ATM robber WinPot: a slot machine instead of cutlets

securelist.com/atm-robber-winpot/89611/

Malware descriptions

Malware descriptions

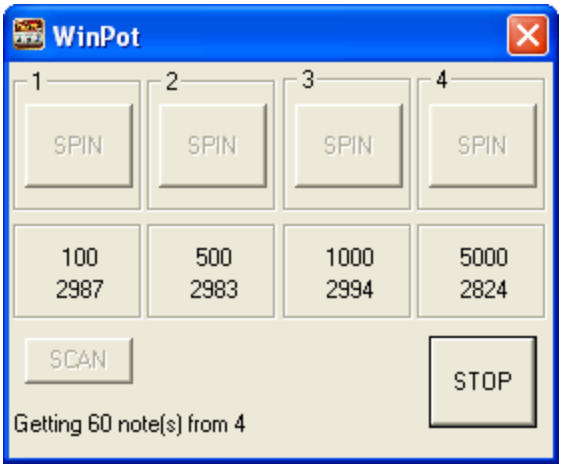
19 Feb 2019

minute read

Authors

Expert Konstantin Zykov

Automation of all kinds is there to help people with their routine work, make it faster and simpler. Although ATM fraud is a very peculiar sort of work, some cybercriminals spend a lot of effort to automate it. In March 2018, we came across a fairly simple but effective piece of malware named WinPot. It was created to make ATMs by a popular ATM vendor to automatically dispense all cash from their most valuable cassettes. We called it ATMPot.



Example of WinPot interface – dispensing in action

The criminals had clearly spent some time on the interface to make it look like that of a slot machine. Likely as a reference to the popular term ATM-jackpotting, which refers to techniques designed to empty ATMs. In the WinPot case, each cassette has a reel of its own numbered 1 to 4 (4 is the max number of cash-out cassettes in an ATM) and a button labeled SPIN. As soon as you press the SPIN button (in our case it is greyed out because we are actually dispensing cash), the ATM starts dispensing cash from the corresponding cassette. Down from the SPIN button there is information about the cassette (bank note value and the number of bank notes in the cassette). The SCAN button rescans the ATM and updates the numbers under the SLOT button, while the STOP button stops the dispensing in progress.

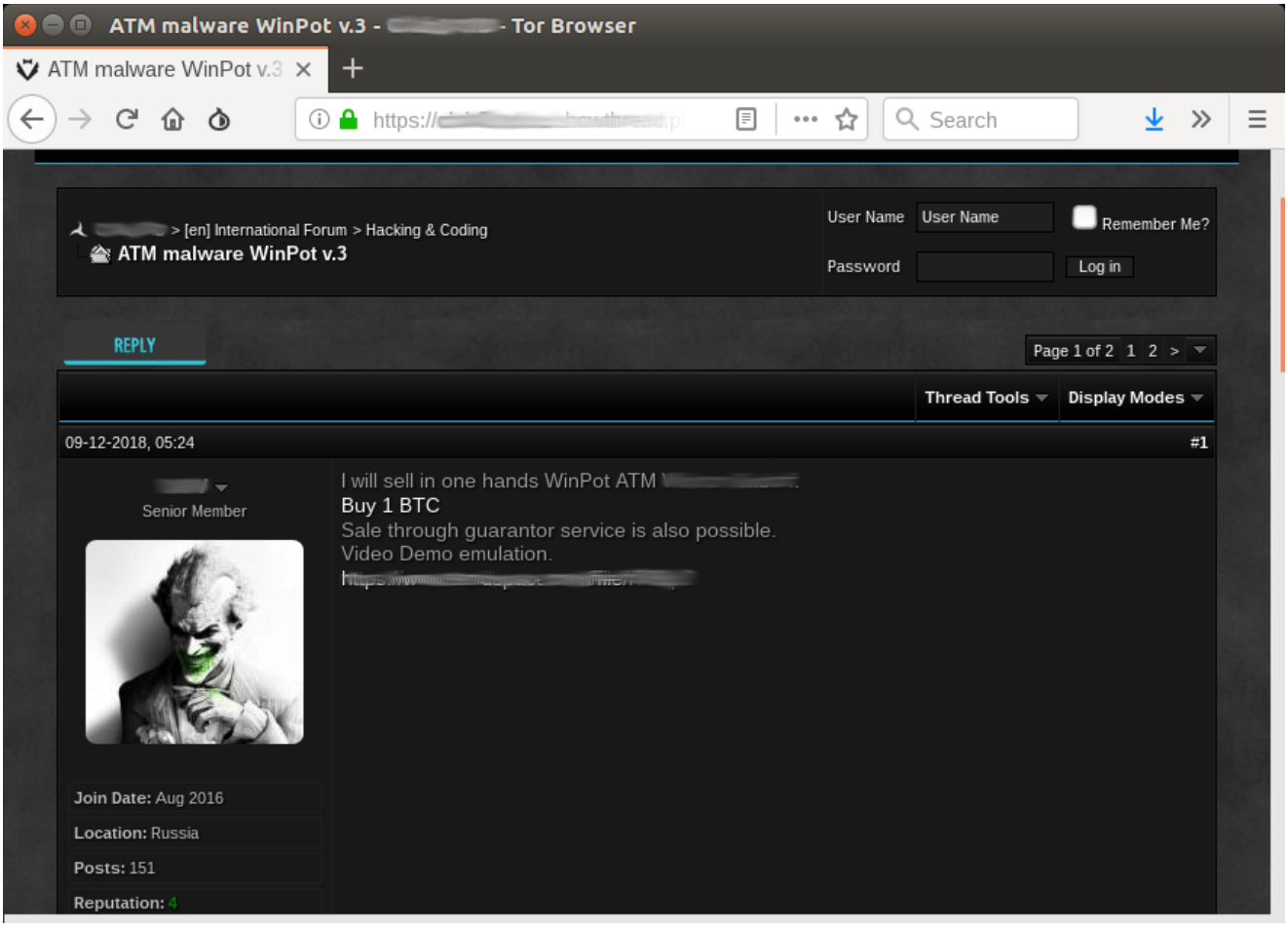
We found WinPot to be an amusing and interesting ATM malware family, so we decided to keep a close eye on it.

