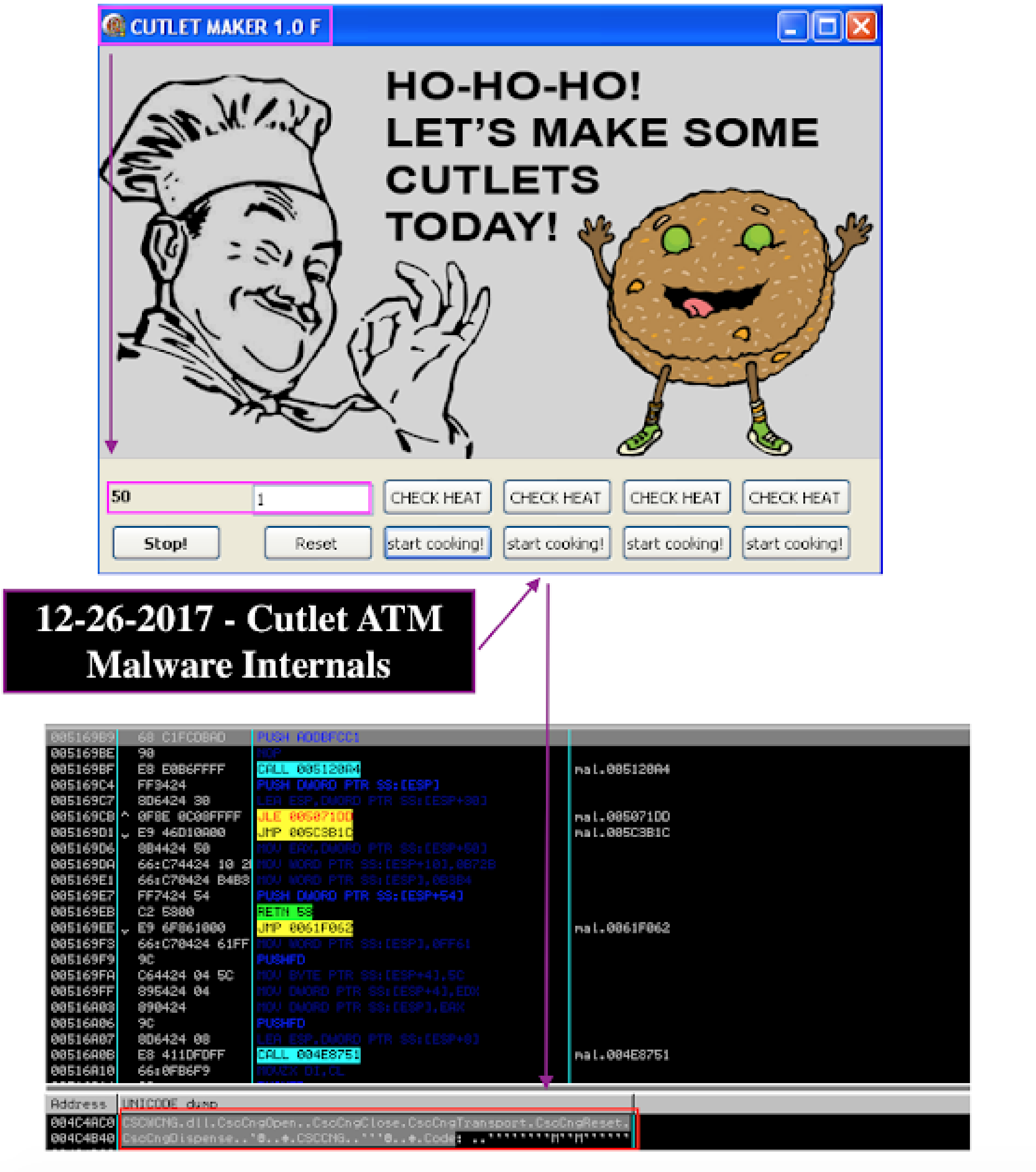
Let's Learn: Cutlet ATM Malware Internals

vkremez.com/2017/12/lets-learn-cutlet-atm-malware-internals.html

Goal: Analyze the internals of the prolific Cutlet ATM malware (VMProtect).
Sample: fac356509a156a8f11ce69f149198108



```
005169B9     68 C1FCD8AD       PUSH AD0BFCC1
005169BE     90                NOP
005169BF     E8 E0B6FFFF       CALL 005120A4                  mal.005120A4
005169C4     FF3424            PUSH DWORD PTR SS:[ESP]
005169C7     8D6424 30         LEA ESP,DWORD PTR SS:[ESP+30]
005169CB ^   0F8E 0C90FFFF     JLE 005071DD                   mal.005071DD
005169D1 ⌄   E9 46D10A00       JMP 005C3B1C                   mal.005C3B1C
005169D6     8B4424 50         MOV EAX,DWORD PTR SS:[ESP+50]
005169DA     66:C74424 10 2B   MOV WORD PTR SS:[ESP+10],0872B
005169E1     66:C70424 B4B8    MOV WORD PTR SS:[ESP],0B8B4
005169E7     FF7424 54         PUSH DWORD PTR SS:[ESP+54]
005169EB     C2 5800           RETN 58
005169EE ⌄   E9 6F861000       JMP 0061F062                   mal.0061F062
005169F3     66:C70424 61FF    MOV WORD PTR SS:[ESP],0FF61
005169F9     9C                PUSHFD
005169FA     C64424 04 5C      MOV BYTE PTR SS:[ESP+4],5C
005169FF     895424 04         MOV DWORD PTR SS:[ESP+4],EDX
00516A03     890424            MOV DWORD PTR SS:[ESP],EAX
00516A06     9C                PUSHFD
00516A07     8D6424 08         LEA ESP,DWORD PTR SS:[ESP+8]
00516A0B     E8 411DFDFF       CALL 004E8751                  mal.004E8751
00516A10     66:0FB6F9         MOVZX DI,CL

Address   UNICODE dump
004C4AC0  CSCWCNG.dll.CscCngOpen..CscCngClose.CscCngTransport.CscCngReset.
004C4B40  CscCngDispense..'@..+.CSCCNG..'''@..+.Code: ..''''''''H''H''''''
```

