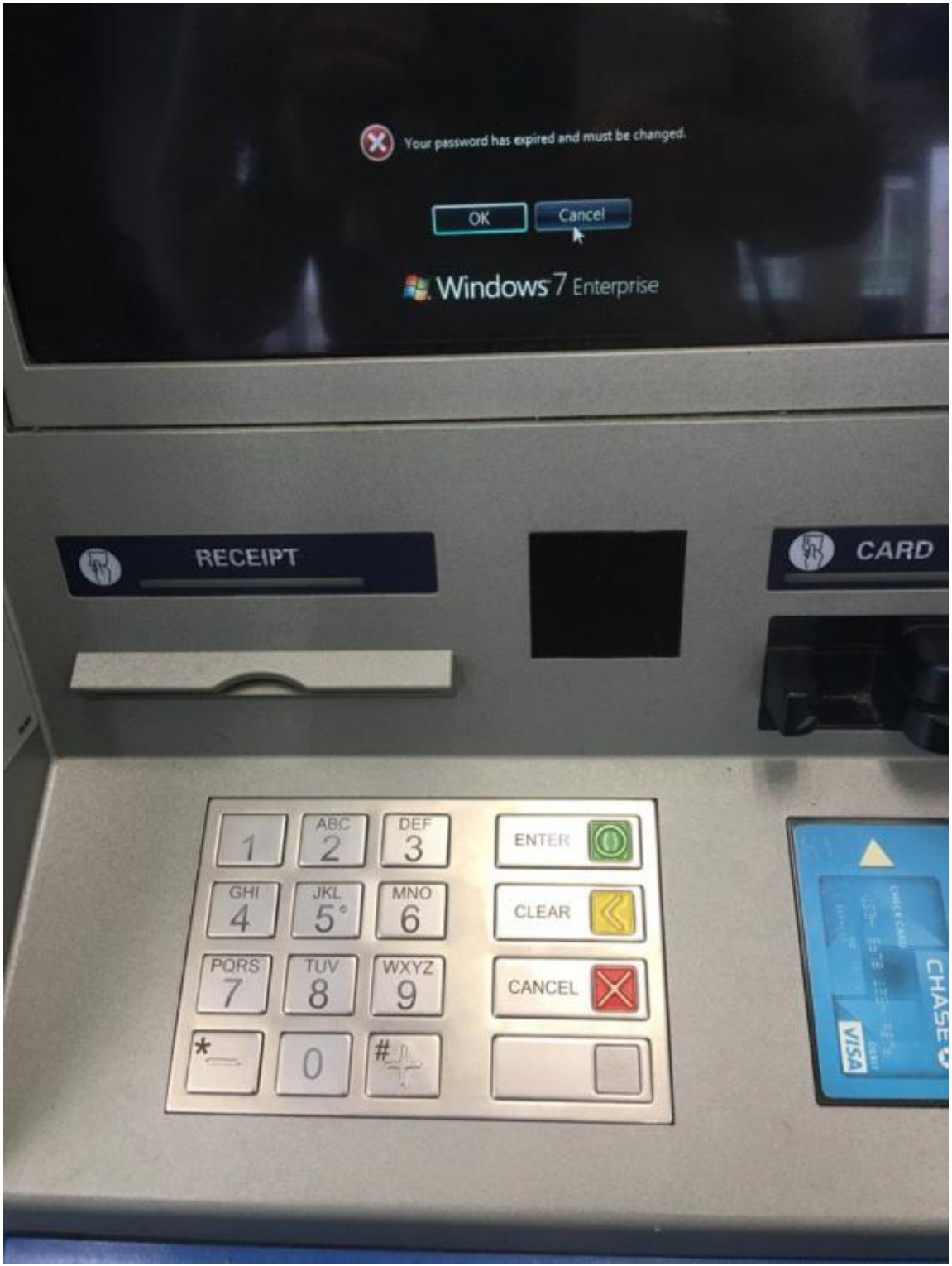
A new kind of malware?

David Sancho, Malware Researcher


LAST TRANSACTION CANCELLED
PLEASE TAKE YOUR CARD
Windows - Virtual Memory Minimum Too Low
Your system is low on virtual memory. Windows is increasing the size of your virtual memory paging file. During this process, memory requests for some applications may be denied. For more information, see Help.


