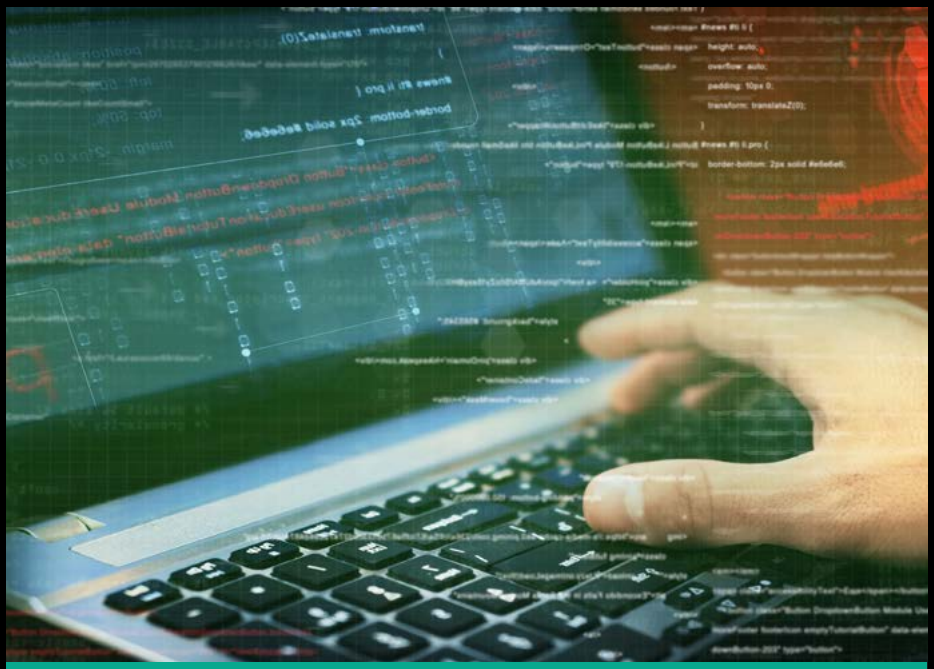
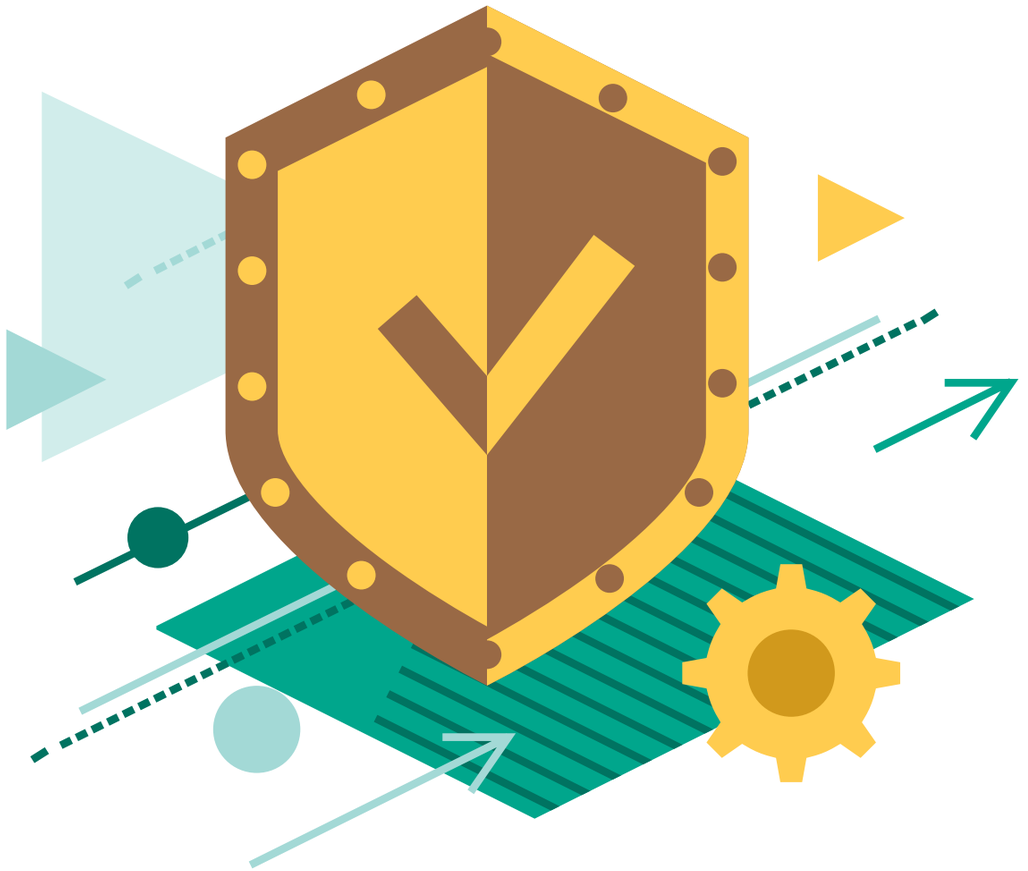
SECURITY SPOTLIGHT



