



ATM or it never happened

Alexey Osipov, Olga Osipova
kaspersky

Moscow, 18 June 2019

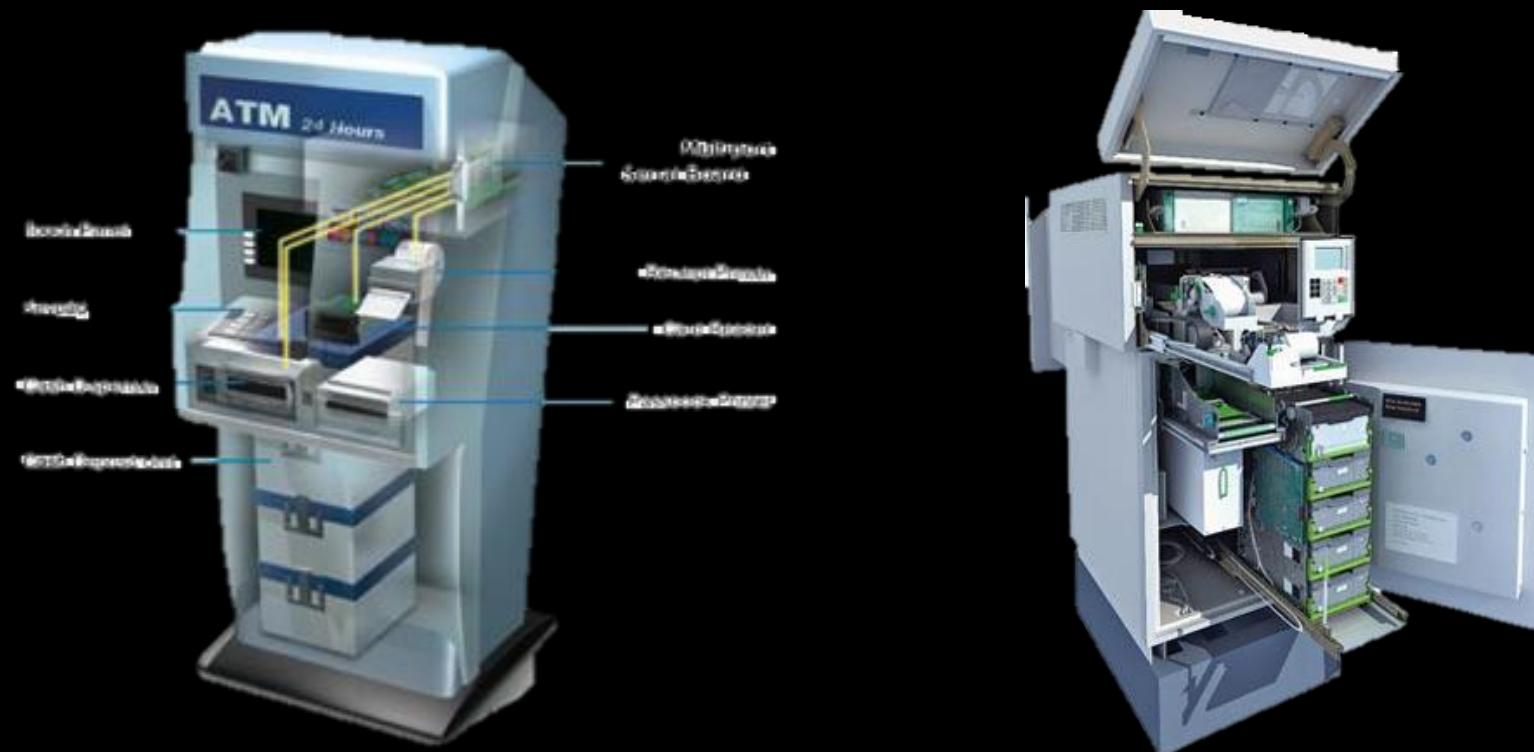
root@root:~#whoami

NO
FF
ONE
2019

- 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



20Ai8Oh

we're watching you

DefCamp
Where Hacking & Security Collide



DefCamp
Where Hacking & Security Collide

1 2 3
4 5 6
7 8 9

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-25



Serial RS232 (m) DE-9



Serial RS232 (f) DE-9

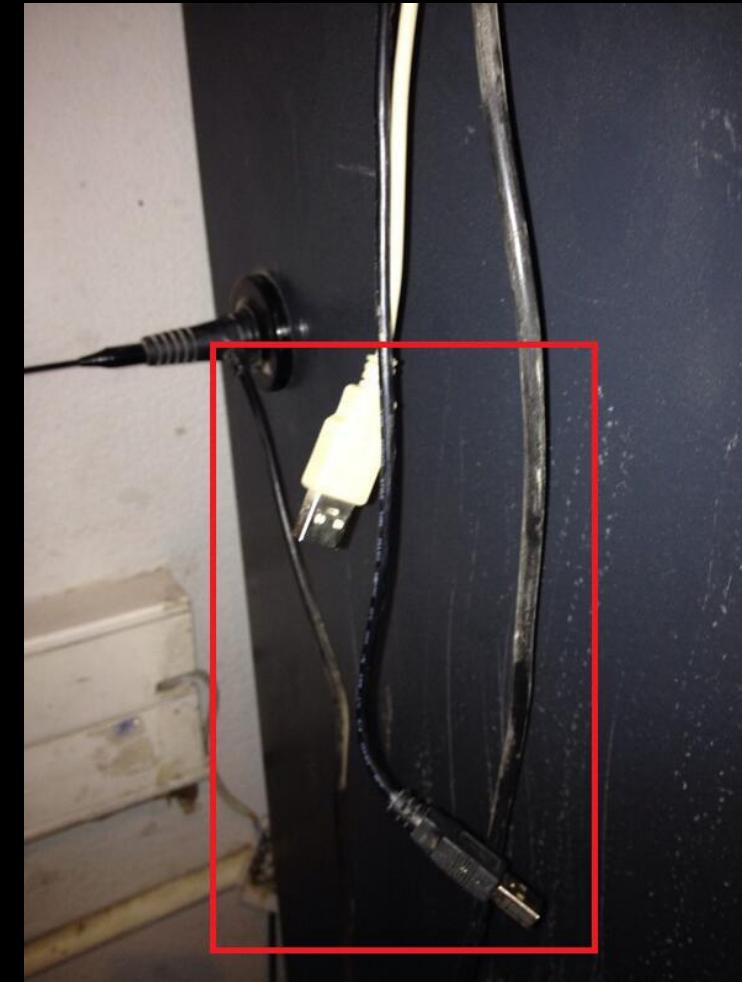
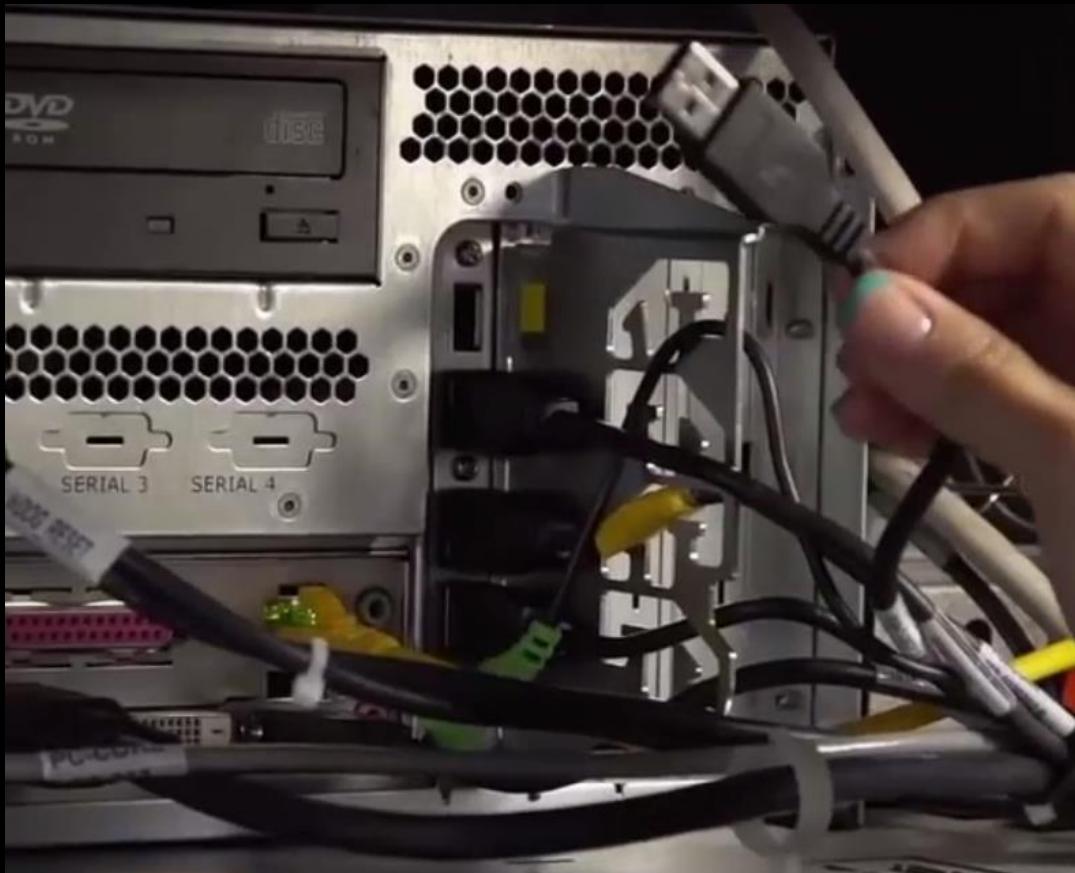


