KASPERSKY lab

A Guide to the Modern Threat Landscape

www.kaspersky.com/business
#truecybersecurity

Kaspersky®
Endpoint Security
for Business

A Guide to the Modern Threat Landscape

As organizations around the world continue to digitally transform, their reliance on IT systems increases. At the same time, global threat actors work to repurpose, refine, develop and build new and innovative tools and approaches to evade detection and unleash cyberattacks. The growing complexity of advanced threats is moving IT security into an incident-centric era – an era that represents mounting challenges for companies and security vendors alike.

For enterprises globally, the average cost of a data breach is over $1.2 million, a 24% increase from 2017 and a 38% increase from 2016. Any company can become a victim and there's no such thing as 100% security, but there is plenty that organizations can do to stay safe. Assuming that standard protection is already in place in your business, in this document we'll look at some of the most prevalent advanced threats, the damage they can cause, and the dedicated, advanced technologies that can protect against them.

For enterprises globally, the average cost of a data breach is over $1.2 million, a 24% increase from 2017 and a 38% increase from 2016.

Fileless threats: Success by stealth

Unlike threats which are downloaded and executed, fileless threat execute in system memory. Because they're contained in memory code rather than on a computer's hard drive and can also hide in the Windows Registry and Windows Management Instrumentation, they can be difficult to detect and often evade traditional anti-virus protection and intrusion prevention. A user unwittingly visits a malicious website, clicks on a maladvertisement (an advert containing malware) and the execution begins....

Fileless attacks are 10 times more likely to succeed than file-based attacks – 77% of successful compromises during 2017 involved fileless techniques. If that's not bad enough, in 2017, 42% of organizations experienced one or more fileless attacks that successfully compromised their data and/or IT infrastructure.* One of the best-known examples of a fileless attack occurred at American consumer credit agency Equifax in 2017 when attackers used an unpatched vulnerability to execute malicious commands that resulted in the theft of 146.6 million personal records...

How we help

Kaspersky Lab's **behavior detection** technology surveys activities within a given system to detect suspicious app behavior. It doesn't matter whether there's a file behind the process being examined or not – all malicious activity is blocked. Behavior detection principles are based on continuously running machine learning processes together with extensive threat intelligence from Kaspersky Security Network's data science-powered processing and analysis of global, real-time statistics. Our **exploit prevention** technology blocks attempts by malware to exploit software vulnerabilities, and **adaptive anomaly control** can block process actions which don't fit a learnt pattern (e.g. prevent PowerShell from starting).

* The 2017 State of Endpoint Security Risk Report, Ponemon Institute

CMD/PowerShell threats: Powerful and opportunistic

Shell script files used to be considered relatively harmless – even though they're not – but PowerShell scripts are extremely powerful; they're a complete scripting environment and offer a vast range of opportunities for attackers. Downloading additional modules online, running bodiless malware, remotely executing arbitrary code on other machines in a network – all in the name of an inherently beneficial app, the PowerShell interpreter, standard Windows equipment since Windows 7.

PowerShell attacks are rising at a spectacular rate with a noticeable proportion of malware using CMD/PowerShell in some way. In April 2018, Kaspersky Lab reported on Operation Parliament, a cyber-espionage campaign aimed at high-profile legislative, executive and judicial organizations around the world but mainly focused on the Middle East and North Africa. The attacks targeted the full range of political entities, from parliaments and top state offices to military and intelligence agencies and election commissions. The malware provides a remote CMD/PowerShell terminal for the attackers, enabling them to execute any scripts or commands and receive the result via HTTP requests.

How we help

Kaspersky Lab is fully equipped to deal with the developing PowerShell malware wave. The strings passed to our engines are analyzed carefully by behavior detection technology and execution is blocked if anything malicious is found. For example, when PowerShell starts from an unusual location (Word, for instance, or the Temp folder), if the PowerShell Command Line contains strange parameters or if the script itself is obfuscated. Our adaptive anomaly control works according to learnt patterns and also detects unusual PowerShell usage.

Ransomware: Declining in volume; growing in sophistication

This class of malware is based on cryptors – Trojans which infiltrate via a vulnerability, an email attachment or a phishing link to a specially crafted website. The attack module then quietly encrypts any data it finds that could be of value to the victim. This might include financial details, legal documents, customer databases, diagrams, and so on. The crypto-lockers then demand payment to decrypt these files. It's usually impossible to decipher files that have encrypted by current crypto-malware.

Ransomware really ramped up in 2017, which saw the biggest ransomware attack in history, WannaCry, spread at breakneck speed, claiming around 700,000 victims worldwide. Consumer goods giant Reckitt Benckiser lost access to 15,000 laptops, 2,000 servers and 500 computer systems in the space of just 45 minutes when it was hit by the NotPetya ransomware attack, with losses expected to top $130 million.

