KASPERSKY lab

Buyer beware: cyberthreats targeting e-commerce, 2018

November 2018

KASPERSKY lab

Contents

Introduction

Caveat emptor (“buyer beware”) is the principle that it is the buyer's responsibility to spot if there is anything wrong with what they are being sold. This principle has been applied for centuries and it remains valid in the digital world. In cyberspace things aren’t always what they seem: hackers have become highly skilled at mimicking or compromising trusted websites to trick users into sharing or granting access to personal or financial information, among other things.

The malware used, known as banking Trojans, target victims through a range of channels, such as email, pretending to be their bank or payment service. Online, this often involves the use of fake websites, with malicious links or content that downloads automatically to the unsuspecting visitor.

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, launching new variants and extending their range. Some are now able to obtain root access to infected devices, perform transactions, inject other malicious code, record video, and more. And the victims of such malware are not just people who bank online but online shoppers in general.

As the world heads into the busiest shopping season of the year, with an increasing number of people shopping online and on mobile, it likely that malware will also be out in force. We decided to take a closer look at Trojans targeting online shoppers in recent years, in order to raise awareness among consumers and online brands of the potential threats they could face.

This report looks at some of the main banking Trojan families targeting users of e-commerce brands. It summarises their activity and the geography of attacks, and also looks at where the stolen information might end up. It concludes with advice and recommendations on how to stay safe from Trojan attacks while shopping online.

Methodology and key findings

This overview is based on data obtained and processed using Kaspersky Security Network (KSN). KSN integrates cloud-based technologies into the company’s personal and corporate products and is one of Kaspersky Lab’s most important technologies. The statistics in this report are based on anonymous data obtained from Kaspersky Lab products installed on users’ computers around the world and was acquired with the full consent of the users involved.

Key findings

- The latest generations of banking Trojan malware families make widespread use of mainstream e-commerce brands to steal data from infected victims. According to Kaspersky Lab data, 46 different brands are used by Betabot, 36 by Gozi and 35 by Panda; with a number of brand names being used for attacks by several families (in particular, Betabot, Panda and Gozi).

- 50% of the brand names used by the malware families are those of well-known fashion, footwear, jewelry, gift and toy retailers, as well as department stores, and include luxury brand names.

- In 2018, malware attacks to steal data through e-commerce brands were particularly active in European countries, including Italy, Germany and France as well as in North America, Russia and emerging markets.

- 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.

Main malware families targeting users of e-commerce brands in 2018

Overall results

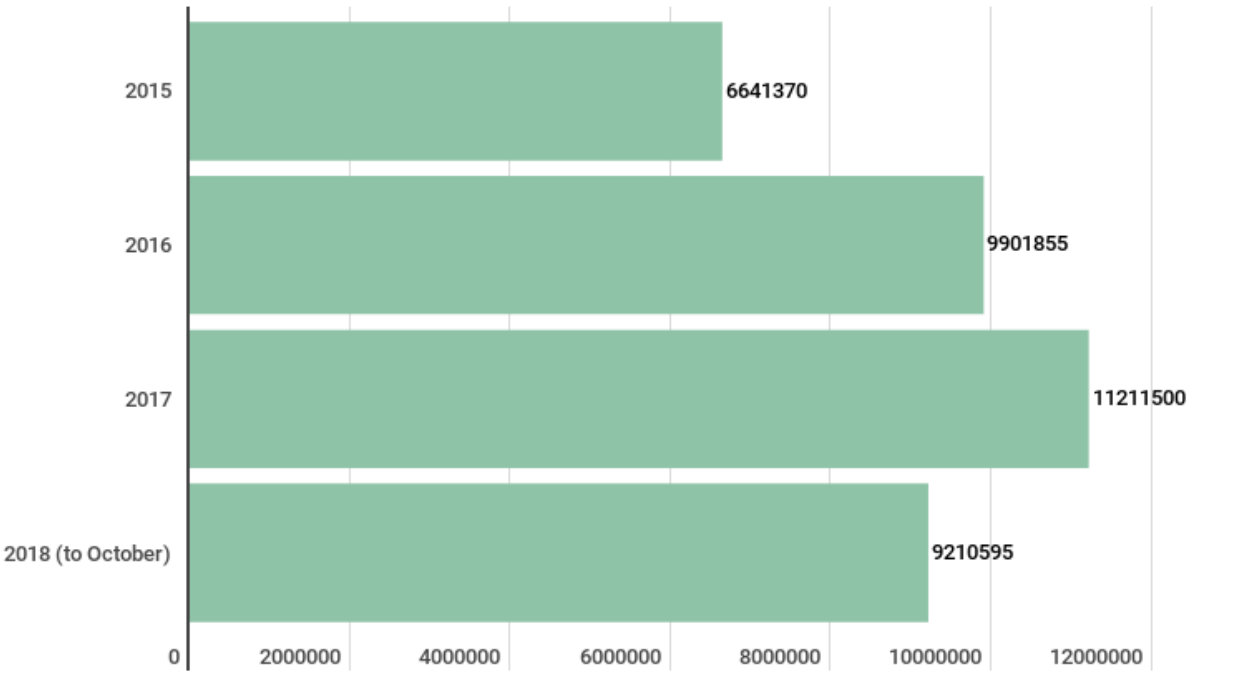
According to Kaspersky Lab data, the main malware families using e-commerce brands to steal from victims are Betabot, Panda, Gozi, Zeus, Chthonic, TinyNuke, Gootkit2, and IcedID. They are all banking Trojans. Banking Trojans are best known for targeting users of online financial services to steal money and build botnets of victim devices. In recent years, many such Trojans have expanded their capability to steal other information, and have extended their target range accordingly.