Your password has expired and must be changed.
OK
Cancel
Windows 7 Enterprise
RECEIPT
CARD
1
ABC 2
DEF 3
GHI 4
JKL 5
MNO 6
PQRS 7
TUV 8
WXYZ 9
*
0
#
ENTER
CLEAR
CANCEL
VISA

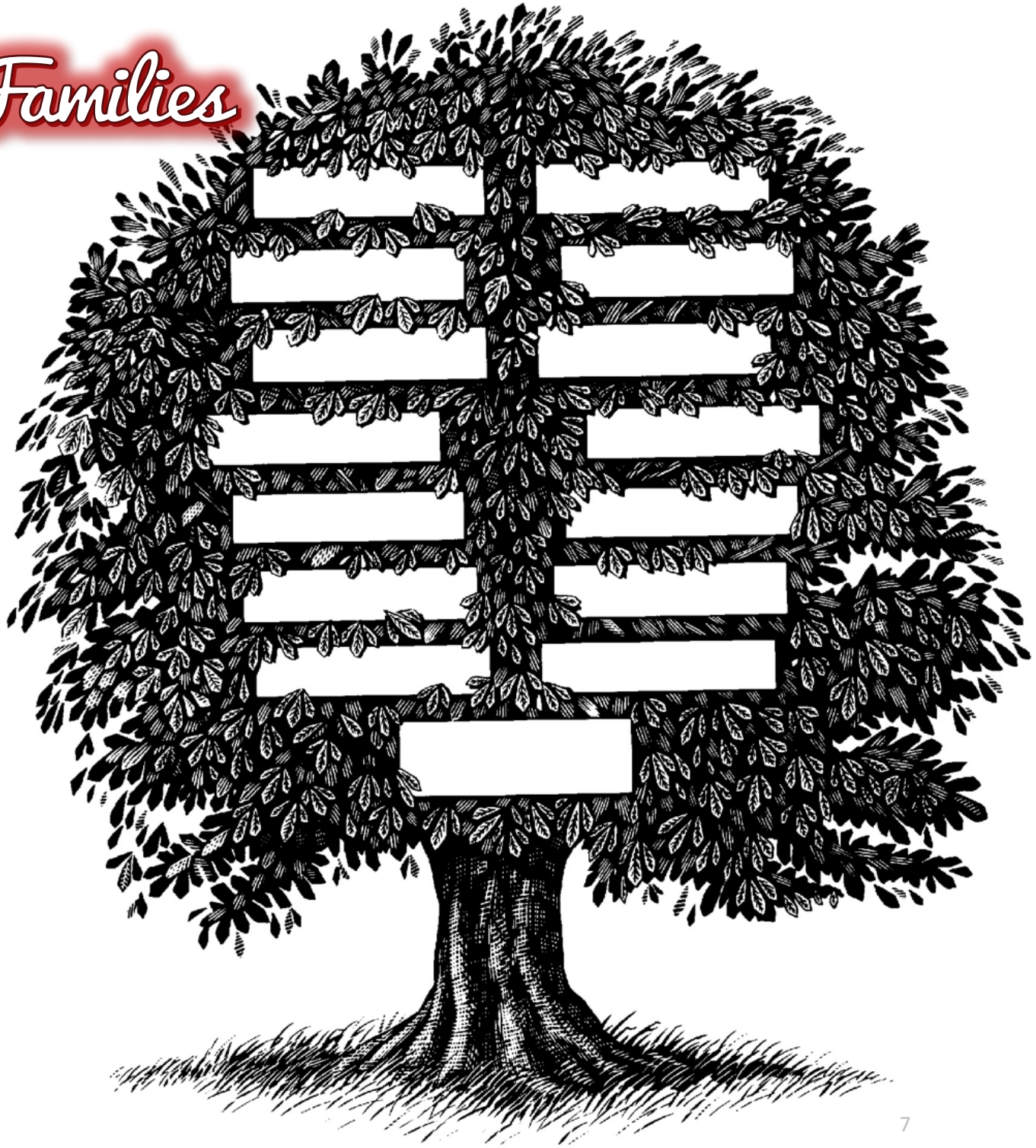
TREND MICRO


Why now?


