Ordering a DDoS Attack is as Simple as Ordering a Pizza

DDOS ATTACKS ARE NOW COMMONPLACE

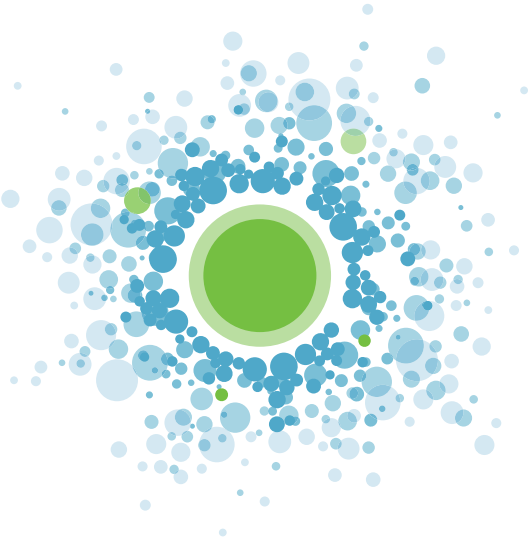
A well-known business received an email demanding two bitcoins (at the time, approximately $130,000), stating, "If you refuse to pay, your site will be subject to a DDoS attack and it will cost 10 bitcoin [approximately $650,000] to stop it. If you think that we are joking, we will soon conduct a demo attack."

The email was noticed, but dismissed as a baseless threat. Unfortunately, it was not a joke— the attack started only a few minutes later, taking the company's servers offline for hours. This cost the company sales, time and money to fix, and severely damaged their reputation by leaving frustrated customers unable to use the company's website.

This was certainly not the first email threat or cyberattack of this kind. In fact, many organizations have received similar Distributed Denial of Service (DDoS) ransom notifications, experienced DDoS attacks, or both. With easy access to "for hire" DDoS attackers, the likelihood of your business experiencing or being affected by a DDoS attack will continue to rise. Mindful businesses would be wise to be aware of the threats, know the vulnerabilities in their own systems, and have ready a plan of response.

Importantly, no business is immune. Even companies who have a significant online existence and devote massive resources to maintaining uptime are subject to these attacks, leading to events like the wide-spread banking attack in 2012, GitHub in 2018, and Google in 2020. Even nations are not immune. In late June, 2022, several official Norwegian governmental websites were hit by what was thought to be pro-Russian actors.[1] Even with professional web security experts on staff, these large organizations still suffered outages. Imagine how much more vulnerable a small business might be to organized cyberattacks.

In general, these attacks are fairly simple to coordinate and launch. There's no special hacking needed, and, ransom money being the exception, there's not necessarily any resulting theft of money or intellectual property. These attacks are essentially a form of espionage, designed to cause chaos by crippling servers. DDoS attacks work by coordinating and sending high volumes of web traffic to a company's server(s) to slow down or disable the server operation.



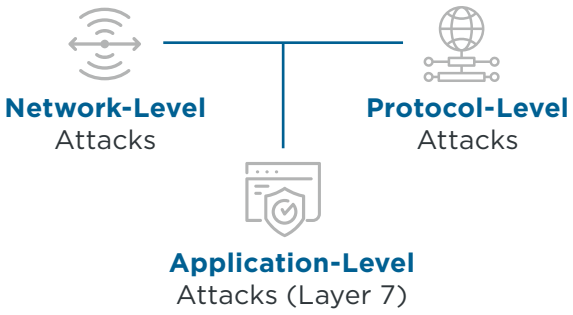
Think of what would happen if **the entire population of greater Chicago** (approximately 12 million people) **descended on a single small-town gas station to ask for directions, all at the same time.** The numbers of requests would overwhelm the attendant, and the local folks (regular web traffic), would be unable to get what they need.

In addition to the immediate operational consequences and loss of business, DDoS attacks negatively impact a corporation's reputation and erode market confidence in the business. Today's consumers have many options, so if one company's website is down, they will simply go elsewhere; therefore, this ultimately outweighs the immediate impacts.

