OWASP
Open Web Application
Security Project

How To Buy And Hack an ATM

Leigh-Anne Galloway & Timur Yunusov

About us

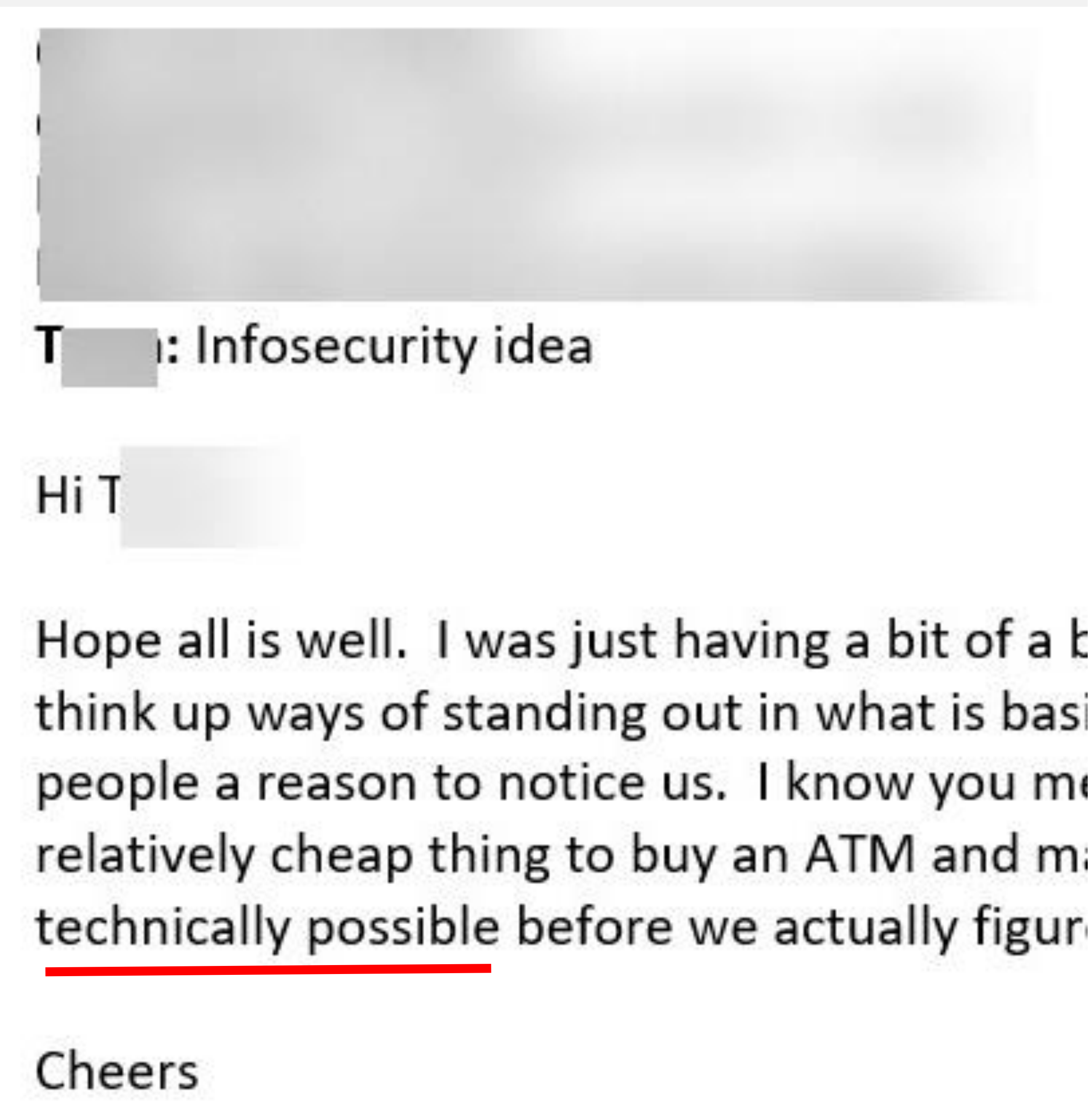
Appsec/websec/banksec/infosec

Incident response (payment investigation)

No experience with ATM acquisition

L_AGalloway

a66at



[redacted]

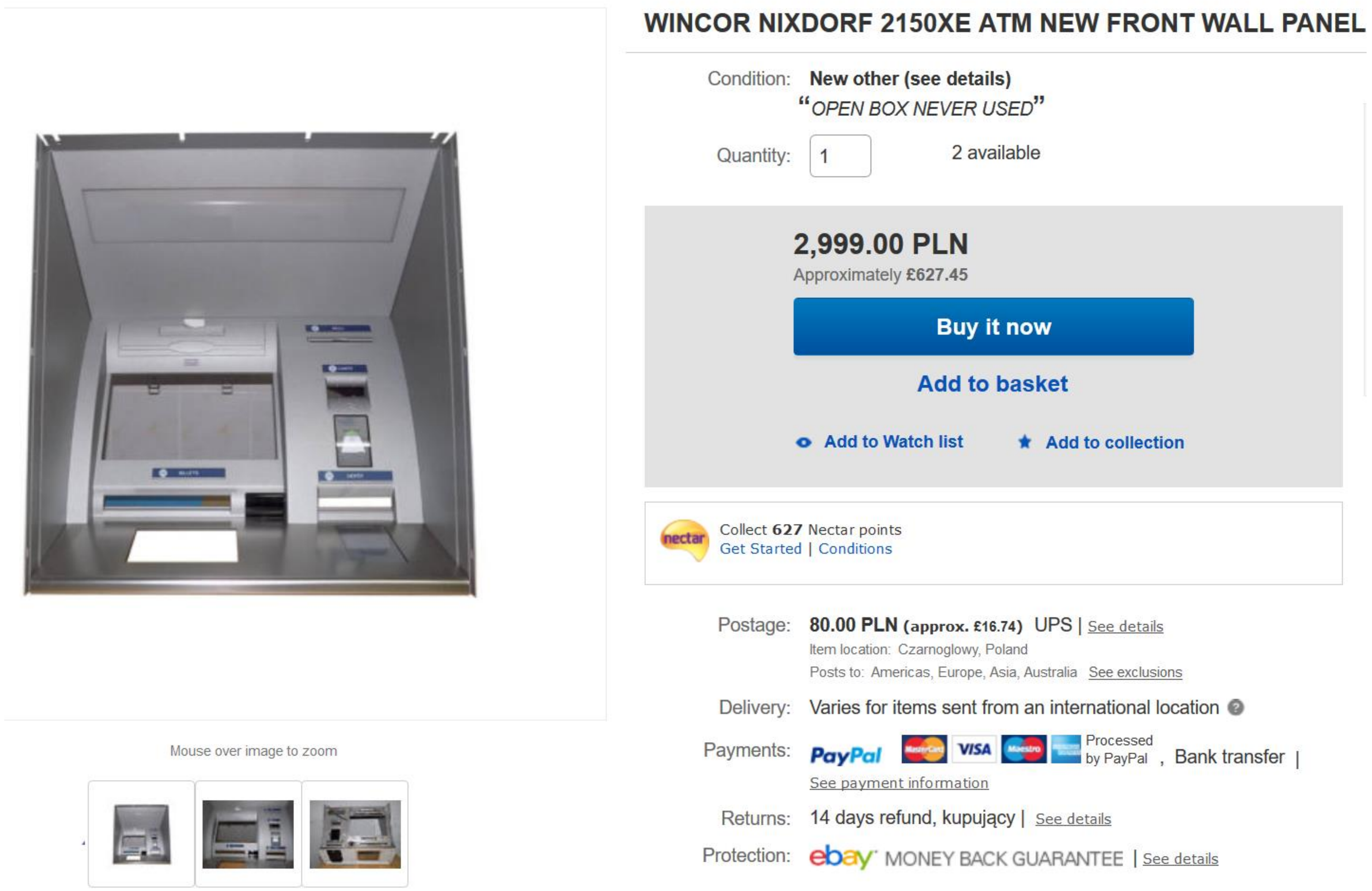
T[redacted]: Infosecurity idea

Hi T[redacted]

Hope all is well. I was just having a bit of a b
think up ways of standing out in what is basi
people a reason to notice us. I know you me
relatively cheap thing to buy an ATM and ma
technically possible before we actually figur

Cheers

THE BIRTH OF AN IDEA



WINCOR NIXDORF 2150XE ATM NEW FRONT WALL PANEL

Condition: **New other (see details)**
"*OPEN BOX NEVER USED*"

Quantity: 1 — 2 available

2,999.00 PLN
Approximately **£627.45**

Collect **627** Nectar points
Get Started | Conditions

Postage: **80.00 PLN (approx. £16.74)** UPS | See details
Item location: Czarnoglowy, Poland
Posts to: Americas, Europe, Asia, Australia See exclusions

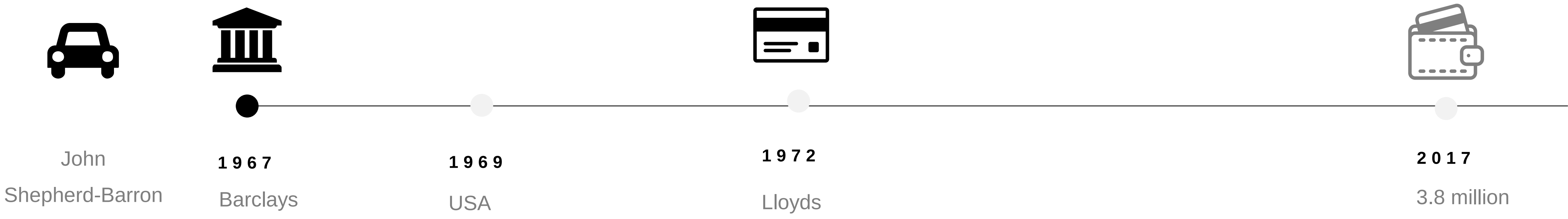
Delivery: Varies for items sent from an international location

Payments: PayPal, Processed by PayPal, Bank transfer |
See payment information

Returns: 14 days refund, kupujący | See details

Protection: ebay MONEY BACK GUARANTEE | See details

HISTORY OF ATM’S



John Shepherd-Barron

1967

Barclays

1969

USA

1972

Lloyds

2017

3.8 million

MANUFACTURERS

Identify market options

Where to buy an ATM

4 WAYS TO BUY AN ATM

LEGAL

ATM maintainers in your region, banks and manufacturers

GREY MARKET

Resellers, aftermarket listings, eBay, private sellers etc.

