WHITE PAPER

FiXS

Banks can fightback against ATM Jackpotting

THE # NEXTGENBANK

AURIGA
the banking e-volution

ATMs are critical devices that provide access to cash and other important banking services for customers, so their continuous availability without interruptions is essential. The sentence "if it works, don't touch it" is especially relevant in this scenario, the modifications or updates of the software and hardware that support the service must always be done in a controlled manner and follow strict processes, certification, and phased deployment.

From a security point of view, however, the lack of **proactive update policies**, added to the **physical accessibility** of these devices, creates a situation that makes ATM devices very difficult to protect with traditional security technologies.

Indeed, ATMs have become a very attractive target for cybercriminals to exploit as they carry sensitive data such as credit card or PIN numbers, plus, of course, large amounts of cash to steal.

FiXS: New malware, old techniques

ATM Jackpotting

ATM Jackpotting is a well-known cybercriminal technique that uses malware to make an ATM dispense large sums of cash without the need for a payment card; fully bypassing the transaction authorisation processes.

As this technique is very lucrative and easy to commit, it has been on the rise over the past few years, and this trend is sure to continue unless banks take action. Jackpotting relies on how ATMs are both physically accessible and often in remote locations without proper

The vulnerabilities in ATMs

surveillance; and have software vulnerabilities that can be too easily exploited. If the hackers succeed, they cash out all the funds in the ATM. As the money technically does not belong to any account, usually none of the bank's customers bear the brunt of the attacks.

It is unclear how much cash has been stolen as a result of Jackpotting to-date, but the machines can be forced to dispense money at a rate of 40 notes every 23 seconds until it is empty, according to the US Secret Service. The only way to stop the machine spitting out cash is to press the cancel button on the keypad.

History of ATM Jackpotting

The first ATM Jackpotting attack was reported in Mexico in 2013, and it quickly spread across Europe and Asia Pacific. The first attack in the US was reported in 2018. In one famous heist called Laszarus it is estimated $14 million was stolen in two hours in India.

Jackpotting presents a global challenge for the financial services industry. With cybercriminals putting in lots of effort to develop innovative ways of attacking the cash and IP address of these ATM machines, there is no doubt that Jackpotting will continue to rise, especially as the return on investment can be huge.

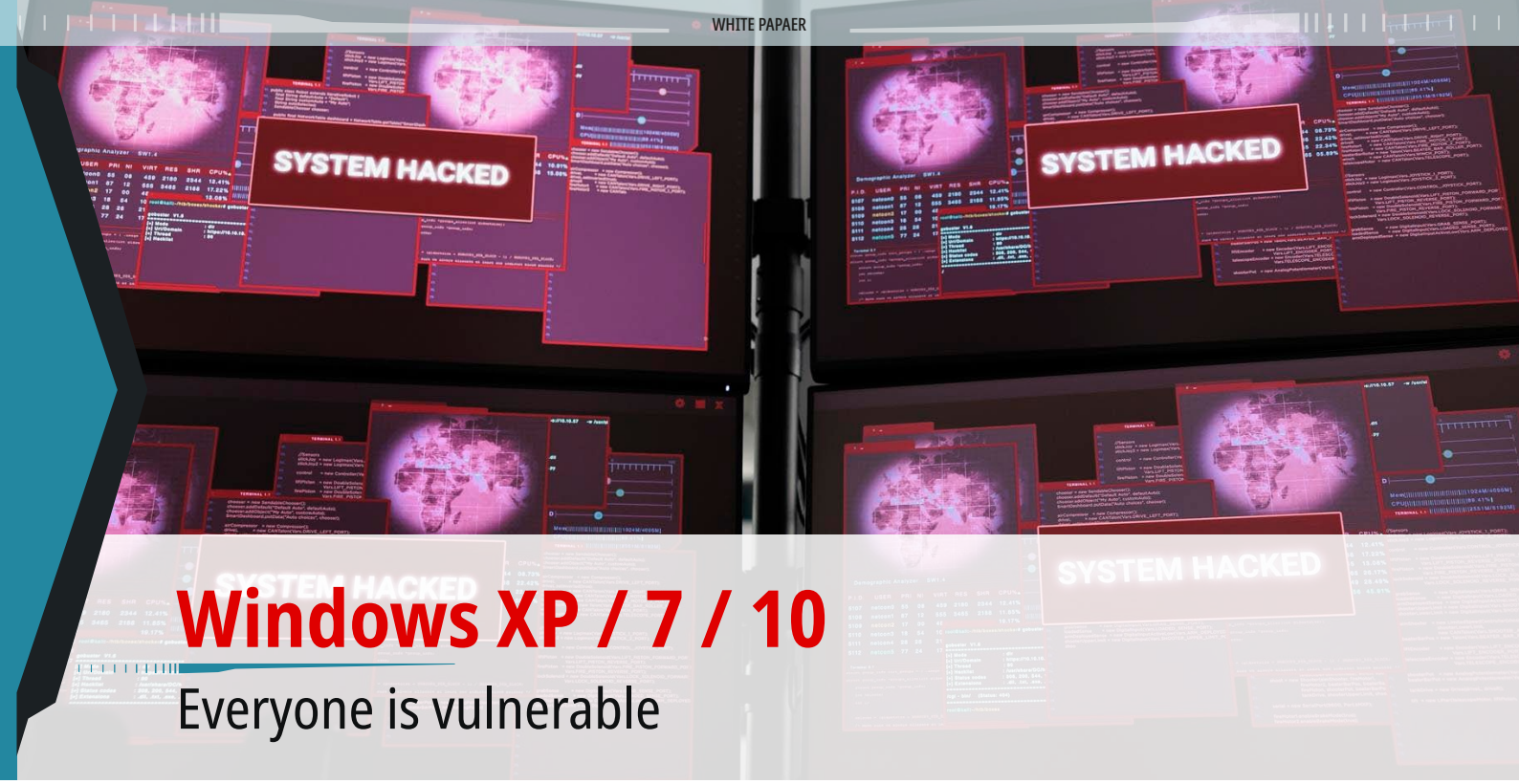
Dissecting FiXS ATM Jackpotting Malware

As a example of how Jackpotting continues to be a threat in February 2023 a new variant of malware, called **FiXS** was reported infecting ATMs in Mexico. This is a new piece of malware,

but the techniques and tactics used ressemble other ATM malware families like Ploutus, Tyupkin, Alice, Ripper, and Cobalt.