Centronics Parallel 36-pin



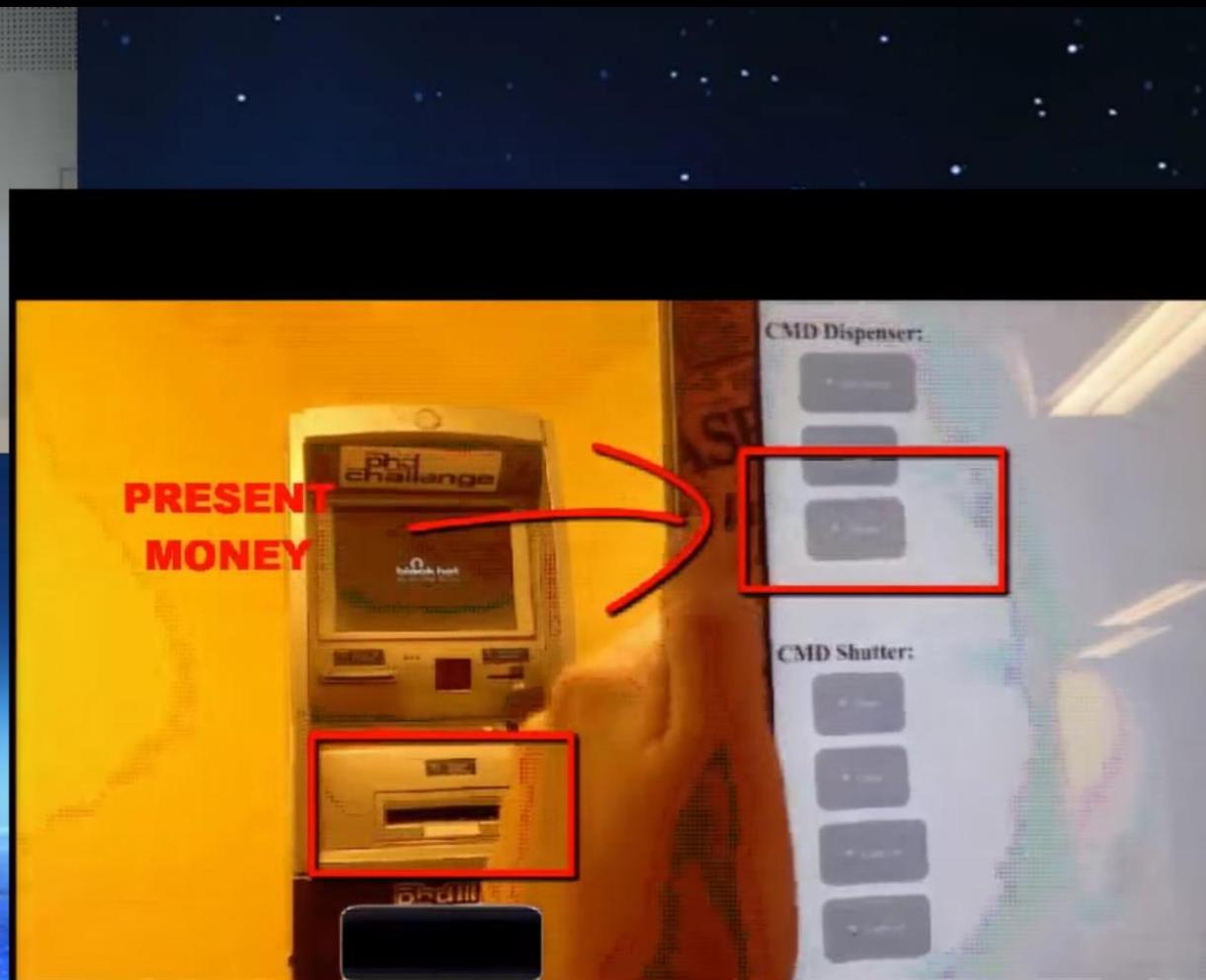
MIDI/gameport/DA-15

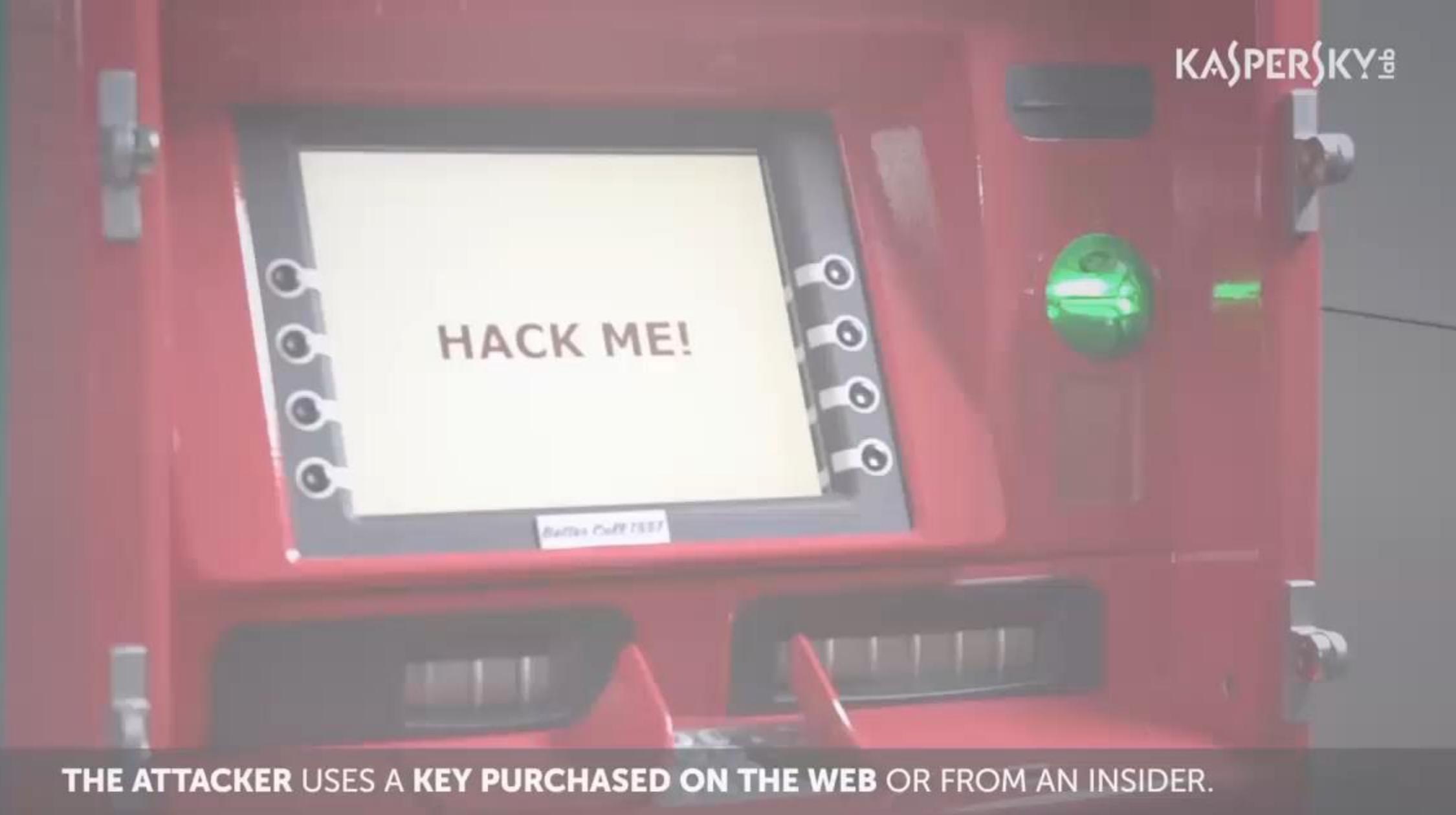
USB. Problem description



USB device classes

Base Class	Descriptor Usage	Description
00h	Device	Use class information in the Interface Descriptors
01h	Interface	
02h	Both	Communications and CDC Control
03h	Interface	HID (Human Interface Device)
05h	Interface	
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
FFh	Interface	Application Specific
FFh	Both	Vendor Specific



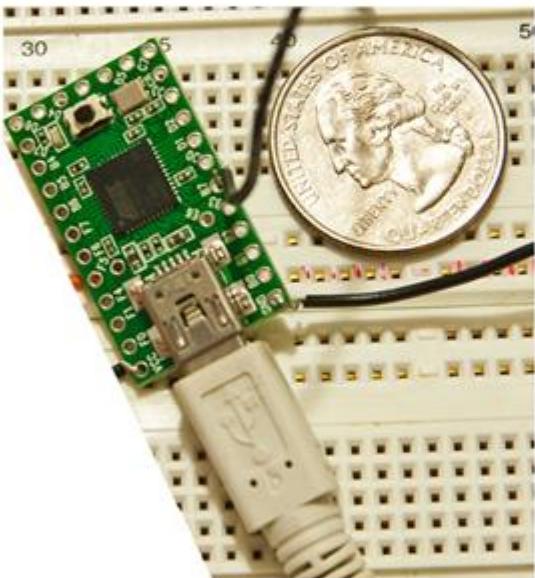


THE ATTACKER USES A KEY PURCHASED ON THE WEB OR FROM AN INSIDER.