BLACK MARKET

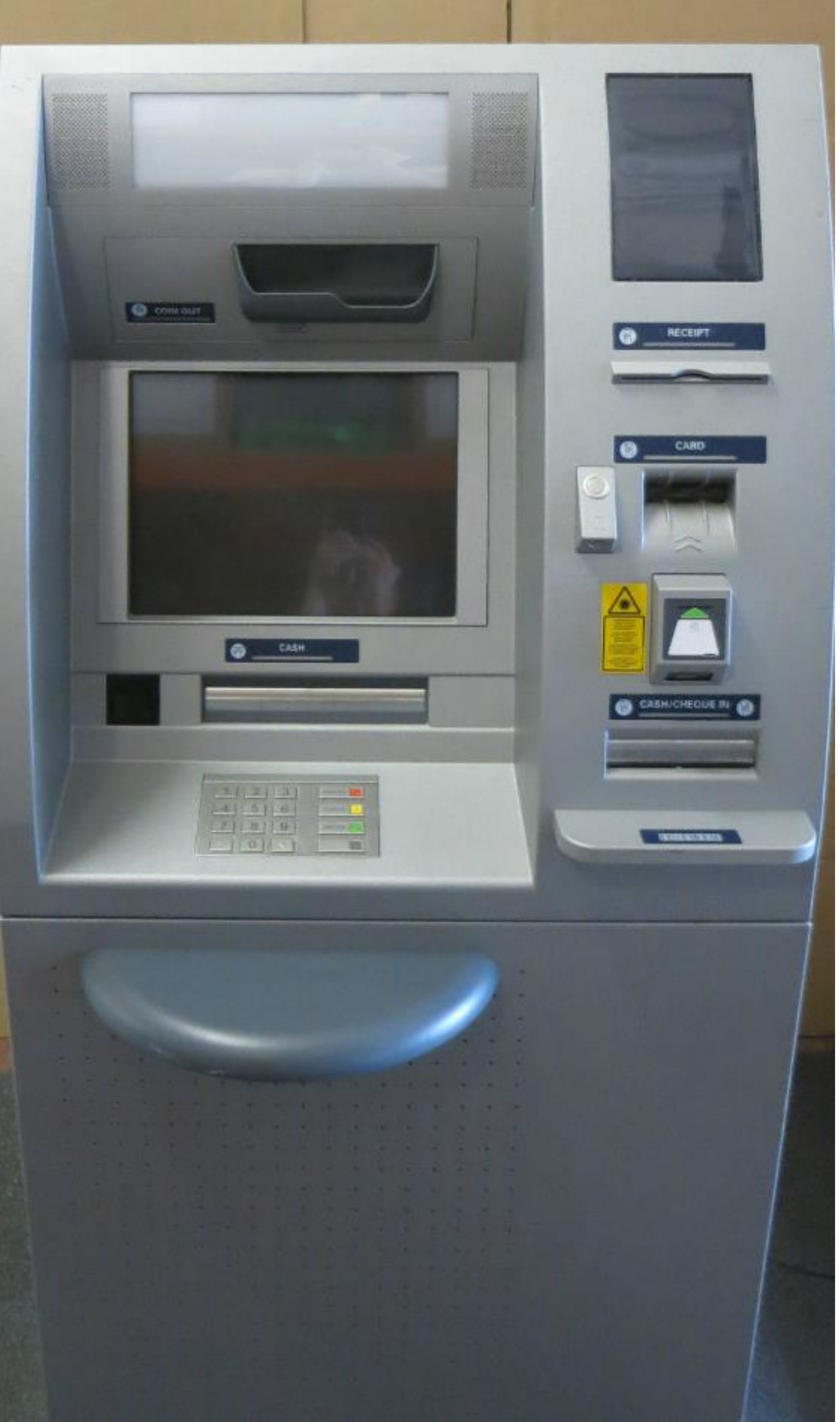
Underground market place

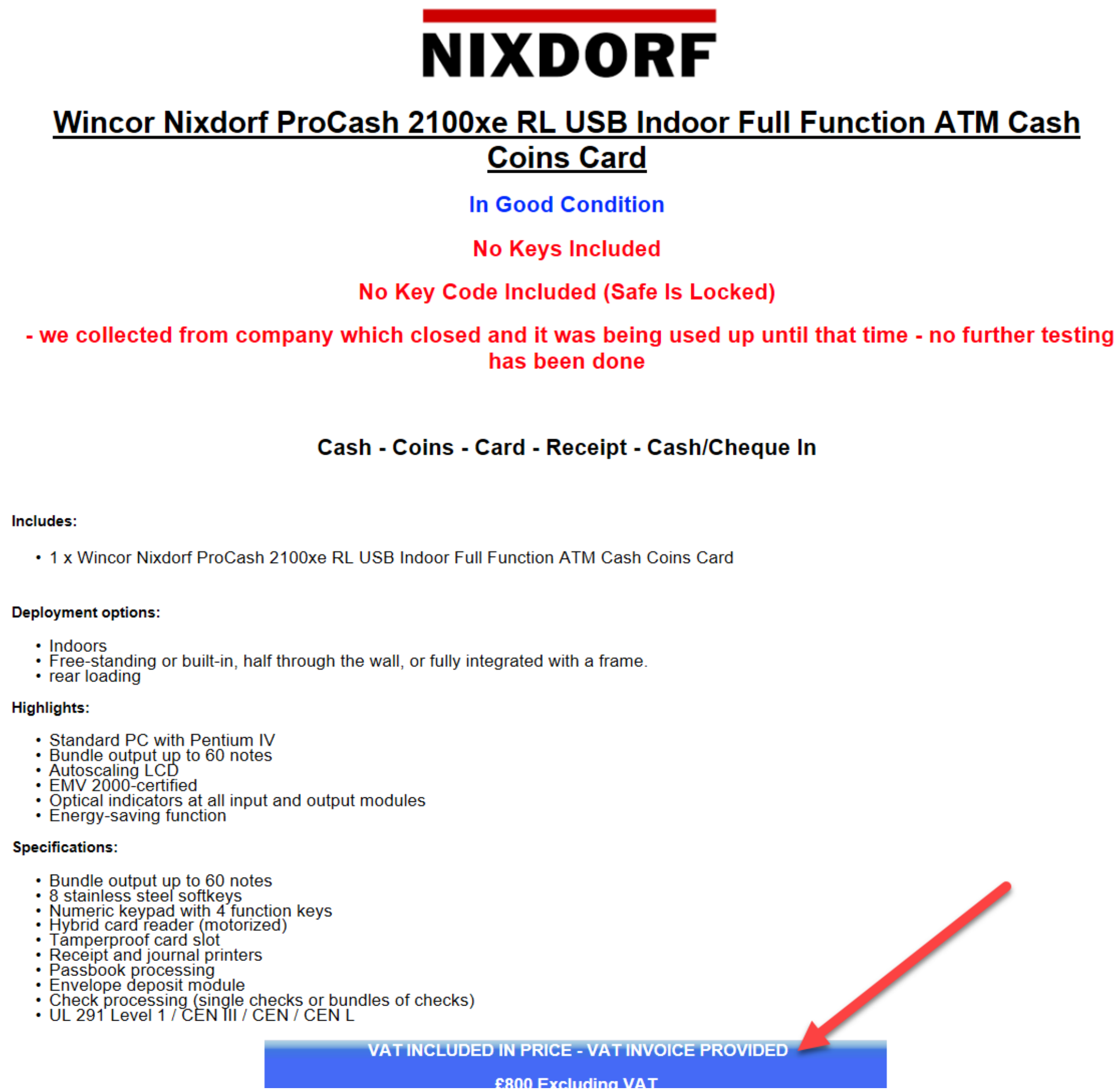
?

THE WILDCARD

Guaranteed ATM but with a possibility of imprisonment

Legal and Grey market options





NIXDORF

Wincor Nixdorf ProCash 2100xe RL USB Indoor Full Function ATM Cash Coins Card

In Good Condition

No Keys Included

No Key Code Included (Safe Is Locked)

- we collected from company which closed and it was being used up until that time - no further testing has been done

Cash - Coins - Card - Receipt - Cash/Cheque In

Includes:

- 1 x Wincor Nixdorf ProCash 2100xe RL USB Indoor Full Function ATM Cash Coins Card

Deployment options:

- Indoors
- Free-standing or built-in, half through the wall, or fully integrated with a frame.
- rear loading

Highlights:

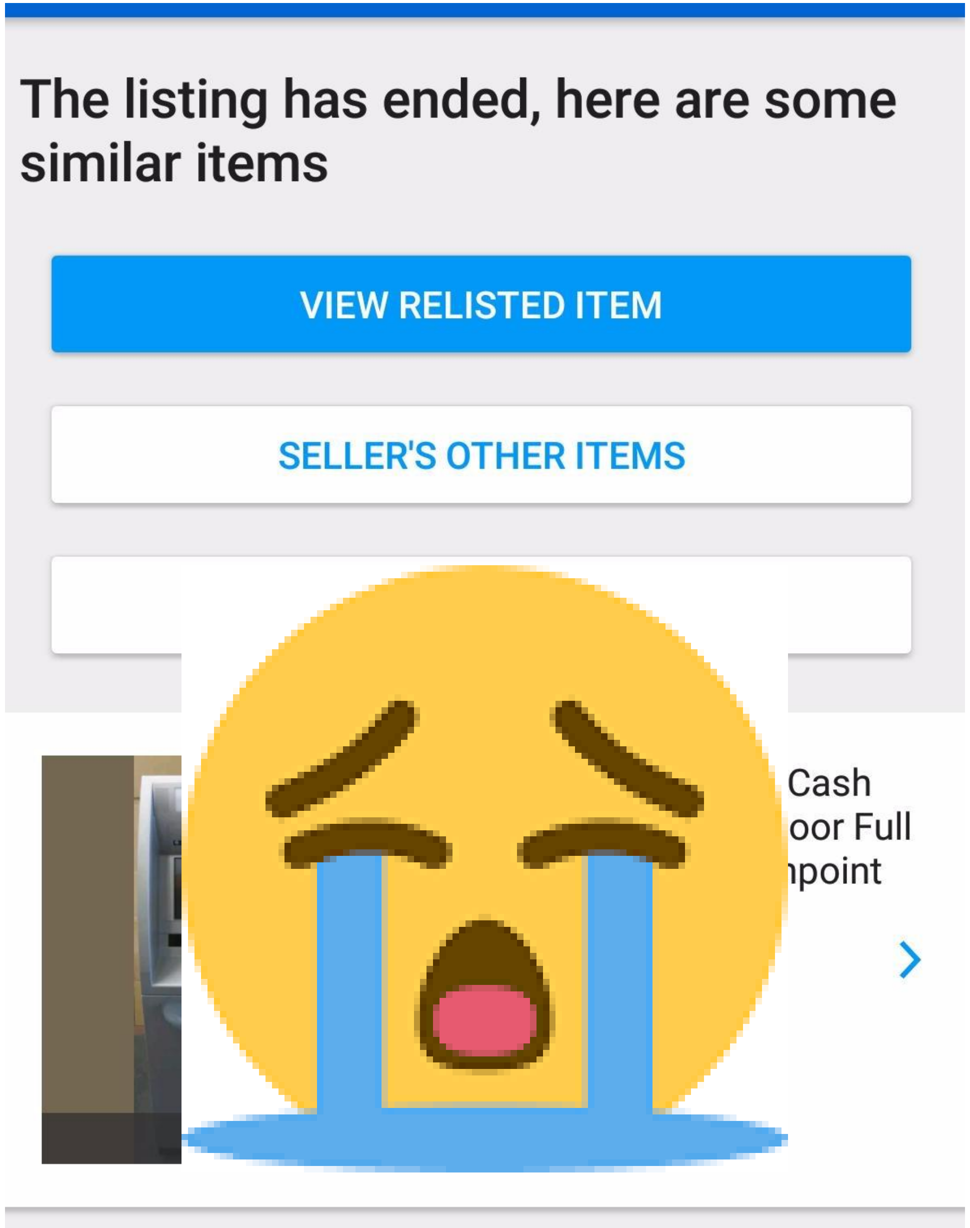
- Standard PC with Pentium IV
- Bundle output up to 60 notes
- Autoscaling LCD
- EMV 2000-certified
- Optical indicators at all input and output modules
- Energy-saving function

Specifications:

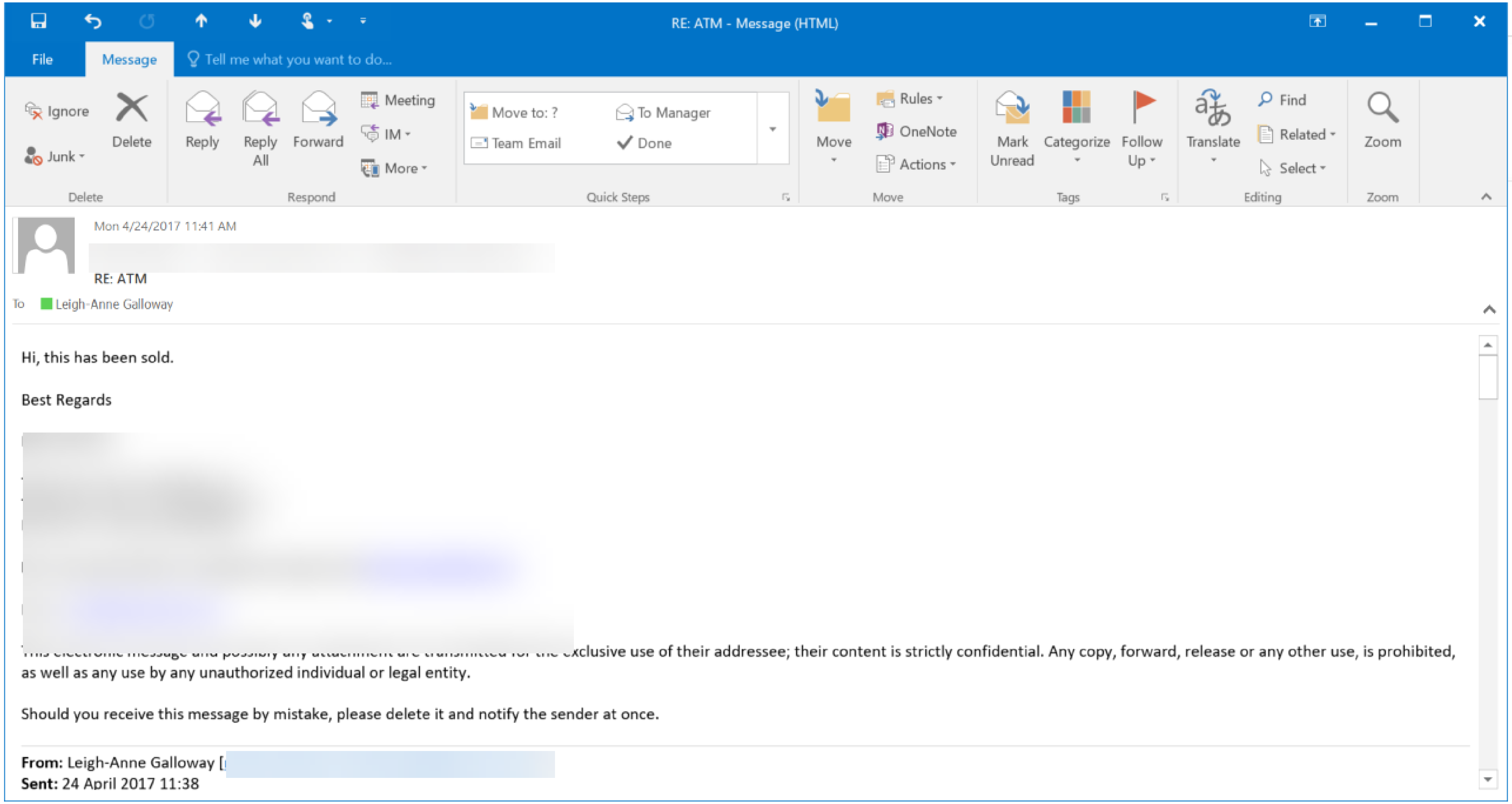
- Bundle output up to 60 notes
- 8 stainless steel softkeys
- Numeric keypad with 4 function keys
- Hybrid card reader (motorized)
- Tamperproof card slot
- Receipt and journal printers
- Passbook processing
- Envelope deposit module
- Check processing (single checks or bundles of checks)
- UL 291 Level 1 / CEN III / CEN / CEN L

VAT INCLUDED IN PRICE - VAT INVOICE PROVIDED

£800 Excluding VAT



The listing has ended, here are some similar items



Mon 4/24/2017 11:41 AM

[redacted]

RE: ATM

To 🟩 Leigh-Anne Galloway

Hi, this has been sold.

Best Regards

[redacted]

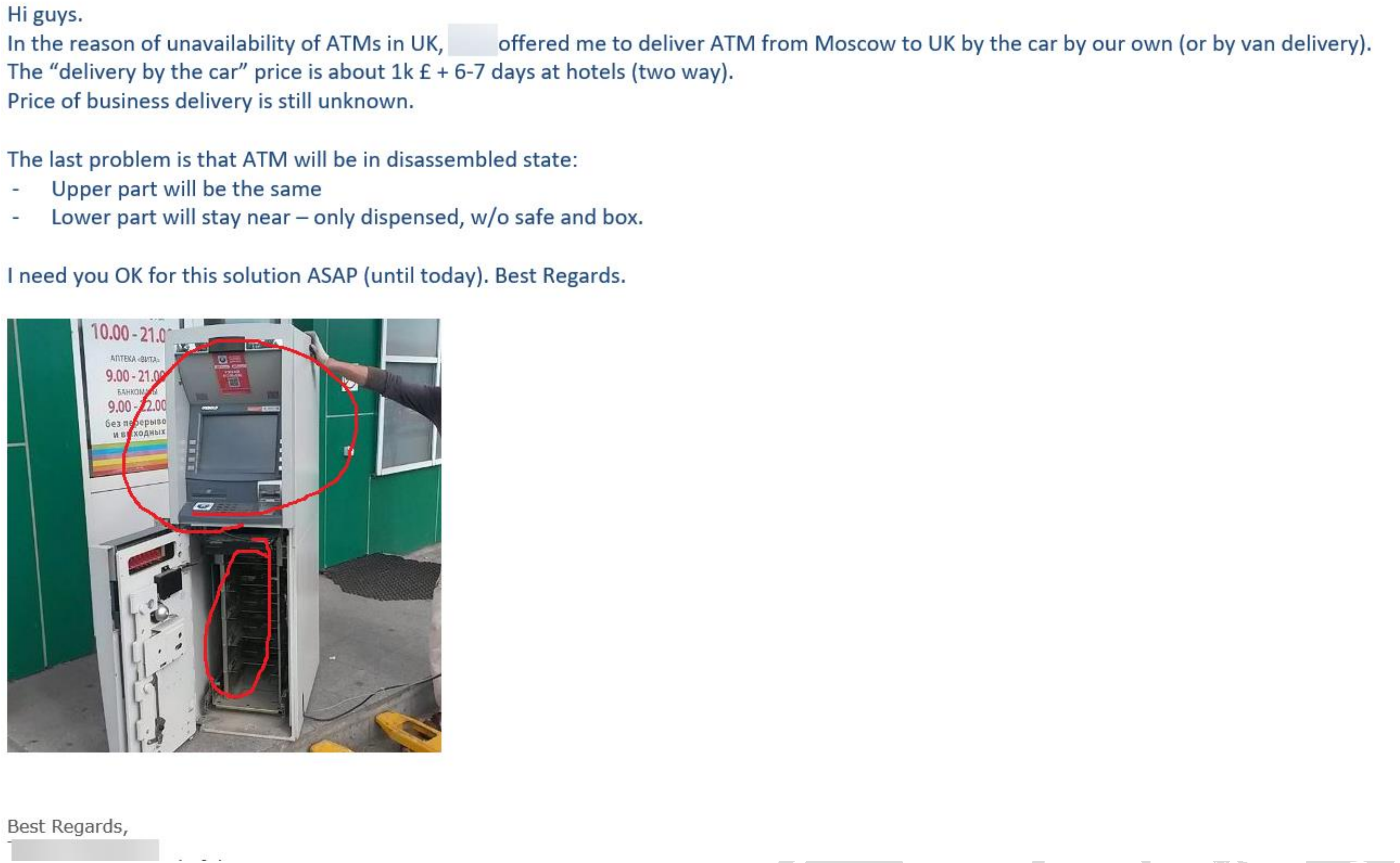
This electronic message and possibly any attachment are transmitted for the exclusive use of their addressee; their content is strictly confidential. Any copy, forward, release or any other use, is prohibited, as well as any use by any unauthorized individual or legal entity.

