digital element®

The Need for Proxy/VPN Data in Today's Heightened Cybersecurity State

Colonial Pipeline. JBS Foods. CNA Financial. Media headlines about these cyberattacks serve as a dire warning about the intense battle today's enterprise IT professionals face on the cybersecurity front lines, where the losses span monetary, reputational, productivity and IP theft, to mention only a few. No industry segment has been immune.

Cybercrime, which includes everything from theft or embezzlement to data hacking and destruction, is up 600 percent as a result of the COVID-19 pandemic.[1]

Global market intelligence firm IDC expects worldwide security spending to reach $174.7 billion in 2024.[2]

In today's world, new technologies usher in new tactics used by criminals. They can launch ransom attacks, take over networks, and illegally infiltrate consumer accounts through diverse devices from anywhere in the world. By leveraging camouflage techniques, they can do so anonymously. Tools such as Virtual Private Networks (VPNs), proxy servers, queue networks, and Domain Name Systems (DNSs) allow them to hide their true identities and locations.

The reliance of cyber criminals on these tactics can be key to deciphering crime networks and their activities if businesses take the right approach.

Corporate VPN Usage Not Surprisingly Grows from Pandemic

A VPN is an encrypted connection over the internet from a device to a network—through a single IP address. A corporate VPN offers organizations the opportunity to provide their employees expanded access to resources on the company's network, no matter where they're working. With stay-at-home orders, many people had to start working remotely during the pandemic, sparking an increase in VPN usage.

The intent behind the use of corporate VPNs is obvious.

A quarter of people rely on VPNs for business purposes only, while another 15 percent use VPNs for both business and personal reasons.[3]

Cybercrime, which includes everything from theft or embezzlement to data hacking and destruction, is up 600 percent as a result of the COVID-19 pandemic.

digital element

Five out of every 10 users of VPN services are circumventing region-locked content to stream Netflix, indicating that tens of millions of people use it for that purpose.

Commercial VPNs Create Multiple Agendas

There are varying levels of different commercial VPN services available for consumers for their everyday online use outside of work. These include NordVPN, Strong VPN, ExpressVPN, TunnelBear and SurfEasy. Corporations are likely not using these to secure their traffic. They're using more reputable and secure VPN providers, such as Norton and LifeGuard. Or, they might have their own software that they've developed in-house.

Top reasons internet users use VPNs: [4]

- **General security reasons**, such as avoiding identity theft
- **General privacy reasons**, such as securing their personal data.
- **While on public WiFi** to mitigate risks
- **Due to job requirements**

Commercial VPNs rent out data centers from hosting companies. These aren't your traditional Internet Service Providers (ISPs) such as AT&T and Xfinity that give internet access at homes. They are providers that expect a significant amount of different traffic from multiple users from all over the world to flow through these data centers.

Some of these commercial VPN providers can set up their data centers in different geographic locations, so end users can change their ISP-given IP address to one that is geolocated to a particular location in the world where they want to be seen as coming from. For example, if an end user located in the United Kingdom is looking to view some U.S.-based content, then he or she will need to get on a hosted server that has an IP address for a data center that is geolocated in the United States.

At this point, the intent has moved beyond the paranoid person who wants to protect his or her identity online for security and privacy reasons to one that is more malicious. Even though this consumer may just be trying to access and watch the popular "Breaking Bad" series now because it's not currently available to stream in the UK, this practice is illegal.

Streaming services, such as Netflix, Amazon Prime, BBC iPlayer, HBO Max and Hulu, have region-restricted content that you can only watch if you're in the right country—or you use a VPN to change your location.

However, a new crop of "high-end, premium" VPN services have also recently emerged that pose a security threat to both consumers and businesses alike.

Five out of every 10 users of VPN services are circumventing region-locked content to stream Netflix, indicating that tens of millions of people use it for that purpose.[5]