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

USB HID – THE MOST HIDDEN MAGIC

NO
FF
ONE
2019



Better Call 1337

PLEASE
INSERT
YOUR CARD

Better Call 1337

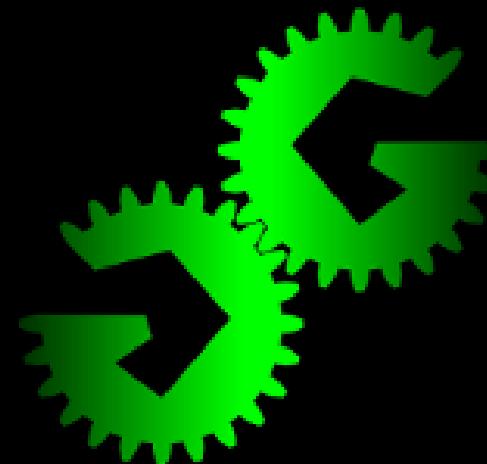
ATM configuration. Problem description

NO
OFF
ONE
2019



NRF21/Bluetooth/Radio keyboards

NO
FF
ONE
2019



<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

NO
OFF
ONE
2019

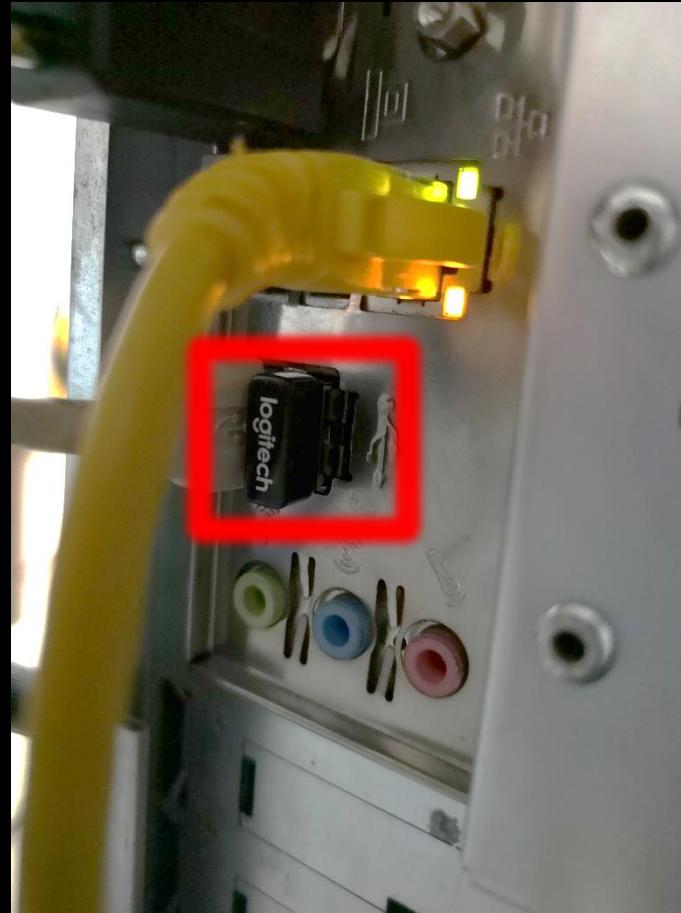




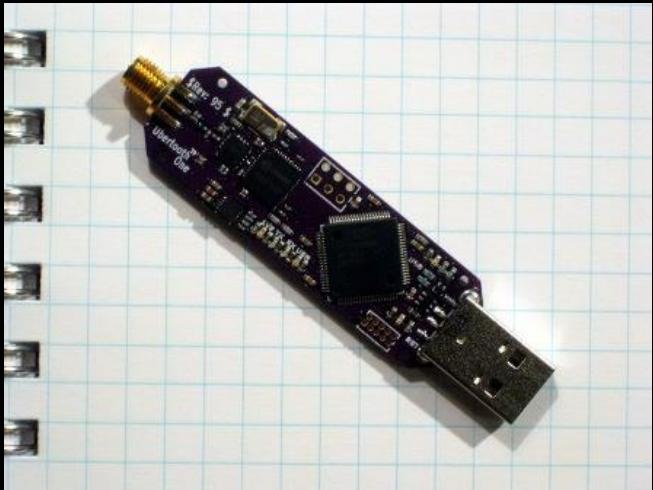
1 2 3
ENTER
CANCEL
CLEAR
...
4 5 6
7 8 9
0

