Digital Browser Identities:
The Hottest New Black Market Good
The dark web is an ever-evolving ecosystem, where new threat actors, black markets, forums, and hacking trends continuously emerge. IntSights constantly tracks new black markets and their usage, and one has seen a particularly strong rise in activity since it emerged at the end of April 2019.

This site is named Richlogs, and it has positioned itself as a competitor to the Genesis market, which emerged in November of 2018 and was the first market to sell digital identities. Like the Genesis market, Richlogs collects and sells stolen “digital fingerprints” of a user’s web browsing device (i.e., IP address, OS information, time zone, user behavior). These sites enable the purchaser to impersonate a legitimate online user and circumvent standard security protocols, offering full credentialed access to any site that was stored in the victim’s browser. This includes Gmail, Facebook, bank accounts, credit cards, government tax sites, and confidential work sites.

Think of it like digital facial recognition, except instead of scanning your face to verify your identity, they’re using your web browsing device properties. The implications are frightening, as it gives anyone the ability to intrude and mimic a user identity online since users commonly save their credentials in their browser—even for financial and work websites—for convenience. The applications for this masquerade tactic go beyond fraud and financial crime. Hackers can target specific companies by searching for their employees; pedophiles can target and impersonate children by searching for victims who access known children’s sites; and intelligence agencies can search for different government employees according to their internal login pages.

In this research brief, we provide an overview of the Richlogs marketplace and the digital identities market, and share key implications that both companies and consumers must consider for effective protection against cyber threats.
The Market for Digital Identities

What are digital identities?
The appearance of the Genesis market in November 2018 drew attention to a new type of underground “good” – a digital identity. This type of black market sells full fingerprinting of a user’s web browser and computer characteristics, allowing an attacker to impersonate the victim almost flawlessly. This empowers the buyer of the digital identity to access websites as another user and circumvent advanced identity protection services. This includes access to mail accounts (i.e., Google, Yahoo, Microsoft), social media profiles (i.e., Facebook, Twitter, LinkedIn), banks and credit card accounts (including PayPal), retail and eCommerce sites (i.e., eBay, Amazon, Best Buy), music services (Spotify), travel apps (Uber), Government services, and even internal login pages for the victim’s company.

What is digital fingerprinting?
Fingerprinting is an anti-fraud method used to verify a user accessing a website with a username and password. These systems use technical details to verify the user—such as screen resolution, time zone, OS information, regular user behavior, and additional details that are unique to that user. This information is then used to determine if the user who is attempting to login is legitimate or a fraudster.

Think about when you log into a website for the first time. You sometimes get a message that states “We don’t recognize this device.” Fingerprinting encompasses all the background details that the website uses to recognize and validate that you are who you say you are.

How are digital identities stolen?
Similar to most forms of cybercrime, digital identity theft typically begins with an infection. These bots (aka infected device) are obtained by infecting computers and mobile devices with different types of specialized malware that harvest multiple indicators and session cookies required to access the site as the user. This type of malware is usually called a stealer. Stealers are not new and have existed since the beginning of the dark web. They are programmed to target specific software and websites, such as Chrome, Firefox, banking sites, Telegram, Steam, or other programs of interest.

Richlogs and Genesis have introduced a new breed of stealers specifically designed to collect digital fingerprints and artifacts. These stealers not only steal credentials but also harvest many other data points to help them create the most accurate impersonation of the victim.

These stealers are often spread through various social engineering tactics, including spam emails, malicious attachments, phishing links, malicious apps, and malvertising. The only way to know if a stealer is designed to steal your digital identity is to do a full analysis of its functionality.
Richlogs Market Overview

Richlogs went online in late April 2019. The site admin’s identity is unknown, but it appears to be Russian, based on the top—level hosting domain for the site and the language options offered (English and Russian).

Since Richlogs is a fairly new market, it offers just 1,105 accounts for sale, compared to Genesis, which currently offers more than 100,000 victim profiles. Richlogs has made many changes to its interface and functionality over the last few months, and states that it’s still in Beta. Just like any new market entrant trying to establish a foothold and gain market share, it attempts to differentiate from Genesis in a few key ways:

- Richlogs provides an interface that allows anyone to sell stolen digital identities, unlike Genesis, which only offers digital identities for sale without new users being able to sell their own. This creates more of a marketplace for buyers and sellers.
- Previous iterations of Richlogs stated who the seller was for each digital identity listed. It appears that that feature has been removed (as of August 2019).
- Richlogs also had a “seller panel” that gave bot owners an interface to manage their offerings; it appears that this feature has been removed or been moved behind the scenes.
- Richlogs provides more granular fraud information for victim accounts, enabling buyers to filter identities by availability of HiddenVNC connection to the bot, presence of cryptocurrency wallets credentials, or credit card information in the logs.

Richlogs isn’t shy about the fact that it competes directly with the Genesis market. In fact, Richlogs takes a jab at Genesis on its main page, stating that “other services” are selling incomplete fingerprinting data that uses random data generation, ultimately reducing the overall success rate of impersonation. This refers to a service offered by Genesis to create random fingerprints of non—existent users in order to try to circumvent security measures. This method is less likely to succeed, as it does not accurately match a real user’s data.

