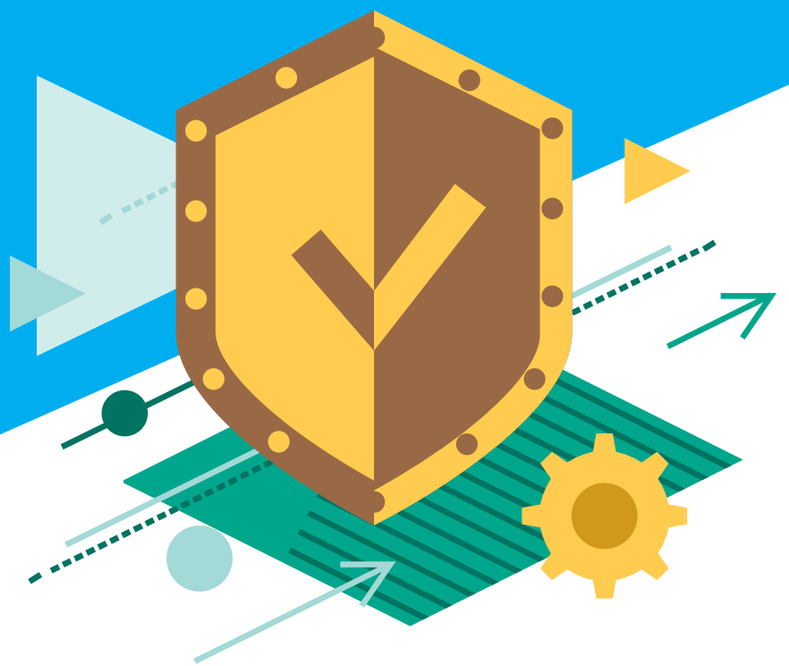
CYBERCRIMINALS: UNMASKING THE VILLAIN

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.



2x

The number of attacks by cybercriminals against businesses doubled in 2015, according to Kaspersky Lab's research.

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. Research by British insurance company Lloyds found that the **damages from cyberattacks are costing businesses a staggering $400 billion per year.**[1]

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.

CYBERCRIMINAL TRICKS AND TACTICS

So, how do they break through these organizations? In 2015, Kaspersky Lab's own data showed some interesting trends.

1. The Big Business Of Cybersecurity Paying Off?
2. Kaspersky Lab Security Bulletin for 2015 shows mobile banking threats among the leading malicious financial programs for the first time

For one thing, cybercriminals are looking to avoid criminal prosecution. This is why they have **switched from malware attacks to the aggressive distribution of adware**. In 2015, adware accounted for 12 of the top 20 web-based threats.[2]

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. The total number of users attacked in 2015 by encryption **ransomware increased by a whopping 48.3 percent compared to 2014**. In many cases, the encryptors include functionality designed to steal data from victim computers.

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.

"High-profile targeted attacks on enterprises are becoming increasingly widespread. Thousands of businesses have already been hacked and had their sensitive data stolen–resulting in multi-billion dollar losses."

—**Eugene Kaspersky**, *CEO, Kaspersky Lab*

7.5x more

Damage to a company's brand is estimated to cost 7.5 times more than the direct costs of recovering from an attack.

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 own research shows that the rate of profit to effort from cybercrime is roughly 20:1.[3] That's a good margin 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. CryptoLocker, one type of ransomware that has infected tens of thousands of machines, **rakes in $30 million every 100 days**, according to a Dell SecureWorks report. According to a survey conducted by Interdisciplinary Research Centre in Cyber Security at the University of Kent, more than **40% of CryptoLocker victims agreed to pay**.[4] 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.[5]

The most profitable threats are banking Trojans that target money directly. They cost about $3,000 per malware, which exploits via spam emails. But in the end, criminals can earn up to $72,000. The average loss for an individual victim—whether it is a person or a business organization—is $722.[6]

Cybercrime is highly profitable. It has a relatively low cost of entry. And victims are easy to find. No wonder that **58% of corporate PCs were hit with at least one attempted malware infection** in 2015.[7]

"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.*

3, 5, 6. Cybercrime, Inc.: how profitable is the business?
4. The ransomware epidemic: why you should be more concerned
7. Kaspersky Lab on business threats: 2015 saw the number of cryptolocker attacks double

$417k

The average cost of recovery from a DDoS attack for a large company.[8]

THEY TAKE DAYS OFF

In our study of key advanced threats, we noticed some interesting patterns. Some days were more active than others, and there were some times of year where there was a dip in activity. How could this be?

In the case of DDoS attacks where cybercriminals use multiple computers and internet connections to flood the targeted resource, cybercriminal activity peaks from Monday to Thursday when an average of 80% of all DDoS attacks take place. In fact, almost a quarter of DDoS attacks fall on Tuesdays.