Cybercriminals: Exposing the Villain

KASPERSKY lab

Cybercriminals hide behind anonymity to carry out their crimes, operating under a veil of secrecy to conceal who they are and what they're up to. By understanding the data we collect through our Kaspersky Security Network (KSN) and absorbing the industry intelligence from our GReAT (Global Research and Analysis Team) researchers, you can learn more about what their tactics are and how you can protect your business.



Cybercrime damages are expected to cost the world $6 trillion by 2021.[1]

Cybercriminals are more organized and efficient than ever before

Cybercrime is big business. No longer solely the realm of rogue hackers operating alone, cybercriminals are increasingly banding together into organized groups and have even taken the step of offering their services for hire to other cybercriminals.

Increasingly, Kaspersky Lab is seeing a shift from attacks on individuals to attacks on corporations and stealing money and data from them. And it is paying off. Cybercrime cost the global economy over $450 billion in 2016, according to the Hiscox Cyber Readiness Report 2017. [2]

Many businesses have a false sense of security around this issue. While large enterprises often shore up their own IT security measures, small- and medium-sized businesses mistakenly assume that they will not be a target of cybercriminals. The fact is that almost any business can become a target, and no industry is immune. If you are a trusted vendor for a larger company, you may have access to information that cybercriminals want and provide the backdoor access that they are looking for.

1. Cybercrime damages expected to cost the world $6 trillion by 2021
2. Cybercrime costs the global economy $450 billion: CEO

Cybercriminal tricks and tactics

So, how do they break through these organizations? In 2016, Kaspersky Lab's own data showed some interesting trends.

For one thing, the underground economy is more sophisticated and bigger than ever. Kaspersky Lab discovered a large cybercriminal trading platform called XDedic, which listed and facilitated the buying and selling of hacked server credentials. Around 70,000 compromised servers were on offer in organizations around the world.[3]

We also observed new techniques for masking exploits, specifically with the use of encryption protocol to make the detection of malicious codes more difficult. Cybercriminals also are increasingly using bitcoin to make transactions in order to avoid detection.

Finally, no assessment of today's cybercriminal is complete without noting the explosive growth of ransomware. Businesses went from being attacked every 2 minutes in Q1 to being attacked every 40 seconds in Q3 of 2016. 2016 also saw ransomware grow in sophistication and diversity. It changed tack if it encountered financial software, was written in scripting languages, or exploited new infection paths.[4]

In this eBook, we'll look closely at these trends to answer your most pressing questions about cybercriminals, such as:

- What motivates them?
- What kinds of targets do they look for?
- When do we see spikes in activity and in what industries?

Most important, we will answer **what you can do to protect your business** from this growing threat.

