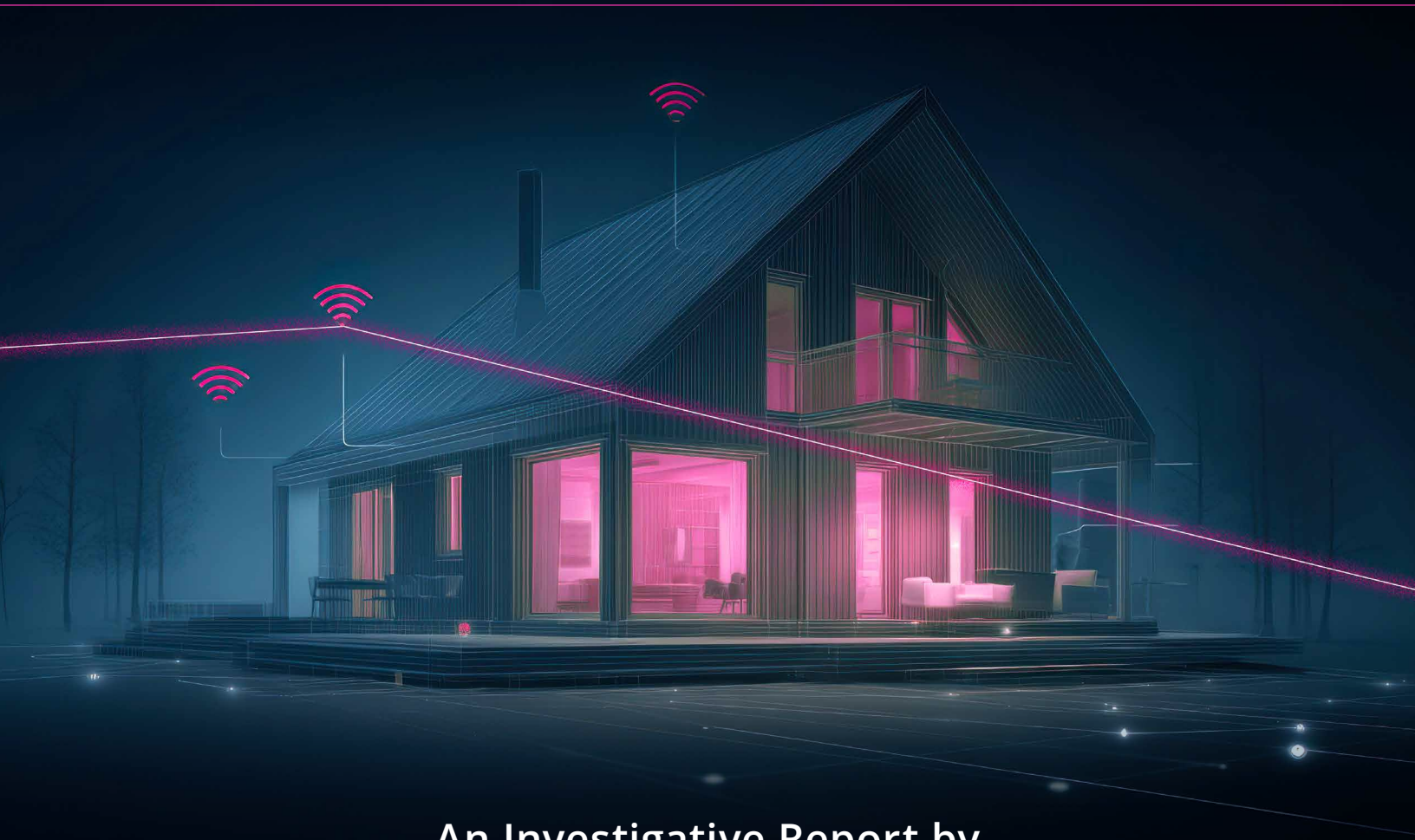
CYBERCRIME BY DOORBELL

How Illicit Actors "Borrow" the Internet Connections of Millions of Americans for Profit and Harm – And the Companies That (Knowingly or Unknowingly) Enable it to Happen



An Investigative Report by

DIGITALCITIZENSALLIANCE
a safer internet is a better internet

risk3sixty

June 2026

Table of Contents

Executive Summary

Somewhere in a quiet American suburban neighborhood, a family's smart doorbell is doing more than monitoring the front porch. Without the family's knowledge, the device is relaying tens of thousands of connections per day — routing spam, enabling fraud, and masking the origins of cyberattacks. The Internet Protocol (IP) connection may even be used by a foreign government to launch cyberattacks in the United States. The homeowners have no idea. Neither does their Internet provider. And that's the way criminals and state actors like it.

That doorbell is just one of over an estimated 20 million or more U.S. IP connections collected annually for use, often without the knowledge of Internet users, by so-called residential proxy services. This ecosystem is built on gaining control over Internet users' IP connections, with or without their knowledge, and then making them available – often to criminals and state threat actors.

The ease with which IP connections are harvested and weaponized is disturbing. For example, compromised streaming devices that can turn an American's doorbell or laptop into a digital weapon are sold by retailers such as Walmart and online platforms such as eBay.

In other cases, malware embedded in software downloaded from the Internet turns a device into a botnet. That's what happened with a Texas high school student, whose compromised IP connection was one of millions used in a scheme that enabled criminals to file $5.9 billion in fraudulent unemployment claims, steal billions of dollars from banks, engage in child exploitation, and make a series of bomb threats in the United States. A Chinese national and his 911 S5 operation made $99 million selling access to 19 million hijacked connections.

When residential proxies were initially introduced a decade ago, they were marketed as a means for companies to conduct ad verification and geo-testing of websites - but are increasingly used to commit crimes and state-sponsored actions against the United States.

Most people – whether regular Americans or policymakers – have never heard of residential proxies. But they are attracting increasing attention in the cyber security community because of their ability to inflict harm on consumers, businesses, and national security interests.

A joint investigation by the Digital Citizens Alliance, and cyber investigation firm risk3sixty, of residential proxies found a web of compromised consumer devices, disguised data centers, foreign infrastructure, and overlapping criminal operations that together represent a serious threat to national and economic security.

The Digital Citizens/risk3sixty investigation took place against the backdrop of escalating enforcement activity, including the dismantling of the world's largest residential proxy network relied upon by 550 threat groups, including state-sponsored actors from Russia, China, and Iran. The FBI has also warned about the so-called BADBOX 2.0 botnet, a network of infected devices used for piracy and other purposes that compromised over 10 million devices.

