

KASPERSKY LAB BLACK FRIDAY THREAT OVERVIEW 2016

Kaspersky Lab

November 2016

Contents

Introduction2

Methodology and Key Findings4

Phishing5

Financial malware17

News from the Underground24

Conclusion and advice27



Introduction

The Internet has changed forever how people shop. By 2018, around [one in five](#) of the world's population will shop online; with ever more people doing so on a mobile device rather than a computer. In fact, it is estimated that by the end of 2017, [60%](#) of e-commerce will come from smartphones. That's millions of people enthusiastically browsing and buying while at home, at work, in restaurants, airports, and railway stations, walking down the street, standing in stores, and on holiday, often outside the protective reach of a secure, private wireless network.

Regardless of the device used, every interaction and transaction will generate a cloud of data that brands will want to capture in order to deliver ever more targeted and personalized offers. Unfortunately, others are waiting to seize consumers' information too – through insecure public Wi-Fi networks, phishing emails and infected websites, among others. They are the cybercriminals, and they don't have a consumer's or even a brand's best interests at heart.

The risks facing retailers and online shoppers peak during the busiest shopping days of the year: the late November Thanksgiving weekend that runs from Black Friday through to Cyber Monday, and all through December to Christmas and the New Year.

As the number and speed of transactions increase, so do the cyberthreats. In this overview, Kaspersky Lab reveals the reality in terms of the top cyber-attacks targeting consumers and retailers during this remarkable buying period.

To put this data in context, it is worth looking back over the last few years to see how the landscape has evolved, focusing in particular on Black Friday and Cyber Monday.

In 2013, the concepts of Black Friday and Cyber Monday were already well established in North America and starting to gain momentum elsewhere. In the US alone, Cyber Monday [saw](#) online sales grow by 21% on 2012, raking in sales of [\\$2.27 billion](#). Black Friday achieved [\\$1.93 billion](#) worth of transactions, but won out on average sales value. [17% of total sales were undertaken on mobile – a 55% increase on 2012](#). In the UK, online sales rose by a slightly more modest [16% in November](#), with over [\\$600 million](#) believed to have been spent online on Cyber Monday alone.

This was also the year when US retailer Target discovered that the credit card details of around [40 million customers were breached](#) between 27 November and 15 December, apparently through hacked in-store point-of-sale systems.

In 2014, the year of the now infamous Sony Entertainment hack, the records set in 2013 were all broken. Thanksgiving Day 2014 in the US marked the moment when more [mobile devices \(52%\)](#) than computers were used (48%) for browsing online; and Black Friday [online sales were up 21%](#) compared to the same day in 2013 – with around one in three (30%) orders placed using a mobile device. [Adobe](#) estimates overall online sales in the US of \$2.4 billion on Black Friday, \$1.3 billion on Thanksgiving Day and \$2.7 billion on Cyber-Monday. In the UK, online sales [peaked](#) during the week of Black Friday sales surged

by 44%, compared to the previous week, and up a staggering 135% on the same week in 2013. Mobile sales rose by 83%.

And the records were all broken again in 2015. In the US, Cyber Monday 2015 was the largest online sales day, ever. Online consumers spent a record [\\$3.07 billion](#) - and [\\$8.03 billion](#) across the four-day Thanksgiving weekend. IBM analysis shows that, overall, online sales were up by a quarter ([26%](#)) on 2014, with [40%](#) of sales now coming from mobile devices.

The big consumer hacks of the season involved malware targeting point-of-sales systems in hotels, including [Hyatt](#), [Starwood](#) and [Hilton](#) worldwide.

2016 looks set to break records all over again, and criminals will probably try even harder to take advantage of all the noise and activity to steal credentials to financial accounts or even to grab the money directly. This overview will cover the types of cyberthreats that buyers, sellers and providers of payment systems may face over the coming weeks.

Methodology and Key Findings

The overview is based on information gathered from Kaspersky Lab malware and phishing detection systems (number of attacks or number of attacked users), and also from the analysis of events and conversations happening on the hacker underground – multiple internet forums where users allegedly involved in financial fraud operations tend to gather. The overview covers Q4 in 2013, 2014, 2015 and partly (in some cases) 2016. Even though, officially, the “Black Friday” sales period ends with Cyber Monday, right after the Thanksgiving holidays, just a few days later another “high” sales period begins: the so-called pre-Christmas period, which is also one of the most profitable times of the year for retailers. We count October as a high sales period as well, because so-called “Black Friday” sales campaigns often start prior to the actual sales days (Halloween sales are a good example), and – what is more important – cybercriminals tend to start preparations in advance of day X.

The overview also contains a list of actions that could be implemented by regular users, business owners and owners of payment infrastructure in order to prevent fraud during the high retail season.

Key Findings:

- The share of financial phishing during the high sales season is 9 percentage points higher than during other times of the year.
- The share of phishing attacks against online shops and payment systems during the period is usually higher than phishing against banks.
- Criminals are trying to connect their malicious campaigns, such as spreading financial malware and phishing pages, to particular dates: Black Friday, Cyber Monday, and the pre- and post-Christmas days.
- Kaspersky Lab’s virus collection now counts 36 families of POS malware, 6 of which were added in 2016. The number of Banking malware families, in contrast, is only 30.
- Underground vendors of skimmers and dummy plastic cards are already experiencing an increase in sales. In December 2015 the sales of skimmers rose more than tenfold: from the regular 25-30 devices to 500.
- Kaspersky Lab researchers expect blackmailing DDoS-attacks against online retailers during the holidays.

More about these findings can be found in the overview.

Phishing

Among cybercriminals, phishing is one of the most popular ways to steal payment card details and credentials to online banking accounts. A phishing scheme is relatively easy to set up (the fraudster doesn't even need to know how to write malware; only basic web development and design skills are required), yet it is effective because it is mostly based on social engineering techniques. During the holiday period, users are eager to find the best goods at the best price and they are expecting to see offers of this kind while surfing the web. Cybercriminals know about that and try to exploit this feature as much as possible.

Share of financial phishing in overall volume of attacks

As statistics from the previous years show, financial phishing usually accounts for no less than a quarter of all phishing attacks registered in a year. For example, in 2013, it was 31.45% of all registered phishing attacks, in 2014 – 28.74%, in 2015 – 34.33%. The current year is not yet over, but judging by the quarterly statistics the trend is the same.

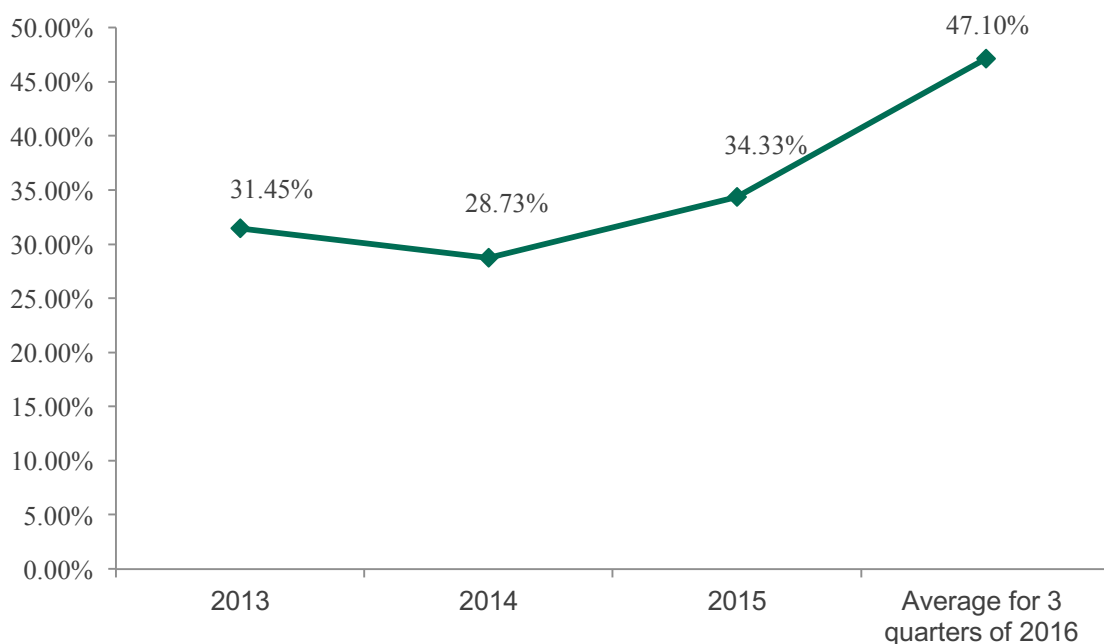


Fig. 1: Share of financial phishing in overall number of phishing attacks 2013 - 2016

And at the same time things are significantly different when it comes to what we call the holiday sales period. As expected, the share of financial phishing at this time is noticeably higher than the typical yearly result.

