ATM malware is being sold on Darknet market

By Konstantin Zykov

Published: 2017-10-17 · Archived: 2026-04-05 14:06:38 UTC

Disclaimer and warning

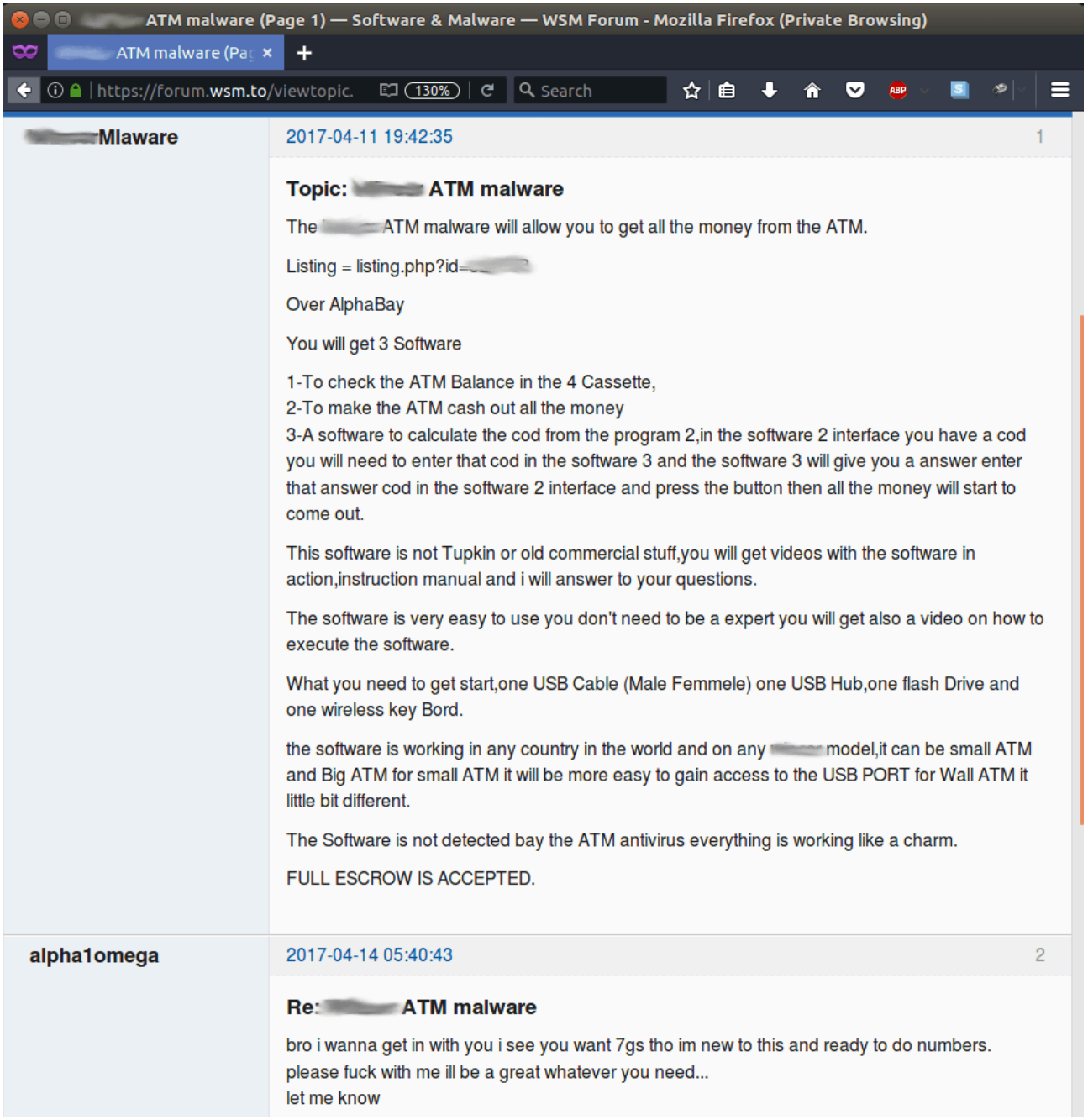
ATM systems appear to be very secure, but the money can be accessed fairly easily if you know what you are doing. Criminals are exploiting hardware and software vulnerabilities to interact with ATMs, meaning they need to be made more secure. This can be achieved with the help of additional security software, properly configured to stop the execution of non-allowlisted programs on ATMs.

