Threat Brief:
Venezuelans Turn to Cybercrime in Wake of Economic Downfall
Venezuela is a nation experiencing severe unrest. Authoritarian rule, mass exodus due to uncontrolled inflation, basic lack of human services, and violence stemming from a dispute between competing government bodies have devastated the country. Censorship of the media and the internet is driving thousands into underground criminal forums for resources to provide for their families.

As nation-states such as Venezuela claim control and sovereignty over the internet, organizations grasp for control over the flow of data within their networks. Crime increases when economic and political unrest ensues. IntSights has observed several important trends in cybersecurity that correlate with the downfall of the Venezuelan state over the past few years:

- Vulnerable technological infrastructure
- An influx of users to the dark web
- Migration to cryptocurrency as a result of local currency collapse

In this report, we address these pressing issues as they relate to global cybersecurity, dark web activity, and defense against the criminal activities that result.

**Desperate Times: Humanitarian Crisis in Venezuela**

Due in large part to the abuse of power by political leaders, Venezuela is a nation in distress. According to humanitarian relief organizations, more than 4 million people have fled Venezuela as refugees in the largest exodus from a Latin American country in over 100 years. The UN estimates there will be 5.3 million Venezuelan refugees and migrants by the end of 2019, rivaling the scale of the Syrian refugee crisis. By 2020, there will be 8 million Venezuelan refugees, making this crisis the largest refugee crisis in the world. Basic necessities like water, food, and hygiene items are scarce, and the people are dying of starvation, malnutrition, and disease.

The Venezuelan economy (and the value of the bolívar) is in ruins. According to the International Monetary Fund (IMF), Venezuela’s hyperinflation rate increased from 9.02 percent to 10 million percent since 2018. The state has almost entirely depleted the world’s largest oil reserves, and it now owes over $100 billion to foreign creditors. In the face of these challenges, the government has reduced the minimum wage to $2 per month. Although the IMF and World Bank think there is hope in strategies like economic “shock therapy” and increased foreign investment, the forecast looks grim. Meanwhile, the people of Venezuela are forced to find new ways to survive. For many of them, this leads to a life in crime.
Censorship and the Dark Web

The internet in Venezuela is a privilege and is available to only a small percentage of citizens. The Venezuelan government has been intimidating, censoring, and prosecuting its critics in the media since 2017. Popular news outlets, such as CNN, El Pitazo, and El Nacional, have been blocked, as well as online news sources, such as vivoplay.net, elcapitolio.tv, vptv.com, and the walkie-talkie app Zello.

Citizens of Venezuela have no free media sources, and nowhere to plan protests, marches, and anti-government campaigns. Still in the early days of censorship, those citizens that can afford electronic devices and can find a place to connect to the internet are forced to use Virtual Private Networks (VPNs) and the Tor browser to anonymize their internet activity and identities.

However, even VPNs and anonymizers are outlawed by the country’s largest Internet Service Provider (ISP), the state-owned CANTV. Initially, when the ISP implemented the blocks to the Tor browser in the summer of 2018, the Tor Project provided Venezuelans with advice on how to use “bridges” to bypass the government’s blocks. Some resources indicate the Tor bridges are now also blocked.

The chart in Figure 2 shows Tor usership in Venezuela before and after the ban was implemented. User activity skyrocketed right before the ban and dropped dramatically right afterward. Based on similar historical use cases in other countries like China, Russia, and Vietnam, users flock to Tor before it is shut down because they seek answers on how to maintain anonymity despite government crackdown. Protesters have now moved en masse to social media applications like Instagram, Snapchat, Facebook, Twitter, and WhatsApp, which are more difficult to censor on a broad scale.

For those who have access to smartphones and laptops, their personal devices tend to be old and outdated, with the majority of devices running Windows 7 and Windows 8. A recent scan of public-facing devices revealed that nearly 60,000 devices are vulnerable to the Bluekeep vulnerability, and many of CANTV’s servers are infected with malware. Cybersecurity is weak, the government does not have the resources to secure infrastructure, and everyone in Venezuela is paying the price.

Desperate Measures:

The Increase of Crime & Cryptocurrency Use

Legitimate opportunities for work and income are extremely limited in Venezuela. Working for the government or the military are not viable options for the many citizens who oppose the current regime. Two major trends stand out in Venezuela: the use of cryptocurrency and the increase of cybercrime as viable employment.

With the failure of the bolívar fuerte (main currency of Venezuela) and the increase in inflation, many people in Venezuela have turned to cryptocurrency to buy, sell, trade, and barter. They turn to deep web cryptocurrency sites for information on how it works, where to buy it, and what type of currency to purchase. The government of Venezuela even created a cryptocurrency called the petro (₽), or petromoneda, which launched in October 2018, to attempt to keep up with this trend.
“Petrocoin” is supposedly backed by the country’s oil and mineral reserves, and is intended as a means to circumvent U.S. sanctions and access international financing. In addition, President Nicolás Maduro authorized various cryptocurrencies as valid payment options to purchase oil exported from Venezuela. DASH and Bitcoin are the two most popular alternatives to petro, and President Maduro is pushing to launch a crypto-powered remittance platform to facilitate domestic and international payments without passing through SWIFT (Society for Worldwide Interbank Financial Telecommunication). Cybercriminals in Venezuela are embracing these currency changes and are taking advantage of the opportunity to monetize criminal opportunities.

