KASPERSKY lab

Kaspersky Embedded Systems Security – Safeguarding ATMs

www.kaspersky.com
#truecybersecurity

Kaspersky Embedded Systems Security – Safeguarding Atms

Big problems for the «Little box of money»

ATMs have always attracted the attention of criminals. To get at the contents of these machines, attackers have resorted (and sometimes still resort) to drastic measures: using power drills, circular saws, blowtorches, explosives and even trying to tow them away with a vehicle.

Later, they began using a variety of skimmers – special devices designed to steal the bank card details that an ATM requires. However, with the introduction of the international standard 'EMV' (Europay, MasterCard, VISA), which defines a number of requirements for interaction between a credit card and a payment device, the security of financial transactions made via ATMs has grown significantly. The volume of ATM skimming has dropped noticeably as a result.

However, the criminals have not given up: instead of the odd attempt to tackle ATMs with power tools or metal rope, they have begun using specially crafted malware. They no longer require explosives or a "white plastic" card (a specially prepared card with data from a stolen payment card). All they need do is infect an ATM with a Trojan, allowing them to withdraw all the banknotes from the ATM whenever they want. As well as stealing money, criminals can also disrupt the operation of the machine, and launch a DoS (Denial of Service) attack, which will cause financial losses for the bank that owns the ATM.

Over the years, financial institutions have witnessed a number of malicious software samples that target ATMs. For example, the first malware aimed at ATMs – Backdoor.Win32.Skimmer – was detected by Kaspersky Lab in 2009 and can still be found on some machines. This Trojan steals the user's bank card data and can also dispense cash without the account holder's knowledge.

Another interesting example is Trojan-Spy.Win32.SPSniffer, or Chupa Cabra. This Trojan was first detected in 2010 by Kaspersky Lab experts in Brazil, and works on all types of ATMs, intercepting data from the cash machine in order to read the card information.

We have accumulated enough examples of these types of Trojan to analyze the most popular samples and determine what measures and technologies are required for ATM protection.

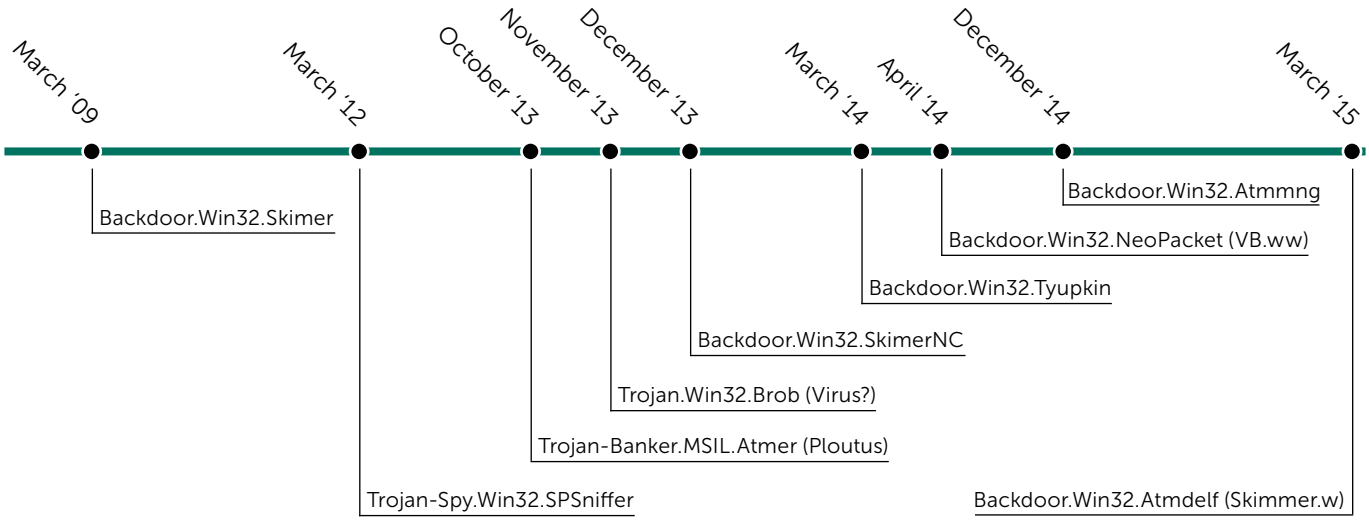


Figure 1: Timeline of ATM malware detection

Backdoor.MSIL.Tyupkin

In March 2014, the world learned about malicious software installed on ATMs that allowed criminals to withdraw huge sums of money. All the attacker had to do was approach an infected ATM, enter a code on the keyboard, and the machine dispensed all the money it contained.

