MITIGATING AND PREVENTING IP ADDRESS ABUSE IN THE IP LEASE MARKET

An analysis of the direct impact of abuse on the IPv4 address lease and monetization market and an overview of mechanisms that help ensure professional IP address abuse mitigation and prevention.

IPXO WHITE PAPER

May 2022

TABLE OF CONTENTS

SUMMARY

IP addresses are the foundation of the internet we know today. They enable internet-connected devices to communicate with one another in a smooth and efficient way. However, when the concept of IPs was first developed, the security of IP addresses was not considered thoroughly. As a result, IP address abuse is rampant today.

The consequences that the holders of abused IP addresses face range from temporarily disrupted services to loss of reputation. This is especially problematic for IP holders who wish to monetize assets by selling or leasing them because abused IPs may be harder to sell and lease.

In the IPv4 lease market, IP holders need to think not only about the reputation of the IPs they put up for lease but also about how potential lessees may treat the resources. Although IP address abuse cannot be contained in 100% of cases, it is crucial to choose a lease platform that can implement professional abuse mitigation and prevention tactics.

Professional IP address mitigation is supported by numerous mechanisms that help handle abuse incidents automatically. These mechanisms can both minimize the damage of abuse incidents and prevent such incidents from occurring in the first place.

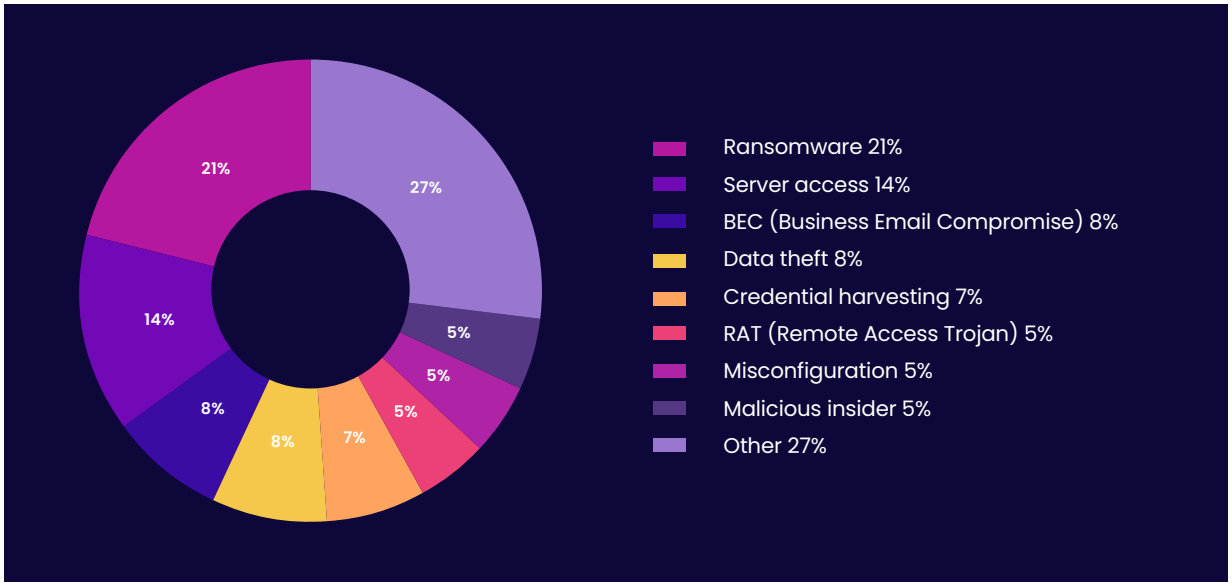
INTERNET ABUSE: FROM FIRST WORMS TO RANSOMWARE

1988 marks the birth of the cyberattack, a malicious act performed with the purpose of disrupting the ordinary digital life. Although the first major cyberattack was just an experiment conducted by a curious university student, not long after, cyberthreats became more malicious and, most importantly, more common.

Nowadays, multiple cyberattacks occur in the time it takes an average human to finish a cup of morning coffee. According to a SonicWall report, 20 ransomware attack attempts occur every second.[1]

The X-Force Threat Intelligence Index 2022 reveals that ransomware is the most common type of cyberthreat, and it was involved in 21%[2] of all cyberattacks observed by X-Force in 2021. While ransomware is one of the most destructive forms of malware, it certainly is not the only cyberthreat.