The joint investigation uncovered alarming findings about how these networks operate, how they source their IP connections, and the tangible harms that occur when these connections are exploited by criminals. Investigators signed up for residential proxy services that identified from scouring criminal forums and conversations among known threat actors. After paying in cryptocurrency to sign up for the services, the providers offered rotating IP addresses designed to make Internet traffic look like it was coming from ordinary American households.

This is not theoretical. Investigators purchased streaming boxes that illicitly harvested IP addresses without consent. When one device, called VSeeBox V5 Pro, purchased at Walmart, was powered on, it connected to a server based in China, authenticating with its unique hardware address. It pinged the server every sixty seconds, sent detailed device information, and received commands - commands that included the ability to install and uninstall apps.

Criminals don't just exploit IP connections to mask their movements. Illicit actors gain a foothold through a compromised smart or piracy device. Once inside a network, illicit actors probe other devices on a user's network looking for weaknesses that can enable them to steal usernames and passwords, access personal information, or take over cameras.

A 2025 hCaptcha report found that "legitimate use cases appear to represent a minority of traffic." Residential proxies are a documented enabler for criminals to harm individuals, companies, non-profits and government, with an estimated $50 billion to $100 billion in annual global losses. That state-sponsored actors such as Chinese hacking group Volt Typhoon rely upon proxies to disrupt U.S. critical infrastructure should be of concern to Congress.

Here are other key findings of the joint investigation:

- **Proxy networks designed for exploitation.** Of the IP connections scrutinized on the seven proxy providers, an average of 85 percent of the connections had been flagged as likely associated with fraud, a strong indicator that they are repeatedly used in cybercrime. Over 80 percent of connections across providers resolved to residential addresses, meaning American households are bearing the burden.

- **Bandwidth-sharing services expose consumers to foreign adversary traffic.** Services such as Honeygain offers to pay users to share their unused bandwidth. It's a popular app among students to earn extra money. Investigators signed up for Honeygain and then monitored how the investigator bandwidth was used. Investigators observed the connections made on shared bandwidth included connections between the service and entities in China and Russia - including traffic tied to a bank sanctioned by the U.S. Department of the Treasury. While we observed malicious connections, we have not found any indication that Honeygain is aware of how those connections are being used.

- **American IP addresses harvested and shared.** Nearly half of the roughly 26 million unique residential IPs tracked over 30 days appeared across multiple proxy providers. That means once acquired, the IP address is shared across multiple platforms used by illicit actors – increasing the risk an American household is compromised.

  This poses a practical concern for Americans and U.S. law enforcement. Illicit actors rely upon residential IP addresses to fly under the radar because they are less likely to be flagged - thwarting law enforcement efforts. However, if authorities do connect an IP address to crime, they don't find a criminal, but the citizen whose IP address was utilized.

- **Dark web marketplaces are a distribution channel.** Nearly half of the 42 dark web markets reviewed included proxy service listings, some featuring how-to guides for using proxies to commit fraud. Dark web proxies tend to cost more and perform worse than what's available on the regular Internet, but within criminal communities, residential proxies remain widely recognized as essential fraud infrastructure.

The illicit use of IP connections is the "blood diamonds" of the digital age. By the time a blood diamond reaches a jewelry store it is several layers from the forced labor that mined the gem and funded civil wars. The jewelers that sold blood diamonds could perhaps claim ignorance, but major players had knowledge. The same is true for residential proxies. The retailers who ultimately sell IP connections to businesses, state actors and cybercriminals may not have sourced the connections, but they are part of an ecosystem built on deception and crimes.

And the target is enormous: there are roughly 2 billion Internet-connected devices in American households, of varying vulnerabilities. Devices over three years old or that are no longer technically supported are considered the most vulnerable. According to a Digital Citizens research survey, XX percent of Americans said at least half of the Internet-connected devices in their home are three years old or older.

The goal of this report is to raise awareness about a threat that has largely remained below the radar of all but the cybersecurity community. That lack of general awareness about the risks has enabled bad actors to more easily exploit IP connections.

At the legislative level, there are gaps in U.S. laws, and a failure to hold providers to a standard. There is no "Kimberley Process" – an international certification that requires diamonds to be certified as conflict-free at each point in the supply chain – for IP connections, even though they are enabling state-sponsored acts against the United States and billions of dollars in cybercrime. Given the threats residential proxies pose to American interests – consumers, businesses, and national security – it's time for policymakers to learn what they are.

Whether it's through a smart doorbell, piracy streaming device, or disreputable VPN provider, millions of American homes are now unknowingly serving as tools for criminals. The cyber infrastructure has been weaponized, creating pressing national and economic security concerns.

We ignore those threats at our own peril.

This report examines the ecosystem, how it works, who it harms, and the providers that, knowingly or unknowingly, service the needs of criminals and state threat actors.

The Rise and Exploitation of Residential Proxies

To understand the residential proxy market, it's important to start with why it exists. For years, retailers and others relied on a simple premise: if traffic came from a known data center IP, it was probably a bot, so it would be blocked or at least challenged. If it came from a residential IP (say from a service provider such as AT&T), it's probably a real customer so let it through.

When the residential proxy market emerged as a service just over a decade ago, the premise was for business-oriented data collection: confirming that ads display correctly in different markets, price comparison across geographies, or seeing search results as a local user would. But it quickly became obvious that criminals saw it as an effective way to get around website and network security.[1] It is impossible to look at the 2025 hCaptcha report and risk3sixty's findings of how residential proxies are used for illicit purposes and not connect that to the growth of the market, which is expected to double from $2.5 billion in 2024 to over $5 billion by 2033.

Like nearly every multi-billion ecosystem, there are a mix of players:

- **Unsuspecting Users.** This is the American family that doesn't know their doorbell has been weaponized. At some point, they signed up for something, clicked "yes" to download an app, or opened a device in their home (such as the so-called piracy box BADBOX to watch movies and TV shows for free). Once they did, their devices were quietly enrolled as proxy nodes, almost always without their knowledge. Once they get into the family's network, the illicit actors probe the devices in the home looking to hack into them as well.

