Opening a dangerous malware store can clean up your bank account on the black web

Usually you have to exploit vulnerabilities in software or hardware to hack ATM accounts but now things are much simpler, just buying a malware will grab millions right away.

Usually you have to exploit vulnerabilities in software or hardware to hack ATM accounts but now things are much simpler, just buying a malware will grab millions right away.

Hack is becoming easier than ever. On a hacking forum, hackers are selling ready-to-use ATM malware, anyone can buy it for about $ 5000.

The post contains descriptive information and instructions for the detailed use of this malware toolkit, designed to target different types of ATM cards that only need to connect to USB ports and run malware, with the help of the API. do not interact with ATM users as well as their data.

Malware does not directly affect users but will trick ATM 'to vomit' without authentication. The guide also mentions the ATM malware Tyup has been used to attack jackpot and earn millions from ATM poisoning in Europe and other regions.

Malware called Cutlet Maker was discovered by researchers at kaspersky Lab when viewing a forum post. Cutlet Maker was sold on AlphaBay Dark Web in May 2017 but after being dropped in mid-July, the author opened a private website called ATMjackpot. The price on ATMjackpot is $ 1500 bitcoin.

The ATMjackpot group also posted 4 videos showing how to gain access to the ATM USB port, connect necessary hardware, run malware and force ATMs to waste money.

How does Cutlet Maker work?

The list of tools in the toolkit includes:

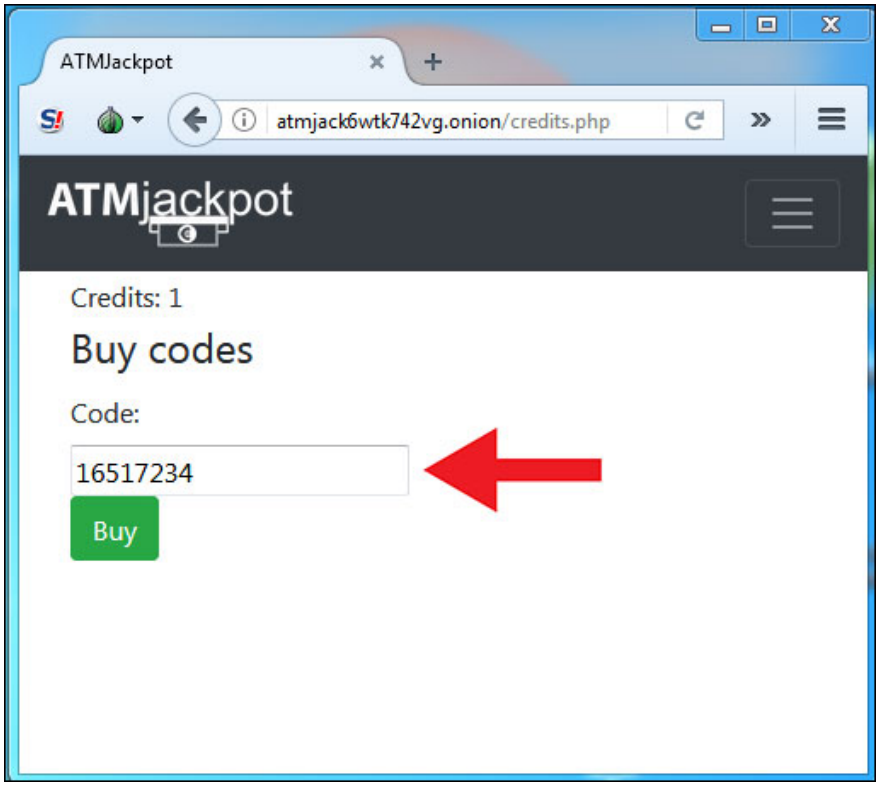
1. Cutlet Maker - main malware
2. Stimulator - the application takes money from ATM trees
3. c0decalc - terminal application for creating passwords for malware (in the old version when selling on AlphaBay)

In order to work, the application needs a specific library, which is part of the exclusive ATM API and controls the ATM tree giving out money. That means hackers use 'legitimate proprietary libraries and a code to get money from ATMs'.

Approaching the ATM, the attacker connected via USB, connecting the wireless keyboard, mouse and portable storage device containing malware. When connecting and running Cutlet Maker, malware displays the code at the bottom of the window.

The code used to retrieve the malware password

If you get the code, you must access ATMjackpot from the phone with Tor installed and enter the code to get the password to unlock Cutlet Maker application. Then use the Simulator application to query account balances on trees and receive money.



Enter the code successfully and start taking money from the ATM tree

The old malware version sold on AlphaBay uses c0decalc file but in the new version, it seems that ATMjackpot port has replaced this file.

Kaspersky said that ATM is protected by Kaspersky Embedded Systems Security (KESS) that will block the malware.

You finished reading the article "**Opening a dangerous malware store can clean up your bank account on the black web**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