THE MOST COMMON CYBERATTACKS IN 2021



Breakdown of top attack types, 2020-2021 (data by IBM Security X-Force)

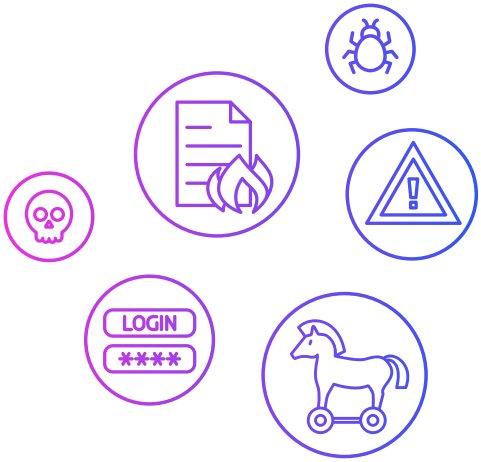
Cloudflare has also been observing a substantial rise in ransom DDoS attacks, during which attackers extort money from targeted organizations. The web performance and security company conducted a survey, which revealed that one in three organizations have received ransom demands specifically associated with DDoS attacks[3].

Although direct financial gain appears to be the most sought-after reward for cybercriminals, they can profit from data as well. The common pursuits include:

- Identifiable information
- Private financial information
- Commercial financial information
- Intellectual property
- Sensitive information

That said, not all malicious agents attack to gain something. Other motives for criminal activity include **cyberterrorism, cyberespionage, destruction of data, hacktivism** or even **revenge.**

The shift from first experimental worms to major cyberterrorist attacks has been gradual, and as the internet and technologies advanced so did cyberattacks. To understand the evolution of network security better, we can glance at some of the major events that occurred between 1969-2022.



MOST MOMENTOUS EVENTS IN THE HISTORY OF NETWORK SECURITY

1969

ARPANET, the first computer network, is launched

1971

Bob Thomas writes the first worm, a self-replicating program, called Creeper

1972

Ray Tomlinson launches the first antivirus program – Reaper – to contain Creeper

1986

Fred Cohen coins the term virus to define a program that can infect other programs

1988

Robert T. Morris builds the Morris worm and performs the first major cyberattack

1988

Computer Emergency Response Team (CERT) emerges to educate the internet community on security protocols and malware prevention and mitigation techniques

1989

Joseph L. Popp creates the first ransomware, the AIDS Trojan

1990

Markus Hess is convicted of the first case of cyberespionage performed in 1986-1987

1991

Robert T. Morris is the first person to be convicted under the Computer Fraud and Abuse Act of 1986 for the Morris worm attacks in 1988

1991

Digital Equipment Corporation releases the first commercial firewall named DEC SEAL

2003

US Department of Homeland Security establishes the National Cyber Security Division

2013–2016

Yahoo experiences the biggest data breach that exposes 3 billion user accounts

A BRIEF HISTORY OF THE INTERNET

If January 1, 1983 is the birth of the internet[4], we will be marking its 40th anniversary next year. During the inception of the internet, no one could have foreseen that a small network would eventually turn into an enormous web of over 29 billion connected devices.[5]

The history of the internet starts with the ARPANET connectivity network. It was developed by the Pentagon's Advanced Research Projects Agency (ARPA) in 1969 to allow researchers to share data and access remote computers. In 1965, ARPANET introduced email, which turned the internet into a virtual, high-speed post office.

In 1974, a team of scientists, with Bob Kahn and Vinton Cerf at the forefront, created a Department of Defense (DoD) model, now known as the TCP/IP suite or the Internet Protocol suite. The DoD model consolidated the previously loose collection of networks into one, creating the basis for the internet we know today.

On January 1, 1983, ARPANET officially began transitioning to the open networking protocols TCP (Transmission Control Protocol) and IP (Internet Protocol).

During the 80s, the internet flourished as companies and individuals invested in personal computers and started communicating digitally.

In 1989, Tim Berners-Lee started developing the World Wide Web along with his colleagues at CERN (Organisation européenne pour la recherche nucléaire). Eventually, the invention allowed individuals to exchange data on the internet in a simple and easy-to-use manner.

THE FIRST COMPUTER WORM

In the early 1940s, the government and a handful of research labs and universities, including some commercial businesses, began using mainframes. These computers were designed to perform complex mathematical calculations faster than any human ever could. Since the internet did not yet exist, only physical measures were taken to protect the computers.

As technology advanced, the demand for data sharing between computers increased. The first person to test the vulnerabilities of ARPANET was Bob Thomas. Thomas hypothesized that a computer program could move across the network. To test the theory, he created a self-replicating program in 1971.

The program named Creeper could travel on the ARPANET, printing the message

```
I'M THE CREEPER:
CATCH ME IF YOU CAN.
```

While Creeper was relatively harmless, it is considered the first computer worm ever created.

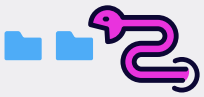
The worm prompted another researcher, Ray Tomlinson, to create a program named Reaper to find the copies of Thomas' program and delete them. Some consider this to be the first antivirus software.

