# ATM security: Identify and fix critical flaws in machines and the connected infrastructure

Remediate exploitable vulnerabilities by understanding how attackers can compromise machines

## Table of contents

2 Executive summary

3 Client needs and challenges

4 Phases of testing

5 Manual versus tool-based testing

5 The limitations of scoping and other considerations

6 IBM solution: IBM X-Force® Red ATM penetration testing

6 Testing methodology and options

7 The X-Force Red portal

7 Conclusion

7 For more information

## Executive summary

Attacks against automated teller machines (ATMs) are relentless due to several factors. Criminals target ATMs because the machines provide direct access to physical cash. Additionally, financial organizations lack visibility into ATM activities because they operate hundreds of machines in disparate locations. In 2018, the FBI warned financial organizations worldwide about ATM "cash-out" attacks, where criminals manipulated ATM withdrawal limits to steal money from customer bank accounts.[1] Other "cash-out" tactics included installing malware, attacking the physical machines, stealing debit card and other customer data to create fraudulent ATM cards and changing the amount of funds in accounts.

From 2017 to 2018, X-Force Red, an autonomous team of veteran hackers within IBM Security, saw a 300 percent increase globally from banks requesting ATM security testing. During one engagement, X-Force Red uncovered a zero-day vulnerability that thieves had exploited to install malware on ATMs and steal the equivalent of USD 8 million in cash.[2]

With hackers becoming more skillful and able to bypass anti-skimming devices and other theft deterrents, financial organizations will likely need many layers of ATM protection. Security controls that worked a few years ago may no longer protect against the latest techniques used by attackers, such as the ability to bypass encrypted software. X-Force Red believes an effective defense for ATMs should include a combination of manual penetration testing and layers of security processes and controls to help protect the machine and connected infrastructure.

## Client needs and challenges

ATMs contain many targets for exploitation, within the machines themselves and connected backend infrastructure. Based on X-Force Red's research, physical manipulation is the most common method of attack. Criminals employing this approach typically start with the machines' locks. Many ATMs ship from manufacturers with surprisingly weak locks, allowing for relatively easy access to the machines. A common vulnerability across many ATM models involves a top cabinet lock comparable to the lock on a standard filing cabinet. Thieves can break into some of the locks within seconds and access the ATM's computer system.

**20** **Number of seconds it took an X-Force Red hacker, who had minimal experience picking locks, to pick a client's ATM lock during a 2018 engagement**

Many attacks against ATMs combine a physical assault on cabinet locks with an attack on the machine's hardware and software. This physical access can occur with sophisticated methods of manipulation that might be missed by standard ATM service technicians.

Once inside a machine, criminals can get extended physical access to exploit vulnerabilities in hardware components like cash dispensers, card readers and barcode scanners. Attackers can conduct several malicious activities, such as:

- Installing a skimming device
- Removing a hard drive, installing malware and reinstalling the infected drive without detection
- Performing a "cash-out" of a dispenser to take all stored money

Additionally, service technicians, who receive access to ATMs to do their jobs, could potentially manipulate the dispenser to perform a "cash-out" without breaking a lock.

To combat efforts to install malware on hard drives, some financial organizations rely on encryption, which might not provide adequate protection against attacks. One X-Force Red client lost millions from its ATM network despite encrypting hard drives. During the client's subsequent testing engagement, the X-Force Red ATM hackers targeted the hard drive encryption, found a previously unknown vulnerability in the encryption software and provided remediation recommendations to help protect against future attacks.

Exploiting ATM software weaknesses to steal customer payment card or account information is another attack method. The upper cabinet of an ATM acts much like a personal computer. The motherboard is similar to a personal computer, and specialized devices like cash dispensers are connected just as a mouse device is to a personal computer. Attackers who exploit vulnerabilities with personal computers may find the same opportunities exist with ATMs.

Some banks may rely on ATM manufacturers to ensure the safety of their products. However, these manufacturers are typically not in a position to test any customized features and capabilities that ATM owners and operators may add onto the machines. These additions may offer potential access points for vulnerabilities that criminals may exploit.

Attackers can also compromise ATMs by exploiting vulnerabilities in the bank's local network. Insecure or misconfigured services can potentially introduce vulnerabilities in these networks for attackers to exploit. Some attackers place a device between the actual ATM and where the machine connects to a local network to exploit the machine's insecure communication with backend services.

