What Organizations Don't Know About DDoS Attacks *Can* Hurt Them.

The threat is real, so is the solution.

DDoS (distributed denial of service) attacks are real and the threat is escalating in volume and complexity. In fact, newsworthy attacks like the following are occurring almost every week:

- At least five major Russian banks came under continuous DDoS attack for two days. The attack was spawned by a wide-scale botnet involving at least 24,000 computers, located in 30 countries.
- Major internet services including Twitter, Spotify and Amazon suffered service interruptions and outages simultaneously over several hours due to a DDoS attack.
- The computer systems of two prominent Boston hospitals were simultaneously crippled by a DDoS attack. The hacker wanted to take revenge on one of the hospitals for personal reasons.[1]

Chad Foos, IT Security Engineer for Verizon Platinum Master Agent SOVA, said, "No one is immune to this. That's the reality of putting your business online today. They are becoming more and more common. If Twitter is vulnerable, anybody is vulnerable."

In a DDoS attack, the perpetrator infects a random army of as many as 100s of 1,000s of poorly protected computers with malware designed to target a specific network(s). This makes it impossible to prevent or stop the attack by blocking a single IP address. It is also nearly impossible to distinguish legitimate traffic from DDoS traffic. This incoming traffic overwhelms the network and either shuts it down or severely compromises it. Foos likens the attack to a few shoppers in a sea of shoplifters all trying to squeeze in a single revolving door.

Driving the increase in depth and breadth of DDoS attacks are hacktivists that tend to target government, university, hospital, and military servers; and professional cyber criminals that seek out high-profile web servers such as banks, credit card payment services, ecommerce sites, and insurance companies. Malicious hackers are just looking for any vulnerable network to take down. Organizations that tend to get hit the hardest financially by an attack are (in this order): financial services, health and pharmaceuticals, and the public sector.

A new and even more insidious DDoS attack is called BlackNurse. It allows hackers to launch large-scale attacks with significantly fewer resources than those required for basic DDoS attacks. Hackers can take down servers and firewalls with a single laptop. BlackNurse does not need that same army of devices and does not rely on high traffic volumes to be effective. Instead, it issues low volume ICMP error messages to servers and firewalls, which can easily overload and nullify main processors.[2,3]

The good news is that DDoS attacks tend not to compromise secure information and the effects are fairly obvious quickly. In addition to a huge spike in network traffic, signs of a DDoS attack include:

---

[1] From: https://www.ddosattacks.net

[2] From: https://www.ddosattacks.net/new-ddos-attack-method-called-blacknurse-lets-hackers-take-down-firewalls-and-servers-from-a-single-laptop/

[3] ICMP (Internet Control Message Protocol) is used by network devices, such as routers, to send error messages and operational information indicating that a requested service is not available or that a host or router could not be reached.

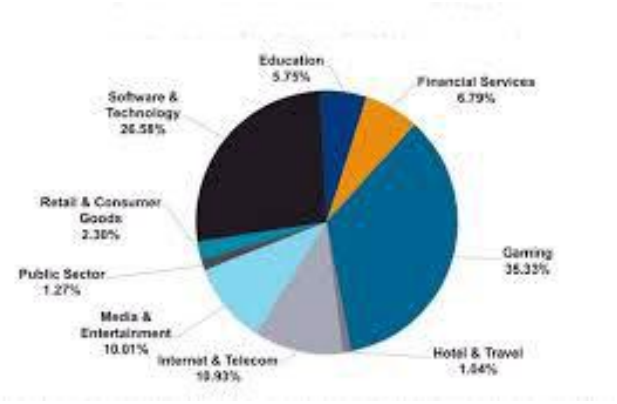
- Unusually slow network performance
- Unavailability of a website (incoming)
- Inability to access any website (outgoing)
- Disconnection of a wireless or wired internet connection

The bad news is that there is no foolproof way to prevent a DDoS attack, typical security software is ineffective. A DDoS attack will last until someone or something steps in to filter and reroute traffic.

Why All Organizations Should Care

It's not a big deal if a network is down for a few hours, right? So why should anyone care? Here's why:

- People that are not able to use a particular site efficiently will turn to competition.[4]
- People that rely on the site for critical services will effectively be turned away—imagine someone with a serious injury attempting to connect to a healthcare site to find a network provider.
- Even though personal information may not be compromised, site users will see the site (and the organization) as unreliable and untrustworthy.
- When the site is back up, unsure if it is still infected, people will shy away from it.
- A poorly performing site just makes people nervous.



Most Frequently Attacked Sectors

And the list goes on…immediate costs include:

- Direct revenue loss—organizations that depend on the site for revenue are hit the hardest.
- Loss of employee productivity.
- IT costs for investigation and response.
- Financial penalties and litigation.
- Loss of intellectual property.

A recent Ponemon Institute study estimated the average cost of a single minute of downtime due to a DDoS attack at $22,000. With an average downtime of 54 minutes per DDoS attack, this amounts to $1.19M.[5,6,7]

What Can Be Done to Mitigate an Attack

"Basic website security software will block IP addresses," Foos said. "But there are issues. For example, a lot of the hardware devices require the site to shut down. DDoS attacks with the potential to create even nominal financial damage will require a more sophisticated solution."

