Chinese Scam Shops Lure Black Friday Shoppers

geminiadvisory.io/chinese-scam-shops/

November 19, 2020

Key Findings

Since the COVID-19 pandemic began, fraudsters have looked for ways to turn the tragedy to their advantage through e-commerce scams, SBA loan and stimulus fraud, and COVID-19 related malware. Now, with Black Friday around the corner, scam shops are looking to cash in on alluring discounts targeting online shoppers.

e-Commerce scam shops operate as follows: the fraudsters create an online shop to advertise and sell their goods, collect customers' payment card data and personally identifiable information (PII) as they unknowingly purchase faulty, counterfeit, or nonexistent products, and then sell that customer data on dark web marketplaces.

US and European banks have experienced a spike in e-commerce fraud linked to China-based sites registered to the Chinese Registrar ename[.]net. Almost 200 of the nearly 600 scam sites identified by Gemini were linked to the Chinese acquiring bank Jilin Jiutai Rural Commercial Bank Co., Ltd.

Gemini Advisory has identified one group of China-based e-commerce fraudsters contributing to this spike that operates hundreds of scam sites and has exposed tens of thousands of US and international payment card records and individuals' PII over the past six months. The full list is available upon request.

Background

Since the COVID-19 pandemic began, fraudsters have looked for ways to turn the tragedy to their advantage through e-commerce scams, SBA loan and stimulus fraud, and COVID-19 related malware. e-Commerce fraudsters selling fake medical products, for example, appeared almost immediately after the pandemic began while hackers circulated interactive COVID-19 tracking maps infected with malware. As the pandemic progressed, cybercriminals exploited the US government's efforts to help struggling businesses and citizens by fraudulently procuring SBA loans and stimulus checks. Likewise, e-commerce fraudsters, recognizing the profits gained from selling fake medical products, leveraged the public's reduced willingness to shop at brick-and-mortar stores to expand into the sale of popular retail merchandise, such as clothing, shoes, handbags, kitchenware, toys, and recreational goods.

More recently, Gemini learned that both US and European banks were experiencing a spike in e-commerce fraud linked to China-based sites registered to the Chinese Registrar ename[.]net. Based on the common link and an analysis of the sites' past activity, Gemini analysts assess with moderate confidence that these China-based domains were not infected through Magecart attacks, but were actually malicious sites themselves that stole payment card data from unwitting shoppers and then sold that data across various dark web marketplaces.

Now, with major stores already signaling they will be closed on Black Friday, these scam shops appear poised to take advantage of millions of shoppers expecting bargains but forced to turn to online shopping. Many of the scam shops pay for ads on Google and Facebook that aim to catch shoppers' eyes with claims of wild discounts and everything must go, going-out-of-business sales. Though online shoppers may be wary of deals that appear too-good-to-be-true under normal circumstances, Black Friday gives scam shops the chance to push advertising into overdrive and target online shoppers while their guard is down.

How Large-Scale e-Commerce Scam Shops Operate

Gemini Advisory has identified one group of China-based e-commerce fraudsters contributing to the spike identified by US and European banks. The group operates hundreds of scam sites and has exposed tens of thousands of US and international payment card records and individuals' personally identifiable information (PII) over the past six months. A list of 50 of these sites can be found in Appendix A, while the full list of these nearly 600 sites is available upon request. The tactics, techniques, and procedures (TTPs) of the group reveal how similar groups operate and provide insights into how they can be identified.

The underlying premise of these e-commerce scams is simple: the fraudsters create an online shop to advertise and sell their goods, steal customers' payment card data and PII, and then sell the data on dark web marketplaces. As a result, e-commerce scams have garnered particular interest from fraudsters as they allow them to earn a double profit: first

from selling counterfeit, faulty, or nonexistent products to customers, and second from selling stolen payment card data and PII to cybercriminals. In the context of the criminal group identified by Gemini, analysts determined the group likely recorded profits upwards of $500,000 in the past six months just from the sale of the stolen payment card data and PII on the dark web. However, the total criminal profits are likely significantly larger based on their illicit sale of faulty, counterfeit, or nonexistent goods.

The China-based e-commerce fraud groups, including the group identified by Gemini, follow the same pattern except they operate on a large scale with hundreds of sites. Once they have their sites up and running, some of these groups work to expand their sites' exposure by building a parallel presence on Facebook.