Before we analyze the malicious code's functionality and how it ended up on the ATM, it's important to understand that each ATM is a computer designed to perform specific tasks. This means it's subject to the same sort of threats as traditional workstations and servers, and operating systems running on ATM computers can contain the same vulnerabilities as their desktop and server counterparts.

According to Kaspersky Lab experts, the Tyupkin malware (Backdoor.Win32. Tyupkin) was installed on ATMs with the help of a bootable CD used by a criminal with direct access to the ATM computer.

Having penetrated the ATM's operating system, the malware maintained its presence on the infected machine, ensuring the criminals had access to its contents.

Once on the device, the Trojan immediately disabled the installed protection solution belonging to a specific vendor by removing its software components, launched an infinite loop waiting for user input and, in order to prevent detection, only accepted commands on Sunday and Monday nights. Armed with the commands and the special code that the Trojan accepted to exclude any interaction with a random user, the criminals could gain access to the contents of the ATM cassettes and withdraw the cash.

However, Tyupkin is not the only threat to ATMs that Kaspersky Lab experts have encountered.

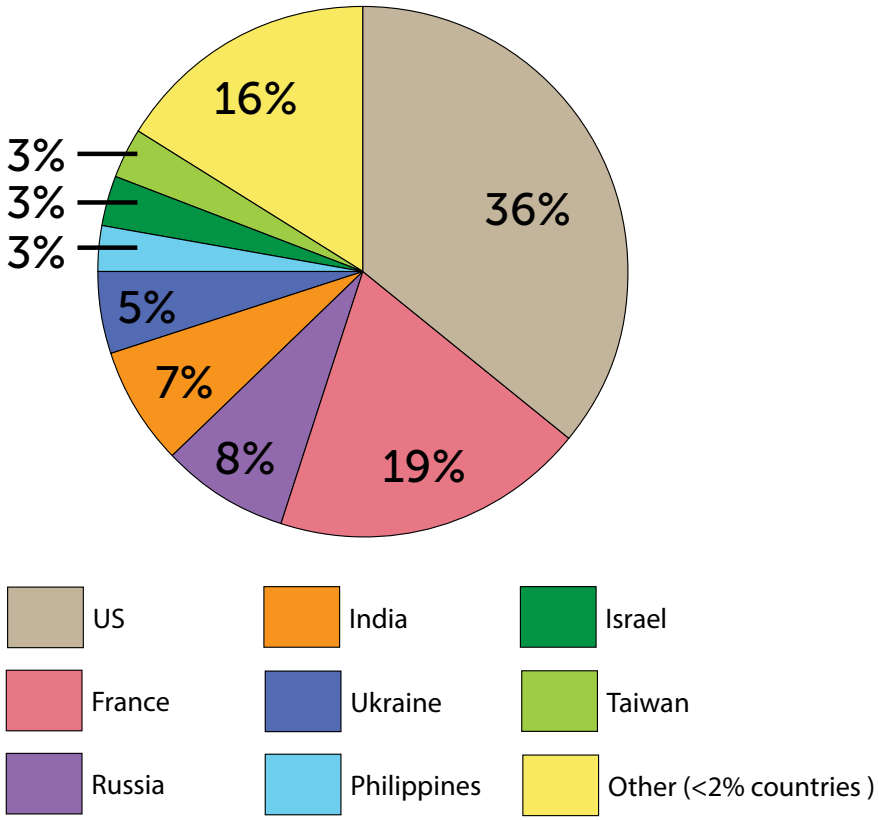


Figure 2: The number of Tyupkin samples by country (according to VirusTotal statistics)