[1] ResProxies – What Hasn't Been Herd Yet

- **Exploiters.** These are the illicit actors who build the tools of compromise. They include malware developers, the operators who create fake VPN apps, the manufacturers who ship pre-infected devices like BADBOX, and the criminal operations that deploy malware to hijack routers. Their purpose is to gain unauthorized access to devices and IP connections. The most prominent example is YunHe Wang, a 35-year-old Chinese national whom U.S. prosecutors charge with operating the "911 S5" botnet — a residential proxy service that allegedly compromised more than 19 million IP addresses worldwide and generated some $99 million by selling cybercriminals access to those hijacked connections. Wang was indicted in the Eastern District of Texas and arrested in Singapore in May 2024 on a U.S. extradition request. As of early 2026 he remains in Singapore contesting his surrender to the United States, and the case is still working through pre-extradition appeals.

- **Brokers.** The platform operators who organize, aggregate, and monetize access to compromised or recruited IP connections at scale. They provide the pre-built code that a developer can plug into an app, so they don't have to build a particular feature from scratch. They also operate the infrastructure and connect supply to demand. Some are overtly criminal. The Chinese company IPIDEA built one of the world's largest residential proxy networks, controlling millions of consumer devices — PCs, smartphones, and smart TVs — that it enrolled largely without their owners' knowledge through malicious software development kits (SDKs) and "free" VPN and game apps. In January 2026, Google's Threat Intelligence Group disrupted the network by obtaining court orders to seize dozens of its command-and-control and marketing domains. Google estimated the action cut IPIDEA's available device pool by roughly 40 percent, though several million infected devices were still connecting to its servers afterward. Another operator, the Israeli-based LumiApps, markets a monetization SDK to app developers as an ad-free way to earn revenue — but the kit quietly turns the user's phone into a residential proxy node. It has turned up mostly in free VPN apps and in "modded" versions of legitimate apps distributed outside official app stores.

- **Proxy Services.** These companies are like retailers in that they sell IP connections. This tier ranges from openly criminal storefronts to companies serving Fortune 500 clients. Services such as SocksEscort and 5Socks market directly to cybercriminals and accepted anonymous cryptocurrency payments. Others are companies that operate entities running multiple storefronts from the same infrastructure.[2]

  The most prominent company is Bright Data, which claims rigorous ethical standards and boasts over 20,000 enterprise customers[3,4], yet under the name Luminati built its business on the IP connections gathered by its parent company VPN, which harvested the IP connections of the users of its free VPN service. It began informing VPN customers that it was turning their devices into nodes only after an outcry.[5]

What these players have in common is that none of them are currently required to independently verify that the IP connections it harvests or sells were acquired with the genuine informed consent of the device owner. The criminal services don't bother with consent at all. Some of the gray area services bury it in terms of service that most users never read. The result for the American whose connection is being exploited is functionally the same.

And the exploitation is rampant. Digital Citizens, working with cybersecurity firm risk3sixty, took a close look at seven companies that sell residential proxy connections. To assess whether these IP connections offered by these residential proxies were being exploited for crimes and other illicit actions, investigators verified where the IP connection is coming from and whether it had been used in previous exploits. Part of the verification process included using the service IP Quality Score, which aggregates data and determines whether an IP connection has or is being used for illicit purposes. The findings were alarming: most of the IP connections these companies were selling had already been flagged as potentially abusive or malicious.

---

[2] Comcast's Proactive Cyber Defense Activities

[3] https://proxyway.com/reviews/bright-data-proxies

[4] https://www.techradar.com/reviews/bright-data

[5] https://www.zdnet.com/article/hola-a-free-vpn-with-a-side-of-botnet/

Statistics by Network			
Provider	**Fraud**	**Residential**	**Unique Loc.**
Waveproxies	93.6%	81.2%	52.3%
PlainProxies	94.8%	81.2%	96.7%
Proxy.fo	98.9%	95.9%	9.3%
9Proxy	44.2%	72.6%	39.7%
Proxylooper	78.9%	78.9%	33.6%
ArealProxy	92.9%	85.8%	61.2%
Proxiware	88.7%	80.6%	88.7%

Table 2: Proxy Provider Network Statistics (risk3sixty, Jan–Feb 2026)

Across the seven providers, 85 percent of the connections examined were found to have high fraud indicators - meaning they had been associated with repeated suspicious or criminal activity. These fraud indicators were sourced from the industry-standard tool IPQualityScore, a fraud prevention and reputation platform used by thousands of companies worldwide. To build fraud scores, IPQS maintains a global network of fraud detection honeypots and deception traps to harvest live malicious traffic data and build risk profiles in realtime.

Based on this reputation scoring, it is clear that these IP addresses had not been used once for something questionable. They're connections that have been flagged repeatedly."

A look at one provider, Proxy.fo found 99 percent of their IP connections already flagged for suspicious or criminal activity. An analysis shows different approaches. Ninety-seven percent of PlainProxies' connections had a unique address, suggesting connections spread across many different addresses. That is consistent with a large pool of compromised residential devices in different homes. Proxy.fo, however, had only 9 percent at unique locations, suggesting connections are clustered in a small number of locations, which could indicate fraudulent inventory, disguised data centers, or concentrated pools of compromised devices in a few places.

The Art of the IP Harvest

The residential proxy ecosystem doesn't work unless tens of millions – potentially even hundreds of millions – of IP addresses are collected. That harvest falls on the wholesalers and partners they sometimes rely upon. It requires ingenuity. Opaqueness. And downright deception.

And, unfortunately, that path towards exploitation of IP connections can start with a simple purchase at a store such as Walmart. As of April 7, there were over 600 SuperBox S6 Max and the VSeeBox V5 devices available for online purchase on Walmart.com.