Worryingly, it is very easy to find detailed manuals of ATM malware. Anybody can simply buy them for around 5000 USD on darknet markets.

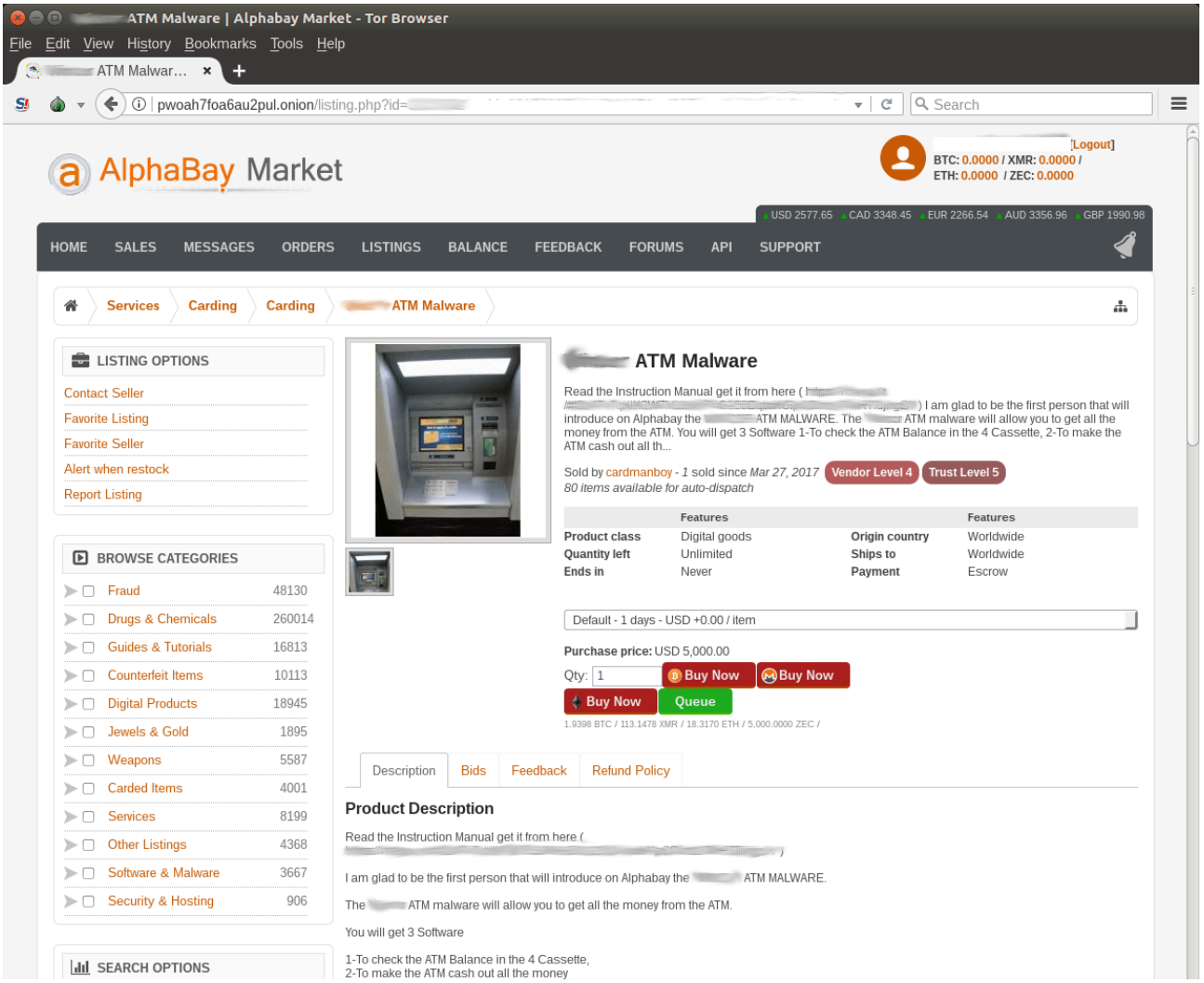
More information about CutletMaker ATM malware is available to customers of Kaspersky Intelligence Reporting Service. Contact: intelreports@kaspersky.com

Introduction

In May 2017, Kaspersky Lab researchers discovered a forum post advertising ATM malware that was targeting specific vendor ATMs. The forum contained a short description of a crimeware kit designed to empty ATMs with the help of a vendor specific API, without interacting with ATM users and their data. The post links to an offer that was initially published on the AlphaBay Darknet marketplace, which was recently taken down by the FBI.

