NETSCOUT®

| WHITE PAPER |

# The Weakest Link

## Attackers Target Connectivity Supply Chain To Disable Enterprise Internet Connectivity

SECURITY

## TABLE OF CONTENTS

## Internet Connectivity Supply Chain is Under Attack

Cars, microchips, steel, lumber—we're all familiar with the growing list of products in short supply as a result of massive disruptions to the traditional global supply chain caused by COVID-19. But the pandemic also has served as a gateway to increased attacks against another supply chain—one that undergirds not only the traditional supply chain but also every enterprise around the world: the connectivity supply chain.

Simply stated, the connectivity supply chain is made up of all of the technologies and services that make it possible for companies and individuals to stay connected to the internet. It not only facilitates services to all interconnected devices—think enterprise Internet of Things (IoT), computers, and mobile phones—but also supports connectivity as enterprises increasingly embrace digital transformation and move resources to the cloud.

During the pandemic, cybercriminals focused increased attention on attacking technologies that enable things such as cloud computing to function over the internet—especially Domain Name System (DNS) servers, virtual private networks (VPNs), and internet exchanges. These attacks have become so invasive that in March 2021, the U.S. Government Accountability Office (GAO) implored federal agencies to strengthen their cybersecurity and information and communications technology (ICT) management efforts. In particular, the GAO noted that few of the 23 federal agencies it reviewed had implemented foundational practices for managing ICT supply chain risks.

To better understand and protect the connectivity supply chain, enterprises should understand the types of attacks that are occurring, as well as how to best protect their resources and ensure uninterrupted connectivity.

*Addressing cybersecurity challenges is important because threats to IT systems and networks supporting the federal government and the nation's critical infrastructure are increasing. These systems and networks are often interconnected with other internal and external systems and networks, including the internet. With this greater connectivity, threat actors are increasingly willing and capable of conducting a cyberattack on our nation's critical infrastructure and federal agencies' IT systems that could be disruptive and destructive.*

– GAO 21-105325, Federal Agencies Need to Strengthen Efforts to Address High-Risk Areas

## Weak Link 1: DNS Servers

**Attack count: ~4,000**

**Primary vectors: DNS and DNS reflection/amplification**

The DNS is a database that stores internet domain names and translates them into IP addresses. During the first half of 2021, there were more than 4,000 attacks against DNS servers, primarily in the form of DNS reflection/amplification and DNS "water torture" distributed denial-of-service (DDoS) attacks.

This User Datagram Protocol (UDP) reflection/amplification attack typically uses abusable, misconfigured open DNS recursors in conjunction with authoritative DNS servers to consume link bandwidth and block the ability of targeted systems to respond to network traffic. A small proportion of DNS reflection/amplification attacks leverage only authoritative DNS servers. Most DNS reflectors/amplifiers are home broadband access routers running open DNS forwarders on their public internet interfaces.

DNS reflection/amplification DDoS attacks pose serious threats to enterprise servers. When massive amounts of traffic are pushed into the victim server, the attack traffic devours server and network resources, significantly slowing systems and preventing real traffic from accessing the enterprise server.

This means that any website serviced by the attacked DNS server will have connection and timeout issues, and users won't be able to get to the services that they want.