Network of Scam Sites

e-Commerce fraud groups attempt to ensnare as many victims as possible by creating a large number of scam sites offering different products for specific customers. Each site is typically linked to a unique merchant name and merchant identification number (MID) to further obscure the link between them. Registering a new MID, however, is a complex process that requires either a direct partnership with an acquiring bank or a relationship with a third-party merchant company that works with a dedicated acquiring bank. Both of these organizations are responsible for processing credit or debit card payments on behalf of the merchant. Gemini determined that nearly 200 of the scam sites from the identified group were linked to the Chinese acquiring bank Jilin Jiutai Rural Commercial Bank Co., Ltd. It is unclear, however, whether these sites' relationship with the bank was direct or managed through a third-party merchant company.

For the average customer, there is no visible link between the different sites within the network as each appears to be a distinct, legitimate shop. The sites use Google Ads and social media advertisement campaigns to attract customers with offers for products at a discount below market deals. The sites' advertisements almost always indicate that the deals are part of a limited-time sale to pressure potential customers into making a purchase. Gemini witnessed other, unrelated scam sites claim they are going out of business due to the COVID-19 pandemic and thus offering products at a steep discount to negate customers' suspicion that the deals may be too good to be true.

Gemini analysts suspect that e-commerce fraud groups are moving away from the more popular and more secure e-commerce platform Shopify and towards OpenCart because OpenCart is open source. This move allows fraudsters to avoid Shopify's documented practice of monitoring for fraud and remediating fraudulent transactions. The group identified by Gemini, for example, used OpenCart as its e-commerce platform and relied on Cloudflare to hide its IP addresses for all of its sites. This cookie-cutter approach was likely taken to facilitate the rapid deployment of a large number of scam sites.

The identified group also resorted to recycling nearly identical text for the About Us sections across the hundreds of sites while using the same seven templates with slight variations in how they presented menus, navigation links, and other information.