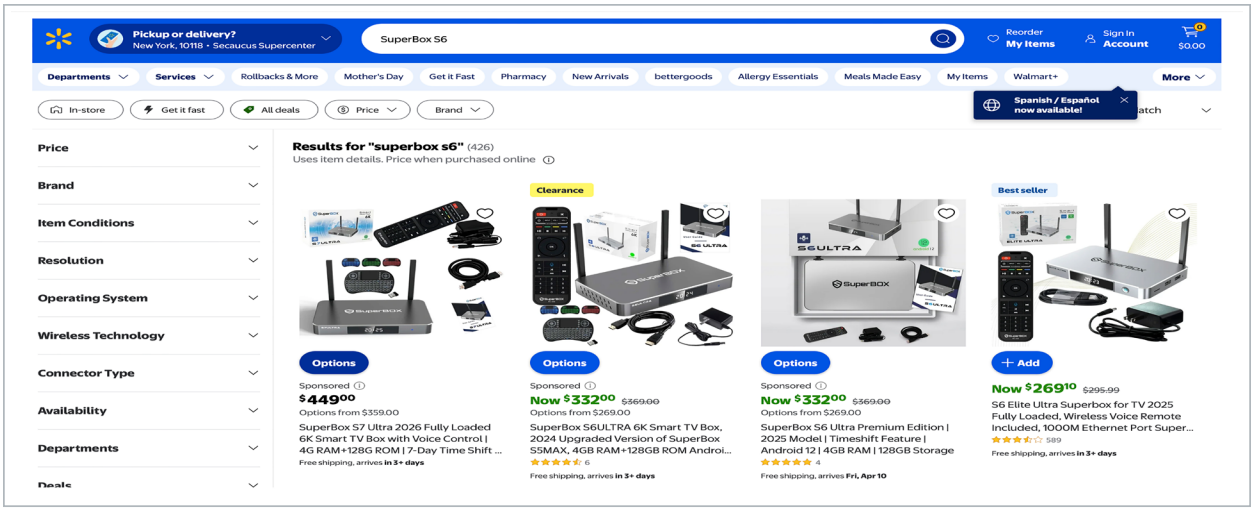


IMAGE 1

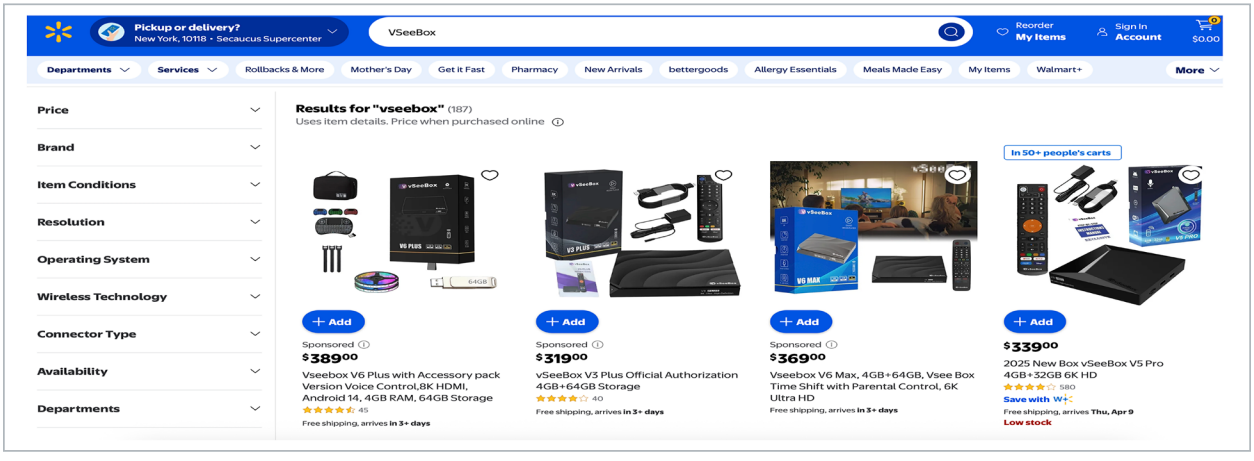


IMAGE 2

Investigators tested a VSeeBox purchased from Walmart.

Every time the VSeeBox powered on, it connected to a server based in China, authenticating with its unique hardware address. It pinged that server every sixty seconds, sent detailed device information, and received commands in return — commands that included the ability to install or uninstall apps, reboot the device, and perform a full factory reset. The VSeeBox also connected to s1276.byte-buff.com, whose subdomain pattern is consistent with malware-as-a-service campaigns. Two preinstalled apps disguised as Netflix were repackaged versions containing obfuscated code, and neither was signed by Netflix.

Here is an image of the actions the box took once powered on.

Show 50 entries Search:

STATUS	HOSTNAME	QUERY TYPE	ADDRESS	FIRST SEEN	LAST SEEN	ASN	COUNTRY
Unknown	www.s1523.byte-buff.com	A	NXDOMAIN	2026-01-31 07:28	2026-01-31 07:28		
Unknown	s1523.byte-buff.com	A	57.128.192.112	2026-01-31 07:10	2026-01-31 07:32	ASNone	Belgium
Unknown	s1316.byte-buff.com	A	146.59.54.55	2026-01-31 05:06	2026-01-31 05:07	AS16276 ovh sas	France
Unknown	www.s1316.byte-buff.com	A	NXDOMAIN	2026-01-31 05:06	2026-01-31 05:06		
Unknown	s1658.byte-buff.com	A	15.235.225.221	2026-01-31 01:36	2026-01-31 01:37	AS16276 ovh sas	United States
Unknown	s1662.byte-buff.com	A	15.235.230.13	2026-01-21 02:44	2026-01-21 07:20	AS16276 ovh sas	United States
Unknown	s1356.byte-buff.com	A	15.235.222.53	2026-01-21 02:41	2026-01-21 07:16	AS16276 ovh sas	United States
Unknown	s1521.byte-buff.com	A	146.59.84.22	2026-01-21 01:55	2026-01-21 06:11	AS16276 ovh sas	France
Unknown	www.s1521.byte-buff.com	A	NXDOMAIN	2026-01-21 01:54	2026-01-21 01:54		
Unknown	www.s1579.byte-buff.com	A	NXDOMAIN	2026-01-21 01:45	2026-01-21 01:45		
Unknown	s1579.byte-buff.com	A	141.95.98.71	2026-01-21 01:43	2026-01-21 05:47	AS16276 ovh sas	France
Unknown	s1583.byte-buff.com	A	141.95.98.155	2026-01-12 02:54	2026-01-12 03:26	AS16276 ovh sas	France
Unknown	www.s1583.byte-buff.com	A	NXDOMAIN	2026-01-12 02:48	2026-01-12 02:48		
Unknown	s1573.byte-buff.com	A	146.59.81.182	2026-01-08 01:28	2026-01-08 08:33	AS16276 ovh sas	France

IMAGE 3

A SuperBox S6 Max, pictured below, that investigators purchased from the company also performed suspicious activity the moment it was plugged in.

