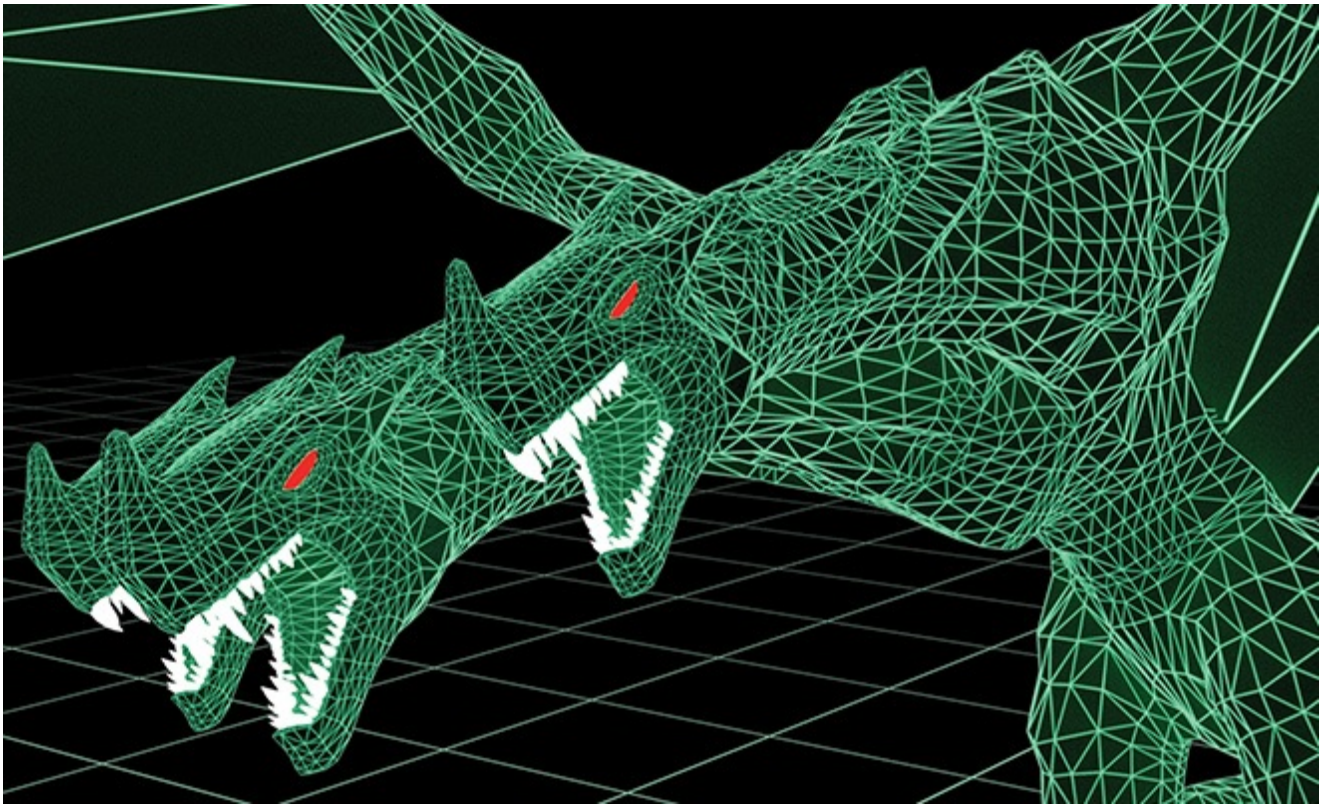
Kaspersky Security Bulletin 2016. Review of the year. Overall statistics for 2016

securelist.com/kaspersky-security-bulletin-2016-executive-summary/76858/



Authors

Expert Kaspersky

Executive Summary

Download Review of the year

Download Overall statistics

Download the consolidated Kaspersky Security Bulletin 2016

Introduction

If they were asked to sum up 2016 in a single word, many people around the world – particularly those in Europe and the US – might choose the word ‘unpredictable’. On the face of it, the same could apply to cyberthreats in 2016: the massive botnets of connected devices that paralysed much of the Internet in October; the relentless hacking of high profile websites and data dumps; the SWIFT-enabled bank heists that stole billions of dollars, and more. However, many of these incidents had been in fact been predicted, sometimes years ago, by the IT security industry, and the best word for them is probably ‘inevitable’.