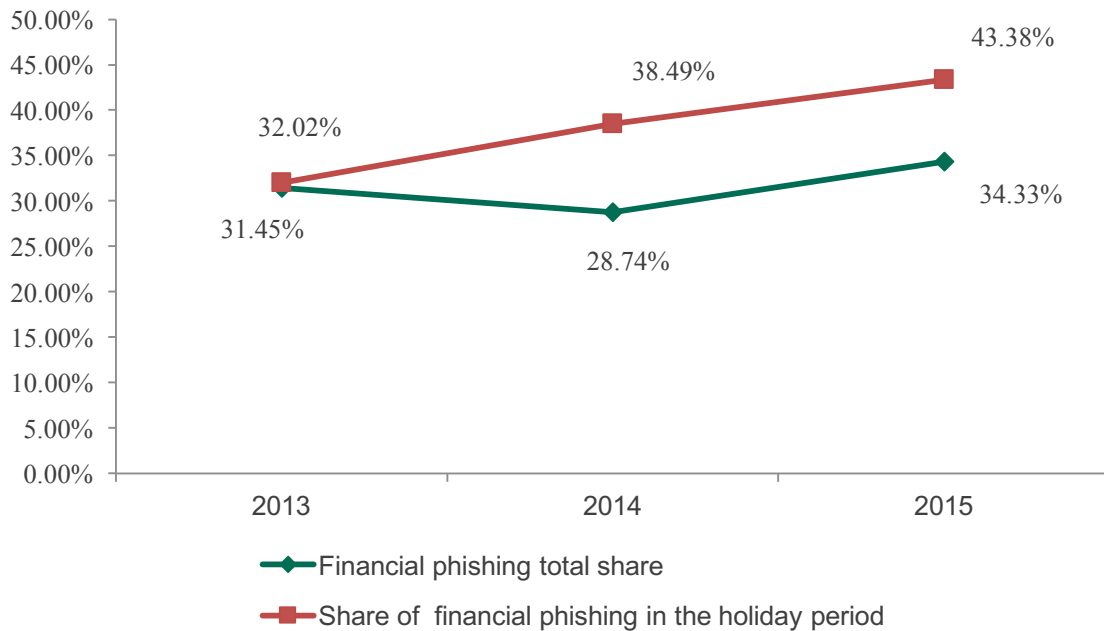


Fig. 2: Share of financial phishing in different periods in comparison to the holiday period

Although in 2013 the number of financial phishing attacks during the high sales period was only 0.5 percentage points higher than the total result for the same year, in 2014 and 2015 we detected a clear difference of around 9 p.p. in favour of attacks during the holidays. Of course these data are not enough to talk about a strong tendency; nevertheless, the chances are high that this year this difference will emerge again.

Types of financial phishing

At Kaspersky Lab we distinguish between three major types of financial phishing: Banking, E-payment and E-shopping. They are all types of phishing pages that imitate the corresponding legitimate services dealing with financial transactions. Based on what we have observed in Q4 in 2014 and 2015, during the “Holiday” period, the separation between different types of financial phishing is different to the result for the full year.

For example, in 2013, shares of phishing attacks during the year and during the last “Holiday” quarter weren’t very different – less than 1 percentage point. However inside the category differences were much more visible.

That year the share of e-shop phishing in Q4 increased more than 1 percentage point to 7.8%. And the share of phishing against users of popular payment systems more than doubled compared to the rest of the year - 5.46% against 2.74%. At the same time, the share of phishing against users of online banking was lower than during the year: 18.76% against 22.2%.

The situation was repeated the next year, but with more visible amplitude. Shopping phishing during the holiday season was 5.32 p.p. higher than the full year result. And the payment systems' phishing was 2.78 p.p. higher.

2013	Full year	Q4
Financial phishing total	31.45%	32.02%
E-shop	6.51%	7.80%
E-banks	22.20%	18.76%
E-payments	2.74%	5.46%
2014	Full year	Q4
Financial phishing total	28.73%	38.49%
E-shop	7.32%	12.63%
E-banks	16.27%	17.94%
E-payments	5.14%	7.92%
2015	Full year	Q4
Financial phishing total	34.33%	43.38%
E-shop	9.08%	12.29%
E-banks	17.45%	18.90%
E-payments	7.08%	12.19%

Fig. 3: The change in shares of different types of financial phishing in 2013-2015

These differences are accompanied by attacks against particular targets. In 2014, Kaspersky Lab researchers conducted a small investigation into the dynamics of attacks during Black Friday and discovered that the number of attempts to load phishing pages detected and blocked by users of Kaspersky Lab products was actually growing.

Here are the timeline graphs for several targets that are traditionally most often used by phishing scammers.

Dynamics of detection of attempts to load phishing page where the American Express brand is mentioned demonstrates very similar behaviour in 2014 and 2015.

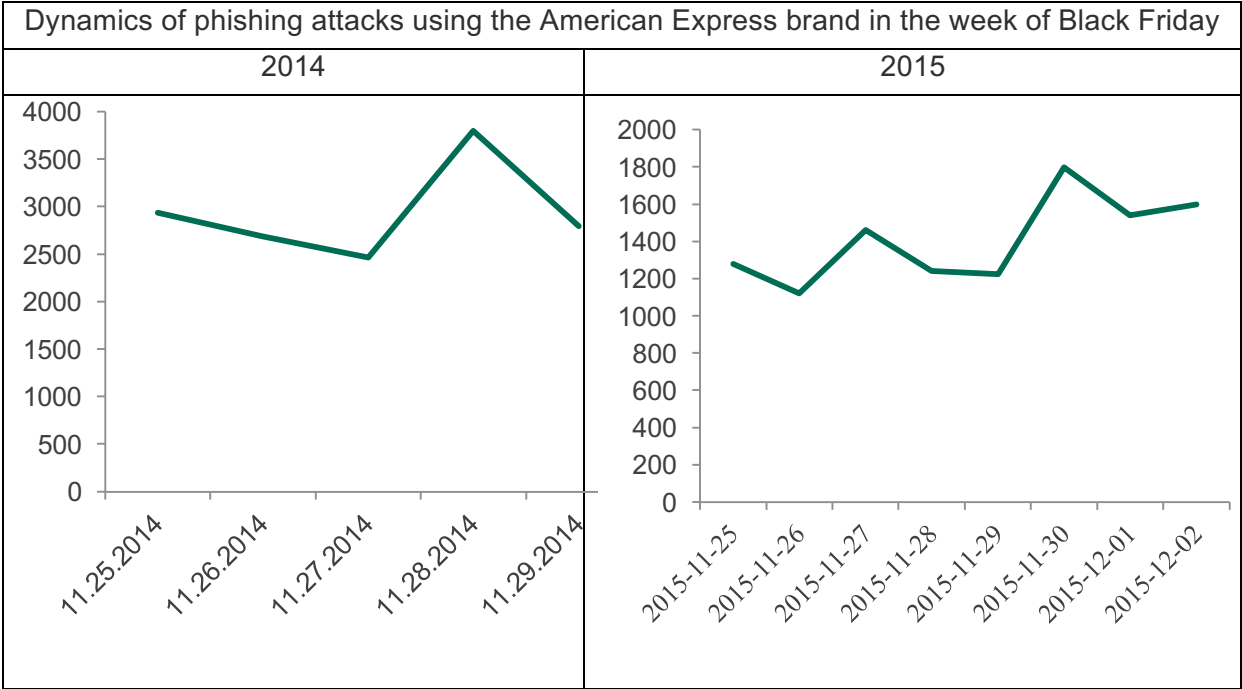


Fig. 4: Example of timeline of attacks against a particular target

And when it comes to other brands connected to online money and shopping the situation is repeated. Though the growth of attacks in 2015 happened after Black Friday and peaked on Cyber Monday.

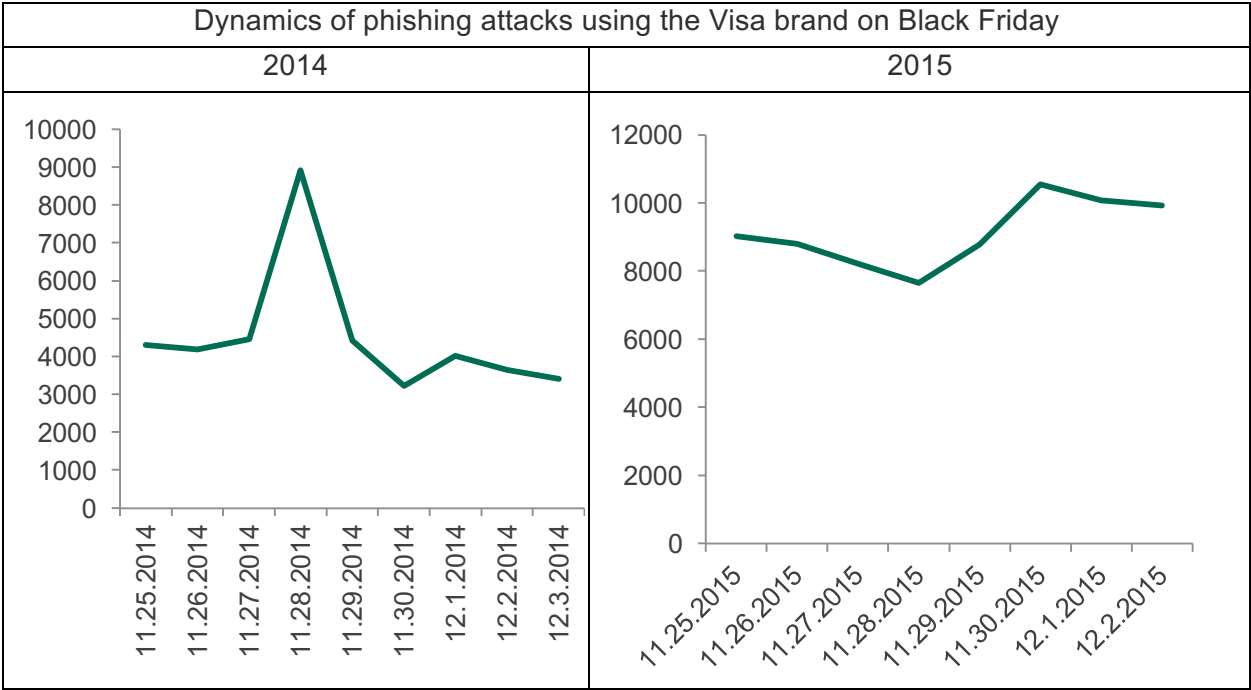


Fig. 5: Example of timeline of attacks against a particular target

Last but not least phishing attacks that utilize online shopping brands also obviously have a connection to specific days, such as Black Friday.