Underestimated hero

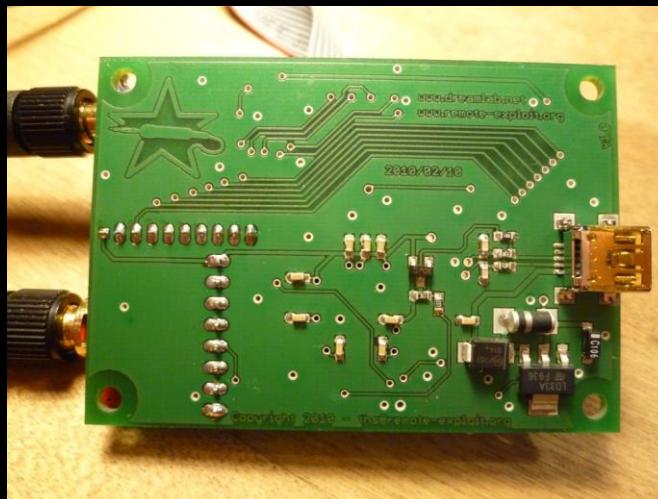
FF
ON
ONE
2019



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

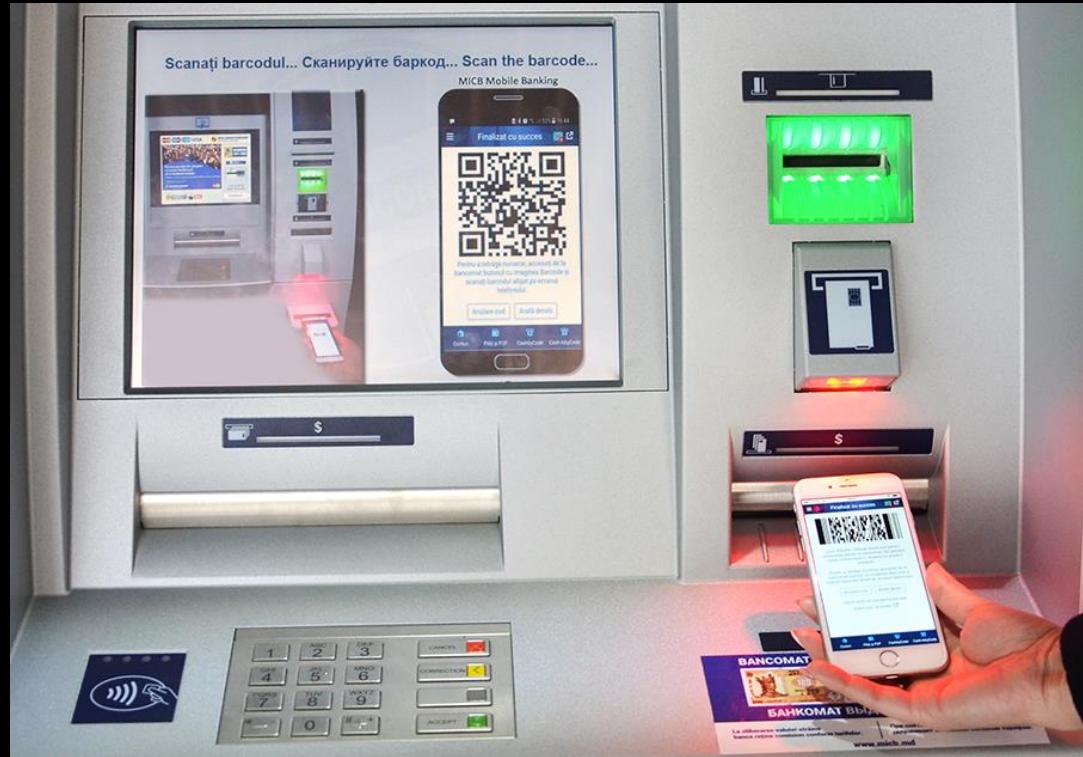
- Obtain some fancy wireless device (CrazyRadio PA/Ubertooth/RTL-SDR/USRP/etc.)
- Sniff nearby devices
 - If something is near the ATM – it's already a problem
- Correlate
- ?????
- Profit



Barcode. Problem description



Fantastic Points and Where to Find Them

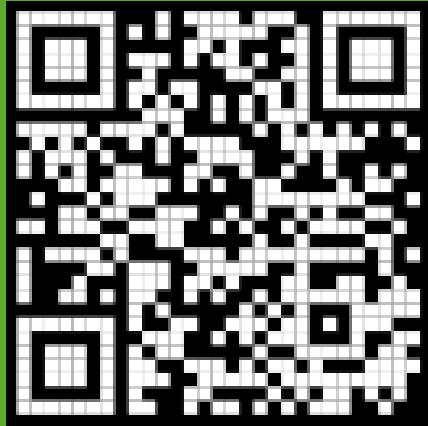


Barcode



OFF
ONE
2019

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

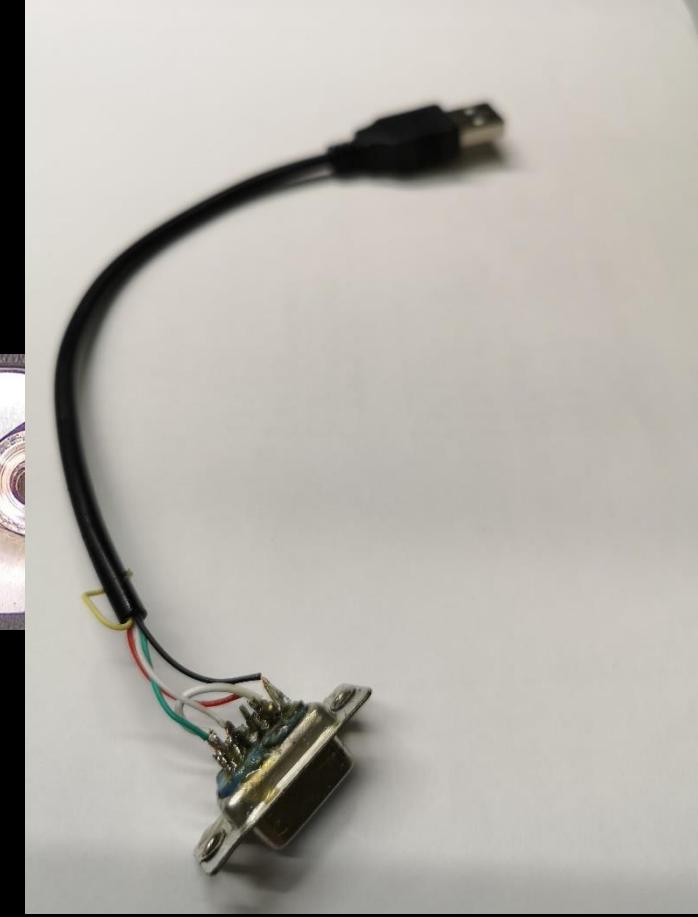
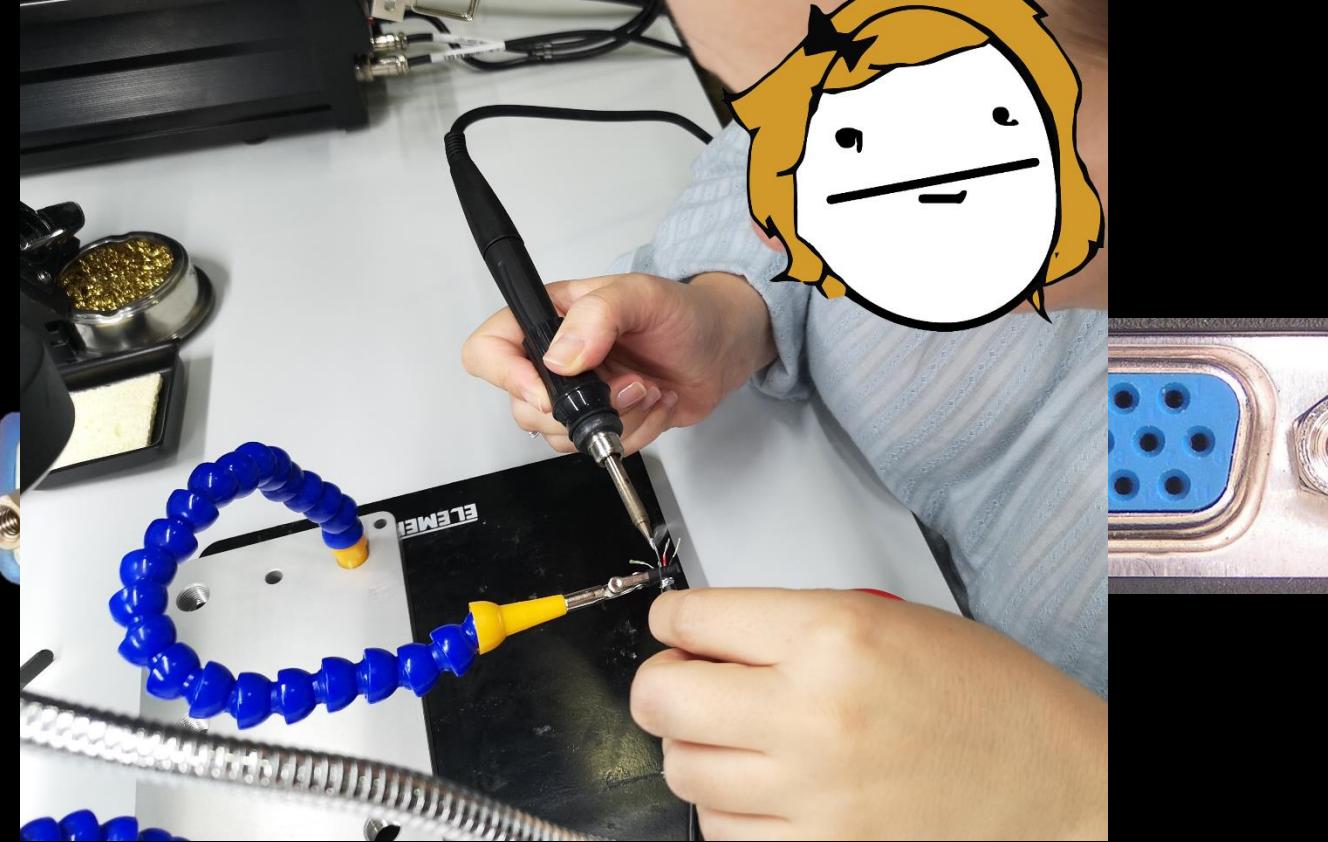