> For cyberthreats, 2016 was the year when “sooner or later” became “now” #KLReport
>
> Tweet

Most of all, in 2016, ransomware continued its relentless march across the world – with more new malware families, more modifications, more attacks and more victims. However, there are rays of hope, including the new, collaborative No More Ransom initiative. Kaspersky Lab has designated the revolution in ransomware its Story of the Year for 2016 and you can read more about its evolution and impact here.

Elsewhere on the cybersecurity landscape, targeted cyberespionage attacks, financial theft, ‘hacktivism’ and vulnerable networks of connected devices all played their part in what has been a tense and turbulent year.

This Executive Summary provides an overview of the top threats and statistics for 2016. Full details are included in the accompanying Review & Statistics.

It also considers what these threats mean to organisations trying spot a breach or cyberattack. How ready are businesses to proactively prevent and mitigate a cyberthreat? What can be done to help them?

Six things we learned this year that we didn’t know before

1. That the underground economy is more sophisticated and bigger than ever: xDedic – the shady marketplace

In May, we uncovered a large, active cybercriminal trading platform, called xDedic. xDedic listed and facilitated the buying and selling of hacked server credentials. Around 70,000 compromised servers were on offer – although later evidence suggests that there could have been as many as 176,000 – located in organisations around the world. In most cases, the legitimate owners had no idea that one of their servers, humming away in a back room or data center, had been hijacked and was being passed from criminal to criminal.

xDedic is not the first underground marketplace, but it is evidence of the growing complexity and sophistication of the black market economic ecosystem.

"xDedic is a hacker's dream, simplifying access to victims, making it cheaper and faster, and opening up new possibilities for both cybercriminals and advanced threat actors."

GReAT

2. That the biggest financial heist did not involve a stock exchange: the SWIFT-enabled transfers

One of the most serious attacks in 2016 was that using the inter-bank network, SWIFT (Society for Worldwide Interbank Financial Telecommunication). In February 2016, hackers used the SWIFT credentials of Bangladesh Central Bank employees to send fraudulent transaction requests to the Federal Reserve Bank of New York, asking it to transfer millions of dollars to various bank accounts in Asia. The hackers were able to get $81 million transferred to the Rizal Commercial Banking Corporation in the Philippines and an additional $20 million to Pan Asia Banking. The campaign was cut short when the bank spotted a typo in one of the transfer requests. You can read the story here. In the following months, further bank attacks using SWIFT credentials came to light.

> Following the theft of $100 million many banks were forced to improve their authentication and SWIFT software update procedures #KLReport
>
> Tweet

3. That critical infrastructure is worryingly vulnerable: the BlackEnergy attacks

BlackEnergy deserves a place in this list even though, strictly speaking, it took place at the end of 2015. However, it was only in early 2016 that the full effect of the BlackEnergy cyber-attack on the Ukrainian energy sector became clear. The attack was unique in terms of the damage it caused. This included disabling the power distribution system in Western Ukraine, wiping software on targeted systems and unleashing a Distributed Denial of Service (DDoS) attack on the technical support services of affected companies. Kaspersky Lab has supported the investigation into BlackEnergy since 2010, with among other things, an analysis of the tool used to penetrate the target systems. You can find our 2016 report here.

> The BlackEnergy cyberattack on the Ukrainian energy sector revealed the vulnerability of critical infrastructures worldwide #KLReport
>
> Tweet

To help organizations working with industrial control systems (ICS) to identify possible points of weakness, Kaspersky Lab experts have conducted an investigation into ICS threats. Their findings are published in the Industrial Control Systems Threat Landscape report.

4. That a targeted attack can have no pattern: the ProjectSauron APT

In 2016 we discovered the ProjectSauron APT: a likely nation-state backed cyberespionage group that has been stealing confidential data from organisations in Russia, Iran and Rwanda – and probably other countries – since June 2011. Our analysis uncovered some remarkable features: for example, the group adopted innovative techniques from other major APTs, improving on their tactics in order to remain undiscovered. Most importantly of all: tools are customized for each given target, reducing their value as Indicators of Compromise (IoCs) for any other victim. An overview of the methods available to deal with such a complex threat can be found here.