The overall number of detections for the malware families' e-commerce brand activity has increased steadily in the last few years, from 6.6 million in 2015 to an estimated 12.3 million by the end of 2018 (based on the extrapolation of a detection number of 9.2 million at the end of Q3, 2018), with a 12% increase between 2016 and 2017, and a 10% expected rise between 2017 and 2018.

Attack method

The Trojans are using the e-commerce brands to hunt user credentials like login, password, card number, phone number, and more. In order to do so, the malware can intercept input data on target sites, modify online page content, and/or redirect visitors to phishing pages.

For example, the Trojans enable the cybercriminals behind them to monitor users' online behavior: tracking which sites are visited on the infected device. If the Trojan spots the user browsing to a target e-commerce website, it activates its form-grabbing functionality. 'Form grabbing' is a technique used by criminals to save all the information that a user enters into forms on a website. And on an e-commerce website, such forms are almost certain to contain: login and password combination as well as payment data such as credit card number, expiration date and CVV. If there is no two-factor transaction confirmation in place, then the criminals who obtained this data can use it to steal money.

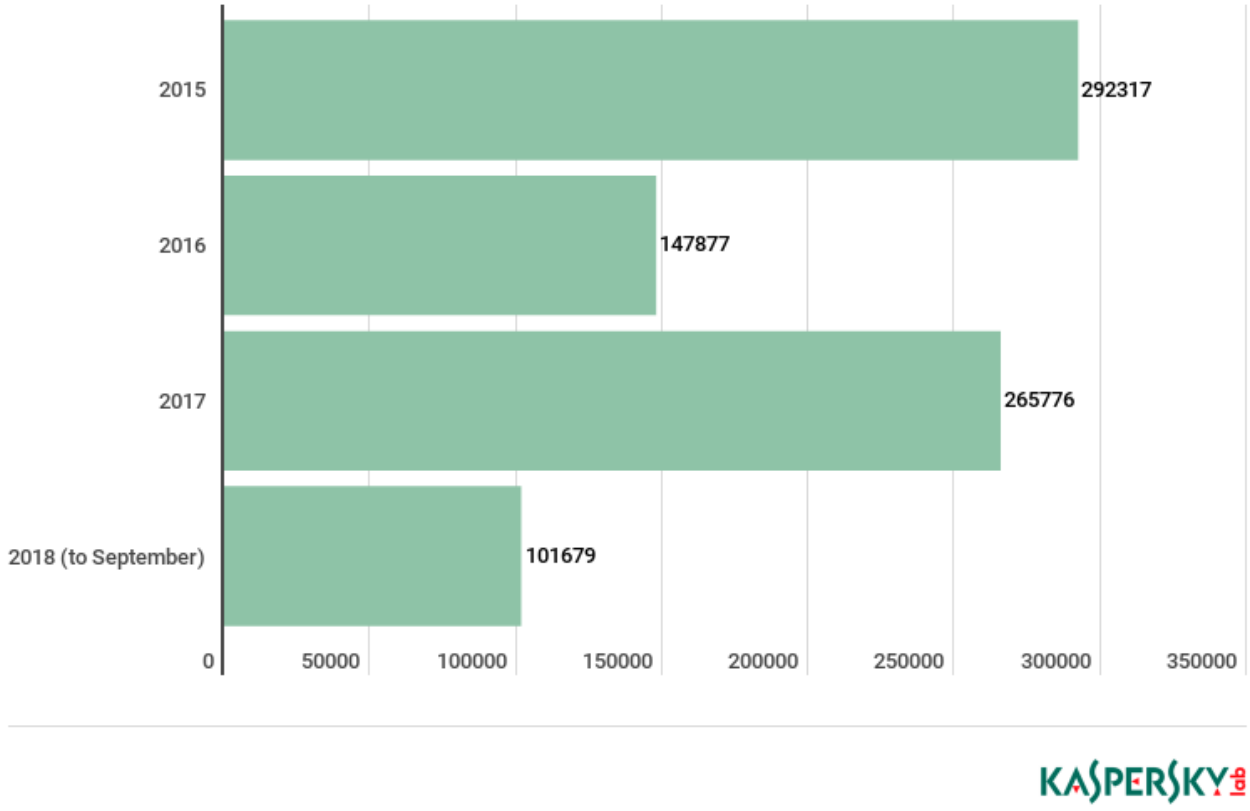


Overall detection data for main malware Trojans targeting users of e-commerce brands, 2015 – 2018. Source: KSN

Betabot

Betabot is a dangerous Trojan known since 2013. Among other things, Betabot attempts to prevent victims from accessing security websites while also disabling their antivirus and malware scan software. It achieves this by asking users to give it access control of the device so that it can make administrator-level changes. These changes include the necessary modification to disable security access and steal information.