Map of Carbanak targets

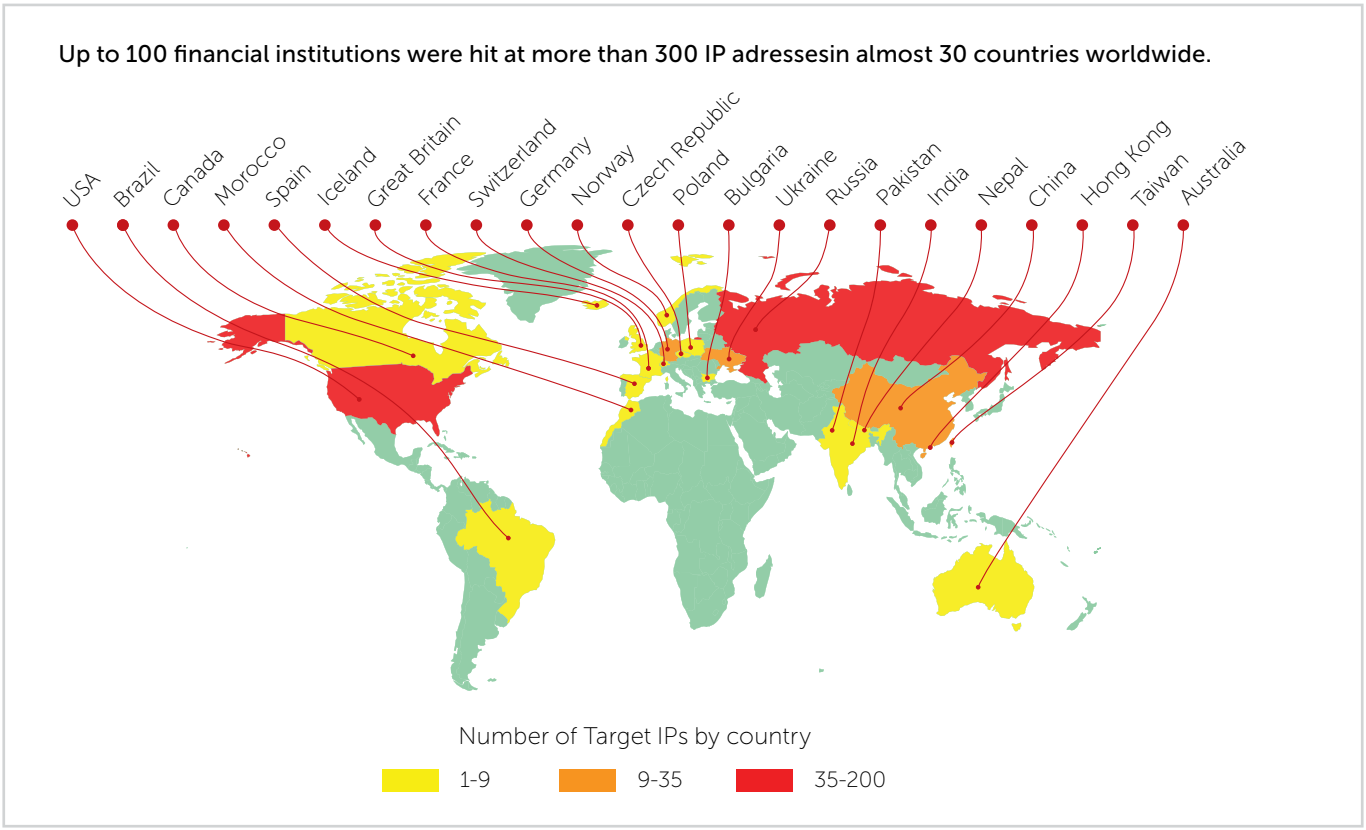


Figure 3: Carbanak infection by country

Carbanak

In the spring of 2014 Kaspersky Lab was involved in a forensic investigation, after the ATMs of one bank dispensed cash without any physical interaction between the recipient and the ATM. This is how investigation of the Carbanak campaign, and research into the eponymous malware, all started.

Carbanak is the Carberp code-based backdoor. It's designed for espionage, data collection and providing remote access to the infected computer. Once the attackers gained access to a machine within the bank network, they explored the network for opportunities to spread the infection to critical systems – processing, accounting, and ATMs. They did this manually, trying to hack the desired computers (for example, the administrators' machines) and using tools that could spread the infection to other computers on the network. In other words, having gained access to the network, they moved from one computer to another until they found an object of interest. The choice of objects varied from attack to attack, but the result was always the same: the attackers stole money from a financial organization, and ATMs were one of the main channels for withdrawals.

If the criminals managed to penetrate computers that had access to the internal ATM network, or if the bank itself had remote access to its ATM devices, the fraudsters used this to withdraw money. They didn't even require special tools to infect ATM software – the attackers used a standard set of tools designed for legitimately controlling and testing ATM equipment.

