

ATM/POS Security Services

ATMs and POS devices are no longer vulnerable only to physical attacks like ATM burglary or card skimming. As protection measures applied by banks and ATM/POS vendors evolve, so attacks against these devices also shift up a gear, becoming ever more sophisticated. Hackers are exploiting vulnerabilities in ATM/POS infrastructure architecture and applications, and are creating malware specifically tailored to ATM/POS. ATM/POS Security Assessment services from Kaspersky Lab help you to recognize the security flaws in your ATM/POS devices, and to mitigate the risk of being compromised.

There is no single solution that offers comprehensive protection. As a business manager, it's your responsibility to protect your organization against today's threats, and to anticipate the dangers that lie ahead in the coming years. This needs more than just smart operational protection against known threats; it demands a level of strategic security intelligence that very few companies have the resources to develop in-house.

Security Assessment Services from Kaspersky Lab – the services of our in-house experts, many of them global authorities in their own right, whose knowledge and experience is fundamental to our reputation as world leaders in security intelligence.



ATM/POS Security Assessment

Comprehensive analysis of ATMs and POS devices, designed to identify vulnerabilities that can be used by attackers:

- unauthorized cash withdrawal
- performing unauthorized transactions
- obtaining your clients' payment card data
- initiating denial of service

Why you should do this

ATM/POS Security Assessment by Kaspersky Lab helps vendors and financial organizations to:

- Understand the vulnerabilities in their ATM/POS devices and improve your corresponding security processes
- Avoid the financial, operational and reputational losses that can result from an attack, through proactively detecting and fixing the vulnerabilities which attackers could exploit.
- Comply with government, industry or internal corporate standards, which include the carrying out of security assessments, e.g. PCI DSS (Payment Card Industry Data Security Standard).

What happens when fraudsters goes in?

Each ATM machine consist of 4 cassettes with up to 3000 banknotes in each cassette. In worst case scenario criminals can obtain up to 255000\$. ATM cash-out scheme happened in May, 2016 showed, that criminals are ready to coordinate their actions to access 1400 ATM machines in couple hours frame. Taiwan incident in July, 2016 with malicious software installed on multiple ATMs given criminals possibility to withdraw 2 million \$ from twenty ATMs. Criminals are ready to attack ATMs. Don't be a victim.

Who we are

Project team members are professionals highly experienced in practical security, who have a deep knowledge in the field and are constantly improving their skills; they regularly provide security consultancy to ATM/POS vendors and present the results of our ATM/POS security researches at leading information security conferences, including Black Hat, Hack in Paris, Positive Hack Days, Security Analyst Summit, Nuit Du Hack, HITB GSEC, DefCamp, ATMIA events, Chaos Communication Congress and many others.

Follow our experts at www.securelist.com

Call us for help 1337@kaspersky.com

What we are testing

The service includes comprehensive ATM/POS analysis including assessment of software components, hardware devices and network communications. Service can be conducted on a single ATM/POS device or on a network of devices. We recommend you to choose for assessment the type of ATMs/POS device in most common use within your organization, or those that are most critical (which have, for instance, already suffered from incidents) in their typical configurations.

How we do this

During analysis, our experts will not just seek out and identify configuration flaws and vulnerabilities in obsolete software versions, but will deeply analyze the logic behind the processes performed by your ATMs/POS devices, undertaking security research aimed at identifying any new (0-day) vulnerabilities at component level. If we uncover vulnerabilities which could profit an attacker (resulting, for example, in unauthorized cash withdrawal), our experts can provide demonstrations of possible attack scenarios using specially crafted automation tools or devices.

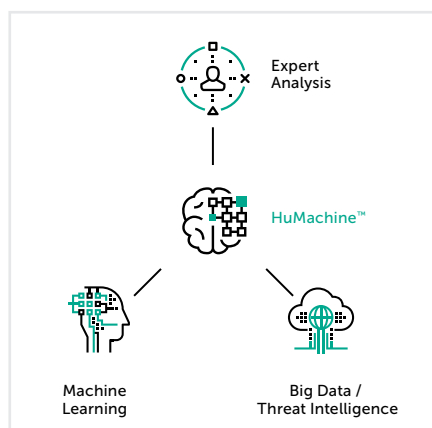
Though an ATM/POS Security Assessment involves emulating the attack behavior of a genuine hacker in order to practically assess the effectiveness of your defenses, it is entirely safe and non-invasive.

Threats for Financial Industry

As banks, stock markets, and other financial institutions are under persistent interest of cybercriminals due to the very nature of the financial business, to avoid financial and reputational losses they have to stay ahead of the curve in the field of cybersecurity. Kaspersky Lab offers a set of proactive threat intelligence services for financial institutions that are looking to enhance their security operations and take a proactive approach against advanced threats:

- Security Assessment Services (Penetration Testing, Application Security Assessment, ATM and POS Security Assessment)
- Threat Intelligence Reports (APT Intelligence Reports, Customer-Specific Threat Intelligence Reports)
- Cyber-Attack Readiness Testing
- Botnet Threat Tracking
- Threat Data Feeds
- Malware Analysis and Digital Forensic
- Training: Threat Analysis, Forensic and Investigation

See more at 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

© 2017 AO Kaspersky Lab. All rights reserved. Registered trademarks and service marks are the property of their respective owners.