The sheer numbers involved in one of these attacks can be overwhelming. Malicious attackers use bot networks to coordinate their strikes, and they can even rout traffic through different nations, all with the focus to knock out a specific server. In August 2021, a European user of Microsoft Azure became a victim of a massive DDoS attack, which peaked at a traffic rate of 2.4 terabytes (2.4 million megabytes) per second. Experts report that this is the largest attack on Azure in its existence. Even more recently, an attack lasting only 30 seconds saw 212 million requests sent from over 1,500 networks in 121 countries.[2] The scope of these massive, coordinated attacks would be enough to shut down almost any unprepared host.

DDoS attacks can be divided into three broad groups, each with their own characteristics and mitigation techniques.

DDoS attacks can be divided into three broad groups, each with their own characteristics and mitigation techniques.



- **Network-Level Attacks:** These attacks are aimed at saturating an organization's bandwidth.
- **Protocol-Level Attacks:** These attacks focus on hardware limitations or vulnerabilities in various protocols.
- **Application-Level Attacks (Layer 7):** These attacks are aimed at vulnerabilities in applications and operating systems, and they lead to the inoperability of any application or the operating system as a whole.

Bad actors are getting more creative and consistently finding more opportunities for attacks. As internet-connected devices (doorbell cams, connected refrigerators, smart lamps, etc.) become more commonplace, hackers have started using them as a tool for DDoS attacks.

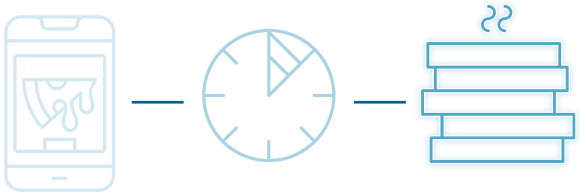
A significant moment came in the September 2016 DDoS attack using the Mirai botnet. In this attack, hundreds of thousands of cameras and other devices from video surveillance systems were exploited and programmed to send coordinated requests to a servers. The successful attack knocked out Twitter, Spotify, Netflix, Amazon, Tumblr, Reddit, PayPal, and other websites.[3] To make matters worse, the code for Mirai botnet was posted online, and has been refined by malicious actors ever since. No one knows when the next exploitation or attack will occur.

While the Mirai botnet used connected cameras, any internet-connected device can be vulnerable, including personal computers and company servers. Sometimes organizations find themselves at the center of these attacks, even though they are not the target. These are known as indirect attacks and can result when vulnerable servers are "taken over" and used as the source of an attack, costing bandwidth, IT services, and other expenses—in addition to the shame of being the unwilling host to cyberwarfare.