Dynamics of phishing attacks using the Wal Mart brand on Black Friday	
2014	2015

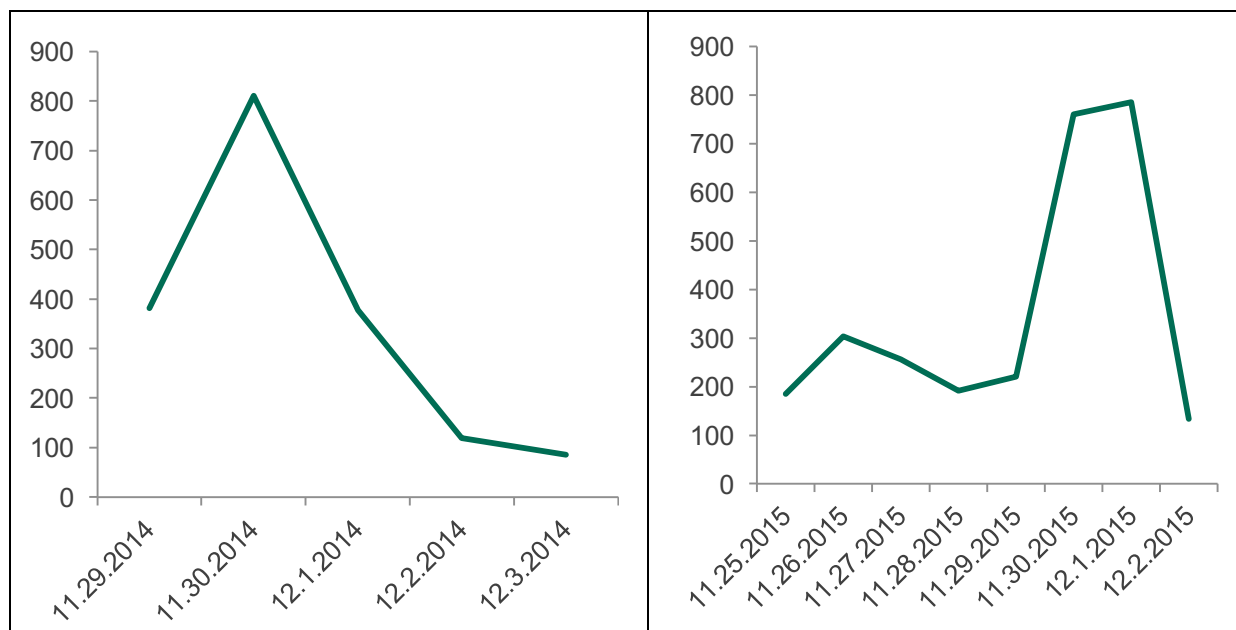


Fig. 6: Example of timeline of attacks against a particular target

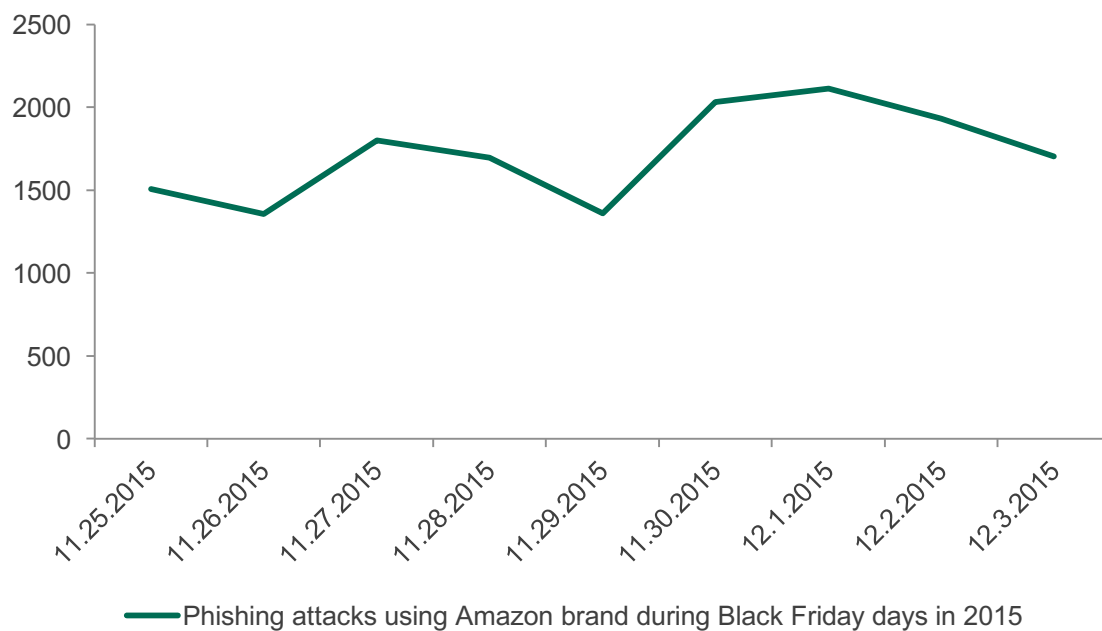


Fig. 7: Example of timeline of attacks against a particular target

Spikes in the number of detections are also typical for Christmas and the New Year period – basically they're the second highest period in the whole quarter. Further in this overview we will show that attack peaks are typical features not only for phishing, but for financial malware attacks as well.

Examples of “Holiday” Phishing

In most cases cybercriminals don't bother themselves with inventing anything special. Instead they just copy pages of legitimate shops, internet banking and payment systems.

As can be seen on the picture below the phishing copies of the Amazon shop quite precisely resemble the original website.

Fig. 8: Example of a fake Amazon e-shop

Which is also true for sites of payment systems and banks. Below are pictures of phishing sites imitating Visa and American Express data submission forms. Along with some others, these two brands are traditionally among the top of those faked by phishers.


1xb7...nluo.mi inticaret.com.tr/verifiedbyvisa/login.php

1 IMMETTI IL CODICE FISCALE

2 VERIFICA IDENTITÀ

3 CODICE VERIFIED BY VISA

4 REGISTRAZIONE COMPLETATA



Gratuito, veloce, sicuro

Per procedere con la registrazione verifica e completa le informazioni richieste.
Queste informazioni verranno trasmesse in modo sicuro e consentiranno di creare il tuo codice Verified by Visa.

***Dati obbligatori**

Codice Fiscale*
Inserire le 16 cifre della carta, senza spazi o trattini.

Email [In che modo verrà utilizzato l'indirizzo e-mail?](#)
Inserire l'indirizzo della casella di posta elettronica.