After peaks in 2015 and 2017, the number of e-commerce-related attacks by this malware appear to have fallen in 2018 (year-end estimates based on numbers to the end of August are just over 152,500 total detections). However, it remains a significant threat, targeting the widest range of different e-commerce brands – 46, according to our research – and being difficult to dislodge from compromised devices because of its root access.



Detection data for the Betabot malware family targeting users of e-commerce brands, 2015 – 2018. Source: KSN

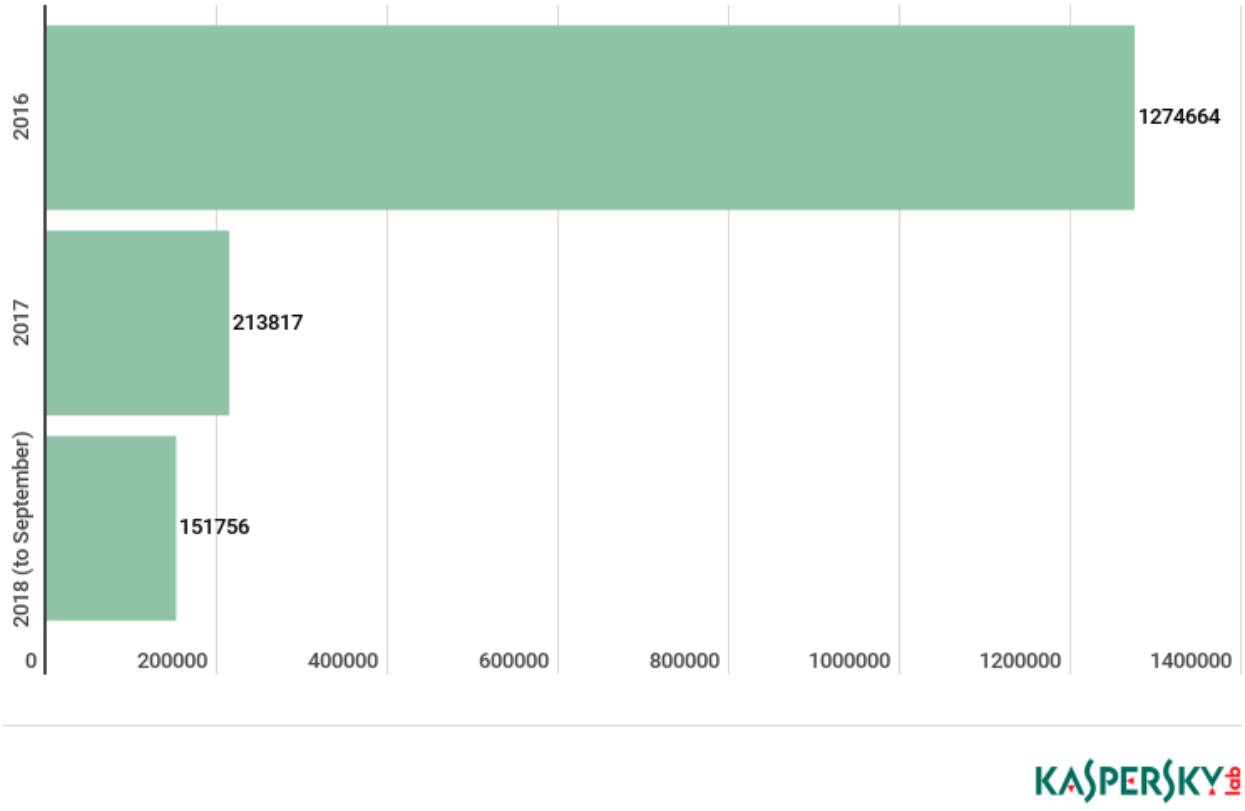
Betabot appears to be a particularly active threat for online shoppers in Europe. Kaspersky Lab detection data shows that the vast majority of users affected by this threat in the first eight months of 2018 are based in Italy (14.13% of all users who encountered malware, were targeted by this threat) and Germany (6.04%), followed by Russia (5.55%) and India (4.87%).

Country	% of users affected by any malware who were targeted by the Betabot malware family through e-commerce brands in Jan-Aug 2018
Italy	14.13
Germany	6.04
Russia	5.55
India	4.87

Vietnam	3.92
Hong Kong	3.46
United Arab Emirates	3.13
Taiwan	2.84
Turkey	2.81
Algeria	2.62

Gozi

The Gozi banking Trojan was first discovered in January 2007. It is an advanced modular malware spread through browser exploits. Gozi's source code was leaked online in 2010, and was quickly repurposed by hackers for other uses. The 2013 version of this malware included a rootkit that can survive a reinstallation of the OS, and in 2016 a man-in-the-browser variant was found that allowed the attackers to monitor victim activity through the latest browser. Although the estimate for 2018 is unlikely to achieve the peak of 2016, total detections based on data to the end of August could be around 227,634, up about 10% on 2017.



