ATM or it never happened

Alexey Osipov, Olga Osipova

kaspersky

Moscow, 18 June 2019

root@root:~#whoami

- Security Assessment Centre, kaspersky
  - ATM and POS Security Assessment
  - Penetration Testing
  - Social Engineering
  - Forensic Investigation
- ATMIA and EAST Members
- Speakers at many IT events
- Authors of multiple articles, researches and advisories
- @ GiftsUngiven, @_Endless_Quest_

Hardware


we're watching you
DefCamp
Where Hacking & Security Collide
DefCamp

Communication lines

- Buses
  - USB
  - SDC (RS485)
  - CAN
- Lines
  - COM (RS232)
  - GPIO
- Wireless

Ultimate Chart of Computer Connectors and Ports

Updated for 2018

USB, Keyboard and Mouse


USB Type A (male)


USB Type A (female)


USB Type B (male)


USB Type B (female)


USB Mini-A (male)


USB Micro-A (male)


USB Type C (male)


USB Type C (female)


USB 3.0 Type A (male)


USB 3.0 Type A (female)


USB 3.0 Type B (male)


USB 3.0 Micro B (male)


PS/2 (male)


PS/2 (female)

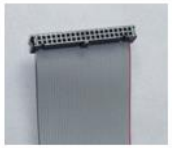

AT Keyboard (male)


AT Keyboard (female)

Storage / Disk


SATA Type A


e-SATA

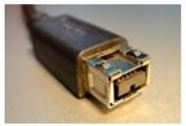

IDE 40-pin Connector


IDE 40-pin Port


Thunderbolt


Firewire 400 1394a 6-pin


Firewire 400 1394a 4-pin


Firewire 800/3200 1394b/c


SCSI VHCDI 8.mm 68-pin


SCSI Micro DB68 (male)


SCSI Micro DB68 (female)


SCSI Micro DB50 (male)


Internal 50-pin SCSI (m)


Internal 50-pin SCSI (f)


Internal 68-pin SCSI (m)


Internal 68-pin SCSI (f)