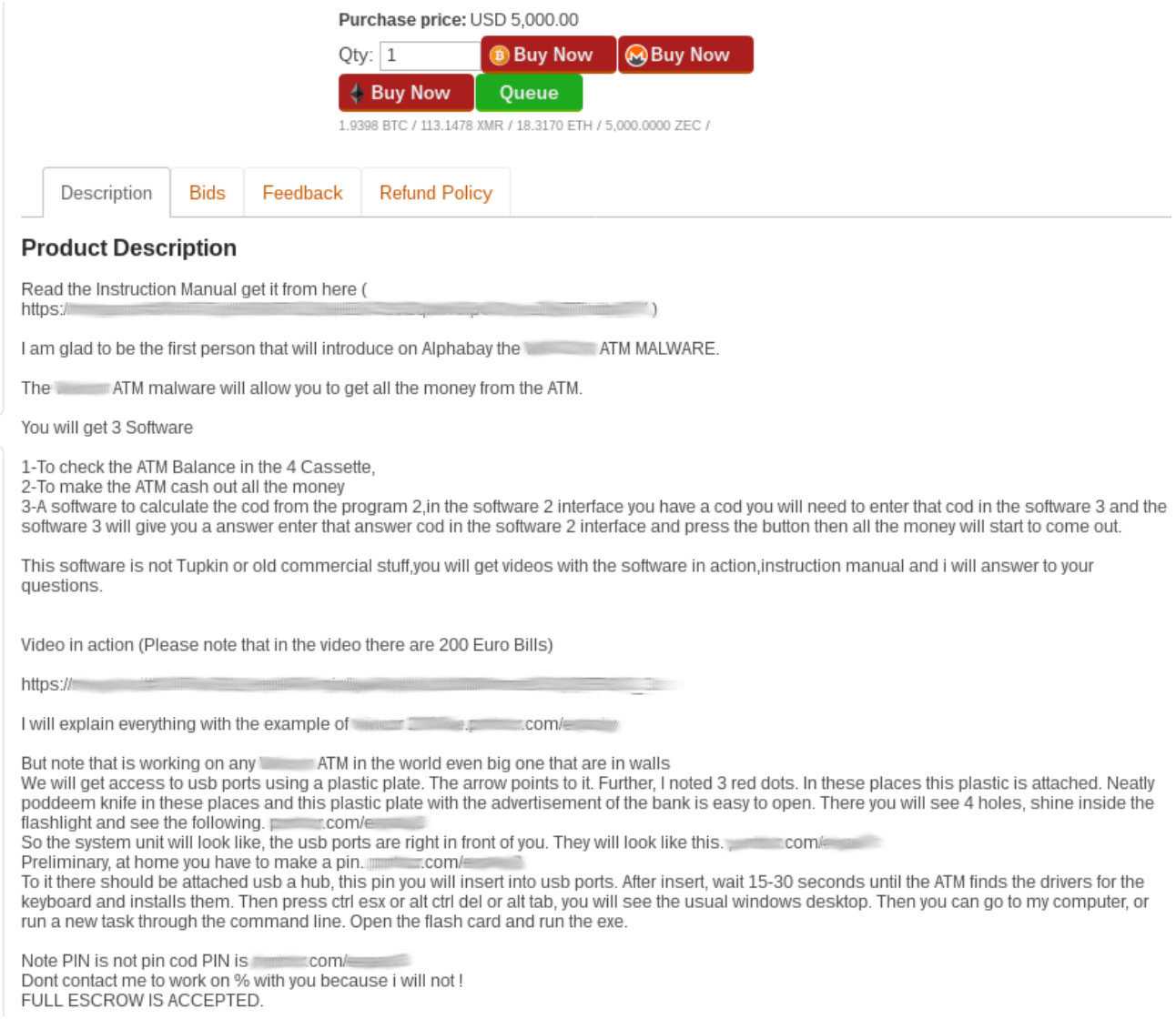


Advertisement post



An offer post on AlphaBay market

The price of the kit was 5000 USD at the time of research. The AlphaBay description includes details such as the required equipment, targeted ATMs models, as well as tips and tricks for the malware's operation. And part of a detailed manual for the toolkit was also provided.