Should you receive this message by mistake, please delete it and notify the sender at once.

From: Leigh-Anne Galloway [[redacted]
Sent: 24 April 2017 11:38

The wildcard option

Our CEO endorses the craziest ideas



Hi guys.
In the reason of unavailability of ATMs in UK, [redacted] offered me to deliver ATM from Moscow to UK by the car by our own (or by van delivery).
The “delivery by the car” price is about 1k £ + 6-7 days at hotels (two way).
Price of business delivery is still unknown.

The last problem is that ATM will be in disassembled state:

- Upper part will be the same
- Lower part will stay near – only dispensed, w/o safe and box.

I need you OK for this solution ASAP (until today). Best Regards.

Best Regards,
[redacted]

Legal procurement

The easiest option

HUSTLE

VERIFY AKA SOCIAL ENGINEERING

You need to convince a company that you are a legitimate company or have a story that is believable. You might need to establish an account just for one item.

FACTOR IN LEAD TIME

Most of these suppliers know when stock is due to come in. They might not have what you are looking for straight away

KNOW THY ATM

You need to know the exact model and specification, cassette configuration. Free-standing is your best option.

LOGISTICS

Do you have a suitable place to store this? More on that later.

NCR 5877

NCR 6676 Cash in

NCR 6622 self service

Wincor 1500XE USB

Wincor 2100 XE Cash in

Wincor 2000XE USB Cash out

TestLink™

Testlink Services Ltd

[redacted]

Order Confirmation

Order No	[redacted]	Order Date	23/05/2017
Contact		Customer Order No.	[redacted]

Customer

[redacted]

Delivery Address

[redacted]

Part Number	Description	Despatch By Date	Unit Cost	Qty	Net Total
ATM5877RA	5877 Rear access		2,600.00	1	2,600.00
	To be supplied cleaned, working and tested with a Pivat Core and a Refurbished EPP for testing purposes.				

Total Items	2,600.00
Carriage	55.00
Tax	531.00
Total	3,186.00

Ship By : Testlink Account
Courier : 1 Pallet

Currency GBP

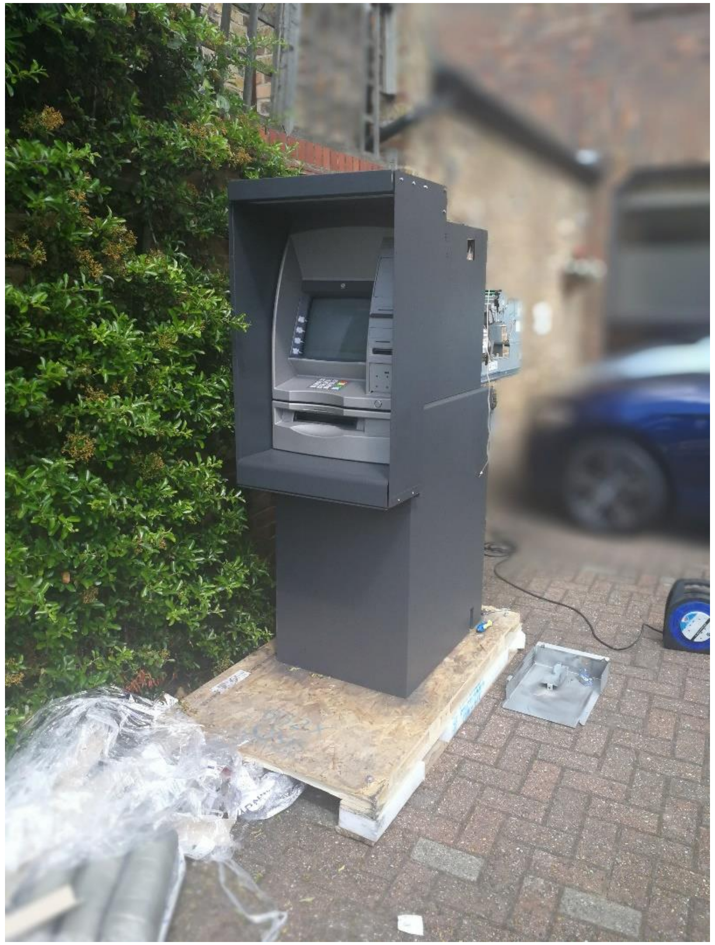
Logistics

A nightmare

DELIVERY DAY

EXPECTATIONS

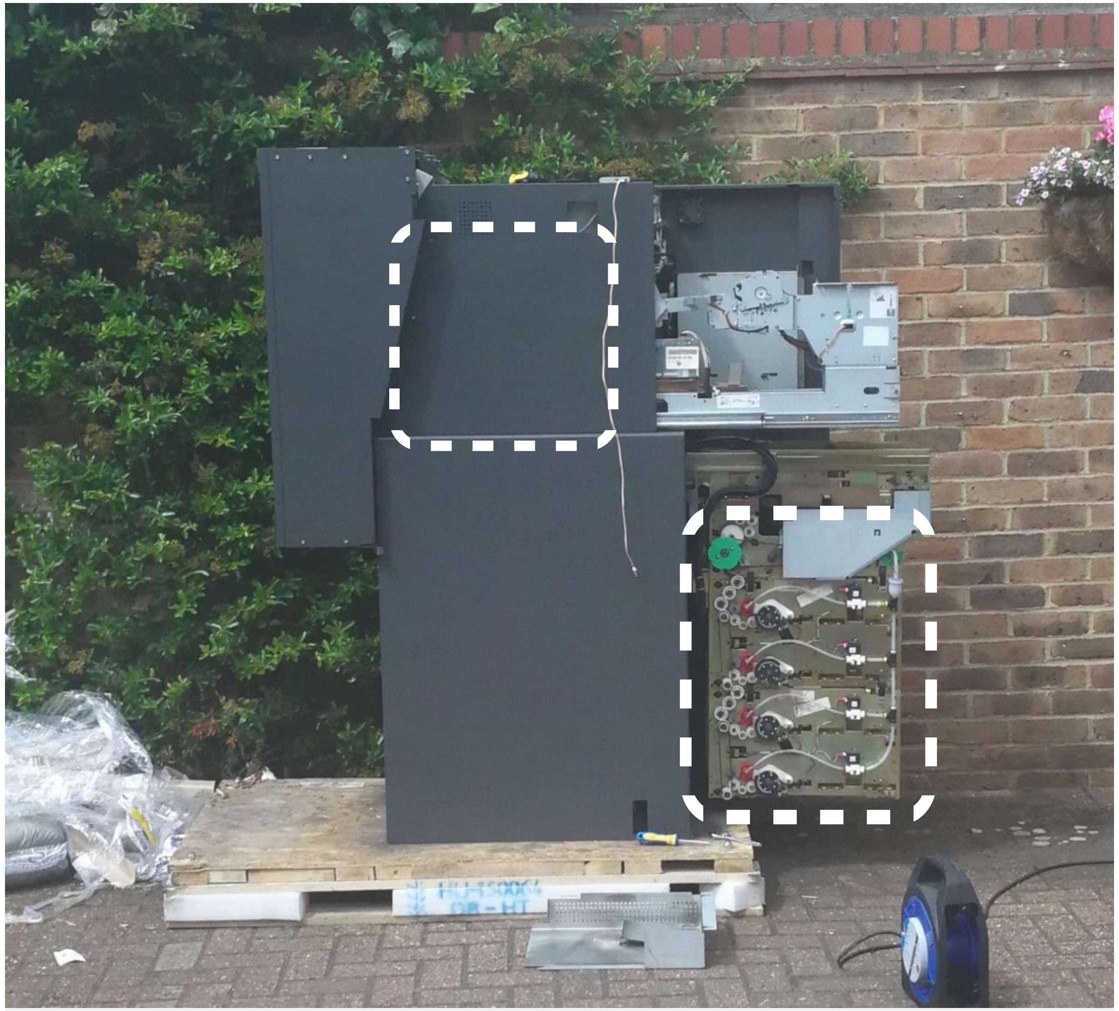
REALITY



POWER AND WEATHER

How does it work, how can I break it?

HOW IT WORKS



Card Reader/PIN pad (EPP)

Card reader and PIN pad verifies account holder

PC

Windows XP/7 80% variants of windows

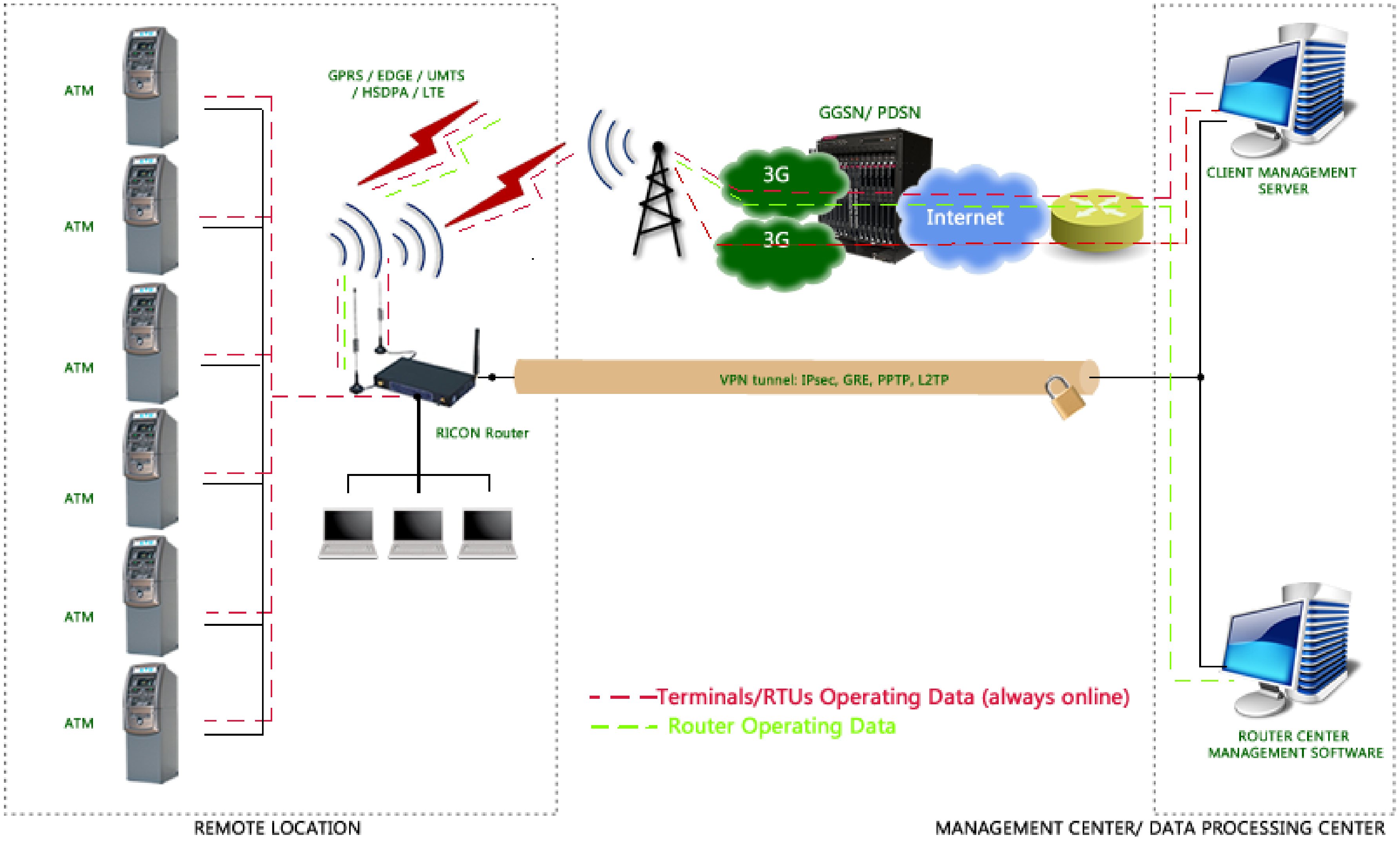
DISPENSER

PC sends instructions to dispenser which selects correct denomination from cassettes.

BANK NETWORK

ATM connects to core banking network directly or through inter bank network or via antennae.