The solutions installed onto ATMs and designed for monitoring are, in most cases, agent programs that receive commands from special workstations on the bank's internal network and to which they then send data. For example, these agents can do the following:

- Monitor events inside the ATM.
- Distribute software across all the bank's ATMs.

- Download files from ATMs to a dedicated server within the bank.
- Provide remote access to ATMs.

These agents are used for the remote administration and configuration of ATMs by bank employees, and are therefore most commonly found in the 'whitelist' of software operating on an ATM device. That's why, as the Carbanak attacks have shown, they're of particular interest to attackers who've gained access to a bank's internal network.

The Security of Embedded Systems

An embedded system is a specialized computer located directly on the device it's managing. In the case of cash machines, it's a control computer embedded in the ATM. These computers run specific versions of an operating system, such as the Embedded Windows system. Despite the fact that only a strictly limited set of the software included in this operating system is required for the functioning of the ATM, it may contain vulnerabilities and so needs additional means of protection, just like its desktop and server versions.

The Tyupkin incidents described earlier show that the attackers faced little difficulty in copying from a bootable CD-ROM to an ATM and running the malware's files. Already at this stage we can see that recommendations for the physical protection of ATMs have not been followed, giving cybercriminals the chance to use the bootable CD. However, the problem is not just the physical vulnerability of the device, but also the fact that the attackers were able to execute arbitrary malicious code. Having launched this malicious code, the fraudsters gained access to the ATM cassettes full of money.

Tyupkin attack scheme

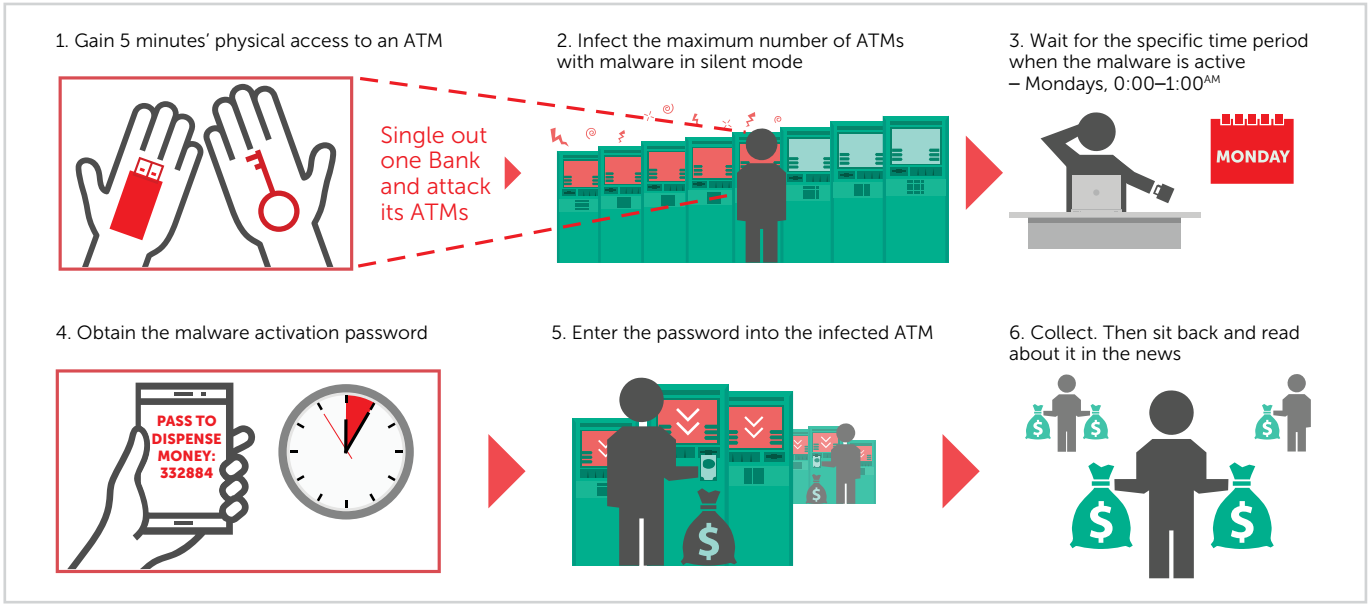


Figure 4: ATM malware 'Tyupkin' forces ATMs into maintenance mode and makes them spew cash