Back in the early 70s, the internet community viewed Creeper and Reaper programs as harmless experiments demonstrating the capabilities of the ARPANET network. However, these experiments revealed that networks can be vulnerable, paving a path to countless cyberattacks in the future.

THE FIRST MAJOR CYBERATTACK

In 1988, a 23-year-old Harvard graduate Robert Morris launched the first major cyberattack. Morris had a seemingly innocent motive – to estimate how many computers are logged into the network. He created a program that traveled from one computer to another, making each of them send a signal back to the control server to keep the count.

Once launched, the program spread across a relatively small network like lightning. Now known as the Morris worm, the program infected around 6,000 computers. While it did not damage the devices or delete any data, it slowed the machines to a halt, making them inoperable.



This attack was similar to a modern-day distributed denial-of-service (DDoS) attack that swarms a network with a series of requests until the service ceases to operate.

It took weeks for computer administrators to remove the Morris worm from each computer. According to the US Government Accountability Office (GAO), the damage caused by the Morris worm could be anywhere from $100,000 to $10,000,000.[6]

While the creator of the Morris worm had no malicious intent, he kick-started a generation of vicious cyberattacks.

WHAT IS IP ADDRESS ABUSE?

IP addresses are numeric and alphanumeric device identifiers that enable connected devices to communicate with one another.

The latest version of the Internet Protocol is v6. There are 340 undecillion IPv6 addresses in total, which, in theory, should support all connected devices infinitely. However, the adoption of IPv6 is slow, and the current internet architecture is still mostly supported by IPv4 addresses.

> The fourth version of the Internet Protocol address – which is also the first version to be used publicly – remains the backbone of the internet despite being almost completely exhausted.[7] When the infrastructure was built in the early 1980s, it was believed that 4.29 billion IPv4 addresses would suffice for a long time or until the more advanced version could replace it.

Evidence shows that we ran out of IPv4 much quicker than expected, and we chose not to adopt IPv6. Unfortunately, IPv4 is not only highly limited in quantity but also in security simply because it was developed back when most of the modern-day cyberthreats did not exist.

Today, IP address abuse is common, and it is an issue that affects companies large and small globally. Although individuals and enterprises are both vulnerable to the threats that abuse IP addresses in one way or another, businesses usually pay a larger price.

IP abuse is the malicious use of IP resources performed to facilitate phishing, spam, malware, distributed denial of service and other attacks

CYBERTHREATS AND IP ABUSE

As recent data shows, ransomware was the most common type of malware in 2021, and that is likely to remain true in 2022 as well. That said, ransomware is not the only kind of malware, and malware is not the only kind of threat that can exploit IP addresses.

According to the IPXO Abuse Prevention team, some of the most common cyberthreats related to IP abuse[8] are:

Malware – malicious software that cybercriminals use for various malicious purposes; examples of malware include ransomware, adware, trojans, spyware, rootkits, keyloggers, bots

Spam – unsolicited messages sent in bulk that often deliver commercial content

Phishing – fraudulent messages (e.g., email, direct messages on social media platforms) sent to extract login credentials, payment card details and other sensitive information

Hacking/Brute-force – an attack that relies on gaining unauthorized access to a computer system or a private network by guessing or using illegally obtained login information

Distributed-Denial-of-Service (DDoS) – an attack that is used to take down a service by overwhelming it with heavy traffic from multiple compromised systems

Port scanning – an attack that leverages open ports to intercept incoming/outgoing data

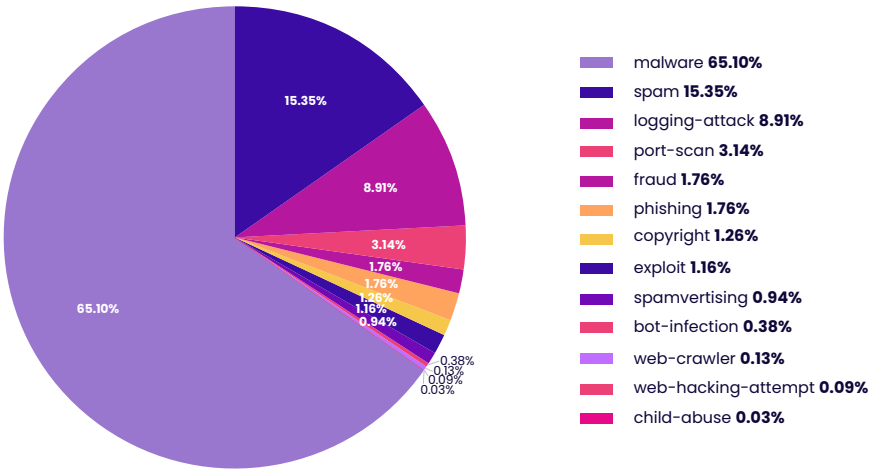
Copyright infringement – illegal use of copyrighted material without authors' permission

Illegal materials – child sexual abuse material (CSAM), harassment, hate speech, terrorism, etc.

