nccgroup

Jan 11, 2021 16:36 GMT

Why ATM security has never gone out of style

Despite a rise in internet-based and cashless banking, ATM security remains as important as ever. Here, Daniel Calvo, Senior Security Consultant, explores the evolution of ATM security and how we can keep these machines secure in the years to come.

Automated Teller Machines (ATMs) are a combination of safe deposits and electronic telecommunications devices. Introduced in the 1960s, they enable customers to perform a wide variety of operations, such as cash withdrawals, transfers or deposits, and have become ubiquitous across the world's banks, high streets and shopping centres.

As ATM technology has become more connected, the associated security risk has increased. Although banking has become more internet-based over the last 60 years, access to cash withdrawals and banking service remains important around the world – there are still around 60,000 ATMs active around the UK, with another 394,000 across Europe and 500,000 in the US.

The evolution of ATM security

ATMs have been evolving since the very first device was installed. For example, the first protection mechanism was a personal identification number (PIN) which was introduced to avoid the need for human intervention to authenticate the user. The design of these early machines also helped to reduce their attack surface as they had no network connectivity, a smaller cash capacity and included a safe.

Around about 1980, ATMs began to be more widely installed around the world and became interconnected via networks such as X.25. TCP/IP was later adopted as the general purpose communication protocol that we see in most modern devices.

As new ATM capabilities were implemented, such as receipts and printers, this attack surface grew. For example, the presence of an SDC bus, a proprietary protocol, was exploited to obtain unauthorised cash withdrawals by drilling a hole in the fascia of the ATM.

Over time, less secure components and protocols have been replaced with more secure alternatives, and now, protection mechanisms such as cryptographic-protected PIN pads, boot security and hard disk encryption are required to meet the PCI PTS validation process.

Considerable improvements have been made to these protection mechanisms since the early days. These include security solutions based on minimal Linux systems which are used to boot an encrypted Windows partition. In addition, SecureBoot mode can be used with integrity checking features enabled, the encryption key can be stored in a TPM cryptographic chipset bundled into the ATM´s motherboard, or stored on USB devices placed within the safe.

Securing the future of ATMs

The challenge for all ATM providers and banking-related companies is how to keep the associated threat modelling up-to-date in this fast-moving environment. With the potential impact of attacks ranging from direct financial loss to reputational damage, it is crucial to be able to accurately estimate the risk and possible impact of ATM attacks.

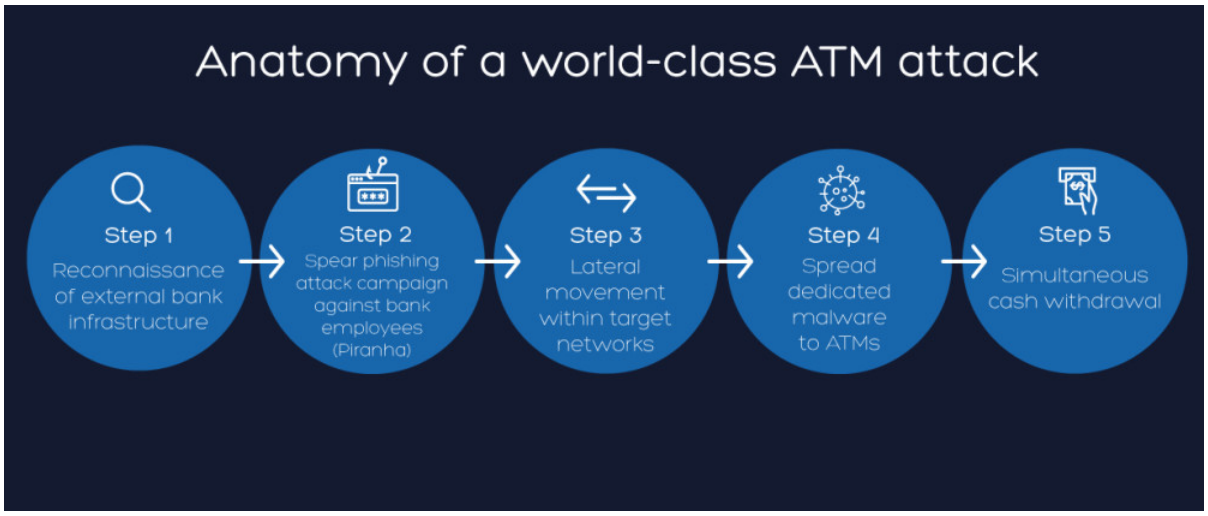
Another new challenge is that ATMs are now deployed in a much wider range of environments. In addition to the traditional hole-in-the-wall deployment, they can now be found in locations as diverse as shopping centres, small independent shops and other small businesses with long opening hours. At the same time, attackers have become more sophisticated; for example, attacks may be aimed at obtaining access to ATM networks instead of individual ATMs.

All of these changes require new efforts from the companies who manage these operations and monitor their health; challenges both in managing different forms of statistics and different approaches to security.

As an example of how ATM attacks have changed from simple, single machine cash thefts, in July 2016 more than 2.63 million US dollars were stolen from 41 different ATMs in Taiwan. Attackers were able to break into the internal bank network - almost certainly after performing some initial reconnaissance - and used a spear phishing attack to target certain key employees in certain banks. As a result, they were able to compromise at least one bank employee's workstation. More recently, in 2018, malicious actors were able to withdraw cash simultaneously from ATMs in 23 different countries, by targeting the retail payment system infrastructure.

Of course, as attacks have become sophisticated, so too have the tools available to the banks and their vendors. As an example, banks can now rely on third party companies to provide mechanisms by which an ATM could be remotely rebuilt if it failed, avoiding the need for technicians to travel onsite to work on the physical ATM.

By ensuring that security is considered at every stage, and consistently taking into account risks associated with physical controls, networks, and operating systems, security teams can keep ATM systems up-to-date and secure in the midst of a changing threat landscape.



About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 15,000 clients worldwide to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience and global footprint, it is best placed to help businesses identify, assess, mitigate and respond to the evolving cyber risks they face.

To support its mission, NCC Group continually invests in research and innovation, and is passionate about developing the next generation of cyber scientists.

With over 1,800 colleagues in 12 countries, NCC Group has a significant market presence in North America, continental Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia and Singapore.

Contacts

NCC Group Press Office
Press Contact
All media enquires relating to NCC Group plc
press@nccgroup.com
+44 7824 412 405
+44 7976 234 970

NCC Group - Financial Media Enquiries
Press Contact
Maitland AMO
Financial Results Media Enquiries
+44 (0)20 7379 5151

Regional Press Office - North America
Press Contact
NCCGroup@cdc.agency
+1 408 776 1400
+1 408 893 8750