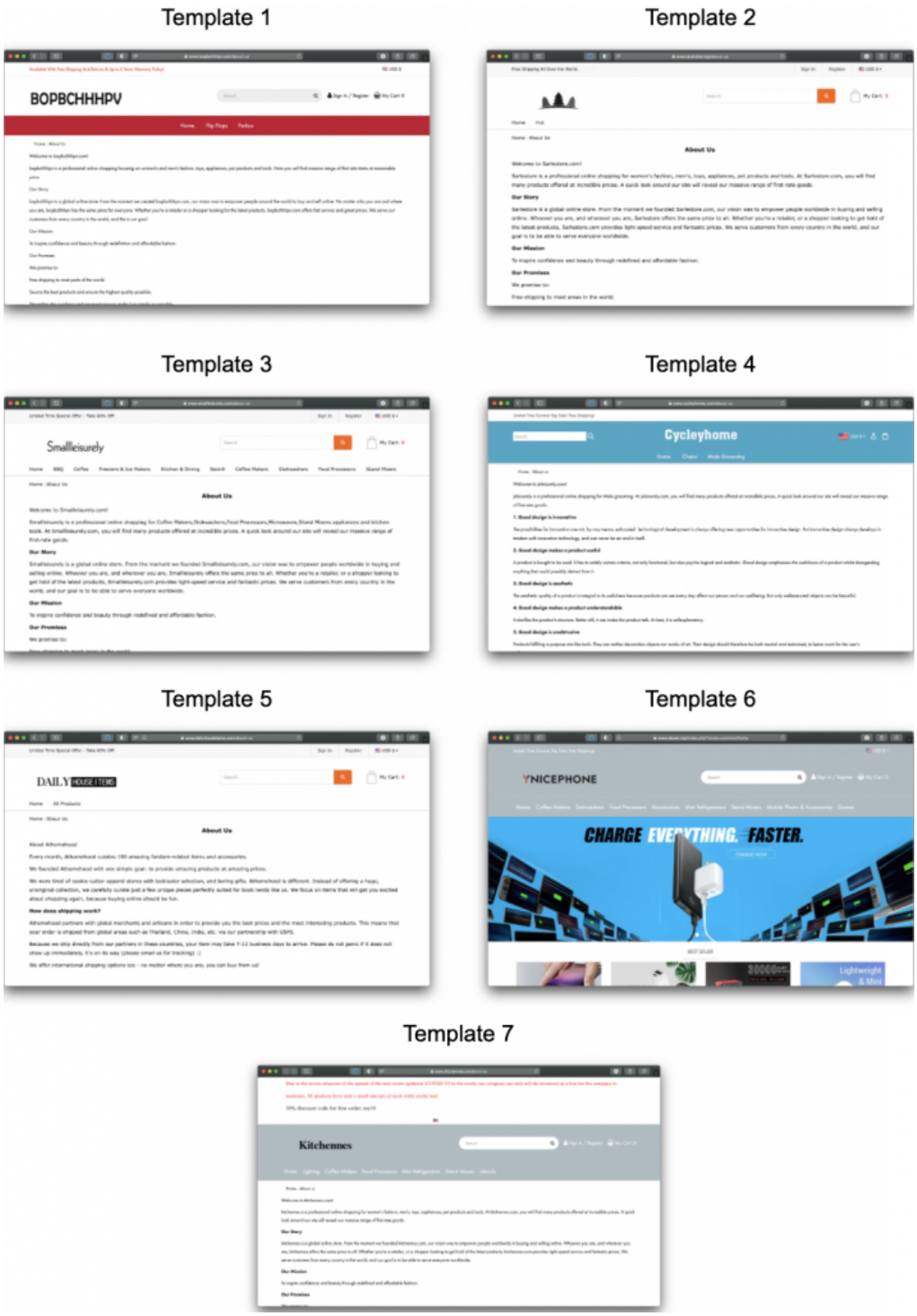

Image 1: The seven website templates used by the scam merchants.

In a similar manner, the group applied an overlapping set of Google Analytics Tracking and Facebook Pixel IDs across the scam sites. Google Analytics codes use tracking IDs with an alphanumeric string to allow an Analytics account to identify where to send data. The

Facebook Pixel codes are used to report conversions, build audiences, and gain insight about a site's users.

While the e-commerce fraud group sped up deployment by replicating processes across the scam sites, these similarities also gave Gemini analysts some of the indicators they needed to connect the scam sites to the criminal group. The formulaic templates and text, for example, raised suspicion while the overlapping Google Analytics Tracking and Facebook Pixel IDs created links between otherwise disparate sites.

Multi-Platform Presence

Like any good business, e-commerce fraudsters know that the key to success is strong marketing. To this end, groups look to build a presence across multiple platforms to build their sites' exposure and attract more customers. The group identified by Gemini, for example, has been recently making forays onto Facebook by launching pages that advertise products and include a link to the corresponding scam site. In keeping with the practice of recycling content, the scam sites and corresponding Facebook pages contained identical About Us sections. Of note, Gemini analysts observed a lag time between when the scam sites were launched and the creation of each site's corresponding Facebook page, which may indicate that this is a new tactic being deployed by the identified group.