Other – other cyberthreats that are not listed above and are generally less common

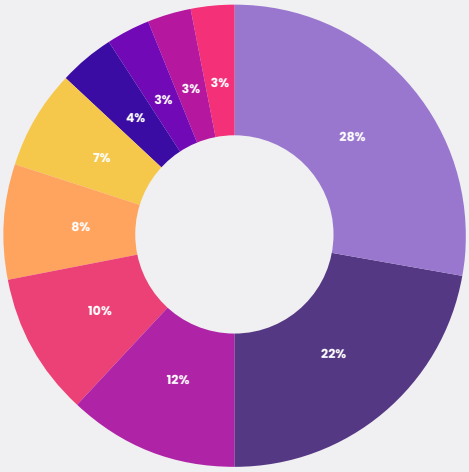
According to an internal analysis of the abuse affecting the IPXO Marketplace, malware was associated with the most IP abuse-related incidents between January and March (2022). These incidents corresponded to 65.1% of all reports. In the second place, at 15.35%, was spam, followed by login attacks, which accounted for 8.91% of all incidents.

MOST COMMONLY REPORTED TYPES OF ABUSE IN JANUARY-MARCH 2022



Malicious software is responsible for the largest portion of all IP abuse-related incidents at the IPXO Marketplace. Out of all malicious programs, these are the top 10*:

TOP 10 MALWARE REPORTED IN JANUARY-MARCH 2022



*% represents the portion of reported malware among the top 10 threats

When asked about the most common types of abuse during an IPXO webinar[9], Tobias Knecht, CEO at Abusix, shared that abuse affects different industries in different ways. According to Knecht, it all depends on what kind of infrastructure is built and what kinds of policies are set in place.

> "On the internet, anything that can be done illegally that makes a little bit of money is going to be done...We're seeing everything from spam – which is annoying, but not really a problem – to the really bad stuff like child exploitation and terroristic content."
>
> - Tobias Knecht,
> Founder and CEO at Abusix

Knecht adds that no one can escape abuse, and there are no networks that have never faced problems. In fact, research shows that cybercriminals can successfully penetrate 93% of networks.[10] Undeniably, the role of a dedicated abuse prevention and mitigation team is crucial.

ABUSE PREVENTION AND MITIGATION

Data shows that cybercrime is on the rise. This is perfectly illustrated by the number-one threat online – ransomware. In 2021, SonicWall observed 623.3 million ransomware attacks globally. This number indicates that there were almost three times more attacks in 2021 than in 2019 and 105% more than in 2020.[11]

With more threats emerging every day, cybersecurity experts are working around the clock to ensure that we not only mitigate threats timely but also prevent them from attacking in the first place.

Although it is impossible to predict or stop every instance of cybercriminal activity, it is crucial to prioritize prevention and mitigation on every occasion to protect information, personal security, businesses and governments globally.

IP ADDRESS ABUSE IN THE IPV4 MARKET

IPXO was built around the idea of creating a sustainable internet that counteracts the consequences of IPv4 exhaustion. It is evident that there are enough IPv6 addresses to satisfy the need of every internet-connected device on the planet for years to come; however, the internet is still mostly supported by IPv4 addresses. A resource that, officially, was exhausted in 2011 when IANA (Internet Assigned Numbers Authority) allocated the last five /8s to Regional Internet Registries (RIRs).[12]

Once the free IPv4 addresses were exhausted, RIRs changed allocation policies to control the remaining reserves more strictly. As soon as companies started facing the scarcity of the highly desirable resource, IPv4 addresses became a tradable commodity that companies started selling, buying and transferring.

As IPv4 sale prices skyrocketed[13], smaller and medium-sized companies faced another challenge – IPv4 addresses became not only hard to come by but also extremely expensive.