ATM NETWORK


ATM
ATM
ATM
ATM
ATM
ATM
GPRS / EDGE / UMTS / HSDPA / LTE
RICON Router
3G
3G
GGSN/ PDSN
Internet
VPN tunnel: IPsec, GRE, PPTP, L2TP
CLIENT MANAGEMENT SERVER
ROUTER CENTER MANAGEMENT SOFTWARE
Terminals/RTUs Operating Data (always online)
Router Operating Data
REMOTE LOCATION
MANAGEMENT CENTER/ DATA PROCESSING CENTER

ATTACK VECTORS

BRUTE FORCE

Requires somehow getting physical access to the vault. The most popular methods being explosives

OS LEVEL

Operating level attacks take advantage of OS level config, Software vulnerabilities and bypassing kiosk mode

HARDWARE

Access via service area or drilling, bypassing OS and connecting blackbox directly to the dispenser etc

NETWORK

Making use of network: unauthorised VPN connection, malware, vulnerabilities in protocols

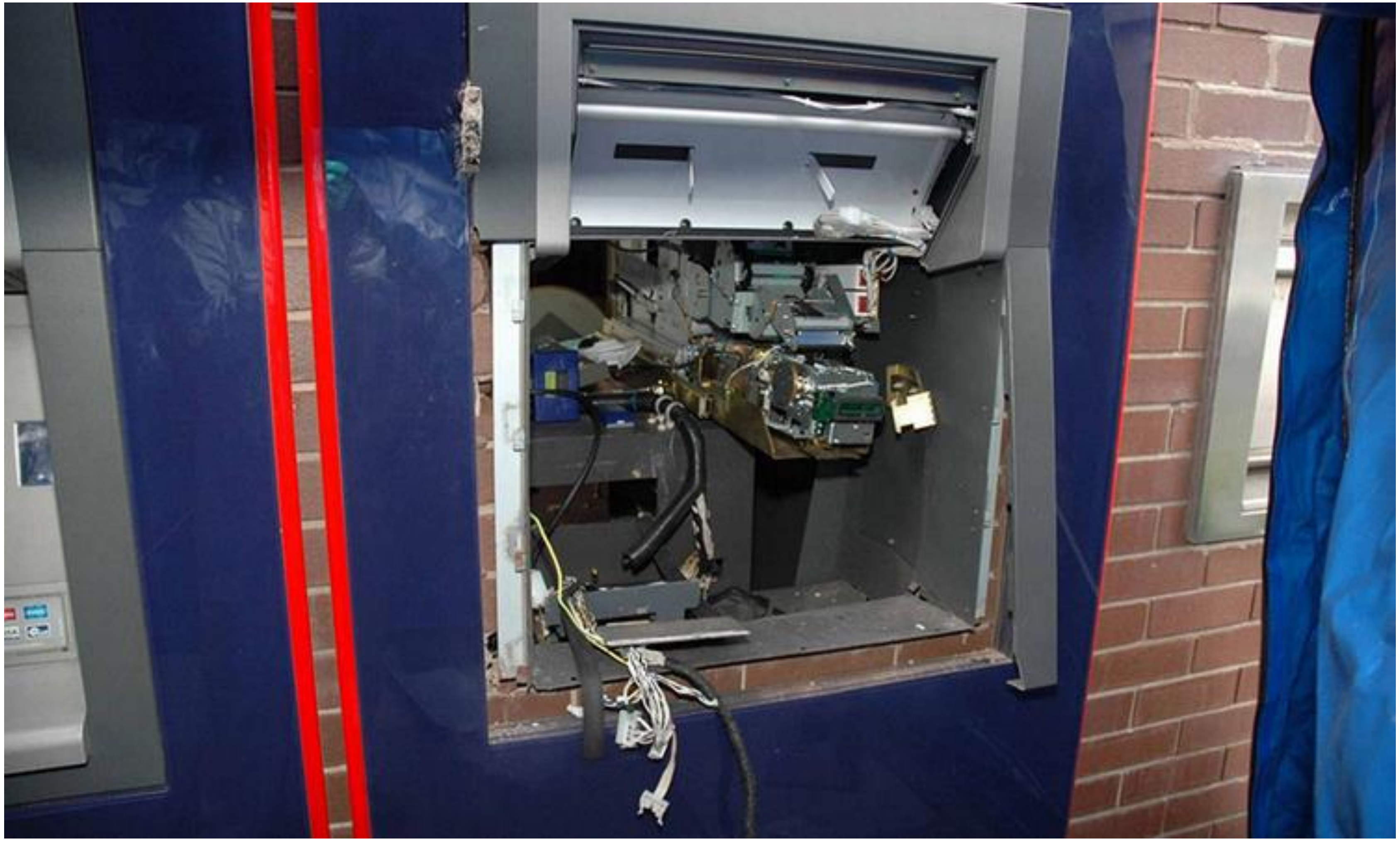
HISTORY OF ATTACKS

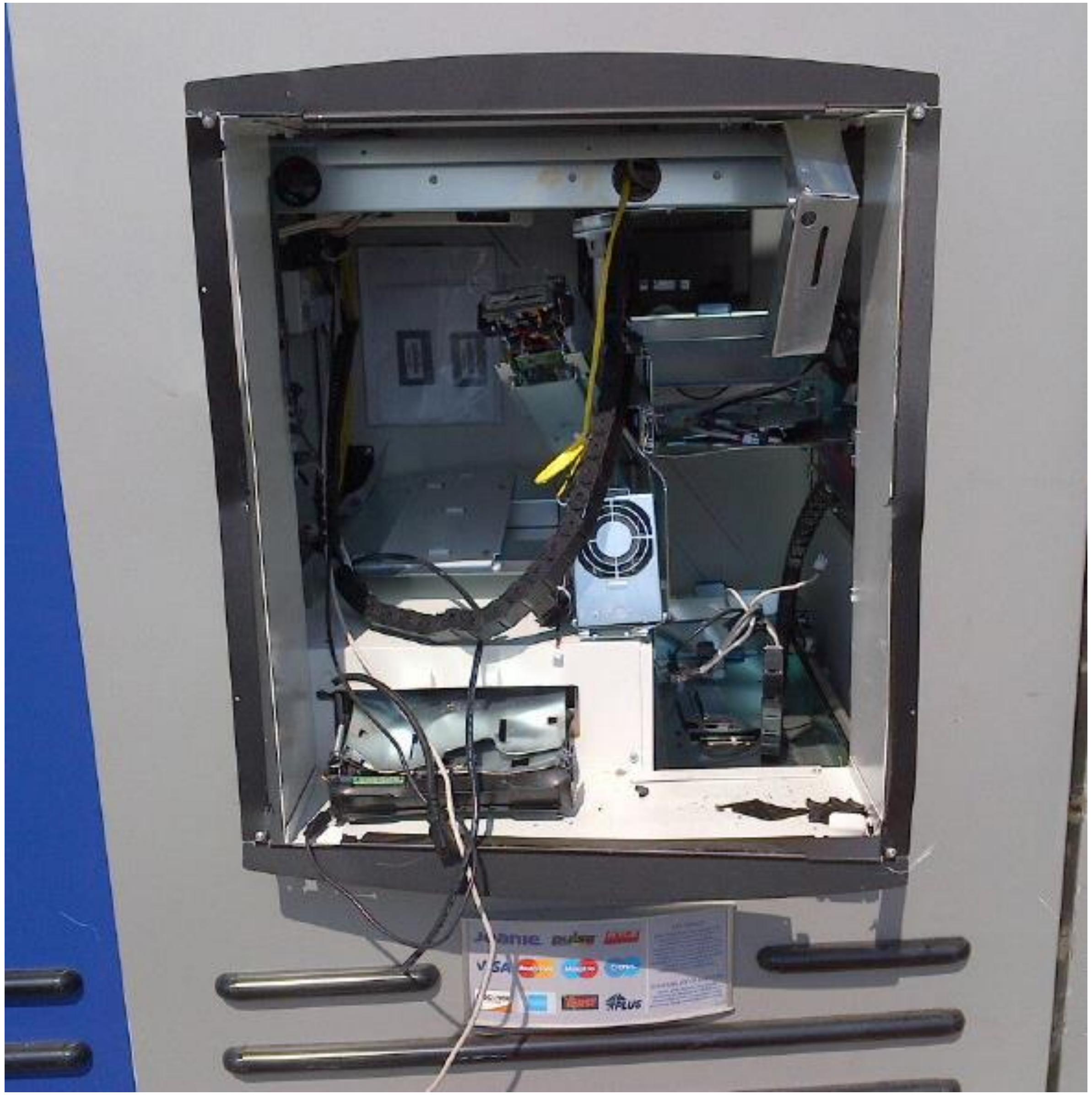
2010
