CEQUENCE SECURITY

Threat Advisory: High Volume Bot Traffic from IPVanish VPN Against Retailers

TL;DR

- A spike in malicious bot traffic with similar characteristics across more than 20 customers emanating from the same VPN vendor and its affiliated companies.
- Between July 21st and August 4th, average daily bot traffic from IP addresses owned by IPVanish, Highwinds Network Group, StackPath Data Center, Netprotect, Reliable Hosting, Inc. and Overplay.com increased 28X to an average of 700K transactions daily, spiking at 1.8M per day.
- Attacks are primarily account takeovers with the end goal of gift card and loyalty points fraud against retail customers.

Recommendations

- Retailers should monitor login and gift card balance APIs for any increase in traffic from the organizations mentioned above and the following Autonomous System Numbers (ASNs): 12989, 33438, 62651, 22781, 11588, 13926. Block based on organization and ASN as necessary.
- Those not in the retail industry should take note, looking for suspicious traffic from these organizations and associated ASNs.
- Security analysts should also ensure that User-Agent (UA) strings like Googlebot are not allow-listed based solely on UA, as that provides attackers an added mechanism to hide in plain sight.

Details

Threat actors have a range of mechanisms at their disposal to mask their identity and location. One approach recommended in some of the bot forums is to use a VPN provider like IPVanish. These commercial VPN services help legitimate users use the web more securely. Those same features allow threat actors to mask identity and location across a global network and in the case of IPVanish, with no cap the number of simultaneous connections, they are an ideal infrastructure to use for executing an automated attack, as described in this threat advisory. Image 1 shows the volume of transactions generated during the recent spike and the number of IP addresses used.

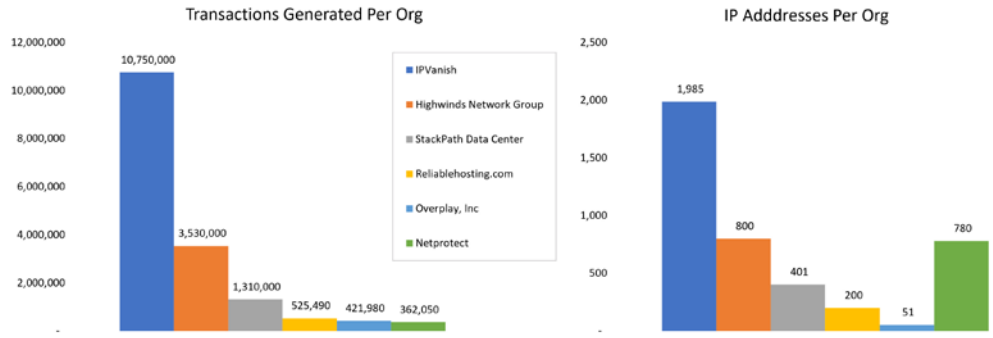

Image 1: Transaction and IP address distribution across different organizations.

The legitimate use of these VPN services makes the "block or not?" security decision difficult. Prior to the spike observed on July 21, usage patterns from these organizations within our customer base were either benign, or limited to periodic, relatively targeted (and mitigated) attack bursts.

As shown in image 2, on July 21st threat actors drove a 57X traffic spike to 1.44M daily transactions reaching a high of 1.87M per day on August 4th.

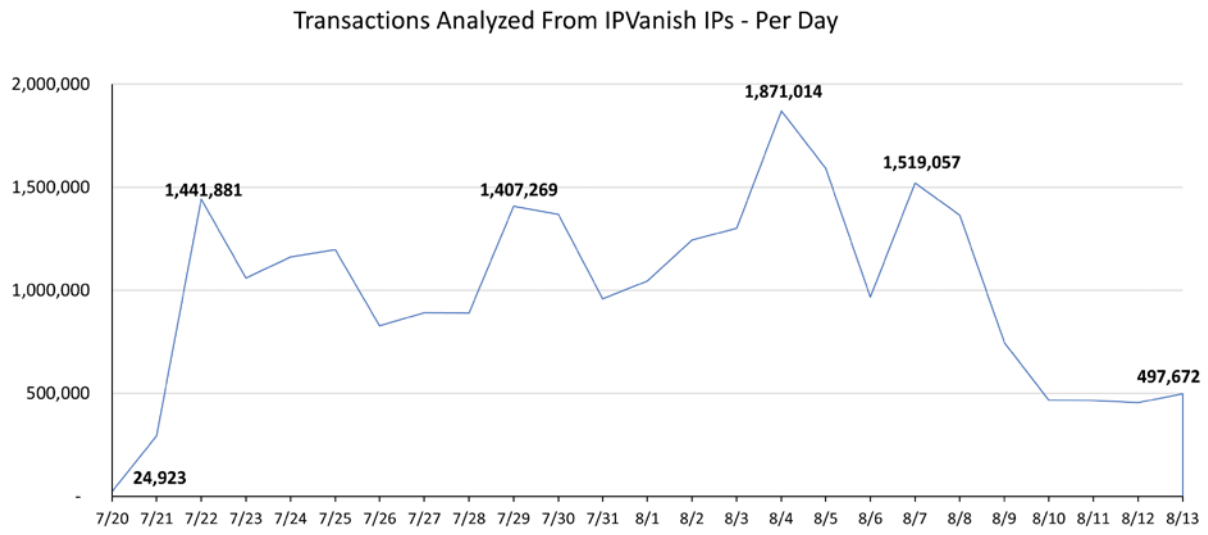

Image 2: Daily transactions from IPVanish and related organizations.

