13 October 2014, 6.23am BST

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

AUTHOR

Bill Buchanan

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

DISCLOSURE STATEMENT

Bill Buchanan does not work for, consult to, own shares in or receive funding from any company or organisation that would benefit from this article, and has no relevant affiliations.

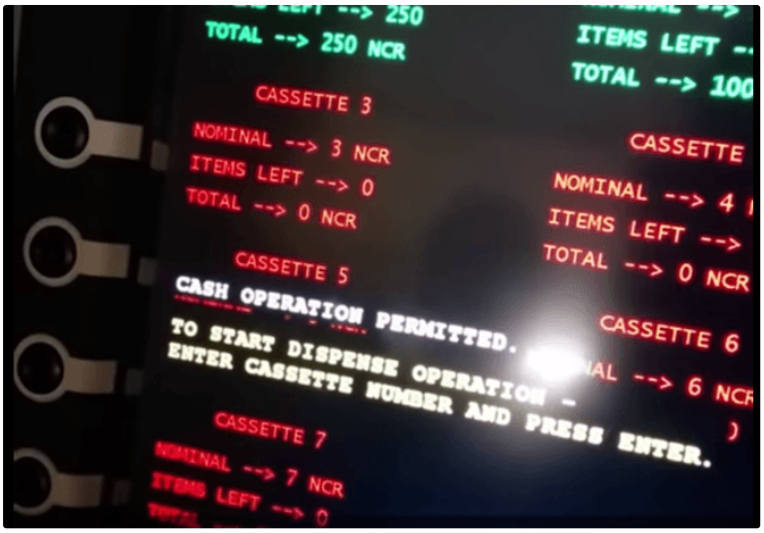
Edinburgh Napier UNIVERSITY

Provides funding as a Member of The Conversation UK.
napier.ac.uk/Pages/home.aspx

EDINBURGH NAPIER UNIVERSITY EVENTS

Are we really safe? Ñ Edinburgh

MORE EVENTS



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

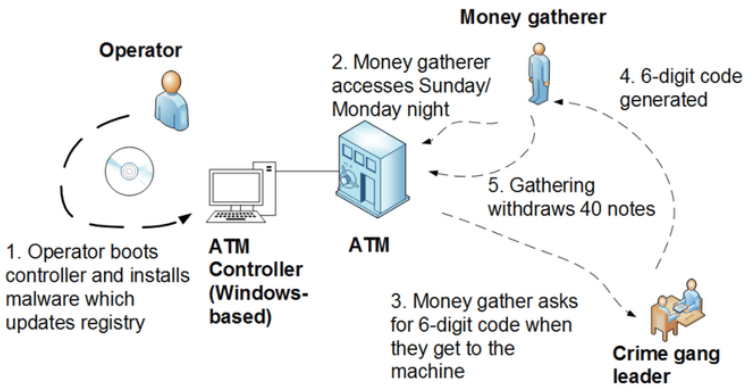
How safe is Microsoft Windows? After all, the list of malware that has caused major headaches worldwide over the last 15 years is long Ð viruses, worms and Trojans have **forced computers to shut down**, **knocked South Korea offline** and even **overloaded GoogleÕs servers**.

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 Ð essentially a Windows terminal Ð 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 ÒmuleÓ 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 cardÕs magnetic stripe and videos the pin number entered into the keypad.

Earlier generations of ATM machines were often built around computer terminals running **IBMÕs OS/2 operating system** (which started life as a joint IBM-Microsoft venture, and which somewhat ironically spawned MicrosoftÕs Windows NT, the grandparent of modern Windows, and IBMÕs 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 ATMÕs 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 ÒmuleÓ 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.

Fact Check: has violent crime gone up?

There is no evidence that the death penalty acts as a deterrent

Manifesto Check: UKIP pledge more police resources, despite falling crime levels

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 Ð 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 Ð as with those before it Ð 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.

Join the conversation

Henry Verberne
Once an IT professional in the fossil fuel industry but now free to speak up

As long as the money of the innocent user is not threatened I refuse to be concerned for the banks if they either cannot be bothered or will not spend money making it very difficult to hack into ATM's.

7 months ago ¥ report

Comment removed by moderator.

David Roth
Postgrad History Student, Retired Software Engineer

The weak links are insufficient controls on procedures for physical access to the ATM software and hardware, not the operating system. It is up to the banks to provide for cross-checking protocols, so that each access is checked and logged independently.

7 months ago ¥ report

Felix Lawrence
logged in via email @gmx.com

I don't see how Windows has anything to do with this security problem. If an attacker is given physical access to the machine to the point where they can boot it off a CD or USB stick, then unless extreme measures have been taken*, it's game over even if the machine is running Linux or OpenBSD.

This is not due to holes in any operating system - it's due to the fact that if you can boot off your own prepared USB stick then you have root access with which you can install any software you like, no need for hacking.

* e.g. encrypting the hard drive with a password that must be manually entered every time the ATM is restarted - but if the attackers are insiders with physical access, they can probably acquire such a password too.

7 months ago ¥ report

Danny Hoardern
Analyst Programmer

In reply to Felix Lawrence

Yeah bios is independent from the operating system, so you're right - it shouldn't matter which operating system was on there once it's booting up.

(Unless Microsoft have somehow managed to modify bios code then reflash to make it less secure - highly doubt it though).

But the overall question of whether it's easier to break into a Windows machine....

Read more

7 months ago ¥ report

Gerd Martin Jansen
retired engineer

When Windows run ATMs should be a better title.

7 months ago ¥ report

Comment removed by moderator.

Comment removed by moderator.

Comment removed by moderator.