The way in...

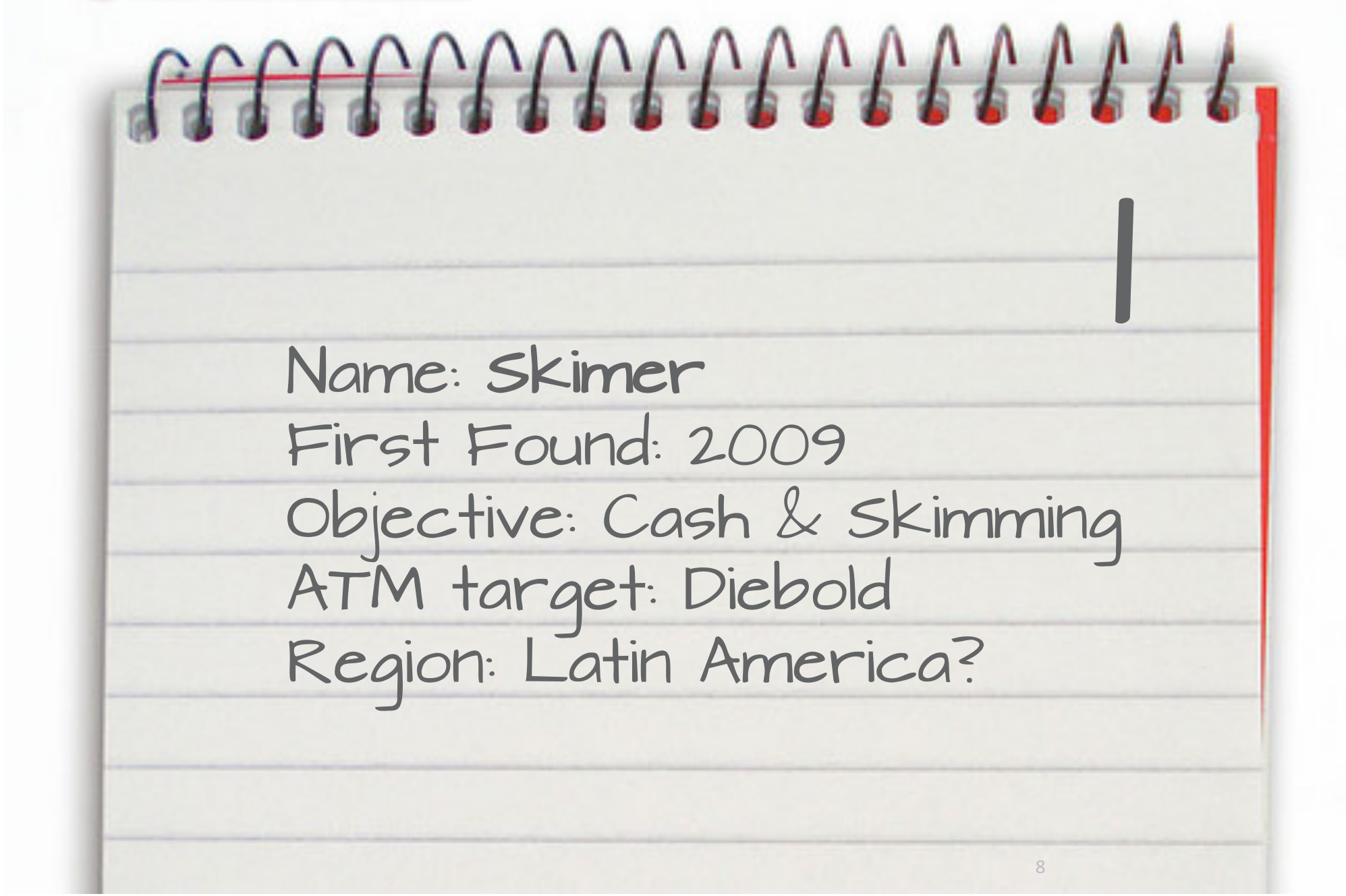

But what do crooks want?
BAR
BAR
7
7
7

The Families



TREND MICRO

The attacks...



Name: Skimer
First Found: 2009
Objective: Cash & Skimming
ATM target: Diebold
Region: Latin America?

