SKIDPOTTING – Automated Teller Machines

Like a walk in the park

MC & Yaniv Miron
Security 1337s @ FortConsult

FORTCONSULT
Straight talk on IT security

E.A.S.T

/ About MC

- Intercontinental man of mystery and security consultant
- Performs security testing and assessments on most continents
- Works in Fcon²Labs team @ FortConsult in Copenhagen, Denmark
- Allegedly from Peahi, Maui
- Used to rock the house on the ones and twos

/ About Yaniv Miron

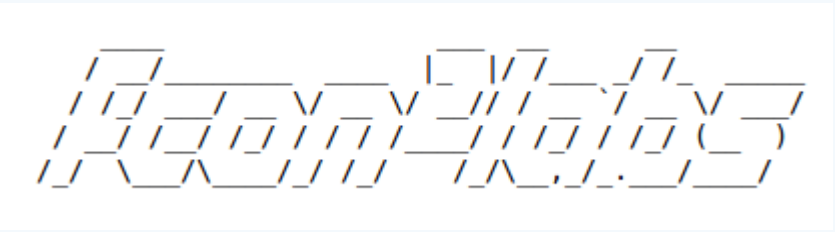
- aka Lament
- Security Researcher and consultant in Fcon²Labs @ FortConsult in Copenhagen, Denmark
- Found security vulns in Microsoft, IBM, Apache, Oracle products and more
- CISO certified from the Technion (Israel Institute of Technology)
- Certified locksmith

/ About FortConsult / Fcon²Labs

- Founded in 2002 by Ulf Munkedal
- HQ @ Copenhagen, Denmark
- Fcon²Labs - Doing cool stuff, for real
- Go ahead, challenge us

FORTCONSULT

Straight talk on IT security



Definition of a SKID

Script kiddie

From Wikipedia, the free encyclopedia

In hacker culture a **script kiddie** or **skiddie**,[1] (also known as *skid*, *script bunny*,[2] *script kitty*,[3]) are unskilled individuals who use scripts or programs developed by others to attack computer systems and networks and deface websites. It is generally assumed that script kiddies are juveniles who lack the ability to write sophisticated hacking programs or exploits on their own, and that their objective is to try to impress their friends or gain credit in computer-enthusiast communities.[4] The term is typically pejorative.

/ Agenda

- Approach
- Remote vs. Local
- Different attackers
- Attack scenarios
- Q & A

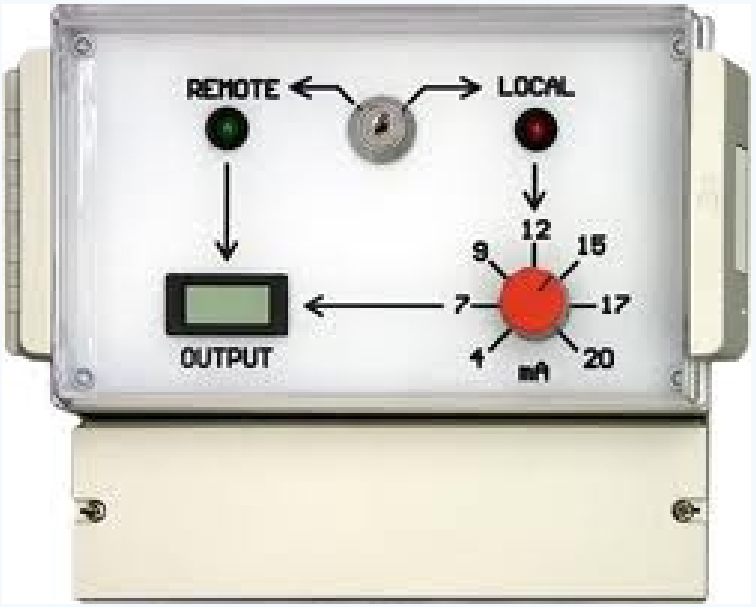
Approach

- Security vs compliance (PCI DSS / PIN et al)
- Focus areas (data/lateral movement vs traditional skimming/cash)
- "Hackers do not give a sh*t!
- Legacy tech (e.g. WinXP EOL)