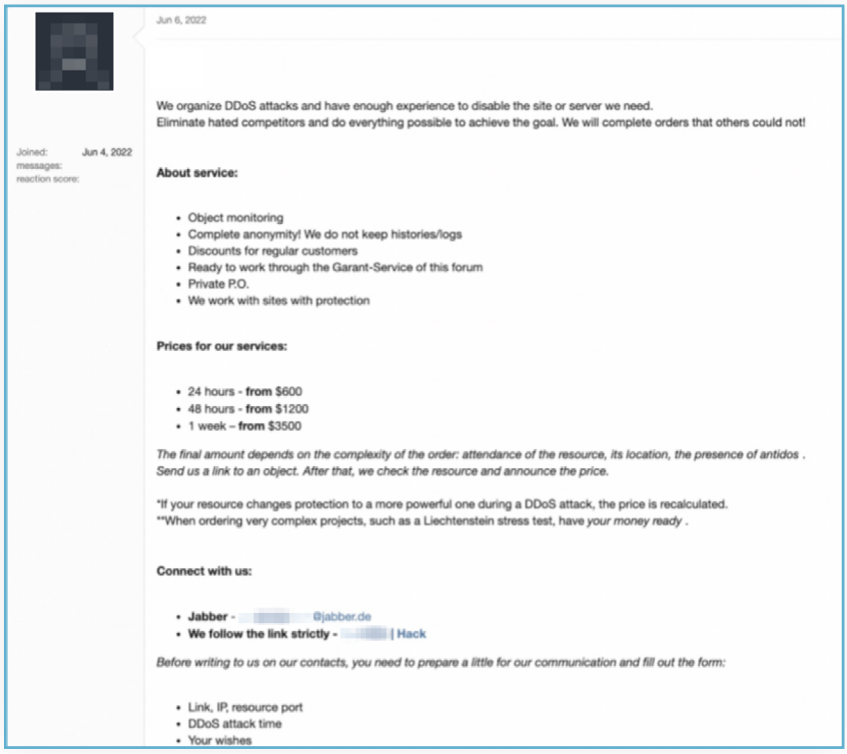
THE NUMBER OF CYBERATTACKS IS CONSTANTLY GROWING

As most businesses know, if there is a value to something, a market will be built around it— cyberattacks are no different. Enterprising internet entrepreneurs harnessed the power of bots and used programs such as Mirai to create a marketplace for ordering such DDoS attacks.

Ordering a cyberattack is now no more difficult than ordering a pizza.



There are hundreds of pages down in the dark web that, for a small fee, offer to "put a website down." For example, a small attack on an unprotected site can be ordered for as low as $10, while "ordering" a day-long attack on a relatively secure organization will cost several hundred dollars. This simplicity and widespread availability is partially to blame for 2021's 29% year-over-year increase in DDoS attacks.[4]


Jun 6, 2022

We organize DDoS attacks and have enough experience to disable the site or server we need.
Eliminate hated competitors and do everything possible to achieve the goal. We will complete orders that others could not!

Joined: Jun 4, 2022
messages:
reaction score:

About service:

- Object monitoring
- Complete anonymity! We do not keep histories/logs
- Discounts for regular customers
- Ready to work through the Garant-Service of this forum
- Private P.O.
- We work with sites with protection

Prices for our services:

- 24 hours - **from** $600
- 48 hours - **from** $1200
- 1 week – **from** $3500

The final amount depends on the complexity of the order: attendance of the resource, its location, the presence of antidos . Send us a link to an object. After that, we check the resource and announce the price.

*If your resource changes protection to a more powerful one during a DDoS attack, the price is recalculated.
**When ordering very complex projects, such as a Liechtenstein stress test, have *your money ready* .

Connect with us:

- **Jabber -** @jabber.de
- **We follow the link strictly -** | Hack

Before writing to us on our contacts, you need to prepare a little for our communication and fill out the form:

- Link, IP, resource port
- DDoS attack time
- Your wishes

Image: SDG Cyber Intelligence Team found Cybercriminal offering DDoS in the Deep Web

Everyone suffers from these threats, from financial institutions and e-commerce businesses to educational institutions to the media and entertainment organizations. The consequences for organizations are clear—they include reputational losses, customer abandonment, and operational disruption, all of which can cause significant income loss.

Whether an organization only receives a sort of "ransom" email, finds themselves the unwilling source of an attack due to a compromised system, or suddenly discovers that millions of requests per second have knocked out their servers and left their customers stranded, it is time to learn more about these attacks and what can be done to minimize their likelihood of hurting businesses.

DEFENDING AGAINST DDOS ATTACKS

Indirect Attacks

To combat these threats, it is necessary to maintain a robust vulnerability management process. For example, many forward-thinking customers use "vulnerability scanning" services which can be used for collecting and analyzing security event logs. This allows security organizations to fully automate the process of finding system weaknesses. In addition, regularly patching software and keeping an active eye on any emerging "0-day" threats remains an effective initial defense.

Extortion or Ransom DDoS Attacks

Sometimes cybercriminals threaten to carry out an attack and demand a ransom. When such threats arrive, the tendency is to ignore them.