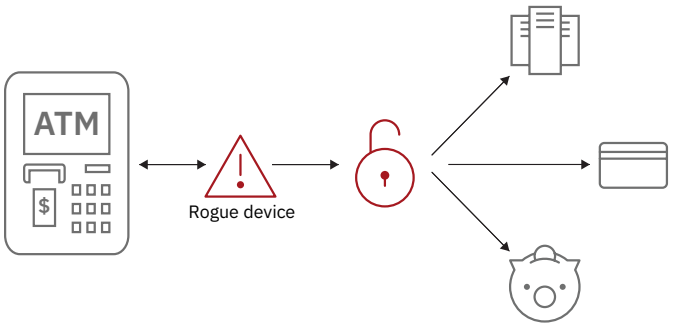


*Figure 1*. Criminals can introduce to ATMs a rogue device that's smaller than an ice cube, which offers a gateway they can exploit.

Remote ATM management tools that lack authentication, encryption or both can offer another way to attack network traffic and affect operations of the ATM. Some criminals plant malware on ATMs to remove only a few thousand dollars at one time. The strategy enables attackers to avoid excessive transactions that may raise red flags. Additionally, service personnel might not notice a small amount of cash missing from the machine, whereas a complete cash-out attack is hard to miss. Attackers using this method can potentially steal currency for months without being detected.

The installed malware can also allow an attacker to access a bank's network remotely and steal valuable data. Some criminals leverage ATM vulnerabilities to compromise other valuable assets. For example, they may compromise an ATM and gain access to the bank's network to collect sensitive corporate information, which they can then use to move deeper into the environment.

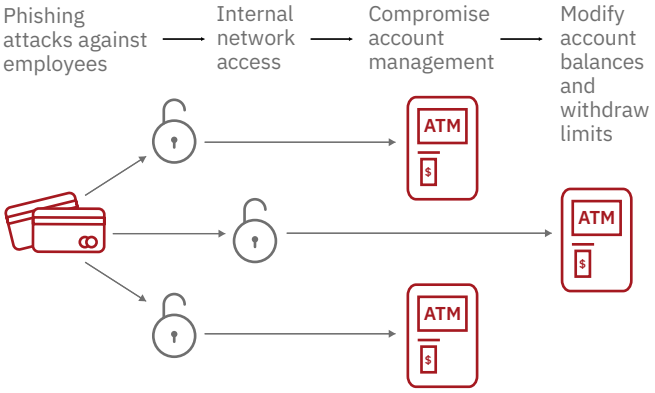


*Figure 2*. By conducting phishing attacks against employees to get usernames and passwords, criminals can manipulate withdrawal limits and create fraudulent ATM cards to take out cash.

Attackers can also use installed malware to access internal bank applications, change withdrawal limits and add funds to accounts. They can use the data to create fraudulent bank accounts.

## Phases of testing

To help protect against the variety of potential attack methods, financial organizations should take advantage of ATM testing programs designed to help protect the machines and connected infrastructure. The testing components should include:

- **Remote network access.** Identifies unpatched software, misconfiguration and default user accounts in remote ATM management tools, remote desktops and other network services
- **Local network access.** Identifies unencrypted network traffic, unenforced encryption and lack of authentication in ATM communication with backend services
- **Momentary physical access.** Identifies unprotected devices and network hardware, undetected rogue devices and weak physical locks on the ATM's chassis, computer and local network infrastructure
- **Extended physical access.** Identifies "cash-out" vulnerabilities, low-level hardware attacks, weak operating system (OS) console hardening and vulnerable disk encryption, and verifies anti-skimming devices
- **Backend services.** Identifies application-level flaws in input validation, logic, authentication and authorization and information disclosure in middleware, mainframe and other network services

Testing that includes all of those components is key. Testing only some components may not provide an accurate picture of the potential vulnerabilities. For example, only testing the ATM's network services won't uncover vulnerabilities unique to the machine's hardware and local software.

## Manual versus tool-based testing

The ideal ATM testing program relies primarily on manual penetration testing with limited automated scanning. Scanning tools can help uncover known vulnerabilities and provide protection against automated attacks. These tools can't discover unknown, complex or physical vulnerabilities, which are responsible for the vast majority of ATM crimes, based on X-Force Red's research.