Screenshot of a description on AlphaBay market

Previously described ATM malware Tyupkin was also mentioned in this text. The manual "*Wall ATM Read Me.txt*" was distributed as a plain text file, written in poor English and with bad text formatting. The use of slang and grammatical mistakes suggests that this text was most likely written by a native Russian-speaker.

First Of all let me tell you to not panic and Read This several time,the software is very easy to use but i will explain you all the necesare steps and it will look complicate when you first Read,it is working on any [redacted] ATM MODEL !!!

What you have here?

1-Software that will alow you to Cashout the Money From the ATM (Software Name cm17F)
2-Software that will alow you to see how much money is inside the ATM,how much bill each casete have and in wich casete the big bills are (Software Name Stimulator22)
3-[redacted] will help you to generate a answar cod that you will need to place it inside the CM17F interface)

What To buy -

1-Wirlles KeyBord with Tuch Pad intergrate.
2-USB HUB
3-USB Stik 1gb (Need to new key not uset)
4-USB Male femmle 50Cm Cable
5-USB Adaptator like this one (http://www.[redacted]/details /usb_adapter_usb_a_female_to_b_female.html)
6-Windows 7 Laptop Or Tablet.
7-one Drill

I advice you to train your self at your place,in order for you to train you will need a windows xp operatin sistem on a Pc/Laptop;if you dont have any xp then simplle google VitualBox(Youtube how to install it Youtube= How to install VirtualBox,Youtube = how to install Windows xp ISO inside VirtualBox)then Grab a ISO Windows XP from Google and install it in the VirtualBox,

Apart of a manual with text formatting applied

The manual provides a detailed picture, though only a fragment of the complete manual is being shown. There is a description for each step of the dispense process:

Prepare an all tools, all the programs should be placed on a flash disk.
Tools are wireless keyboard, usb hub, usb cable, usb adapter usb a female to b female, Windows 7 laptop or a tablet (to run code generator) and a drill.
Find an appropriate ATM
Open ATM door and plug into USB port.
Execute Stimulator to see full information of all the ATM cassettes.
Execute CUTLET MAKER to get it is code.
Execute password generator on a tablet or on a laptop and paste CUTLET MAKER code to it, put the result password to CUTLET MAKER.
Dispense the money from chosen cassette.

The manual provides usage descriptions for all parts of the toolset. The list of crimeware from the kit consists of *CUTLET MAKER* ATM malware, the primary element, with a password generator included and a *Stimulator* – an application to gather cash cassette statuses of a target ATM. The crimeware kit is a collection of programs possibly written by different authors, though *CUTLET MAKER* and *Stimulator* were protected in the same way, *c0decalc* is a simple terminal-based application without any protection at all.

Delicious cutlet ingredients: CUTLET MAKER, c0decalc and Stimulator

The first sample was named “CUTLET MAKER” by its authors and has been designed to operate the cash dispense process on specific vendor ATMs.

To answer the question of how a cook from the CUTLET MAKER interface and cutlets relate to stealing money from ATMs, we must explain the meaning of the word “*Cutlet*“. Originally, it means a meat dish, but as a Russian slang term “*Cutlet*” (котлета) means “a bundle of money”, suggesting that the criminals behind the malware might be native Russian speakers.

The “Cutlet Maker” malware functionality suggests that two people are supposed to be involved in the theft – the roles are called “drop” and “drop master”. Access to the dispense mechanism of CUTLET MAKER is password protected. Though there could be just one person with the *c0decalc* application needed to generate a password. Either network or physical access to an ATM is required to enter the code in the application text area and also to interact with the user interface.

