DDoS Attacks Are Back. These 10 Steps Can Protect Banks, Governments, and Other Targets

Hacktivists motivated by politics or greed (or both) are using old-school disruption tactics to wreak havoc on finance, governments, and other vital sectors. We asked experts to outline the best evasive strategies to implement before an attack – and after.

Perspective

AUGUST 15, 2024

They're *baaaaack*, and with a vengeance: Distributed denial of services (DDoS) attacks, one of the oldest and simplest forms of cyber assault, are experiencing a startling resurgence, disrupting banks, government institutions, political parties, and other entities more intensely than we've seen in decades.

In recent months, politically or sometimes financially motivated attackers have launched waves of botnets – webs of compromised computers – to overwhelm and knock servers offline, targeting (to name a few) the state of Alabama's websites, the Pennsylvania state court system, Los Angeles and San Francisco international airports, the iRacing.com motorsport simulation company and Final Fantasy 14 game site, Russian bank apps, Czech and Polish banks and stock exchanges, and the French, Swedish, Canadian, and Macau governments.

Whereas most cybersecurity attention has been focused on ransomware because of the often huge payouts involved, lower-profile DDoS attacks are becoming equally concerning due to the serious damage they can cause to operations and reputations. Not coincidentally, the DDoS surge comes at a time of heightened political tension around the world and an ever-increasing public reliance on certain websites, apps, and systems.

Wendy Lowder

Wendy Lowder is a freelance writer based in Southern California. When she's not reporting on hot topics in business and technology, she writes songs about life, love, and growing up country.

Key takeaways

- Back to basics: Hacktivists are leveraging simple, inexpensive DDoS attacks in cyberwarfare.
- Smart prevention plans include robust network monitoring and detection tools to spot suspicious traffic patterns.
- If you're hit, scale up network bandwidth, alert ISPs, document the details, and update incident-response playbooks.

They're *baaaaack*, and with a vengeance: Distributed denial of services (DDoS) attacks, one of the oldest and simplest forms of cyber assault, are experiencing a startling resurgence, disrupting banks, government institutions, political parties, and other entities more intensely than we've seen in decades.

In recent months, politically or sometimes financially motivated attackers have launched waves of botnets – webs of compromised computers – to overwhelm and knock servers offline, targeting (to name a few) the state of Alabama's websites, the Pennsylvania state court system, Los Angeles and San Francisco international airports, the iRacing.com motorsport simulation company and Final Fantasy 14 game site, Russian bank apps, Czech and Polish banks and stock exchanges, and the French, Swedish, Canadian, and Macau governments.

Whereas most cybersecurity attention has been focused on ransomware because of the often huge payouts involved, lower-profile DDoS attacks are becoming equally concerning due to the serious damage they can cause to operations and reputations. Not coincidentally, the DDoS surge comes at a time of heightened political tension around the world and an ever-increasing public reliance on certain websites, apps, and systems.

Accelerate IT ops and security incident response tasks on a single platform—and in real time—before threats spread across your network.

Wendy Lowder

Wendy Lowder is a freelance writer based in Southern California. When she's not reporting on hot topics in business and technology, she writes songs about life, love, and growing up country.

Key takeaways

- Back to basics: Hacktivists are leveraging simple, inexpensive DDoS attacks in cyberwarfare.
- Smart prevention plans include robust network monitoring and detection tools to spot suspicious traffic patterns.
- If you're hit, scale up network bandwidth, alert ISPs, document the details, and update incident-response playbooks.

Banks and other financial institutions are under particular fire, with attacks against them jumping 154% in 2023 compared to the year before, according to a recent report from the Financial Services Information Sharing and Analysis Center (FS-ISAC).

Among attacks targeting governments, Russia-based hacktivist groups like Anonymous Sudan, HackNeT, and the People's Cyber Army have been going after anyone even remotely tied to the conflicts in Ukraine and Gaza.

154%

The rise in DDoS attacks on banks and other finserv groups in 2023 over the previous year

And the net is getting wider: Gaming, telecommunications, and humanitarian organizations are now frequent targets, as various reports have noted; the retail sector has seen a recent uptick; and Paris Olympics officials maintained a heightened alert throughout the games, given previous DDoS attacks on the Olympics in 2016 and 2018.

