Cybercriminals shop around for schemes targeting retail

intel471.com/blog/retail-cybercrime-threats-2021

Retail has long been a cornerstone of business on the internet, giving people a convenient way to track down any and every product or service they could possibly want. However, even as subsets of the retail industry — such as dining or hospitality — find ways to leverage the internet to enhance their business, the cybercriminal underground has found ways to attack that growth for their own illegal financial gain.

While top echelon brands have a near cult-like following of customers who have come to know them for their products or services, the cybercriminal underground understands the bigger the company, the bigger portfolio it likely has connected to the internet. Given the underground's ability to either find unprotected systems or get around the security guarding them, criminals know they don't have to attack a retail company's flagship product for their efforts to be profitable.

Intel 471 has observed criminals going after large retail and hospitality companies in a number of ways. Be it trying to attack user accounts, cloud-based infrastructures, or public-facing internet assets, any part of a company's overall portfolio will likely be targeted by a criminal if they feel they can derive value from it. Below are some examples of what Intel 471 has observed when it comes to cybercrime focused on the retail industry.

Rewards programs are a prime target

One such scheme Intel 471 has observed is criminals breaking into retail-associated accounts for their “rewards” points in an attempt to exchange those points for gift cards at various retailers. In March 2019, we observed a Maldivian actor selling access to an international hotel chain’s rewards points in a Discord dedicated to breaking into various online accounts. Upon purchase, the actor would take points out of various accounts and cash them in for Amazon gift cards.

On the low end, access to lists with rewards accounts that held between 14,000 and 75,000 points were priced between $10 and $50. On the high end, access to lists with rewards accounts that held approximately 335,000 to 880,000 rewards points were priced between $200 and $600.

Intel 471 observed several users paying between $50 and $875 for access to points, which were then converted into gift cards.

This actor has an extensive history in account checking, with reputable personas on the CrackingPro and Nulled forums, and provided proof of monetizing the hotel rewards accounts on Amazon. The information received positive comments from multiple actors on the Discord channel.

Access to infrastructure

In September 2020, Intel 471 observed a Russian-speaking actor trying to sell unauthorized access to cloud-based infrastructure they claimed to belong to “one of the most famous hotel chain brands in the world.” The actor allegedly gained unauthorized access to a Microsoft Azure instance operated by the company, along with a management panel catering to about 100 domain names associated with the company’s lines of business.

Due to this access, the actor was able to discern that the company paid millions of dollars for the infrastructure. However, they were unable to do anything beyond edit WHOIS records for various websites; the actor could not tamper with a name server (NS) or start of authority (SOA) records.

Shortly after Intel 471 confirmed this information, the actor claimed the access no longer was available. It was unclear whether the actor sold or lost it at the time of this report.

Cracking creds

In March 2021, Intel 471 observed a long-standing member of the cracked.to cybercrime forum offering account-cracking tools and related services, with one in particular built to target a rewards program.

The actor advertised configuration files for the free penetration-testing tool OpenBullet that would allow an attacker to collect various information from a hotel chain’s rewards program. The actor provided a brief demonstration video to a configuration file targeting the program,

revealing the script made 4,557 checks per minute (CPM) and captured credit card information, reward points balances, and email addresses.

The actor was selling this in a private Discord server alongside a similar OpenBullet configuration file that targeted a multinational credit card company.

Moving money

If cybercriminals aren't dealing with money itself, they often reach for gift cards as their next best option. Whether it be physical cards or solely online credits, the underground has long used gift cards as a conduit to move money.

The buying, selling and trading of gift cards is still prevalent in 2021. While cards tied to high-end multinational retailers have always moved through underground forums, the actors involved are new, using the gift card trade to find a footing in the cybercrime underground.

In September 2020, Intel 471 observed one such newcomer on a Turkish-language cybercrime forum sharing a tactic that would allow someone to use compromised PayPal accounts on an United Arab Emirates (UAE)-based website where users can buy online gift cards. The method involved manipulating cookies, disguising IP addresses and using various HTML codes to bypass security protocols used by the website. The method also worked on two Turkish retail sites that sell gift cards and other goods.