3. Kaspersky Security Bulletin 2016. Review of the year. Overall statistics for 2016
4. Kaspersky Security Bulletin 2016. The Ransomware Revolution

240K

Total number of sensitive customer or employee records that are compromised at a large enterprise if a data breach goes undetected for over a year.[5]

They want to make money

It should come as no surprise that the main motivation behind cybercrime is, ultimately, money.

In some cases, attacks are motivated by geopolitical causes, but the research points to one main reason they keep dipping back into this well—it's incredibly lucrative. Kaspersky Lab's research shows that the cybergang Carbanak has stolen $1 billion from different companies around the world.[6] That's a good return for any venture.

Ransomware, a type of software that blocks access to a computer system until a ransom is paid, is just one example of how profitable cybercrime can be. While Ransomware-as-a-Service is not a new trend, in 2016 this propagation model continued to develop, with more and more ransomware creators offering their malicious product 'on demand'. This approach has proved immensely appealing to criminals who lack the skills, resources or inclination to develop their own. Someone looking to use the Stompado ransomware, for example, needs to come up with just $39.[7] With those kinds of numbers, it's no wonder cybercriminals are following the profit.

On the front end, the cost of entry into cybercrime is relatively cheap. Creating a phishing page to mimic a popular social network and setting up a spam mass email that links to the fake site currently costs an average of $150. If the criminals catch 100 people, they can net up to $10,000 by selling sensitive data.

Ransomware is also a lucrative criminal business. One of the most direct ways for cybercriminals to make money is by targeting bank customers. In 2016, Kaspersky Lab solutions blocked attempts to launch malware capable of stealing money via online banking on 2,871,965 devices.[8]

> "Buying malware is currently not a problem: it's easy to find them on various hacker forums, and they are relatively cheap, making them attractive."
>
> —Alexander Gostev, Chief Security Expert at Kaspersky Lab

5. Corporate IT Security Risks Survey 2016 from Kaspersky Lab and B2B International
6. Dozens of banks lose millions to cybercriminals attacks
7. Dirt Cheap Stampado Ransomware Sells on Dark Web for $39
8. Kaspersky Security Bulletin 2016 Review of the Year

2x-5x

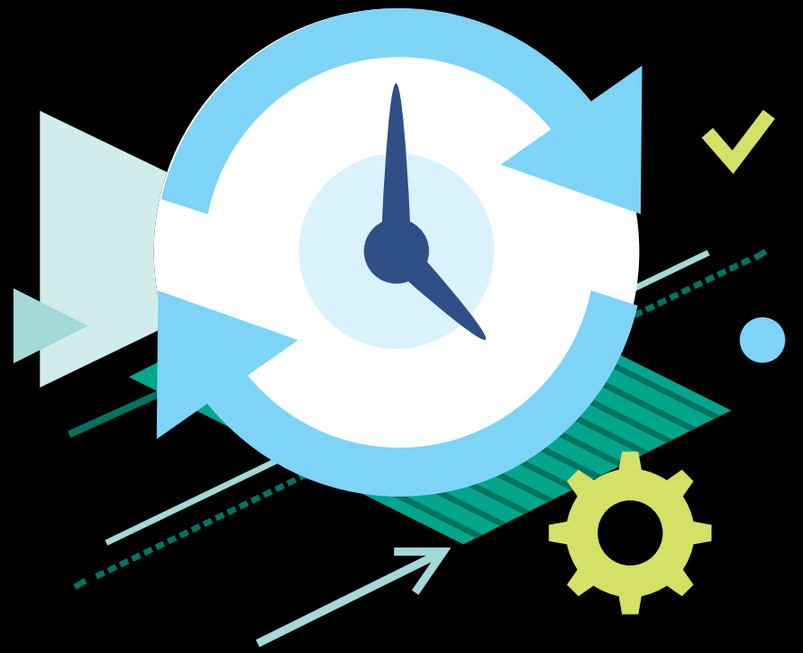
Businesses experiencing a DDoS attack have been targeted more than once in the past 12 months, with most being hit between 2 and 5 times.[9]

DDoS attacks break records in 2016

Kaspersky Lab's Q4 2016 DDoS Intelligence report showed record breaking numbers for the longest attack and number of attacks in one day. Cybercriminals are using more sophisticated methods of attack, and the array of devices being harnessed by botnets is becoming increasingly diverse. The attackers have been showing off their capabilities by choosing bigger and more prominent targets.