In these examples, note the variety of sites the victim accessed that a buyer can impersonate. An account is typically priced based on the amount of login data it contains. A user who has only a couple of sites in the cache will be sold for a few dollars. A user with dozens of sites can be sold for about $200—$250.
Digital Browser Identities: The Hottest New Black Market Good

Trends and Implications of the Digital Identities Market

The level of intrusion into a victim’s life that digital identities provide is alarming. It’s not just credit cards, bank accounts, or PII at stake. Digital identities offer threat actors the ability to almost completely take over someone’s online browsing identity. This includes everything from accessing expenses, to tracking daily travel routes, to seeing tax information. The bigger the victim’s digital footprint, the more he or she can be impersonated by a threat actor.

While malware that captures saved browser credentials is nothing new, online security screening has become more sophisticated by cross-referencing user details beyond just the username and password. As a result, attackers have started searching for methods to circumvent these security measures, and digital identities help them do that. It’s the perfect crime when done correctly because it seems legitimate to the accessed server, with almost no way to differentiate real users from threat actors.

Just as credential stuffing became a popular technique for brute force hacking, fingerprinting fraud is becoming more broadly utilized to obtain access to user accounts. And as more user data becomes accessible across the dark web, it only becomes easier to buy login credentials and impersonate users online to bypass standard security protocols.

Digital identities, as they are sold on Richlogs and Genesis, offer the whole digital fingerprint of an individual on a plate, providing endless opportunities for fraud, scams, theft, and access to the victim’s personal life.

An Inside Look at Digital Identities

While reviewing the profiles offered for sale, we discovered multiple corporate login pages that could enable hackers to easily access a corporate network. For example, if a bot contains credentials for internallogin.bank.com, that’s a good indication it’s an employee of that bank. Government sites are also prevalent. For example, one of the victims accessed a portal of the Serbian Traffic Police (Figure 5), identifying himself as a member of the Serbian police force.

Another victim accessed the New Zealand internal revenue service, identifying himself as a New Zealand citizen (Figure 6). And another victim was most likely an Indian national living in Qatar (Figure 7). We know this because while the profile mostly accessed Indian sites, it also accessed the Qatar government national authentication system.

Richlogs does not discriminate between regions and countries. We observed victims from all around the globe, including the US, Western and Eastern Europe, Asia, and the Middle East. If you get infected, your whole digital profile will be offered for sale.

Figure 5: Serbian police force login page access by a victim (translated)

Figure 6: A victim’s harvested login page to the Inland Revenue of New Zealand, identifying the person as a New Zealand citizen

Figure 7: Qatar’s national authentication system
Different Motives
Although these sites do not currently offer any direct PII on individuals, they do allow you to search for different technical attributes, such as operating system, site accessed (domain), bot (computer) name, country, and more. They recently introduced a credit card scraping capability, which automatically provides any credit card that was used in the browser and on which site it was used.

Buying someone’s digital identity grants access to a trove of personal data. This means that in addition to financial crime, hackers can buy access to identities based on other nefarious motives. For example, hackers who are conducting corporate espionage can search for internal login pages for specific companies they are targeting. This can be used by intelligence agencies to phish for individuals who have access to various government sites. Even worse, pedophiles can target children’s computers and data by searching for digital identities that visited popular children’s websites. It’s fair to assume that the next phase of these markets will allow users to search for people by name, making these sites very versatile and extremely dangerous.

Protecting Your Organization from Digital Identity Fraud
Since we began monitoring these digital identity sites, we’ve generated more than 1,000 alerts for identities discovered that related directly to our customers. Mitigating the risk of these stolen identities is difficult, as you often can’t trace the identity back to a specific individual—the way you can for leaked credentials, for example. However, there are some steps you can take to better protect yourself and your organization:

- **Continuously monitor digital identity markets:** Visibility and awareness are key to proactive protection. Monitoring these markets can help you identify compromised identities early (for example, to one of your internal login pages), so that you can more diligently monitor traffic to that page and/or increase verification methods when users log in.

- **Enable two-factor authentication:** Asking for a second (or even third) variable for verifying users makes it increasingly difficult for threat actors to hack accounts. This might include mobile verification or providing answers to additional security questions that only the customer or employee will know.

- **Regularly update fingerprinting protocols:** If your company uses digital fingerprinting to verify customers or users, make sure you regularly update these protocols and add additional points of authentication in order to keep up with the stealer’s version upgrades.

- **Consistently clear cookies and browsing history:** Clearing your cookies and browsing history limits the extent of your “digital history” and therefore won’t put additional websites and/or profiles at risk if your device becomes infected.

- **Change passwords regularly:** This is always a cybersecurity best practice, and it certainly applies here as well. Changing passwords and avoiding password reuse both help significantly reduce your risk of compromise.

The digital identities market has brought about a wave of new risks that both organizations and individuals must consider. Threat actors continue to innovate in order to find new ways to gain unauthorized access, steal information, and conduct fraud. Security professionals must monitor the landscape closely to identify these new tactics and take proactive measures to protect their networks, employees, brands, and customers from new forms of cyberattack.
About the Author
Ariel Ainhoren is the Head of Research at IntSights, focused on discovering new cyber trends, threats, hacker strategies, and vulnerabilities. He is a seasoned security professional with over 9 years of experience in the cyber industry, including expertise in computer forensics, malicious programs, cyber intelligence gathering, and investigations. Ariel enjoys riding motorcycles and solving cyber puzzles, preferably byte by byte.

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 open, 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, Singapore, Tokyo, New York, Dallas, and Tel Aviv. learn more, visit: https://www.intsights.com