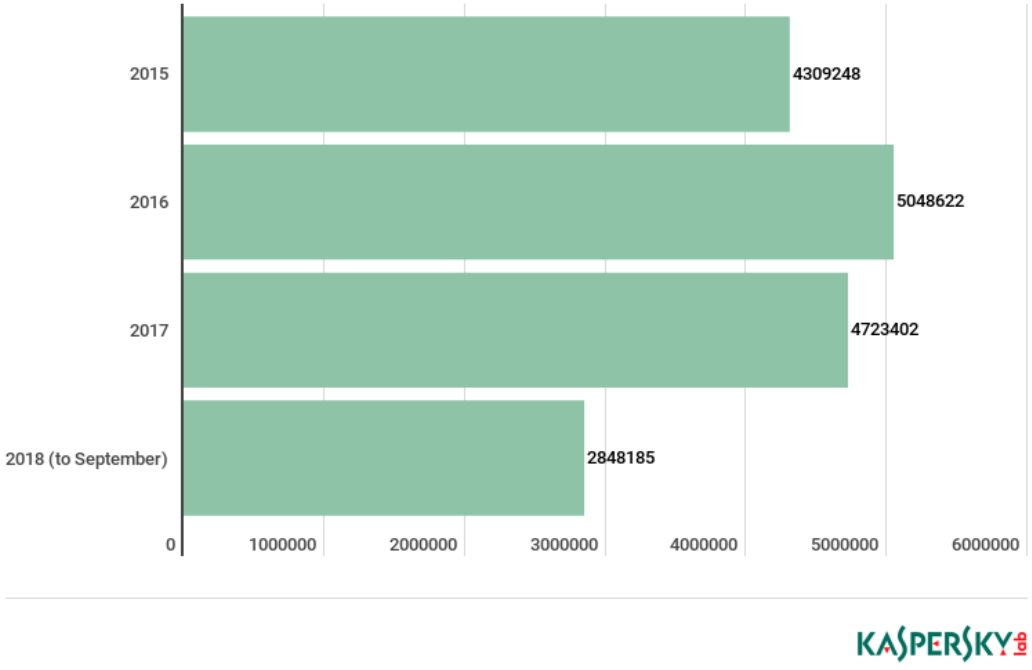
Detection data for the Gozi malware family targeting users of e-commerce brands, 2015 – 2018. Source: KSN

Italy again features among the most affected countries: just under one in five (19.57%) users who encountered malware in January-August 2018 were targeted with this threat, followed by Russia (13.89%) and Brazil (11.96%).

Country	% of users affected by any malware who were targeted by the Gozi malware family through e-commerce brands in Jan-Aug 2018
Italy	19.57
Russia	13.89
Brazil	11.96
France	5.91
Germany	5.11
Vietnam	3.54
Turkey	3.51
Mexico	3.29
Spain	3.29
United States	3.1

Zeus

The father of so many banking Trojans, Zeus was first detected in 2007, and is one of the most successful banking Trojans of all time. It remains a potent threat in its own right, particularly in emerging markets, with new variations and components adding to its power. In addition, it has given rise to a host of similar malware, built on the basis of its source code that was publically released in 2011.



Detection data for the Zeus malware family targeting users of e-commerce brands, 2015 – 2018. Source: KSN

Overall detection numbers look set to decrease by around 10% for 2018, with around 5.7 million total detections (based on data to the end of August).

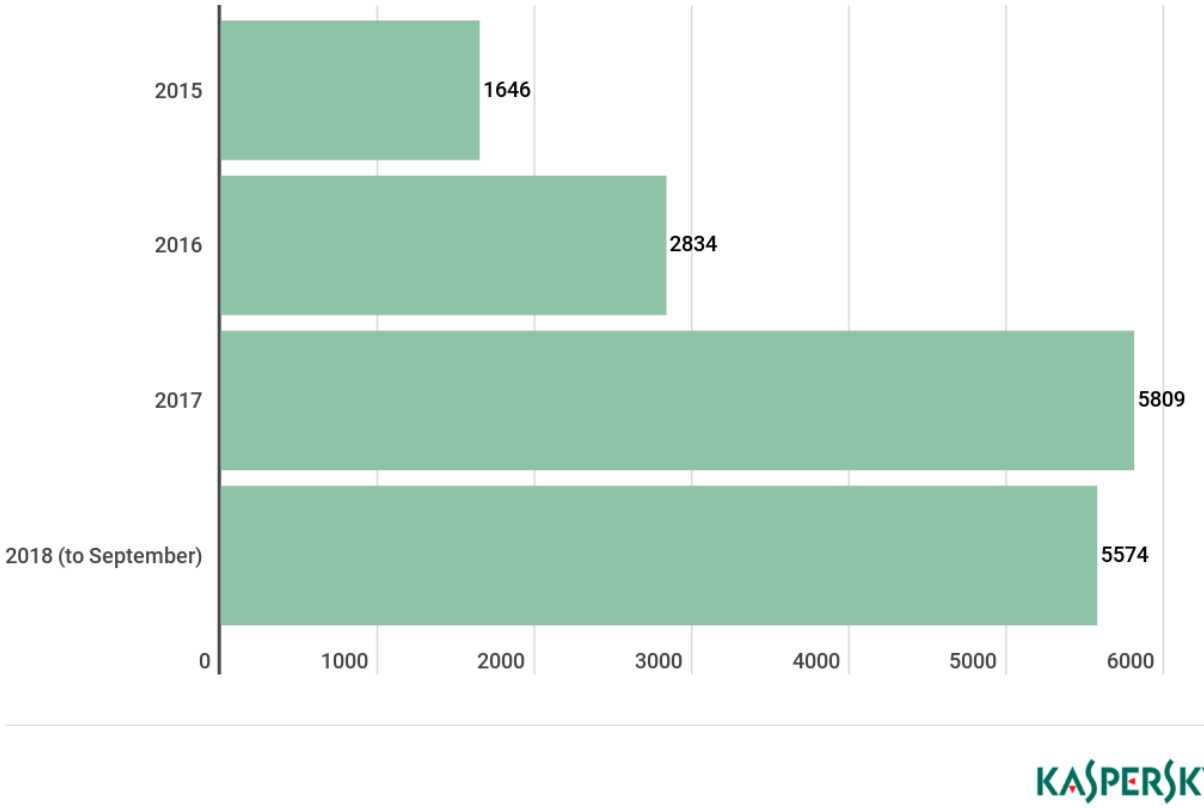
The top target is Russia, where 17.28% of users who encountered malware in the first eight months of 2018 were faced with this threat, followed by Vietnam (6.18%), and India (5.06%). However, other countries that regularly appear in the top target list for e-commerce malware, like Germany, Italy, Brazil, China and the US, also make that list for Zeus.