In Q4 of 2016, Kaspersky Lab's DDoS Intelligence system reported the longest DDoS attack of the year, which lasted for 292 hours or 12.2 days. The 2016 record was also broken for the number of DDoS attacks in one day – with 1,915 launched on November 5, 2016.[10]

Only 24% of businesses have some kind of specialized solution in place, according to the Corporate IT Security Risks 2016 survey by B2B International and Kaspersky Lab. Many businesses don't think sufficiently about the downtime costs that a DDoS attack could bring.[11]



Top cybercrime-fighting tip: You set aside time on your schedule for system backups and patching.It's just as important to put cybersecurity assessment time on your calendar, too. Pick a quieter time of the month or year to regularly audit where your company's security stands and what needs to be addressed. Involve departments outside of IT to get an overview of employees' needs and online behavior.

9. Corporate IT Security Risks Survey 2016 from Kaspersky Lab and B2B International
10, 11. Kaspersky Lab Q4 2016 DDoS Attack Report Shows Record Breaking Data for the Year

$105K

Average total financial impact of a data breach to a small business if it takes more than a week to detect.[12]

Every size business is a target

In 2016, Kaspersky Lab noticed an interesting shift. The number of new files detected every day rose from 310,000 in 2015 to 323,000 in 2016. What's going on?

There are a few notable changes going on in cybercrime. First, like everyone else, cybercriminals are looking for a better return on their investments through cost cutting and efficiency. Complex malicious programs, such as rootkits, bootkits and replicating viruses, can cost tens of thousands of dollars to develop and don't always get the desired results. In addition, cybercriminals have become more sophisticated and are offering mass produced malware that is tailor-made for cybercrime. Buying or stealing software certificates is now a thriving business in the malware world, and it's an approach that is paying off, producing millions of dollars in profit for cybercriminals.

More and more, the users under attack are small- and medium-sized businesses. If you are a small business who is a preferred vendor of a large organization, you could be a prime target of cybercriminals looking for easy access to the mother lode of information that some large enterprises have. They know that while their real target may have shored up their security, the vendors and service providers that serve them may not have been as vigilant. They count on this lapse as their point of entry.

Efficiency. Cost cutting. More high value targets. It's clear that cybercriminals are looking for more bang for their buck. With this shift in mind, they are ready to use what's already on the market to make sure they succeed.

Top cybercrime-fighting tip: Hacking a small business to get into a larger business is now standard operating procedure for cybercriminals. As a result, more and more large enterprise companies want to know what security their vendors and SaaS providers have in place. Be ready to answer in detail about your security solution and how you protect your valuable clients and customers.

12. Corporate IT Security Risks Survey 2016 from Kaspersky Lab and B2B International

891K

The average total impact of a data breach for enterprises[13]

Location, Location, Location

Unlike high value real estate, location is not everything to cybercriminals.

While it's true that certain countries have looser regulations that make it easier to carry out attacks, it's a mistake to assume that these crimes are only perpetrated by people in certain regions of the world. In May of 2017, the WannaCry ransomware attack quickly became one of the largest cyberattacks in the world, spreading quickly to 300,000 machines in 150 countries. It affected businesses, hospitals and other organizations—anyone using out-of-date Microsoft Windows software.

