, Mass.-based security services provider, reported that its clients were getting DDoS attacks an average of three times a day, and in the second quarter of 2015 daily attack volume reached an average of 4.5 attacks, a 32 percent increase from the previous quarter.

Additionally, more than 95 percent of the attacks combated by Corero last 30 minutes or less, and the vast majority of the attacks were less than 1 Gbps.

Only 43 percent rate their organizations as highly effective in quickly containing DoS attacks, and only 14 percent claimed to have had the ability to prevent such attacks, according to the Ponemon report.

Pretty sobering statistics. One wonders how the internet works as well as it does.

"It's pretty hard to stay one step ahead of these guys," admits Mark Tonnesen, chief information officer and chief security officer of Neustar. In a recent survey of 760 security professionals, DDoS attacks increased in 2015 six-fold when compared to the previous year. The survey was commissioned by the Neustar (and conducted by Simply Direct of Sudbury, Mass., for the U.S. market and Harris Inter-

Inside: DDoS forensics

Volumetric attacks, such as DNS or NTP reflections or UDP (User Datagram Protocol) or SYN/ACK (Synchronize/Acknowledge) floods, consume all available bandwidth targeting the largest internet carriers.

"They're created to take them down," says Ondrej Krehel, digital forensics lead and CEO of New York-based cybersecurity firm LIFARS. "It's a brute force."

Layer 7 attacks target consumer web server resources or application protocols. "The attacker is not stealing the pipe but stealing the request," Krehel explains, likening it to when a banking system locks you out after a number of attempts using incorrect passwords.

Protocol attacks consume server resources via SYN floods, UDP or ICMP (Internet Control Messaging Protocol) fragments, a server-crashing "ping of death," or the so-called "teardrop" attack that sends seemingly overlapping data packets. In this scenario, initial communication is made, but not completed. It's the equivalent of repeatedly calling the front desk, put on hold and then hanging up. Meanwhile, the server gets filled up with incomplete requests and the CPU gets bogged down or runs out of memory.

"All three types of attacks can happen at the same or any time from seconds to minutes, or combined," points out Krehel.

37%

of DDoS attack traffic originated from IP addresses in China in Q2 2015.

– Statista

active of London for the Europe, Middle East and Africa markets).

"Everyday there's an announcement of some [DDoS attack] going on with a company caught unprepared, trying to ramp up with people and technology," Tonnesen says. "Companies are looking for any way they can grab an edge in identification, detection and reaction time to eliminate the attack."

Interruption versus outage

Creating havoc via an outage is not necessarily an attackers' modus operandi. Their ulterior motive generally is to capture real value from the attack, such as financial gain, brand carnage or intellectual property resold on the underground market. Any of those scenarios happen nine out of every 10 DDoS attacks, according to Neustar. The impact on a company's customers and a firm's bottom line "negatively impacts everybody's financials," Tonnsesen points out.

Mark Tonnesen, CIO, CSO and VP operations, Neustar

DDoS attacks, which can take the form of an interruption or the more serious outage, almost always serve as a smokescreen diverting attention from a data breach. Meanwhile, the IT staff is trying to figure out why the website isn't working properly. "Unbeknownst to you, [the malware is] already in your network," Tonnsesen says.

A DDoS outage is a complete slaughter of messaging to a network, such as an e-commerce platform. Effectively, the network appears to shut down completely due to the bandwidth overload, making it nearly impossible to get traffic through to the website. In contrast, a DDoS interruption involves a targeted attack, such as to a customer service organization affecting intellectual property or customer records and identity.

"[An interruption] certainly has a major impact, but it wouldn't be an outage," explains Tonnesen. "It's more of a disruption, not a flat-out attack." The attackers, he says, are much more intelligent and organized. They know what they're looking for, and are out to affect your brand or reap a financial impact. There's an element of showcasing their capability and illustrating a company's weaknesses, he adds. As a result, IT security and network teams must be vigilant and always be on high alert.

The hybrid solution

Some CISOs are moving to a "hybrid" approach to combating DDoS attacks of the Application Layer 7 variety. The approach uses an on-ground client security product that links with a cloud-based mitigation tool. One argument for this approach is that attack victims can react more quickly to a specific attack on a business area, such as engineering or customer support, if they have the benefit of cloud-based updates rather than waiting for a network-based device to be updated.

Layer 7 refers to the seven common layers within an application. Each layer serves a specific purpose in a connected networking framework called the Open System Interconnection (OSI) Model, following a set of standard protocols with the aim of enabling the interoperability of diverse communication systems.

OSI separates into seven layers that transport data up and down the chain – from the user all the way to the physical server and back again. Each layer employs its own protocol, responsible for carrying out an assigned function.

"Based on the customers I talk to, hybrid approaches are becoming mainstream," says Tonnesen.