Country	% of users affected by any malware who were targeted by the Zeus malware family through e-commerce brands in Jan-Aug 2018
Russia	17.28
Vietnam	6.18
India	5.06
Germany	5.01
Italy	4.14
Indonesia	2.99
Brazil	2.97
Malaysia	2.95
China	2.74
United States	2.64

Chthonic

Chthonic is one of the most well-known Zeus modifications, with a modular structure that allows it to provide the full suite of activities: collect system information, steal passwords, log key strokes, insert a malicious script into web pages and intercept data entered in online forms in web browsers, remotely connect to the infected computer and perform banking transactions, and more. In addition, VNC (virtual network computing) and cam-recorder modules enable attackers to connect remotely to the infected computer and use it to carry out transactions, as well as recording video and sound if the computer has a webcam and microphone.

Chthonic was first reported in late 2014. After an expected decline in use in 2015, the number of detections has risen strongly year on year.



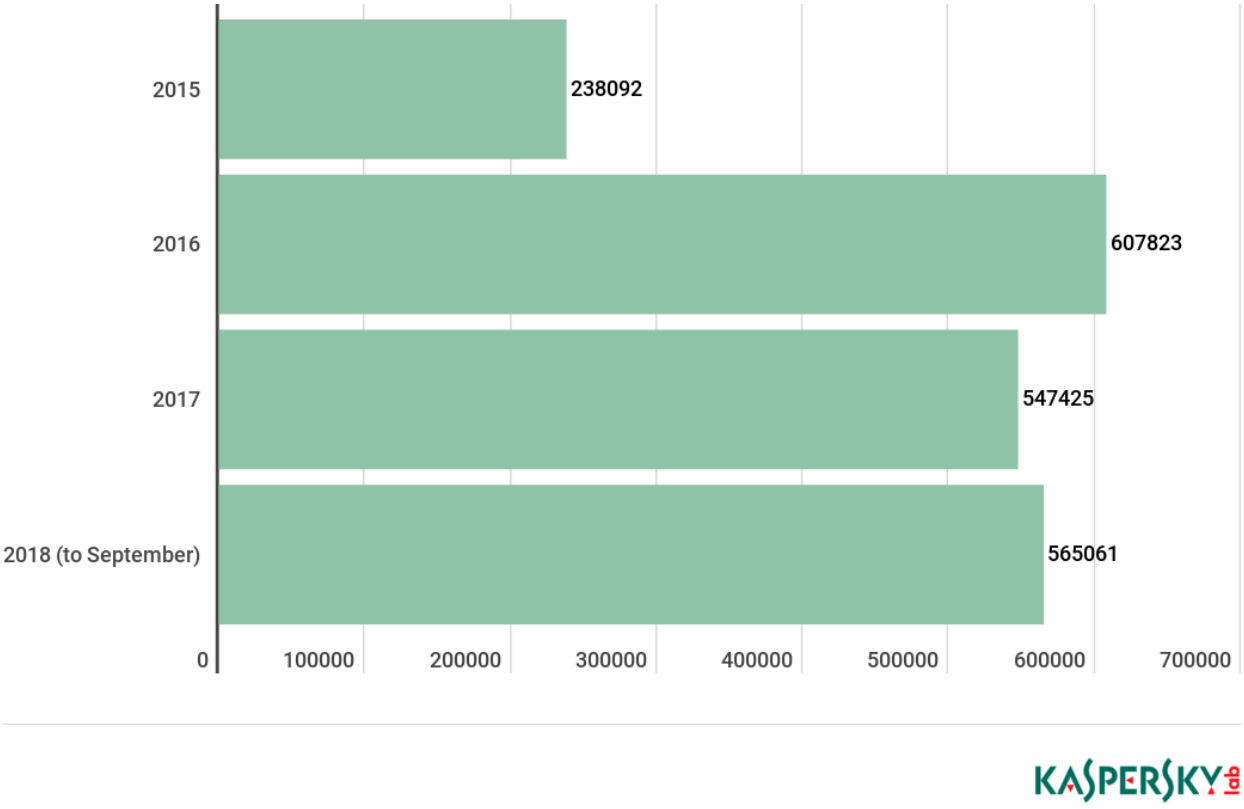
Detection data for the Chthonic malware family targeting users of e-commerce brands, 2015 – 2018. Source: KSN

Emerging and Spanish-speaking markets are the most affected by Chthonic, with 18.81% of users targeted by malware in Brazil affected by this threat, followed by Colombia (7.59%) and Mexico (5.42%), with Spain also in the list at fifth (4.16%).