As an example of malware that knows no borders, ransomware hit businesses and institutions all over the world in 2016. The Hollywood Presbyterian Medical Center in Los Angeles paid $17,000 in bitcoin after treatment at their hospitals was brought to a halt by a ransomware attack. The University of Calgary in Canada was shut down by a ransomware attack and paid $20,000 in bitcoin after the school was hit the very week that it was hosting a major conference. The UK Healthcare Service Trust had 48 of its facilities affected by the WannaCry attack.

If you are a high value target in the U.S., the fact that your servers are located halfway around the world is of little consequence to a cybercriminal intent on getting your data. And with the advent of bitcoin as a preferred currency for their dealings, cybercriminals have an exchange that makes it much easier for them to cover their tracks.

Gone are the days of rifling through the wastebaskets of large corporations to steal information. Cybercriminals operate in a borderless world where always-on connectivity is easily exploited and where, with the right hacking skills, they can break into your business without ever leaving the comfort of their office—the ultimate work-from-home opportunity.

Top cybercrime-fighting tip: Whether or not your business is the direct target of an attack or collateral damage is immaterial. The results can still be devastating with denied access to programs you need to run your business and enormous reputational damage to your brand. Prevention is the best protection with a security solution that reinforces your perimeter and anticipates–and eliminates–even the most dangerous threats to your business.

13. Corporate IT Security Risks Survey 2016 from Kaspersky Lab and B2B International

Total financial impact of a cyberattack for enterprises when the attack involves three or more vectors.[14]

The hacker in a hoodie is a mythological creature

Books and movies have created an archetype of the cybercriminal. He is a young man in a darkened room in front of a bank of computers who is intent on using his smarts to bring an organization to its knees. The uniform is always the same—neutral color t-shirt and hoodie with an ever-present backpack tossed on the floor. The only problem is, it's a complete oversimplification of what is actually a much more complex story.

Viewing a cybercriminal as someone who is acting alone out of some higher cause may work well for movie scripts, but it is woefully short-sighted. These days, most cybercriminals are operating like well-oiled machines. Their level of skill and professionalism is rising, and they are increasingly banding together into organized groups. Many have even developed an elaborate mercenary network who offer their services out for hire. This kind of Access-as-a-Service is sure to only increase as cybercrime becomes more and more profitable.

Let's take a look at the more common types of cybercriminals on today's landscape.

Cybercriminals

- Readily understand the value of corporate information
- Know that there are opportunities to gain from extortion and ransom campaigns
- Will profit from selling stolen data on the black market

Hacktivists

- Focused on causing reputation damage and disruption to an organization that they have issues with
- Weapon-of-choice is leaking confidential information about customers, suppliers or employees that could lead to severe embarrassment or legal penalties

Cybermercenaries

- Seek payment from anyone who will hire them, including governments, protest groups or businesses
- Method is to steal information on behalf of their client

Nation States or Government Agencies

- Focus on collecting strategic information or disrupting industrial facilities in hostile countries
- Could also be government contractors

"Cybercrime has lost the last touch of romance. Today, malware is created, bought and resold for specific tasks. The commercial malware market has settled, and is evolving towards simplification. I think will we no longer see malicious 'code for the code'. This trend is also observed among the operators of targeted attacks,"

—Vyacheslav Zakorzhevsky, Head of Anti-Malware Team at Kaspersky Lab

14. Corporate IT Security Risks Survey 2016 from Kaspersky Lab and B2B International

1 in 5

One in five cases involving significant data loss came about through employee carelessness or lack of awareness.[15]

Don’t forget the insider threat

In the 2016 Cyber Security Intelligence Index, IBM found that 60% of all attacks were carried out by insiders. Of these attacks, three-quarters involved malicious intent, and one-quarter involved inadvertent actors.[16]

So, while it’s important to understand who cybercriminals are and what motivates them, every company needs to be aware that the greatest threats come from malicious insiders. Malicious actions of internal staff equated to 41% among the most prevalent security incidents in 2016.[17]

Even apart from malicious insiders, well-meaning employees threaten data security every day by opening unauthorized email attachments, forwarding sensitive information or storing data insecurely. Cybercriminals know and exploit this weakness. Careless or uninformed employees are the second most likely cause of a serious security breach.[18]

Defending your business from cybercrime with a multi-layered approach is crucial to your business. These layers include a robust security system, as well as educating your employees on how they can act as a first line of defense. **Read more in our eBook *The Threats from Within***.