Fig. 9: Example of a fake Visa payment form

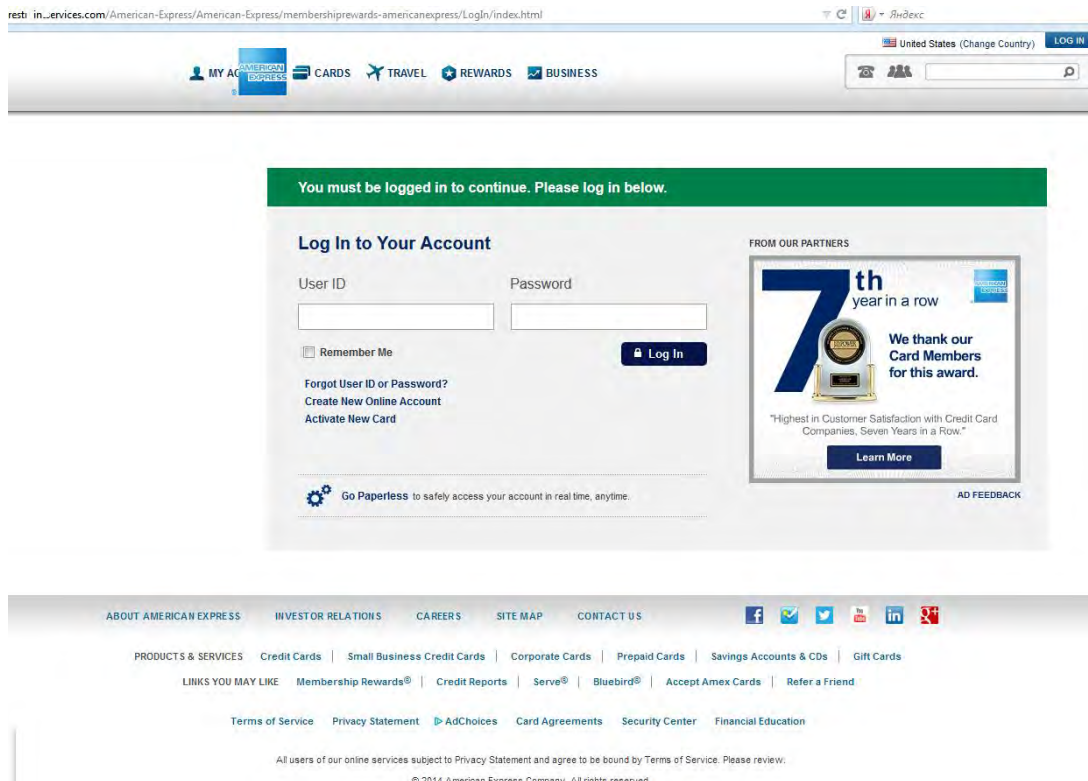


Fig. 10: Example of a fake American Express payment form

Sometimes criminals create whole fake web-shops simply to collect victims' credit card data.

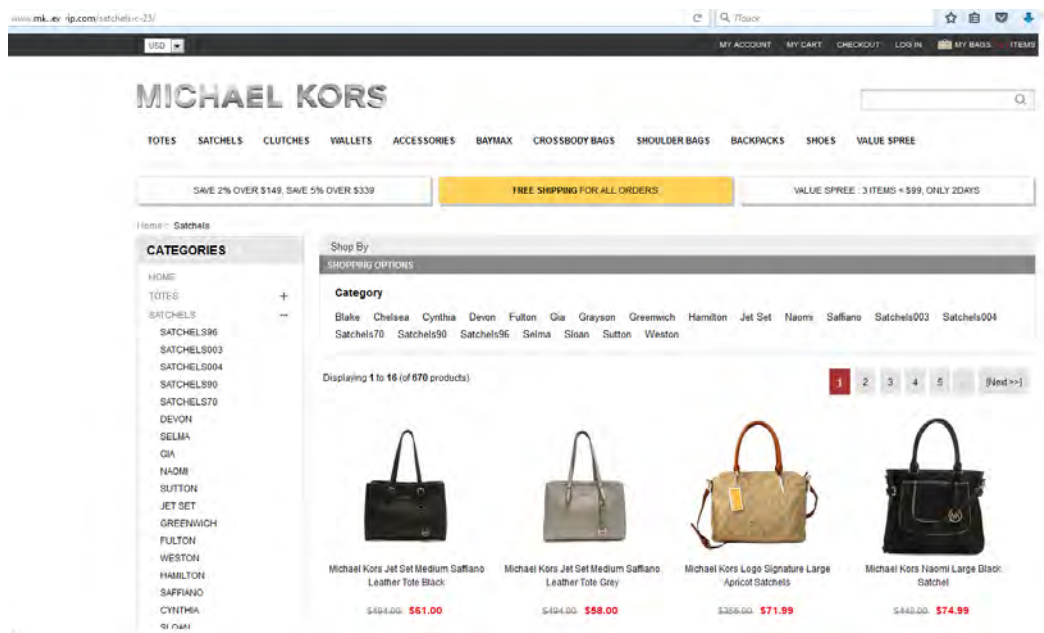


Fig. 11: Example of 100% fake internet shop

They attract victims with extremely low prices for goods from famous brands. And then – when the victim has chosen the item they like and proceeds to the payment page, they simply steal their financial credentials.

www.mkr w tp.com/index.php?main_page=checkout&fession=null

Sub-Total: \$149.00
Free Shipping Options (Free Shipping): \$0.00
Quantity Discount: -\$2.98
Total: \$146.02

Discount Coupon
Please type your coupon code into the box next to Redemption Code. Your coupon will be applied to the total and reflected in your cart after you click continue.
Please note: you may only use one coupon per order.
Redemption Code

Step 1 - Delivery Information
Shipping Details
Shipping Address
ascac ascac
ascac
ascac
ascac, AL 12345
United States
This is currently the only shipping method available to use on this order.
Free Shipping Options
☒ Free Shipping \$0.00

Step 2 - Payment Information
Billing Details
Billing Address
ascac ascac
ascac
ascac
ascac, AL 12345
United States
Please select a payment method for this order.
Payment (1) (Default)
☒ VISA ☐ MasterCard
Payment (2)
(If you are failed to make payment in the first payment, please try the second one again. Thank you!)
☒ MasterCard ☒ VISA ☒ JCB
Card Type:
Card Number:
Expiry Date:
CVV Number:
* Please wait while we process your transaction. It will be done within a moment....
* Browsers lower than IE 6.0 not supported.

Fig. 12: Example of 100% fake internet shop, part 2, the payment page

Another way in which criminals exploit the hot sales period is by creating allegedly legitimate websites that are selling gift cards and coupons that – if they're real – can be monetized in legitimate internet shops. However, criminals sell phony coupons, not real. The only purpose of these websites is to collect card credentials. An example of such a website is displayed in the picture below.

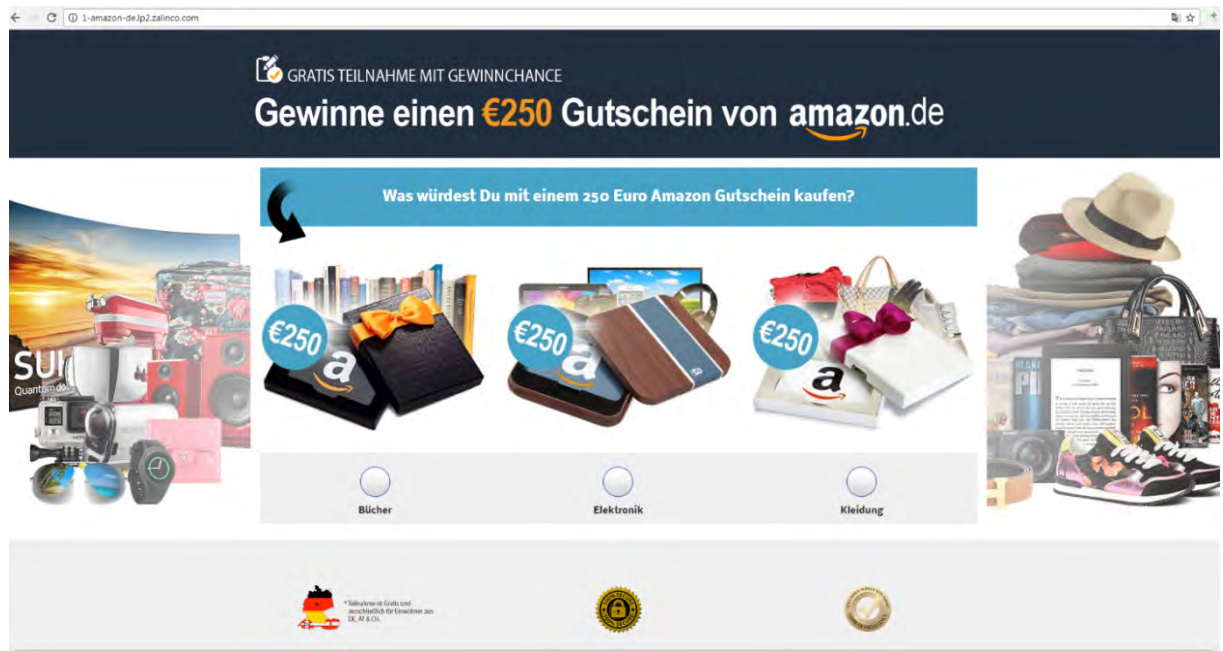


Fig. 13: Example of a fake shop selling phony coupons

And of course criminals exploit the brand of Black Friday itself and they start their preparations way in advance. While preparing this overview Kaspersky Lab researchers came across a number of fake websites, which have the word Black Friday in the name and the content of which offers outstanding discounts on expensive goods.