## Weak Link 2: Commercial VPNs

**Attack count: ~41,000**

**Max attack bandwidth: 307 Gbps**

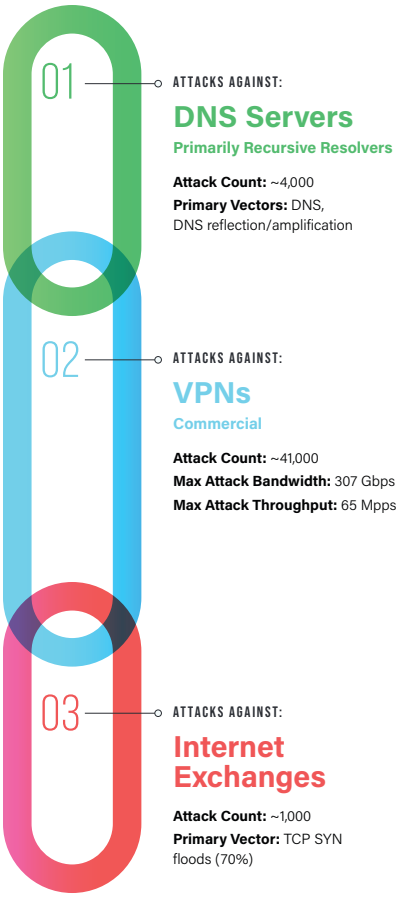
**Max throughput: 65 Mpps**

It's important to point out that the bulk of the attacks shown here are against commercial VPNs, primarily those used by gamers and other non-enterprise users to hide their source or access things they otherwise would not be able to access.

There's no question, however, that attacks against corporate VPNs have increased as well. Traditionally, enterprises haven't made constant use of VPNs. But the pandemic changed that significantly, because companies had to rely on them to support home-based workers during lockdowns. Moreover, as new variants of the virus proliferate and employees increasingly demand work-from-home (WFH) options from companies, reliance on VPNs continues.

Cybercriminals, meanwhile, recognize that enterprises are more exposed and are targets for extortion when employees are working remotely and weathering a pandemic. That's all the motivation they need to launch targeted attacks, which can crash servers and burden systems of any size. A DDoS attack can impact performance or bring down a VPN gateway. Such is the case with the Lazarus Bear Armada (LBA) DDoS extortion campaign, through which the attacker launches a small DDoS attack alongside an extortion note that threatens a larger and more sophisticated attack in the future unless a ransom is paid.

Such attacks often target corporate VPNs to disconnect users from the online assets of an enterprise or to prevent security teams from responding to attacks. Because commercial VPNs make the list of VPN exit nodes public, it doesn't take much work for adversaries to find a slew of potential targets. In many cases, attackers perform some network reconnaissance to figure out the IP addresses or hostnames a company uses for VPN, and they target those. From there, they can also mine those nodes for individual IP addresses, creating an even larger target for attack.




Data courtesy of Neustar UltraGeoPoint data

## Weak Link 3: Internet Service Providers (ISPs) / Internet Exchange Points (IXPs)

**Attack count: ~1,000**

**Primary vector: 70% TCP SYN floods**

Internet Service Providers (ISPs) / Internet Exchange Points (IXPs) increasingly are being targeted with TCP SYN flood attacks—DDoS attacks in which the attacker floods the system with SYN requests to overwhelm the target and make it unable to respond to new real connection requests. The purpose of a SYN flood DDoS attack is to exhaust system resources such that the attack fills up a state table or results in so much network saturation that it greatly diminishes connectivity or takes down the targeted system. SYN floods are often called "half open" attacks because they are used to send a short burst of SYN messages, leaving connections open, which often results in a complete server crash.

As the impact of such attacks on enterprises, governments, and other entities grows, DDoS attacks against ISPs/IXPs are generating increasing media attention:

- In May 2021, Belgian ISP Belnet was hit by a DDoS attack that caused disruption to the services of more than 200 organizations, including government, parliamentary, healthcare, and academic institutions. Belnet is a government-funded ISP that provides internet services to government, educational, research, and scientific institutions, as well as a number of other organizations across the country. As a result of the attack, a number of scheduled meetings of the Belgian Parliament and other virtual events were disabled, and remote learning for some Belgian academic institutions was disrupted by connectivity stability issues.
- Also in May 2021, numerous Irish ISP networks were intermittently targeted with DDoS attacks over the course of several days. Some of the ISPs received extortion messages demanding bitcoin payments. The attacks occurred at the same time that the country's health service computer systems were attacked by ransomware.
- In August 2020, a DDoS attack against Spark, New Zealand's largest ISP, resulted in the New Zealand Stock Exchange (NZX) being taken offline for four days.
- In September 2020, more than a dozen European ISPs in Belgium, France, and the Netherlands were hit by DDoS attacks. The attacks were launched against DNS infrastructure of ISPs in Benelux, a union made up of Belgium, the Netherlands, and Luxembourg.