Barnaby Jack

2012
Blackbox

2013
Logical Attacks

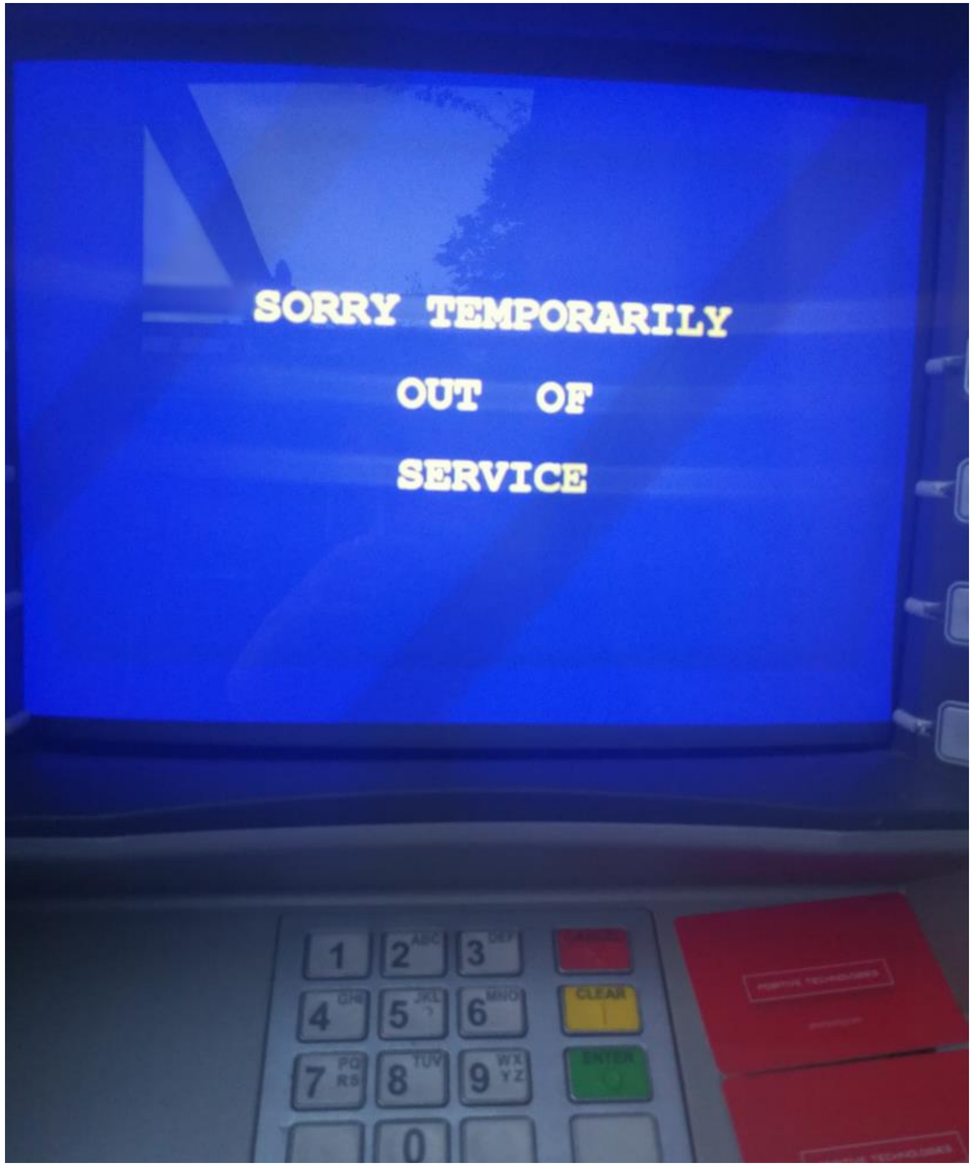
2014
PT published research



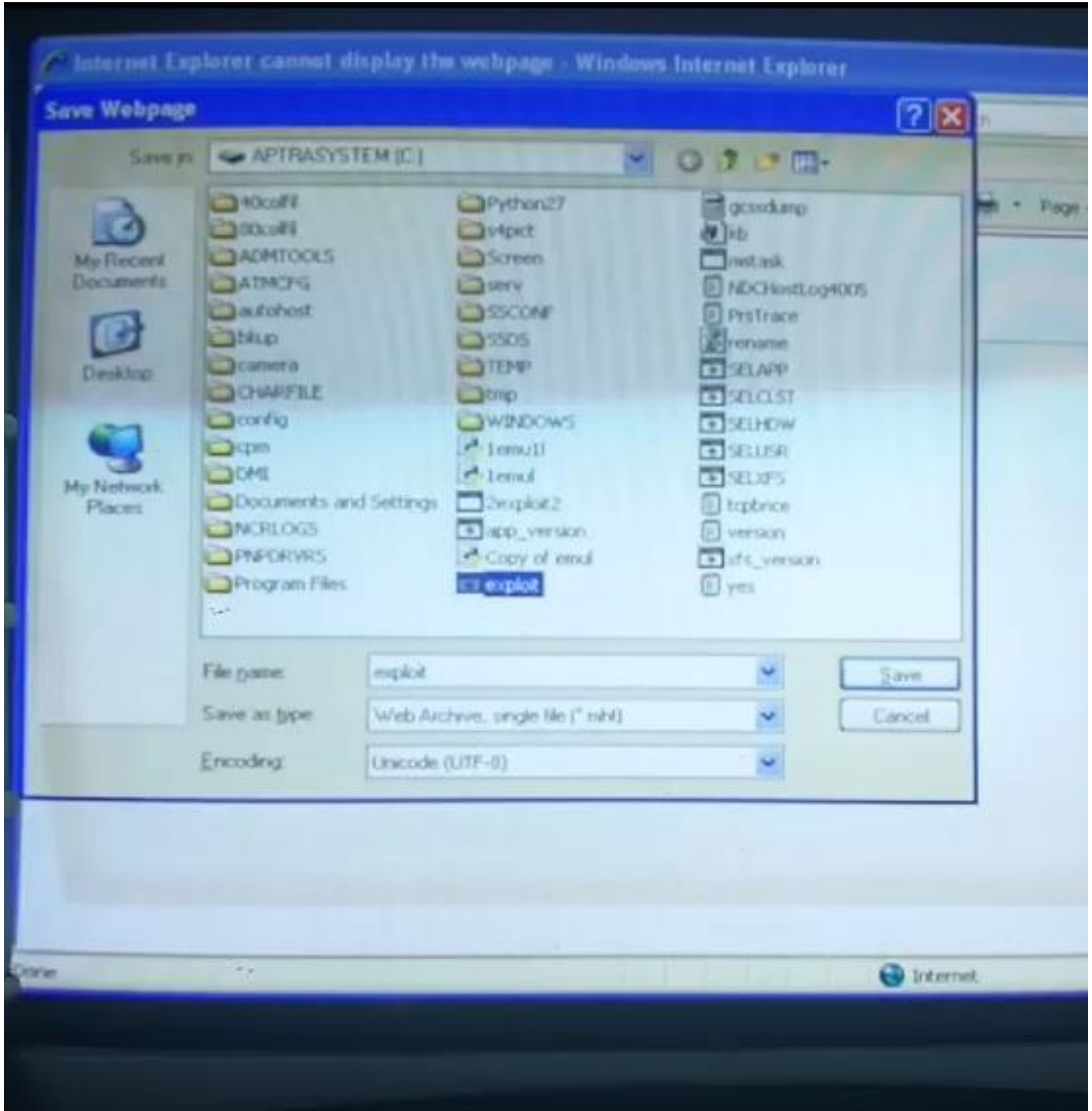

Jeanie
pulse
VISA
PLUS

C10
C10
RBS NatWest

OS LEVEL



SORRY TEMPORARILY OUT OF SERVICE



Internet Explorer cannot display the webpage - Windows Internet Explorer

Save Webpage

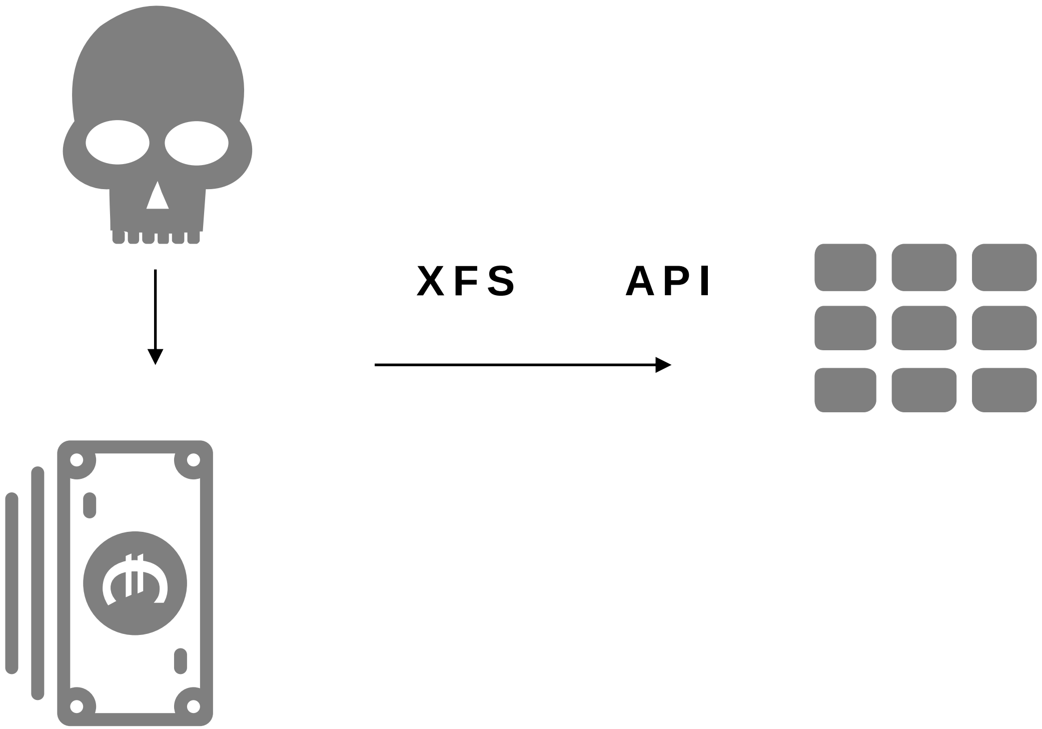
Save in: APTRASYSTEM (C:)

40colN
80colN
ADMTOOLS
ATMCFG
autohost
bkup
camera
CHARFILE
config
cpm
DMI
Documents and Settings
NCRLOGS
PNPDRVRS
Program Files
Python27
s4pict
Screen
serv
SSCONF
SSDS
TEMP
tmp
WINDOWS
1emu11
1emul
2exploit2
app_version
Copy of emul
exploit
gcsxdump
kb
netask
NDCHostLog4005
PrtTrace
rename
SELAPP
SELCLST
SELHOW
SELUSR
SELXFS
tcpbnce
version
xfs_version
yes

File name: exploit

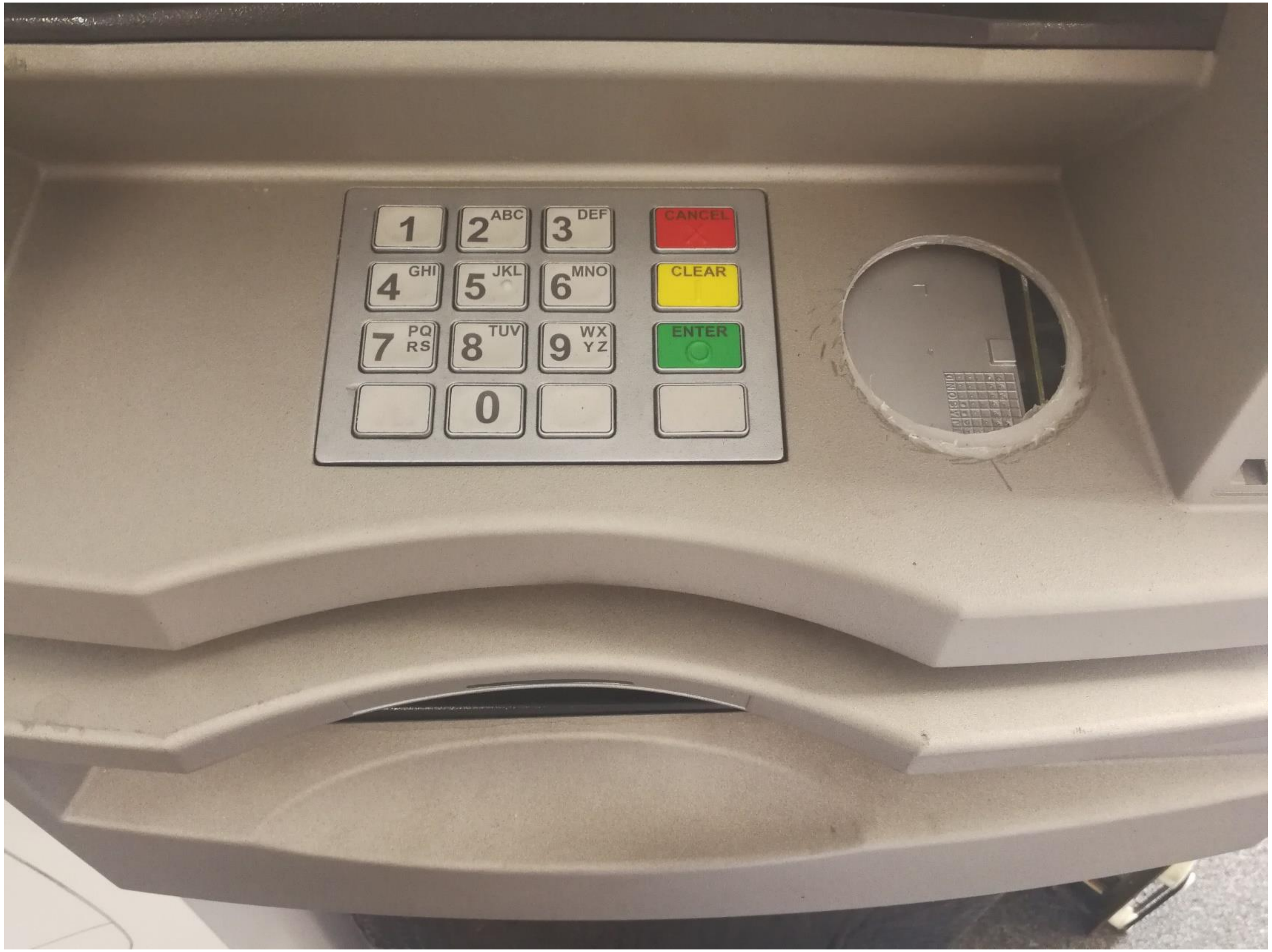
Save as type: Web Archive, single file (*.mht)

Encoding: Unicode (UTF-8)