79

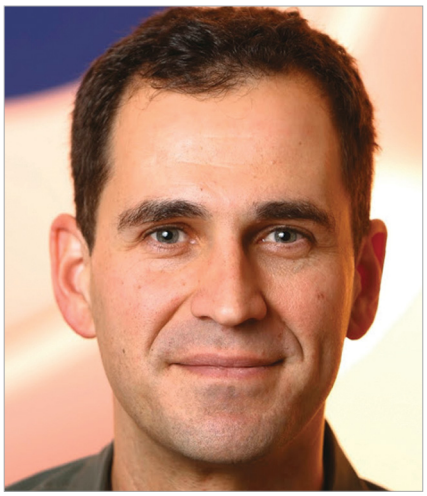
In Q2 2015, botnet-assisted DDoS attacks targeted victims in 79 countries.

– Kaspersky DDoS Intelligence Report Q2 2015

Best practices: A telecom/defense contractor

ViaSat is a Carlsbad, Calif.-based global broadband services and technology company, whose internet services are used by consumers throughout the world. In addition, its services are used by international military forces on the frontlines of battle, as well as commercial, business or government aircraft and maritime vessels. With that kind of customer base, it obviously must keep up its guard regarding potential DDoS attacks.

Charles Renert, vice president of cybersecurity at ViaSat, lays out some best practices to combat what he calls today's "commodity-grade attacks," the more sophisticated DNS- and NTP-based (Network Time Protocol) assaults that are currently commonplace. Under this scenario, he says, attackers send high volumes of data and a target's ability to intercept a known traffic pattern or source conducting an attack is tested.



Charles Renert, VP of cybersecurity, ViaSat

"That's the old-school way of doing things that gets you a little way there," he says.

Attackers use reflective capabilities, throwing large volumes at the target. Then they request DNS or NTP services as somebody else. This way, he says, "the response doesn't come back to you; it goes to whoever you're targeting." Adding insult to injury, the increase in bandwidth increases the internet access fees companies pay their service providers, so it becomes a financial hit on both ends – being the victim and paying for the right to be the victim. "So you get 200 or 300 times bang for the buck, creating some absolutely massive attacks, as much as the 1,000-gigabit range we've seen in the last couple of years," he says. Tools can be purchased and services can be rented by the hour to combat such tactics and techniques.

It behooves organizations susceptible to such threats to increase network capacity well and above what's required to absorb and distribute such attacks, especially when they get into the 100-plus gigabit capacity, he says. "DDoS attacks are fundamentally repetitive. There are characteristics that you can identify. They come and go and typically appear over a short period of time, such as a half hour."

Renert says organizations should also be equipped to correlate and identify new attacks by their nature, and then have a process that automatically drops packets redirecting the traffic.

"There are false positives," Renert notes. "It's good to have humans in there to be able to identify what's happening. That's a good practice as well."

Client and cloud security products work together with one or the other configured as a rules-based defense working on certain types of data attacks that affect key assets and applications. Typically, underlying attacks involve a DNA-like sequence that lives in a lower level of an organization's technology stack, such as malware sitting on a server some place, and begin to take over key assets.

"That's where a DDoS mitigation service can really help a weakness or attack sector," Tonnesen says. "One approach really isn't good enough anymore."

That's because miscreants are employing several tactics in carrying out their cam-

64

The longest network-layer attack of Q2 2015 lasted 64 days, with slightly more than 20% lasting five days or more.

– Incapsula Q2 2015 Global DDoS Threat Landscape

paigns. Mike Weber, vice president of labs at Coalfire, a cyber risk management and compliance company based in Louisville, Colo., says, "Being able to diagnose a denial-of-service attack does take some time. Generally, understanding if it's a problem internally, such as an application malfunction, system problem or faulty hardware, those kinds of diagnostics take a while."

When Weber was fending off DDoS attacks at a former employer, a web-hosting company, he received an insider's view of old-fashioned corporate espionage. The client-hosting company had known adversaries but could never pin the frequent attacks on a single entity. "They had a good idea who was behind the attacks," he remembers. "A lot of times, it was their competition. It was used as a revenge tactic. Sometimes it was intended to impact that company from a business perspective for whatever reason. Maybe it's a page rank or advertising issue."

J.J. Cummings, managing principal of Cisco's security incident response team

Mike Weber, VP of labs, Coalfire

Attackers leverage those kinds of attacks to consume personnel/intellectual capital being used for diagnosis. While the victim attempts to identify the strategy, attempting to thwart it typically sends victim companies into a state of chaos.

An attack against a website can be set to look like a denial-of-service interspersed with an attack that achieves the end goal of flooding log servers. The logs' giant volume makes it harder to find who is launching specific targeted attacks.

Typically, the obvious attack needs to be stopped before one can diagnose the other less obvious attack. "Think of that as DNS (Domain Name System) amplification," Weber says. "It's a DDoS attack where the attacker basically exploits vulnerabilities in the DNS servers to be able to turn small inquiries into large payloads, which are directed back to the victim's server." Those are a different protocol than those other attacks that are attacking different parts of the infrastructure – whether they're operating systems or applications, he says. "So, typically, they would be targeted toward two different parts of the client environment."