Some basic DDoS Mitigation Tools Include:

- Application Front-End Hardware: This analyzes data packets as they enter the system, and then identifies them as priority, regular, or dangerous.
- Blackholing and Sinkholing: All traffic to the target site is sent to a non-existent server. A DNS sinkhole routes traffic to a valid IP address which analyzes traffic and rejects invalid traffic. This is not particularly effective.

---

[4] According to Microsoft, a customer will be less likely to visit a website if it is slower than a competitor site by more than 250 milliseconds. Source: : https://blog.radware.com/security/2013/05/how-much-can-a-ddos-attack-cost-your-business/

[5] This estimate depends on several variables, such as business segment, volume of online business, competitors, and brand value.

[6] From: https://blog.radware.com/security/2013/05/how-much-can-a-ddos-attack-cost-your-business/

[7] Ponemon Study at: https://security.radware.com/uploadedFiles/Resources_and_Content/Attack_Tools/CyberSecurityontheOffense.pdf

- IPS-Based Prevention: This is effective only if the attacks have signatures (illegitimate content) associated with them, which is almost never the case today. However, because it has more processing power and granularity, an ASIC-based IPS can be effective.[8]
- DDS-Based Defense: Can block connection-based DDoS attacks and those with legitimate content but malicious intent.
- Firewalls: A simple rule could be added to deny all incoming traffic from the attackers based on protocols, ports, or the originating IP addresses.
- Routers and Switches: They have some rate-limiting capability. But most can be easily overwhelmed under a DDoS attack.

Automated Bandwidth Accommodation and Upstream Filtering

In order to wreak havoc, DDoS bandwidth-saturating floods count on the attacker having higher bandwidth availability than the target. High level tools, such as Verizon's DDoS Shield, identify a standard Quality of Service (QoS) level, for example *response time should be less than 200 milliseconds*. This rule is linked to an automated platform that raises more bandwidth from Verizon in order to meet the defined QoS levels during the flood of DDoS traffic. As the bandwidth is increasing, all traffic is passing through a scrubbing center that separates bad traffic from legitimate traffic. It then sends only the legitimate traffic through to the server. The result is that those using the site will not experience any disruption in service.

Foos explained, "DDoS Shield is one of the most exciting tools that SOVA offers its agents. The way Verizon's DDoS Shield works is that it says, *OK you are under an attack. Send the traffic to us and we will clean it.* It will all happen behind the scenes and will not interrupt service to your site. One of the reasons this is so effective is that Verizon has enormous DDoS reservoir services—they have a lot of capacity for filtering DDoS attacks."

Back to the earlier analogy…legitimate holiday shoppers and nefarious shoplifters all trying to squeeze in a single revolving door. Now imagine that this goes on for hours and it's during a peak holiday shopping season (a time when DDoS attacks tend to be more frequent). And imagine that there is some way to instantly screen out all of the shoplifters and let the holiday shoppers through. That's what DDoS Shield does—it takes the damage factor out of DDoS attacks.

About Verizon's DDoS Shield

DDoS Shield, backed by Verizon's years of experience in the market, detects and identifies attacks and prevents them from taking down the targeted site. It is a high-capacity, cloud-based DDoS protection service that quickly reroutes DDoS traffic and keeps IT resources readily available. It seamlessly scales broadband to control even large DDoS attacks no matter which carrier or internet service provider the customer is using. It also handles attacks against most internet-connected services; web, email, file transfer protocol (FTP) and more. DDoS Shield can be customized to align with risk management policies and can leverage the customer's existing hardware to maintain IP traffic routing control. Even organizations whose own DDoS mitigation services fall short can easily send their traffic to DDoS Shield.

The hybrid, always-on method combines dedicated, locally deployed, fully managed MSS appliances to detect and allay initial attacks with a cloud-based mitigation service. This allows Verizon to easily move traffic from MSS to the cloud-based service if an attack is large or complex. DDoS Shield offers protection from the smallest to largest attacks.

About SOVA

Agents think of SOVA first for Verizon solutions, including DDoS Shield. As a valued Verizon Partner Program member since 1994, SOVA has earned Platinum level status; agents benefit from select privileges that many telecom solution providers cannot offer. SOVA has customized programs for telecom agents, VARs, MSPs, and telesales organizations and provides customer solutions in every product category including voice and data, network, cloud, mobility, machine-to-machine, managed internet, VoIP, and global services. SOVA's award-winning agent program features no quotas, no minimums, no commitments; dedicated pre-sales and post-sales specialists; simplified quoting and ordering; and a state-of-the-art agent portal. SOVA is headquartered in Plains, Pa., with additional locations in Pittston, Pa.; Boston; Denver; and West Palm Beach, Fla.

[8] An ASIC (application-specific integrated circuit) is an integrated circuit customized for a dedicated use.