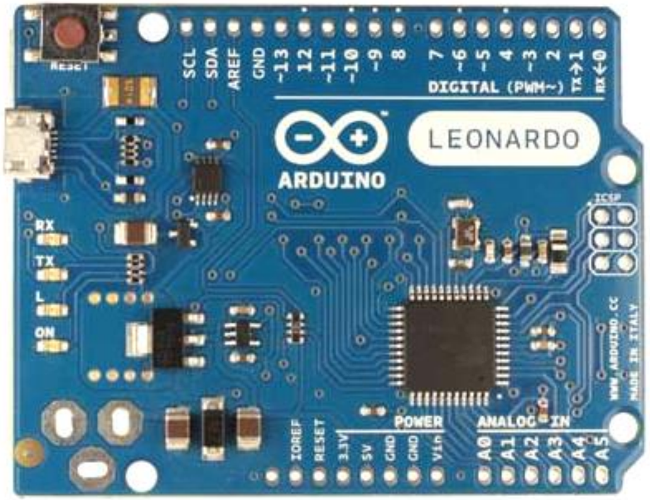
XFS API

HARDWARE

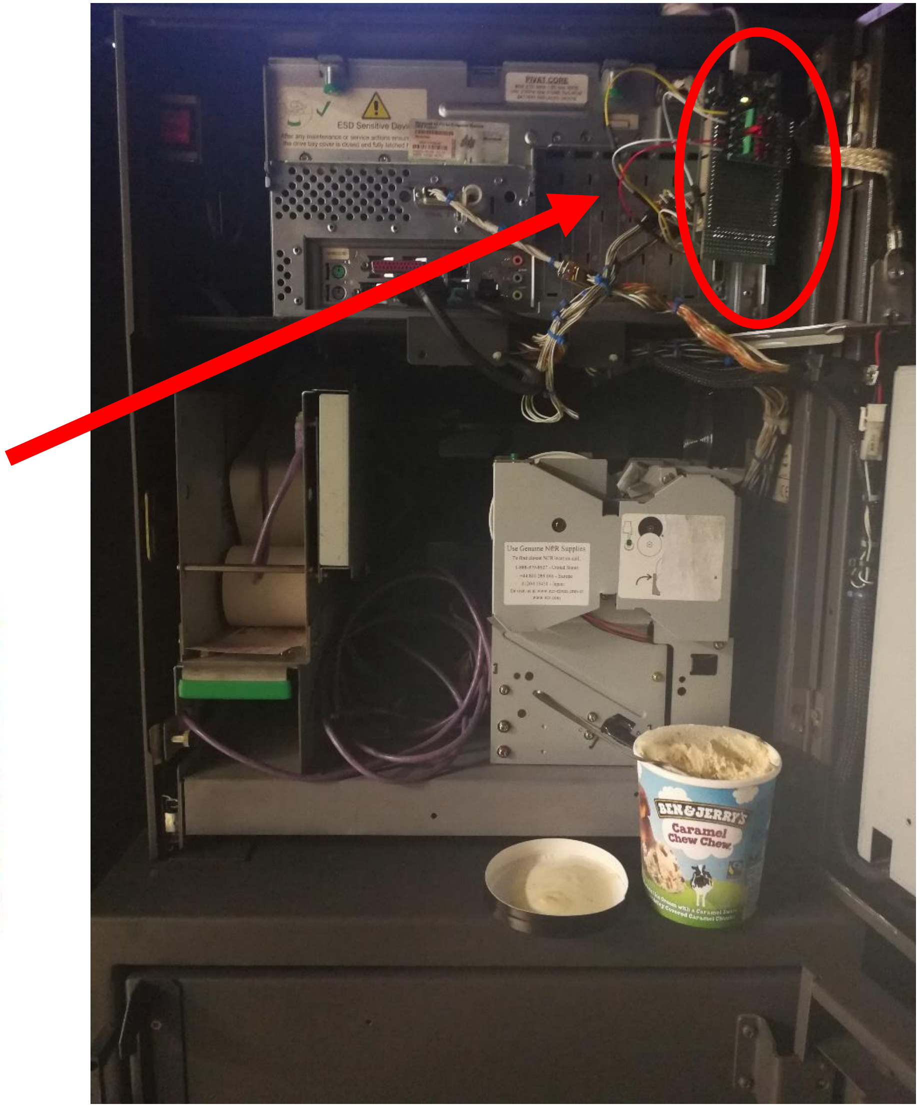

1
2 ABC
3 DEF
CANCEL
4 GHI
5 JKL
6 MNO
CLEAR
7 PQRS
8 TUV
9 WXYZ
ENTER
0

HARDWARE

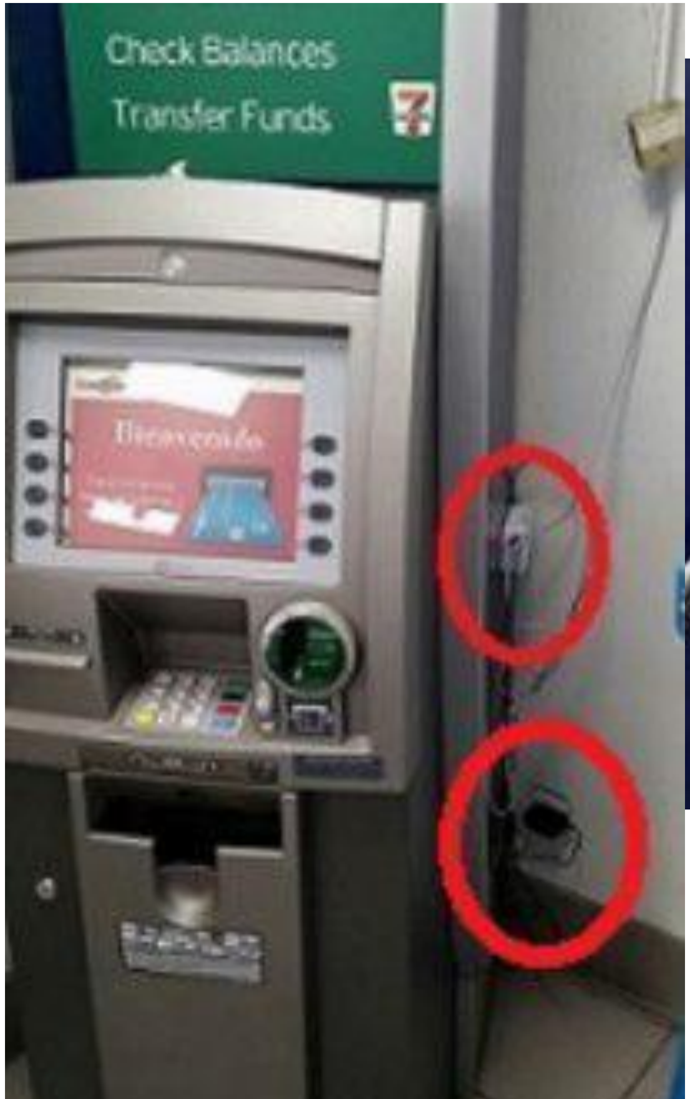
MK20DX256
VLH7

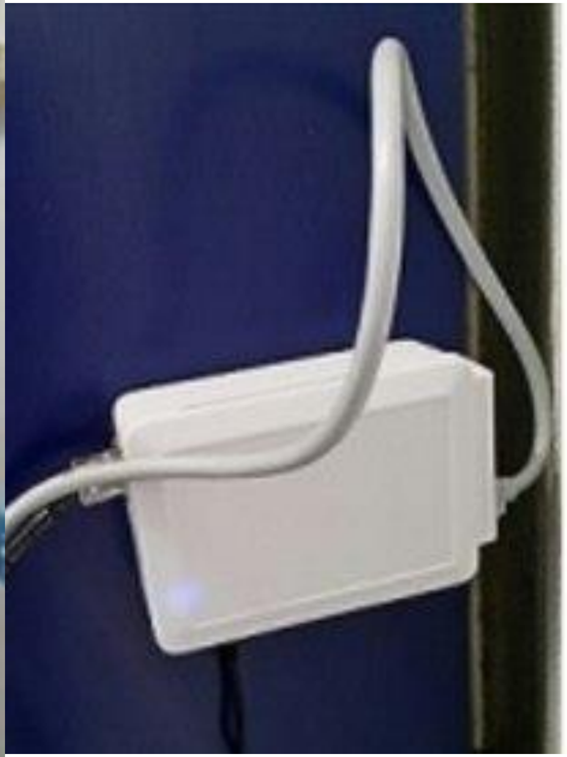


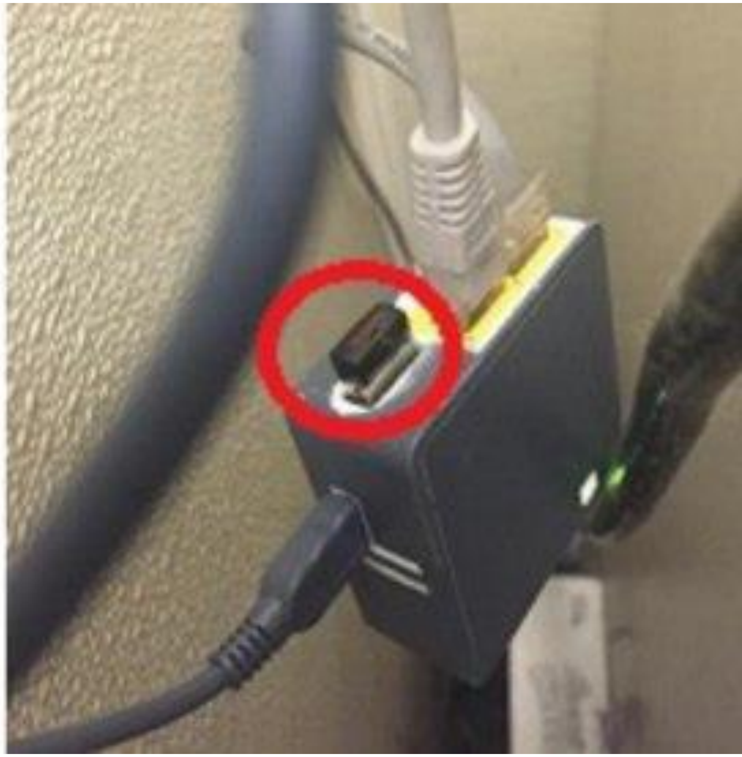
ARDUINO
LEONARDO
DIGITAL (PWM~)
POWER
ANALOG IN
RESET
ICSP



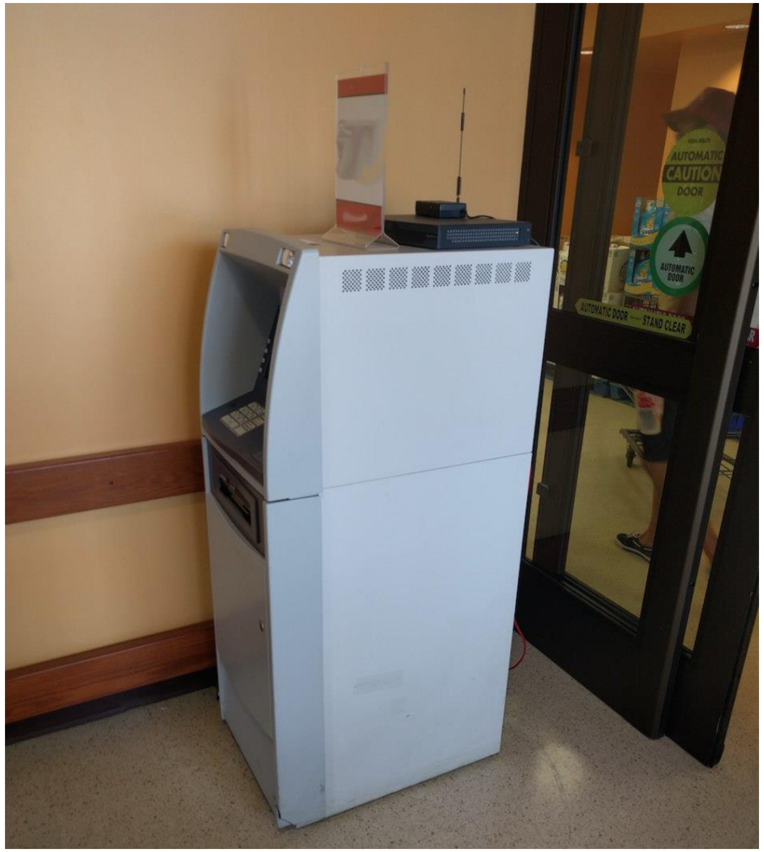
NETWORK

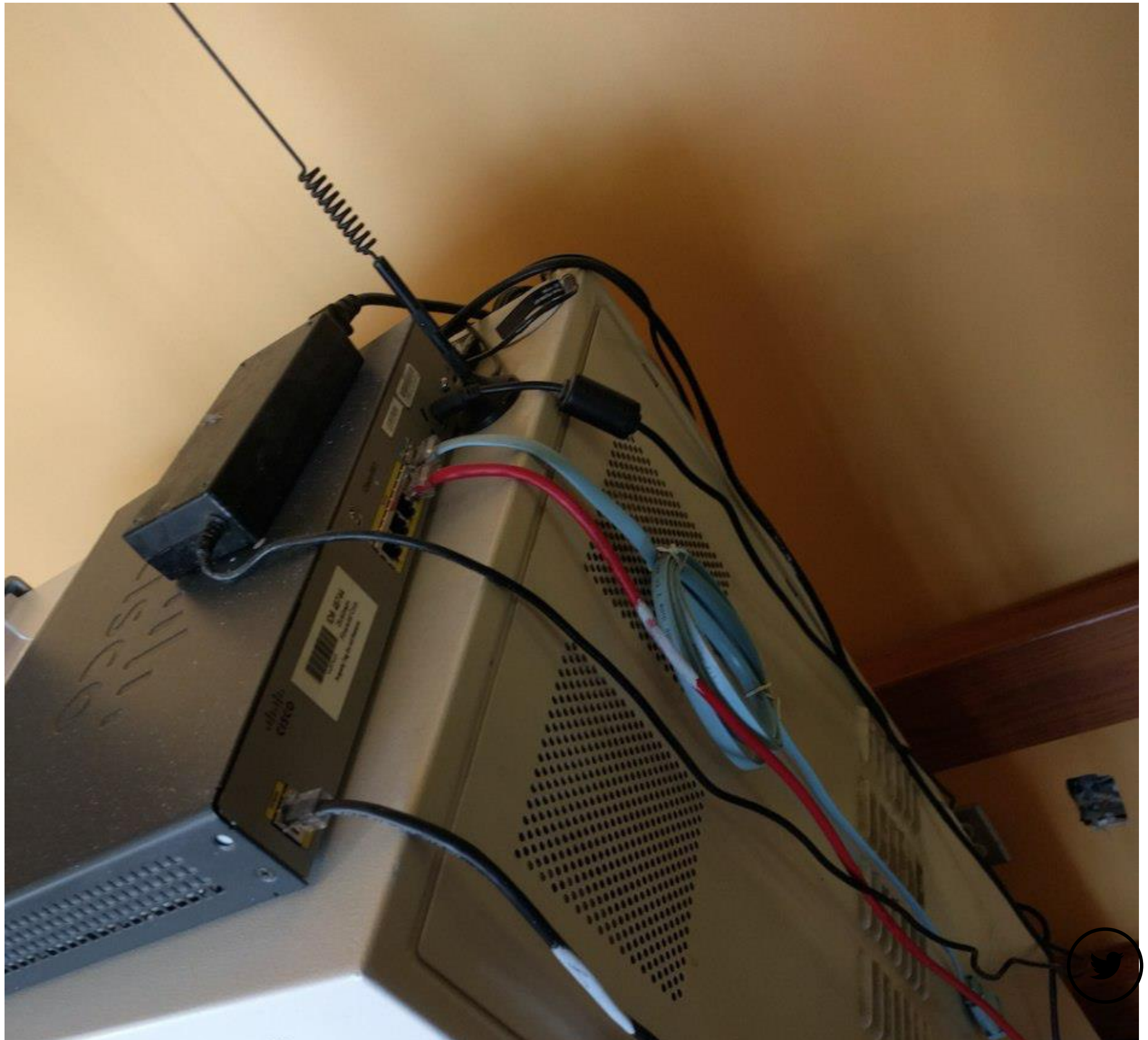






NETWORK


AUTOMATIC
CAUTION
DOOR
AUTOMATIC DOOR
AUTOMATIC DOOR STAND CLEAR


cisco

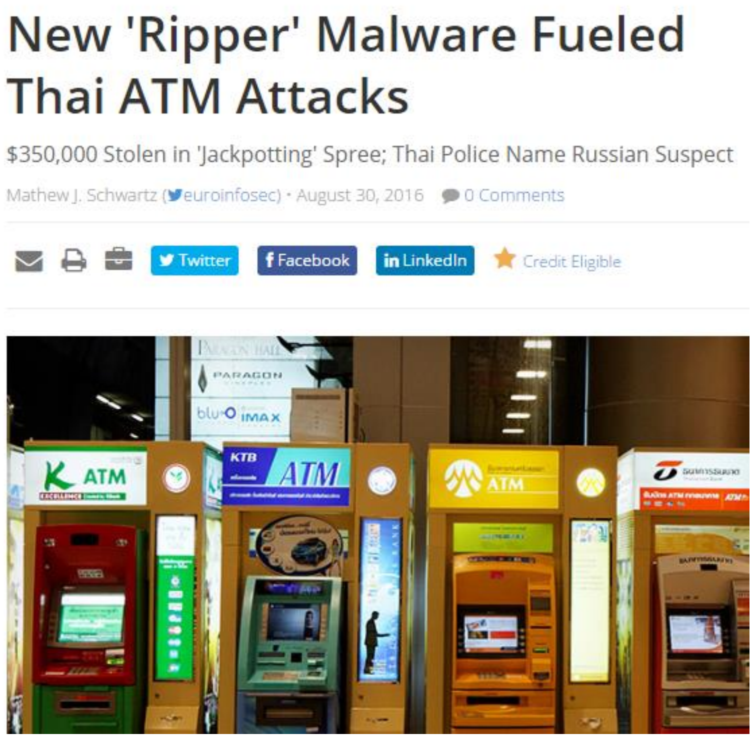
NETWORK

Euronet WORLDWIDE
ATM
change
Papír
paper

Beszállás To gates B1–B19
Beszállás To gates A1–A19
Euronet WORLDWIDE
ATM

ATMs everywhere

>20 ATMs over a last year



New 'Ripper' Malware Fueled Thai ATM Attacks

$350,000 Stolen in 'Jackpotting' Spree; Thai Police Name Russian Suspect

Mathew J. Schwartz (euroinfosec) • August 30, 2016 0 Comments

Application control for Application security

KASPERSKY lab McAfee™ gmv® INNOVATING SOLUTIONS Check Point® SOFTWARE TECHNOLOGIES LTD. TREND MICRO™

https://evi1cg.me/archives/AppLocker_Bypass_Techniques.html

https://cansecwest.com/slides/2016/CSW2016_Freingruber_Bypassing_Application_Whitelisting.pdf

https://www.ptsecurity.com/ww-en/about/news/131496/

https://www.ptsecurity.com/ww-en/about/news/240117/

https://www.ptsecurity.com/ww-en/about/news/283971/

https://embedi.com/blog/hack-atm-anti-hacking-feature-and-walk-away-1m-2-minutes/

Controls flow

vs

Whitelist of dirs (c:\windows\system32, etc)
Whitelist of files (c:\windows\system32\calc.exe, ipconfig.exe, etc)
Hash comparing (usually SHA-256)
Digital signatures (MS, Adobe, etc)
Extensions blacklist

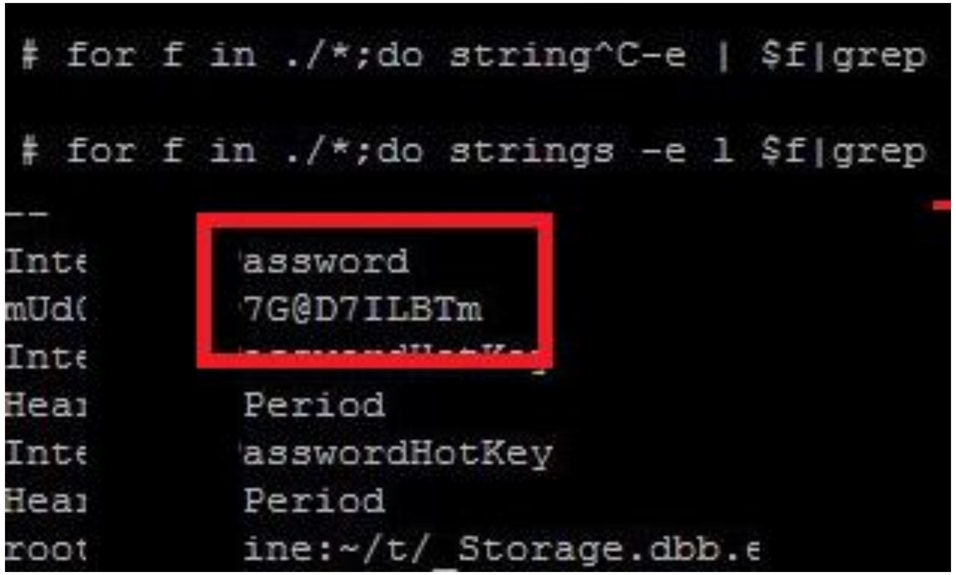
Bypassing techniques

Code execution in trusted apps (cmd, powershell)
Hash collisions
Bypassing extensions blacklist
Another trusted applications (.NET, Java, PHP, etc)
Misconfigurations
- DLL injections
- Poor restrictions(**CL_Invocation.ps1, CL_LoadingAssembly.ps1**)