> ProjectSauron's pattern-less spying platform has far-reaching implications for some basic principles of threat detection #KLReport
>
> Tweet

5. That the online release of vast volumes of data can be an influential tactic: ShadowBrokers and other data dumps

2016 saw a number of remarkable online data dumps. The most famous is probably that by a group calling itself the ShadowBrokers. On August 13, they appeared online claiming to possess files belonging to the ultimate APT predator, the Equation Group. Our research suggests there are similarities between the data dumped by ShadowBrokers and that used by the Equation Group. The initial data dump included a number of unreported zero-days, and there have been further dumps in recent months. The long-term impact of all this activity is unknown, but is has already revealed the huge and rather worrying influence such data dumps can potentially have on public opinion and debate.

In 2016 we also witnessed data breaches at beautifulpeople.com, Tumblr, the nulled.io hacker forum, Kiddicare, VK.com, Sage, the official forum of DotA 2, Yahoo, Brazzers, Weebly and Tesco Bank – for motives ranging from financial gain to personal reputation blackmail.

> A LinkedIn hack made public in 2016 revealed over a million uses of the password '123456'. #KLReport
>
> Tweet

6. That a camera could be part of a global cyber-army: the insecure Internet of Things

Connected devices and systems, from homes and vehicles to hospitals and smart cities, exist to make our lives safer and easier. However, many were designed and manufactured without much thought for security – and sold to people who underestimated the need to protect them with more than default factory security settings.

> The risk of connecting everything without proper safeguards – after 2016, need we say more? #KLReport
>
> Tweet

As the world now knows, all these millions of insecure connected devices represent a powerful temptation to cybercriminals. In October, attackers used a botnet of over half a million internet-connected home devices to launch a DDoS attack against Dyn – a company that provides DNS services to Twitter, Amazon, PayPal, Netflix and others. The world was shocked, but warnings about unstable IoT security have been around for a long time.

For example, in February, we showed how easy it was to find a hospital, gain access to its internal network and take control of an MRI device – locating personal data about patients and their treatment procedures and obtaining access to the MRI device file system. In April, we published the results of our research into, among other things, the vulnerability of city traffic sensors and smart ticket terminals.

> Manufacturers need to work with the security industry to implement 'security-by-design' #KLReport
>
> Tweet

Other top threats

Inventive APTs

> At least 33 countries were targeted by APTs reported on by Kaspersky Lab #KLReport
>
> Tweet

In February, we reported on Operation Blockbuster, a joint investigation by several major IT security companies into the activities of the Lazarus gang, a highly malicious entity responsible for data destruction.

> The Lazarus group is believed to have been behind the attack on Sony Pictures Entertainment in 2014 #KLReport
>
> Tweet

Adwind, is a cross-platform, multi-functional RAT (Remote Access Tool) distributed openly as a paid service, where the customer pays a fee in return for use of the malicious software. It holds the dubious distinction of being one of the biggest malware platforms currently in existence, with around 1,800 customers in the system by the end of 2015.

> Adwind's malware-for-rent had a customer base of 1,800 #KLReport
>
> Tweet

APTs everywhere continued to make the most of the fact that not everyone promptly installs new software updates – in May we reported that at least six different groups across the Asia-Pacific and Far East regions, including the newly discovered Danti and SVCMONDR groups, were exploiting the CVE-2015-2545 vulnerability. This flaw enables an attacker to execute arbitrary code using a specially-crafted EPS image file. A patch for the vulnerability was issued back in 2015.

> Over six APT groups used the same vulnerability – patched back in 2015 #KLReport
>
> Tweet

New zero-days

Zero-days remained a top prize for many targeted attackers.

In June, we reported on a cyber-espionage campaign launched by a group named ScarCruft and code-named Operation Daybreak, which was using a previously unknown Adobe Flash Player exploit (CVE-2016-1010). Then in September we discovered a Windows zero-day, CVE-2016-3393, being used by a threat actor known as FruityArmor to mount targeted attacks.