Top cybercrime-fighting tip: The importance of employee education and awareness cannot be overstated. Many employees believe that cybersecurity has nothing to do with them when, in reality, they are your first line of defense. Set up regular employee education programs and communications to let them know the dangers of phishing, the reality of ransomware and the role they play in keeping your business safe.

15. Kaspersky Lab’s “Story of the Year: The Ransomware Revolution”
16. Harvard Business Review, “The Biggest Cyberthreats are Inside Your Company”
17. Kaspersky Lab’s “Business Perception of IT Security: In the Face of an Inevitable Compromise”
18. Corporate IT Security Risks Survey 2016 from Kaspersky Lab and B2B International

How to gain the upper hand

For any business, there are many concrete steps you can take to shore up your defenses from cybercriminals:

- Focus on cybersecurity education for staff
- Ignore the detractors and implement mature, multi-layered endpoint protection
- Patch vulnerabilities early and often and automate the process
- Mind everything that's mobile
- Implement encryption for communications and sensitive data
- Protect all elements of the infrastructure—gateways, email, collaboration
- Adopt a "Security First" mindset when it comes to "new" applications, such as IoT, Cloud or Virtual Systems. Before you implement any system, ask where your security stands
- Create and deploy a complete security strategy, which Kaspersky Lab defines in four parts: Prediction, Prevention, Detection and Response.

When dealing with the threats to your company, it may feel like you are engaging with an invisible enemy. This is far from the truth. At Kaspersky Lab, we are continually studying their behaviors, patterns and motivations in order to give our clients the latest information on how to combat cybercriminals, and we are known for sharing the information we have so that everyone is protected from these malicious actors.

We are proud to work with global IT security vendors, international organizations and regional law enforcement agencies all over the world. Our partners in the field of law enforcement include INTERPOL, Europol, The National High Tech Crime Unit (NHTCU) of the Netherlands' Police Agency and The City of London Police, as well as Computer Emergency Response Teams (CERTs) worldwide. We hold regular training courses for Interpol and Europol officers, as well as the police forces of many different countries.

Together with our partners, we have exposed criminal networks, pulled the curtain back on the most sophisticated advanced threats and helped our clients to protect their most precious assets—their data, their clients and their reputations.

True Cybersecurity for Business

Kaspersky Lab's True Cybersecurity approach combines multi-layered security with cloud-assisted threat intelligence and machine learning to protect against the threats your business faces. True Cybersecurity not only prevents attacks, but also predicts, detects and responds to them quickly, while also ensuring business continuity for your organization.

Watch us on YouTube

Like us on Facebook

Review our blog

Follow us on Twitter

Join us on LinkedIn

Get your free trial now >

Learn more at
kaspersky.com/business

About Kaspersky Lab

Kaspersky Lab is one of the world's fastest-growing cybersecurity companies and the largest that is privately-owned. The company is ranked among the world's top four vendors of security solutions for endpoint users (IDC, 2014). Since 1997 Kaspersky Lab has been an innovator in cybersecurity and provides effective digital security solutions and threat intelligence for large enterprises, SMBs and consumers. Kaspersky Lab is an international company, operating in almost 200 countries and territories across the globe, providing protection for over 400 million users worldwide.

To learn more about Kaspersky Endpoint Security for Business,
call Kaspersky Lab today at 866-563-3099 or
email us at corporatesales@kaspersky.com.

www.kaspersky.com/business

KASPERSKY lab