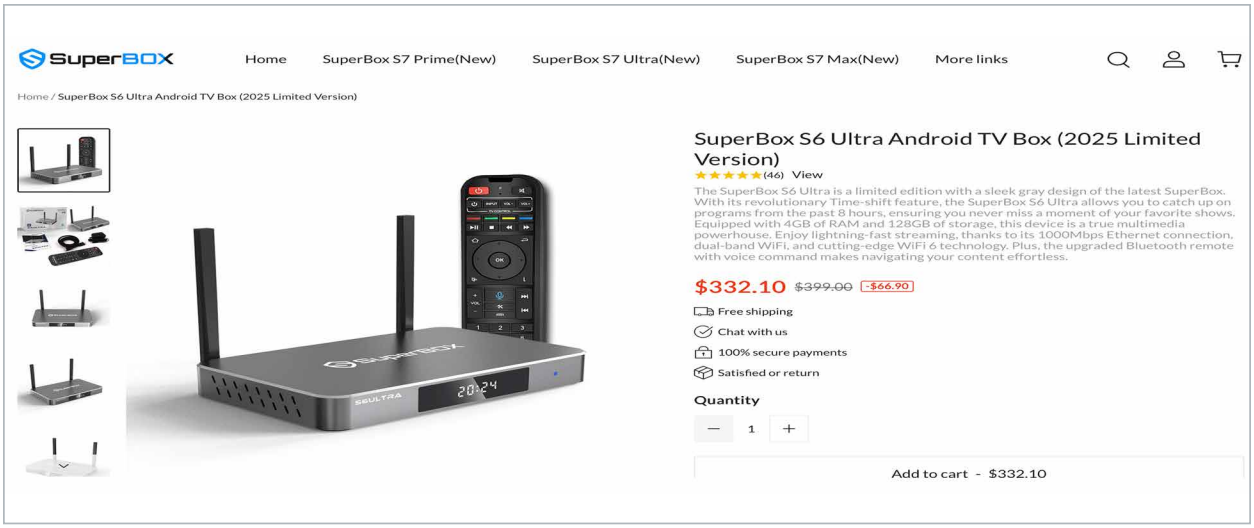


IMAGE 4

After it was booted up, the streaming device reached out to external servers, transmitting the device's IP address, location, and proxy status. It downloaded a third-party app store from a Google-spoofing domain that bundled piracy-enabling apps alongside legitimate ones. One of those domains was flagged as malicious by multiple security vendors. The device also connected to a known BitTorrent tracker.

The SuperBox findings align with what cybersecurity investigative journalist Krebs on Security reported last fall about devices purchased off the shelf at Best Buy that once booted up connected to a Chinese instant messaging as well as a residential proxy service.

Walmart and eBay were contacted about the report findings. Walmart responded: "We take the trust and safety of our customers seriously. The product referenced is no longer available on our site. We expect all items sold on our site through third-party sellers to meet our standards. When violations are detected, we take swift action, including removal of listings, to maintain a trustworthy experience for our customers." As of publication date, eBay had not responded.

Another common way that IP connections are harvested is through free mobile apps.

Hundreds of applications, particularly free VPN and utility apps, purchase of a piracy-enabled device or Firestick, or other malware techniques embed software development kits (SDKs) that silently enroll users' devices into proxy networks.

For example, a user downloads what appears to be a free VPN or file-cleaning tool and buried in the terms of service is consentto share their Internet bandwidth. A prime example involved a case where 28 apps on the Google Play Store using a library called PROXYLIB linked to a commercial proxy service. These apps turned Android phones into relay points for credential-stuffing, ad fraud, and scraping operations - all without meaningful disclosure to users.

The scale of SDK-based enrollment became clear during Google's January 2026 disruption of the IPIDEA network. IPIDEA operated proxy and VPN brands — including Galleon VPN, Radish VPN, Door VPN, and Aman VPN — that secretly enrolled devices into a massive proxy network. The analysis found that many well-known residential proxy brands were not only related but were controlled by the same actors behind IPIDEA.

The mechanism was ruthlessly effective. IPIDEA controlled domains related to Software Development Kits for residential proxies: Castar SDK, Earn SDK, Hex SDK, and Packet SDK. The operators marketed these kits to developers as monetization tools, offering compatibility across Android, Windows, iOS, and WebOS. The distribution footprint was enormous. Over 600 applications across multiple download sources with code connecting to IPIDEA's command-and-control domains - apps that were largely benign in function, such as utilities, games, and content apps, but utilized monetization SDKs that enabled proxy behavior.

Another pipeline for IP connections runs through Internet of Things (IoT) devices: smart doorbells, set-top boxes, security cameras, and Android TV units. Many ship with insecure defaults, exposed management interfaces, default passwords, outdated firmware, that make them subject to compromise. The security firm Spamhaus has documented IoT devices like video doorbells generating traffic spikes of nearly one million daily connections to known blocklists.

These findings are troubling given last year's FBI Public Service Announcement warning consumers that cyber criminals were gaining unauthorized access to home networks by either configuring devices with malicious software prior to purchase or infecting devices during setup. BADBOX 2.0 represents the largest botnet of infected connected TV devices ever uncovered.

Like the boxes scrutinized by the investigative team, BADBOX 2.0 devices frequently arrive pre-compromised from the factory, with malware embedded in firmware before the consumer opens the box. Most affected devices are manufactured in mainland China and shipped globally through unregulated supply chains. Compromised product categories include TV streaming devices, digital projectors, aftermarket vehicle infotainment systems, and digital picture frames. At least four distinct threat groups participate in the ecosystem, including the MoYu Group, which advertised residential proxy services built directly on BADBOX 2.0-infected devices.

Illicit actors also harvest IP connections through the direct compromise of home routers. Organized teams of cyber attackers, sometimes state-sponsored or state-affiliated, exploit vulnerabilities such as outdated firmware or weak credentials to convert residential routers into proxy infrastructure. One investigation uncovered over 800 KeeneticOS routers with identical fingerprints, all functioning as proxy nodes, traced to a single data leak of router credentials.

In one case, a botnet infected outdated wireless router until the operation was dismantled in 2025 through Operation Moonlander. The operators, three Russian nationals and one Kazakhstani national, allegedly amassed over $46 million over two decades.