Free VPN Services and the Rise of Residential IP Hijacking

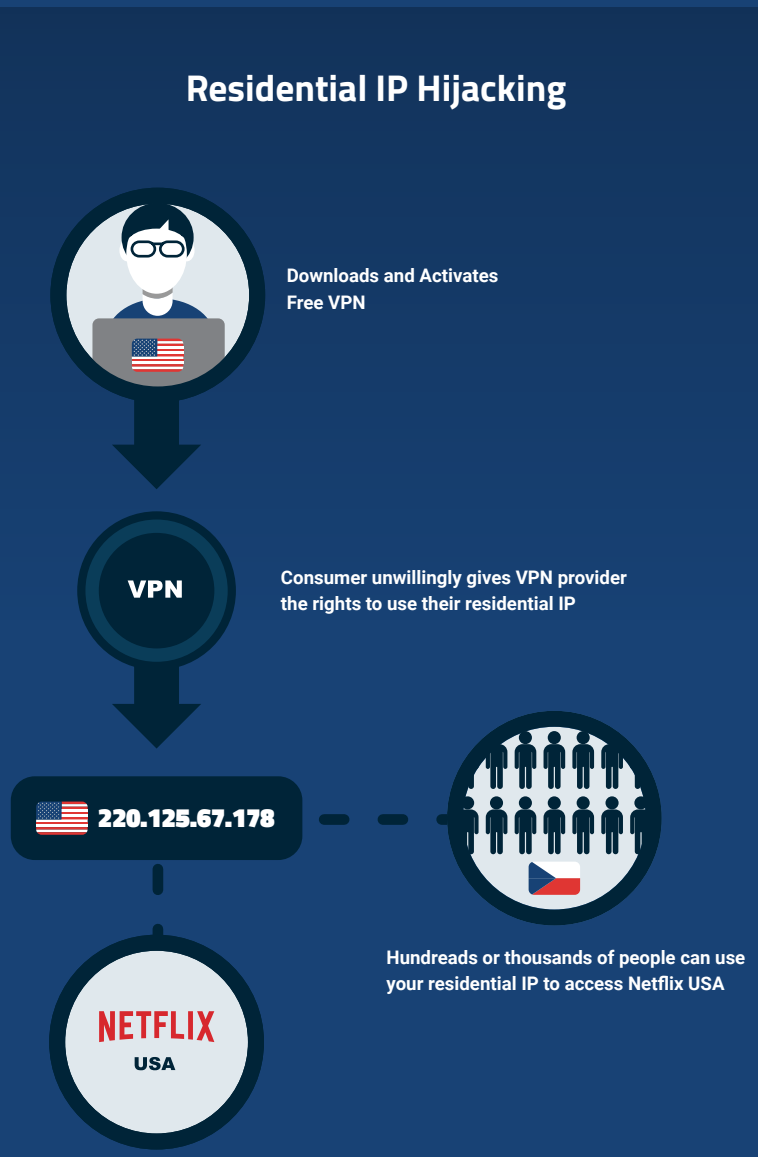
There is a new kind of provider that touts residential VPN proxy service—meaning they're not dealing with IPs in those hosting data centers. They are after IPs that are in use by regular consumers, coming through home residential IP connections.

Users who have download free VPN software in order to bypass geographic content restrictions have unknowingly had their residential IPs hijacked by these VPN providers. By agreeing to their Terms of Service, the consumers' residential IPs are then sold to other VPN providers that, in turn, sell them as a premium offering.

Consumers using residential ISPs, such as Charter or Xfinity, are having their IP addresses compromised without their direct knowledge, and they're being circulated in the proxy space by these commercial VPNs.

This is how it works.

A consumer signs up for a free commercial VPN. He doesn't have to pay for anything. He downloads it, installs it and turns it on. At that very moment, the commercial VPN provider has now seen his residential IP address. Somewhere in the Terms of Service (that he more than likely didn't read but signed), the consumer agreed to give that VPN provider the right to use his residential IP address in the entire proxy pool for routing purposes. That VPN provider then goes to the new crop of residential proxy services, such as Luminati, Oxylabs, and Smartproxy, and sells that residential IP address.



digital element

Approximately one-third of global online users access the internet using a VPN or proxy server.

Once that consumer goes online and his IP address is detected, then that residential proxy service can reroute hundreds of thousands of users from the Czech Republic, for example, providing them with a U.S. IP address (which now appears to be routed through a residential ISP) to access and watch Netflix USA.

Separating the Bad Guys from the Good Guys

Cyber criminals, in particular, have found the use of proxies to be effective. But, it's important to remember that not all proxies have malicious intent. As discussed, VPNs are widely used by legitimate users for diverse purposes and are a popular choice for enhancing security and privacy.

Approximately one-third of global online users access the internet using a VPN or proxy server. [6]

As a result, stopping all VPN users is not practical. It increases the danger that real customers or employees are mistakenly labeled as crooks. If that is not enough, this method fails to discover the root of cybercrime. In order to mitigate risks and protect real users, companies must find the means to separate the bad guys from the good guys— and one of the tools for accomplishing this is the incorporation of IP-based VPN and proxy data into your platforms and technologies.

Detecting proxy traffic is an IP-based phenomenon. The presence and type of proxy dictates how certain IP traffic is handled.

The following types of proxies often warrant a red flag:

Anonymous: Actual IP address of the end user is not available which often includes the use of services that change location to circumvent digital rights management, Tor points (free software for enabling anonymous communications), temporary proxies and other masking services.

Transparent: Actual IP address of the end user is available via HTTP headers, although the value is not necessarily reliable (i.e. it can be spoofed).

Hosting: Addresses belong to a hosting facility, and end users are not typically located in a hosting facility.

Corporate: Generally considered harmless, their location can occasionally be a concern. Multiple users proxied through a central location or locations, and thus sharing a single network-apparent IP address, are not reliable.

Public: Multiple users are proxied from a location allowing public internet access (i.e. libraries).

Incorporating IP Data for Protection

By connecting to the internet through proxies, the IP address of the criminal's device will not be shown accurately, but rather the IP of the proxy server.

The ability to identify if an online user is connected through a proxy and what type of proxy it is enables companies to flag potential criminal activities, set protocols for handling this type of "non-human" traffic differently and then review the post-facto analytics behind these types of connections. By incorporating proxy/VPN data on the front-end of online security measures, companies can automatically flag an IP address as suspicious and reject or block the incoming IP from connecting to their service, website or network.