Props to Kiwicon crew \m/

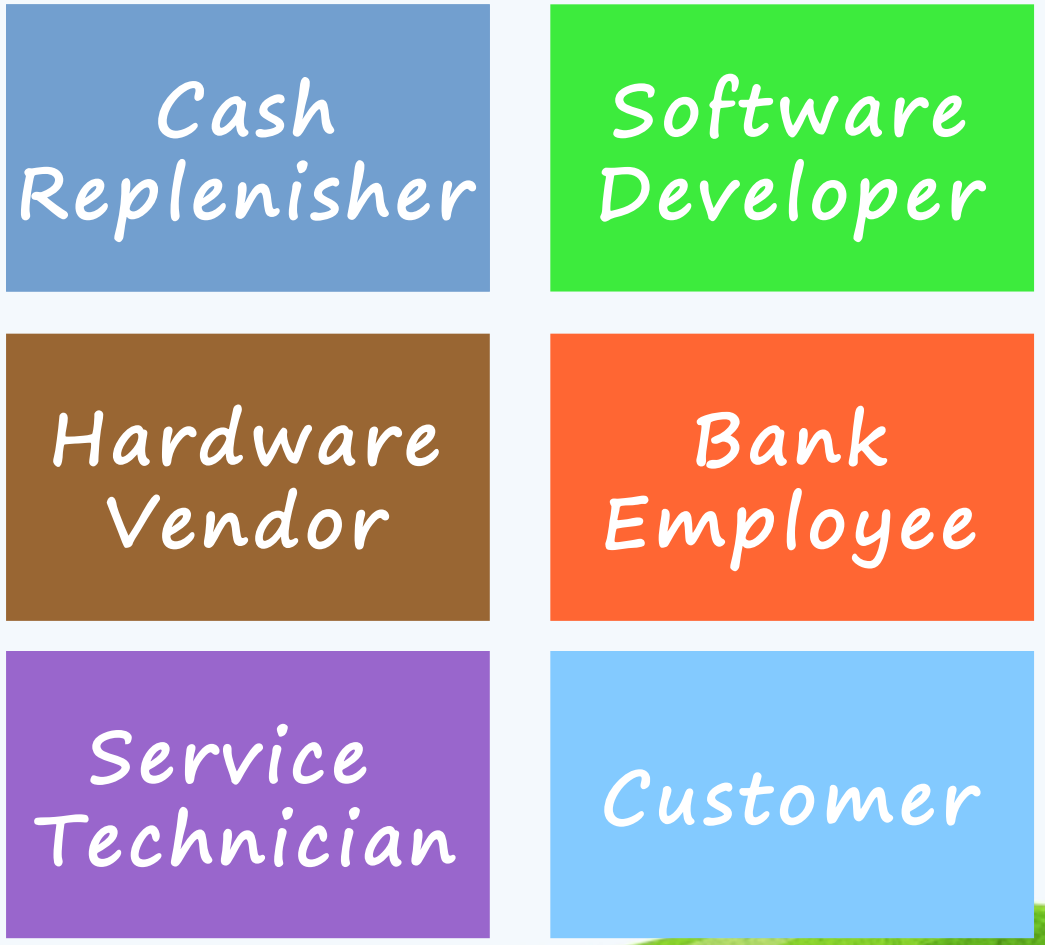
Remote vs. Local

- What do you mean by remote?
- What do you mean by local?
- What the difference?
- What is better?



Different roles – different threats

- Different roles have different goals as an attacker
- Complex ATM eco-system
- Don't have to be hard core hackers
- Is it only for the money? Or maybe to gain control? Steal data?



Different roles – complex trust relationships

Hardware vendor

OS vendor

Application Vendor

Cash Handling Vendor

Outsourcing Vendor

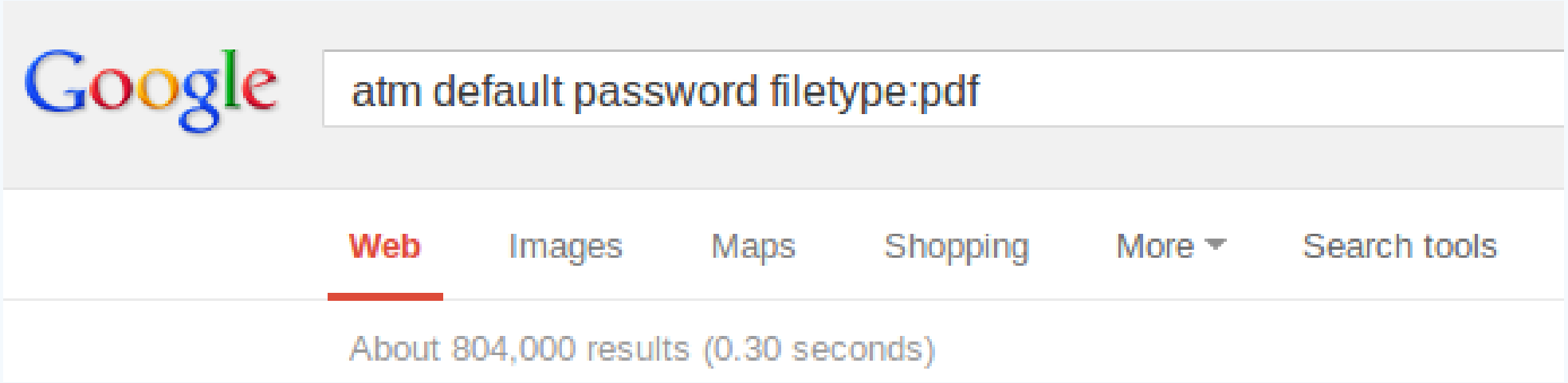
Bank Employees

Networking Vendor

Telco Vendor

Passwords

- Default
- Available online, guessable or brute force
- Shared or reused >> attack other systems

