OffendingIPs List Documentation

A report out from Cybersecurity Ventures estimates Cybercrime is expected to cost the world $6 trillion by 2021, up from $3 trillion in 2015. This includes damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm.

Many companies do suffer the poor services they are offering through the internet. They are not conscious of the fact that the problem comes from the slowness and bad functioning coming, the bigger part, from the massive increase in Brute Force Attacks we are detecting these last few months. These are automated polymorphic attacks, aimed at discovering online services' user names and passwords, to put them in the black market and get a profit out of stolen personal and financial data. Bad functioning alienates potential customers. And personal and financial data access put the company in strain with legal personal information protection rules.

Cybercrime has become a nightmare to companies and internet users as more and more cyber criminals add more resources and pressure to get the money and the control over the Internet. Thousands of new connected systems are hacked every day and added to any of the existing Z (Bot) networks. The attacking procedures are changing every day. Thus, many patterns based protecting systems become obsolete too fast and reputational IP's systems are both not covering all sources of offense and refreshing their lists too slowly. The only efficient way to protect our connected systems has become to enhance security and preventively ban the offending IPs, used by the hacked systems to attack the rest of the Internet, in our systems' firewalls, almost in real time.

For all companies that face endless email spams, ransomware and server attacks, and for companies that want to protect their websites from the soaring brute-force attacks, the same as their mail servers and critical systems against DDOS or any other kind of malicious attacks coming from hacked systems behind offending IPs, we introduce you to a resource that has been specifically designed to keep corporate systems safe and just ready to deliver the requested corporate workload.

After several years of development, we have created, through our own entity, a list of offending IPs out of a set of successful algorithms that will work worldwide.

This list has grown to more than 120,000 offending IPs that, if used to attack altogether, or by groups, could cause a tremendous negative impact in any corporate network or system. And it grows every day by a number of newly detected Offending IPs that we add to our list. These

IPs, if blocked in firewalls and updated twice a day, will become the perfect tool to avoid DDOS, BRUTE FORCE, SQL Server Injection, SMTP, SPAM and RANSOMWARE attacks to websites, corporate networks and critical systems.

TECHNICAL DETAILS

I4conAnalytics OffendingIPs list is produced by a set of different resources that are listening the internet, filtering any incoming call through very clever algorithms and putting all offending IPs detected in a common list. These offending IPs come together 96 times a day.

This list has been produced and refined throughout the last 11 years to add all possible sources of attacking systems and to optimize the filtering algorithms.

The list is serviced several times a day in an encrypted text file by a secured web service that can be called only from accepted internet IPs and the number of times under contract.

USE CASES

1. **Ransomware attacks**: Any employee whose email has been added to list of botnets attacking hackers will receive every day, despite corporative antivirus or spam filters, all kind of different appealing emails to get their click on any of the links or attachments to download the ransomware that will spread and attack all kind of accessible corporative resources. Cost of damage may ascend to high figures. With i4conAnalytics OffendingIPs list blocking attacking IPs, those emails will disappear most of the days and, when they come, will only arrive a little few before they are fully banned in next OffendingIPs list load.

2. **Brute Force attacks**: They consist in repeated attempts aimed at discovering users' names and passwords to get access to private servers and or web applications available through internet. These attempts are executed by specifically designed applications, fully parametrizable to find the html fields were to put the test data and to adequately time the attempt attacks. Several simultaneous attempts are usually launched from different IPs and in coordinated per-second waved processes. These attacks' effect is demolishing for the attacked service. It does not only put at risk services' and sites' security, but users' security too. It also causes a drop, sometimes a huge drop, in the service's/sites' performance when answering so many per second Access attempts. These are the most active web attacks nowadays and can be fully avoided from the 115000+ offending IPs in our list.

3. **DDOS attacks**: Many companies need an internet open web site/service to sell or to show their products to the public. Under a DDOS attack, with standard DDOS firewall solutions, that website will suffer several hours until all offending IPs have been detected and blocked. The customers' penalty may be high in terms of lost sales and confidence. With i4conAnalytics OffendingIPs list uploaded and protecting the website, that attack would have never taken place. All attacking IPs would be already blocked. No loss of sales or confidence.

4. **Trojans attacks**: trojans need to connect to their master's systems to execute any internal or external attack. No firewall will know the masters IP. If the IPs of those masters are blocked in the corporate firewalls by the i4conAnalytics OffendingIPs list, no attack will ever begin.