Honeygain is a good case study because there is no trickery. It markets itself as a proxyware app that once installed, will utilize and pay for idle bandwidth. Users earn roughly $0.10 per gigabyte of data shared, with a reported $20 minimum payout threshold. Once deleted, it stops working.

As the screenshot below shows, Honeygain markets to students and others.

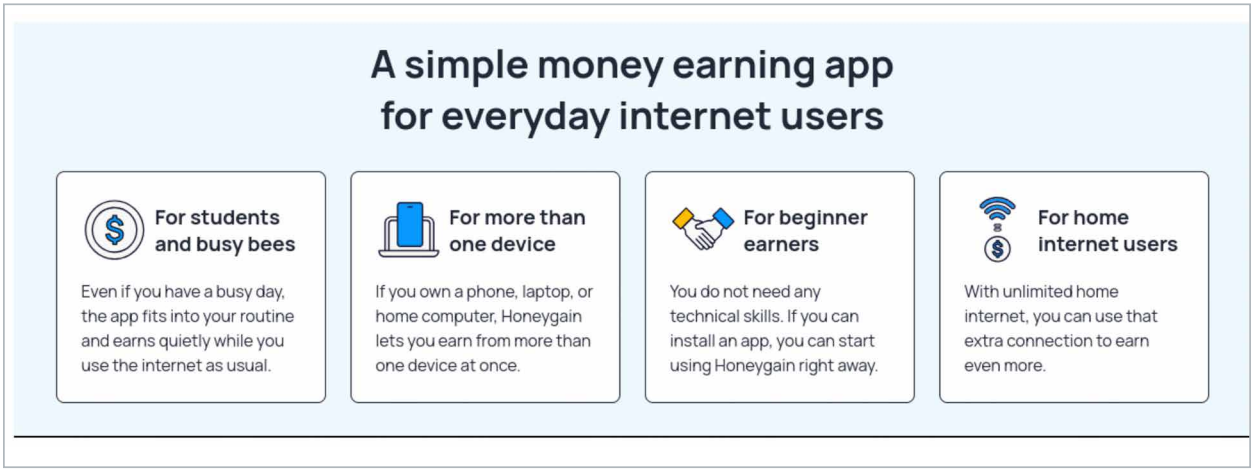


IMAGE 5

However, the case study gets more complicated once Honeygain claims that its partners are reputable businesses that use a user's Internet for legitimate reasons are compared with what investigators found and previous concerns raised by Trend Micro.

Investigators monitored traffic flowing through Honeygain over several days, finding incoming traffic from China and Russia, including from Tinkoff Bank (now T-Bank), which has been sanctioned by the U.S. Department of the Treasury. It appears T-Bank was paying Honeygain or one of their downstream resellers for access to the network, connecting to the testing laptop, and using our IP to connect somewhere else. Because the service obscures what traffic is passing through a user's connection, most have no idea what they're enabling. If they're using their home or work network, those connections could extend into privileged corporate environments.

In addition, when Trend Micro investigated Honeygain and other proxyapps, they observed malicious and dubious network traffic flowing through these proxy networks and found no evidence that "passive income" providers were policing the traffic being routed into exit nodes. Trend Micro classified these apps, Honeygain included, as "riskware" - not malware, but software that introduces risk the user may not fully appreciate.

There is a separate part of the ecosystem, although not as prominent as it once was. As part of this investigation, 42 Dark Web markets were analyzed, with 18, include listings for proxy services, although many appear to simply be guides or directions on how to use such proxies for fraudulent services, such as the image below.

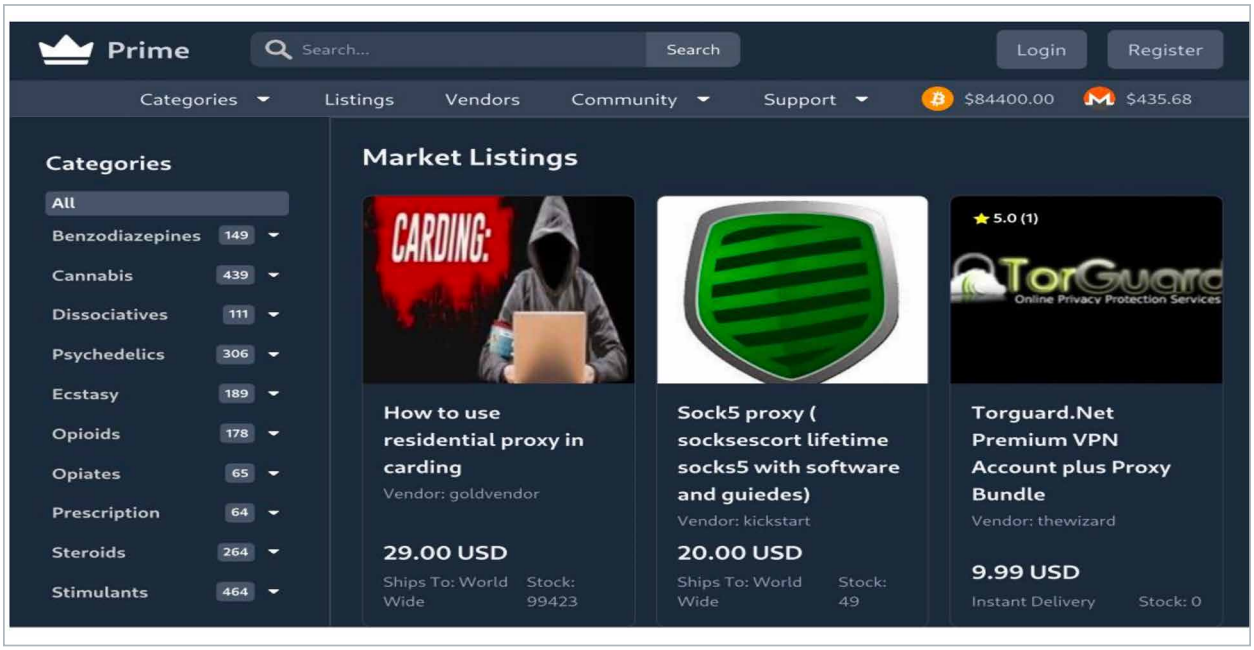


IMAGE 6

The relatively low occurrence of these listings on these marketplaces appears consistent with observed trends in cybercrime activity, which have displayed a gradual movement away from dark web infrastructure in favor of more easily accessible services such as social media. As noted by Chainalysis in May of 2025, dark web market revenues have declined, and many markets have focused on the sales of illegal drugs, breached databases, and stolen credit card data.