The blog outline is as follows:

I. Cutlet ATM Malware Background

II. Method of Operation

III. Threat Scope

IV. Cutlet ATM Malware Analysis

A. "start cooking" and "CHECK HEAT" functions

B. Cutlet's CSCWCNG API calls to dispense and transport cash

I. Cutlet ATM Malware Background

This Cutlet malware became one of the most widely used malware targeting Automated Teller Machines (ATMs). The ATM malware is available on the underground and leveraged by multiple actors in numerous ATM jackpotting heists. The malware targets one ATM vendor only, which is Diebold Nixdorf, formerly known as Wincor Nixdorf.

II. Method of Operation

The Cutlet malware is to be installed into individual ATMs, designed to make targeted machines dispense bills automatically via emptying cash-carrying cassettes. Typically, the ATM malware operation requires two individuals to be involved: one with the direct physical access to the ATM device connected to its backend USB port via a controlled PC; another one - remotely connected and able to release the key to dispense the cash to the first individual. By and large, the Cutlet malware, written in Borland Delphi, demonstrates its developer familiarity with the ATM-specific model proprietary API calls.

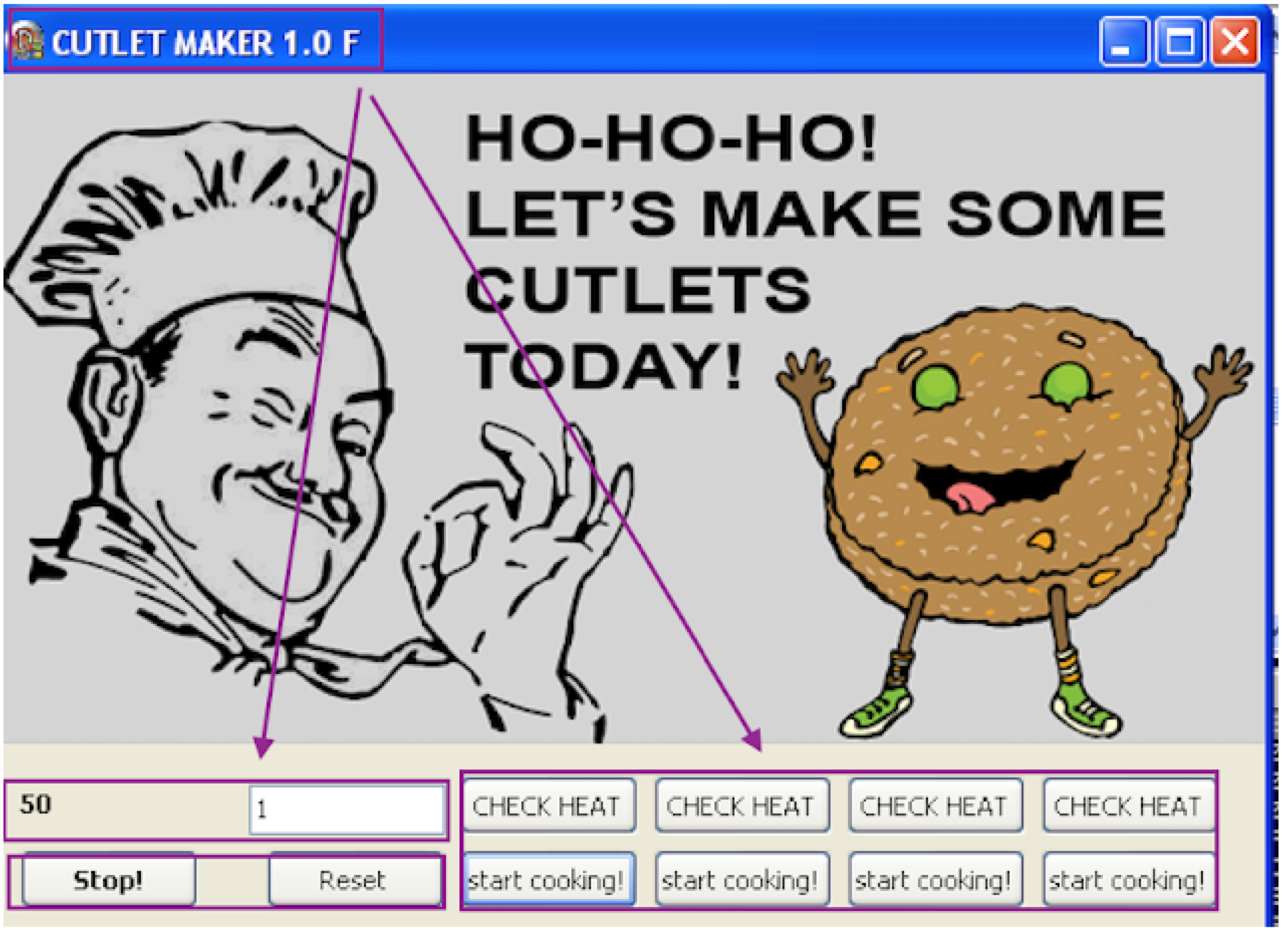
III. Threat Scope

Alongside with the infamous Tyupkin, Skimer, and Ripper ATM malware, the Cutlet ATM malware is a formidable threat on the ATM malware landscape. The surfaced reports generated a significant amount of attention to the malware from the industry(1)(2) and has sparked interest within the cybercriminal underground.

IV. Cutlet ATM Malware Analysis (version 1.0 F)

A. "start cooking" and "CHECK HEAT" functions

Essentially, while heavily packed, the core Cutlet ATM malware is rather trivial and targets only ATM manufacturer. The variant accepts the integer input from 1-9, which corresponds to ATM cassette slot number from 1-9.



<cassette slot number (integer) x 50 "CUTLETS" of banknotes count 60>

The main malware functions work as follows:

"start cooking!" -> Dispense 50 "CUTLETS" of banknotes count 60

"**CHECK HEAT"** -> Dispense 1 "CUTLET"

"Reset" -> Reset the cash dispensing process

"Stop!" -> Terminates the cash "cooking" process

B. ATM's CSCWCNG API calls to dispense and transport cash

The malware operates leveraging the Nixdorf proprietary CSCWCNG.DLL API calls to manipulate the machine as follows:

