DESCRIPTION OF ATTACKS AND COUNTERMEASURES

CONTENT

DESCRIPTION OF ATTACK: “MAN IN THE MIDDLE” (NETWORK) 3

DESCRIPTION OF ATTACK: “STEALING AUTHENTICATION DATA USING A USB-PORT SNIFFER” (SOFTWARE)........................ 4

DESCRIPTION OF ATTACK: “STEALING BIOMETRIC DATA USING SKIMMER” 5

DESCRIPTION OF ATTACK: “MAN IN THE MIDDLE” (NETWORK)

Attack phase	1	2	3	4	5
Phase name	Information gathering	Victim identification	Obtaining logical access to ATM network	Network traffic manipulation	Money withdrawal
Description	Attacker gathers information about the maintenance supplier of the bank and prepares a specially crafted device which emulates the processing center	Attacker chooses the victim ATM devices. These must have network equipment available on the outside, an exposed Ethernet-cable or insecure wireless communications (e.g. GSM)	Attacker connects the specially crafted device to the exposed Ethernet-cable or into the adjacent network socket	Attacker conducts man-in-the-middle attack (e.g. ARP or DHCP spoofing) in order to connect other ATMs to the rogue processing center. Not all machines are susceptible to spoofing attacks, because of network segregation or implemented network security measures.	Attacker withdraws money from ATMs by issuing commands from the rogue processing center and emulating legitimate commands
Countermeasures	• Conduct security awareness trainings • Inform users and employees about information security measures • Monitor the situation on the black market (e.g. with Threat Intelligence reports	• Conduct regular visual inspections of ATMs • Mount video surveillance cameras inside and outside the ATM top box • Use ATM monitoring systems • Implement organizational and technical measures to protect the ATM top box and external communication lines (including wireless) • Conduct regular ATM security assessments	• Remove unused services and applications • Handle network segregation properly • Eliminate network misconfigurations, and security flaws • Use network access control mechanisms (e.g. 802.1x) • Use a network security operation center (SOC) • Monitor newly added devices and hosts	• Handle network segregation properly • Eliminate network misconfigurations, and security flaws • Use antivirus and firewalls to protect against network attacks • Remove excessive communication between ATMs, and between ATMs and the local network hosts (such as ATM administrator host, AD server etc.) • Establish a patching process and put upgrade procedures in place for the operating system and all software • Network communications between the ATMs and the processing center, as well as communications between the ATM core and ATM units must be encrypted (e.g. with TLS or VPN connections). The authenticity and integrity of these communications must be verified. • Enable all security measures implemented by manufacturers • Conduct regular penetration tests on the infrastructure	• Use fraud monitoring systems • Implement authenticated dispense (network communications between the ATM processing center and ATM units must be encrypted. The authenticity and integrity of these communications must be verified) • Conduct forensic investigations to obtain information on the scale of attack

DESCRIPTION OF ATTACK: "STEALING AUTHENTICATION DATA USING A USB-PORT SNIFFER" (SOFTWARE)

Attack phase	1	2	3	4	5	6
Phase name	Information gathering	Victims identification	Spear-phishing attack	Privileges escalation	ATM infections	Customer data leakage
Description	Attackers gather information about the bank's maintenance supplier (i.e. from the company / employee profile on the bank's website, social media, etc.), and prepares malicious emails	Attacker uses social engineering techniques to send phishing e-mails to employees of the ATM maintenance suppliers with malicious contents (such as the exploit code in an attachment)	The victim opens the malicious attachment, a malware with a backdoor, which allows the attacker to obtain a foothold in the internal network. Not all the users open the email because they are aware or they have updates their antivirus software.	Exploiting vulnerabilities, the attacker escalates privileges and obtains ATM administrator credentials. Using AD functionality for group policies, the attacker uses on ATM software USB-port sniffer.	Using the installed sniffer, the attacker collects customer authentication data and card data, allowing him to perform fraud	Attacker sells obtained data on the black-market
Countermeasures	• Social media acceptable user policy • Social media awareness campaign • Conduct security awareness trainings • Inform users and employees about information security measures	• Use Intrusion detection system/ intrusion prevention systems • Run an anti-phishing awareness campaign, • Install anti-virus programs, with anti-spam systems on employees hosts	• Behavioural monitoring system • Install anti-virus programs, and anti-spam systems on employee hosts • Use special sandbox tools to check the content of an unknown file • Monitor the situation on the black market (e.g. with threat intelligence reports)	• Implement software integrity check mechanisms • Implement a trust program zone on the ATM • Use a strict access policy	• Use ATM malware protection systems • Use strong encryption mechanisms for stored data • Encrypt data in-transit • Implement the white-listing of software on ATMs	• Use fraud monitoring systems • Implement a strategy for card data revocation in case of customer data leakage • Conduct forensic investigations to obtain information on the scale of the attack

DESCRIPTION OF ATTACK: “STEALING BIOMETRIC DATA USING SKIMMER”

Attack phase	1	2	3	4	5
Phase name	Information gathering	Preparing skimmer	ATM infections	Biometric data interception	Money withdrawal
Description	Attacker gathers information about the maintenance supplier of the bank	Attacker prepares a specially crafted device for biometric data skimming	Attacker mounts skimmer on the ATM biometric reader, which will collect customer authentication data (fingerprints, for example)	Biometric data obtained via biometric skimmer If the chosen ATM uses another type of biometric authentication, this biometric data cannot be intercepted	Attacker uses obtained biometric data to authenticate and withdraw money
Countermeasures	• Conduct security awareness training • Inform users and employees about information security measures • Monitor the situation on the black market (e.g. with threat intelligence reports)	• Monitor the situation on the black market (e.g. with threat intelligence reports)	• Conduct regular visual inspections of ATMs • Mount video surveillance cameras inside and outside the ATM top box • Use ATM monitoring systems • Use anti-skimming devices • Implement organizational and technical measures to protect the ATM top box • Conduct regular ATM security assessments • Increase customers awareness on secure usage of cards, ATM and necessity of authentication data secrecy	• Conduct regular ATM security assessment • Enable all current security mechanisms implemented by manufacturers	• Use fraud monitoring systems • Use additional authentication factors to confirm the financial transactions • Implement strategy for authentication data revocation in case of customer data leakage • Conduct forensic investigations to obtain information on the scale of the attack

Securelist, the resource for Kaspersky Lab experts' technical research, analysis, and thoughts.

Follow us

Kaspersky Lab global Website

Eugene Kaspersky Blog

Kaspersky Lab B2C Blog

Kaspersky Lab B2B Blog

Kaspersky Lab security news service

Kaspersky Lab Academy