Retail Gift Card and Loyalty Points Programs Targeted

Traffic flowing through these organizations' IP addresses attacked as many as 15 different customers across multiple industries. However, more than 99% were targeted retailers with popular gift card and loyalty programs. Continuing the trend seen over the past year, threat actors continue to target APIs as opposed to web apps, with 90% of all attack traffic funneled through APIs.

Industry	Transactions Analyzed	% of Total
Retail/E-Tailer/E-Commerce	16,098,621	99.6%
Romance/Relationship	35,425	0.2%
Financial Services	18,410	0.1%
Digital Media	3,689	0.0%
	16,156,145	100.0%

Attacks and Characteristics Observed

While the attacks were seen in multiple industries, the focus was on retailers specifically to execute ATO and gift card fraud as described below.

- **"Scrape and Sell" gift card abuse:** The attackers are using a bot to commit account takeover, log into the compromised accounts and request gift card balance information from the profile APIs. This information would then be resold later on the market for future abuse.
- **"Steal and Purchase" gift card abuse:** The attackers used a bot to commit account takeover, using the compromised account to purchase goods, paying for them with the value extracted from the gift card. In some cases this appeared as attackers using loyalty points to then purchase more gift cards, which were then redeemed for goods.
- **Shopping bot gift card abuse:** Attackers used a bot to execute a shopping journey faster than a competing human, and then during the checkout phase attempt to enumerate possible gift card numbers against a separate API, applying any valid numbers to the checkout.

Unique characteristics used to evade defenses:

- **Masking themselves as a Googlebot:** In some cases, the threat actors tried to mask themselves as a Googlebot by modifying the user agent string to Googlebot/2.1 (http://www.google.com/bot.html). Security analysts should review Googlebot Documentation and observe the characteristics of legitimate Googlebot traffic. For instance, it is coming from "Google Cloud", "Google Partners", "Google inc.", etc. by DNS ISP or Organization name records. Analysts should also ensure that Googlebot User-Agent strings are not whitelisted by default.
- **Using nurtured or fake accounts:** In other cases, attackers used a set of fake accounts that have been harvested over time. As these accounts were often created by the attackers themselves, the patterns don't appear like account takeover, as they always log in successfully. These nurtured accounts can later be sold, or used as mule accounts to execute any purchases/transactions on the site.

Global Distribution

The transactions observed emanated from more than 20 locations, distributed across all six of the providers mentioned. Patterns observed include:

- The primary country of origin was the U.S. with 69% or 11M of the 16M transactions analyzed.
- The largest attack observed targeted a large retail organization with traffic distributed across all 6 organizations, originating from 15 countries.
- Across all customers that were under attack, traffic was distributed across 11 global locations.

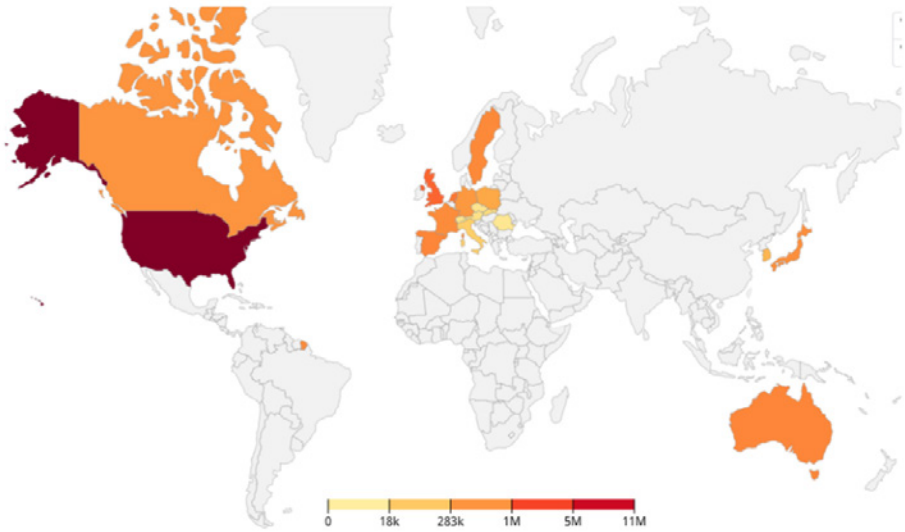

Image 3: Global distribution of transactions analyzed.

As most of the IPVanish exit nodes are geolocated in commonly used countries like the US and the UK, the recommendation for security analysts is to use geo-location only as a datapoint. Monitoring these organizations and executing any blocks should be done based on ASN data and CIDR ranges to maximize effectiveness and avoid false positives.

Summary

The data and attack patterns described are intended to provide retail security and fraud teams with usable threat intelligence that may be impacting their own environment. As with any recommendation to block traffic, appropriate analysis should be applied to ensure legitimate users are not prevented from using the application of services.