CscCngOpen -> Connect to the ATM cashout module called "CNG" and open the device

CscCngDispense -> Dispense cash function to tray

CscCngTransport -> Transport cash to the collection for pickup

V. Possible Mitigation

Monitoring, and reviewing any third-party applications that leverage the CSCWCNG API calls might assist with mitigating exposure to the Cutlet malware once it is already installed. It might be a good idea to whitelist only necessary applications to allow them to leverage these API calls.

VI. YARA RULE

```
rule crime_win32_atm_cutlet_unpacked_in_memory {
        meta:
                description = "Detects Cutlet ATM malware"
                author = "@VK_Intel"
                reference = "Detects the Cutlet ATM malware"
                date = "2017-12-26"
                hash = "fac356509a156a8f11ce69f149198108"

        strings:
                // DIEBOLD NIXDORF DLL ATM LIBRARY
                $dll = "CSCWCNG.dll" wide ascii

                // DLL PROCEDURES ASSOCIATED WITH CUTLET ATM
                $dll_proc1 = "CscCngClose" wide ascii
                $dll_proc2 = "CscCngTransport" wide ascii
                $dll_proc3 = "CscCngReset" wide ascii
                $dll_proc4 = "CscCngDispense" wide ascii
                $dll_proc5 = "CscCngOpen" wide ascii

                // CUTLET MALWARE STRINGS
                $str0 = "CSCCNG" wide ascii
                $str1 = "Code:" wide ascii
                $str2 = "Delphi" wide ascii

        condition:
                $dll and 4 of ($dll_proc*) and all of ($str*)
}
```

Update (01-01-2017): The observed Cutlet ATM malware variants are as follows:

CUTLET ATM MD5 Hash	Date First Seen	Version Seen	Filename First Seen	Country First Seen
fac356509a156a8f11ce69f149198108	2016-08-04 20:49:28	VERSION 1.0 F	cm.vmp.exe & cm17F.exe	Unknown & Moldova
ee1b05b6c3b51472c98f3640cdec278b	2017-11-12 12:56:22	VERSION 1.0 F	cm17F [1-1139].exe	Ukraine
dcf51a144816275fa4e3c3724731dca9	2016-08-18 14:54:11	VERSION 1.0 F	cm16F.exe	Sweden
3c3a3923e457467c39d0075f5c72a1b7	2017-11-13 08:15:35	VERSION 1.0 F	000538.exe	Ukraine

c97d2add446e75f88d65a9f9747e7ef7	2017-11-10 17:36:07	VERSION 1.0 F	Cutlet17.exe	Russia
27640bb7908ca7303d13d50c14ccf669	2016-08-04 19:48:31	SIMULATOR SOFT	Stimulator.exe	United States
277ced0b4094ce608bccce5acd24be88	2017-11-13 08:11:14	VERSION 1.0 F	000538 [1-3125].exe	Ukraine

The world heatmap of all uploaded variant is as follows displaying Ukraine as the top uploader of Cutlet ATM samples: