THE CURRENT STATE OF CYBERSECURITY FOR ATMS

WHITE PAPER

THE # NEXTGENBANK®

AURIGA
the banking e-volution

www.aurigaspa.com

There has been a growing number of cyberattacks against ATMS and central servers, which are the systems that control ATMs. This pressing threat has resulted in the theft of personal data, such as account numbers and pin codes. However, these types of attacks still require further actions to convert the data into money, so a simpler effort for ATM cyber-criminals is to obtain the cash directly from the ATM they have targeted.

One form of ATM cyberattacks is 'jackpotting', where cyber-criminals exploit the physical and/or software-based vulnerabilities of an ATM to try and obtain cash. This action has been popular as it provides an immediate reward; in the last five years, financial organisations from around the world have lost millions because of jackpotting. For example, the Ploutus family of ATM malware first discovered in Mexico in 2013 has accumulated a loss of over 450 million dollars (398 million Euros) globally.

HOW SERIOUS ARE THE VULNERABILITIES IN ATMS FOR CYBER-ATTACKS?

ATMs have become subject to both physical attacks (skimming, explosive gas) and logical attacks (malware, software skimming, black box). They have become an attractive target for cyberattacks for a few reasons. The cash in the ATM acts as an incentive, as well as the confidential information (credit/debit cards and PINs), which can also be converted into cash.

There are two types of attacks:

1. ATM Malware Attacks (logical)
2. ATM Black Box Attacks (logical/physical)

However, ATMs often have weak points that criminals exploit for their own personal gain. ATMs are sometimes poorly monitored and little to no logical action is taken to safeguard the data in them.

Another vulnerability is the large number of actors involved in cybersecurity, such as financial institutions, installers, service providers, developers, etc.). This can mean too many people have admin rights to ATM systems and this can be a potential increased risk of unauthorised access. Additionally, these disparate teams, often from third party suppliers, involved in ATM maintenance and support, don't work in tight collaboration and there isn't a cohesive overview of their activities, creating the potential for serious gaps in security oversight.

An ATM ecosystem is complex, consisting of a variety of hardware and software. Because of this, organisations find it difficult to have and apply proactive software and operating system update policies or have a centralised, full visibility of their security infrastructure. Outdated hardware and software can even result in non-compliancy with PCI regulations, even though banks are required to fulfil these regulations.

Financial institutions face several challenges in making ATMs available 24/7/365 while ensuring maximum security. On one side, they need to minimise the burden of software deployment and hardware maintenance and maintain visibility and control over changes in software and hardware. One the other side, security policies must be applied and adhered to and integrated visibility and management of the security status must be ensured.

WHY HAVE CYBERCRIMINALS BEEN SUCCESSFUL IN TARGETING ATMS?

Cybercriminals have realised that within a bank's security infrastructure, the ATM networks is often one of the weakest points.

One reason for this is that the legacy hardware and software in ATM networks is too expensive and difficult to update. This leaves the systems in a very insecure position. For example, many ATMs are still using Windows 7 or in the process of migrating to

Windows 7, which Microsoft no longer supports. This means there are known vulnerabilities that cybercriminals could use to perpetrate attacks as the OS does not receive the patches from Microsoft anymore to be protected. Auriga estimates that 40% of ATMs globally are running on even older operating systems (like Windows XP-OS) that have not been supported by Microsoft since 2014, making such machines even more vulnerable to attacks.

One of the main attack vectors on ATMs, however, is the XFS layer, which is the standard interface designed to allow multivendor software to run on manufacturers' ATMs and other hardware. The XFS layer uses standard APIs to communicate with self-service applications. This middleware was not designed with an integrated authentication process, so criminals have understood this and exploits this fact enormously. Cybercriminals could deploy the malware onto hardware devices such as ATM cash dispensers to 'cash out' commands and dispense cash (jackpotting) or the malware could be used to steal card numbers (software skimming) which makes the XFS layer an attractive target.

OUR TOP TIPS FOR BANKS THAT ARE AT HIGH RISK OF FINANCIAL FRAUD

Generic endpoint protection technology such as anti-malware solutions or technologies designed to protect PCs and laptops is not enough to protect ATMs and ATM networks. ATMs represent critical infrastructure that cannot be taken offline to be rebooted; they need to be available 24/7, 365 days a year, and so require a different approach to cybersecurity. Attacks are more targeted than in the IT world and require specific protection from specialized solutions designed to protect critical infrastructure such as ATM networks.

Banks need a centralised security solution that **protects**, **monitors**, and **controls** their ATM networks so they can manage their entire ATM network in one place to stop malware attempts or fraudulent activity at compromised ATMs.

An integral ATM security solution which allows central management of the ATM network and execution of remote actions, saves banks time and money. It is very important for banks to have several layers of protection in one single platform, which is exactly what really differentiates Auriga's LDM ATM cybersecurity solution.

The different layers are:

- Application Whitelisting: the layer that prevents execution of malware or unauthorized software by defining a whitelist of processes that can be executed on the ATM.
- Full Disk Encryption of all hard disks and volumes: an absolute must for any bank to protect their ATM network, as without this, criminals can steal hardware and perform reverse engineering to introduce malware onto the hard disk and then replace it in another bank branch.
- File System Integrity Protection to block any attempt to modify any critical file for anybody unless the process of software updates which is predefined.
- Hardware Protection: Prevents connection of fraudulent hardware, blocking devices not included in the white list.