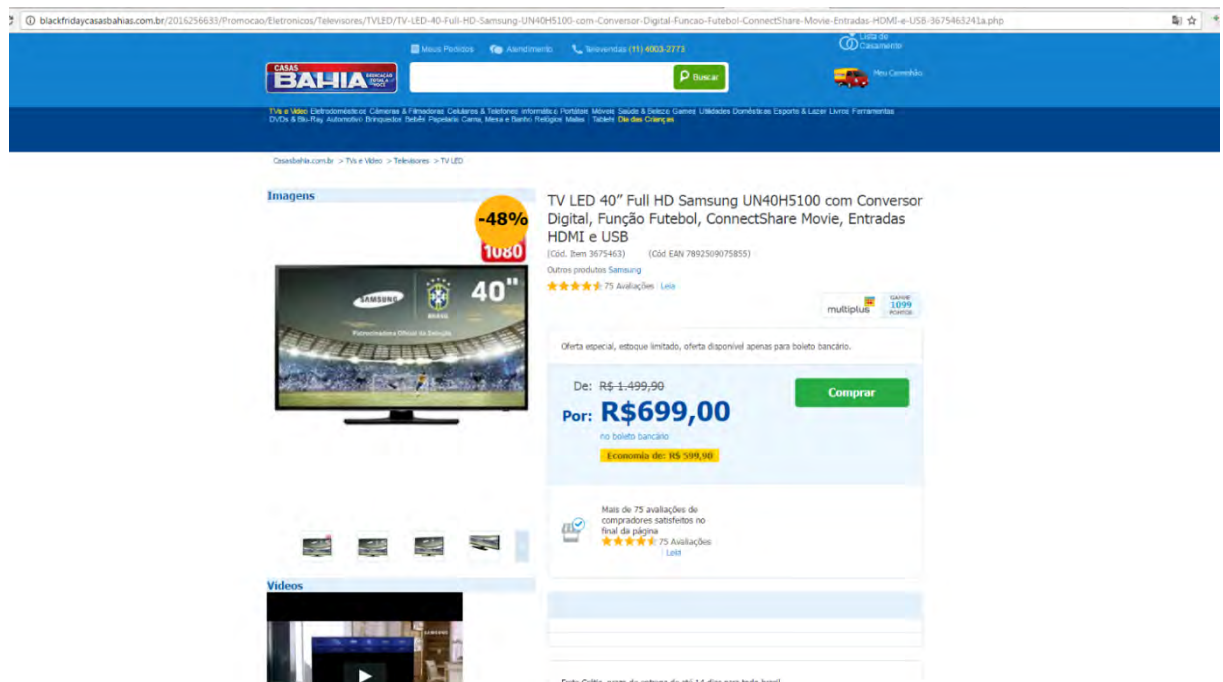


Fig. 14: Example of a fake Black Friday themed shop

In all, Kaspersky Lab security specialists expect that in 2016 the trends which emerged in previous years (higher than average percent of financial phishing, topical Black Friday scams, etc.) will continue their development as phishing remains one of the main source of credit card data for criminals and is still one of the easiest ways to set up a fraud scheme.

Financial malware

For years, banking trojans were one of the most dangerous cyberthreats out there. Unlike usual spyware which hunts for any type of credentials and, in most cases, is not very sophisticated, banking trojans are aimed specifically at users of internet banking and remote banking systems. Criminals tend to invest a lot of resources in the development of such malware and also develop different sophisticated techniques to avoid detection by AV products, and spread the malware as effective as possible. The most famous examples of banking malware are: [ZeuS](#), SpyEye, Carberp, Citadel, [Emotet](#), [Lurk](#) and others.

In previous years Kaspersky Lab experts have prepared two reports covering the global financial malware landscape, in [2013](#) and in [2014](#). And since then multiple things have changed: first of all the number of users attacked with banking malware has started to decrease. Most likely this is due to the fact that criminals have largely switched their attention from clients of banks to the banks themselves, because a sophisticated attack against a bank can bring much more profit than an attack against a regular user. Another reason is the rise of encryption ransomware which has proven itself a relatively effective way of getting money illegally. What hasn't changed a lot is the attention of criminals to the high sales season.

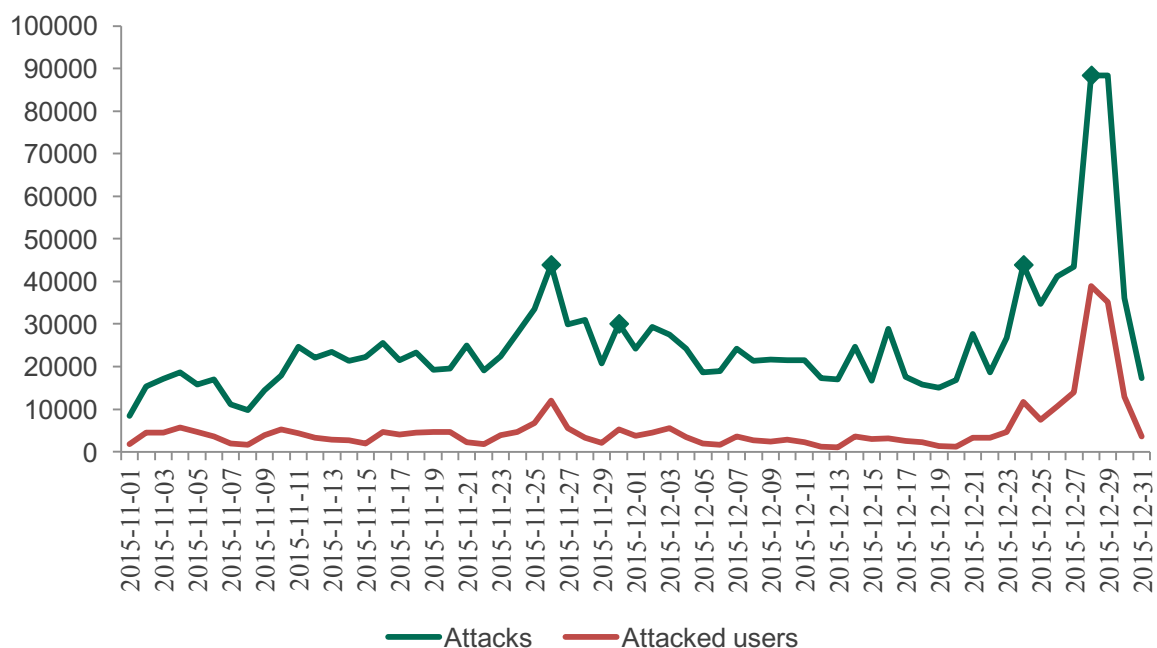


Fig. 15: the change in the number of attacks and attacked users from November to December 2015

According to Kaspersky Lab telemetry, during the holiday season of 2015, 261,000 users were attacked with banking malware. That's significantly less than in the same period a year ago, when 307,600 users were attacked. However, 2015 has shown the fairly obvious

interest that criminals are showing in Black Friday, Cyber Monday and Christmas. In October the number was 61,674 users, in November – 81,038, and in December – 154,324 attacked users. A year before, in 2014, 101,300 users were hit in October, 164,000– in November and 102,900 in December.

The pattern is obvious.

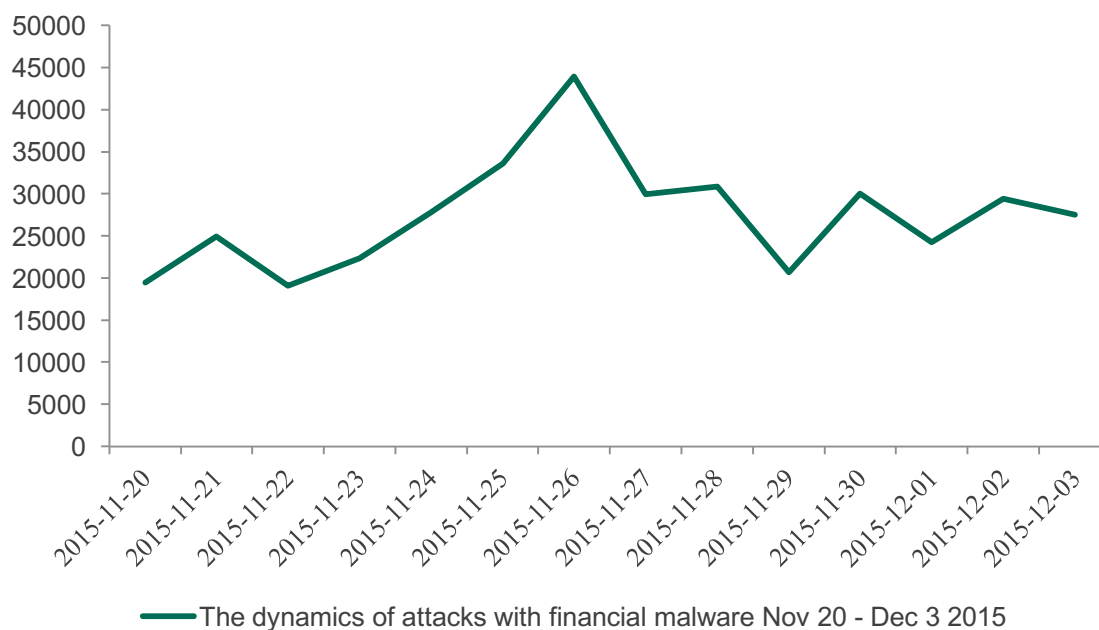


Fig.16: The dynamics of attacks with help of financial malware from November 20 to December 3 2015 (Black Friday through Cyber Monday)

As can be seen on the graph above, the number of attacked users started to grow from November 22nd and peaked on November 26th, the day before the Black Friday 2015. The next visible peak happened on November 30th, which was the day of Cyber Monday that year. These two peaks were noticeably the biggest since the beginning of the period.