According to the historical IPv4 sales data by IPv4.Global, the price per IPv4 address climbed from $6 in 2014 to $60 in 2021

IPV4 SALE PRICES BETWEEN 2014-2021

SUBNET / YEAR	2014	2015	2016	2017	2018	2019	2020	2020
/24	$6-24	$9-20	$11-17	$13-19	$15-23	$15-26	$19-29	$23-60
/23	$9-15	$8-13	$11-14	$13-17	$14-21	$19-27	$19-25	$23-53
/22	N/D	$7-10	$9-15	$12-15	$13-18	$19-24	$19-25	$23-60
/21	$8	$6-8	$8-13	$11-16	$13-20	$19-24	$19-25	$27-46
/20	$7-8	$7-9	$8-10	$10-15	$15-20	$17-21	$19-26	$26-45
/19	N/D	$7-8	$8-10	$10-15	$15-19	$17-20	$19-24	$27-49
/18	$8	$8	$7-8	$11-13	$15-22	$18-22	$20-23	$26-45
/17	N/D	N/D	N/D	N/D	N/D	254	$20-23	$36-50
/16	N/D	N/D	N/D	N/D	N/D	N/D	$20-21	$23-40
/15	N/D	N/D	N/D	N/D	N/D	N/D	N/D	$26-38

As a response to the growing IPv4 prices, IPv4 leasing was introduced. Although IPv4 leasing was once regarded as a suspicious and, perhaps, even untrustworthy activity, today, it is the new normal.

First and foremost, leasing IPs is easy, quick and does not require high upfront costs. Second, when IPs are leased via an abuse prevention-focused platform, leasing is also safe.

IPXO, the first fully automated IPv4 address lease and management platform on the market, now accommodates more than 2 million IPv4 addresses ready for lease. And the number keeps growing. Of course, the more IPs are brought to the IPXO Marketplace, the more important the role of the Abuse Prevention team becomes.

According to Vincentas Grinius, CEO at IPXO, back in the 80s, when the Internet Protocol was still being developed, no one realized the role that spam and other forms of IP abuse would play today.

> Despite that it's impossible to prevent 100% of IP abuse incidents, all efforts are put into ensuring that abuse is mitigated professionally. This is important to ensure that only reputable IP lessees join the platform and that they lease IP resources only from reputable IP lessors.
>
> - Vincentas Grinius,
> CEO at IPXO

The IPXO Abuse Prevention team employs 92 reputation engines to check for malicious or untrusted IP resources. This helps maintain the reputation of leased IP addresses and, simultaneously, enables predicting IP abuse.

All IP addresses are checked before they are added to the Marketplace to prevent disreputable IPs from entering the platform in the first place. Once IPs are in the Marketplace, IPXO takes the responsibility of monitoring their reputation 24/7.

THE IMPORTANCE OF ABUSE PREVENTION AND MITIGATION

If IP addresses are not protected appropriately, they can end up on blocklists – lists of malicious or untrusted IPs. In the best-case scenario, this could result in a temporarily unusable IP resource. In the worst-case scenario, the IP holder could lose both money and reputation.

According to Grinius, some IP blocklists are more severe than others. For example, the **Spamhaus Don't Route or Peer (DROP)** blocklist lists IP addresses that have been deemed stolen or used in spam hosting operations. Another example is the **UCEProtect Level 3** blocklist that denotes the so-called worst ASNs (autonomous system numbers). At the time of research, this list contained 576 ASNs.[14]

According to Gustavas Davidavičius, Abuse Prevention Team Lead at IPXO, the time it takes to react to abuse incidents is the most important factor in abuse mitigation.

> "The longer abuse reports are ignored, the greater the chance that the abused resources will end up on a blocklist. If IPs are blocklisted, that can cause major problems for any business."
>
> - Gustavas Davidavičius,
> Abuse Prevention Team Lead at IPXO

Davidavičius shares an example of a company facing a DDoS attack. In the wake of the incident, if an IP range ends up on a blocklist, the company cannot send emails outside its network.

The repercussions can be very serious, and those interested in selling or monetizing IPv4 addresses via leasing should be especially motivated to keep their IP assets off all blocklists. Otherwise, the assets could lose monetary value and selling or leasing them could become extremely difficult.

ABUSE PREVENTION AND MITIGATION MECHANISMS

To provide IP monetization and lease services that clients can trust, IPXO prioritizes abuse prevention and mitigation. Therefore, from the moment the client creates an account on the platform to the moment they might decide to take resources back for their own needs, trained abuse prevention professionals are working around the clock.

The main mission of the IPXO Abuse Prevention team is to perform background checks on clients when they first join the platform and then maintain the reputation of the IP resources that are put up for lease. These essential tasks would not be possible without the following mechanisms:

- **KYC checks**
  IPXO Marketplace clients go through strict KYC checks to disable potentially unreliable parties from joining the platform and to catch existing IP reputation issues before IP addresses are put up for lease.

- **Direct reporting**
  Automated IP reputation monitoring and direct reporting ensure that IPXO clients can freely access information about the reputation of the leased IPs.