In all, new Kaspersky Lab technologies designed to identify and block such vulnerabilities helped us to uncover four zero-days in 2016. The other two are an Adobe Flash vulnerability CVE-2016-4171 and a Windows EoP (Escalation of Privilege) exploit CVE-2016-0165 .

The hunt for financial gain

Tricking people into either disclosing personal information or installing malware that then seizes the details for their online bank account remained a popular and successful option for cyber-thieves in 2016. Kaspersky Lab solutions blocked attempts to launch such malware on 2,871,965 devices. The share of attacks targeting Android devices increased more than four-fold.

> A third of banking malware attacks now target Android devices #KLReport
>
> Tweet

Some APT groups were also more interested in financial gain than cyberespionage. For example, the group behind Metel infiltrated the corporate network of banks in order to automate the roll-back of ATM transactions: gang members could then use debit cards to repeatedly steal money from ATMs without ever affecting the balance on the card. At the end of 2016 this group remains active.

> Metel launched targeted attacks on banks – then sent teams to ATMs at night to withdraw the cash #KLReport
>
> Tweet

In June, Kaspersky Lab supported the Russian police in their investigation into the Lurk gang. The collaboration resulted in the arrest of 50 suspects allegedly involved in creating networks of infected computers and the theft of more than 45 million dollars from local banks, other financial institutions and commercial organizations.

During the investigation, researchers spotted that users attacked by Lurk had the remote administration software Ammyy Admin installed on their computers. This led to the discovery that that the official Ammyy Admin website had most probably been compromised, with the Trojan was downloaded to users' computers along with the legitimate Ammyy Admin software.

> The takedown of the Lurk gang was the largest ever arrest of hackers in Russia #KLReport
>
> Tweet

The ultimate vulnerability: people

2016 also revealed that targeted attack campaigns don't always need to be technically advanced in order to be successful. Human beings – from hapless employees to malicious insiders – often remained the easiest access route for attackers and their tools.

In July, we reported on a group called Dropping Elephant (also known as 'Chinastrats' and 'Patchwork'). Using high quality social engineering combined with old exploit code and some PowerShell-based malware, the group was able to successfully steal sensitive data from high-profile diplomatic and economic organisations linked to China's foreign relations.

> Dropping Elephant and Operation Ghoul confirmed the fearsome power of high quality social engineering #KLReport
>
> Tweet

Further, Operation Ghoul sent spear-phishing e-mails that appeared to come from a bank in the UAE to top and middle level managers of numerous companies. The messages claimed to offer payment advice from the bank and attached a look-like SWIFT document containing malware.

*"*Cybercriminals are using insiders to gain access to telecommunications networks and subscriber data, recruiting disaffected employees through underground channels or blackmailing staff using compromising information gathered from open sources." Threat Intelligence Report for the Telecommunications Industry

Mobile advertising

The main mobile threats in 2016 were advertising Trojans able to obtain 'root' or superuser rights on an infected Android device – a level of access that allowed them to do pretty much whatever they wanted. This included hiding in the system folder, thereby making themselves almost impossible to delete, and silently installing and launching different apps that aggressively display advertising. They can even buy new apps from Google Play.

> 22 of the 30 most popular Trojans in 2016 are advertising Trojans – twice as many as in 2015 #KLReport
>
> Tweet

Many such Trojans were distributed through the Google Play Store: some of them were installed more than 100,000 times, and one – an infected Pokemon GO Guide app was installed more than 500,000 times.

> Malware distributed through Google Play was downloaded hundreds of thousands of times #KLReport
>
> Tweet

