# Cybercriminals Target Company Values with DDoS Attack

*IPXO experienced a massive DDoS attack, believed to have been caused by dissatisfied customers who were banned from the platform due to abusive behavior.*

DDoS attack was launched against company values that do not support malicious behavior

LONDON, UK, April 14, 2023 /EINPresswire.com/ -- Yesterday, the all-in-one Internet Protocol platform IPXO experienced the biggest cyber-attack, believed to have been caused by dissatisfied customers who were banned from the platform due to abusive behavior.

The first wave of Distributed Denial-of-Service (DDoS) attacks began on Wednesday with the second wave taking place Thursday night reaching traffic increase towards IPXO website by 1000 times at peak time.

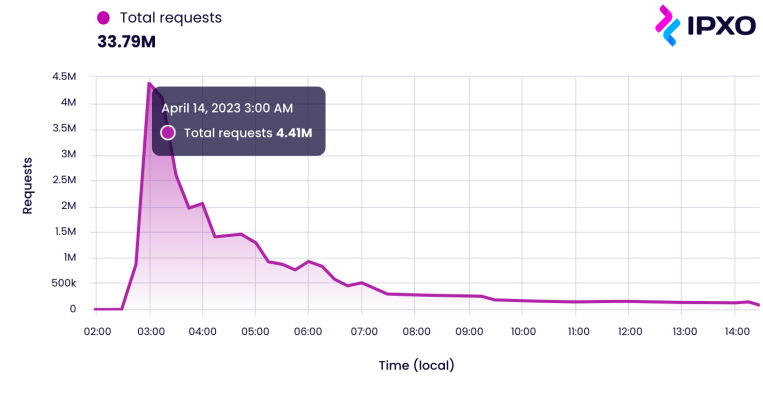
> Even with maximum security measures in place, IP abuse can still occur and preventing it may come at a cost to revenue. Yet, the willingness to keep fighting to create a safer internet remains crucial”
> *Vaidotas Januska, CTO of IPXO*

During the attack, over 30 million abnormal requests were sent to the website peaking at 4.4 million within a 15-minute window. Fortunately, the Platform Engineering team was quick to react by analyzing the first wave and making necessary adjustments to existing policies in place. While these types of attacks are not uncommon, this was the first time the company had experienced an attack on such a massive scale.

ZERO TOLERANCE POLICY AGAINST ABUSERS

Strict policies are necessary to ensure the overall safety of the marketplace. Some time ago, the company's Operations team noticed abusive behavior patterns among lessees who were using leased IPv4 addresses for spam, malware, and phishing.

“Despite our attempts to discuss and understand the observed abusive patterns, we received no response and saw no improvement in the lessees' behavior. This ultimately led us to make the strict decision to ban the abusers from using our services,” explains Andrius Kleinas, COO of IPXO.



The DDoS attack was held on Thursday night when over 30 million requests were sent to IPXO website peaking at 4.4 million within a 15-minute window

The team took extra precautions to stop such activities by eliminating dozens of bad actors and related accounts from the platform.

“It is possible that banned lessees were resentful and launched a DDoS attack as an act of revenge. The first attack took place only an hour after the ban was implemented,” says Vaidotas Januska, CTO of IPXO.

As per its Terms of Service, IPXO has the right to ban malicious actors and immediately terminate services if they are intentionally and deliberately used to cause damage to any property in any shape or form.

## THE IMPORTANCE OF ABUSE OBSERVABILITY

The malicious activity undertaken by IP lessees harms not only their own reputation but also that of the IP addresses they are using. Lessees who engage in malicious activity on the platform adversely affect the reputation of thousands of IPs. This is why abusive actions cannot be tolerated.

IP reputation is a critical aspect of managing valuable IPv4 addresses. Therefore, IPXO takes responsibility for monitoring its platform to ensure that only clients who have successfully passed several levels of business verification and Know Your Client (KYC) processes can access its resources.

To maintain a good IP reputation, IPXO regularly checks blacklists and promptly responds to any incidents of abuse by blocking them.

By proactively preventing such activities, IPXO ensures that its IP resources are used only for legitimate purposes. This contributes to maintaining the overall trust and reliability of the Internet.

THE MOST POPULAR TYPES OF IP ABUSE

According to data gathered by IPXO's Abuse Prevention team, DDoS is one of the most common types of IP abuse, that occurs as deliberate attacks to overload servers or web services by flooding them with heavy traffic from multiple sources.

Other forms of IP abuse include:

- Phishing/Fraud: An unlawful act to acquire sensitive information like passwords and credit card details
- Spam: Unwanted emails ranging from harmless to unlawful
- Malware: Malicious software, including viruses, Trojans, and ransomware that intentionally causes harm

IP address abuse can take on various forms, each requiring distinct strategies and measures to combat. Unfortunately, any type of IP abuse can leave a lasting impact on IP reputation, which can in turn disrupt companies that offer hosting, marketing, and cybersecurity services.

“Even with maximum security measures in place, IP abuse can still occur and preventing it may come at a cost to revenue. Nevertheless, the willingness to continue fighting to create a safer internet remains crucial,” believes Januska.

Given these challenges, it is vital to have a trustworthy and responsive IPv4 lease provider that can not only ensure the IP resources remain of good reputation but can also protect itself against the cyber-attacks that such values may provoke.

ABOUT IPXO:
IPXO is an all-in-one Internet Protocol platform designed to address global IPv4 exhaustion by enabling companies in over 75 industries to lease and monetize IPv4 resources. The company aims to create a more secure and sustainable Internet Protocol ecosystem and set a new standard for efficient IP management with business-grade solutions. For more information, visit www.ipxo.com.

Agne Srebaliute
IPXO LLC
email us here
Visit us on social media:
LinkedIn
Twitter
YouTube

try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.