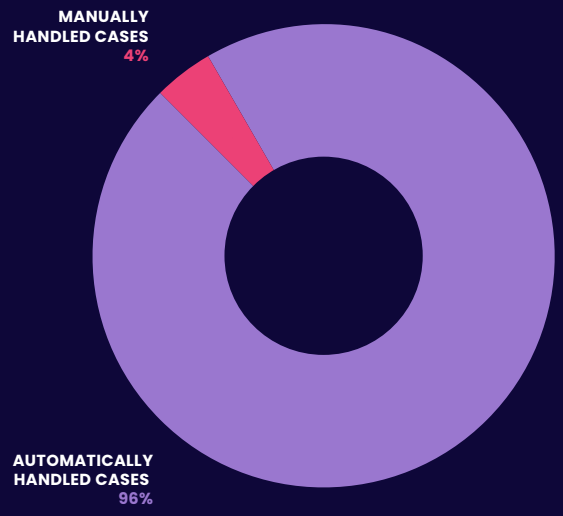
- **Real-time IP address monitoring**
  Automated real-time IP monitoring helps maintain the reputation of the leased resources. 92 reputation engines are employed to help cross-check IP addresses and catch any abuse incidents.

- **Professional abuse prevention team**
  The IPXO Abuse Prevention team is trained to evaluate clients who want to join the IPXO Marketplace, handle all abuse incidents and maintain IP address reputation.

- **Automated abuse reporting system**
  An automated abuse reporting system enables filling abuse reports quickly so that the Abuse Prevention team can handle any abuse incident quickly and efficiently.

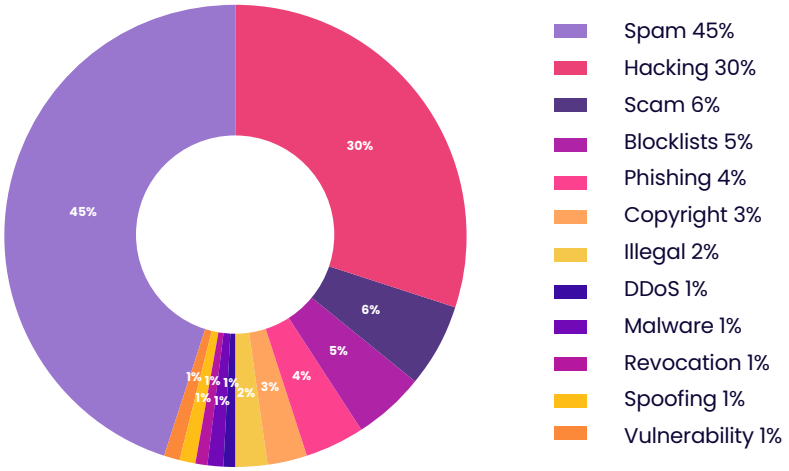
96% of all abuse reports received by the IPXO Abuse Prevention team between January-March 2022 were handled automatically. Only 4% required manual handling, which ensures that the team can address all abuse incidents quickly and efficiently.

AUTOMATIC VS. MANUAL ABUSE HANDLING IN JANUARY-MARCH 2022



Most IP abuse incidents reported to the IPXO Abuse Prevention team that required manual handling were related to **spam** (45%). Less than a third of cases (30%) were associated with **hacking** attacks. **Scams** (6%), **blocklist**-related issues (5%) and **phishing** (4%) were the following incidents that the IPXO team had to handle manually. **Spoofing, DDoS** attacks and **malware** were among the issues that required the lowest level of manual intervention.

TYPES OF ABUSE HANDLED MANUALLY IN JANUARY-MARCH 2022



THE ROLE OF COMPLIANCE CHECKS

Compliance is defined as strict adherence to the set guidelines and rules. When it comes to IP leasing and monetization, compliance plays a key role in building trust between IP holders and IP lessees. Essentially, compliance reassures IP holders that their resources will be handled by reliable IP lessees.

Compliance checks reassure IP holders that their resources will be handled by reliable IP lessees

The role of compliance checks

When a company creates an account with the goal to rent IP addresses available via the IPXO Marketplace, it must fill out the Declaration of Subnet Usage. The declaration includes the following checklist:

- **Is your company GDPR compliant?**
- **Is mailing activity involved?**
  - **Is it M3AAWG compliant?**
  - **What is the nature of mailing?**
- **Designated abuse department**
- **Abuse email**
- **Can abuse be expected?**
  - **Abuse type**
- **Doing business since**
- **Industries served by the company**
- **Company size**

M3AAWG compliance

Companies involved in mailing activities cannot start leasing IP resources via IPXO unless they pass the **M3AAWG** compliance check. The **Messaging, Malware and Mobile Anti-Abuse Working Group** is a US-based association that works against malware, viruses, spam, botnets, DoS attacks and other DNS exploits.

