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
Hi T,

Hope all is well. I was just having a bit of a brainstorm and was thinking up ways of standing out in what is basically a saturated market. I know you mentioned you had a relatively cheap thing to buy an ATM and make it look like a bank, but I was thinking maybe we could do something technically possible before we actually figured out how to make it look real. Cheers
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 £827.45

Buy it now
Add to basket

Collect 627 Nectar points
Get Started | Conditions

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

Delivery: Varies for items sent from an international location

Payments: PayPal, Visa
See payment information

Returns: 14 days refund, kupujący | See details

Protection: eBay MONEY BACK GUARANTEE | See details
HISTORY OF ATMs

John Shepherd-Barron
1967
Barclays
1969
USA
1972
Lloyds
2017
3.8 million
Identify market options

Where to buy an ATM
4 WAYS TO BUY AN ATM

**LEGAL**
ATM maintainers in your region, banks and manufacturers

**BLACK MARKET**
Underground market place

**GREY MARKET**
Resellers, aftermarket listings, eBay, private sellers etc.

**THE WILDCARD**
Guaranteed ATM but with a possibility of imprisonment
Legal and Grey market options
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:
- Indoor
- 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
- Autochek LOU
- EMV 2000 certified
- Optical indicators at all input and output modules
- Energy-saving function

Specifications:
- Bundle output up to 60 notes
- 8 stainless steel safes
- Numeric keypad with 8 function keys
- Hybrid card reader (magnetic)
- Tamperproof card slot
- Receipt and journal printers
- Passbook processing
- Envelope deposit included
- Check processing (remote checks or bundles of checks)
- UL 291 Level 1 / CEN III / CEN+ / CEN L

VAT INCLUDED IN PRICE - VAT INVOICE PROVIDED
The listing has ended, here are some similar items
Hi, this has been sold.

Best Regards

[Redacted text]

Your use of this message and posting any attachment is 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 |
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, 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.
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.
**Order Confirmation**

<table>
<thead>
<tr>
<th>Part Number</th>
<th>Description</th>
<th>Despatch By Date</th>
<th>Unit Cost</th>
<th>Qty</th>
<th>Net Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATM5877RA</td>
<td>5877 Rear access</td>
<td></td>
<td>2,600.00</td>
<td>1</td>
<td>2,600.00</td>
</tr>
</tbody>
</table>

To be supplied cleaned, working and tested with a Primat Core and a refurbished EPP for testing purposes.

<table>
<thead>
<tr>
<th>Ship By</th>
<th>Testlink Account</th>
</tr>
</thead>
<tbody>
<tr>
<td>Courier</td>
<td>1 Pallet</td>
</tr>
</tbody>
</table>

| Carriage | 55.00  |
| Tax      | 531.00 |

**Total Items** | 2,600.00

| Currency | GBP  | Total | 3,186.00 |
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.
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
OS LEVEL

SORRY TEMPORARILY
OUT OF
SERVICE
HARDWARE
HARDWARE
NETWORK
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

Matthew J. Schwartz (@suroinfosec) - August 30, 2016  0 Comments
Application control for Application security

https://evi1cg.me/archives/App Locker_Bypass_Techniques.html
https://embedi.com/blog/hack-atm-anti-hacking-feature-and-walk-away-1m-2-minutes/
Controls flow

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

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 HTTPS
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
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(pyTh0n.exe) will be run multiple times
1. Local unauthorised privileges escalation (you need to launch exploit.exe to bypass restrictions for launching exploit.exe)

2. Network-based BOF => RCE
<table>
<thead>
<tr>
<th></th>
<th>Update</th>
<th>Network attack</th>
<th>Local bypass</th>
<th>Poor ruleset*</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>-</td>
<td>-</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>-</td>
<td></td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>http + sig</td>
<td></td>
<td>Logical</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>-</td>
<td></td>
<td></td>
<td>+</td>
</tr>
<tr>
<td>6</td>
<td>-</td>
<td>RCE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>http - nosig</td>
<td></td>
<td></td>
<td>+</td>
</tr>
<tr>
<td>8</td>
<td>-</td>
<td>RCE</td>
<td></td>
<td>+</td>
</tr>
<tr>
<td></td>
<td>Update</td>
<td>Network attack</td>
<td>Local bypass</td>
<td>Poor ruleset*</td>
</tr>
<tr>
<td>---</td>
<td>--------</td>
<td>----------------</td>
<td>--------------</td>
<td>--------------</td>
</tr>
<tr>
<td>1</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>

The table highlights the following issues:
- Update
- Network attack
- Local bypass
- Poor ruleset*

*Note: The poor ruleset is marked with a green box.
Industrial 3G modems

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

- Terminals/RTUs Operating Data (always online)
- Router Operating Data

REMOTE LOCATION

MANAGEMENT CENTER/ DATA PROCESSING CENTER
End-To-End tunnel's binaries RCE
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