Network / Communications


Ethernet RJ-45


Modem/Phone RJ-11


Serial/Parallel (m) DB-25


Serial/Parallel (f) DB-

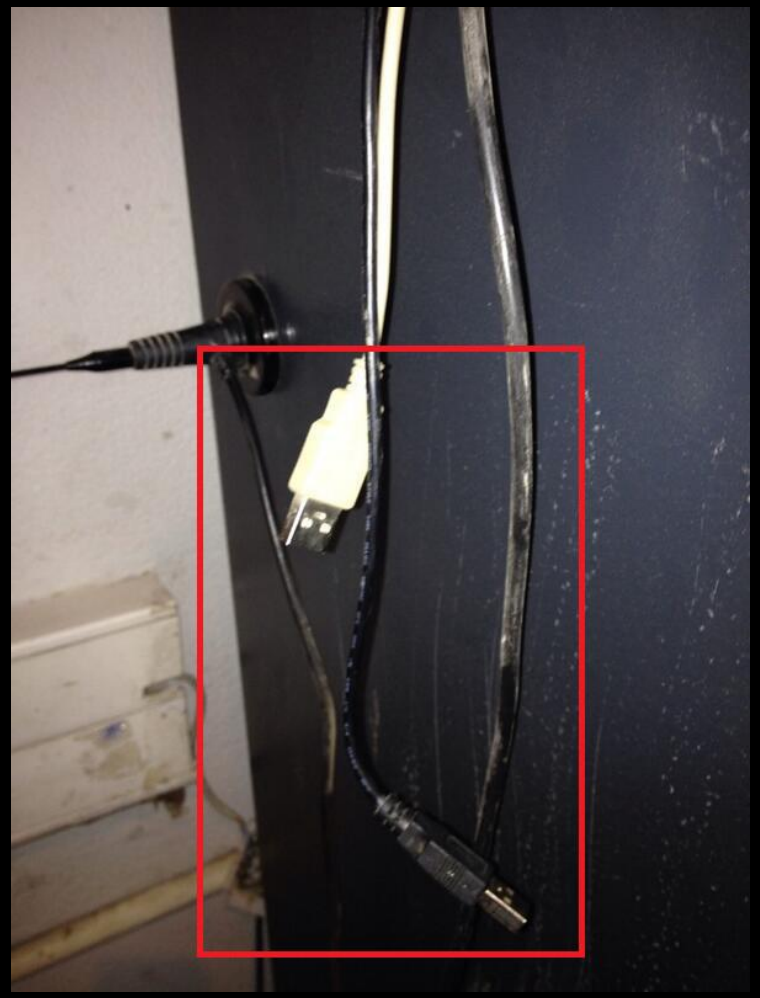

Serial RS232 (m) DE-9


Serial RS232 (f) DE-9


Centronics Parallel 36-pin


MIDI/gameport/DA-15

USB. Problem description



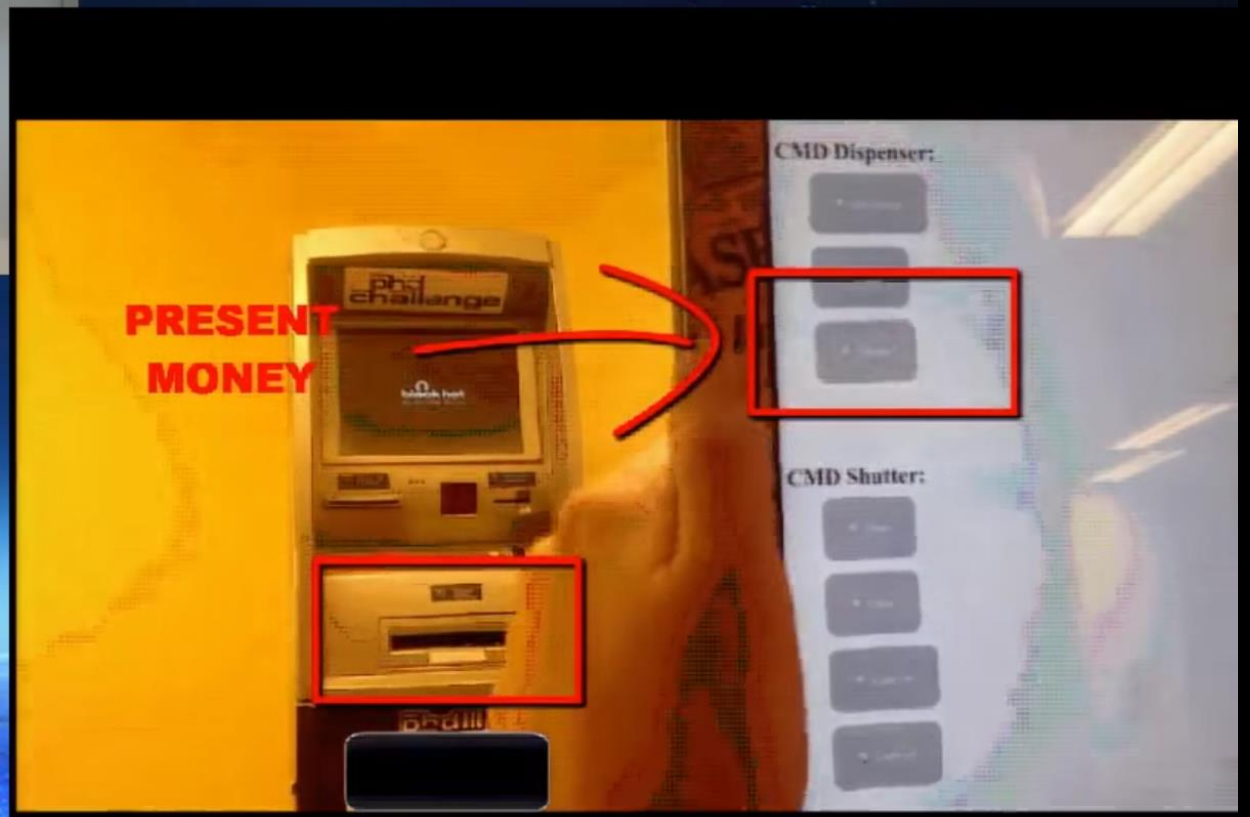
USB device classes

Base Class	Descriptor Usage	Description
00h	Device	Use class information in the Interface Descriptors
01h	Interface	Audio
02h	Both	Communications and CDC Control
03h	Interface	HID (Human Interface Device)
05h	Interface	Physical
06h	Interface	Image
07h	Interface	Printer
08h	Interface	Mass Storage
09h	Device	Hub
0Ah	Interface	CDC-Data
0Bh	Interface	Smart Card
0Dh	Interface	Content Security
0Eh	Interface	Video
0Fh	Interface	Personal Healthcare
10h	Interface	Audio/Video Devices
11h	Device	Billboard Device Class
12h	Interface	USB Type-C Bridge Class
DCh	Both	Diagnostic Device
E0h	Interface	Wireless Controller
EFh	Both	Miscellaneous
FEh	Interface	Application Specific
FFh	Both	Vendor Specific

https://www.usb.org/defined-class-codes


black hat
EUROPE 2014

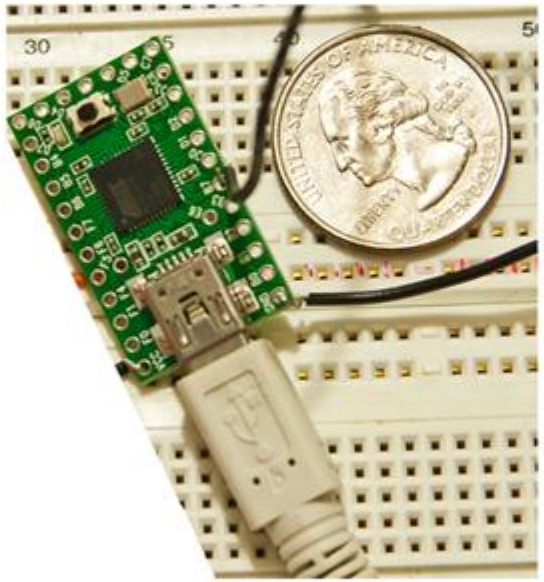

black hat
EUROPE 2014


PRESENT
MONEY
CMD Dispenser:
CMD Shutter:

THE ATTACKER USES A **KEY PURCHASED ON THE WEB** OR FROM AN INSIDER.

THIS VIDEO IS A PROOF-OF-CONCEPT OF A BLACK BOX ATTACK AGAINST AN ATM.

USB HID – THE MOST HIDDEN MAGIC




Better Call 1337
PLEASE
INSERT
YOUR CARD
Better Call 1337
Better Call 1337

ATM configuration. Problem description

NRF21/Bluetooth/Radio keyboards

https://www.mousejack.com/

https://greatscottgadgets.com/ubertoothone/

Mousejack

- https://www.mousejack.com/
- https://github.com/BastilleResearch/keyjack
- https://github.com/insecurityofthings/jackit

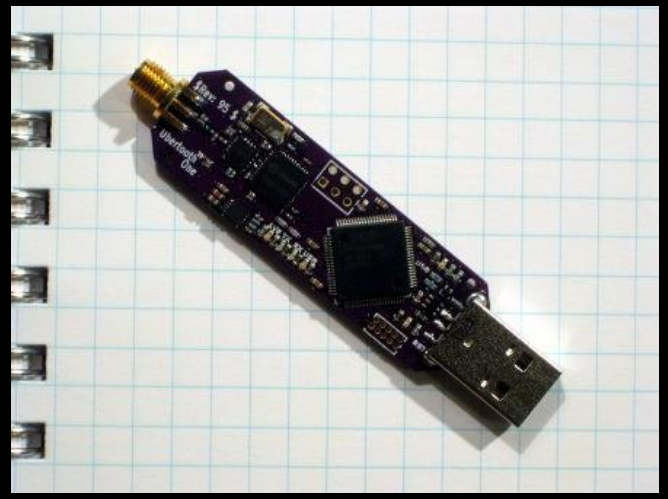
https://www.bitcraze.io/crazyradio-pa/

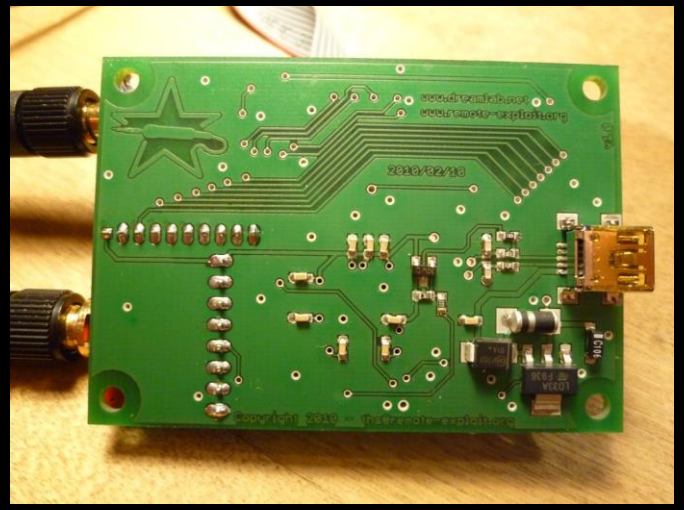
Typical MouseJack setup


Better Call 1337
MouseJack
Last Seen
Device
CANCEL
1
2
3

Underestimated hero

Other flavors





- http://ubertooth.sourceforge.net/usage/start/
- http://www.remote-exploit.org/articles/keykeriki_v2_0__8211_2_4ghz/index.html