Exploits

Attacking AppControls

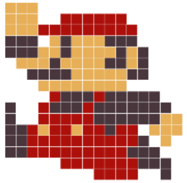
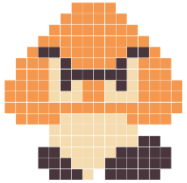
Product 1



```
# for f in ./*;do string^C-e | $f|grep

# for f in ./*;do strings -e l $f|grep
--
Inte        'assword
mUd(        '7G@D7ILBTm
Inte        'asswordHotKey
Hea1         Period
Inte        'asswordHotKey
Hea1         Period
root         ine:~/t/ Storage.dbb.e
```

1. **From admin to GOD**

2. **Hello from 90’th**  

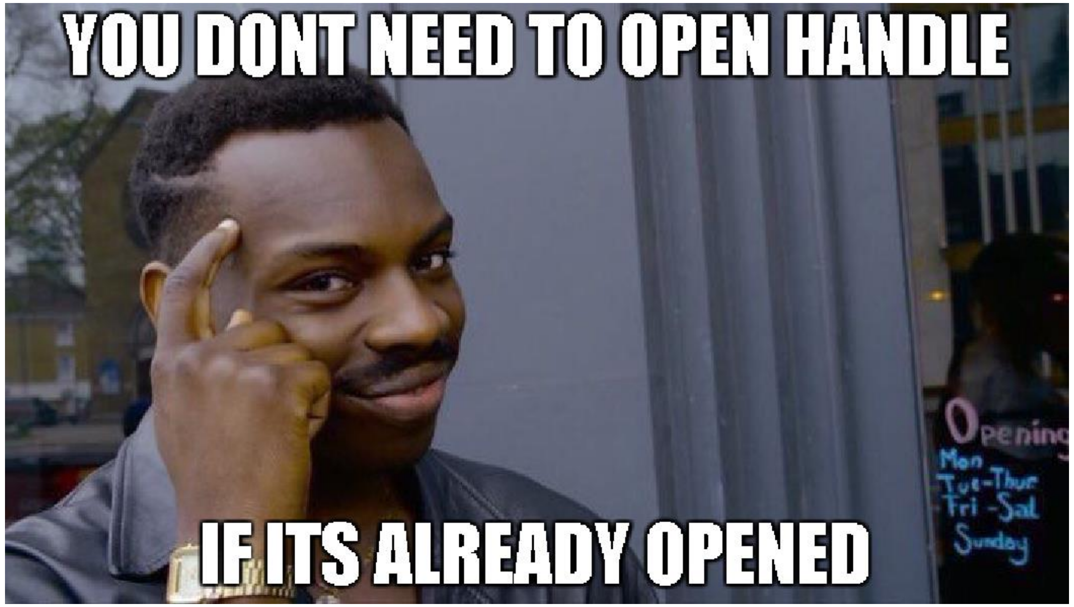
3. %SYSTEMROOT%\System32\msiexec.exe “signed.msi”

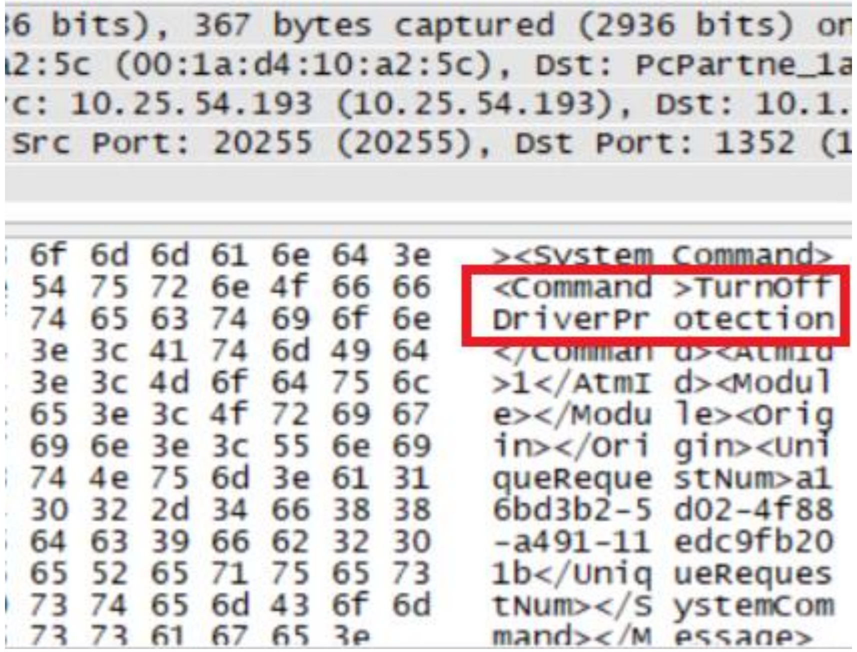
4. Updates over HTTP, no application level signatures

5. Updates with signatures. **Round 2, Fight! …**

Product 2

1. Very Safe Mode
2. Open HANDLE before product
3. Remote control over HTTP~~S~~
4. No application level signatures
5. Turning protection off || RCE
6. **Round 2. Fight!** MD5(command)
    1. *MD5(RCE || turnoff)*
    2. *Del Protector.sys*
    3. *No self-control*





```
6 bits), 367 bytes captured (2936 bits) on
2:5c (00:1a:d4:10:a2:5c), Dst: PcPartne_1a
c: 10.25.54.193 (10.25.54.193), Dst: 10.1.
Src Port: 20255 (20255), Dst Port: 1352 (1

 6f 6d 6d 61 6e 64 3e    ><System Command>
 54 75 72 6e 4f 66 66    <Command >TurnOff
 74 65 63 74 69 6f 6e    DriverPr otection
 3e 3c 41 74 6d 49 64    </Comman d><AtmId
 3e 3c 4d 6f 64 75 6c    >1</AtmI d><Modul
 65 3e 3c 4f 72 69 67    e></Modu le><Orig
 69 6e 3e 3c 55 6e 69    in></Ori gin><Uni
 74 4e 75 6d 3e 61 31    queReque stNum>a1
 30 32 2d 34 66 38 38    6bd3b2-5 d02-4f88
 64 63 39 66 62 32 30    -a491-11 edc9fb20
 65 52 65 71 75 65 73    1b</Uniq ueReques
 73 74 65 6d 43 6f 6d    tNum></S ystemCom
 73 73 61 67 65 3e       mand></M essage>
```

Very secure Product 3

Signatures, drivers and two smoking barrels

Checking algo:

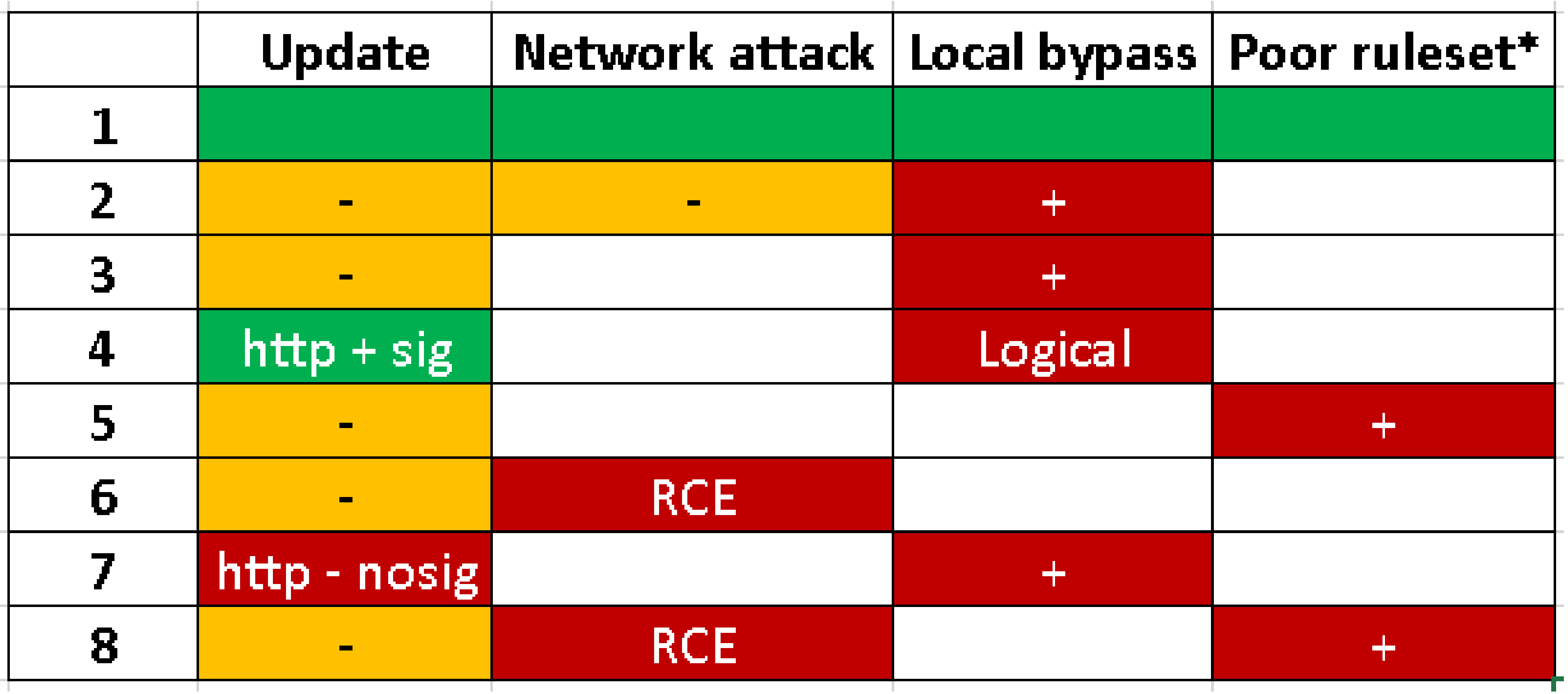
```
If checked(file)==false
    while(!timeout){Hashcalc(file);}
```

- Hashcalc(loo***0000***oong-exploit.exe) will be run once
- Hashcalc(py**T**h**0**n.exe) will be run multiple times

Products 4-5-6

1. Local unauthorised privileges escalation (you need to launch exploit.exe to bypass restrictions for launching exploit.exe)
2. Network-based BOF => RCE

Review



	Update	Network attack	Local bypass	Poor ruleset*
1	🟩	🟩	🟩	🟩
2	🟨 -	🟨 -	🟥 +	
3	🟨 -		🟥 +	
4	🟩 http + sig		🟥 Logical	
5	🟨 -			🟥 +
6	🟨 -	🟥 RCE		
7	🟥 http - nosig		🟥 +	
8	🟨 -	🟥 RCE		🟥 +

Review

	Update	Network attack	Local bypass	Poor ruleset*
1	🟩	🟩	🟩	🟩
2				
3				
4				
5				🟥
6				
7				
8				🟥

Industrial 3G modems

Different boxes, same vulnerabilities (http://blog.ptsecurity.com/2015/12/critical-vulnerabilities-in-3g4g-modems.html)