Better Call 1337

USA
INTERNATIONAL

Barcode reader in a proper way

NO
OFF
ONE
2019

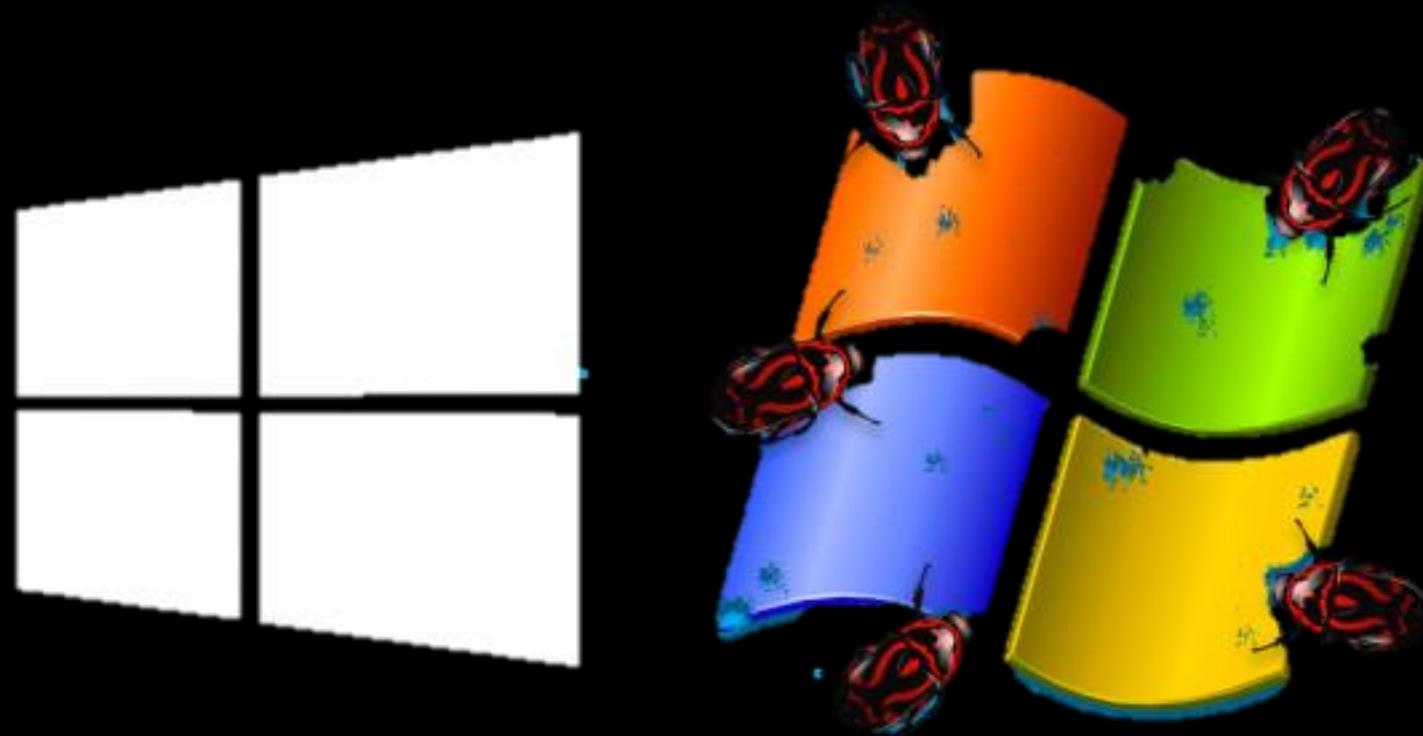


Barcode.. fuzzing?

- 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

NO
OFF
ONE
2019



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:
|_SMB check vulns.
|_ 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 up) u
[*] Selected Target:
[*] Attempting to ex
[*] Sending stage (7

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Owner>
Mark
Copy   Enter
Paste
Select All
Scroll
Find...
```

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/ms17-010
|   https://blogs.technet.microsoft.com/msrc/2017/05/12/cve-2017-0143/
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
```