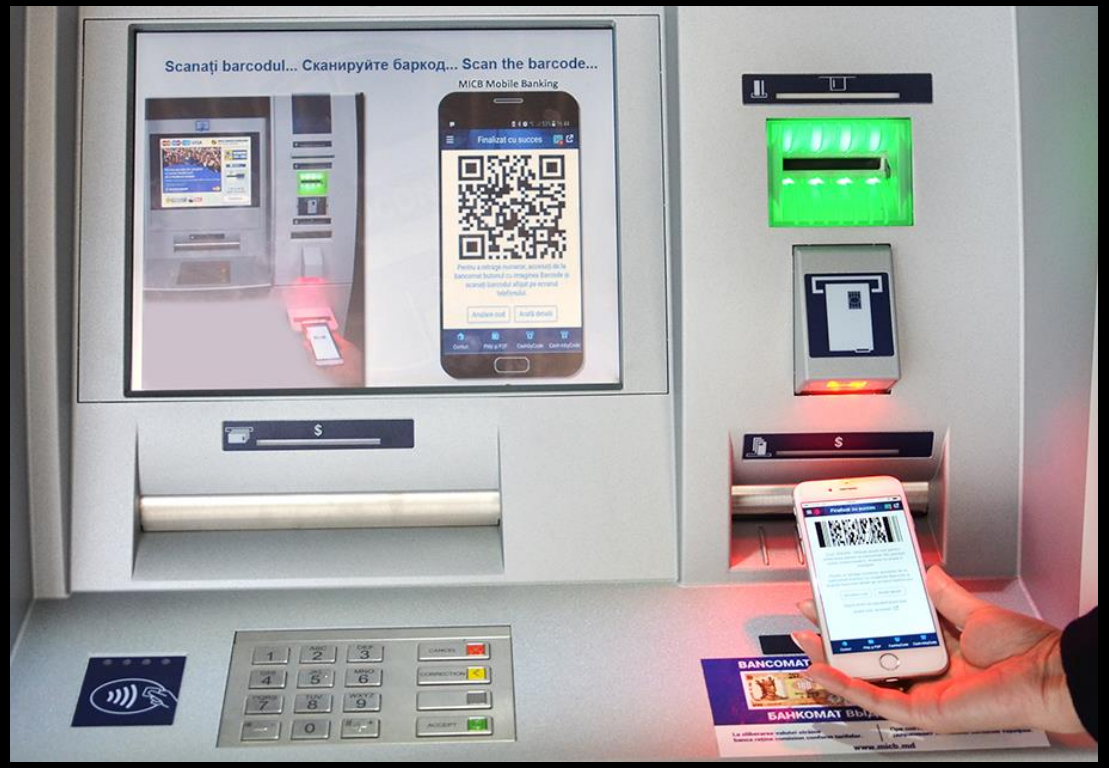
How to detect

- Obtain some fancy wireless device (CrazyRadio PA/Ubertooth/RTL-SDR/USRP/etc.)
- Sniff nearby devices
  - If something is near the ATM – it’s already a problem
- Correlate
- ?????
- Profit

https://krebsonsecurity.com/tag/bluetooth-skimmer/

Barcode. Problem description

Fantastic Points and Where to Find Them



Barcode


Получите 100 Offcoin за платежи по
штрихкоду в Finance.Zone
OFFZONE

BadBarcode attacks

Is BadBarcode a bug?

BadBarcode is not an implementation bug but a design flaw. Symbologies such as Code 128 supports encoding control characters, and devices work in Keyboard Simulation Mode. These two seemingly logical designs, when combined, become a security vulnerability.

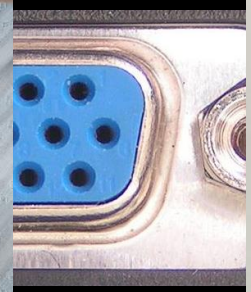
What does BadBarcode attack look like?

Scan QR code on a cellphone, resulting in an application download and execution:

https://xlab.tencent.com/badbarcode/


Better Call 1337
Better Call 1337

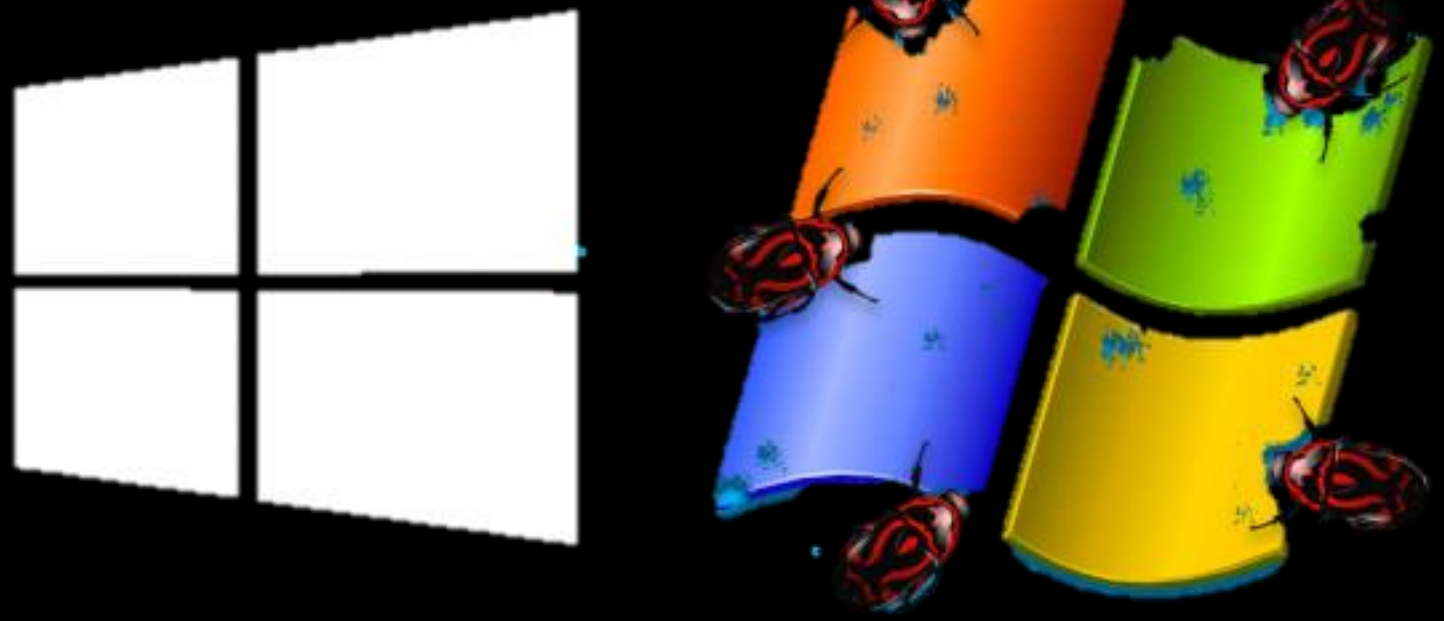
Barcode reader in a proper way



Barcode.. fuzzing?

- Find menu item that tries to read 1D/2D code
- Try Code128 code, that starts with FNC3 code
  - If barcode reader beeps differently – it possibly accepts reprogramming codes
- Try QR codes with symbols codes > 128 or < 16
  - Observe abnormal behavior (like arrow keys presses, function keys, etc.)
- Do it responsibly and with formal agreement of the device owner

Windows XP vs Windows 7



Windows XP vs Windows 7

- General availability: October 25, 2001; 18 years ago
- Final release: April 21, 2008; 11 years ago
- End of support: July 13, 2010; 9 years ago

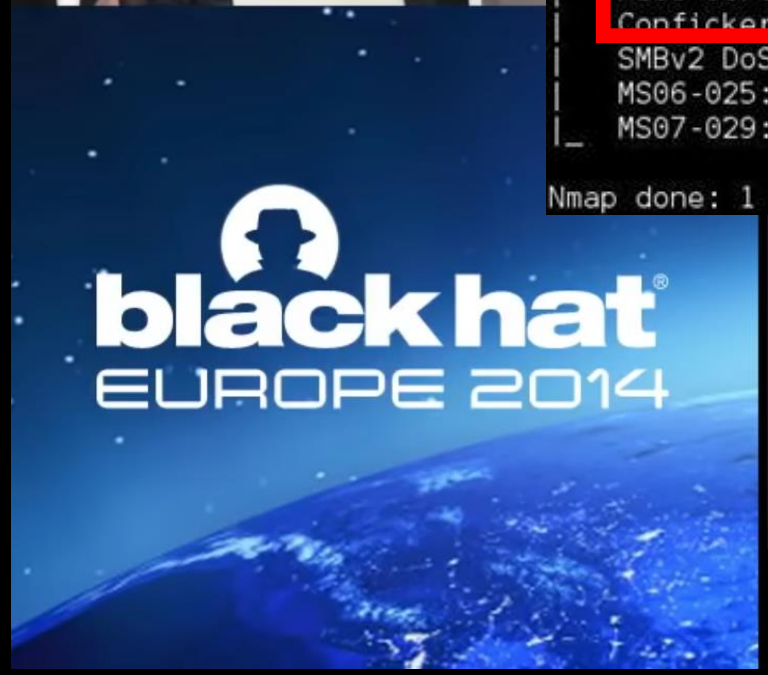
- MS08-067 vulnerability fix deployed on all ATM: never

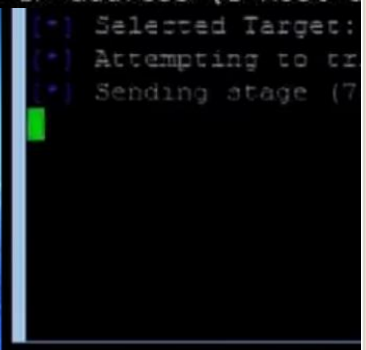
- General availability: October 22, 2009; 10 years ago
- Latest release: February 22, 2011; 8 years ago
- End of support: Jan 14, 2020; next year

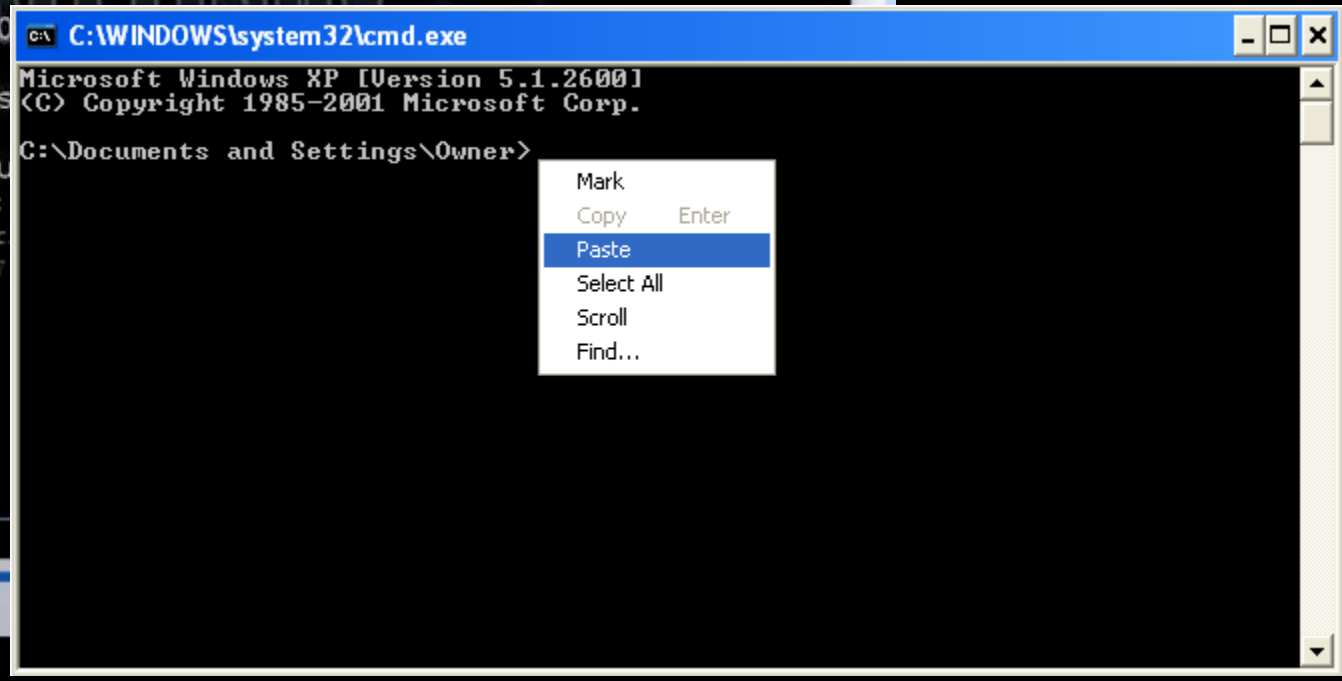
- MS17-010 vulnerability fix deployed on all ATM: never
- Adoption by ATM industry: 2016-2017