## Weak Link 4: Vertical Applications and the Gaming Industry

When attacks are targeted against the connectivity supply chain, they almost always target vertical applications. In many cases, such attacks start with vertical applications and spread to the supply chain. Such is the case in the gaming industry.

Online gaming has always been a significant target for DDoS attacks. Unfortunately, however, such DDoS attacks often end up affecting large swathes of an ISP's adjacent customer base along with the target. For large broadband operators, the collateral damage can involve internet outages that affect thousands of users.

Now, however, attackers are using solutions that allow them to pinpoint attacks by mapping players' online user names to IP addresses. Doing so enables attackers to launch DDoS attacks that knock gamers out of gaming sessions, disrupt their internet connectivity, and often cause collateral impact to uninvolved customers of the associated ISP.

Some of these tools are linked into associated online databases that store gamer info and their associated IP addresses. Attackers use the information to prevent gamers from playing online, while also disrupting their household internet access for extended periods of time. These same services also sell "delisting services" to gamers with no guarantee of success, as well as paid VPN services that they claim will shield gamers from DDoS attacks by hiding IP addresses. In reality, attackers can apply the same tools to find VPN-supplied IP addresses, rendering such VPN services completely useless.

**Why Is NETSCOUT Seeing So Many More DDoS Attacks?**

It doesn't take much research to realize that NETSCOUT® is reporting much higher rates of DDoS attacks than other firms that track cyberattacks. And it's important to understand why the disparity exists.

To understand—and ultimately stop—attacks to the connectivity supply chain, you must be able to see them first. NETSCOUT partners with almost every ISP around the world, enabling us to see attacks that occur on their networks, as well as on their customers' networks. Because such attacks traverse a network into which we have visibility, we have a wide spectrum of visibility that isn't available to companies that only track attacks on enterprise networks.

In the first half of 2021, NETSCOUT identified almost 5.4 million attacks. To ensure the accuracy of that number, we took random samplings of attacks occurring against IP addresses on the internet—a quality control measure made possible only because of our relationships with global ISPs. This visibility into the connectivity supply chain is unique and underpins NETSCOUT's goal of identifying and protecting against all of the ways in which adversaries attempt to attack connectivity.

## How to Protect the Connectivity Supply Chain

Network Operators can take several actions to protect the connectivity supply chain against DDoS attacks, including the following:

- Organizations with business-critical public-facing internet properties should implement industry best current practices (BCPs), including situationally specific network access policies that permit internet traffic only via required IP protocols and ports.
- Implement situationally appropriate DDoS defenses for all public-facing internet properties and supporting infrastructure, including regular testing to ensure that any changes to servers, services, and applications are incorporated into the DDoS defense plan. Combine organic, on-site intelligent DDoS mitigation capabilities with cloud- or transit-based upstream DDoS mitigation services to ensure maximal responsiveness and flexibility during an attack.
- To optimize DDoS protection, organizations that operate mission-critical, public-facing internet properties or infrastructure should include all servers, services, application, datastores, and infrastructure elements in recurring, realistic tests of the DDoS mitigation plan. It's important to ensure that authoritative DNS servers, application servers, and other critical service delivery elements are protected against attack.
- Customize the specifics of countermeasure selection, tuning, and deployment based on the particulars of individual networks and resources.

## LEARN MORE

To learn more about protecting the connectivity supply chain against DDoS attacks, contact us today.

NETSCOUT

**Corporate Headquarters**
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

**Sales Information**
Toll Free US: 800-309-4804
(International numbers below)

**Product Support**
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us



SECWP_021_EN-2101 10/2021