<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
--	

Powershell

ZIP

34 / 59

34 engines detected this file

SHA-256 d47f5a872b1f19434762c579fcc011c6d1fa2786615a0e89fef451f52129e777

File name PowerSploit-3.0.0.zip

File size 1.33 MB

Last analysis 2018-08-29 00:23:07 UTC

Detection Details Relations Community 2

AegisLab	⚠️ Trojan.PowerShell.Generic.4!c	AhnLab-V3	⚠️ Script/Mimikatz
Arcabit	⚠️ Application.HackTool.PowerSploit.C	Avast	⚠️ PwrSh:Injector-A [Trj]
AVG	⚠️ PwrSh:Injector-A [Trj]	Avira	⚠️ TR/PowerShell.Gen
Baidu	⚠️ Multi.Threats.InArchive	BitDefender	⚠️ Application.HackTool.PowerSploit.C
ClamAV	⚠️ Txt.Malware.Agent-1811928	Cyren	⚠️ Trojan.SSKI-3
DrWeb	⚠️ PowerShell.Shellcode.1	Emsisoft	⚠️ Application.HackTool.PowerSploit.C (B)
eScan	⚠️ Application.HackTool.PowerSploit.C	ESET-NOD32	⚠️ PowerShell/Injector.B
F-Prot	⚠️ PSH/HackTool.A	F-Secure	⚠️ Application.HackTool.PowerSploit
Fortinet	⚠️ JS/Moat.3B45BB5E!tr	G Data	⚠️ Script.Trojan.Agent.8NUBNI
Ikarus	⚠️ Trojan.PowerShell.PowerSploit	K7GW	⚠️ Trojan (34f855551)
Kaspersky	⚠️ HEUR:Trojan.PowerShell.Generic	MAX	⚠️ malware (ai score=87)
McAfee	⚠️ HTool-PowerSploit	McAfee-GW-Edition	⚠️ HTool-PowerSploit
Microsoft	⚠️ Trojan:PowerShell/Powersploit.L	NANO-Antivirus	⚠️ Trojan.Script.ExpKit.eydujq

be used to aid
s comprised of the

:ts a DLL in to a remote process.