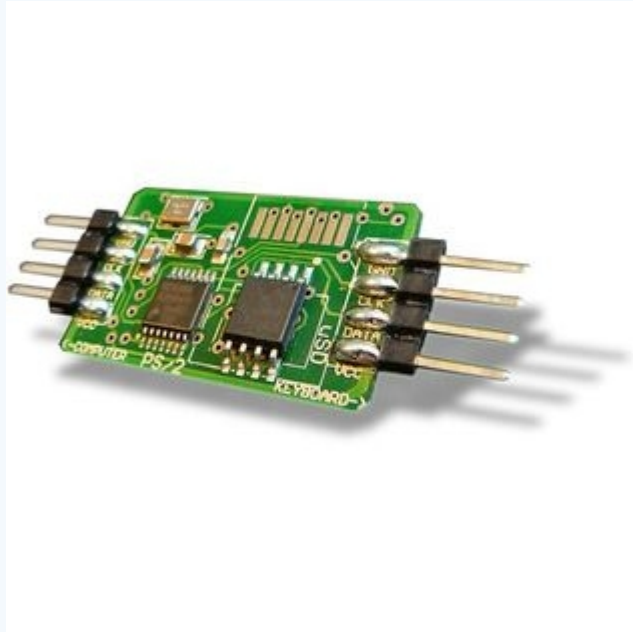


PAN data

- PCI DSS
- Legacy data
- Legacy system >> paper rolls
- Debug verbose logging mode
- Automate with scanner

Key/Screen logger

- Credentials (local or domain admin)
- Screen dumps
- Intelligence gathering >> other systems



Lock picking/Getting keys

- Pick lock with cheap lockpick or roll own
- Keys available online to buy for cheap
- Strong cash lock >> weak key management

File tampering

- Weak file integrity check
- Tamper with any file
- Bypass AV
- Add root kit

Remote tampering

- Weak remote access control
- Not restricted according to job role and business need

Exfiltrate data remotely

- Weak access and authorization controls
- Weak or no monitoring
- No or weak data prevention/detection exfiltration mechanism or process

Hardening

- Swiss cheese everywhere
- Physical
- Network
- Operating system
- Applications
- Users
- Mass storage devices

Memory dump and FireWire

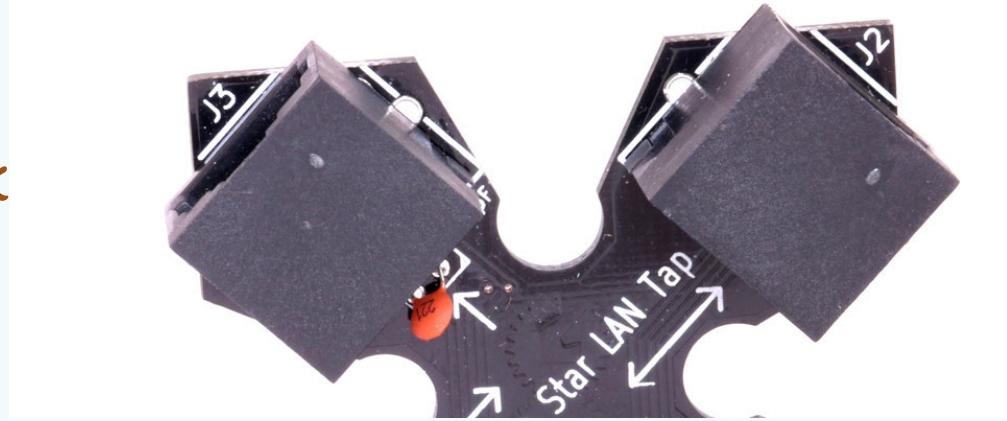
- Weak physical controls
- Weak logical controls

Anti Virus bypass

- Broken concept
- Ineffective control
- Easy for an attacker

Network attacks and MITM

- Lack of Network Access Controls
- Network software downgrade attack
- Network software upgrade attack
- Sniff data
- Traffic analysis << intelligence gathering



ATM Physical Alarm

- No weak or physical perimeter alarm
- Bypass or spoof alarm
- Monitoring overhead a business constraint

Messing with the meatware

- Load own ATM distro and application
- Social engineering to gain physical or access
- Social engineering to gain logical access

/ To wrap it all up

- ATM security can be bypassed by a skid
- ATM hacking is not only about money >> data
- Complex set of trust relationships
- Test your ATM fully end-to-end in all of eco system

[E O F]

Questions?

» Yaniv Miron aka Lament

ymt [at] fortconsult.net (work)

lament [at] ilhack.org (private)

MC

mc [at] fortconsult.net (work)