Country	% of users affected by any malware who were targeted by the Chthonic malware family through e-commerce brands in Jan-Aug 2018
Brazil	18.81
Colombia	7.59
Mexico	5.42
Italy	4.58
Spain	4.16
Peru	3.8
India	3.68
Germany	3.62
Russia	3.25
Ecuador	3.13

SpyEye

SpyEye is another banking Trojan based on the Zeus malware. SpyEye launches its attacks through browsers and carries a broad suite of malicious functionality. Among other things, it is able to steal funds even while users are logged into their accounts, so they could potentially watch their funds disappear before their very eyes. The number of SpyEye detections targeting online shoppers is rising: with overall detections up around 34% on 2017 (to 847,591, based on numbers for January-August 2018).



Detection data for the SpyEye malware family targeting users of e-commerce brands, 2015 – 2018 Source: KSN

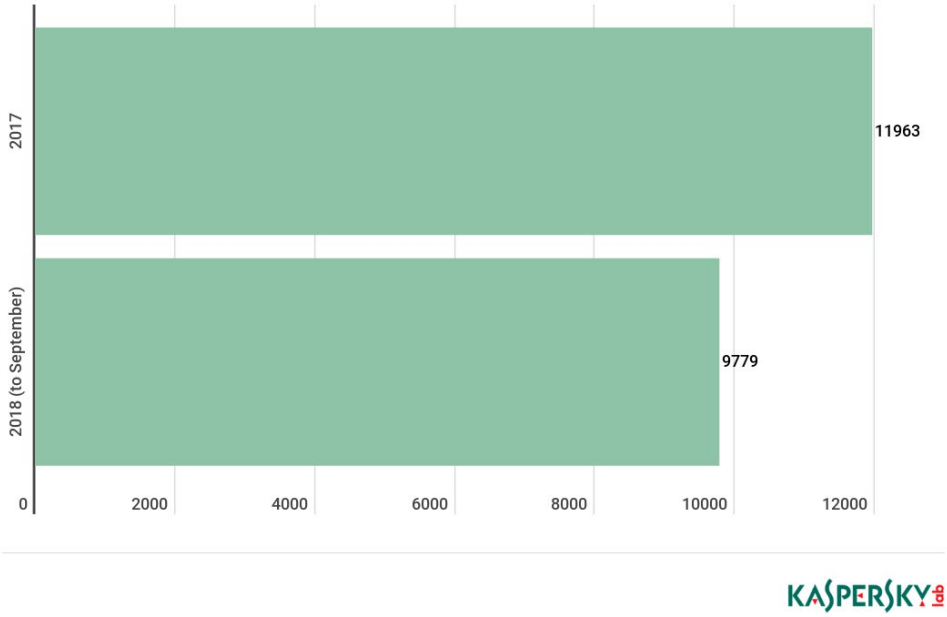
Russia is the most targeted country: 18.8% of users who encountered malware in the first eight months of 2018 faced this threat, followed by much lower numbers elsewhere.

Country	% of users affected by any malware who were targeted by the SpyEye malware family through e-commerce brands in Jan-Aug 2018
Russia	18.81
India	5.71
Vietnam	5.11
Italy	4.52
Germany	4.42
Malaysia	3.13
South Africa	2.6

Spain	2.44
Indonesia	2.4
Algeria	2.07

TinyNuke

TinyNuke, also known as NukeBot, is a fully-fledged banking Trojan that was discovered after it was made available on the dark web in 2016 (it is not the only banking Trojan on our list to be available to other cybercriminals on the underground). Its functionality resembles that of Zeus. The author behind the malware published TinyNuke's source code on Github in 2017. TinyNuke is a growing threat for online shoppers. The number of e-commerce related detections involving this malware are rising rapidly.



Detection data for the TinyNuke malware family targeting users of e-commerce brands, 2015 – 2018. Source: KSN