Manual penetration testing, performed by hackers, can uncover unknown vulnerabilities by using the same tools, techniques and practices that criminals use to find and exploit an ATM's security weaknesses. Manual testing can be an effective technique for identifying critical ATM vulnerabilities that attackers could use to their advantage.

The consequences of lacking a multifaceted testing approach for ATMs can be very costly. Consider the large theft one bank encountered from just one model of several compromised ATMs.

**USD 7 million +**

**Amount in cash taken from one ATM of a large bank**

During its testing, X-Force Red ATM hackers identified the following flaws along with the original source of exploitation, which was the ability to completely bypass drive encryption:

- External ATM locks were compromised in seconds
- Gaps in chassis security allowed for easily accessed internal components
- Major flaws in how drive encryption software stored keys
- Deficiencies in remote monitoring
- Other major vulnerabilities related to remote hardware management tools and local user interface for field technicians

## The limitations of scoping and other considerations

ATM testing is only as effective as what the service provides. For example, if a company decides to use custom scoping prior to the test being performed, it's critical that a global view of threats and vulnerabilities is applied to the process. Custom scoping is the first step of a testing process where the customers determine which parts of their ATM environment should be tested. In some cases, customers may be asked to fill out lengthy questionnaires to determine the scope of the test, which may not be the most efficient nor effective method. The questionnaires typically don't consider active threats or known vulnerabilities exposing certain assets in the environment. Removing questionnaires and having an outside testing team work with customers to determine the scope of the ATM testing engagement would factor in the global threat and vulnerability landscape as well as the company's specific requirements.

X-Force Red uses custom scoping, working with customers directly to determine the number of ATM models to be tested and whether backend systems are included. The decisions can be based on actual thefts from the customers' ATM fleet, the results of previous tests, or new technology that will be deployed into production.

Another component to consider is how the ATM testing is performed. Some customers may request only an automated scan due to cost limitations. Scanning is an effective service for finding known vulnerabilities that can be exploited in purely automated attacks, which are rare against ATMs. Automated scans are poorly suited for identifying real-world ATM vulnerabilities. The scans can identify missing patches or simple operating system misconfigurations but are typically unable to discover complex or previously unknown vulnerabilities. Only manual testing can find unknown vulnerabilities that can be exploited by human attackers. Manual testing can also show how vulnerabilities can be chained together by an attacker to gain deeper access into an ATM environment.

Additionally, multifaceted ATM testing requires specific expertise. Testers must have a strong knowledge of a machine's operating systems, applications, protocols analysis, networking, electronics, physical locks and so on. X-Force Red's hackers have specific experience manually testing ATMs and their connected infrastructure.

## IBM solution: X-Force Red ATM penetration testing

X-Force Red ATM penetration testing is a multistep service delivered by X-Force Red, an autonomous team of veteran hackers within IBM Security. This global team provides manual testing against clients' ATM hardware, software and connected infrastructure. X-Force Red hackers have years of experience testing ATM processes, hardware, software, configurations and features, using the same tools, techniques, practices and mindsets as criminals. Their methodology is ATM vendor and model agnostic. By simulating attacks from multiple access points, X-Force Red hackers can potentially identify critical ATM flaws that may not yet be known by attackers and clients.

As part of the testing service, X-Force Red hackers can also capture and review ATM logs to inform clients if their machines align with industry standards. The X-Force Red team can test against any industry standard clients want.

X-Force Red sells its services using a format where clients pay a flat, monthly rate for testing. Before the project starts, clients can change what they want to test at no additional cost outside the flat rate, depending on the tier of service chosen. The flat rate model gives clients more flexibility to change the scope of the test, without having to re-sign contracts.

## Testing methodology and options

X-Force Red offers two tiers of ATM testing services—standard and advanced. Standard testing involves two testers assigned onsite for a full week to work on ATM models and associated software. The testing includes assessing local network traffic between the ATM and other devices. The X-Force Red hackers test all ATM processes, hardware, software, configurations and features. Testers also perform an offline analysis of the bank's environment and backend systems connected to the ATM. Standard testing typically lasts approximately 12–15 workdays.

