malaymail online
HAPPY CHINESE NEW YEAR

Outdated software could have left ATMs vulnerable

KUALA LUMPUR — Banks could be exposing their automated teller machines (ATM) to cyber attacks if the machines are still running on the Windows XP operating system, says techie Farhan Gazi.

He said Windows XP was now outdated, and its developer Microsoft announced it ended support for the operating system since last April.

"If the machines are using an operating system that is no longer being supported, it will face a lot of threats," said Gazi, who writes on technology online.

Commenting on the use of SIM cards in the high-tech heist involving Latin Americans, he said: "When the ATM information can be placed in a SIM card, it may fool the machines and the only way to really protect yourself from this is to not use ATMs at all."

Another method that could be used, he said, is to turn the ATM's user manual against itself.

"All you need is a user manual which can be found online to give the user complete access to the ATMs," he said.

"A lot of ATM owners don't change the default password and this password is usually in the user manual. Once they enter the default passwords, they can have access as an administrator and do whatever they want."

On the use of viruses in hacking, web designer Michael Kwan, 29, said a virus could override an ATM's control to release the money.

"After getting to know the story from newspapers, it seems the syndicate didn't hack into the user database as they went from ATM to ATM," he said.

"This means they did not touch anyone's account and directly withdrew money."

Kwan said the SIM card used likely contained fake information for it to access certain parts of the ATM software.

"As far as I know, the SIM card is a simple interface providing a small database into a system. It tells the machine that you are there, then it prompts you for a password as it doesn't store sensitive data electronically," said the computer enthusiast.

Infowatch – an international company that develops information software products and solution and experts in preventing data loss – gives Malay Mail an insight into hacking and automated teller machine theft.

BELOW ARE EXCERPTS FROM THE INTERVIEW WITH INFOWATCH INTERNATIONAL SALES DIRECTOR VADIM KUSNETSOV:

SYSTEM FAILURE

1) HOW HAS HACKING DEVELOPED OVER THE YEARS?

HACKING HAS GONE FROM THE PRANKS OF THE EARLY DAYS TO BIG BUSINESS. WHILE THIS SERIES OF ATM HEISTS USING A VIRUS MAY SEEM EXTREME AND DARING, IT CANNOT BE COMPARED TO THE LOSSES THAT CAN BE RACKED UP VIA BREACHES OR LEAKS FROM WITHIN AN ENTERPRISE'S INTERNAL NETWORK SECURITY.

IN THOSE CASES, LOSSES CAN HEAD INTO HUNDREDS OF MILLION DOLLARS. MOST OFTEN THESE DATA LEAKS REMAIN UNKNOWN TO PUBLIC. ON THE CONTRARY, ATM HACKING IS VISIBLE, AND DIRECTLY AFFECTS PEOPLE AND THEIR POCKETS. IN THE CASE OF MALAYSIAN BANKS HIT, IT COULD BE A CASE OF A TARGETED ATTACK, WHICH IS ONE OF THE MAIN SECURITY THREATS TODAY.

WORLD BUSINESSES LOSE BILLIONS YEARLY FROM THEFT OF FUNDS WITH HELP OF INFORMATION TECHNOLOGY. BUT THE PROBLEM OF TARGETED ATTACKS IS NOW A MAJOR CONCERN.

2) CAN IT BE EASILY DONE WITH CHEAP GADGETS? IN THE RECENT HACKINGS, A MOBILE PHONE SIM WAS USED.

IT IS EASY, BUT RISKY. ALL MAJOR DATA LEAKS ARE DONE NOT BY MOBILE PHONE, BUT USING CORPORATE OR WEBMAILING OF SENSITIVE DATA OUTSIDE CORPORATE NETWORKS WHICH ARE UNPROTECTED BY DATA LOSS PREVENTION SOLUTIONS. STILL, MOBILE DEVICES NOW HAVE ALL THE SAME FUNCTIONALITY AS COMPUTERS AND SO CAN BE USED BY MALEFACTORS FOR THEIR MALICIOUS ACTIONS. THAT'S WHY FINANCIAL ORGANISATIONS SHOULD IMPLEMENT MODERN ADVANCED SECURITY SYSTEMS TO PROTECT THEIR FUNDS FROM HACKERS, INSIDERS AND OTHER MALEFACTORS.

3) HOW DO HACKERS GAIN EASY ACCESS?

EVEN THE MOST ADVANCED SECURITY SOLUTION CANNOT GUARANTEE 100% EFFICIENCY. THAT DOESN'T MEAN WE DO NOT NEED PROTECTION. SECURITY MUST BE MULTILAYERED AND COMPLEX TO PROTECT THE ORGANISATION THREATS. THAT WILL MAKE THE ACTIONS OF MALEFACTORS EXTREMELY DIFFICULT.