From Click to IP Connection Exploitation

Criminals count on Internet users' desire for "now." Get something free now. Watch a movie or TV series now. Get a small monthly payment now. Access to an online game now. For the sake of example, imagine two scenarios:

- A teenager in Toledo downloads a free VPN app to get around parental filters or access a streaming service outside the United States. The app does exactly what she wants – and more. Buried in its code is an SDK that silently enrolls her device as a proxy node. The teenager has no idea. The app didn't make it obvious, and the terms of service mentioned something about "sharing idle resources" in a document she didn't read.

- A thirty-something in Seattle purchases a cheap Android TV box from an online marketplace because it promises free access to movies, live sports, and TV shows. He plugs it in, connects it to his Wi-Fi, and starts streaming. What he didn't know is that the device came pre-infected with malware from the factory. The moment it connected to his network, it connected to a command-and-control server and registered the IP address in a residential proxy pool.

Each of these delivered what the user wanted, just more than they expected.
Within minutes of each of these actions, the users' IP address is registered in a proxy provider's inventory – available for purchase by anyone for just a few dollars. Someone looking for a residential IP address in Toledo snaps up the teenager's connection.

To the two users, nothing seems amiss. But in the background, their connections are now quietly relaying other people's Internet traffic.

Now it's the criminal's turn.

Using those IP connections, a fraud ring in Eastern Europe buys access to the IP address in Seattle and tests stolen credit card numbers against American retail sites. Because the traffic comes from a residential IP in Seattle, the retailer's fraud detection system treats it as legitimate.

Next, a credential stuffing operation uses the connection to test username-and-password combinations stolen from data breaches against banking sites. The bank sees login attempts coming from a residential IP in the same region as the account holder, so it doesn't flag the activity. Finally, someone uses a connection to transmit child sexual abuse material. In each of these instances the digital trail leads to their homes.

That may not be it.

Criminals have access to the IP connection and may not stop at just using to as a proxy. The investigation of IPIDEA found proxy software doesn't just route traffic through your device. It also sends traffic to your device, opening pathways for what is called "lateral movement."

They then move from device to device, testing each one for weaknesses. When they find one, they can install keyloggers to capture passwords. They can access security cameras. They can intercept unencrypted traffic and capture login credentials as to access banking information, email, and files stored on a network drive such as tax returns or financial documents.

Will they? It's a game of cybercrime roulette.

The consequences are predictable. An Internet user may find when they try to visit a website, they are constantly required to prove their identity. That is because the website operators see the reputation score of the user's IP address and suspect it's a bot. The user's Internet provider may contact them to say the IP address has been blacklisted for suspicious activity.

In some cases, a person finds out someone opened credit cards in their name, filed and received a tax refund, or in a doomsday scenario they face legal scrutiny because criminal activity such as child sexual abuse material has been transmitted over their IP address.

IP Connections and National and Economic Security

State-sponsored cyber actors have adopted residential proxy infrastructure as a core operational tool. In early 2026, Google and others identified over 550 individual threat groups, including state-sponsored actors from Russia, China, Iran, and North Korea, utilizing residential proxy exit nodes to mask communication channels used to remotely manage compromised devices.

These 550 threat groups were identified in just one week's time. Google analyst John Hultquist provided specific examples: "Residential proxies have been used by a whole host of threats, but they're showing up frequently in incidents involving Russian and Chinese cyber espionage."

China's Volt Typhoon campaign is a consequential example. The state-sponsored hacking group has targeted U.S. critical infrastructure since at least 2021 and been the subject of multiple joint advisories from CISA, the NSA, and the FBI. In February 2024, the U.S. Intelligence Community assessed that Volt Typhoon, and related Chinese actors that position themselves within IT networks to enable lateral movement to operational technology systems, the hardware and software controlling critical infrastructure. The purpose? Disrupt critical functions.

The connection to residential proxies is direct and documented. Volt Typhoon routes traffic through compromised SOHO network devices, including residential routers manufactured by ASUS, Cisco, D-Link, NETGEAR, and Zyxel. By proxying through these devices, the group's operations appear to originate from legitimate residential IP addresses within the geographic area of their targets, defeating geographic filtering and reputation-based security.

The FBI dismantled a Volt Typhoon-associated botnet of compromised residential routers in January 2024, but the group continues to operate through alternative infrastructure. U.S. cyber officials warned that Volt Typhoon has maintained persistent access to critical infrastructure sectors, including water, energy, and transportation systems. The implications are troubling. A compromised residential router, a device enrolled without consent into a proxy network, or bandwidth-sharing apps that connect a consumer's home network to unknown parties represents a potential node in a foreign adversary's operational infrastructure.

IP Connection-Driven Crime Pays

The crimes where residential proxies are a documented, significant enabler collectively cause an estimated $50 billion to $100 billion in annual global losses. Those losses come from account takeover and credential abuse, in which residential proxies become the delivery mechanism for credential-stuffing and password-spraying campaigns. Each login attempt appears to originate from a unique home IP address in the same geographic region as the legitimate account holder, making rate-limiting and geo-blocking defenses ineffective.

The Department of Justice's case against the 911 S5 botnet — described by then-FBI Director Christopher Wray as "likely the world's largest botnet ever" — alleged that its operator, Chinese national YunHe Wang, amassed over 19 million unique IP addresses across more than 190 countries, including 613,841 in the United States. Wang allegedly earned approximately $99 million selling access to these compromised addresses. The scope of the harms was enormous. The DOJ stated that criminals used the residential connections to "conceal their true originating IP addresses and locations and anonymously commit a wide array of offenses. These offenses including financial crimes, stalking, transmitting bomb threats and threats of harm, illegal exportation of goods, and receiving and sending child exploitation materials."

Investigators estimated that criminals using 911 S5 submitted approximately 560,000 fraudulent unemployment insurance claims during the COVID-19 pandemic, resulting in losses exceeding $5.9 billion. An additional 47,000 fraudulent EIDL applications are suspected. Wang was arrested in Singapore in May 2024 and faces up to 65 years in prison. The Treasury Department sanctioned Wang and his associates, and blockchain analysis identified over $136 million in cryptocurrency in his wallets.