Malicious traffic

A typical approach to prevent DDoS from inflicting damage is to re-route non-malicious traffic to a cloud-based or third-party provider whose sole purpose is to mitigate denial-of-service-type attacks at what's known as a "scrubbing" center.

"Only clean traffic gets through," says J.J. Cummings, managing principal of Cisco's security incident response team.

DDoS traffic then purposely gets diverted to the external provider, which takes the brunt of the attack and roots out all that's evil and bad, he says. Denial-of-service attacks are extremely challenging and can be expensive from a mitigation perspective, in terms of pipe size and technology, he admits.

"At the end of the day, it comes down to how critical these business applications are," Cummings says. "How much do you want to

$40K

DDoS attacks cost businesses on average $40,000 per hour.

– Incapsula Q2 2015 Global DDoS Threat Landscape

spend to withstand an attack – and an attack of what size?"

Assaults come in various ways. DDoS can be enabled by a web page's application flaw, resulting in considerable CPU cycles. The attacker figures out the flaw and shoves data at it, overloading the web server's capacity. The same could be done to a network segment or servers, knocking them offline.

The first questions that need to be addressed before, during or following a DDoS are how big is your internet pipe and how much bandwidth has been thrown at you historically?, says Cummings. The answers determine a network's required level of operational capability, as well as what the needs are at a bare minimum to resume the business.

Larry Ponemon, chairman & founder, Ponemon Institute

Security products are available from multiple vendors to help harden a company's public-facing systems so they're less susceptible to targeted types of attacks. "Those technologies presume you have enough of an internet pipe to withstand that amount of bandwidth," says Cummings. Otherwise, it's a moot point.

Detection analytics is another important tool to put DDoS mitigation measures in place. "You don't all the sudden get a terabyte of traffic hitting," he adds. "It kind of spools up, as that botnet starts to distribute the attack commands." ISPs can know in advance to block certain IP addresses or certain traffic streams upstream.

More sophisticated attacks often are focused on a profit motive and target companies with a lot of money, or a gambling site that is taking bets on a major sporting event. In online video gaming or gambling, some players go to the extreme, firing off a DDoS attack to disrupt the network where the opposition is hosted. Retribution is another scenario with DDoS attacks. A former employee or student gets mad and rents a botnet to conduct an attack.

Whatever the motivation, a consequence of a denial-of-service attack is damage to the victim organization's reputation, in addition to a potential dollar loss for every minute that the network is offline. Nearly two-thirds (64 percent) of respondents in Ponemon's denial-of-service study say reputation damage is the main consequence of a DoS attack, with 35 percent for diminished IT staff productivity and 33 percent for revenue losses.

"We try to come up with metrics on how to measure reputation loss, which is pretty significant," says Larry Ponemon, chairman of the Ponemon Institute, the cybersecurity think tank based in Traverse City, Mich. "When people hear the bad news, what do they do? The churn can be significant from a revenue point of view. People leave, they find alternatives."

Citing research from the institute's recent "Cost of Data Breach" study, Ponemon says when compared to other security incidents, such as phishing, the most expensive attack type, on a unit cost per attack, is DDoS, because it takes a lot of effort to stop it. Meanwhile, he adds, "there's an extraction of data while people are worrying about the website being down." ■

For more information about ebooks from SC Magazine, *please contact Stephen Lawton, special projects editor, at stephen.lawton@haymarketmedia.com.*

If your company is interested in sponsoring an ebook, contact David Steifman, VP, publisher, at 646-638-6008, or via email at david.steifman@haymarketmedia.com.

17%

Sunday was the most popular day of the week for DDoS attacks in Q2 2015 with 16.6% of all attacks

– Kaspersky DDoS Intelligence Report Q2 2015

Sponsor

Masthead

EDITORIAL
VP, EDITORIAL Illena Armstrong
illena.armstrong@haymarketmedia.com
ASSOCIATE EDITOR Teri Robinson
teri.robinson@haymarketmedia.com
SPECIAL PROJECTS EDITOR Stephen Lawton
stephen.lawton@haymarketmedia.com
MANAGING EDITOR Greg Masters
greg.masters@haymarketmedia.com

DESIGN AND PRODUCTION
ART DIRECTOR Michael Strong
michael.strong@haymarketmedia.com
PRODUCTION MANAGER Brian Wask
brian.wask@haymarketmedia.com

SALES
VP, PUBLISHER David Steifman
(646) 638-6008 *david.steifman@haymarketmedia.com*
REGION SALES DIRECTOR Mike Shemesh
(646) 638-6016 *mike.shemesh@haymarketmedia.com*
WEST COAST SALES DIRECTOR Matthew Allington
(415) 346-6460 *matthew.allington@haymarketmedia.com*