Crime is big business in Venezuela. Cybercriminals and fraudsters thrive given the government’s limited resources to hold them accountable for their actions. Carding operations, hacking, fake IDs, fake passports, and various types of fraud are the top moneymakers for Venezuelan threat actors. Countless hackers have fled to neighboring countries, like Colombia, to continue their hacking operations with more reliable internet infrastructure and access to better technology.

During investigations into active phishing campaigns targeting our customers in Latin America, IntSights researchers discovered large-scale Venezuelan cybercriminal operations. Unlike some sophisticated threat actors around the world, these fraudsters are not concerned with hiding their identities or remaining anonymous. They have very public social media profiles, photos with their friends and fellow fraudsters, and extensive evidence that leads back to their cybercriminal operations, which indicates they are not afraid of being caught or prosecuted by local law enforcement.

Facebook groups with public settings give a glimpse into the Venezuelan carding community, a thriving underground where hackers and fraudsters bounce ideas off of each other and share tips on how to steal and resell credit card information, and anonymize internet traffic.

The hacking community in Venezuela is growing every day. Hacktivist groups such as Anonymous Venezuela form powerful alliances against the government and set up large-scale cyberattacks on government assets. They manage social media groups with significant followings and set up protests, hacks, and attacks to fight corruption in the government.
IntSights analysts have discovered several databases of information stolen from Venezuelan government victims. This data sells on various dark web forums for high prices, and sales often happen behind the scenes on open-source chat platforms such as ICQ, Telegram, Facebook, and Twitter.

**The Future of Cybercrime in Venezuela**

Venezuela is facing many of the same challenges as other nation-states: government instability, censorship and internet control, and a failing economy. These factors create an environment that drives people to the deep and dark web for access to information and income. Much like the findings of the threat brief we published on Vietnam earlier this year, we have observed a population desperate to escape government censorship and monetize the internet.

However, Venezuela is unique in many ways. The extreme economic collapse and hyperinflation have driven Venezuelans to a widely adopted use of cryptocurrency. This trend favors cybercriminals, as they are already set up to accept it and pay with it. Although the nation’s primary ISP banned the use of the Tor browser, criminals in Venezuela are finding ways around this obstacle, turning to open-source chat platforms and social media accounts to collaborate and find work. Carding operations, fraud, and large-scale phishing operations are paying off handsomely, and it appears that local law enforcement is turning a blind eye to the welcome source of income.

This is a motivated population of people turning to cybercrime as a viable way to make money. They are efficient, effective, and capable of doing severe damage to organizations and networks worldwide. They are funneling money into Venezuela through the easiest methods they know -- fraud and cyber theft.

Companies that face off with these threats are confronted by two major challenges: getting the government-owned CANTV ISP to take down malicious infrastructure, and convincing law enforcement to take action against specific threat actors. Both of these remediation methods require cooperation from a government that is not universally recognized and has lost control to a great extent.

The Maduro regime’s priorities do not include protecting internet infrastructure or global enterprises at the moment. Even if besieged corporations were to approach the new disputed president, Juan Guaido, there is little that his government can do to control the cybercrime emerging from Venezuela.
During investigations of cybercrime affecting IntSights customers, we were able to uncover the leadership of some large cybercrime operations. Despite obtaining detailed attribution, specific residential addresses, geolocations, and phone numbers of these criminal leaders, law enforcement will do very little to stop them. If they are apprehended in neighboring countries like Colombia, they could be extradited to their native Venezuela but will likely not be prosecuted for their crimes.

About IntSights
IntSights is revolutionizing cybersecurity operations with the industry’s only all-in-one external threat protection platform designed to neutralize cyberattacks outside the wire. Our unique cyber reconnaissance capabilities enable continuous monitoring of an enterprise’s external digital profile across the clear, deep, and dark web to identify emerging threats and orchestrate proactive response. Tailored threat intelligence that seamlessly integrates with security infrastructure for dynamic defense has made IntSights one of the fastest-growing cybersecurity companies in the world. IntSights has offices in Amsterdam, Boston, Dallas, New York, Singapore, Tel Aviv, and Tokyo. To learn more, visit: intsights.com or connect with us on LinkedIn, Twitter, and Facebook.

To see the IntSights External Threat Protection Suite of solutions in action, schedule a demo today.

What can enterprises do to protect themselves against these threats and challenges?

1. **Proactively monitor underground sources of chatter in the Venezuelan hacker community.** When a hacker targets your website, your people, or your money, you need to know who, what, when, where, how, and why. This strategy makes you proactive in your defense, not reactive. Social media and open sources are great places to start, if done carefully and covertly. If your organization does not have a Cyber Threat Intelligence team set up and experienced enough to conduct this type of reconnaissance, hire an experienced CTI vendor to do it for you. IntSights specializes in monitoring the criminal underground and has automated the process to scale to the needs of your organization.

2. **Understand what hackers are saying.** Professional language analysts are trained to collect human intelligence from sources like these in the native languages like Spanish, Russian, Chinese, Arabic, and more. IntSights has a team of linguists to translate and collect intelligence on cryptologic language and can help you interpret what the threat actors are saying and translate it into timely, relevant intelligence that will help you proactively defend your assets.

3. **Understand your vulnerabilities to the threat.** In order to protect your organization, you must know yourself better than the enemy does. One way to do that is to have a clear understanding of what your external digital footprint looks like. What assets are exposed or vulnerable to threat actors? They are persistent and will find a way in, whether through an open port, an outdated security certificate, or by using exposed login credentials. Many organizations focus solely on their network and internal assets while threat actors spend countless hours probing from the outside to find a hole in your security. Know what is exposed so you can remediate it before it is targeted.