Despite law enforcement crackdowns, it's ultimately a game of whack-a-mole. Case in point: When the 911 S5 proxy service was dismantled in May 2024, competitors released new front-end services within weeks. For criminal operations engaged in advertising fraud, residential proxies are essential infrastructure. The BADBOX 2.0 operation demonstrated this directly: infected devices rendered hidden ads, launched hidden browser windows, and simulated thousands of ad impressions per day per device — generating revenue through fake traffic that appeared to originate from real consumers. But it got worse: Android botnet Kimwolf hijacked the existing proxy infrastructure that BADBOX and IPIDEA had built to take control of proxies to launch massive cyberattacks.

Path Forward Starts with Awareness

The research in this report converges on a troubling conclusion: traditional defenses are failing. Because proxy traffic originates from legitimate consumer ISPs and mimics normal browsing behavior, IP reputation systems and geographic filtering are increasingly ineffective.

Yet despite the scale of the threat residential proxies pose, the issue is largely absent – whether around American dinner tables or in the halls of Congress. As the Institute for Security and Technology observed after convening a roundtable of ISPs, threat intelligence organizations, and law enforcement in February 2026, many policymakers have never heard of residential proxies.

But it's a given that Iranian, Russian, Chinese and other adversaries are utilizing residential proxies to conduct operations against U.S. infrastructure. And the scope of the financial and other harms enabled by the illicit use of IP connections is well documented.

If the illicit use of IP connections is the "blood diamonds" of the digital age, then it's critical that Americans, both citizens and policymakers, know about how their IP connections can be exploited. Internet users can take steps to check for exploitation:

- Tools such as an IP security checks called Grey Noise or Spur that can analyze whether an IP connection is part of a residential proxy network and compromised. It takes less than a minute to do.
- Avoid streaming devices that claim to provide free sports, TV shows, and movies, as they may contain malware or backdoors that hijack your IP connection The FBI has specifically warned about cheap, off-brand Android TV boxes.
- Be skeptical of "free" apps. Free VPNs, pirated software, and other apps from unofficial marketplaces expose users to risk. Steer clear of "earn money by sharing your bandwidth" offers. Proxy services convince people to download applications on their device that promise to pay them for their Internet bandwidth. What users don't realize is that criminals and state threat actors can then use their Internet connection to commit crimes.

- Replace routers or other household devices older than 5 to 7 years. When a hardware device is end of life, the manufacturer no longer sells the product and is not actively supporting the hardware, which means software updates or security patches are no longer released. Also change the default admin username and password all devices in your home.

If you suspect your IP connection or device is compromised, file a complaint with the FBI Internet Crime Complaint Center (IC3) at ic3.gov.

On the policy side, there is a "blood diamonds" model to follow. There is so-called Kimberley Process created an international certification program that requires diamonds to be certified as conflict-free at each point in the supply chain. Creating a similar standard for residential proxies would be a good start: require proxy services operating in or selling to U.S. customers to verify buyer identity or intended use. That is a model that has worked well with financial institutions and would be effective with residential proxies.

The residential proxy provider Massive is the closest to embracing such a model. It provides third-party validation of 100 percent opt-in, consent-based IP acquisition. Their 100% SDK-based sourcing model means IPs aren't being acquired through opaque wholesaler chains.

The gaps in addressing the threat of residential proxies speak to a broader issue. The threat spans the FCC (communications infrastructure), FTC (consumer protection), DOJ (enforcement), CISA (critical infrastructure), and Commerce (import controls).

No agency has clear ownership of the problem. To address that gap, the Administration should create an interagency task force with clear authority and funding would ensure coordination, avoid duplication, and enable the kind of sustained attention that this threat requires. This task force should also include the Treasury Department's Office of Foreign Assets Control, given the documented connections between proxy infrastructure and sanctioned entities.

There may also be lessons to be learned in what European countries are doing. The Dutch Data Protection Authority opened an investigation into "IP leasing without informed consent" in early 2026, and the growing regulatory focus on GDPR-compliant proxy sourcing is driving some market participants toward transparency. The United States has no comparable framework.

The residential proxy ecosystem is not a niche cybersecurity concern. It is foundational infrastructure for a vast range of criminal and state-sponsored activity, from pandemic fraud costing billions of taxpayer dollars to the pre-positioning of Chinese military-linked hackers inside American critical infrastructure. The wholesale-to-retail structure of the market means that targeted enforcement against key upstream operators can have outsized effects, while the white-label structure ensures that piecemeal enforcement against individual brands will be insufficient.

Consumers need to understand the risks. The family with the compromised doorbell, the student running Honeygain on their phone, the customer who purchased an Android streaming box for entertainment — none of them consented to having their Internet connection weaponized.

There are concrete steps that both Americans and U.S. policymakers can take. The Digital Citizens intends to do its part by building an initiative to create more awareness among Internet users. Hopefully, policymakers will take appropriate steps, including with measures that create a standard for ethical use of IP connections and law enforcement tools to deter illicit actors.

Until the ecosystem is restructured around genuine consent, accountability, and enforcement, millions of Americans will remain unwitting participants in a global criminal enterprise.

About Digital Citizens Alliance

The Digital Citizens Alliance is a nonprofit, 501(c)(6) organization that is a consumer-oriented coalition focused on educating the public and policymakers on the threats that consumers face on the Internet. Digital Citizens wants to create a dialogue on the importance for Internet stakeholders—individuals, government, and industry—to make the Web a safer place. Based in Washington, DC, the Digital Citizens Alliance counts among its supporters: private citizens, the health, pharmaceutical, and creative industries, as well as online safety experts and other communities focused on Internet safety. Visit us at www.digitalcitizensalliance.org.

About risk3sixty

risk3sixty is an elite boutique cybersecurity firm headquartered in the greater Atlanta area, serving clients nationwide with continuous threat exposure management (CTEM), threat intelligence, and proactive security services through its Armada Proactive Services practice.

Unlike software-only exposure management platforms that bury teams in unvalidated alerts, Armada embeds senior practitioners who run continuous threat intelligence, manually exploit findings to prove what's actually dangerous, and stay on every exposure until it's closed for good.

In addition, risk3sixty offers a comprehensive suite of services for CISOs, including internal audit, compliance, and GRC program optimization. Learn more about risk3sixty's proactive services at armada.risk3sixty.com