Stimulator was possibly developed by the same authors. Its purpose is to retrieve and show the status information of specific vendor ATM cash cassettes (such as currency, value and the amount of notes).

CUTLET MAKER and c0decalc

CUTLET MAKER is the main module responsible for dispensing money from the ATM. The sample analysed in this research has the MD5 checksum “fac356509a156a8f11ce69f149198108” and the compilation timestamp Sat Jul 30 20:17:08 2016 UTC.

The program is written in Delphi and was packed with VMProtect, however it is possible that multiple packers might have been used.

Different versions of the main component were found while researching this toolset. The first known submission of the first version sent to a public multiscanner service took place on June 22nd 2016. All submissions discovered by Kaspersky Lab were performed from different countries, with Ukraine being the chronological first country of origin.

Known CUTLET MAKER filenames (according to public multiscanner service information):

cm.vmp.exe
cm15.vmp.exe
cm16F.exe
cm17F.exe

The following version information was captured from the application's window caption, followed after a "*CUTLET MAKER*" name. Known versions at the time of research were:

1.0
1.02
1.0 F

The assumed development period is from 2016-06-22 to 2016-08-18, according to the first submission date of the earliest version and the last submission date of the latest version at the time of writing. The application requires a special library to operate, which is part of a proprietary ATM API, controlling the cash dispenser unit.

With all the dependencies in place, the interface shows a code.

CUTLET MAKER challenge code marked with red rectangle

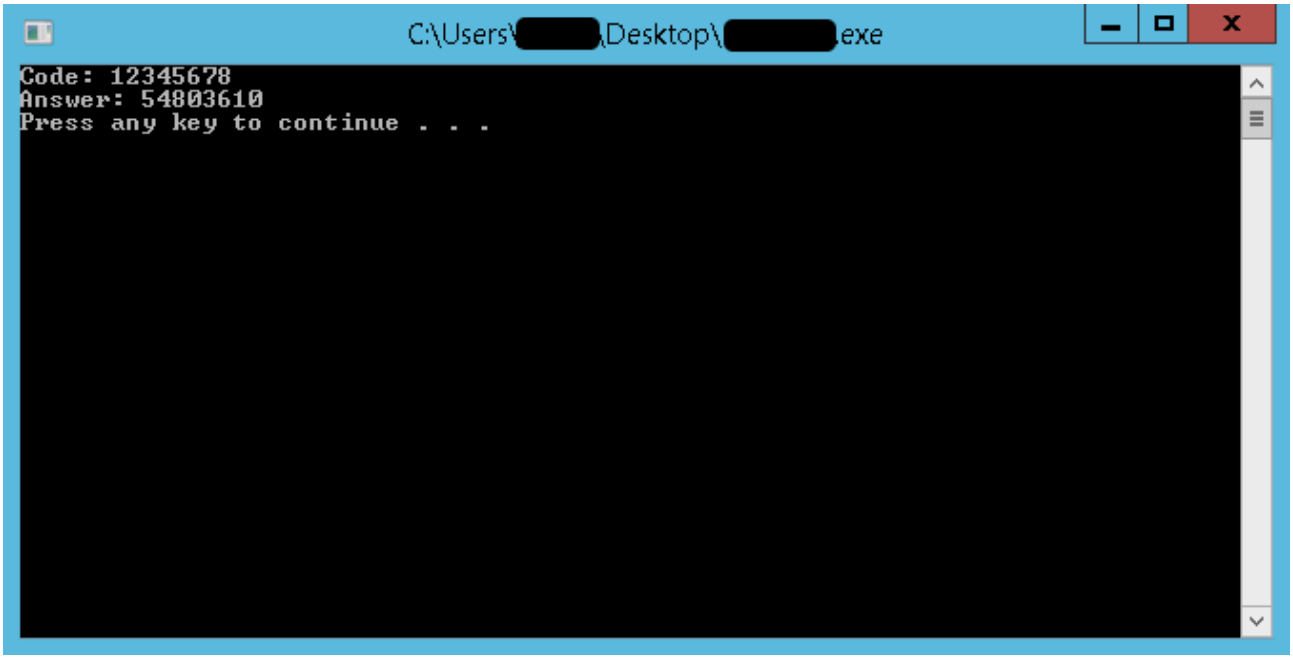
In order to unlock the application, a password from *c0decalc* generator needs to be entered, thereby answering the given challenge code. If the password is incorrect, the interface won't react to any further input.