There are cases when scammers, using a well-known name of a large hacker group, send a mass mailing to hundreds of addresses with random threats. Some businesses may pay, being frightened of the hacker threat and the possible consequences. This is a classic case of phishing, in which the brands of infamous cybercriminals or ransomware groups are abused.

The rule of thumb for defending extortion attacks is that organizations don't need to make a deal with an attacker to avoid the reputation of an "easy victim." Industry experience demonstrates that such threats have rarely led to the promised serious attack on the infrastructure. In addition, internet security organizations realize that they are all on the same side and share information with their industry partners and colleagues. Collaboration helps prevent extortion.

Direct Attacks

The most common and most newsworthy attacks are the direct ones, where both the publicly hosted applications and also the network connectivity provided by the ISP are targets. This is the

classic DDoS attack that is driven by heavy requests, the processing of which dramatically increases the load on the infrastructure, which causes a drop in application performance and leads to its unstable operation.

Code-level security can act as an embedded defense mechanism; therefore, security considerations must be taken into account when writing the code. It is recommended that organizations follow "safe coding" standards and thoroughly test their applications to avoid common bugs and vulnerabilities such as cross-site scripting and SQL injection.

The most critical infrastructure elements should be behind service providers of DDoS protection services or CDN providers. **Application layer attacks are common on websites and e-commerce portals, and a web application firewall can serve to protect against such attacks.**

CONCLUSION

Remember that the main motive of cybercriminals (in 70% of cases) is either theft of data or the threat of data destruction for the purpose of receiving a ransom payment. Less frequently, the motive may be political or social goals. This is why a defense strategy is important—they can help organizations prepare for attacks and minimize any consequences, reducing financial and reputational risks.

Whatever method of protection against DDoS a company chooses, it is critical to be prepared for attacks in advance. In addition, the IT infrastructure of the organization must fully comply with the volume of the company's business to minimize damage and not lose customer loyalty even in the most active business season.

Next time you place an order for pizza, remember that some bad actor could be placing a similar order for an internet attack. In those instances, you'll want some security professionals watching your back.

We know the internet can be a scary place, full of malicious actors, and looming threats. Fortunately, we know more about security than they do about being malicious, and we're on your side. So, you can order your large pepperoni with confidence.

If your organization would like to learn more about DDoS attacks, or about potential vulnerabilities in your IT systems, give SDG a call. As a a global IT risk management and cybersecurity solutions provider, SDG Managed Security Services and SaaS solutions deliver a comprehensive range of cybersecurity, identity, GRC, and cloud security capabilities that enable organizations to identify and mitigate cyber risk, protect cyber assets, and grow their business securely.

Give us a call or visit our website to learn more about how we can help you brave this internet-driven business world.

ABOUT SDG

With more than 30 years of experience partnering with global enterprises on complex business and IT initiatives, SDG is a trusted provider of advisory, transformation, and managed services. The firm empowers organizations to strengthen cyber resilience by integrating AI into identity, threat, and risk management solutions that protect digital assets and deliver measurable business value. Learn more at www.sdgc.com.

ABOUT THE AUTHOR – SOUMAK ROY

Soumak Roy, Global Cybersecurity Practice Leader at SDG, has more than 20 years of experience in cybersecurity leadership roles with preeminent technology organizations. He is an experienced practitioner in both enterprise and consumer security including Advanced Cyber Defense Strategies, Identity & Access Management, Fraud & Risk Intelligence, Security Operations, and Cyber Intelligence.

RESOURCES

1. https://bdnews24.com/world/2022/06/29/norway-blames-pro-russian-group-for-cyber-attack
2. https://www.digitaltrends.com/computing/hackers-just-launched-the-largest-https-ddos-attack-in-history/
3. https://www.nj.com/news/2017/12/inside_the_massive_cyber_scam_launched_by_a_kid_fr.html
4. https://www.techradar.com/news/ddos-attacks-soared-to-new-highs-in-2021

SDG

Contact Us: solutions@sdgc.com

- 55 North Water Street
  Norwalk, CT 06854
- 203.866.8886
- sdgc.com