NMAP + MS08_067

```
root@kali:~# nmap --script-args=unsafe=1 --script smb-check-vulns.nse -p445 192.
168.1.121

Starting Nmap 6.46 ( http://nmap.org ) at 2014-11-21 16:42 MST
Nmap scan report for 192.168.1.121
Host is up (0.0027s latency).
PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:18:6B:DB (VMware)

Host script results:
|  MS08-067: VULNERABLE
|  Conficker: Likely CLEAN
|  SMBv2 DoS (CVE-2009-3103): NO
|  MS06-025: NOT VULNERABLE
|_ MS07-029: NO SERVICE (the Dns

Nmap done: 1 IP address (1 host u
```







MS08-067 goes to MS17-010

```
PORT    STATE SERVICE      REASON
445/tcp open  microsoft-ds syn-ack

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/m
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/cu
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-201
```

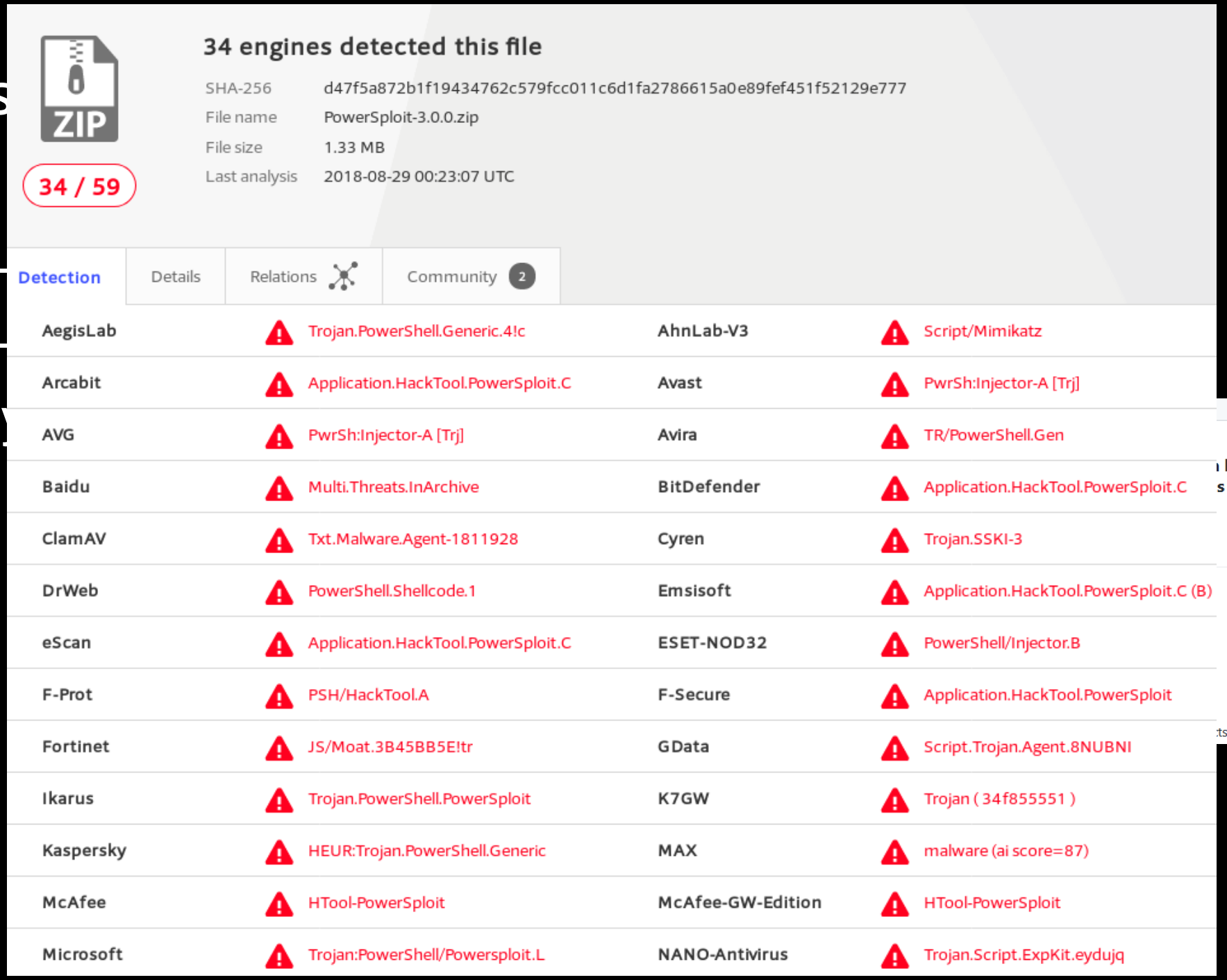
https://www.blackhat.com/eu-14/archives.html#hack-your-atm-with-friends-raspberry-py

IPv4 goes to IPv6

```
Rule Name:                                      Core Networking - IPv6 (IPv6-In)
----------------------------------------------------------------------------
Enabled:                                        Yes
Direction:                                      In
Profiles:                                       Domain,Private,Public
Grouping:                                       Core Networking
LocalIP:                                        Any
RemoteIP:                                       Any
Edge traversal:                                 No
Action:                                         Allow
--
```

Powers

- Invoke-
- Invoke-
- Get-Ke
- etc



PS> Give me the money!