FiXS has only been detected in Mexico so far, but its appearance does mean ATM operators would be wise to review and even renew their efforts to prevent these extremely sophisticated attacks. It is particularly lethal because of its ability to infect multiple ATM vendors and models, thanks to its interaction with the **XFS (eXtended Financial Services) middleware** that controls the ATM hardware, including the cash dispenser.

By connecting to the XFS layer, FiXS sends commands directly to the **ATM dispenser to cash-out**, fully bypassing the transaction authorisation process. FiXS is packaged in a dropper that masquerades as a common system executable, conhost.exe. This embeds the malware (FiXS.exe), which is extracted and copied to the ATM File System. Using the MSXFS.dll library, the malware can interact with the XFS API and send commands to the ATM hardware like the dispenser. Interaction with FiXS is done via a connected keyboard, which launches the malware Graphical User Interface (GUI) to allow the attacker to display information of the cash units and to send dispensing commands.



Windows XP / 7 / 10

Everyone is vulnerable

There are claims that ATMs running outdated operating systems, such as **Windows XP** or **Windows 7**, are more vulnerable to Jackpotting because they are no longer supported by new security patches. However, even after migration to **Windows 10** and patch updates, Windows 10 ATMs are just as susceptible as those running Windows 7 or XP. Due to the fact that ATM malware, like FiXS, is highly targeted; it does not exploit operating system vulnerabilities but rather design vulnerabilities of the ATM software stack, like the lack of authentication in the XFS layer.

FiXS attack lifecycle - from infection to execution.

Leveraging an in-depth knowledge of the software stack and the hardware setup of the targeted ATMs is critical to mitigation. Physical accessibility to the ATM is another key factor. A successful ATM Jackpotting attack consists of four phases: preparation, infection, persistence, and final execution.

- **01 – Preparation:** The attacker first steals a hard disk from a production ATM, containing the software stack used by the financial institution, to analyse and reverse engineer it to prepare a targeted attack. A full R&D process is conducted, including the development, packaging, and testing of a new malware such as FiXS.

- **02 – Infection:** The targeted malware is ready to infect ATMs or ASSTs that are loaded with cash. This is accomplished by physically accessing the device and manipulating it to copy the malware with the help of external keyboards and USB sticks, or by accessing the operating system.

- **03 – Persistence:** The attackers need to make the infection persist in time, which can be achieved by replacing legitimate system executables or by setting autorun keys during startup. The persistent malware will then run silently waiting for an activation code.

- **04 – Execution and Clean Up:** With these steps done, the illegitimate extraction of cash can take place. The attacker activates the malware by entering a code that wakes it up and launches a GUI to dispense cash, which is picked up by the gang.

"Zero Trust" protection model

Adopting the right approach

Every organisation operating an ATM network is a potential target for Jackpotting attacks, which makes the application of robust and efficient cybersecurity countermeasures essential.

Any modifications or updates of the ATM software and hardware must always be done in a controlled manner.

The **Zero Trust protection model** assumes that the infrastructure managing ATM and ASST devices will be compromised, and enforces the principle of "never trust, always verify" to prevent cyber attacks from taking place. It is based on the drastic reduction of the attack surface and a tight control of hardware and software changes in the ATM.
To design a robust security framework, organisations must identify the most critical points.
Access to software, hardware, and communications must be continuously verified, only granting access to the minimum set of resources that are legitimate and required for the proper functioning of the device.

Furthermore, hardware changes made by third-party companies with physical access to the ATM should only be possible in authorised time periods, where a specific security policy that allows modifications is applied. These changes should also be subject to total monitoring of technical operations and explicit authorisation.

LOOKWISE DEVICE MANAGER (LDM)

The right solution

Lookwise Device Manager (LDM) is Auriga's response to cyber attacks on self-service banking devices. As a specialist cybersecurity solution for preventing attacks on ATM and ASST technologies, LDM applies a Zero Trust approach, as well as utilising the knowledge of the network infrastructure, and the attacker's tactics and techniques. It provides the most comprehensive layered protection model for ATMs, ASSTs, and other critical devices at all stages of the attack lifecycle, ensuring full availability of services for customers.

Firewall protection is also important to avoid communication with external "command and control" panels. Many malware families use callback functions to communicate with external panels to receive orders.

LDM firewall protection prevents a malicious process from communicating with an unauthorised external system.

The latest ATM Jackpotting attack using FiXS shows that banks and other operators of ATMs must adopt a robust **Zero Trust cybersecurity model** to protect their ATM and ASST devices. The physical accessibility of ATMs, the lack of proactive update policies, and the critical nature of these devices creates an inherently vulnerable environment. It is important to understand that these characteristics or limitations are an integral part of the nature of these devices - instead of trying to fight against windmills, what we must do is define an appropriate security strategy for the environment we want to protect and turn the weaknesses into strengths.

THE # NEXTGENBANK®

AURIGA
the banking e-volution

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

www.aurigaspa.com