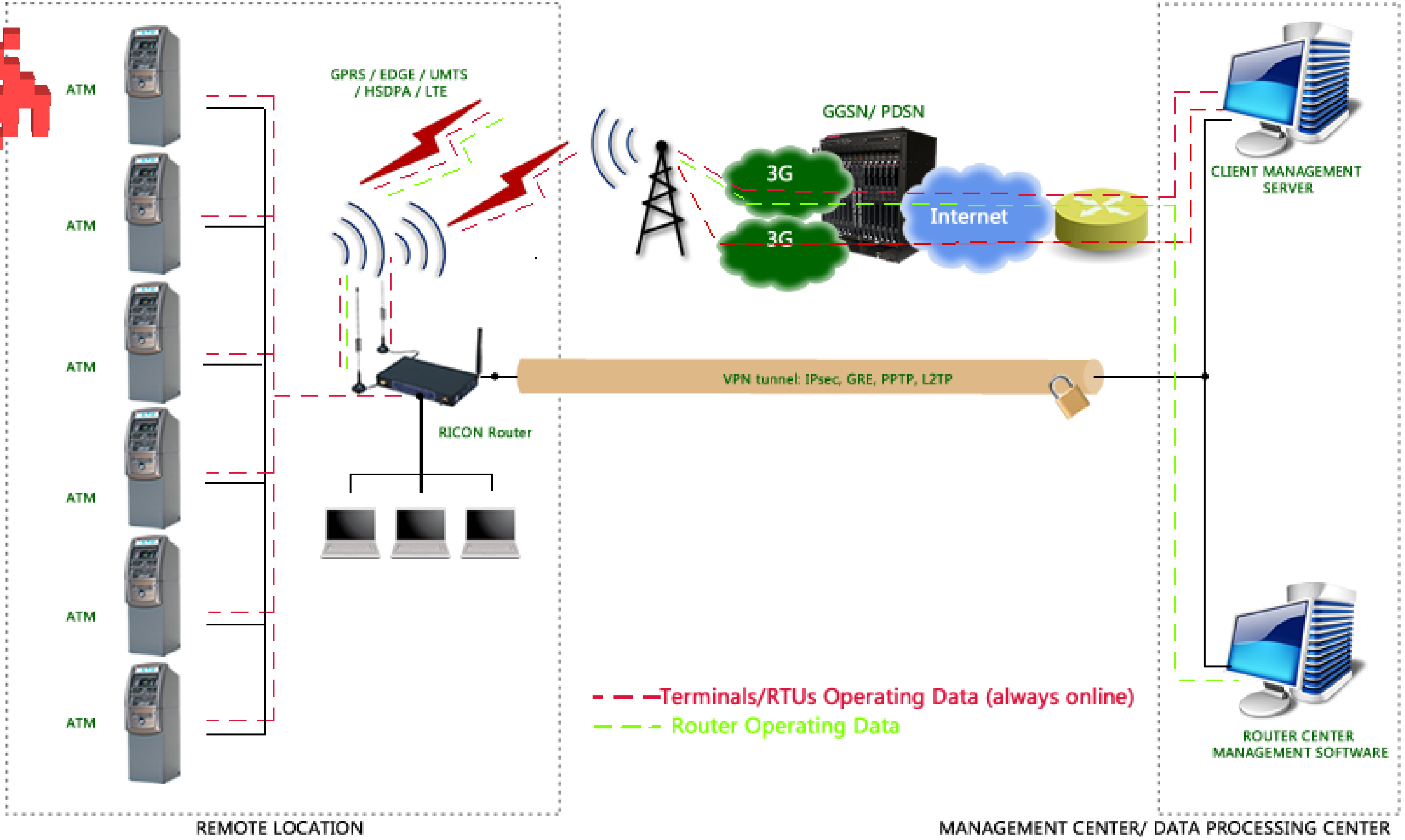
3g/4g downgrading attack + FakeBTS

Access to web interface outside of VPN channel

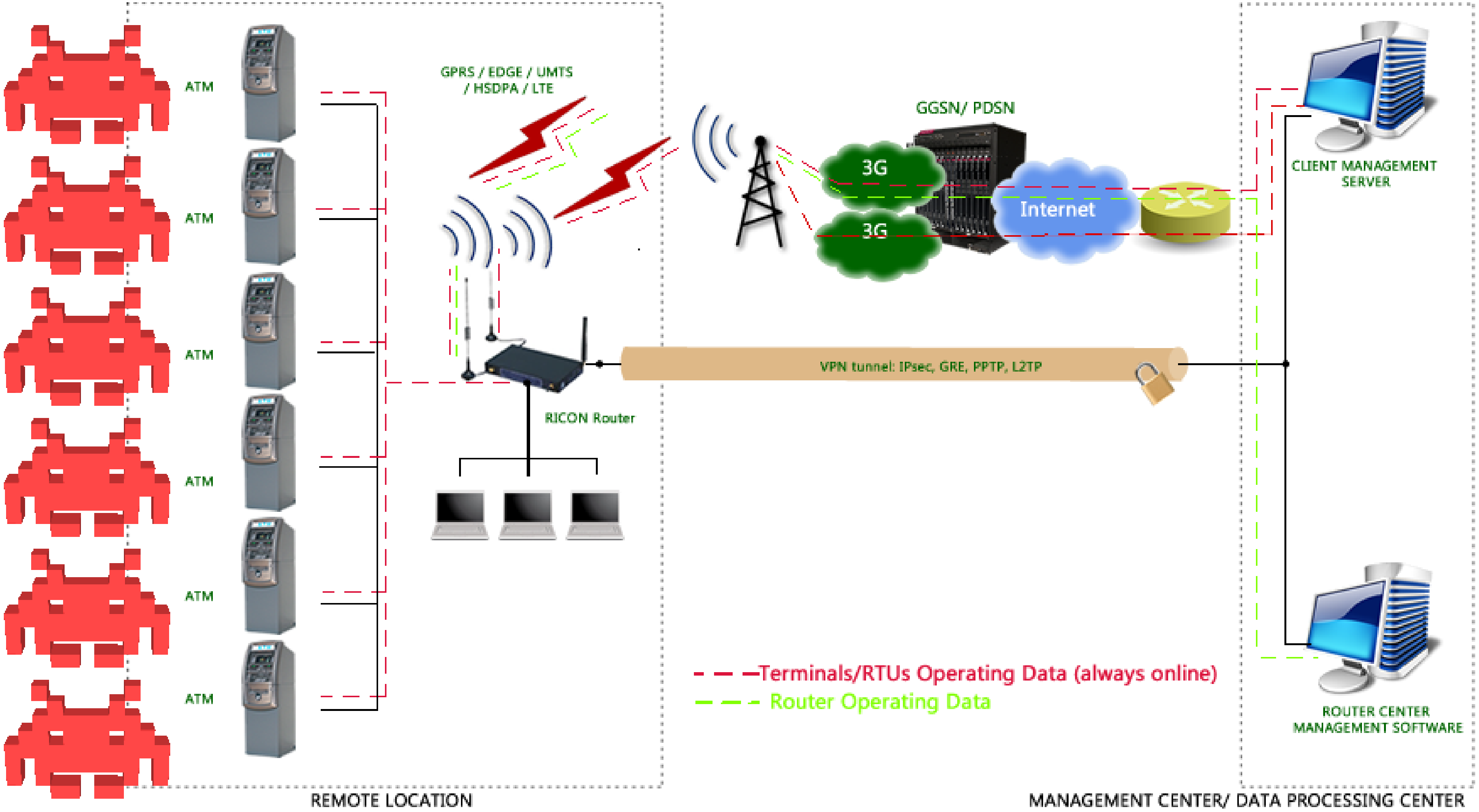
Authentication/Authorisation bypasses

Proprietary VPN

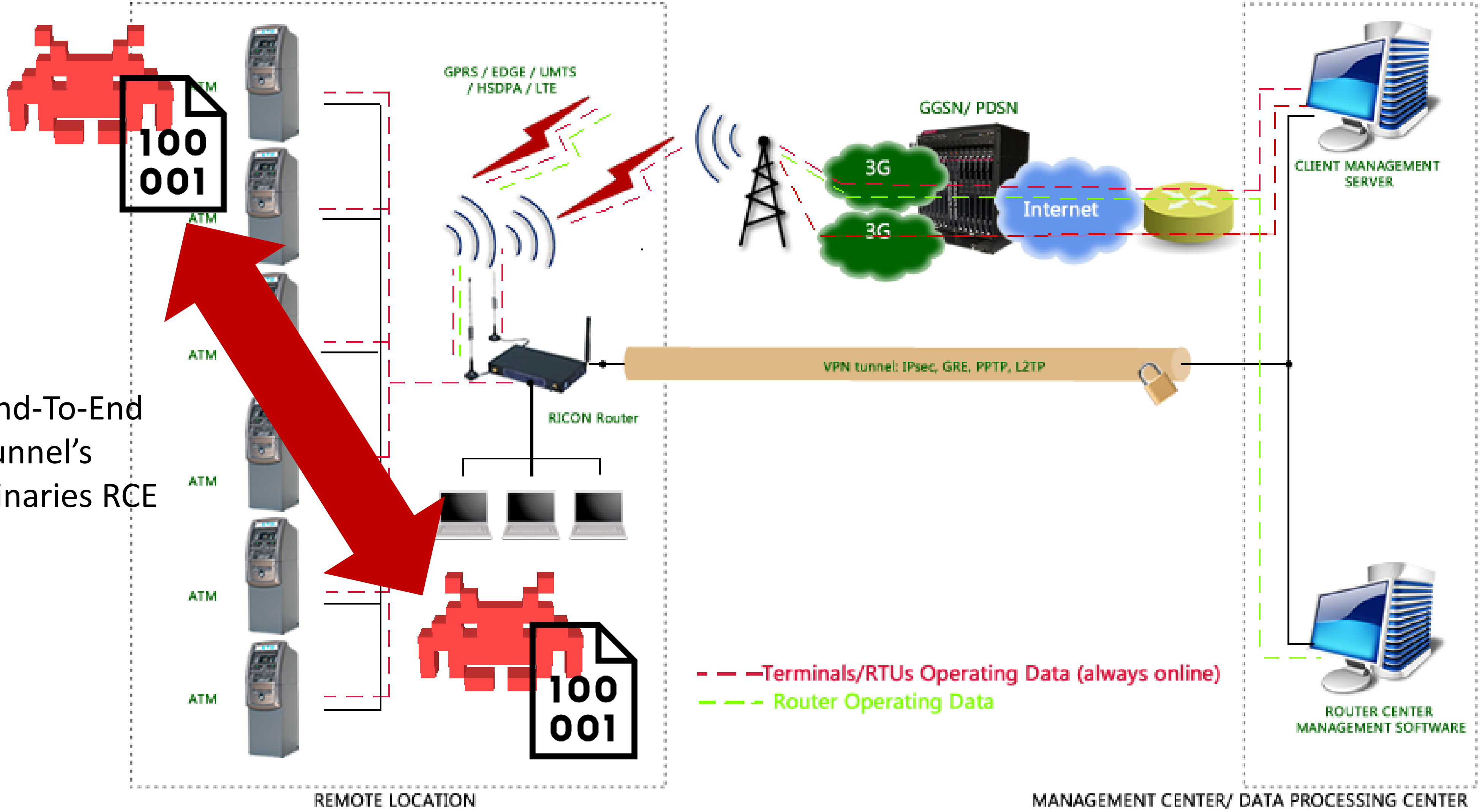
Industrial 3G modems

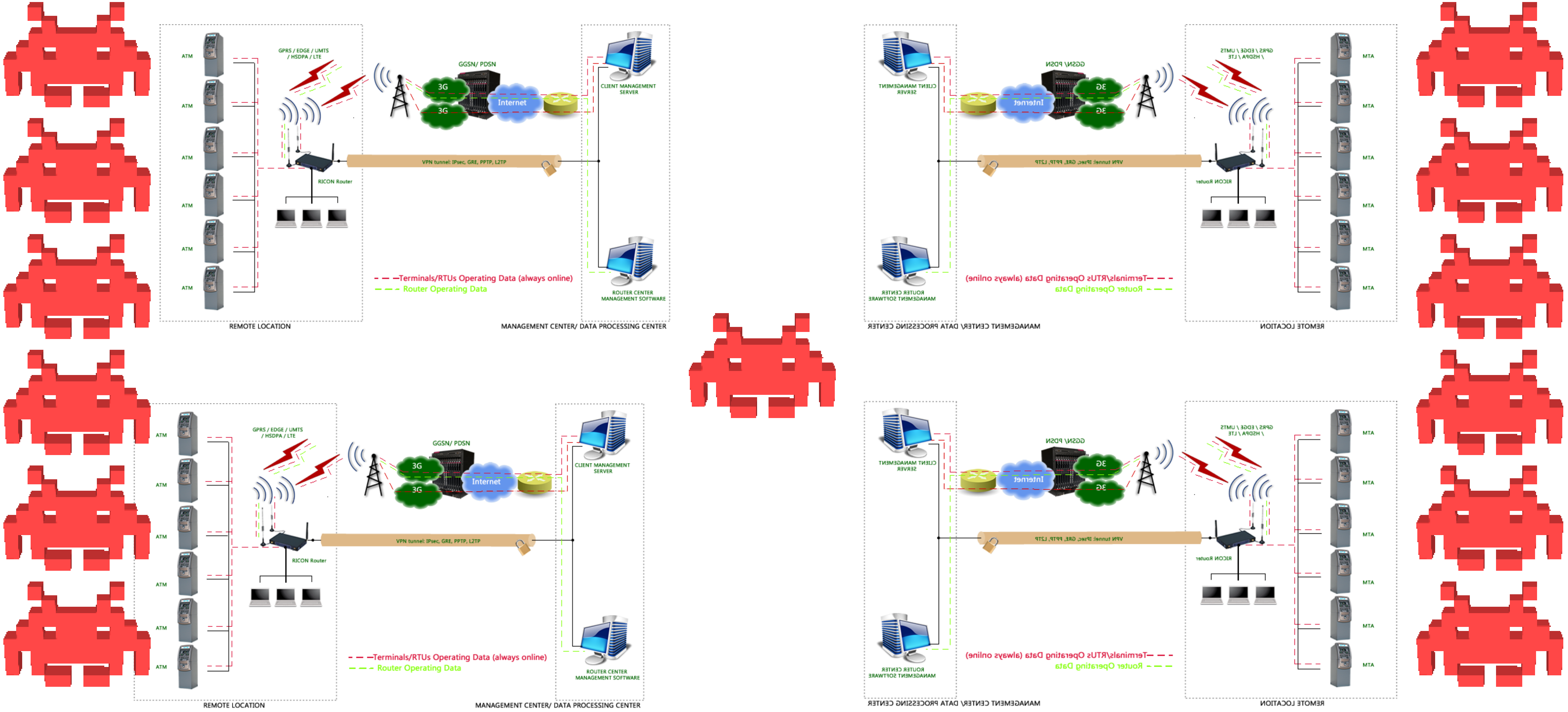

ATM
ATM
ATM
ATM
ATM
ATM
GPRS / EDGE / UMTS / HSDPA / LTE
RICON Router
GGSN/ PDSN
3G
3G
Internet
VPN tunnel: IPsec, GRE, PPTP, L2TP
CLIENT MANAGEMENT SERVER
ROUTER CENTER MANAGEMENT SOFTWARE
Terminals/RTUs Operating Data (always online)
Router Operating Data
REMOTE LOCATION
MANAGEMENT CENTER/ DATA PROCESSING CENTER

Industrial 3G modems


ATM
ATM
ATM
ATM
ATM
ATM
GPRS / EDGE / UMTS / HSDPA / LTE
GGSN/ PDSN
3G
3G
Internet
CLIENT MANAGEMENT SERVER
VPN tunnel: IPsec, GRE, PPTP, L2TP
RICON Router
ROUTER CENTER MANAGEMENT SOFTWARE
Terminals/RTUs Operating Data (always online)
Router Operating Data
REMOTE LOCATION
MANAGEMENT CENTER/ DATA PROCESSING CENTER

End-To-End tunnel's binaries RCE


100
001
ATM
ATM
ATM
ATM
ATM
ATM
GPRS / EDGE / UMTS / HSDPA / LTE
GGSN/ PDSN
3G
3G
Internet
CLIENT MANAGEMENT SERVER
VPN tunnel: IPsec, GRE, PPTP, L2TP
RICON Router
100
001
Terminals/RTUs Operating Data (always online)
Router Operating Data
ROUTER CENTER MANAGEMENT SOFTWARE
REMOTE LOCATION
MANAGEMENT CENTER/ DATA PROCESSING CENTER


ATM
ATM
ATM
ATM
ATM
ATM
GPRS / EDGE / UMTS / HSDPA / LTE
RICON Router
GGSN/ PDSN
3G
3G
Internet
VPN tunnel: IPsec, GRE, PPTP, L2TP
CLIENT MANAGEMENT SERVER
ROUTER CENTER MANAGEMENT SOFTWARE
Terminals/RTUs Operating Data (always online)
Router Operating Data
REMOTE LOCATION
MANAGEMENT CENTER/ DATA PROCESSING CENTER

Kudos to PT Research Center

@groke
@ivachyou
@yarbabin
Maxim Kozhevnikov
Leonid Krolle

https://uk.linkedin.com/in/tyunusov
https://uk.linkedin.com/in/leighannegalloway

tyunusov@ptsecurity.com
lagalloway@ptsecurity.com

@a66at
@L_AGalloway