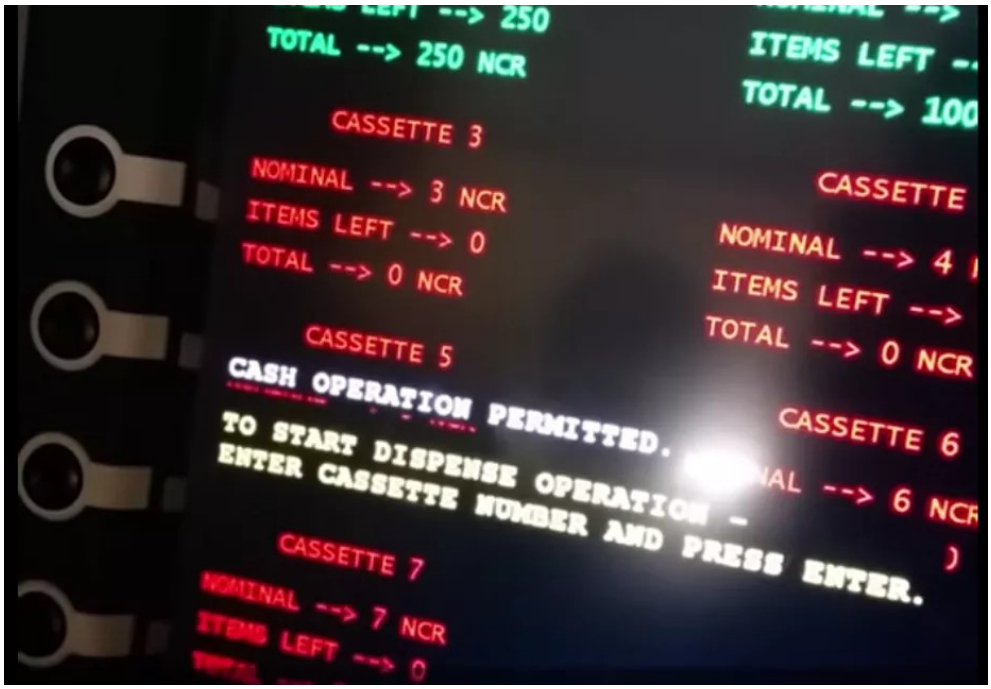
THE CONVERSATION
Academic rigour, journalistic flair

When the ATM runs Windows, how safe is your money?

October 13, 2014 6.23am BST



Roll up, roll up for your free money. Kaspersky Lab

Author

Bill Buchanan

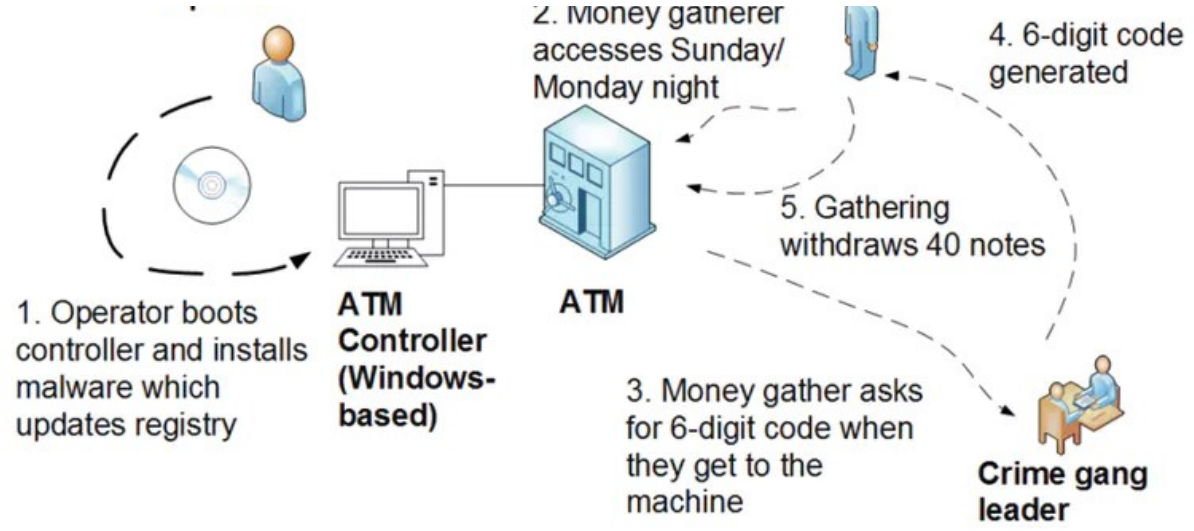
Head, Centre for Distributed Computing, Networks and Security, Edinburgh Napier University