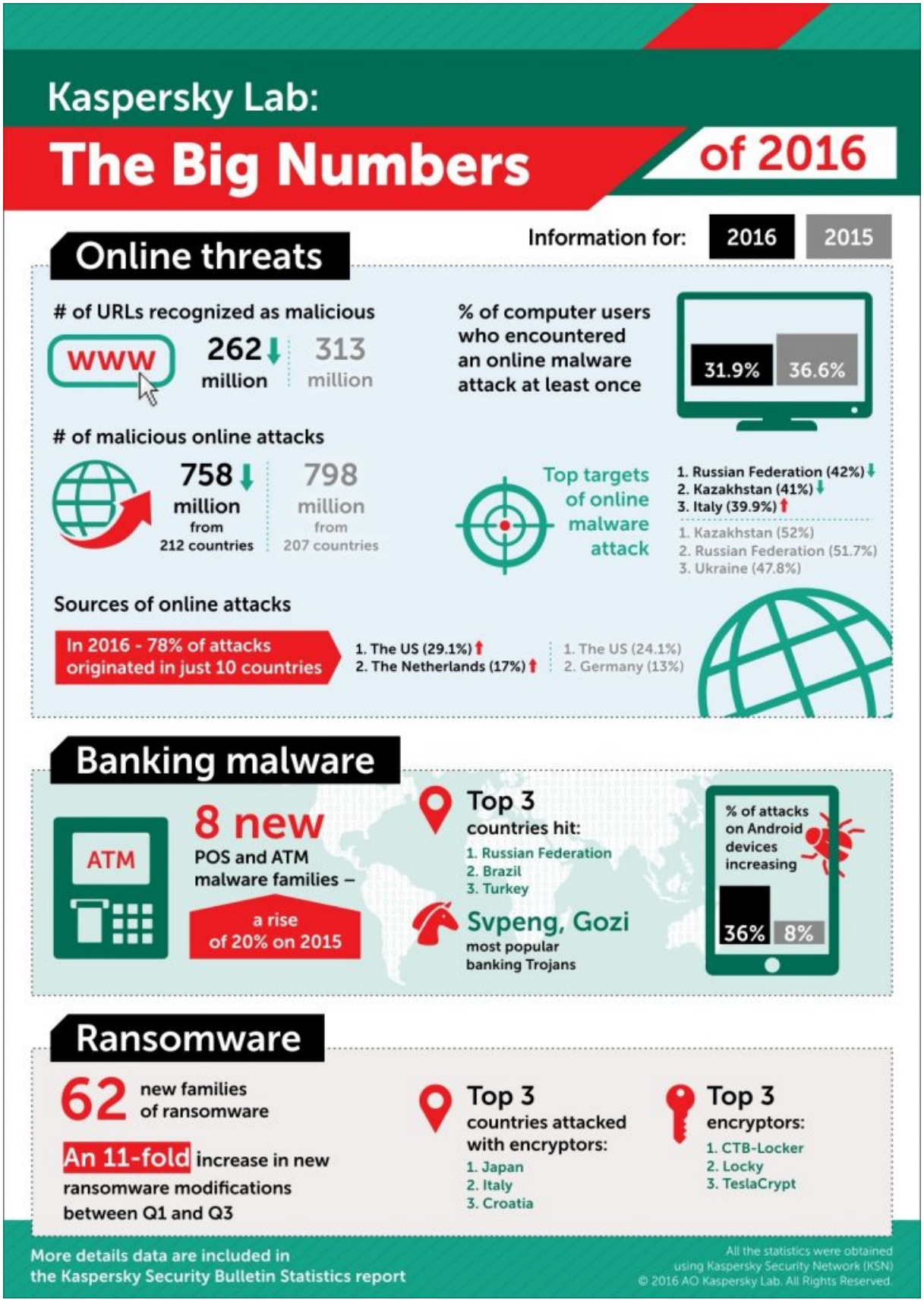
One Android Trojan installed and even updated as a 'clean' (malware-free) app before hitting targets with an infected version. Others, including Svpeng, used the Google AdSense advertising network for distribution

Further, some Trojans found new ways to bypass Android security features – in particular the screen overlays and the need to request permission before opening a new app – forcing the user to sign over the access rights the Trojan was looking for.

Mobile ransomware also evolved to make use of overlays, blocking rather than encrypting data since this is generally backed-up.

To read more on these stories, please download the full annual Review for 2016 here.

For an in-depth look at the Statistics for 2016, please register to download the Statistics report here.