With advanced testing, three X-Force Red hackers assess ATM models and associated software onsite for one week, applying more complex testing methods. This testing includes reverse engineering, where testers disassemble software and monitor its activity as it's running. Reverse engineering can help detect undocumented backdoors. Reverse engineering is especially useful for reviewing proprietary software installed by other vendors. Being that ATMs communicate with backend systems, advanced testing also covers application-level testing of those systems. Advanced testing typically lasts approximately 20–25 workdays.

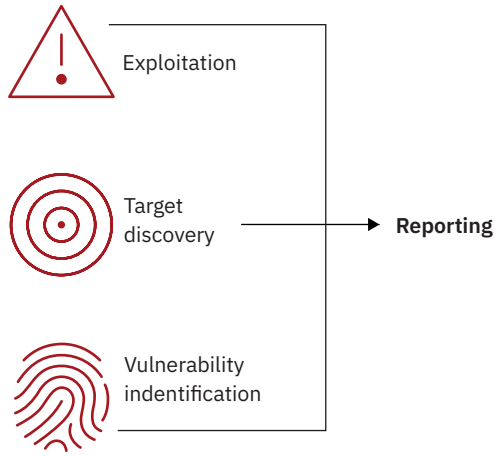


*Figure 3.* X-Force Red hackers perform exploitation, target discovery and vulnerability identification for clients and report their findings for standard and advanced testing.

If clients prefer that X-Force Red teams perform the testing off-site, they can ship ATMs to four global, secured labs operated by X-Force Red. The X-Force Red Labs are located in Austin, Texas and Atlanta, Georgia in the United States, Hursley in the United Kingdom and in Melbourne, Australia. Many of the X-Force Red hackers inside the labs are engineers with security experience, so they can assess ATMs and other devices from a developer's viewpoint.

When testing ends, the X-Force Red team provides clients with a report, which includes vulnerabilities found, methodology used, an attack narrative and high-level strategic recommendations. The findings may uncover other types of problems, such as the need to improve the remote administration of ATMs or re-engineer devices from scratch.

## The X-Force Red Portal

The X-Force Red Portal is a communication and collaboration platform. Through the portal, clients can schedule tests, change the testing scope, communicate directly with testers and view their findings as they are uncovered so that remediation can begin immediately. With the X-Force Red Portal, clients don't need to wait for the test to be completed to review the findings. X-Force Red hackers submit findings when identified, giving the client the opportunity to view and remediate vulnerabilities quickly.

The reports entered into the portal include key findings, evidence of exploitation and actionable guidance for remediation. When entering reports into the portal, X-Force Red hackers allow security leaders to determine who has permission to see the results. Clients can isolate sections of the report into segments so that remediators only see vulnerabilities within their scope.

The X-Force Red Portal acts as a central repository for all reports for clients. Clients requesting multiple tests can monitor, track and review their reports at their convenience. Additionally, clients can view trending data to see and report how their ATM security posture has improved over time.

The portal has its own security controls, which include Transport Layer Security (TLS), which has replaced Secure Sockets Layer (SSL), storage encryption, two-factor authentication and more.

## Conclusion

Millions of dollars in cash are at stake when ATM security fails. X-Force Red ATM testing can help organizations reduce the risk of an ATM compromise by uncovering vulnerabilities across the ATM environment that criminals can also find and leverage. X-Force Red hackers perform manual penetration testing against an ATM and its connected infrastructure and provide actionable remediation recommendations to help clients know which vulnerabilities to fix first and how to go about doing so.

## For more information

To learn more about IBM X-Force Red ATM testing, please contact your IBM representative or IBM Business Partner, or visit ibm.com/security/services/atm-testing.

To read a case study, visit ibm.com/case-studies/large-commercial-bank.

To watch the X-Force Red webinar about cash-out attacks, visit https://ibm.biz/BdY8tr.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
July 2019



1. Vito Pilieci, “FBI warns banks about looming cyber attacks,” *Ottawa Citizen*, August 16, 2018, ottawacitizen.com/news/local-news/fbi-warns-banks-about-looming-cyber-attacks

2. X-Force Red ATM testing case study, www.ibm.com/case-studies/large-commercial-bank

11025611USEN-00