How safe is Microsoft Windows? After all, the list of malware that has caused major headaches worldwide over the last 15 years is long – viruses, worms and Trojans have forced computers to shut down, knocked South Korea offline and even overloaded Google's servers.

Now, how safe do you feel knowing that cash machines across the world run Microsoft Windows?

An exploit has been discovered, apparently spread across Russia, India, and China, whereby cash machines can be turned into a free money vending machine.

The hack requires re-starting the cash machine – essentially a Windows terminal – from a prepared CD that injects malware into the system to circumvent the security. At set times of the week, a unique code is generated and given to a "mule" who would approach the machine, enter the code, and withdraw up to 40 notes, anonymously and without trace.



Hacking ATMs for profit. Bill Buchanan, Author provided

From skimming to hacking

Attacks on ATMs (those more sophisticated than removing the cash machine and cutting into its safe) started around 10 years ago with card reader devices containing a tiny integrated camera and card reader. As a user withdraws cash, the device reads the account details from the card's magnetic stripe and videos the pin number entered into the keypad.

Earlier generations of ATM machines were often built around computer terminals running IBM's OS/2 operating system (which started life as a joint IBM-Microsoft venture, and which somewhat ironically spawned Microsoft's Windows NT, the grandparent of modern Windows, and IBM's OS/2 when that project collapsed). Due to its more esoteric and rare nature there are far fewer attacks for OS/2, but now it is standard builds of Windows, potentially vulnerable to all the usual malware and exploits, that run modern ATMs.

So it is not surprising that intruders have started to find ways inside the ATM's card processing and cash dispensing systems. Malware that can offer external control to an ATM have been reported for some years, allowing attackers to dispense cash, record and print out card details and PIN numbers.

Under the hood

This latest malware is Backdoor.MSIL.Tyupkin, which while running continuously will only listen for commands on a Sunday and Monday night. The criminal gangs operating the malware generate a random, unique, six-digit keycode that activates the program, which is given to the "mule" who is withdrawing the money.

Like previous efforts to crack into ATMs, the malware requires physical access to the ATM, typically by booting the ATM from a CD prepared to install the malware. At present the malware has been active on at least 50 ATMs in Russia and Eastern Europe, but also in the US, China and India.

The malware is the file ulssm.exe, which is copied into the c:\windows\system32 directory and which is protected and maintained on the system between reboots by modifying the Windows registry (a database of configuration settings) so that Windows automatically runs the program at startup. The program then interacts with the ATM through the Extension for Financial Services (XFS) library, MSXFS.dll. To avoid detection it will only allow access controller commands on Sunday and Monday evenings.

This shows an example of malware installing itself onto a system, updating the Windows registry to autorun when started (at 25:20), and then going into hiding.

Playing catch up

The threat of re-booting machines from CDs or bootable USB sticks in order to install malware and abusing Windows autorun feature to sustain the program in memory, is an exploit that has been common for over a decade. It seems few lessons have been learned in terms of securing physical access to the device, and also in the privileged rights that malware can gain. Even as companies focus on improving and securing the user interface, often the debugging and diagnostic side can provide further routes into a system.

Versions of Windows used in embedded control systems are now sufficiently secure, but as ATM manufacturers use standard installations of Windows they are opening themselves up to further problems – not least because it allows hackers the opportunity to simulate and craft their malware on well-known versions of the operating system.

However, at the core of this attack – as with those before it – is the need for physical access to the device, which implies an insider working in the bank. That means with monitoring of who has access to the cash machine, this can be prevented. The key lesson is that the ATM operating system is a weak link in the chain which needs to be closed.

Hacking **Crime** **Fraud** **Cybercrime**