CONTROL ENGINEERING

Why DDoS attacks are a major threat to industrial control systems

Distributed denial of service (DDoS) attacks can cause severe damage to an industrial control system (ICS) in the short- and long-term and have lasting impacts on the company affected.

BY DR. JAMES STANGER JUNE 24, 2021

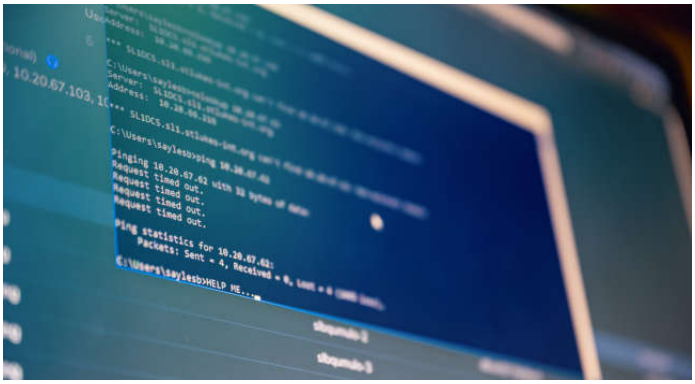

Image courtesy: Brett Sayles

A distributed denial of service (DDoS) attack is a malicious attempt to sabotage a network by overwhelming its ability to process legitimate traffic and requests. In turn, this activity denies the victim of a service, while causing downtime and costly setbacks. A DDoS attack is a network-based attack; it exploits network-based internet services like routers, domain name service (DNS) and network time protocol (NTP), and is aimed at

disrupting network devices that connect your organization to the internet. Such devices include routers (traditional WAN, as well as ISP edge routers), load balancers and firewalls.

There is quite a bit of confusion among information technology (IT) professionals about the difference between a DDoS attack and a standard denial of service (DoS) attack. A DDoS attack differs from a standard DoS attack in two specific ways.

1. A standard DoS attack directly attacks a particular resource, such as a web server, email server or industrial control system (ICS) device. A DDoS attack targets the devices that provide access and connectivity to the servers and services on a network.
2. Another difference between DoS and DDoS attacks lies in the first "D," which stands for distributed. That means the former comes from a single source, whereas the latter comes from a huge network of devices, which we call a botnet. The use of reflection, spoofing and distribution often makes thwarting DDoS attacks very difficult.

It is common for even experienced IT pros to think the majority of DDoS attacks involve using large amounts of traffic. This is not the case. More than 99% of successful attacks use a very small number of malicious packets. Large-volume attacks (sometimes called volumetric) often gain attention because it is easy to explain how a massive amount of traffic has overwhelmed network resources.

Attack motives

DDoS attack perpetrators have many motives. They can be politically or financially motivated. Nation-states have been known to conduct DDoS attacks as part of efforts to disrupt communications during military campaigns or as part of efforts to cause chaos worldwide. Some

part of efforts to cause chaos worldwide. Some actors have no particular motivation at all. In any case, an attacker will deny the victim access to their servers, disable physical network equipment or simply wreak havoc.

While no one is completely safe from DDoS attacks, critical infrastructures and centralized control systems are the most vulnerable. These industries should be the ones paying the most attention to DDoS attacks and investing the most in their cyber protection.

ICSs are vulnerable to DDoS attacks

ICSs are an integral part of our lives today. They allow for easier management of our most critical infrastructures and processes. Manufacturing, gas, water, power distribution and transportation all depend on ICSs to keep their processes running on a daily basis.

What's more, the emergence of the Industrial Internet of Things (IIoT) allowed users to automate some tasks in the process. We can now control everything simultaneously from a remote location. Of course, that improved workflow efficiency big time, helping us reach never-before-seen speed and accuracy.

ICSs also have many cybersecurity issues. From weak passwords in internet of things (IoT) devices and open-source software, to using commercial communication protocols — ICSs have more than a few DDoS vulnerabilities. With so much operational equipment and so many ICS layers to audit, malware can easily sneak by manufacturers without getting noticed. That's frightening, considering how much we depend on these systems and what's at stake.

Anyone can execute a DDoS attack

In 2020, DDoS attacks were on the rise, partly

In 2020, DDoS attacks were on the rise, partly due to the COVID-19 pandemic, which forced many sectors into digitalization. Unsurprisingly, hackers took this as an opportunity to cause disruption and earn some money on the side.

State-sponsored actors saw 2020 as an opportunity to disrupt business worldwide.

As devastating as they can be for the target, DDoS attacks can be relatively easy to execute.

With the emergence of booters/stressers, also known as botnets for hire, even those without any programming knowledge can carry out a successful DDoS attack. Many attackers are also enlisting long-existing botnets to help with DDoS attacks.