NO OFF ONE 2019

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()
```

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



Let's have fun with Shodan



NO
OFF
ONE
2019

The screenshot shows the Shodan search interface with the query "country:PK". The results page displays various metrics and details for found hosts. Key sections include:

- TOP COUNTRIES:** Pakistan (1,491), followed by India, China, United States, and others.
- TOP CITIES:** Islamabad (1,115), Karachi, Lahore, Hyderabad, and Rawalpindi.
- TOP ORGANIZATIONS:** PTCL (1,466), followed by Pakistan Telecommunications, Transworld Associates (Pvt), and others.
- Host Details:** A specific host entry for IP 198.249 is shown, identified as PTCL in Islamabad, Pakistan. It was added on 2015-01-09 15:12:48 GMT. The host has 1 processor and is multiprocessor free. Its hardware is x86 Family 6 Model 22 Stepping 1 AT/AT COMPATIBLE.
- Services:** The host is running NetBIOS Response via UDP and NetBIOS, and SNMP via UDP.
- Software:** The host is running Windows 2000 Version 5.1 (Build 2600) Multiprocessor Free.
- Sharename:** Error returning browse list: NT_STATUS_ACCESS_DENIED
- Comment:** Anonymous login successful
- Server:** ATM
- Workgroup:** Master
- WORKGROUP:** ATM

This screenshot shows the detailed services and software information for the host 198.249. The services listed are:

- NetBIOS Response (137, udp, netbios): Servername: ATM, MAC: [REDACTED] f7:cfc:bf. Names: ATM <0x0>, WORKGROUP <0x0>, ATM <0x20>, WORKGROUP <0x1e>, WORKGROUP <0x1d>, _NSBROWSE_ <0x1>.
- SNMP (161, udp, snmp): Software: Windows 2000 Version 5.1 (Build 2600) Multiprocessor Free.
- Anonymous login successful (445, tcp, smb): Sharename: Error returning browse list: NT_STATUS_ACCESS_DENIED, Comment: Anonymous login successful.

KASPERSKY

And the winner is...

SHODAN

Exploits Maps

TOTAL RESULTS 72

TOP COUNTRIES

Country	Count
Russian Federation	57
Tajikistan	6
Canada	6
Kazakhstan	2
Uzbekistan	1

TOP ORGANIZATIONS

Organization	Count
OJS Moscow city telephone network	5
MTS PJSC	5