Writing to a Serial Port

```
PS> [System.IO.Ports.SerialPort]::getportnames()
COM3
PS> $port= new-Object System.IO.Ports.SerialPort COM3,9600,None,8,one
PS> $port.open()
PS> $port.WriteLine("Hello world")
PS> $port.Close()
```

Reading from a Serial Port

```
PS> $port= new-Object System.IO.Ports.SerialPort COM3,9600,None,8,one
PS> $port.Open()
PS> $port.ReadLine()
```

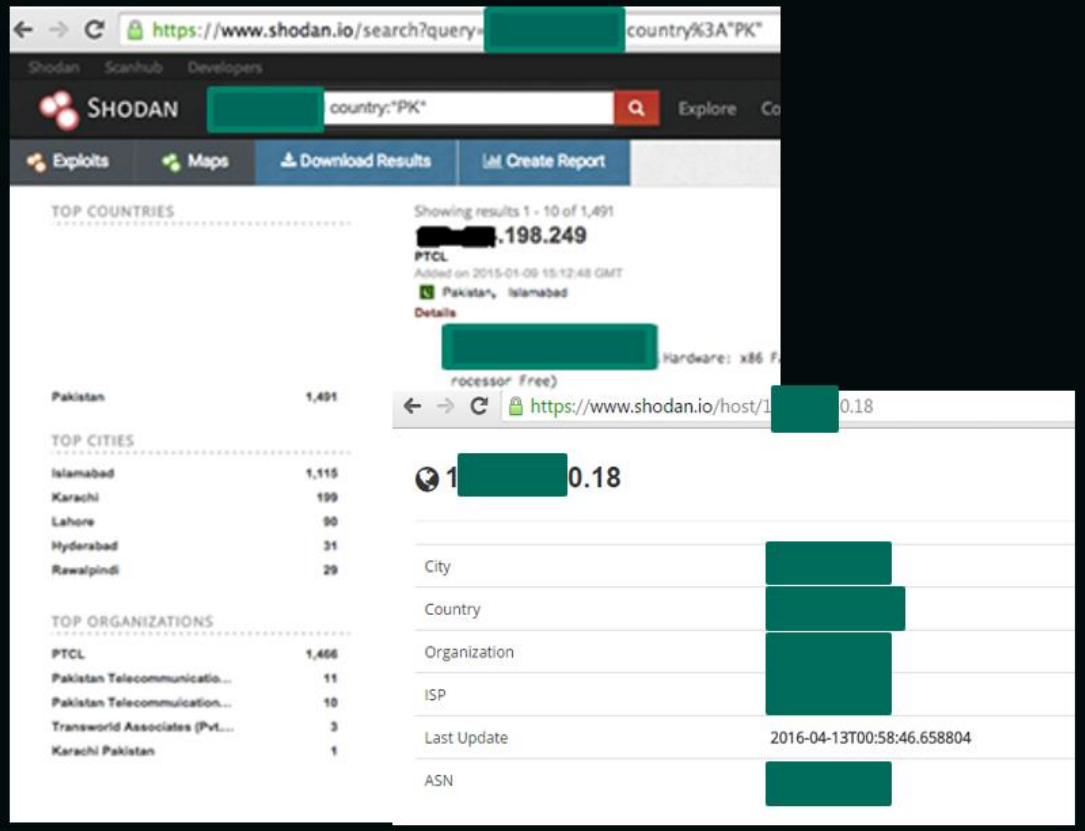
Via MSDN

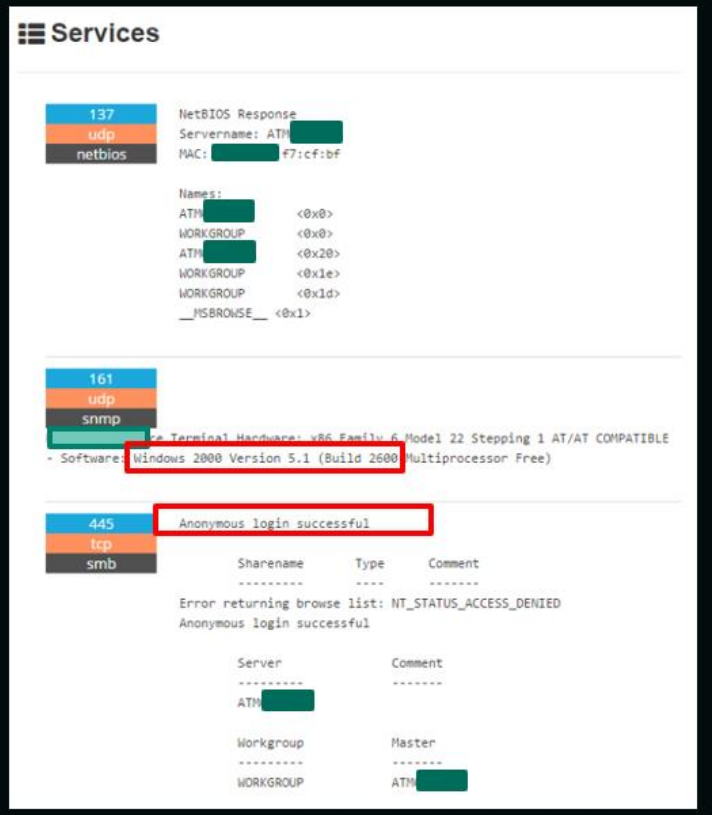
```
$MethodDefinition = @'
[DllImport("kernel32.dll", CharSet = CharSet.Unicode, SetLastError = true)]
public static extern bool CopyFile(string lpExistingFileName, string lpNewFileName, bool bFailIfExists);
'@
```

https://blogs.technet.microsoft.com/heyscriptingguy/2013/06/25/use-powershell-to-interact-with-the-windows-api-part-1/

