Chip and pin terminals shown to harvest customer info

31 July 2012, by Nancy Owano

(Phys.org) -- For all customers, merchants and restaurant owners making use of card readers for transactions, well, this is not the best of news. Experts have found a security flaw in chip and PIN terminals that allows thieves to download customers' card details. According to a UK-based security firm, MWR InfoSecurity, hackers can steal details from chip and PIN machines. MWR was able to prove how easily it can be done. According to a report on Sunday, thousands of credit and debit card readers, such as those sitting in shops and restaurants, will need to be reprogrammed following revelations that they can be hacked into and used to steal cardholders' details.

For criminals, lifting info would be all in a day's work, enjoying a daily catch of many cardholder details. MWR performed a test to show how this can work. Criminals can load their fake cards with malicious software. The card can be made to look like any credit or debit card. A criminal could use it in any retail shop or eating establishment.

Using second-hand terminals that they purchased on eBay, MWR accessed the computer code on which the terminals run. They used this code to program a fake chip and PIN card, loading the chip with malicious software that is capable of reprogramming the reader. Once used in shops, the fakes - made to look like a normal credit or debit card - infect the card readers. Once the malicious card transfers its software to the reader, it begins storing details of all subsequent cards inserted. The criminal can then return later and use a second card to download this data, which by then has all the card details and PINs.

The team purchased three point-of-sale terminals on eBay, one of which is a popular model that comes with a touchscreen and a feature for capturing cardholder signatures. The other two have a port for inserting chip-and-PIN cards, as well as a mag stripe reader.

As a result of this feat, thousands of terminals need reprogramming, according to reports. VeriFone, which makes most of the UK's terminals, confirmed that MWR was on to something and the terminal maker said it is working on an "expedited" update after learning of the hacking vulnerability.

"We have confirmed that MWR implemented a sophisticated scenario that is technically feasible on some older systems," said the company."VeriFone has developed a software update to resolve this issue in deployed systems and has already submitted the code for testing and approval on an expedited basis." The company said it will provide the software update "to all impacted parries" to implement.

Security watchers see the significance in the fact that the chip could be loaded with malicious software capable of reprogramming the reader, leaving the system open to data theft.

Law enforcement agents have discovered that

account numbers and PINs are being sold in bulk on carding websites, as the Internet has become an easy conduit to leverage stolen credit card, bank account, and other personal identification information of victims globally.

At the recent Black Hat 2012 meeting, MWR InfoSecurity also demonstrated how to attack point of sale terminals that use a microchip and PIN identification system with a specially prepared chip-based credit card. The security company first showed how a bogus chip credit card could be used to pay for an item and obtain a receipt for a valid transaction without the payment ever being processed. The second display from MWR was the terminal reader demo, showing how a card with malware can harvest all the card numbers and PINs from previous users of the terminal.

More information:
www.channel4.com/news/credit-c … e-hacked-for-details

APA citation: Chip and pin terminals shown to harvest customer info (2012, July 31) retrieved 29 November 2021 from https://phys.org/news/2012-07-chip-pin-terminals-shown-harvest.html