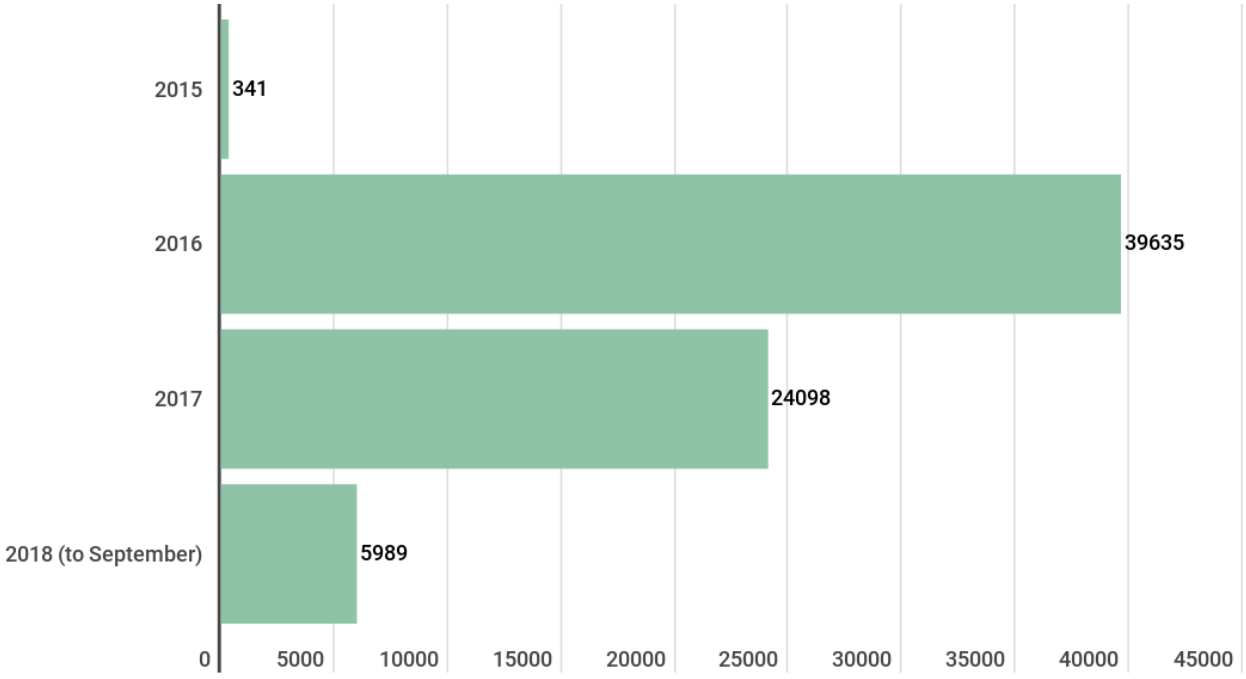
The country most at risk of TinyNuke, by an immense margin, is France, where 64.5% of those who encountered malware in the first eight months of 2018 were faced with this threat. Next, with far fewer detections are Germany (5.16%) and Italy (4.31%).

Country	% of users affected by any malware who were targeted by the TinyNuke malware family through e-commerce brands in Jan-Aug 2018
France	64.65
Germany	5.16
Italy	4.3
India	3.74
Russia	2.9

Poland	1.99
Algeria	1.37
Brazil	1.18
United Kingdom	1.14
United States	1.04

Gootkit2

Discovered in 2014, GootKit is a fairly uncommon banking Trojan, known for keeping its infection numbers and attack campaigns very small and focused. Researchers believe that this, combined with a general lack of distinguishing features, has helped it to stay under the radar. Gootkit version 2 was reported on in 2016, after which there appears to have been a decline in detection numbers.



Detection data for the Gootkit2 malware family targeting users of e-commerce brands, 2015 – 2018. Source: KSN

Italy was the country most affected by Gootkit2 in the first eight months of 2018, with nearly one in three of users who encountered malware during this time affected by the threat. It is followed by France (10%) and then Russia (6.4%) and the United Arab Emirates (6.2%).

Country	% of users affected by any malware who were targeted by the Gootkit2 malware family through e-commerce brands in Jan-Aug 2018
Italy	29.3
France	10
Russia	6.4
United Arab Emirates	6.2
Germany	5.2
United States	4.3
India	4
China	3.9
Spain	3.9
United Kingdom	2.7

IcedID

IcedID was detected in 2017, a new modular banking Trojan that has functionality comparable to Zeus, Gozi and other similar malware, but does not appear to have borrowed their code. It has an interesting network propagation module that suggests businesses are among its targets.

IcedID's initial targets appeared to be banking or finance-related, including e-commerce targets in the US and a few in the UK, and it quickly spread to other geographies. In 2018, researchers discovered that the banking Trojan Gozi had started to distribute IcedID in some form of malware collaboration. In the first eight months of 2018 there were 44,490 detections of this threat.