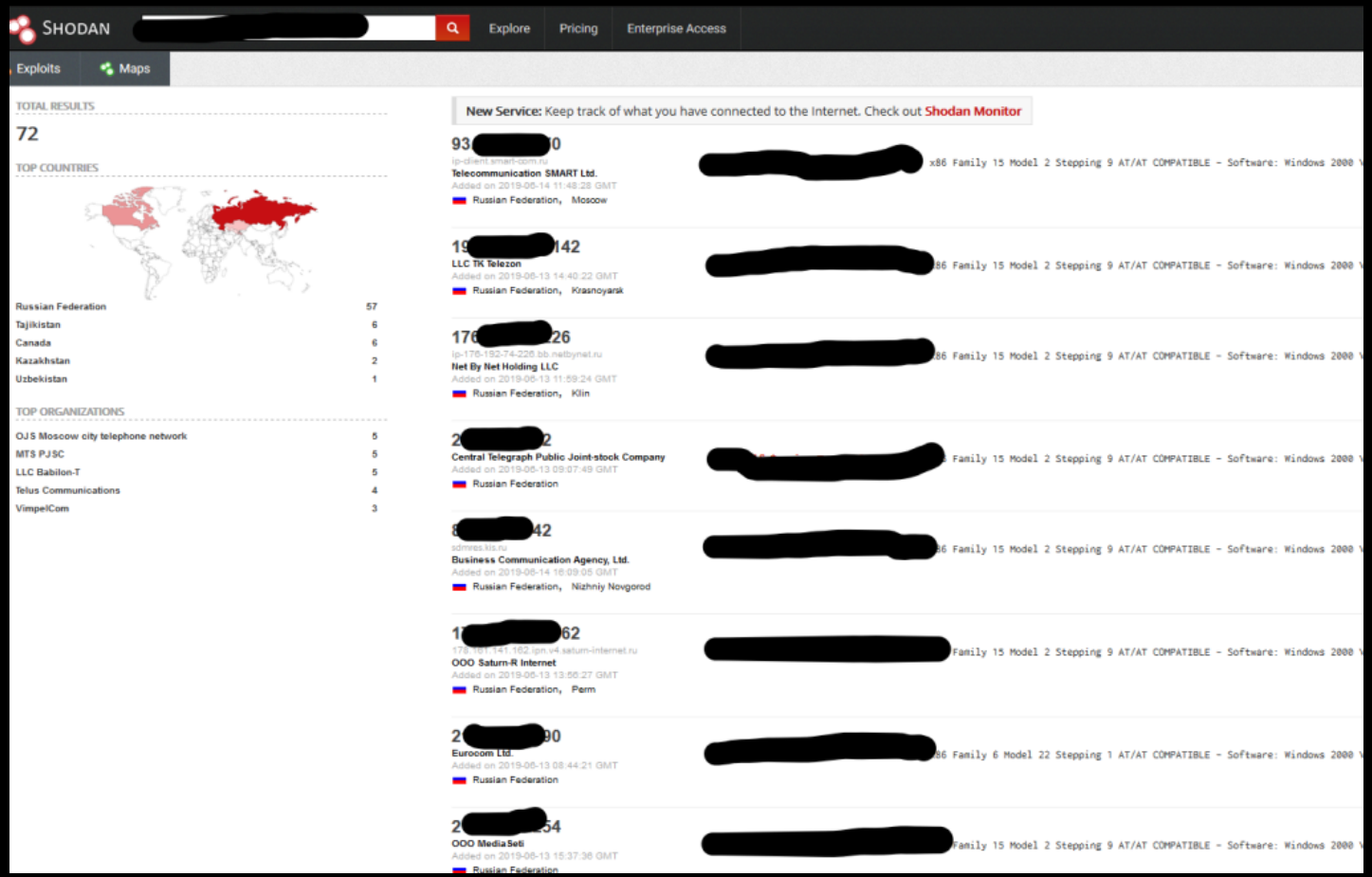

ROB THE BANK!
Better Call 1337

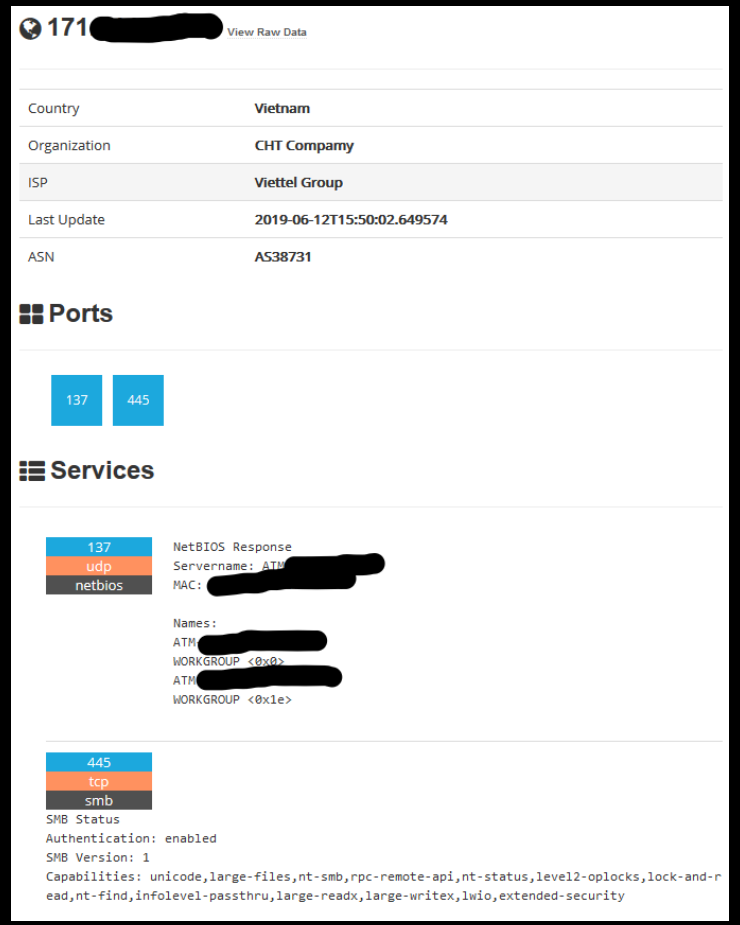
Let's have fun with Shodan





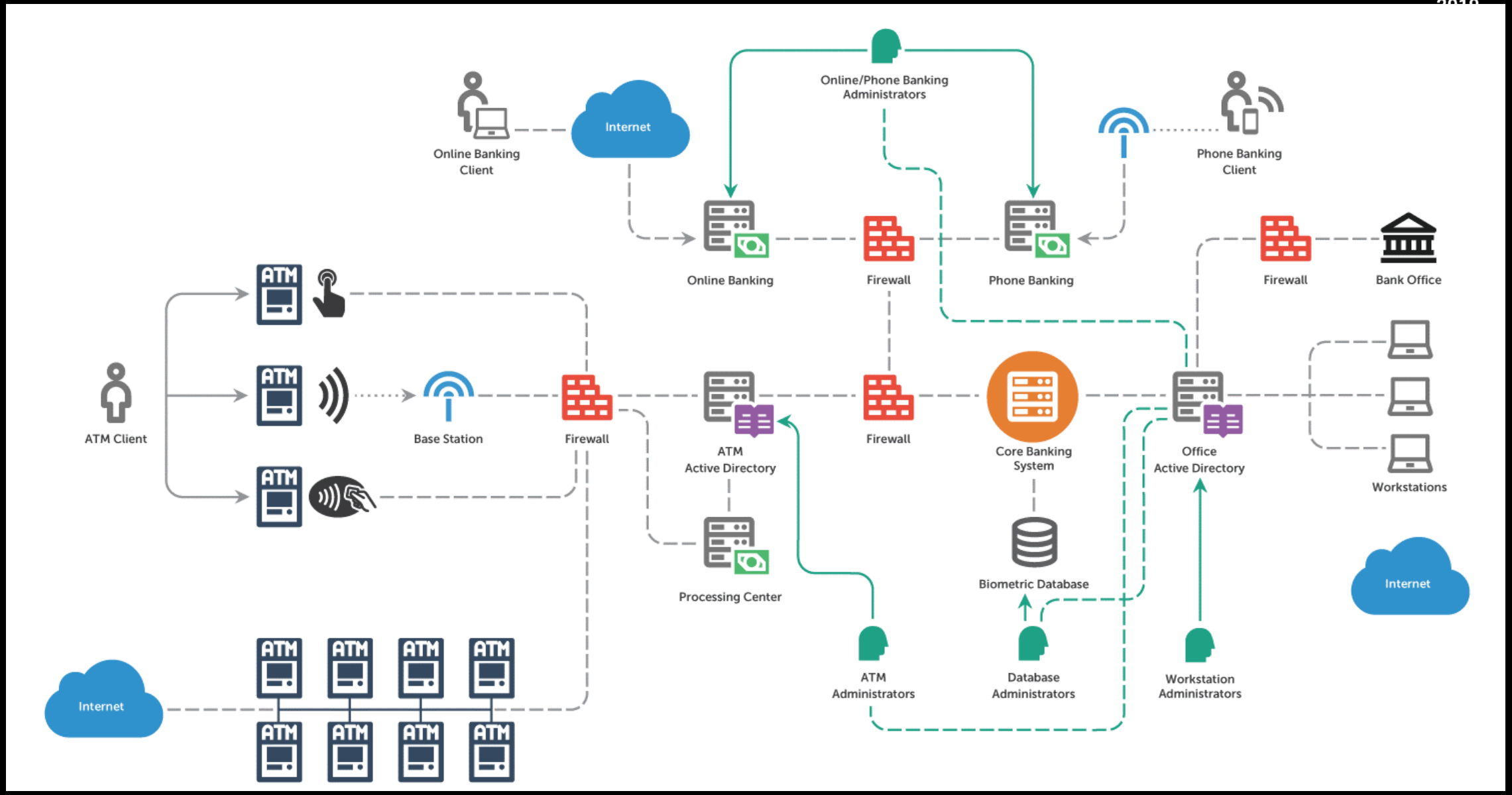
And the winner is…





Not a conclusion

Typical banking network



ATM device status

Previously

- Card reader
- Function Display Key
- PIN pad
- Dispenser

Now

- Touch screens
- NFC reader
- 1D/2D barcode readers
- Consumer keyboard
- Biometric devices
- Scanners of all sorts
  - (cheque, document, etc.)
- Cash recyclers
- Coin in/out