Companies that perform the following activities cannot pass the **M3AAWG** compliance check[15] and, thus, pass the IPXO compliance requirements overall:

- Advertising on pornographic websites
- Distributing chain letters, phishing scams, computer viruses
- Exposing email recipients to email fraud
- Offering stocks of unknown or non-existent companies
- Promoting bulk emailing services for sending spam, fake health products and remedies, Get Rich Quick/Make Money Fast schemes, software that collects email addresses and sends spam, pirated software, pyramid schemes

Subnet validation (for lessors)

When a company creates an account with the goal to monetize IP addresses via the IPXO Marketplace, it must pass the **Subnet validation** checks. The validation includes the following checklist:

- ✓ **Ownership Confirmation**
- ✓ **WHOIS**
- ✓ **RIR**
- ✓ **Authorization Status**
- ✓ **BGP Configuration**
- ✓ **Reverse DNS Delegation**
- ✓ **Initial IP Reputation Check**

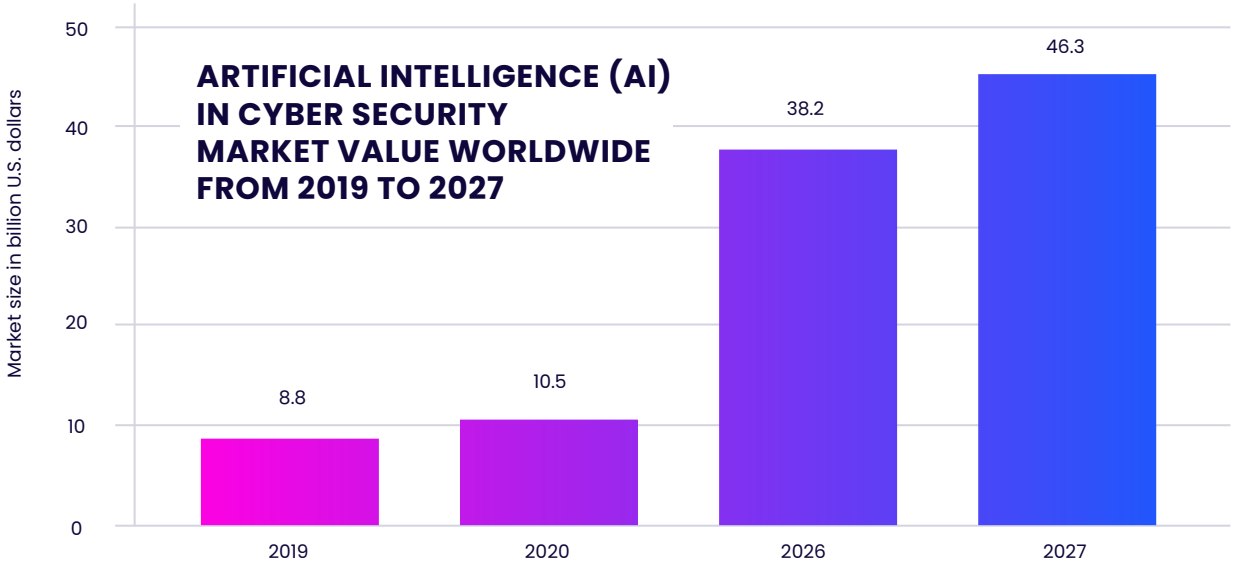
THE ROLE OF CYBERTHREAT INTELLIGENCE

Data is highly valued in cybersecurity. Collected and analyzed data can help better understand the patterns and trends of various cyberthreats and, consequently, help better mitigate these same threats.

Artificial Intelligence (AI) plays an important role in cyberthreat intelligence as it can help:

- Uncover patterns and threat characteristics
- Speed up threat prioritization and investigation
- Enable managing high volumes of threats efficiently
- Empower abuse prevention teams to make informed decisions
- Optimize threat mitigation capabilities
- Inform stakeholders about potential risk scenarios

Undeniably, cyberthreat intelligence is gaining traction, and businesses have found immense value in it. As a direct result of that, the market of AI is booming. According to Statista, the market value of AI in cybersecurity will reach $46.3 billion in 2027[16]. A significant increase from $10.5 billion in 2020.



Artificial intelligence (AI) in cyber security market value worldwide from 2019 to 2027 in billion US dollars (data by Statista)

It is agreed that AI and automation – the essential parts of cyberthreat intelligence – can significantly increase cyberthreat observability.