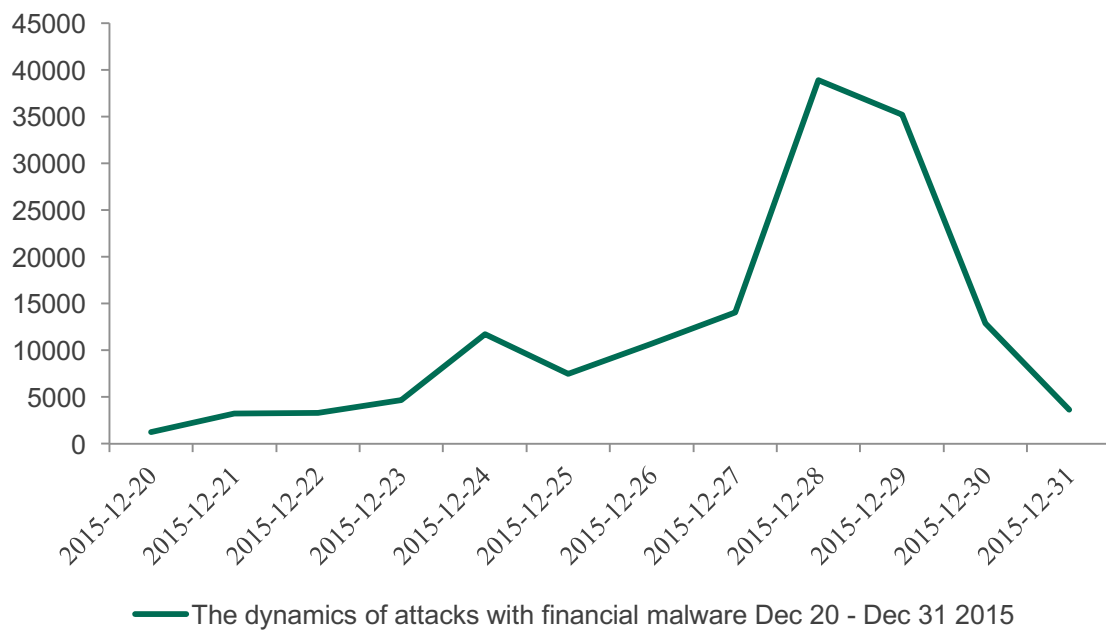


Fig. 17: The dynamics of attacks with financial malware in Christmas period 2015

The next big rise in the number of attacks and attacked users happened on 24th of December, right before Christmas, followed by a huge two-day spike detected on 28th and 29th, not long before New Year's Eve.

In 2014, the spikes of attacks in the holiday season weren't that obvious, but still it was clear enough that the Black Friday period is of interest: a visible rise in attacks started on November 24th and peaked on November 27th, which was again the day before Black Friday. After that another spike was registered on 1st December, which was the day of Cyber Monday.

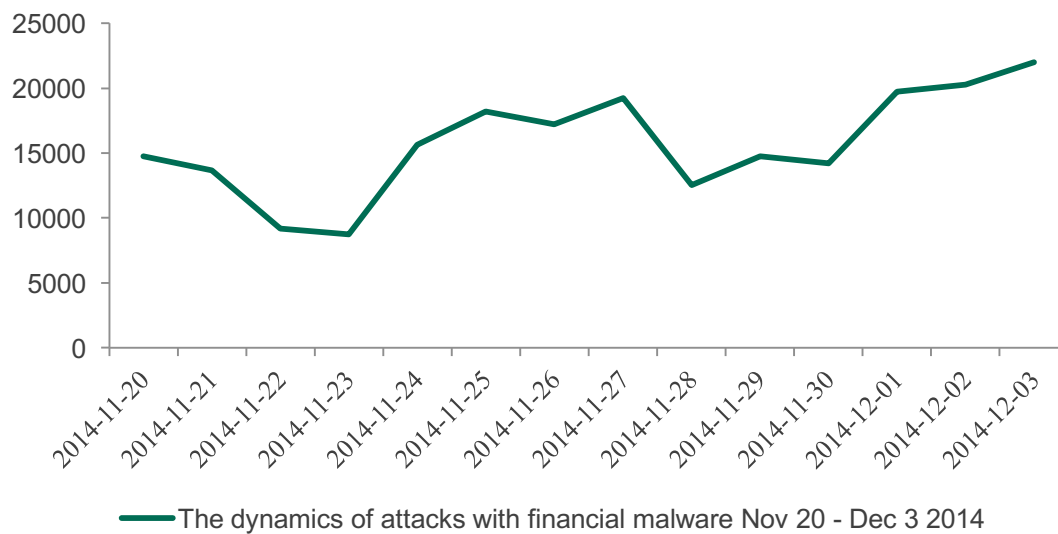


Fig. 18: The dynamics of attacks with financial malware from November 20 to December 3 2014 (Black Friday through Cyber Monday)

Christmas 2014 also has shown correlation between holiday dates and attacks: on 24th and on 28th of December.

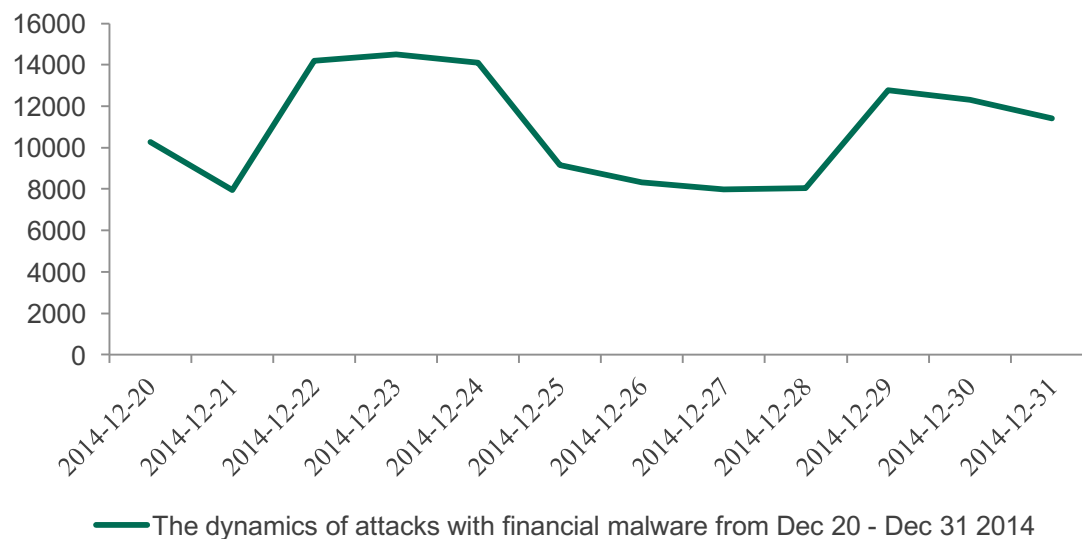


Fig. 19: The dynamics of attacks with financial malware in the Christmas period 2014

Almost the same spikes appear when it comes to Mobile malware. Most of the detections on the graphs below were generated by a few families of malware: Faketoken, Svpeng, Marcher

and Acecard. These four are the main threats when it comes to mobile banking on Android, and the criminals behind them obviously used the holidays to actively propagate these malicious programs. It was especially visible in 2014:

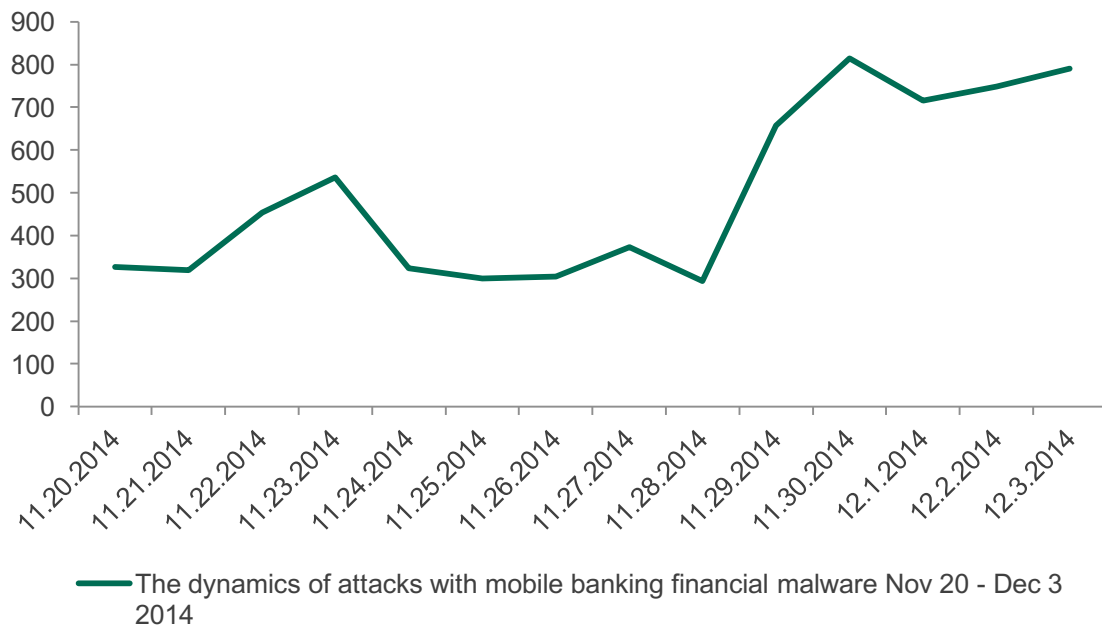


Fig. 20: The dynamics of attacks with mobile financial malware on Black Friday through Cyber Monday 2014 period

2015 was significantly calmer in terms of the number of detections, but certain spikes were still in place.