"DDoS attacks are an effective and inexpensive method of disruption, and hacktivists are increasingly leveraging the method as a tool of cyberwarfare," says Teresa Walsh, FS-ISAC's chief intelligence officer.

The M.O. and motivations behind DDoS attacks

A DDoS attack attempts to disrupt a network's normal traffic by drowning it in internet traffic from numerous sources. It usually does this by infiltrating large numbers of computers and then leveraging that botnet to overwhelm a target with data – much like sending so many missiles toward air defense systems that they ultimately exceed their capabilities.

> **DDoS attacks are an effective and inexpensive method of disruption, and hacktivists are increasingly leveraging the method as a tool of cyberwarfare.**
>
> Teresa Walsh, chief intelligence officer, FS-ISAC

Common motivations for DDoS attacks include wanting to bring down a public-facing website or operation and extortion, where a cybercriminal (much like a mobster) demonstrates the ability to kill a site and says they'll go through with it if the organization doesn't pay a regular protection fee, says Fernando Montenegro, senior principal analyst with Omdia in Toronto. DDoS attacks can also serve as decoys to draw the attention of security personnel while an attacker goes after more lucrative targets, he adds.

The good news is that DDoS attacks are rarely very sophisticated and can be defeated if the proper steps are taken. Case in point: OVHcloud, a French cloud computing company, said it fended off a record 840 Mpps (million packets per second) DDoS attack in April. OVHcloud said the attack failed because the company had enough internet capacity to withstand the digital onslaught coming its way. By comparison, popular media streaming services are thought to handle around 100 Mpps during peak hours when millions of users are viewing videos simultaneously. Social networks might handle about 200 Mpps during peak times when users actively post, like, and share content.

[Read also: Could GenAI's vulnerable code leave us more at risk for DDoS attacks? This security pro has ways to prevent that]

Of course, not every organization can deter the three most common DDoS attacks:

- **Volume-based –** which overwhelm a network's bandwidth with high amounts of traffic.
- **Protocol-based –** which exploit weaknesses in network protocols to consume server resources.
- **Application-layer-based –** which target specific web apps to exhaust those resources.

As such, experts say companies must take a multi-layered approach to prevent and mitigate DDoS attacks.

WHAT TO DO BEFORE A DDoS ATTACK

Prevention is worth a pound of cure. Because attackers typically look for gaps in an organization's security, it's essential to implement best practices for closing those openings as quickly as possible to minimize damage from DDoS attacks. Experts recommend several approaches for accomplishing this, including:

1. Know what's out there

Walsh says organizations must focus on studying and understanding changing attack tactics, techniques, and procedures to defend against them.

840 Mpps

That's the "million packets per second" that a cloud computing firm fended off in a record-busting DDoS attack in April

2. Include DDoS in threat modeling

When designing a system, Montenegro says, it's important to do so with specific potential threats in mind, including DDoS attacks. This underscores the importance of threat modeling, a structured process for identifying, assessing, and

prioritizing potential cybersecurity threats. Enterprise leaders should make sure that this element in the development process is not glossed over or sidestepped.

3. Monitor for suspicious activity

In a joint report, the FBI, Cybersecurity and Infrastructure Security Agency (CISA), and Multi-State Information Sharing and Analysis Center (MS-ISAC) recommend implementing robust network monitoring and intrusion detection tools to identify unusual or suspicious traffic patterns. They also advise regular traffic analysis to catch anomalies.

4. Keep assets and traffic moving

Montenegro says organizations can potentially benefit from moving critical digital assets to hosted cloud servers, like AWS or Snowflake, with ample capacity and security infrastructure to withstand many types of DDoS attack attempts. "The question you should be asking is: Can I have my company's critical infrastructure located in a way that is more resistant to DDoS?" he says. "The best choice in an attack is not to have your assets there to be attacked."

Load balancing solutions can also help, according to the FBI, CISA, and MS-ISAC. Distributing traffic across multiple servers or data centers helps disperse loads, preventing single points of failure during attacks.