The impact on business

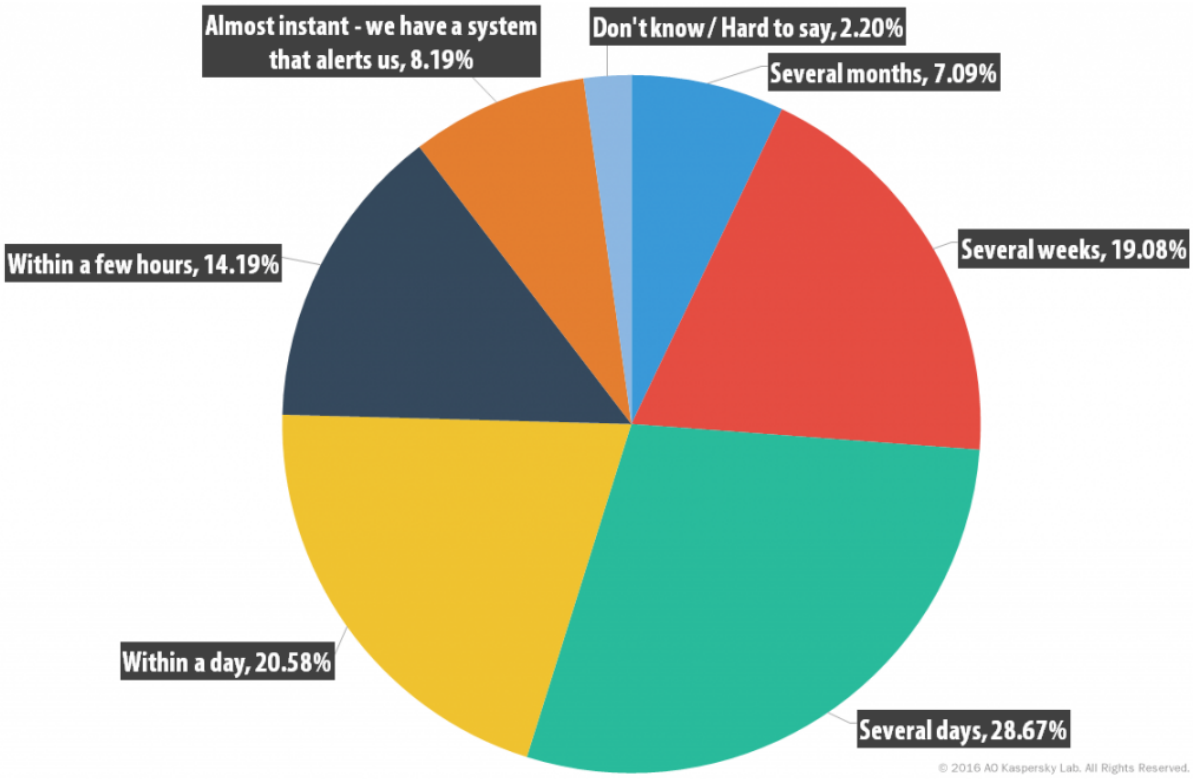
The 2016 threat landscape indicates a growing need for security intelligence

The Kaspersky Security Bulletin 2016 highlights the rise of complex and damaging cybersecurity threats, many of which have a far-reaching impact on businesses. This impact is also reflected in our Corporate IT Security Risks Reports (1, 2) based on a 2016 survey of more than 4000 businesses worldwide.

Among other things, the survey asked companies about the most crucial metric of incident detection and response: time.