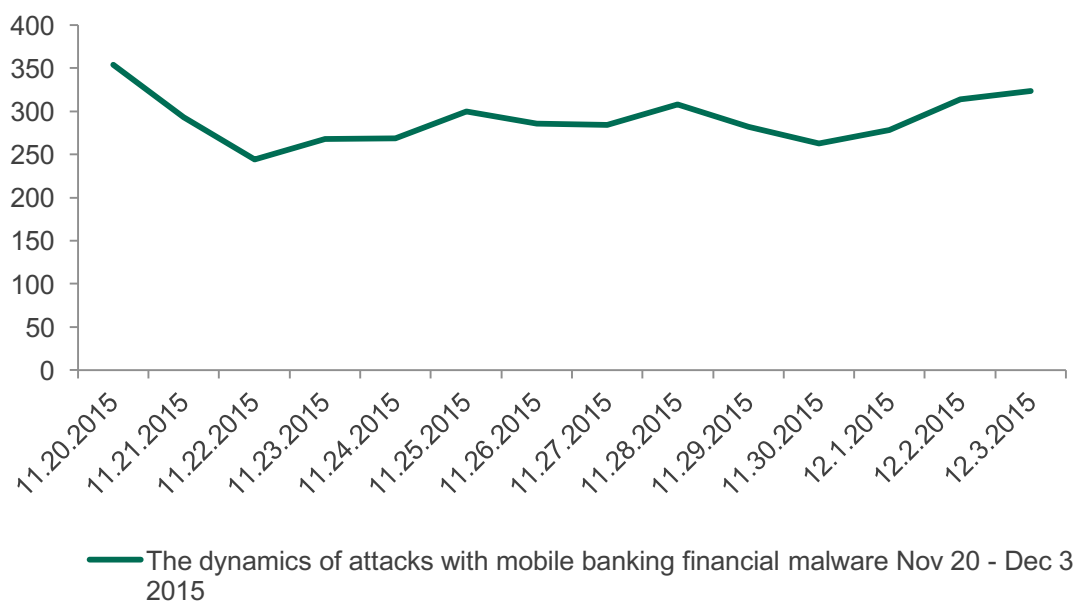


Fig. 21: The dynamics of attacks with mobile financial malware on Black Friday through Cyber Monday in 2015

POS malware

Another dangerous type of malware which we have already seen and are expecting to see during this season is POS-malware – the type of financial malware which infects the OS of point of sales terminals and then steals the credentials of the credit cards processed by these devices. So far, due to the specific nature of the devices that this type of malware tends to attack, we don't yet have relevant statistics on the number of detections during the holiday period.

However we can estimate the threat by counting the number of families which our experts added in recent years. In 2013 only 4 families were added to our collection, but the 2013 Target breach inspired many criminals to attempt to reproduce the “success” of those who hacked the famous retailer, and the next year 12 more families of POS-malware were added. 2015 was the hottest year in terms of POS malware with 14 new families. 2016 is fairly calm so far: 6 new families were added to our collection since the beginning of the year. In total there are at least 36 families of malware capable of stealing data from POS terminals out there in the wild. The number is even bigger than the amount of banking malware families, 30 species of which are now in the Kaspersky Lab collection.

Expect new attacks

The motivation behind attacks that are tied to concrete dates are clear: cybercriminals suggest that the chances that users will be working with their financial accounts online more

than usual are higher than on any other day. Therefore they tend to increase their hacking efforts to raise their own chances of stealing money. Judging by the dynamics of attacks of “holiday” dates from 2014 and 2015, Kaspersky Lab expects that in 2016, the situation may be repeated.

News from the Underground

While online shoppers are drawing up their wish-lists for the upcoming sales, retailers are preparing their stores for a massive rise in visitors, and financial infrastructure owners – banks and payment systems - are getting ready for a huge increase in the number and value of transactions, criminals are also preparing for the season. For this report Kaspersky Lab experts have conducted some research into events and discussions taking place on several secret, invitation-only underground forums, where users allegedly involved in different types of financial fraud tend to gather and discuss things.

More about Cyber Monday

Based on the results of the research, we can say that underground cybercriminals, at least on East European fora, are more excited about Cyber Monday than about Black Friday. This may be because Cyber Monday is more about online sales. There will be a lot of online advertising of special deals and it will be easier for them to hide phishing scams inside the stream of legitimate offers.

Also, from a logistics perspective, Cyber Monday is more convenient than Black Friday, which is more about offline sales. Criminals don't have to deal with physical access to ATMs in order to set up, and later collect a skimmer. Instead they could use a phishing or malware attack in order to collect credentials and then monetize them in a number of ways.

That said, ATM skimming attacks will happen during Black Friday and will continue through other holidays: Christmas and New Year.

ПРОБИН
ДАННЫХ
АБОНЕНТА

ПОД ОБНАЛ


ЗАЛИВЫ НА
QIWI
КОШЕЛЕК

ГОТОВЫЕ КАРТЫ
С БАЛАНСОМ

ВСЕ СТЕПЕНИ ЗАЩИТЫ

ЗАЛИВЫ

МОШЕННИКИ
НЕ ДАЮТ ПОКОЯ



Продажа скиммеров, купить скиммер по низкой цене

3/24

ажа скиммеров

ено 30 Март 2013 - 13:24

представляем вашему вниманию сервис по продаже скиммеров на банкоматы WINCOR, NCR, DIEBOLD.

анный момент мы поставляем следующие модели скиммеров, производство Китай:

ELANVA, HUP FOUNTAIN, HUP FOUNTAIN COME, HUP PLAC FANTO, HUP GREEN KAPIT

GREEN AND GREEN UNIT, SUBMINI ULTRA 4 GEM

берем нужную вам модель скиммера по фотографии банкомата, с клавишей, полный комплект.

Fig. 22: Example of an online advertisement of skimmers on one of hacker forums

Based on information from the last year, during December 2015 more than 500 skimmers were sold on an East European black market, while “usual” sale rate is 25 – 30 devices per month. These devices come packed with everything necessary for successful data-stealing, like fake PIN-pads, hidden cameras etc. The vast majority (around 96.5%) of skimmers mimic the products of four popular vendors, and the rest 3.5% are skimmers that replicate custom models.

As a result of the 2015 holiday fraud campaign, criminals experienced certain problems with the cashing out of compromised cards. Based on conversations on the corresponding web resources, the cash-out projects (groups that undertake the cash-out for other criminals) were heavily overloaded so the cash-out orders took three months to complete. This was due to a large number of stolen credentials waiting to be cashed-out. According to Kaspersky Lab data, during December 2015 criminals were able to collect approximately 10 times as many credentials as during a non-holiday period. Basically this equates to the total number of card details they are usually able to steal during the rest of the year.

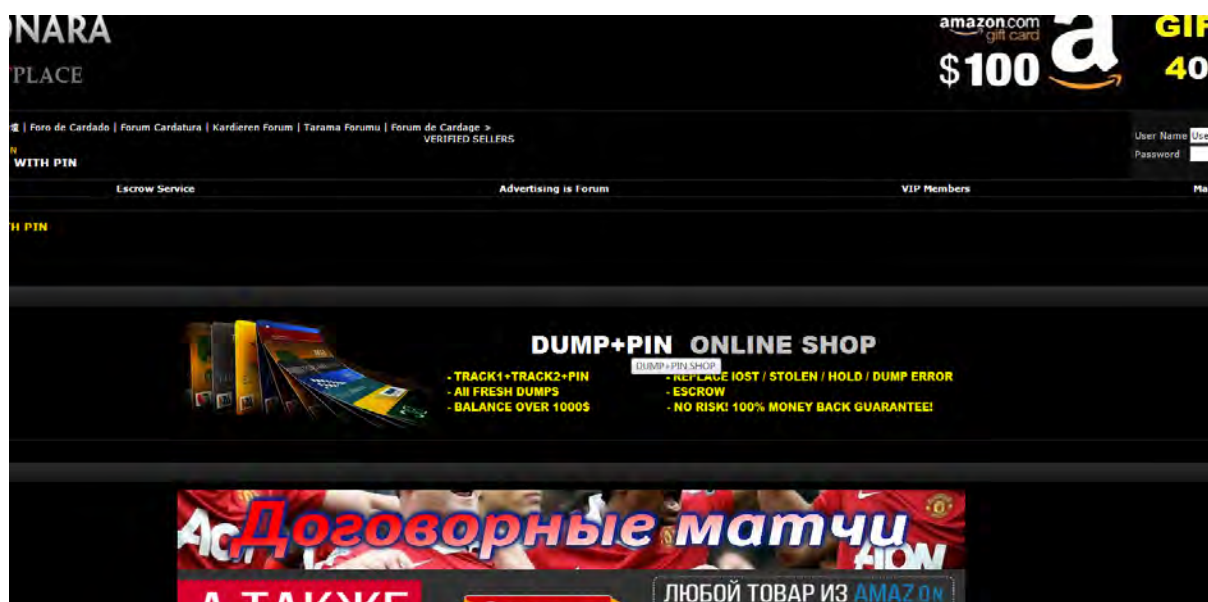


Fig. 23: Example of advertisement of an online-shop of stolen credit cards credentials

Information on several forums suggests that, in 2016, a month prior to the start of the Black Friday, vendors of skimmers were already experiencing an increase in sales, alongside vendors of blank cards that will later be used to clone stolen cards. Also, some vendors are offering new generations of POS skimmers which are attached to legitimate POS's. Unlike earlier skimmers, the new generation is placed inside the card reader, which makes them much harder to spot with the naked eye.