DDoS attacks are costly for the target

DDoS attacks are expensive for the victim, causing economic and reputational losses. According to Kaspersky's 2017 report, the average cost of a DDoS attack for enterprises was around $2 million. However, years have passed and attacks have evolved and are now even more devastating. It's fair to say this figure would be much higher today.

Cost isn't the only loss. Some things simply can't be measured, such as brand reputation damage and loss of trust with clients and customers, among many other intangible effects.

Aside from the resulting downtime and legal fees, a DDoS attack can be costly in many other ways, especially for ICSs. The energy, manufacturing and health care sectors, for example, are being increasingly targeted. An attack can stop all production and deny vital services and resources to millions of people. And shutting down crucial processes and equipment could potentially cause major, even fatal, incidents.

DDoS attacks are becoming

DDoS attacks are becoming more sophisticated

Recent technological advances have brought about efficiency in every possible way. Many

people possess or benefit from multiple IoT devices, from everyday personalized gadgets and appliances to complex machines and robots that can build entire structures. However, as technology evolves, so do DDoS attacks.

DDoS attacks are expected to become even more devastating as they deny network connectivity to our smart devices, rendering them useless. DDoS threat actors threaten to exploit various emerging — and emerged — technologies.

First of all, 5G and Wi-Fi 6 have made connection and communication between devices faster and smoother than ever. Of course, DDoS attackers took advantage of that, expanding their botnets at incredible rates.

Artificial intelligence (AI) has found its way into the hackers' arsenal, as well. Today, they can automatically find, breach and hijack devices for their botnets. That's how Mirai, history's most notorious botnet, is one of the biggest cyber threats to this day.

DDoS attack tactics are also changing with time. Recently, hackers have been modifying their use of longstanding DNS amplification techniques. In short, this method allows them to magnify small queries and turn them into large traffic-hogging responses.

What users can do to prevent DDoS attacks

Examples like Stuxnet, a computer worm that managed to shut down many of Iran's industrial facilities, and the Ukrainian power grid attacks highlight the importance of investing in cyber protection.

We must build better defenses — address the

We must build better defenses — address the security concerns surrounding IoT devices, implement multilayer security solutions and closely monitor every single activity in the ICS. After all, not doing so could compromise our critical infrastructures.

On the bright side, we already have what it takes to effectively fight DDoS attacks. All in all, the best way to fight a DDoS attack is to prevent it. That often involves using scrubbing services, increasing available bandwidth during attacks and using a content delivery network (CDN).

It's important to have a detailed response plan in order to quickly stop attacks and mitigate the consequences as much as possible.

Dr. James Stanger, chief technology evangelist, CompTIA. Edited by Chris Vavra, web content manager, *Control Engineering*, CFE Media and Technology, cvavra@cfemedia.com.

Do you have experience and expertise with the topics mentioned in this content? You should consider contributing to our CFE Media editorial team and getting the recognition you and your company deserve. Click here to start this process.

Related Articles

- *DDoS attacks on rise due to COVID-19*
- *Fighting advanced DDoS attacks*

Dr. James Stanger

Author Bio: As CompTIA's Chief Technology Evangelist, Dr. James Stanger has worked with Information Technology (IT) subject matter experts, hiring managers, CIOs and CISOs worldwide. He has a rich 25-year history in the IT space, working in roles such as security consultant, network engineer, Linux administrator,

web and database developer and certification program designer. He has consulted with organizations including Northrop Grumman, the U.S. Department of Defense, the University of Cambridge and Amazon AWS. James is a regular contributor to technical journals, including Admin Magazine, RSA and Linux Magazine. He lives and plays near the Puget Sound in Washington in the United States.

RELATED CONTENT

Cloud and the Component SDK

IXON CLOUD B.V.

Securing the edge in a manufacturing facility

CHRIS VAVRA

Top 5 Control Engineering content: August 22-28, 2022

MORGAN GREEN

Cybersecurity advice for industrial networks

JIM MANSFIELD, DAN MCKARNS AND DAVID SCHULTZ

Nine reasons why ICS/OT infrastructure is insecure

RITESH SRIVASTAVA

How cross-domain solutions can protect OT from IT-level attacks

LARRY O'BRIEN

Black-channel approach to functional safety

ROBERT TRASK, PE

TRENDING TOPICS

Control Systems

Control Systems

IIoT, Industrie 4.0

Discrete Manufacturing

Info Management

Networking and Security

Process Manufacturing

System Integration

Workforce Development

3010 Highland Parkway Suite 310
Downers Grove, IL 60515
(630) 571-4070