Although banks are making a determined effort to improve their security, cybercriminals are continuously investing in creating more sophisticated attacks to develop new techniques and identify new vulnerabilities to exploit. To keep pace, banks must be proactive in implementing and testing their cyber defences.

So, complementing their investment in specialist ATM cybersecurity solutions should be an ongoing effort to have ATM security independently tested. This involves specialised security consultancies to check security plans and processes. Essential elements of this approach include ATM network penetration testing, vulnerability assessment techniques, Blue teams, Red teams, and the performance testing of a bank's security operation centre.

Cyber Threat Intelligence (CTI) can be utilised as an early warning system to detect and contain potential threats before they escalate. The intelligence is vital for all businesses including banks as cybersecurity threats become increasingly targeted and successful.

When banks become aware of any relevant threats and vulnerabilities, they will then understand where and how these can be exploited and the impact that this may have on the business as well as individuals. CTI provides banks with visibility into their own landscape, and identifies which areas need to be prioritised for protection.

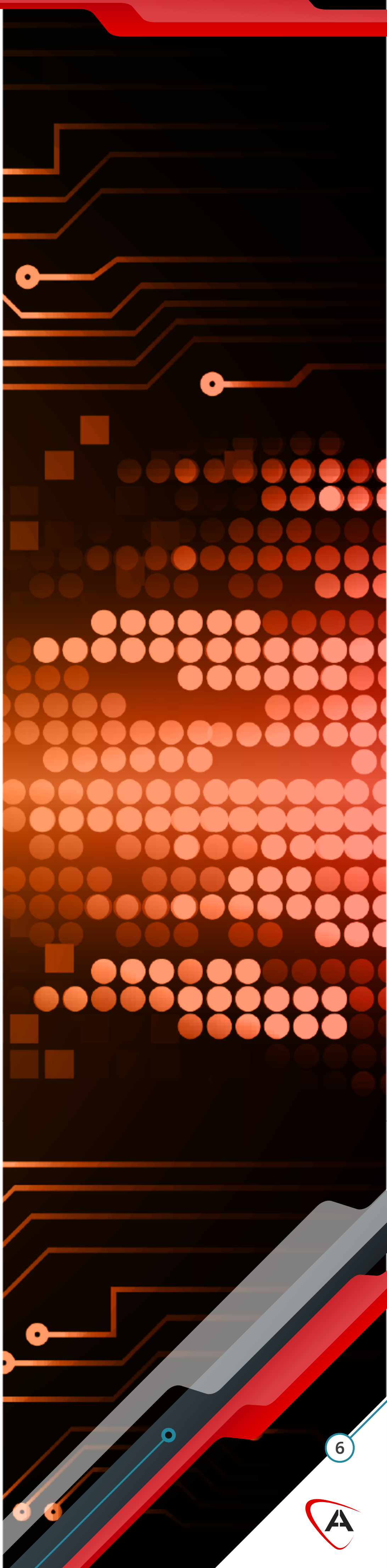
While banks must be concerned with the next strain of malware, many of the variants will seek to exploit existing vulnerabilities that may have already been patched. A good first step as a preventative approach is combining vulnerability management with threat intelligence.

Banks must be aware of the threat landscape to understand what could be exploited and utilised for future cyberattacks. However, there will always be instances where variants of malware are successful and it is critical that banks possess a robust business continuity and disaster recovery plan, which is part of the operational resilience framework. This must include how to react to such incidents, alongside the ability to quickly restore affected data and systems with little impact to operations.

Cybersecurity that is effective will only rise in importance. As financial institutions remain a constant target for criminals, they will have to maximise efforts to protect themselves from this dynamic threat and avoid data breaches, which could expose hundreds and thousands of people's sensitive personal information. While banks are also shifting to cloud after recognising its advantages, it is important to note that Cloud services must comply with cyber security standards that safeguard the data of the users and companies that contract the services. It can be a very complex process, especially when ATM hardware sometimes does not allow for migration, or there are dependencies on the software, as there are different software layers in the ATM software stack. What we propose is a consultancy phase before the actual installation of such solutions to make sure that everything works properly before you go into production.

A close cooperation between software developers and financial organisations is required to assure the right integration between ATM hardware providers, software providers, security solution providers and companies that manage ATMs. When it comes to implementing a new project, hardware and software developers need a deep understanding of the entire environment of the ATM network. They need to take into consideration all the elements when defining the scope and interconnectivity of the solution with the software and hardware pieces which compose the network.

Ultimately, it is important for banks to be aware of all the threats within the environment to know what can be exploited and utilised for future cyber-attacks. If not, they run the risk of being exposed to future security breaches, stolen cash, and loss of customer data.



WHITE PAPER

THE # NEXTGENBANK®

AURIGA
the banking e-volution

Building 3, 566 Chiswick High Road
London W4 5YA - United Kingdom
www.aurigaspa.com
london@aurigaspa.com