Art of Darkness

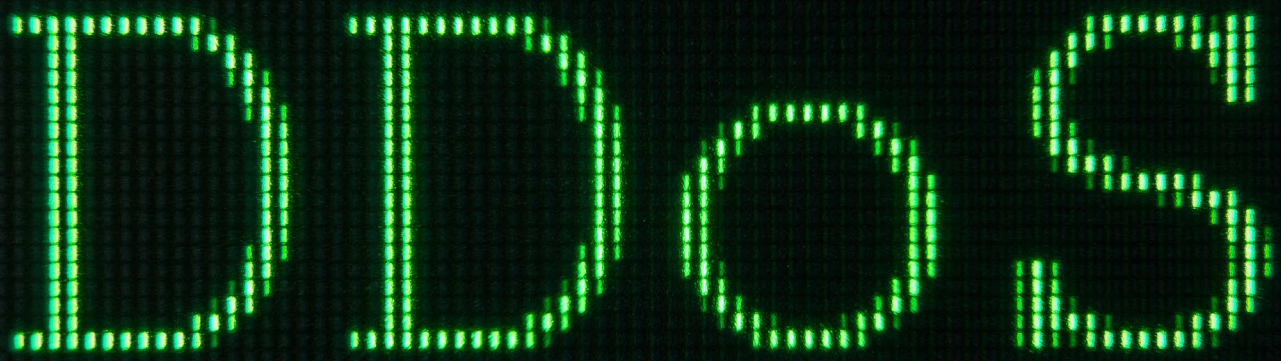
UNDERSTANDING THE DDoS THREAT

neustar®
Security

The biggest cybersecurity issue of our time...

Distributed Denial of Service (DDoS) attacks — owes its origins to a brute force concept fans of professional wrestling might appreciate: The Takedown. It's a bully tactic, a power play, and an attempt on the part of the perpetrator to flex their cyber muscle by turning order into disorder.

Fast forward to the present. Long considered the domain of cyber geeks and their friends, DDoS attacks are no longer the straightforward phenomenon they once were. These days, they're increasingly used as smokescreens to cover more nefarious activities aimed at businesses, financial institutions and governments. The real damage is done while IT staffers are busy trying to stop the attack.



Smells Like Teen Spirit:

A BRIEF HISTORY OF DDoS

The first ever denial-of-service attack occurred more than forty years ago, courtesy of 13-year-old David Dennis, a high school student in Urbana, Illinois. Born of curiosity, not criminal enterprise, Dennis's efforts to "test the limits" of a roomful of computer terminals did, indeed, turn order into disorder, though it was largely confined to a University of Illinois research lab.

The first known DDoS attack to affect the Internet was perpetrated in February 2000 by a Quebec teen, Michael Calce, who went by the online moniker Mafiaboy. His victims included such well-known commercial enterprises as Yahoo, Amazon, CNN, eBay and Dell.

Teens being teens? With the rise of big data around the corner, it's unlikely any of these youths realized their brazen exploits had inadvertently taken the lid off a tactic that cybercriminals would be all too happy to utilize for years to come.

A Powerful Weapon Unleashed

It's easy to see why DDoS attacks have grown in number and sophistication. The distributive nature of this type of attack makes it a highly effective weapon, hard to identify and even harder to block. It was only a matter of time before geeks gave way to gangs and other criminal enterprises that sought to launch DDoS attacks on bigger targets in the hopes of reaping even greater rewards.

Finding themselves increasingly vulnerable to cybercriminals, businesses, financial institutions and government agencies all began to invest in DDoS mitigation. No longer able to rely solely on their own IT teams to defend against DDoS attacks, they turned to cybersecurity specialists and DDoS service providers to analyze risk and develop strategies to prevent future breaches.

Yet despite the increased emphasis on DDoS protection, the attacks have continued. Matt Wilson, Director of Network Engineering for Neustar, says the attacks haven't simply grown in quantity; they've actually evolved, adapting themselves to the changing times. "While many of the most common DDoS attack vectors have remained static," Wilson says, "new attack vectors are often related to new technologies such as the Internet of Things (IoT) and home video cameras."