The actor requested 200 Turkish lira (about US $25) for access to this method.

Criminals value video games

A more seasoned actor who has a presence on multiple well-known cybercrime forums has made a name for himself in the past few months by buying and reselling gift cards and video game keys. Intel 471 observed this actor holding a presence on over 10 cybercrime forums, advertising that he would buy cards and keys for 65 percent to 85 percent of their value to resell them through other platforms.

The actor said he was looking for cards tied to well-known e-commerce and app stores, and keys tied to e-commerce sites that serve both PC and console gamers, as well as stores run by game developers.

Big stashes for cash

In February 2021, an actor Intel 471 has been tracking for several years offered to sell 895,000 gift cards issued by more than 3,000 companies that included well-known brands in clothing, online retail, transportation and technology sectors, among others. The actor aimed to sell the entire database for US $20,000, even as the gift cards' value allegedly amounted to more than US $38 million. The actor also expressed willingness to consider offers by other actors to monetize the database for a share of profit.

After testing some of the accounts, the actor amended the offer, claiming many of the gift cards were invalid. After the change, the actor expressed readiness to provide a sample from the database to test and showed a willingness to negotiate the price with a prospective buyer.

Retail's ransomware threat

Ransomware is a top threat for all internet-connected businesses. Retail is no different.

Over the past year, Intel 471 have observed numerous retailers or third-party partners falling victim to ransomware attacks. These incidents have all the hallmarks of other ransomware attacks: systems locked, data exfiltrated, and business operations left crippled or shut down altogether.

In November 2020, South Korea-based conglomerate E-Land Group was hit with CLOP ransomware, forcing the company to shut down a portion of its corporate network, along with 23 of its 50 physical retail locations. The attackers told media outlets that they had been in the system for nearly a year, gathering data on customers that they would eventually take for themselves. Intel 471 discovered in December that the operators took and released Track 2 payment card data, which other threat actors could use to produce fake credit cards.

Operators pulled off this attack by taking advantage of vulnerabilities in the Accellion file transfer appliance (FTA) software, which has been linked to a series of high-profile compromises including the Singaporean telecom company Singtel, U.S. law firm Jones Day, and U.S. grocery store chain Kroger. CLOP reportedly used this flaw to also go after U.S. railroad company CSX Corp. and multinational tech company Qualys.

Supply chain in the crosshairs

Intel 471 has not only observed direct attacks on retailers, but also those that hit companies tied to their supply chain. In April 2020, operators of the NEIFILIM ransomware variant attacked Sri Lankan lingerie and apparel manufacturer MAS Holdings, which makes various clothing items for highly-known brands around the world. The operators leaked 9 GB data on their leak blog, claiming that they stole around 300 GB in total.

While the attack was launched in April, operators were likely inside the MAS Holding's systems for weeks prior to the ransomware being launched. Intel 471 observed an actor selling access to the company's network in March 2020.

Another company — U.S.-based packaging company Westrock — was attacked by operators of DarkSide ransomware in January 2020. In an investor note released by the company a week after the incident began, Westrock said it had shut down certain systems "in an abundance of caution" and shipments from some of the company's facilities "lagged" behind normal production levels. That may have partly been due to the company's negotiations with operators: Intel 471 observed a DarkSide representative tell Westrock that

the group retained access to the company's network and continued to encrypt data on the servers, even during negotiations. In all, the ransomware operators allegedly attacked two local domains that hosted more than 500 databases and backup servers with more than 1.2 PB of data.

Conclusion

So much of retail business depends on the internet, especially given that consumers have depended on online-only options during the COVID-19 pandemic. That has forced retail companies to embrace more of a technology-driven business profile, which then leads to more of their business needing to be as secure as possible. As long as this continues to be the trend, cybercriminals will look for vulnerable targets, hoping to siphon money away from businesses that have not taken the right security precautions. It's imperative that security teams understand what schemes are proliferating on the cybercrime underground and compare it against their own security posture in order to proactively defend against their business and customers falling prey to these various schemes.