This is significant because **when businesses are hit by noticeable DDoS attacks, three-quarters of the time, those attacks are accompanied by another security incident**. This means that many businesses who are hit by a DDoS attack find themselves under assault from multiple sources during peak business hours. And since 50% of DDoS attacks lead to a noticeable disruption of services,[9] this is not just something that hits the IT department. Every customer-facing department, such as sales and customer service, must handle the unpleasant task of explaining the situation to clients and customers.

Interestingly enough, when we studied attacks for Q3 2015, our findings revealed a dip in DDoS attacks in August. Hard as it is to believe, we can only conclude that even cybercriminals take vacations. While this doesn't mean that we recommend putting your guard down during the peak of summer vacation time, it does mean that there may be a quieter window of activity to assess your systems and identify areas for improvement while the threat of a more serious attack is slightly lower.

By analyzing these patterns and understanding their tactics, Kaspersky Lab can conclude that cybercriminals are acting more like businesses—coordinating their efforts, focusing their attacks and even taking some downtime to enjoy the spoils of their activities.

8, 9. Kaspersky Lab's "Denial of Service: How Businesses Evaluate the Threat of DDoS Attacks"

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.

90%

Percentage of organizations who have experienced some form of external threat.[10]

THEY'RE LOOKING FOR BETTER ROI

In 2015, Kaspersky Lab noticed an interesting shift. After years of increasing numbers, the number of new malware files detected every day fell from 325,000 in 2014 to 310,000 in 2015.[11] What's going on?

Like everybody else, cybercriminals are looking for a better return on their investments, and they're getting there by cutting costs and increasing efficiency. Complex malicious programs, such as rootkits, bootkits or replicating viruses, can cost tens of thousands of dollars to develop and don't always get the desired results. Cybercriminals know that they can get equally good results by using intrusive advertising programs or legitimate digital signatures in their cyberattacks. Buying or stealing certificates is now a thriving business in the malware world, and it's an approach that is paying off. Results show that despite the cost-cutting in malware creation, **the number of users attacked by cybercriminals in 2015 increased by 5%.**[12]

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. In fact, the U.S. Department of Homeland Security reported that **31% of all cyberattacks are directed at businesses with less than 250 employees.**[13]

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.

10. Kaspersky Lab Global IT Security Risks Survey 2015
11, 12. Kaspersky Lab's New Malware Count Falls by 15,000 a Day in 2015, as Cybercriminals Look to Save Money
13. Hackers Want "Two for One" Security Opportunities. Hack a Small Biz to Get a Big Biz

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.

60%

Businesses that suffered a data breach that found their ability to function afterwards severely reduced.[14]

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 fact, **Kaspersky Lab detected ransomware in 200 countries and territories in 2015 alone.**

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.

At the same time, certain attacks are more likely to be an issue in certain countries. In Kaspersky Lab's Q3 report on DDoS attacks, China, the U.S. and South Korea occupied the top positions as both the frequent sources and targets of these kinds of attacks.

For mobile banking threats, 80% of attack notifications blocked by antivirus components were received from online resources located in ten countries.[15] This shows that cybercriminals prefer to operate and use hosting services in different countries where the hosting market is well-developed.

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.

14. Kaspersky Lab Global IT Security Risks Survey 2015
15. Kaspersky Lab Security Bulletin for 2015 shows mobile banking threats among the leading malicious financial programs for the first time

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.

$551k

Average cost of a serious data breach for enterprises.[16]

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.

16. Kaspersky Lab Global IT Security Risks Survey 2015

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

42%

Percentage of confidential data loss caused by employees.[19]

DON'T FORGET THE INSIDER THREAT

Let's not overlook the fact that **73% of companies had an internal security incident in 2015**.[17] 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. Small-and medium-sized businesses lose up to $40,000 on average from fraudulent activity by employees, while the figure for enterprises exceeds $1.3 million.[18]

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. Kaspersky Lab's recent research shows that **42% of confidential data loss is by employees**—the largest single data loss cause.[20]

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.

17. Kaspersky Lab Global IT Security Risks Survey 2015
18, 19, 20. The Threat Within: 3 Out of 4 Companies Affected by Internal Information Security Incidents

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.

TRY KASPERSKY LAB

Discover how Kaspersky Lab's premium security can protect your business from malware and cybercrime with a no-obligation trial. Register today to download full product versions and evaluate how successfully they protect your IT infrastructure, endpoints and confidential business data.

GET YOUR FREE TRIAL TODAY >

JOIN THE CONVERSATION

Watch us on YouTube

Like us on Facebook

Review our blog

Follow us on Twitter

Join us on LinkedIn

Learn more at usa.kaspersky.com/business-security

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. Learn more at usa.kaspersky.com.

Contact Kaspersky Lab today to learn more about Kaspersky Endpoint Security for Business and our other IT security solutions and services:
usa.kaspersky.com/business-security
(866) 563-3099
corporatesales@kaspersky.com

KASPERSKY lab
THE POWER OF PROTECTION