Another interesting trend is that many criminals are avoiding starting their campaigns with malware, choosing instead phishing attacks because they consider them to be more efficient and safe. Besides that they are actively utilizing schemes that involve direct contact with the

victim. In these attacks the fraudsters will call the victim, seemingly on behalf of a bank, and try to find out their credit card credentials with help of psychological tricks.

Kaspersky Lab experts also expect that more cases of cash-out through Apple Pay and Samsung Pay payment systems will happen during this holiday season. The recent increase in the list of countries where the systems are supported has brought a certain inspiration to criminal community. The ability to attach a card to an Apple ID and then use it to pay for real goods creates a relatively convenient way to cash-out for so called “stuffers” – criminals who specialize in cashing out through buying goods from internet and physical shops, as well as for virtual carders – criminals who monetize stolen credentials through virtual goods

Another rather interesting conclusion made by Kaspersky Lab researchers during their research of the cybercriminal underground, is that fraudsters expect a lot of profits from attacks during the holiday period, especially the pre- and post- Christmas to New Year period, not only due to the high number of buyers seeking to spend money, but also because (based on their experience, which they share on forums) in this period the anti-fraud departments of banks are weakened. Due to many employees going on vacation around these dates, banks suffer from a lack of personnel, and it is theoretically easier for criminals to hide fraudulent operations in the stream of legal ones.

The screenshot displays a website interface with four main service categories, each with a list of options and prices:

- Услуга DDoS атак.** (DDoS Attack Service)
 - Заказать DDoS атаку на сайт или сервер?! (Order a DDoS attack on a website or server?!)
 - Протестировать нагрузку сайта?! (Test the website load?!)
 - 1 Сервера VPS от - от 50\$.
 - 2 Сервера VDS - от 75\$.
 - 3 Сервера под защитой - от 250\$.
- Защита от DDoS атак.** (Protection from DDoS attacks)
 - Защита сайта, сервера от DDoS атак. (Protection of website, server from DDoS attacks.)
 - Выделенные сервера в аренду (Dedicated servers for rent)
 - 1 Защита сайта от DDoS - от 50\$.
 - 2 VPS, VDS сервера - от 100\$.
 - 3 Dedicated сервер - от 300\$.
- Блокировка сайта** (Website blocking)
 - Заблокировать доменное имя на заказ? Нет проблем, мы уберем любые сайты которые Вам необходимо стереть с интернета.. (Block domain name on order? No problem, we will remove any websites you need to delete from the internet..)
 - 1 Услуга блокировки домена - от 1200\$.
- Услуга флуд - атак на телефоны** (Flood attack service on phones)
 - Заказать атаку на мобильные, стационарные телефоны по всему миру с подменой номера. (Order an attack on mobile, landline phones worldwide with number spoofing.)
 - 1 Час - от 20\$.
 - 2 Сутки - от 100\$.
 - 3 Неделя - от 500\$.

Fig. 24: Example of fraudster's website selling DDoS-attacks service

Other types of criminal groups – such as those specializing in DDoS attacks, will most likely try to attack online shops for the purpose of blackmailing. That is a well-known tactic which they use against small and medium retail organizations. By setting up a DDoS attack they would block access to the attacked store and, until the owner pays a ransom, they would keep it blocked. Not wanting to lose money because of the unavailability of the store the owners will often pay the criminals. This is likely to happen in the coming holiday season.

Conclusion and advice

The main purpose of this paper is to raise awareness of the threats that may ruin the upcoming holiday season for regular users and shoppers and owners of online stores and owners of financial infrastructure. Both Kaspersky Lab telemetry and the analysis of conversations happening on the underground suggest that cybercriminals will pay special attention to the upcoming high sales season. But this doesn't mean that the holidays are already doomed.

If prepared, each legitimate party of this process: buyers, sellers and financial services providers will end up in profit. All they have to do is to follow some simple advice.

For regular users

- Do not click on any links received from unknown people or on suspicious links sent by your friends on social networking sites or via e-mail. They can be malicious; created to download malware to your device or to lead to the phishing webpages aimed at harvesting user credentials.
- Do not download, open or store unfamiliar files on your device, they can be malicious.
- Do not use unreliable (public) Wi-Fi networks to make online payments, as hotspots can be easily hacked in order to listen to user traffic and to steal confidential information.
- Do not enter your credit card details on unfamiliar or suspicious sites, to avoid passing them into cybercriminals' hands.
- Always double-check the webpage is genuine before entering any of your credentials or confidential information (at least take a look at the URL). Fake websites may look just like the real ones.
- Only use sites which run with a secure connection (the address of the site should begin with HTTPS:// rather than HTTP://) to hinder theft of information transmitted.
- Don't tell anybody your one-time password or PIN-code, not even a bank representative. Cybercriminals can use this data to steal your money.
- Install a security solution on your device with built-in technologies designed to prevent financial fraud. For example, Safe Money technology in Kaspersky Lab's solutions creates secure environment for financial transactions on all levels.
- And don't forget about the same rules when using your mobile device for financial transactions, because cybercriminals and fraudsters target them too.

For retailers

- Keep your e-commerce platform up-to-date. Every new update may contain critical patches to make the system less vulnerable to cybercriminals.
- Pay attention to the personal information used for registration. Fraudsters tend to hide their identities but lack of creativity can serve as an indication of fraud. John Smith whose email address reads as 21192fjdj@xmail.com is likely to be a criminal. Check again and request more details from customers if needed. Adding captcha might be effective measure against this.
- Restrict the number of attempted transactions. Criminals usually make multiple attempts to enter correct card numbers for one purchase. Use captcha and increased time intervals for attempts to re-enter card numbers.
- Use two-factor authentication (Verified by Visa, MasterCard Secure Code and etc.). It will dramatically drop the number of cases of illegal card usage.
- Be careful with suspicious orders. Several unrelated high-value items for more than \$500 and extra payment for fast shipping to another country can be a sign of a criminal hurrying to resell as soon as possible. In such cases it is recommended to contact the customer on the phone and confirm the order.
- Use tailored security solution to protect your point of sales terminals from malware attacks and make sure your POS terminals run the latest version of software.
- Criminals may attempt to DDoS the website of your shop for blackmail purposes. Make sure that your IT security team is prepared for such attacks or, if you don't have one, ask your hosting provider if it is possible to purchase a DDoS-protection service from them.
- Educate your clients on possible cyberthreats they may encounter while shopping online and offline

For financial organizations

- Introduce enterprise-wide fraud prevention strategy with special sections on ATM and internet banking security. Logical security, physical security of ATMs and fraud prevention measures should be addressed altogether as attacks are becoming more complex.

- Conduct annual security audits and penetration tests. It is better to let professionals find vulnerabilities than wait until they will be found by cybercriminals.
- Choose a multi-layered approach and techniques against fraud. Training employees to spot suspicious transactions should be combined with implementation of dedicated fraud prevention solutions. Financial security software based on innovative technologies helps to detect and fight fraudulent activity beyond human control.
- Do not leave self-protection to customers. It is hardly possible to educate all customers – and it is always better to create a multi-layer security architecture that will provide all the services with the necessary level of security.
- Remember that insiders are usually involved in half or more cybersecurity incidents. Use security approaches that allow for the detection of suspicious and potentially dangerous activity inside your infrastructure.
- Make sure that your anti-fraud department is fully staffed during the holiday period.

For more info contact us at: intelreports@kaspersky.com
(Kaspersky Security Intelligence Service)



[Securelist](#), the resource
for Kaspersky Lab experts'
technical research,
analysis, and thoughts.

Follow us



[Kaspersky Lab global Website](#)



[Eugene Kaspersky Blog](#)



[Kaspersky Lab B2C Blog](#)



[Kaspersky Lab B2B Blog](#)



[Kaspersky Lab security news service](#)



[Kaspersky Lab Academy](#)