Kaspersky Lab warning: popular online fashion shops among top targets for data stealing malware in 2018

As the big annual holiday shopping season gets underway, new Kaspersky Lab research shows that banking Trojans are actively targeting online users of popular consumer brands, stealing credentials and other information through these sites. Kaspersky Lab technologies detected 9.2 million attempted attacks by the end of Q3, 2018, compared to 11.2 for the whole of 2017, with detections for one malware family up by 34%. Half all online shops attacked were well known consumer apparel brands including fashion, footwear, gifts, toys and department stores. Online shoppers in Italy, Germany, the US, Russia and emerging markets appear to be particularly at risk.

Traditionally, banking Trojans target mostly users of online financial services, looking for financial data to steal, or building botnets out of hacked devices for future attacks. Over time, several of these banking Trojans have enhanced their functionality and reach to target the data and credentials of online shoppers, and obtain root access to their devices.

The main malware families stealing from victims through e-commerce brands are Betabot, Panda, Gozi, Zeus, Chthonic, TinyNuke, Gootkit2, IcedID and SpyEye (where detections are expected to be up 34% on 2017). The Trojans target well known e-commerce brands to hunt for user credentials like login, password, card number, phone number, and more. They seize the data from victims by intercepting input data on target sites, modifying the online page content, and/or redirecting visitors to phishing pages.

The main findings of the research report include:

• Half (50%) of the brand names targeted by the malware families detected are established high street labels, including fashion, footwear, jewelry, gifts, toys and department stores, followed by consumer electronics brands (12%) and entertainment/gaming (12%).

• Overall, the research found 14 malware families targeting a total of 67 consumer e-commerce sites, which include 33 consumer apparel sites, eight consumer electronics sites, eight entertainment and gaming sites, three popular telecoms sites, two online payment sites, and three online retail platforms, among others.

Of these:
– Betabot was found to be targeting 46 different brands, including 16 different consumer apparel brands, four consumer electronics brands and eight entertainment/gaming brands; with most of those affected in Italy (14.13% of users affected by any malware were targeted by this threat), Germany (6.04%), Russia (5.5%) and India (4.87%).

– Gozi was found to be targeting 36 brands, including 19 consumer apparel and three consumer electronics brands; with most of those affected in Italy (19.57% of users affected by any of malware), Russia (13.89%), Brazil (11.96%) and France (5.91%).

• Over three million sets of e-commerce credentials were found up for sale on a marketplace easily accessible through the Google search engine. The highest prices are charged for what appear to be hacked merchant accounts.

"Credential-stealing banking malware is nothing new. However, the existence of families hunting for data related to online shopping accounts is perhaps more unexpected. If your computer is infected with one of the listed Trojans, then criminals are able to steal payment card details while you enter them on the shop's website. After that, it is easy for a hacker to get to your money through a compromised credit card. Cybercriminals could also use the stolen accounts in money laundering schemes: buying things from a website using victims' credentials so they look like known customers and don't trigger any anti-fraud measures, and then selling those items on again. As we come into the busiest online shopping season of the year, we urge consumers and retailers to be extra vigilant about their security, and to check and double check the integrity of websites before entering or downloading any data." said Yury Namestnikov, principal security researcher, Global Research and Analysis Team, Kaspersky Lab.

Kaspersky Lab recommends the following steps to stay safe when shopping online:

If you are a consumer

- A powerful, updated security solution is a must for all devices you use to shop online. Avoid buying anything online from websites that look potentially dangerous or which resemble an incomplete version of a trusted brand's website.
- Don't click on unknown links in email or social media messages, even from people you know, unless you were expecting the message.

If you are an online brand or trader

- Use a reputable payment service and keep your online trading and payment platform software up-to-date. Every new update may contain critical patches to make the system less vulnerable to cybercriminals.
- Use a tailored security solution to protect your business and customers.
- Pay attention to the personal information used by customers to buy from you. Use a fraud prevention solution that you can adjust to your company profile and the profile of your customers.
- Think about how much money you wish to keep in an online payment transaction account at any one time. The greater the balance, the higher the value of that account to hackers.
- Restrict the number of attempted transactions and always use two-factor authentication (Verified by Visa, MasterCard Secure Code and etc.).

The research is based on data obtained with user consent and processed using the Kaspersky Security Network (KSN). All malware belonging to the banking Trojans covered in the report are detected and blocked by Kaspersky Lab security solutions.