Wilson goes on to point out that many of these new vectors have been identified right away by so-called "white hat hackers", but that the failure on the part of service providers to issue emergency patches in a timely manner has enabled them to take hold and flourish as live attack mechanisms.

"While many of the most common DDoS attack vectors have remained static, new attack vectors are often related to new technologies such as the Internet of Things (IoT) and home video cameras."

Matt Wilson
Director of Network Engineering
Neustar

Not Your Father's Bad Guys

It isn't just the nature of DDoS attacks that has evolved. The bad guys themselves have evolved, too. So-called "computer geeks", like David Dennis and Michael Calce, are still out there, and they're still capable of wreaking plenty of havoc. In 2016, a 21-year old college student and two friends pleaded guilty to masterminding an unprecedented attack on key Internet services. (The students claimed they were trying to gain the upper hand in the sandbox video game Minecraft, not take down the Internet.) Additionally, when banks and websites in the Netherlands fell victim to aggressive DDoS attacks in January of 2019, the culprit turned out to be a local 18-year-old.

Yet recent years have seen a rise in the number of DDoS attacks perpetrated not by teens but by cyber criminals. By flooding a "target" with superfluous service requests, these enterprising cybercrooks are able to overload the target's system, block customer access, plant malware, and, crucially, extract ransom payments from their victims.

Chaos for Hire

How are they doing it?

Hacking isn't paddy cake. It's a complex enterprise that requires a distinct skillset. The good news for criminals these days is that sophisticated hacking knowledge is for sale. DDoS attack services are increasingly bought and sold online, a development that makes it possible to disrupt a business for profit with little or no knowledge of computer programming.

With attack tools and services increasingly easy to access, the number of potential attackers has grown ever larger, as has the number of potential targets. Criminally minded gangs and nation states are discovering that it's faster and easier to pay for DDoS-as-a-Service than it is to deploy digital armies or build botnets of their own. Highly skilled, financially motivated hackers have become invaluable resources to cyber terrorists seeking to take down and extort a target.

Evolving Tactics, Darker Attacks

Never underestimate the capacity of the criminal mind to seek out new and inventive ways to subvert and sabotage for profit. Today's DDoS attacks are increasingly waged not simply as modes of *disruption* for the purposes of extortion, but as modes of *distraction* to mask fraud that's taking place in the background.

How does it work? According to Neustar's Matt Wilson, in a typical DDoS attack, a large amount of data or traffic is sent to the targeted website, effectively crashing its servers and denying users access to its services. For the criminally minded hacker, the ensuing disruption is only the beginning. "The attack is implemented to distract," Wilson explains. "It's intended to consume resources and IT attention, while an entirely different activity is taking place."

This might be the insertion of malware or the theft of personal information for future phishing expeditions. Another cybersecurity expert compared it to setting a fire in the front yard of a house, then slipping in through the back door.

The criminals are simply following the money. In the age of big data, as more of our lives are conducted over the Internet, attacks designed to block access to our favorite websites, or to use DDoS attacks as a front for identity theft, have become increasingly lucrative. The phenomenon is sometimes referred to as a "Dark DDoS attack" because its true purpose, data exfiltration, remains largely hidden.

It's a variation on "The Takedown" with a whole new class of victim – consumers.

Here are a few examples.

Sony PlayStation | 2011

In one of the biggest breaches of cyber security ever witnessed, hackers mounted a DDoS attack to disguise a more serious assault on Sony's popular PlayStation Network. The Sony attack lasted three weeks and was originally thought to be a straightforward DDoS affair. It turned out to be a diversionary ploy with a loftier ambition – accessing the details of more than 75 million user accounts.

We may never know precisely how Sony's PlayStation Network was hacked, though some security analysts suspect the involvement of the notorious international hactivist group Anonymous. They posit that after discovering a hole in PlayStation Network's security apparatus, Anonymous simply passed the info on to another group of enterprising hackers. Assuming the security hole was big enough, analysts contend that a Structured Query Language (SQL) injection would have enabled this second group of hackers to secure access to the company's customer database.

Other experts point to a custom firmware known as Rebug, which was released the same year as the attack, and gave retail PlayStation 3's much of the same functionality of debug/developer PS3 units. These experts contend that by making PS3's developer network more readily available, a security flaw may have been created that allowed criminals to gain access to the company's database.