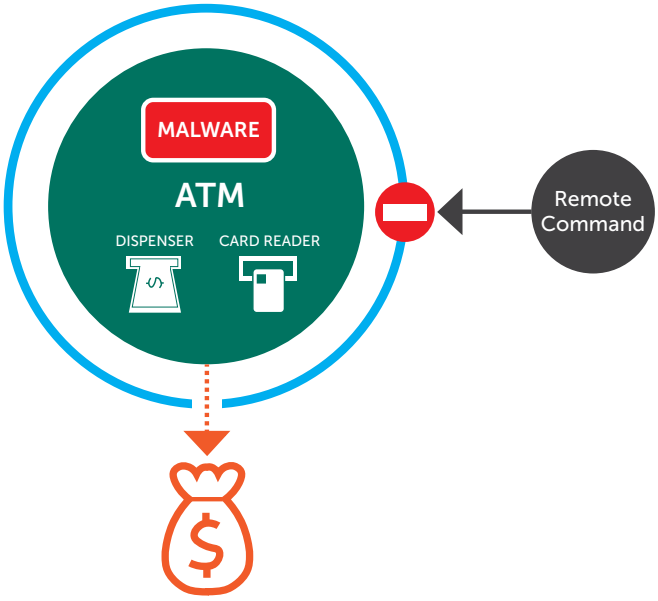


Figure 5: Even if the ATM doesn't include remote access tools, criminals can use malicious software to illegally withdraw money or steal payment data

The Default Deny approach

The world of traditional workstations and servers has long used the Default Deny approach, and the corresponding 'whitelist' technology, that only allows the use of business-related software on office computers. However, traditional software solutions that use these technologies and run on workstations and servers are not designed for embedded systems, which in most cases operate on hardware with very limited computing resources. This imposes some restrictions on the use of existing security solutions, which require computing resources not available on embedded computers in ATMs.

Kaspersky Lab experts have developed the specialized Kaspersky Embedded Systems Security solution to protect embedded systems. It takes into account the specifics of such devices and contains Default Deny technology to combat cyberthreats targeting embedded operating systems. This means all applications on the ATM operating system are run according to the following scenario:

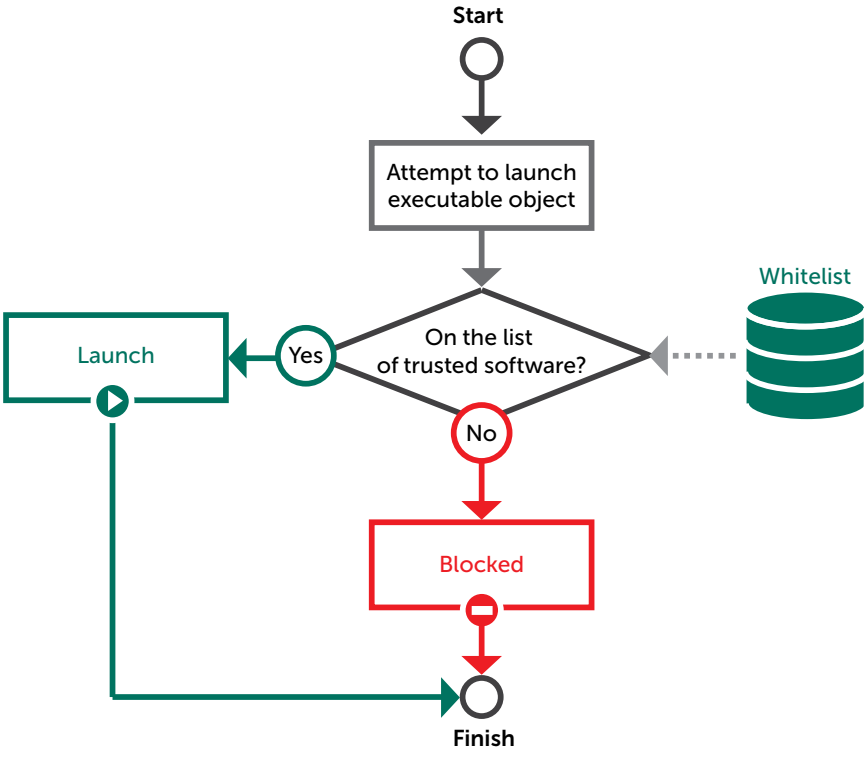
- The operating system initiates the launch of an application, script or library.
- The product safety system checks whether the application, library or script is trusted, by using a whitelist of trusted applications and their components.
- If the object is recognized as trusted, it's allowed to run. Otherwise, it's blocked.