Incident detection time is critical

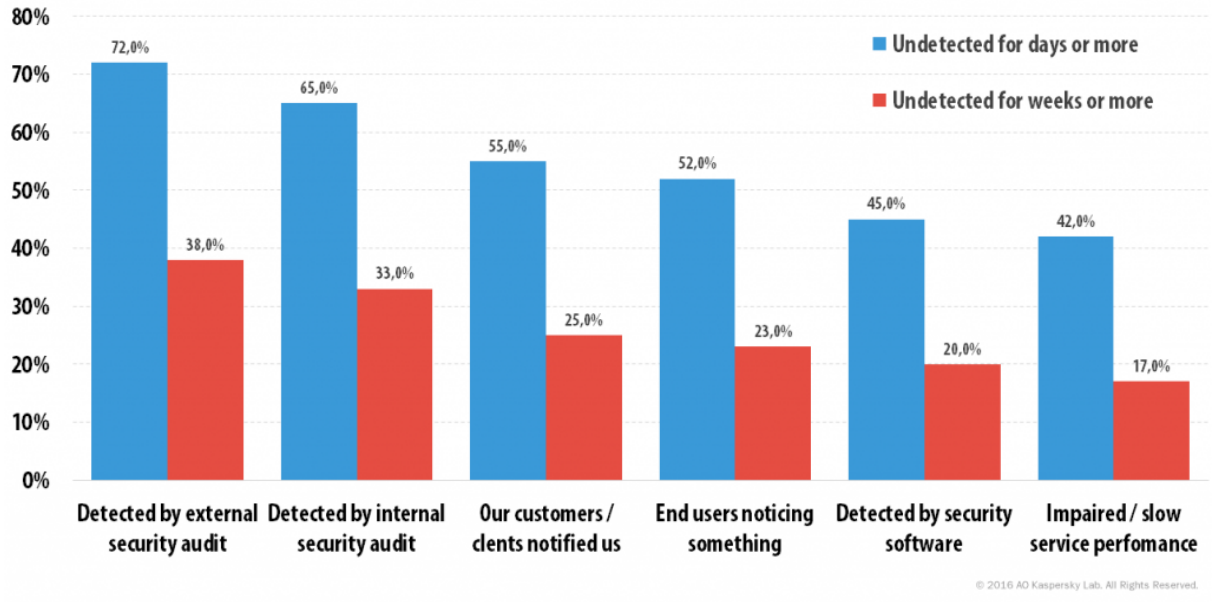
Previously unreleased findings from the research show that the typical time required to detect an IT Security event is several days – **28.7%** of companies said it took them that long to detect a security breach on average.



Time required to detect an IT security event

Only **8.2%** of businesses managed to detect security breaches almost instantly, and for **19.1%** of businesses it took several weeks to detect a serious security event. When we asked how they eventually detected a long-standing breach, the replies were revealing.

Going beyond prevention



Average time frame required to detect a security event, across all security events within the last 12 months

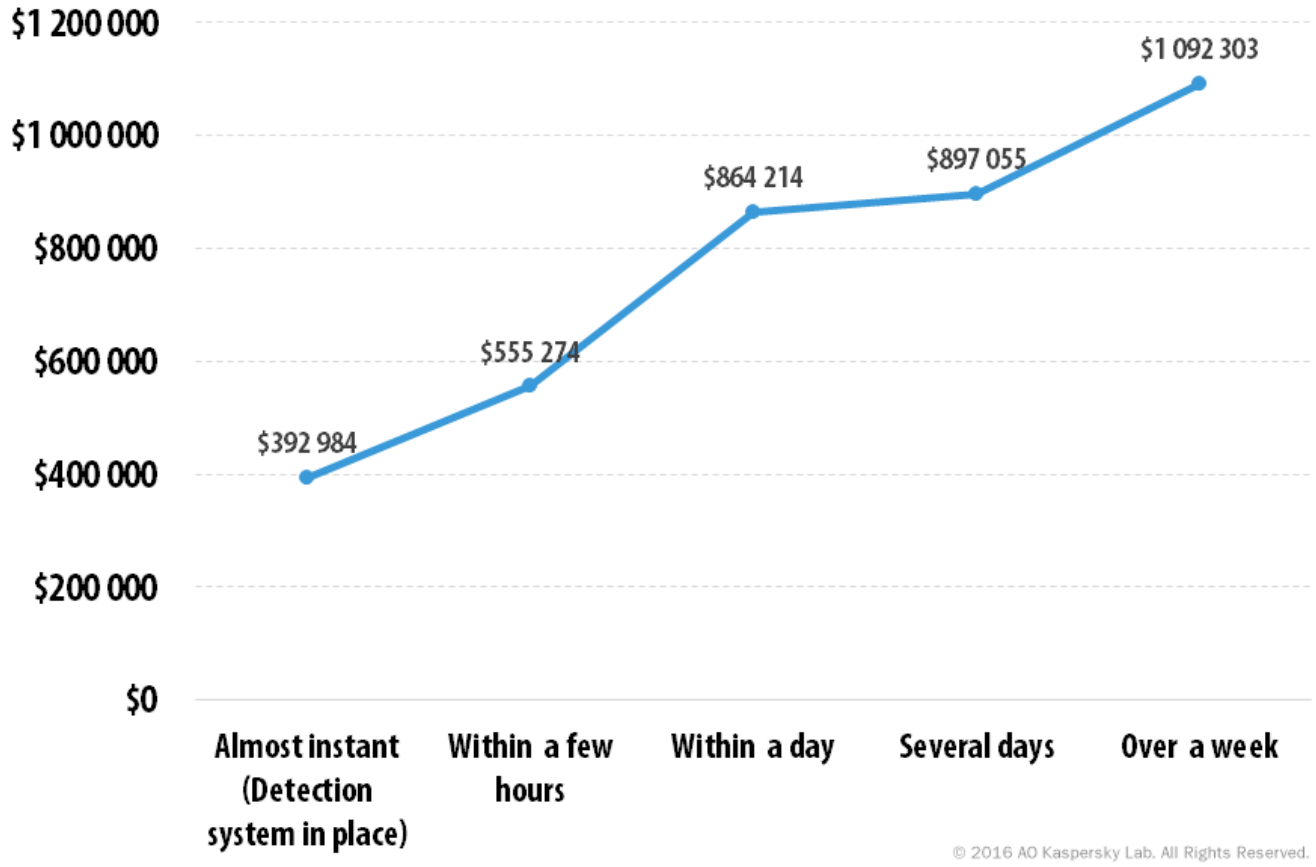
In this chart we combine the average time to discover a security event with the responses we received on how businesses detected a breach. Apparently, businesses that struggle to detect a breach quickly, eventually spot them through one or more of the following: an external or internal security audit, or, sadly, notification from a third party.