The attacks...

2

Name: Ploutus
First Found: 2013
Objective: Cash
ATM target: NCR
Region: Latin America

The attacks...

3

Name: GreenDispenser
First Found: 2015
Objective: Cash
ATM target: Wincor/Nixdorf
Region: Latin America

The attacks...

4

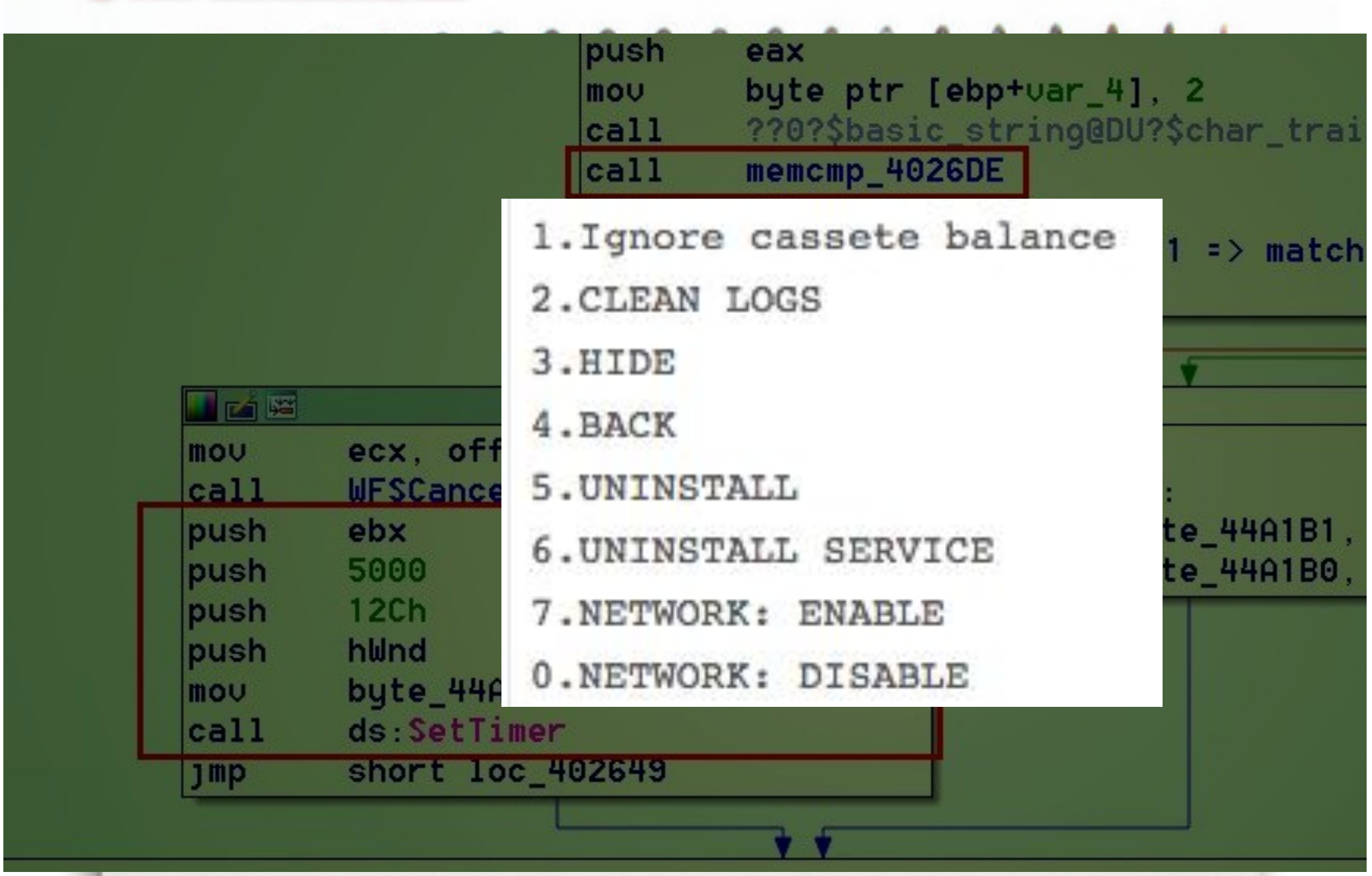
Name: Neopocket
First Found: 2014
Objective: Skimming
ATM target: Diebold
Region: Latin America

The attacks...