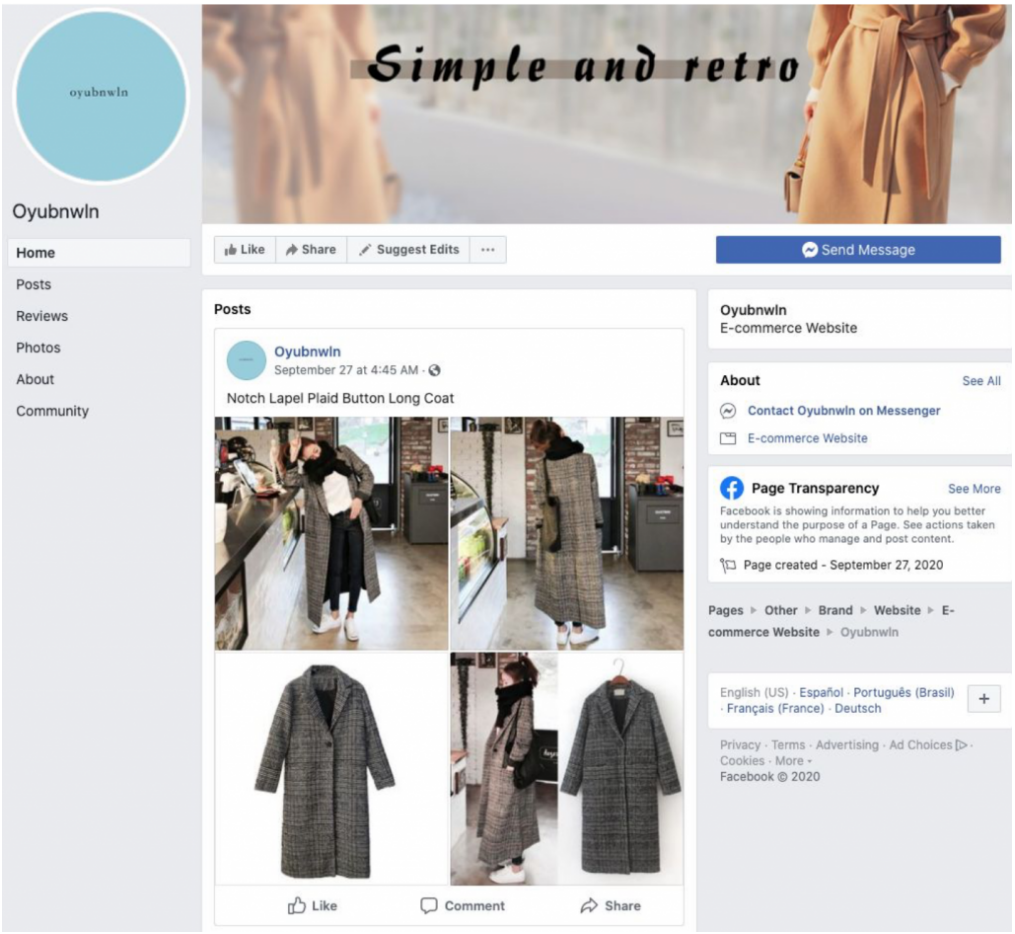

Image 2: One of the scam merchant's Facebook pages created on September 27, 2020.

Sale of Customer Payment Card Data and PII

Beyond often selling counterfeit, low-quality, or nonexistent products, e-commerce scammers steal the card payment data and PII of customers and then sell this data on the dark web marketplaces. The group identified by Gemini, for example, stole customers' payment card data, cardholder and billing information, and additional PII, such as the phone number. Cybercriminals purchase this type of payment card data to perform a range of fraudulent activities and could potentially combine the information with the full phone number to conduct tailored phishing attacks.

It is also important to note that these e-commerce scam sites are distinct from sites infected by Magecart attacks, a rising category of e-commerce fraud previously reported on by Gemini. For e-commerce scam sites, the fraudster has created the site and then intentionally injected a malicious script into that site; the script skims customers' payment card data and PII. For Magecart attacks, a cybercriminal injects malicious script into an external e-commerce site without the owner of the site being aware.

Conclusion

As the COVID-19 pandemic has driven more customers to purchase products online and governments to implement stimulus programs, fraudsters have capitalized on the opportunity by ramping up and complexifying their forms of fraud. Now, with Black Friday, holiday shopping, and a tight economy added to the mix, scam shops are eyeing a unique opportunity to concentrate advertising toward a large demographic of shoppers in search of discounts but less accustomed to the dangers of online shopping.

More broadly, the spike in fraud linked to China-based sites witnessed by US and European banks and identified by Gemini represents one only instance of cybercriminals adapting operations to the unusual, changing circumstances driven by the pandemic. Gemini analysts, for example, are already witnessing cybercriminals increase their interest in travel services fraud as governments begin to roll back travel restrictions. Ultimately though, due to the scale and evolving nature of the e-commerce scam sites, Gemini analysts assess with a high degree of confidence that the criminal group behind the sites will likely continue to steal and sell payment card data and PII on dark web marketplaces.

Appendix A

List of 50 scam domains identified by Gemini Advisory. The full list of nearly 600 domains is available upon request.

List of Scam Domains

dzxybmq[.]com	pkpauyg[.]com	xpqszyi[.]com	bxwzhs[.]club	okayep[.]com
ejgvriw[.]com	pviqyhh[.]com	xudnall[.]com	fazdht[.]shop	timeswake[.]com
ezmbzps[.]com	qkpxekr[.]com	zmcpqki[.]com	gzxdhk[.]club	topshipy[.]com
gdqzykg[.]com	rkaszfs[.]com	easybue[.]com	hiugou[.]club	morewanter[.]com
lqcjidt[.]com	rvsdhca[.]com	homeuclub[.]com	jwfang[.]club	asmater[.]com
lvvxfqb[.]com	rxaznbf[.]com	nbhjo[.]com	hnhggc[.]shop	costhelpercom[.]com
nkvbgwr[.]com	sptizar[.]com	prfetv[.]com	nicequity[.]com	dayscomp[.]com
ntpdcnl[.]com	tlxvjxc[.]com	yxxkan[.]com	inpopcolor[.]com	geospreader[.]com
osjqowb[.]com	wdeatuz[.]com	hawjwl[.]shop	intopopular[.]com	healshopping[.]com
pcrrowr[.]com	wlxmxch[.]com	apidh[.]shop	inlute[.]com	keepfunning[.]com

Gemini Advisory Mission Statement

Gemini Advisory provides actionable fraud intelligence to the largest financial organizations in an effort to mitigate ever-growing cyber risks. Our proprietary software utilizes asymmetrical solutions in order to help identify and isolate assets targeted by fraudsters and online criminals in real-time.