It turns out that for these businesses a security audit of any kind is the best measure of 'last resort' to finally bring it to light. But should it be only a last resort?

This is where our report detects an obvious discrepancy between theory and practice. Although **65%** of businesses admit that a security audit is an effective security measure, less than half of the companies surveyed (**48%**) have conducted such audit in the last 12 months. Further, **52%** of companies operate under the assumption that their IT security will inevitably be compromised at some point, although 48% are not ready to accept this. In short: **many businesses find a structured detection and response strategy difficult to embrace**.

The cost of delay

It is safe to assume that the longer it takes to detect a security breach, the higher the mitigation costs and the greater the potential damage. The results reveal the shocking truth that failure to discover an attack within a few days, results in a doubling, or more of the costs.



Cost of recovery vs. time needed to discover a security breach for enterprises

For enterprises, an attack undiscovered for a week or more costs 2.77 times that of a breach detected almost instantly. SMBs end up paying 3.8 times more to recover from an incident detected too late.

It is clear that better detection significantly reduces business costs. But the implementation of incident detection and response strategies is quite different from ensuring proper prevention. The latter provides a choice of well-established corporate solutions. The former requires security intelligence, a deep knowledge of the threat landscape, and security talent capable of applying that expertise to the unique specifics of a company. According to our special Corporate IT Security Risks report, businesses that struggle to attract security experts end up paying twice as much for their recovery after an incident.

Kaspersky Lab's solution: turning intelligence into protection

In 2016 Kaspersky Lab significantly expanded its portfolio with products like Kaspersky Anti-Targeted Attack Platform and security services like Penetration Testing and Threat Data Feeds, all to help meet customer needs for better detection and response. Our plan is to offer security intelligence via any means necessary: with a technology to detect targeted threats, a service to analyze and respond to a security event, and intelligence that helps investigate an issue properly.

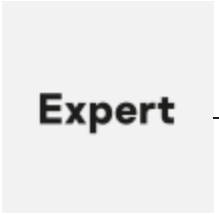
Watch Video At:

https://youtu.be/9myhQw1exTE

We appreciate that, for many businesses, going beyond prevention is a challenge. But even a single targeted attack that is detected early and mitigated rapidly is worth the investment – and increases the chances that the next assault on the corporate infrastructure is prevented outright.

- APT
- BlackEnergy
- Equation
- Financial malware
- Internet of Things
- Malware Statistics
- ProjectSauron
- Shadow Brokers
- Zero-day vulnerabilities

Authors



Kaspersky

Kaspersky Security Bulletin 2016. Review of the year. Overall statistics for 2016

Your email address will not be published. Required fields are marked *