Over the course of time, new samples popped up, each one with minor modifications. For example, a changed packer (like Yoda and UPX) or updated time period during which the malware was programmed to work (e.g, during March). If system time does not fall in with the preset period, WinPot silently stops operating without showing its interface.

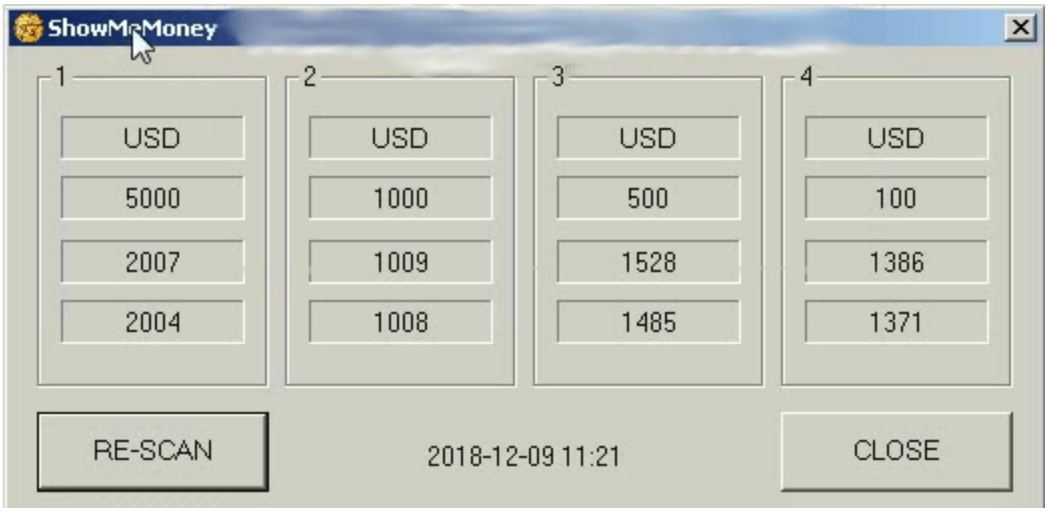
The number of samples we had found was also reflected in the European Fraud Update published in the summer of 2018. It has a few lines about WinPot:

> *"ATM malware and logical security attacks were reported by nine countries. Five of the countries reported ATM related malware. In addition to Cutlet Maker (used for ATM cash-out) a new variant called WinPot has been reported…"*

Same as Cutler Maker, WinPot is available on the (Dark)net for approximately 500 – 1000 USD depending on offer.



One of the sellers offers WinPot v.3 together with a demo video depicting the “new” malware version along with a still unidentified program with the caption “ShowMeMoney”. Its looks and mechanics seem quite similar to those of the Stimulator from the CutletMaker story.



Unidentified Stimulator-like sample from demo video

Winpot v3 sample from demo video

Due to the nature of ATM cash-out malware, its core functionality won't change much. But criminals do encounter problems, so they invent modifications:

- To trick the ATM security systems (using protectors or other ways to make each new sample unique);
- To overcome potential ATM limitations (like maximum notes per dispense);
- To find ways to keep the money mules from abusing their malware;
- To improve the interface and error-handling routines.

We thus expect to see more modifications of the existing ATM malware. The preferred way of protecting the ATM from this sort of threat is to have device control and process allowlisting software running on it. The former will block the USB path of implanting the malware directly into the ATM PC, while the latter will prevent execution of unauthorized software on it. Kaspersky Embedded Systems Security will further help to improve the security level of the ATMs.

Kaspersky Lab products detect WinPot and its modifications as Backdoor.Win32.ATMPot.gen

Sample MD5:
821e593e80c598883433da88a5431e9d

- ATM
- Financial malware
- Malware Descriptions

Authors

Expert Konstantin Zykov

ATM robber WinPot: a slot machine instead of cutlets

Your email address will not be published. Required fields are marked *

GReAT webinars

13 May 2021, 1:00pm

GReAT Ideas. Balalaika Edition

26 Feb 2021, 12:00pm
17 Jun 2020, 1:00pm
26 Aug 2020, 2:00pm
22 Jul 2020, 2:00pm
From the same authors

CactusPete APT group's updated Bisonal backdoor

How we developed our simple Harbour decompiler

Hello! My name is Dtrack

Criminals, ATMs and a cup of coffee

ATM malware is being sold on Darknet market

Subscribe to our weekly e-mails

The hottest research right in your inbox