Shipping giant Maersk announced a revenue loss of around $300 million due to a NotPetya ransomware attack. While ransomware has declined in volume in 2018, it's increased in sophistication and continues to inflict massive financial havoc on enterprise-level businesses. Ransomware is in the top 5 most expensive security incidents for enterprises.

Different strains of ransomware use different attack technologies and infection methods, which is why a multi-layered solution equipped with specialized anti-ransomware technologies that protect your entire system is so important.

How we help

Kaspersky Endpoint Security for Business includes a **behavior detection** and **remediation engine** that blocks malware and reverts any files it's already encrypted to their former state. For scenarios when encryption processes are initiated through a different host on the network, our complementary anti-cryptor engine blocks the activity and refuses network connection to the malicious host. Even for companies using other vendors' solutions, the standalone (and free) **Kaspersky Anti-Ransomware Tool** can deliver basic protection against ransomware.

Miners: Greed on the rise

Cryptocurrency has become a hot topic in recent years, attracting more and more admirers around the world. The opportunity to make money from cryptocurrency has attracted cybercriminals too, and even in the age of ransomware, the majority of ransoms are demanded in cryptocurrency (such as anonymous and unregulated Bitcoins). It was only a matter of time before miners arrived on the threat scene.

Miners, or currency miners, are a class of malware that's growing fast. The ongoing development of the cryptocurrency market has led to a huge increase in cases of miners being installed without users' knowledge – when a new cryptocurrency is emerging, it's much easier to mine and make money from it than when it's more established.

Cryptocurrency mining is completely legal – the problem arises when criminals con unsuspecting users into installing mining software on their systems or exploiting software vulnerabilities to do so. This results in threat actors receiving cryptocurrency, while their victims' computer systems experience a dramatic slowdown. Or as MIT's Technology Review puts it: 'Cybercriminals use old tricks and new cryptocurrencies to turn stolen computing power into digital coins'...

Between 2017 and 2018, the total number of users who encountered miners rose by almost 44.5% and the share of miners detected, from overall risk tool detections, increased from over 5% in 2016-2017 to almost 8% in 2017-2018. The number of users who encountered mobile miners is also steadily rising, albeit less dramatically – growing by 9.5% between 2016 and 2018. Kaspersky Lab has observed an uptick in attempts at installing miners on company servers – attempts that, when successful, cause data processing speeds to drop and business processes to be interrupted.

How we help

Kaspersky Lab's **behavior detection** identifies stealth threats which traditional anti-virus and protection technologies fail to detect. It identifies all apps – legitimate or malicious – attempting to communicate with a mining address. For example, an attempt at starting command line parameters (including crypto wallet numbers, pool addresses, etc.), an attempt starting in an unusual location (the Temp folder, for example) and attempts at connecting to mining pool addresses. Our **adaptive anomaly control** works according to learnt patterns and also detects hidden attempts to start processes and applications.

There have been numerous reports of rogue employees using their organization's resources - computers, servers and even data center – to mine for cryptocurrency after hours. **Web control** can identify and block communication with mining pool addresses, avoiding the load that miners put on the system.

Mobile threats: The endlessly moveable feast

The extensive use of mobile platforms continues to be a boon for threat actors. Across 2018 so far, mobile threat levels have remained relatively steady. In the third quarter, Kaspersky Lab detected over 1.3-million malicious installation packages for mobile devices. Statistics overall show that the number of financial threats against mobile devices increases every quarter. The financial impact of a malware infection on a company owned device is estimated at $713k and on a BYOD at $664k...

Perhaps the most important development is the wholesale evolution of epidemic banking Trojan Asacub. First encountered in 2015, Asacub has evolved into the top performer in terms of numbers of mobile banking Trojans – its scale and power has surpassed the most powerful mobile campaigns in the history of these events.

How we help

Kaspersky Security for Mobile is a Mobile Threat Defense and Mobile Threat Management solution that helps businesses ensure that their mobile workers can use mobile devices for work tasks without exposing the business to risk. Powerful **anti-malware** combined with cloud-assisted threat intelligence and machine learning protect against known, unknown and advanced threats to data stored on mobile devices and from online activities. **Web control** and **anti-phishing** capabilities ensure reliable, safe web filtering to block access to malicious and other undesirable websites.

ATM/PoS threats: No signs of withdrawal

A combination of factors such as the use of obsolete and unsupported operating systems and the availability of easy to use development platforms has made it possible for almost anyone to create malicious code.

ATMs and PoS (Point of Sale) systems remain a targeted asset for cybercriminals. ATMs have been under attack since at least 2008, when the first malicious program targeting ATM Backdoor.Win32.Skimer was discovered. The first incident of ATM malware-as-a-service took place in 2017, when cybercriminals packaged all the necessary malicious programs together with video instructions and released them onto the market for anyone wanting to gain access to ATMs. In the same year, Kaspersky Lab researchers uncovered attacks on ATM systems that involved new malware, remote and fileless operations.