ATM device status

Previously

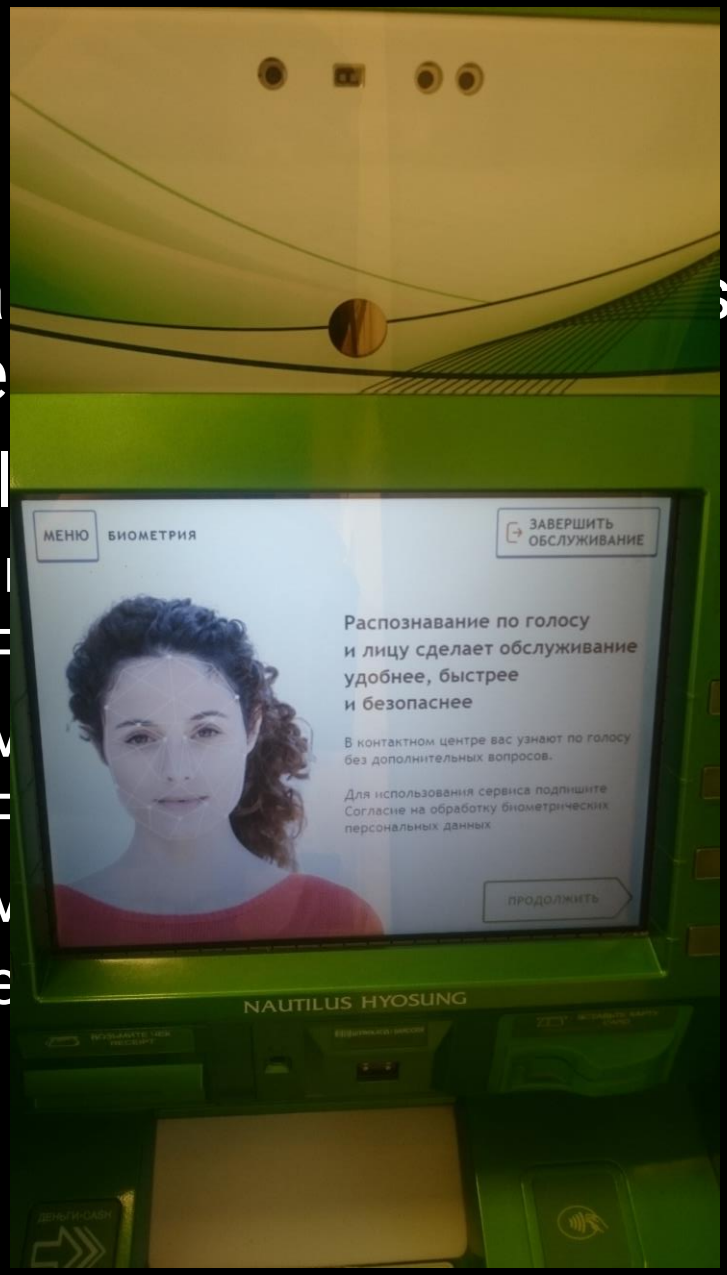
- Card reader
- Function Display Key
- PIN pad
- Dispenser

Now

- Touch screens
- NFC reader
- 1D/2D barcode readers
- Consumer keyboard
- Biometric devices
- Scanners of all sorts
  - (cheque, document, etc.)
- Cash recyclers
- Coin in/out

Biometric authentication devices

- Gra s of use
- Mul
  - I
  - F
  - V
  - F
  - V
  - e



Kudos

Security is a process

Alexey.Osipov@kaspersky.com, @ GiftsUngiven
Olga.Osipova@kaspersky.com, @_Endless_Quest_

kaspersky