Understanding the type of proxy a visitor is connecting to the internet with can trigger fraud alerts. Responses to the type of proxy can vary depending on what type of proxy it is—for example, an anonymous proxy may warrant a higher fraud score than a corporate one. By identifying connections that obscure the end-user location or those that seek to portray a connection from an "acceptable" city or country can now be easily identified and categorized.

Of course, success depends on data quality. Reliability of information can vary significantly among data sources. But the most accurate proxy data providers not only ensure that information is constantly updated on a daily basis, but that information also originates from excellent sources.

Some examples of security use cases applying proxy/VPN datasets:

Online Gambling and iGaming

A statewide lottery for Minnesota that allows consumers to participate online, for example, has two options to: 1) Ensure players are "human" (and not bots); or 2) Certify players are from that state—not right across the border in South Dakota. By incorporating IP-based VPN data, the lottery can see if an IP address is associated with a proxy. If yes, then access can automatically be denied. Additionally, a subscriber-level commercial VPN could be used to change a player's actual location to appear to be from Minnesota. In the absence of proxy data, using IP-based geolocation data in the verification process can help the lottery identify down to a state level where that online player is actually originating from—automatically granting or denying access to participate.

Government

An air-service branch of the government can use IP-based VPN data to filter, identify safe VPNs, then develop traffic exemptions for approved vendors, such as Lockheed Martin, in order to automatically grant access to the agency's networks and websites.

Financial Services/E-commerce

Whether an insurance company or an e-tailer conducting business online and accepting digital payments, they can incorporate proxy/VPN data to implement smart rules to automatically verify consumer IP addresses then determine which transactions to review—and which to approve or decline.

Cybersecurity

Managed security service providers (MSSPs) can use proxy/VPN data as a foundational, front-line layer of fraud-prevention security. They can use these datasets to help prevent unauthorized network and system access attempts. By understanding how online users access and interact with their clients' networks, MSSPs can be better positioned to more quickly respond to potential cyber threats when unusual activities occur.

Streaming and OTT

A sports streaming service that broadcasts regionals sporting events around the world can use proxy/VPN databases to determine which IP addresses to geo-block from piracy attempts. The streaming service can also use other IP information parameters to determine when a potential pirate is using a new proxy IP to try and gain access again.

The Future: Incorporating Other IP Data to Go Beyond Proxies

In order to thrive in the digital world, companies must equip themselves with tools that identify and exploit crooks and cyber criminals to strip them of their anonymity without jeopardizing real users—and this can be accomplished effectively and seamlessly through proxy/VPN data and other IP-intelligence factors.

The analysis of criminal activity can go far beyond proxies. Initially, this may include an assessment of the connection type. For example, a hosting center can be a tool for traffic, not a source. Then traffic originating from it can be examined alongside existing records, such as information stored in a Customer Relationship Management (CRM) database. The same goes for proxy, VPN and queue servers. By evaluating the type of proxy used against the highest quality proxy data, companies can start distinguishing between a reliable VPN and a mechanism that is more suited to suspicious activity.

Beyond connection features, IP geolocation allows companies to run comparisons. For example, in retail, this includes the implementation of smart rules where IP location is automatically checked when there are log-ins from high-risk locations. Alternatively, companies can secure internal networks by tracking speed patterns and identifying suspicious trends, such as people jumping between locations at illogical speeds or in illogical order.

After analysis, companies can choose their preferred mode of action. Any suspicious activity that poses a low threat can be flagged for a form of authentication, such as sending an email or SMS that allows the user to confirm their identity. In the meantime, serious threats can be blocked immediately to prevent damage. Alongside reducing false positives, this approach shows consumers that companies are committed to cybercrime prevention.

Understanding the type of proxy a user is connecting to the internet with has become increasingly important to improving online security for any type of business.

digital element

About Digital Element

Digital Element is the global IP geolocation and intelligence leader. In business for more than two decades, the company has unrivaled expertise in leveraging IP address insights to deliver new value to companies in a privacy-sensitive, transparent manner. Leveraged by the world's most recognized brands, Digital Element provides clients with innovative solutions designed to optimize engagement across industries and applications, creating unique value at every consumer touchpoint.

US Headquarters:
+1 678.258.6300

UK Headquarters:
+44 (0) 2035 142 663

www.digitalelement.com

[1]Embroker, "2021 Must-Know Cyber-Attack Statistics and Trends," Apr. 1, 2021.
[2]Columbus, Louis, "The Best Cybersecurity Predictions for 2021 Roundup," Forbes, Dec. 15, 2020.
[3]Vigderman, Aliza, "2021 VPN Usage Statistics," Security.org., Apr. 13, 2021
[4]Ibid.
[5]Vojinovic, Ivana, "VPN Statistics for 2021 – Keeping Your Browing Habits Private," DataProt, Apr. 13, 2021
[6]Bulatovaite, Ieva, "Your Master Guide to VPN Usage Statistics," Surfshark, Nov. 27, 2020.