5. **SQL Server Injection attacks**: Most companies are afraid at sharing any SQL port to the internet due to the constant flow of attacks it will suffer while showing up. Most of these attacks are brute force meaning that endless access attempts are to be suffered until the right user and password are obtained. To avoid this, the firewall should block all but the accepted connecting IPs. This has the cost of having this accepted source IPs updated and loaded into the firewall. None of them will ever gain access to SQL server if the i4conAnalytics OffendingIPs is already blocking all attacking IPs in the firewall. SQL Server ports will come back to the internet if companies use our services.

6. **SPAM**: Many companies fight seamlessly against undesired spam emails that enter their employees' inboxes. Spam do not only include Sex or Viagra ads, but also all kind of undesired commercial offers that steals time from employees. While some of them you may get rid of by clicking the unsubscribe link, employees are many times warned of not doing so for the possibility of getting into undesired pages that may lead to a download of unwanted malware. With i4conAnalytics OffendingIPs list in place, most of the really harmful Spam emails are blocked at the front door. Employees will no longer lose their time reading or trying to remove such spam from their inboxes.

Q&A

1. **Is this list a regional one?** No. Although some minor hackers do target only local companies, most big hackers are worldwide players and they create systems that attack other systems around the world in an automated way.
2. **Is it needed a professional firewall to block IPs with the OffendingIPs list?** No. Any firewall where you may upload the OffendingIPs list will do. You may even load the list in the Windows/Linux systems' own firewall. Just remember that the list includes already more than 120.000 IPs and it is growing every day.
3. **Do you have any script to ease the load of such OffendingIPs list into corporate firewalls?** Yes, we do have scripts for Windows 2003-2008-2012-2016 servers. These scripts may be used as a base to create other scripts for Linux, Fortinet systems or any other kind of firewall that accept blocking IPs from uploads -scripts-. If you have troubles creating your own, you may always contact our consultancy services for a quote.
4. **How should it be loaded into corporate firewalls?** Every existing firewall allows for the upload of a new IPs list while keeping the old one as active. Once the new list is in place, in less than a second, the old list may be deactivated and the new one activated. No unprotected span of time.
5. **Do you have any kind of technical support?** Yes, we do have consultancy on setting the OffendingIPs list upload to the corporate firewall and on solving any issue that may occur during the adoption or daily use process.
6. **Does the firewall need to have a big amount of ram to use the OffendingIPs list**? Not at all. The i4conAnalytics OffendingIPs list occupies a few Kbytes both in the file and once in memory.

7. **What kind of software may I use to get the offending IPs list?** The i4conAnalytics OffendingIPs list is serviced by a WCF web service available in the Internet. So, any software that can connect to the web service placing a given user and password as the call parameters, decrypt the downloaded IPs file and work the list into the firewall, may be used.
8. **What kind of encryption is used?** OffendingIPs list file is encrypted using the DES asymmetric method. This means that the keyword used to encrypt it cannot be used to decrypt it. Keywords used are created distinct for each customer.
9. **How is the web service secured?** User and Password are needed as the web service call's parameters. Besides, we control the number of times the file is downloaded from each IP and the IPs that try to access the service. Any IP that serves any system that tries to get the list and is not allowed will be included into the OffendingIPs list.
10. **How long it takes to upload the OffendingIPs list into the firewall?** The list takes no more than 30 seconds to be uploaded and ready in partial mode in a windows 2008R2/2019 server while it takes about 4-10 minutes to be uploaded and ready in a windows 2003/2008 server. The full list may take about 12 minutes to load in a windows 2008R2/2019 server while about 24 hours in a windows 2003/2008 server. The good news is that server performance is not affected during the upload process, and until the new list has been uploaded and is ready to be activated, the old one continues filtering the incoming IPs.

PRICING

Pricing is established in a per firewall schema with a volume discount:

Nb. of firewalls	Price per Firewall per Month	Discount
1-3	50€	0%
4-10	40€	20%
11-25	35€	30%
25+	30€	40%

CONTACT

Go to https://www.i4con.com/i4conanalytics-expertise-areas/offendingips/ to ask for a service contract or some more info.

DISCLAIMER

This Offending IPs list has been created with the intention of protecting systems from the immense malware out in the internet. It is being offered as a helping tool and it is your sole responsibility if, on using it, any of your systems becomes unresponsive or broken. Use it with care and the due checks.

On the other hand, if your IP is black-listed, you are not a spammer or an offender, and you want it to be removed from our list, please send an email explaining the actions taken to clean the infection behind. We will do our best to analyze each case and remove the IP from our list if so considered.

November 2019

Would you allow thieves try your home's front or back door every day?