According to Zoltan Balazs, Head of Vulnerability Research Lab at CUJO AI, machine learning and AI are important in mitigating the global shortage of IT experts.[17]

> Machine learning is very useful to do tedious human work at a very large scale for very cheap. With the help of machine learning and maybe AI, a significant amount of human work can be done, and everyone knows there's a huge shortage in IT security talent. So, whatever we can automate is always a big win.
>
> - Zoltan Balazs,
> Head of Vulnerability Research Lab, CUJO AI

Andrius Lapienė, Staff Security Engineer at IPXO, believes that small organizations might be unable to gather cyberthreat intelligence on their own. Therefore, Lapienė suggests that the security intelligence community should be open and transparent with the information that is shared.

Undoubtedly, large companies can achieve more in cybersecurity because they have the capital and resources to spare, and Lapienė believes that information sharing is the most important aspect in achieving a high level of cyberthreat intelligence and, consequently, the mitigation of cyberthreats.

> There is a saying that you can achieve 95-98% of security with quite modest investment...our goal should be to make the cyberthreat intelligence available beyond the Fortune 500 companies so that everybody could be able to tap into [intelligence] and protect their business and their personal information.
>
> - Andrius Lapienė, Staff Security Engineer at IPXO

CONCLUSION

IPv4 addresses – the building blocks of the internet today – have been scarce since IANA allocated the last resources from its pool in 2011. Although RIRs exhausted their pools of allocated IP addresses later, the depletion of the resource has already affected businesses in various industries.

With the number of cyberthreats growing globally, IP address abuse incidents are likely to increase in numbers as well. In many cases, abused IP addresses are blocklisted, which prevents IP holders from using IP addresses for different services, most notably, mailing.

Because there are so few IPv4 addresses available, IP address abuse is especially disruptive. Companies cannot just replace blocklisted IPs with fresh ones. Therefore, professional IP address abuse mitigation and prevention are crucial. If IP holders manage to keep their assets clean, they can continue using them efficiently.

IP address abuse mitigation and prevention are of particular importance to IP holders who choose to monetize unused IPv4 resources via selling or leasing. Undoubtedly, it is much more difficult to both sell and lease IPs that have been blocklisted and have a bad reputation. Even if IP holders can find buyers or lessees, their abused assets are likely to lose monetary value.

The IPXO IP address lease and management platform employs numerous strategies and mechanisms to ensure that IP addresses brought to the IP address Marketplace are clean and remain clean for the duration of the lease period.

To prevent IP address abuse, the IPXO Abuse Prevention team utilizes strict KYC policies, compliance checks and professional 24/7 IP reputation monitoring. Cyberthreat intelligence enables the team to better predict abuse incidents and, ideally, prevent them from occurring at all.

The high standards ensure that IPv4 leasing is a safe and convenient option for IP holders monetizing unused IP resources as well as companies leasing those resources to efficiently scale their operations.

REFERENCES

[1] SonicWall. 2022. 2022 SonicWall Cyber Threat Report. SonicWall

[2] IBM Security. February 2022. X-Force Threat Intelligence Index 2022. IBM

[3] Ganti, V., Yoachimik, O. January 10, 2022. DDoS Attack Trends for Q1 2021. Cloudflare

[4] Board of Regents of the University System of Georgia. A Brief History of the Internet. University System of Georgia

[5] Collela, P. January 2017. Ushering In A Better Connected Future. Ericsson

[6] Halliday, J. September 21, 2010. Internet worms: a guide. The Guardian

[7] Huston, G. April 2022. IPv4 Address Report. Potaroo

[8] IPXO Knowledge Base. July 22, 2021. Reporting Abuse. IPXO

[9] IPXO. December 11, 2020. Webinar: Abuse Desk Policies and IP Reputation Management. YouTube

[10] Barker, I. December 20, 2021. Cybercriminals can penetrate 93 percent of company networks. BetaNews

[11] SonicWall. 2022. 2022 SonicWall Cyber Threat Report. SonicWall

[12] ARIN Vault. February 3, 2011. The IANA IPv4 Address Free Pool is Now Depleted. ARIN

[13] IPXO Blog. October 8, 2021. IPv4 Price History. IPXO

[14] UCEProtect Network. March 31, 2022. Level 3 lists IP Space of the worst ASN's. UCEProtect Network

[15] IPXO Knowledge Base. July 22, 2021. What is M3AAWG Compliance? IPXO

[16] Sava, J. A. February 17, 2022. AI in cyber security market size worldwide 2019-2027. Statista

[17] IPXO. April 20, 2022. Cyber Threat Mitigation. YouTube

ABOUT IPXO

IPXO is a fully automated IP address lease and management platform built to help lease and monetize unused IP resources while alleviating the global IPv4 shortage problem.

IPXO provides clients with a full automation stack that ensures accessibility and innovative solutions for companies in 75+ industries. We combine 10+ years of experience in the industry and innovative thinking to build a sustainable internet that supports the growth of any business.

IPXO

LEARN MORE

ipxo.com

contact@ipxo.com