Each "*CHECK HEAT*" and "*start cooking!*" button corresponds to a specific ATM cash cassette. Buttons labeled "*CHECK HEAT*" dispense one note, "*start cooking!*" dispenses 50 "cutlets" with 60 notes each. The "*Stop!*" button stops an ongoing "*start cooking!*" process. "*Reset*" is intended to reset the dispense process.

c0decalc a password generator for CUTLET MAKER

This tool is an unprotected command line application, written in Visual C. The purpose of this application is to generate a password for CUTLET MAKER's graphical interface.

The compilation timestamp for this specific sample is Sun Nov 13 11:35:25 2016 UTC and was first uploaded to a public multiscanner service on December 7th 2016.



Example output for "12345678" input

Kaspersky Lab researchers checked the algorithm during the analysis and found "*CUTLET MAKER*" working with the passwords generated by "c0decalc".

Stimulator

The *Stimulator* sample analysed in this research has the MD5 hash *"27640bb7908ca7303d13d50c14ccf669"*. This sample is also written in Delphi and packed the same way as "CUTLET MAKER". The compilation timestamp is Sat Jul 16 18:34:47 2016 UTC.

The application is designed to work on specific vendor ATMs and also uses proprietary API calls.

Some additional symbols were found in the memory dump of a "Stimulator" process, pointing to an interesting part of the application. After execution and pressing the "STIMULATE ME!" button, the proprietary API function is used to fetch an ATM's cassette status. The following cassette state results are used:

1CUR
2CUR
3CUR
4CUR
1VAL
2VAL
3VAL
4VAL
1NDV
2NDV
3NDV
4NDV
1ACT
2ACT
3ACT
4ACT

Each preceding number is mapped to an ATM cassette. The three character states are interpreted as follows:

nCUR	cassette **n** currency (like “USD”, “RUB”)
nVAL	cassette **n** note value (like 00000005, 00000020)
nACT	cassette **n** counter for specific notes in a cassette (value from 0 to 3000)
nNDV	number of notes in the ATM for cassette **n** (value from 0 to 3000)

The result of "STIMULATE ME!" button press in proper environment

Each column, shown in the picture above, describes the state of one corresponding ATM cassette.

The background picture used in the application interface turns out to be quite unique, the original photo was posted on a DIY blog:

https://www.oldtownhome.com/2011/8/4/Knock-Knock-Whos-There-Merv-the-Perv/

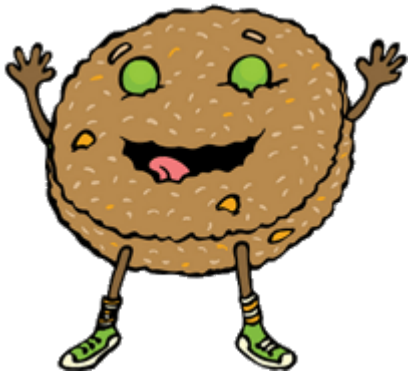
Original picture as used in "Stimulator" application (photo by Alex Santantonio)

Conclusion

This type of malware does not affect bank customers directly, it is intended for the theft of cash from specific vendor ATMs. CUTLET MAKER and Stimulator show how criminals are using legitimate proprietary libraries and a small piece of code to dispense money from an ATM. Examples of appropriate countermeasures against such attacks include default-deny policies and device control. The first measure prevents criminals from running their own code on the ATM's internal PC. It is likely that ATMs in these attacks were infected through physical access to the PC, which means criminals were using USB drives to install malware onto the machine. In such a

case, device control software would prevent them from connecting new devices, such as USB sticks. Kaspersky Embedded Systems Security will help to extend the security level of ATMs.

Kaspersky Lab products detects this threats as Backdoor.Win32.ATMletcut, Backdoor.Win32.ATMulator, Trojan.Win32.Agent.ikmo



Source: https://securelist.com/atm-malware-is-being-sold-on-darknet-market/81871/