TalkTalk | 2015

When hackers flooded the British telecom firm TalkTalk's website with Internet traffic they weren't simply trying to overload the company's digital systems and take it offline. A second attack, aimed at the telecom giant's database, was occurring simultaneously. The company was forced to tell roughly four million customers that personal information such as names, credit card details may have been compromised.

A SQL injection may also have been to blame for the TalkTalk attack, which was perpetrated by two teenagers, a 16-year-old from West London and a 15-year-old from County Antrim. The Information Commissioner's Office (ICO), an independent authority tasked with protecting data privacy for British citizens, suggested the disruption may have been prevented entirely had the company simply bothered to implement basic cybersecurity measures.

Fortunately for TalkTalk, the attack proved less than successful than was first believed, with about four percent of the company's four million customers affected.

Carphone Warehouse | 2017

In June of 2017, Carphone Warehouse, a UK-based mobile phone retailer, was hit by a cyberattack that lasted 15 days and left millions of customers' details exposed. Hackers reportedly swamped the company with junk traffic while simultaneously compromising the personal details of nearly 2.5 million customers, including names, addresses, date of birth, and bank details. Much of this personal data was not encrypted.

A detailed investigation conducted in the aftermath of the attack suggests that intruders exploited a considerably out-of-date WordPress installation to enter the company's system and upload web shells they then used to gain access to basic file management and database functionality. The failure to carry out routine security testing, or to take steps to secure customer data, created multiple vulnerabilities. It also resulted in Carphone Warehouse being assessed a £400,000 fine by the ICO, the largest ever issued by the authority.

Adapting to "the new normal"

With more people conducting more of their lives online, personal data has become the most prized commodity of the digital age. Policing against data breaches resulting from DDoS attacks has become an everyday reality for the modern business world, as Equifax, Yahoo and Marriot have all been reminded in recent months. Nearly 50% of enterprises surveyed in March of 2018 have been on the receiving end of a DDoS attack, an increase over previous reporting periods. The potential payouts are simply too big for the criminals to ignore.

With cyber intrusions becoming the new normal, what can be done to protect your business? Many small and medium-size businesses rely on a firewall solution to handle their DDoS protection needs. Larger enterprise organizations with more complex infrastructures are turning to direct connect services like **Neustar NetProtect**™ to complement their own internal security systems and provide the most robust DDoS protection available.

At the same time many companies are also implementing "honeypot systems" on their internal networks. The objective of the honeypot is to trick the hacker into thinking they have successfully infiltrated a company's system. The honeypot typically offers access to limited or false data, even as it isolates, monitors, and reports the hacker's activity to security personnel. The value of the honeypot system is the information it collects on the cybercriminals, information that can be used to enhance the company's security platform.

For companies that hold consumer information, the biggest risk posed by DDoS attacks may be to their brand. Nobody wants to be known as the company that failed its customers by allowing their personal information to fall into the hands of criminals. Every company is as vulnerable as its own defense system. The fact remains that 80 percent of all cyberattacks could be thwarted if organizations addressed the basics of enterprise cyber hygiene. *Why wasn't the data encrypted?* is often the first question cybersecurity firms ask clients that have suffered costly breaches.

80% of all cyberattacks could be thwarted if organizations addressed the basics of enterprise cyber hygiene.

neustar

Feeling disturbed? Here's a silver lining.

It's worth noting that even as DDoS attacks have become bigger and more sophisticated, cybersecurity firms have become increasingly adept at thwarting them. In March of 2018, a cybersecurity firm successfully defended the platform developer GitHub against a 1.3 Terabit per Second (Tbps) attack. As disturbing as the prospect of a terabit attack may be, it's encouraging to know that the ever-evolving cybersecurity industry proved up to the challenge. After all, it's safe to assume that deterring cyberattacks of every type – from nations, criminals, and, yes, even teenagers – will remain not just a top priority for the business world, but one of the defining issues of our time.

LEARN MORE

If you're interested in learning how Neustar Security can secure your company's online digital presence against risks, visit

www.security.neustar

or give us a call at

1-855-898-0036 (US)

+44 (0) 1784 448 444 (UK).

SS-SEC-156672-03.06.2019