LLC Babilon-T	5
Telus Communications	4
VimpelCom	3

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

93 [REDACTED] 0 ip-client-smart.com.ru Telecommunication SMART Ltd. Added on 2019-05-14 11:48:28 GMT Russian Federation, Moscow

19 [REDACTED] 142 LLC TK Telezon Added on 2019-05-13 14:40:22 GMT Russian Federation, Krasnoyarsk

176 [REDACTED] 26 ip-176-150-74-222.bb.netbynat.ru Net By Net Holding LLC Added on 2019-05-13 11:59:24 GMT Russian Federation, Klin

2 [REDACTED] 2 Central Telegraph Public Joint-stock Company Added on 2019-05-13 09:07:49 GMT Russian Federation

8 [REDACTED] 42 sdmres.kts.ru Business Communication Agency, Ltd. Added on 2019-05-14 16:09:05 GMT Russian Federation, Nizhny Novgorod

1 [REDACTED] 62 172.16.1.45:4021 ipm-4.satur-internet.ru OOO Satur-R Internet Added on 2019-05-13 13:55:27 GMT Russian Federation, Perm

2 [REDACTED] 90 Eurocom Ltd. Added on 2019-05-13 08:44:21 GMT Russian Federation

2 [REDACTED] 54 OOO MediaSeti Added on 2019-05-13 15:37:36 GMT Russian Federation

171 [REDACTED] View Raw Data

Country	Vietnam
Organization	CHT Company
ISP	Viettel Group
Last Update	2019-06-12T15:50:02.649574
ASN	AS38731

Ports

Protocol	Count
tcp	137
udp	445

Services

137 udp netbios

NetBIOS Response
Servername: ATM [REDACTED]
MAC: [REDACTED]

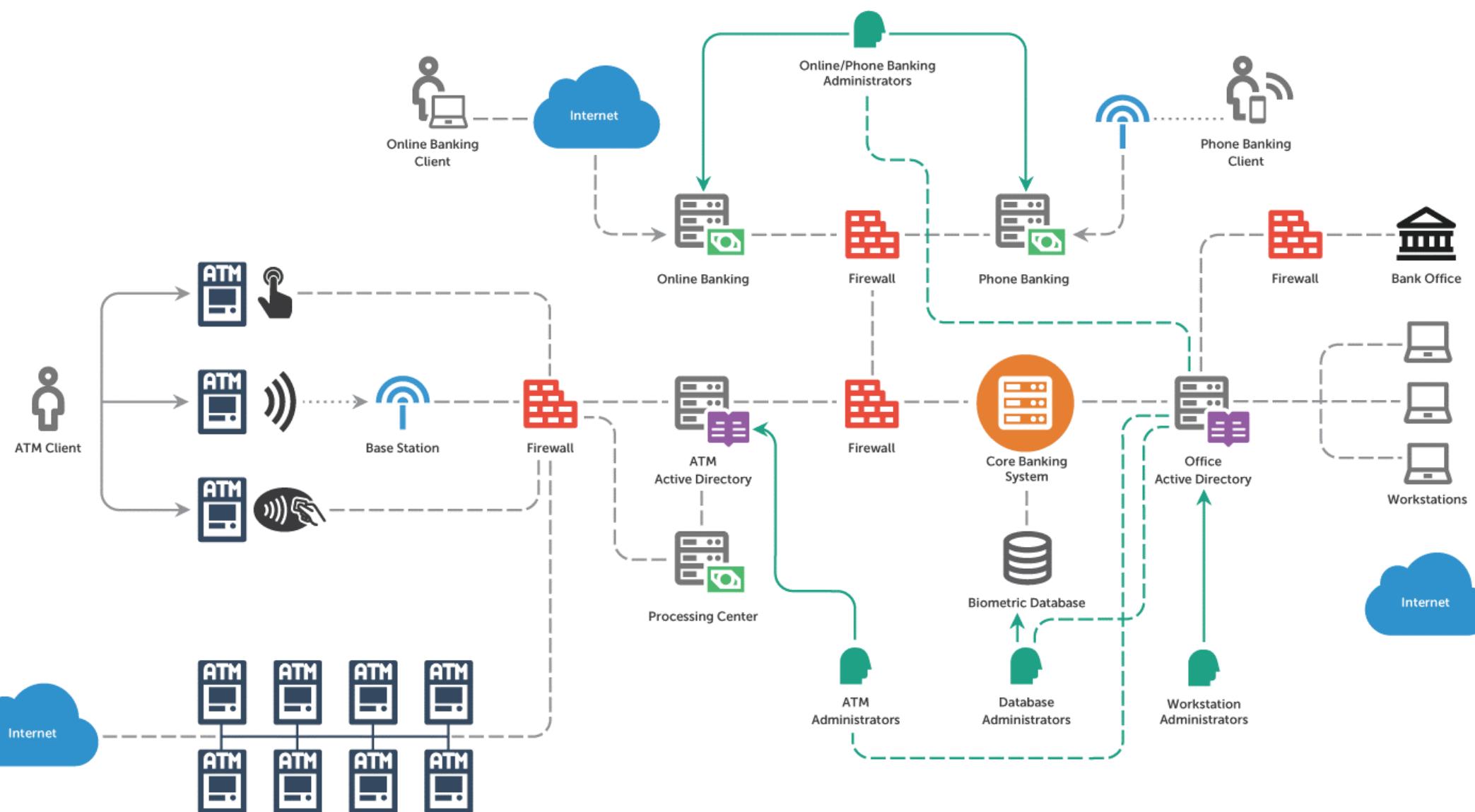
Names:
ATM [REDACTED]
WORKGROUP <0x0>
ATH [REDACTED]
WORKGROUP <0x1e>

445 tcp smb

SMB Status
Authentication: enabled
SMB Version: 1
Capabilities: unicode,large-files,nt-smb,rpc-remote-api,nt-status,level2-oplocks,lock-and-read,nt-find,infolevel-passthru,large-readx,large-writex,lwio,extended-security

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



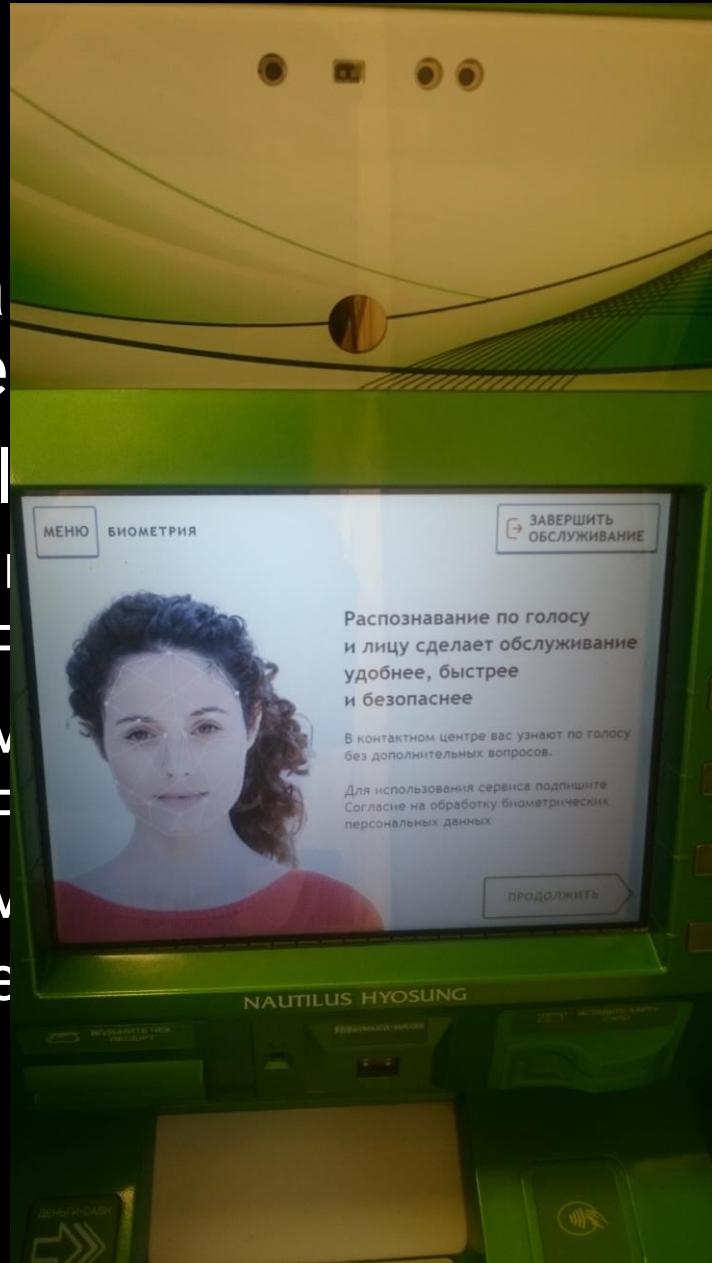
Now

- 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



- Gravity
- Use
- Multiple
- Hand
- Fingerprint
- Voice
- Facial
- Vein
- Eye



es of

Kudos

Security is a process

NO
FF
ONE
2019



THERE WILL ALWAYS BE SOMEONE WHO
SAYS THAT THEY CAN DO IT CHEAPER...



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