5

Name: Padpin
First Found: 2014
Objective: Cash
ATM target: NCR
Region: Eastern Europe

The attacks...


push eax
mov byte ptr [ebp+var_4], 2
call ??0?$basic_string@DU?$char_trai
call memcmp_4026DE
1 => match
mov ecx, off
call WF$Cance
push ebx
push 5000
push 12Ch
push hWnd
mov byte_44A
call ds:SetTimer
jmp short loc_402649
te_44A1B1,
te_44A1B0,
1.Ignore cassete balance
2.CLEAN LOGS
3.HIDE
4.BACK
5.UNINSTALL
6.UNINSTALL SERVICE
7.NETWORK: ENABLE
0.NETWORK: DISABLE

Padpin criminal arrested

Grigore Paladi: Gang member jailed for helping steal £1.6m from cash machines in ONE weekend

10:46, 6 FEB 2015 | **UPDATED** 10:49, 6 FEB 2015 | **BY** SAM ADAMS

Grigore Paladi was sentenced to five years inside for conspiring to insert malware into cash machines and physically stealing more than £554,860

2
SHARES

Enter your e-mail for our daily newsletter Subscribe

Padpin World Tour

KUALA LUMPUR: A MAN, believed to be responsible for using malware to steal more than RM3.42 million from automated teller machines of several banks here in September, is expected to be charged in a London court today.

The 37-year-old man, identified as Grigore Paladi, fled to London after his gang hacked into 19 ATMs in Johor, Kuala Lumpur, Selangor, Penang and Malacca between Sept 24 and 29.

He was nabbed by the British authorities on Oct 24 in London for siphoning RM8.13 million (£1.5 million) using a similar malware there in May.

Federal Commercial Criminal Investigation Department deputy director (cyber and multimedia crimes) senior Assistant Commissioner Mohd Kamarudin Md Din said the

"We believe that he continued his crime spree in several countries before fleeing to London. Investigations showed that he had carried out similar thefts in the United Kingdom, Russia, Malaysia, Germany and Canada.

He also holds dual Romanian and Republic of Moldova citizenship.

"He is also believed to be involved in hacking 58 ATMs in the UK, causing a total loss of £1.5 million; two ATMs in Russia amounting to 287,000 roubles (RM16,300); and 18 ATMs in Germany amounting to €195,000 (RM833,000)."

TREND MICRO

Padpin criminals arrested

INTERNATIONAL CRIMINAL GROUP BEHIND ATM MALWARE ATTACKS DISMANTLED

The Hague, the Netherlands

7 January 2016

The Romanian National Police and the Directorate for Investigating Organised Crimes and Terrorism (DIICOT), assisted by Europol and Eurojust as well as a number of European Law Enforcement authorities, disrupted an international criminal group responsible for ATM malware attacks. This operation, one of the first in Europe against this kind of threat, resulted in multiple house searches in Romania and the Republic of Moldova and the final arrest of 8 individuals. The criminals used Tyupkin ATM malware which allowed the attackers to manipulate ATMs across Europe and illegally empty ATM cash cassettes.

The criminal group, composed of Romanian and Moldovan nationals, was involved in large scale ATM "Jackpotting", causing substantial losses across Europe to the ATM industry. ATM "Jackpotting" refers to the use of a Trojan horse, physically launched via an executable file in order to target an ATM, thus allowing the attackers to empty the ATM cash cassettes via direct manipulation, using the ATM PIN pad to submit commands to the Trojan.

Padpin...

ATM Malware

Discussion in 'Physical Carding' started by zazaza13, Mar 23, 2015.

Page 1 of 2 1 2 Next >

zazaza13
Member
Vendor

Joined: Mar 19, 2015
Messages: 170
Likes Received: 8

I have a working custom/modified version of tyupkin malware.
If you know what this is, and would like to cooperate hit me up a PM and we'll work out th
Very lucrative and a lot of $$.

contact through PM.

zazaza13, Mar 23, 2015

Report

TREND MICRO

Recommendations

Physical Security

Offline Security

Online Security


Thank you!


Questions?