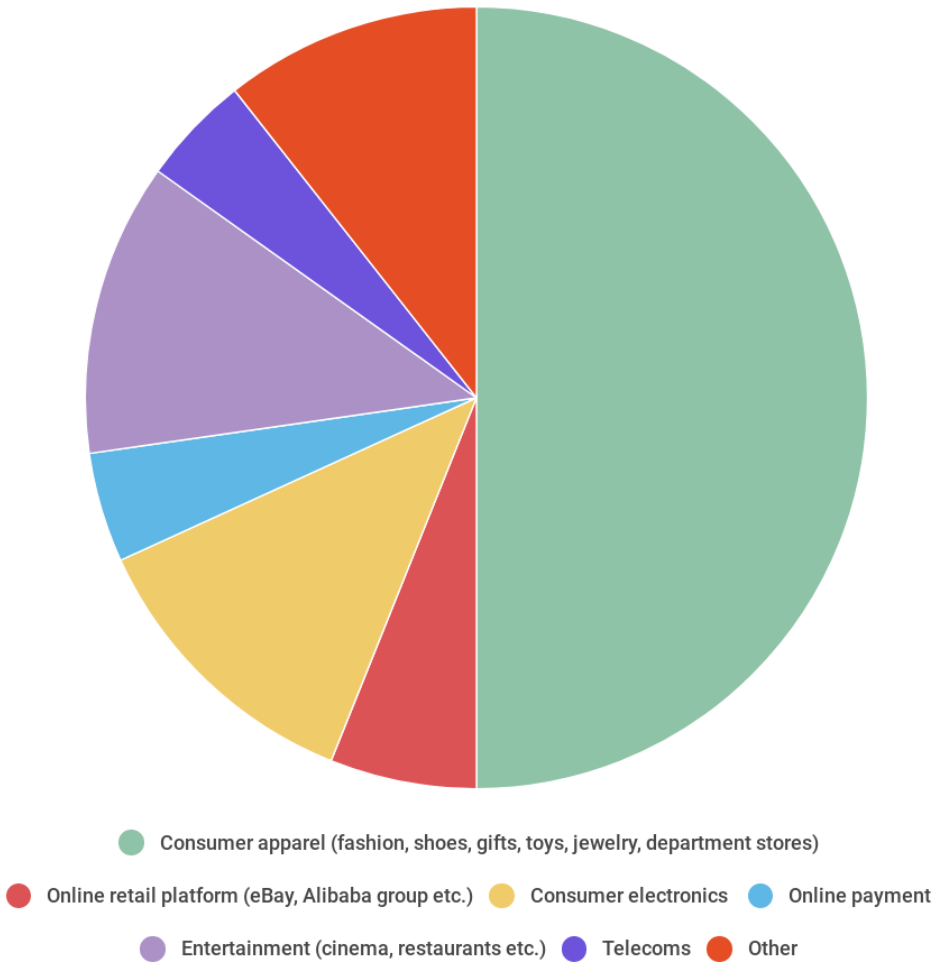
The majority of those affected by this new threat are in the US (51.13% of users who encountered malware in the first eight months of 2018 faced this threat), followed by India (9.55%) and Italy (8.25%).

Country	% of users affected by any malware who were targeted by the IcedID malware family through e-commerce brands in Jan-Aug 2018
United States	51.13
India	9.55
Italy	8.25
China	4.85
Japan	3.56

United Kingdom	2.91
Canada	2.75
Germany	2.75
Russia	1.78
Mexico	1.46

The brand categories (mis)used by e-commerce malware

The brands used by the malware cover a wide range of commercial sectors including clothing, footwear and jewelry, entertainment, leisure, electronics, and more.



KASPERSKY lab

E-commerce industry categories most targeted by malware families in 2018. Source: KSN

The malware families target many different brands. According to our detection list, 46 different brands are used to steal information by Betabot, 36 by Gozi and 35 by Panda; while Zeus variations account for just five different brands. Further, the malware families Betabot, Panda and Gozi often overlapped in terms of target brands.

The market for stolen e-commerce credentials

What do the hackers do with all the stolen information? Stealing financial credentials or being able to execute financial transactions from a victim's account is clearly about making money, but what do they do with the passwords, logins and other information stolen from online shoppers?

To answer this question, researchers decided to take a look at the availability on underground markets of data stolen via e-commerce sites. First, they analysed an open site, available directly from Google, and then they reviewed 39 top-rated Tor marketplaces (based on information available on the open Tor site DeepDotWeb).

In all, they found 3.7 million sets of credentials for sale, with the vast majority (3.5 million) available on the open and accessible website. Darknet stores, which tend to focus more on illegal weapons, drugs, etc., offered only around 1,900 sets of e-commerce user data, although it should be noted that some sites only provided a per-credential price with no information on the actual numbers available.

The top e-commerce accounts for data sale on the underground were:

- PayPal (2,118,007 sale offers)
- Amazon (3,742 sale offers)
- eBay (2,456 sale offers)

The underground traders appear to be most interested in merchant accounts, the small businesses that use these platforms to sell their goods and services and manage their online payments. This is deduced from the fact that the price for a user account with zero credit balance (likely to be a transactional consumer account with possibly a linked payment card) is just a few dollars, rising to $1,000 for an account with a $10,000 balance (likely to be a merchant account).

If the price for a single user account is so low, why mount the attacks and steal the data? The answer could lie in the fact that the data is generally fairly easy and low cost to steal, so any price is a profit. Also, the data can be used to mount other future attacks, such as phishing or ransomware, and a compromised victim device with administrator rights offers untold future benefits, for botnets, spying, cryptocurrency mining and more.

Conclusion and advice

The main purpose of this paper is to alert consumers and retailers coming into the year-end's busy holiday shopping season of the need for caution when shopping online. The results show that even trusted brands can be misused by increasingly advanced modular malware to steal money and information from unwary consumers.

Our recommendation is to implement the following steps to stay protected:

If you are a consumer

- A powerful, regularly updated security solution is a must for all devices you use to shop online. These solutions will not only help protect you from visiting unsafe websites where you might find a Trojan but can detect the Trojan when it tries to download, install or run on your system. Additionally, these solutions can scan your system and remove any malware if it already exists on your machine.
- Avoid entering data into or buying anything online from websites that look suspicious 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.
- Don't fall for critical warning messages – check with the provider directly if there is an issue with your account.

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 and ensure all levels of your company network is protected, from core data centers if you have them to specialized e-commerce systems, and install a dedicated security solution which makes it possible to catch even unknown malware.
- 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 use two-factor authentication (Verified by Visa, MasterCard Secure Code, etc.).
- Educate your customers on possible cyberthreats they may encounter while shopping online and offline.

All malware belonging to the banking Trojans in this report are detected and blocked by Kaspersky Lab security solutions.