In the first seven months of 2018 alone, malware directed at ATMs/PoS systems infected 57% more targets than in all of 2017. Experts predict that attacks via software designed specifically for financial organizations, including software for ATMs and PoS terminals, will continue to rise. PoS breaches are in the top 3 most popular breach patterns...

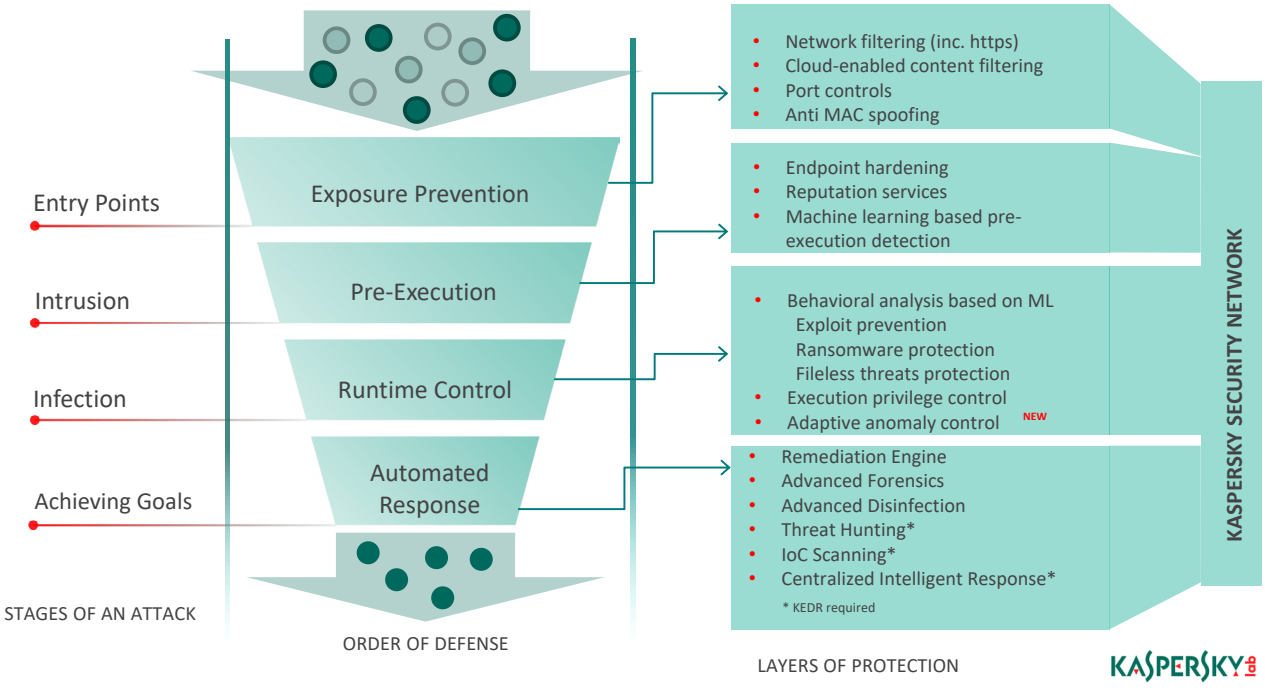
How we help

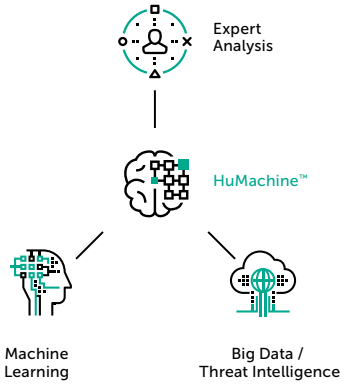
Kaspersky Embedded Systems Security has been specifically designed for organizations operating ATM and PoS systems and the challenging threat environment they operate in. Incorporating powerful **anti-malware** and **application** and **device controls** as well as **memory protection** and **firewall management**, it protects the attack surfaces unique to these architectures, reflecting their unique functionality and OS, channel and hardware requirements, while fully supporting the Windows XP family. All these components, together with **file integrity monitoring** and **log inspection**, ensure that Kaspersky Embedded Systems Security is fully compliant with the relevant PCI DSS requirements.

Advanced threats need full-stack protection

As the modern threat landscape continues to develop and evolve, traditional protection technologies are not enough – even though those technologies should still be in place. To boost their protection in order to deal with the advanced threats we've mentioned in this document, companies need to take their IT security to another level – this means next-generation solutions that combine multiple technology layers with machine learning, threat intelligence and expert analysis to deliver meaningful and effective protection now and in the future.

Kaspersky Lab: Full stack of protection technologies addressing known, unknown and advanced threats





Kaspersky Lab
Find a partner near you: **www.kaspersky.com/buyoffline**
Kaspersky for Business: **www.kaspersky.com/business**
True Cybersecurity: **www.kaspersky.com/true-cybersecurity**
IT Security News: **www.business.kaspersky.com**

#truecybersecurity
#HuMachine

www.kaspersky.com