[Read also: These 10 cybersecurity frameworks offer structured approaches to reducing cybersecurity risk]

The agencies also suggest that if organizations

Election disruption

DDoS Attacks Pose (Limited) Threat to U.S. Election

¶ In an attempt to put concerns about the integrity of the U.S. election in perspective, the Cybersecurity and

aren't shifting their assets to a cloud provider, they should evaluate their bandwidth capacity and consider increasing it to handle spikes in traffic during an attack.

5. Stay true to the basics

Walsh says maintaining basic cybersecurity hygiene can minimize an organization's exposure to threats. She says the most cost-effective methods involve staying current with all critical security updates, implementing complex password requirements, and embracing multifactor authentication.

Also vital: maintaining state-of-the-art access control practices, which should be part of any identity and access management program. The FBI, CISA, and MS-ISAC suggest Captcha challenges for websites and online services to determine if an authorized human being or an automated bot is seeking network access. Experts say having an active backup and recovery plan, including regular testing, should also be core to every company's cybersecurity strategy.

And don't forget proper endpoint management. Remove any unused endpoint devices from a network, limit admin access to existing devices, and restrict software to small groups of authorized users, Walsh urges.

Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) jointly released a new public service announcement last month advising that DDoS attacks may hinder access to election information but won't impact the overall security of election processes.
¶ "DDoS attacks against election-related websites could temporarily disrupt access to some online election functions, like voter look-up tools, but would not prevent voting or compromise the integrity of voting systems," said FBI deputy assistant director Cynthia Kaiser.

WHAT TO DO AFTER A DDoS ATTACK

If an organization suddenly experiences problems with unavailable web services, increased network congestion, unusual traffic patterns, or unexplained server or application crashes, it might be under a DDoS attack.

> **The question you should be asking is: Can I have my company's critical infrastructure located in a way that is more resistant to DDoS?**
>
> Fernando Montenegro, senior principal analyst, Omdia

Experts recommend taking a few steps in those situations, including:

6. Confirm the attack

Use network monitoring and traffic analysis tools to determine the nature of the attack. If DDoS is the culprit, immediately activate the organization's documented and approved incident response plan. Presumably this exists; if not, get one. (New next-generation autonomous incident response plans can accelerate remediation and response times.)

7. Scale up bandwidth

The FBI, CISA, and MS-ISAC recommend scaling up the organization's network bandwidth if possible to help absorb the brunt of the attack. This could involve adding servers or temporarily increasing network capacity.

8. Notify whoever needs to know

The agencies recommend immediately alerting internet service providers (ISPs) to the attack and seeing if they have mitigation measures for rerouting traffic to help moderate the attack. If you're carrying cyber insurance, also connect with the carrier to possibly get their help and inquire about what they will or will not cover to soften the blow.

9. Capture and compare notes

Document and collect as much information as possible about the attack, including timestamps, IP addresses, packet captures, and any logs or alerts, the FBI, CISA, and MS-ISAC say. This can be useful when reporting the incident to law enforcement officials. Also, consider sharing identified vulnerability and intelligence with industry peers to help others guard against potential DDoS attacks, Walsh says. "Sharing intelligence across the sector is critical to helping organizations build their incident response playbooks," she adds.

[Read also: "Sharing intelligence" is what the SEC has in mind but its slew of new regs has finserv leaders wary – we lay out the new rules]

10. Learn from the attack

Because every moment can be a learning moment, Walsh counsels business continuity teams to conduct regular exercises based on previous DDoS attacks to "build an organization's muscle memory" and decrease future incident response times.

The FBI, CISA, and MS-ISAC say such exercises should include a thorough post-incident analysis to understand the attack vectors used and the vulnerabilities exposed. They advise that incident response plans be updated based on these findings.

As cyber threats keep evolving, organizations must step up their defenses. The recent surge in DDoS attacks underscores the need to stay vigilant and proactive. Companies can better protect their digital assets from these relentless attacks by following best practices, staying informed about new threats, and continually improving security measures.

Related

What Return-to-Office (RTO) Means for Your Cybersecurity

I Almost Fell for This Online Scam. Why Even Tech Pros Can Be Taken

How AI Is Redefining Data Loss Prevention (DLP)