Default Deny technology creates a software environment in the ATM operating system in which only applications required to perform ATM tasks are allowed. So attempts by cybercriminals to run arbitrary code within an ATM operating system protected by Default Deny will be unsuccessful.

Eliminating unauthorized downloads

However, in the case of Tyupkin, the cybercriminals used a non-trivial approach to running malicious code by downloading from a specialized bootable CD-ROM. They then got access to the directories of the ATM operating system and manipulated the files. This made it possible to download malicious code that then received all the necessary privileges to function inside the operating system.

In order to protect ATMs from this kind of threat, it's necessary to eliminate the possibility of unauthorized downloads from external media that may contain malicious code or allow cybercriminals to disable an installed protection solution. This procedure can be implemented by setting the correct load order in the BIOS (loading the ATM operating system from the hard drive should come first) and protecting the BIOS settings with a password. Another approach to ATM protection is Full Disk Encryption (FDE) of the disk from which the ATM operating system is loaded. When FDE technology, which is implemented in Kaspersky Endpoint Security for Windows, is deployed on an ATM, it can block attempts by cybercriminals with access to the ATM input device to modify operating system files, manipulate the ATM file system, or launch malicious code when the operating system is run. However, it's worth noting that the use of this mechanism poses certain risks in terms of integrity and device availability, and for this reason the use of FDE on such devices may be inappropriate in some cases.



However, as the Carbanak attacks have shown, even non-malicious specialized monitoring and remote access tools, which are whitelisted by default, installed on an ATM, could pose a threat if cybercriminals penetrate computers that have access the internal ATM network.

Monitoring for safety

To protect against threats where cybercriminals use the standard tools installed on ATMs, IT security administrators need to take proactive measures:

- Eliminate the possibility of remote access to the ATM.
- Prevent any critical manipulations of its equipment (if it's not possible to block remote access to the ATM device, it is necessary to at least exclude workstations controlling ATMs from the corporate network).
- Use a single tool to monitor and ensure ATM safety.

In our case, this monitoring tool is Kaspersky Security Center, part of Kaspersky Embedded Systems Security. It gathers information on the status of each ATM device and also supports reporting from third-party monitoring tools installed on ATMs. So ATM administrators can analyze the status of each device in Kaspersky Security Center, while at the same time keeping additional "front doors" (Remote Access Tools) shut against attackers.

Safeguarding ATMs; the bottom line

The ATM operating system is a specific counterpart to the traditional workstation OS, with all the accompanying risk. This means that even if the ATM isn't subjected to a targeted attack involving a specially developed Trojan, there's always the risk of being infected with standard desktop malware, which can also disrupt the operation of the machine and result in serious financial losses. For this reason, Kaspersky Lab's security solution for embedded systems integrates anti-virus technologies designed to protect not only against ATM-specific threats but also against all forms of malicious software that may occur in the operating system and which could disrupt services.

Financial institutions need to pay more attention to the protection of their cash machines and consider the security of both hardware components and ATM operating systems, as well as the wider network infrastructure. They can do this by using protection tools that have long been used in corporate networks, as well as specialized security solutions for embedded systems. However, if an incident does occur, it's important to react quickly and actively cooperate with law enforcement agencies and companies specializing in IT security.

A world of expertise in Kaspersky Lab Technologies

The effectiveness of Kaspersky Lab products is proven on a regular basis by the results of independent testing. In 2015, the company headed the Top 3 rating of security solution manufacturers. According to the results of 84 different tests performed by respected test organizations in several countries, Kaspersky Lab solutions finished in the Top 3 in 82% of tests and topped the rating on 60 occasions. This is undeniable proof that Kaspersky Lab provides the industry's best protection.

About Kaspersky Lab

Kaspersky Lab is a global cybersecurity company founded in 1997. Kaspersky Lab's deep threat intelligence and security expertise is constantly transforming into security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky Lab technologies and we help 270,000 corporate clients protect what matters most to them.

Learn more at http://www.kaspersky.com/enterprise

Kaspersky Lab
Enterprise Cybersecurity: **www.kaspersky.com/enterprise**
Cyber Threats News: **www.securelist.com**
IT Security News: **business.kaspersky.com/**

#truecybersecurity
#HuMachine

www.kaspersky.com