KASPERSKY lab

APT

Advanced threats

Targeted Attack

Abnormal Behavior

Internal threats

BANKING THREATS IN DEPTH
BANKS ARE UNDER ATTACK 2016

Sergey Lozhkin
Senior Security Researcher
Kaspersky Lab Italia

GREAT: ELITE THREAT RESEARCH

- Global Research and Analysis Team, since 2008
- Threat intelligence, research and innovation leadership
- Focus: APTs, critical infrastructure threats, banking threats, sophisticated targeted attacks

IN 2014…WE PREDICTED AND WE WERE RIGHT

Escalation of ATM and PoS attacks

Attacks against cash machines (ATM) seemed to explode this year with several public incidents and a rush b law enforcement authorities globally to respond to this crisis. A corollary of this publicity is an awareness tha ATMs are ripe for the taking and cybercriminals are sure to notice. As most of these systems are running Windows XP and also suffer from frail physical security, they are incredibly vulnerable by default and, as the impersonal gatekeepers of the financial institutions' cash, cybercriminals are bound to come knocking here first.

> The next stage will see attackers compromising the networks of banks to manipulate #ATM chines in real time

Tweet

The Great Bank Robbery: the Carbanak APT

By GReAT on February 16, 2015. 4:20 pm

rther evolution of these ATM attacks with the use of APT techniques to gain machines. The next stage will see attackers compromising the networks of f access to manipulate ATM machines in real time.

KASPERSKY lab

THEY STARTED OPERATIONS WORLDWIDE

KASPERSKY lab

CASES 2015-2016

- CARBANAK 2.0
- METEL (RUSSIAN BANKS)
- GCMAN (MOSTLY RUSSIAN BANKS)
- CARBANAK 2.0 (WORLDWIDE)
- UNKNOWN (BANGLADESH)

KASPERSKY lab

SPEARFISHING – STILL NUMBER 1

KASPERSKY lab

LEGITIMATE TOOLS

- PUTTY (WHITELISTED)
- VNC
- METERPRETER(IN POWERSHELL)
- AMMY
- MIMIKATZ (IN POWERSHELL)

KASPERSKY lab

MONEY EXFILTRATION

- ONLINE BANKING
- E-PAYMENT SYSTEMS
- INFLATING ACCOUNT BALANCES
- DATABASE MANIPULATION
- CONTROLLING ATM'S

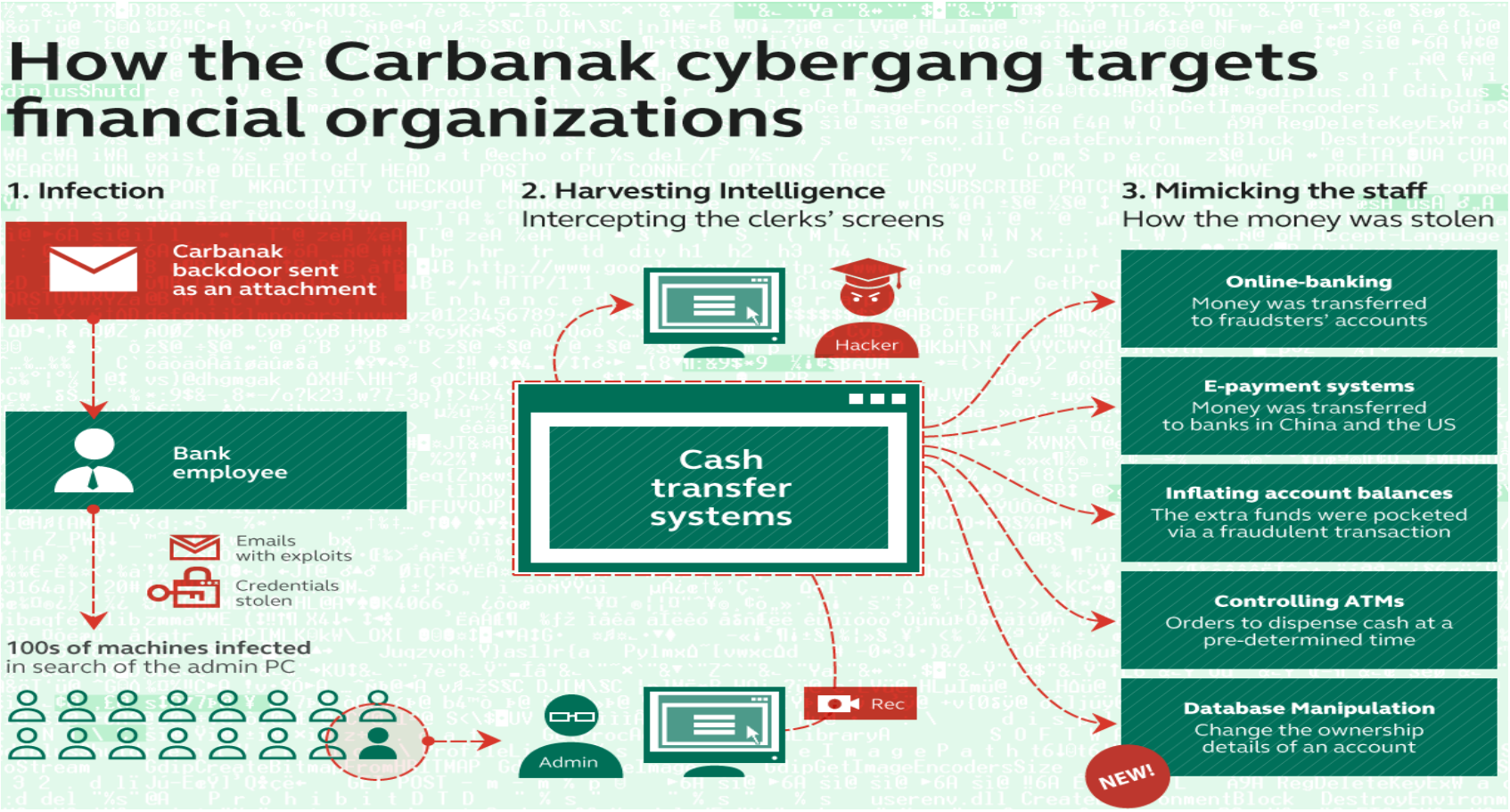
KASPERSKY lab

CARBANAK 2.0

- Attacks in budget deps
- Change registration data of shareholders' in depository

KASPERSKY lab

How the Carbanak cybergang targets financial organizations

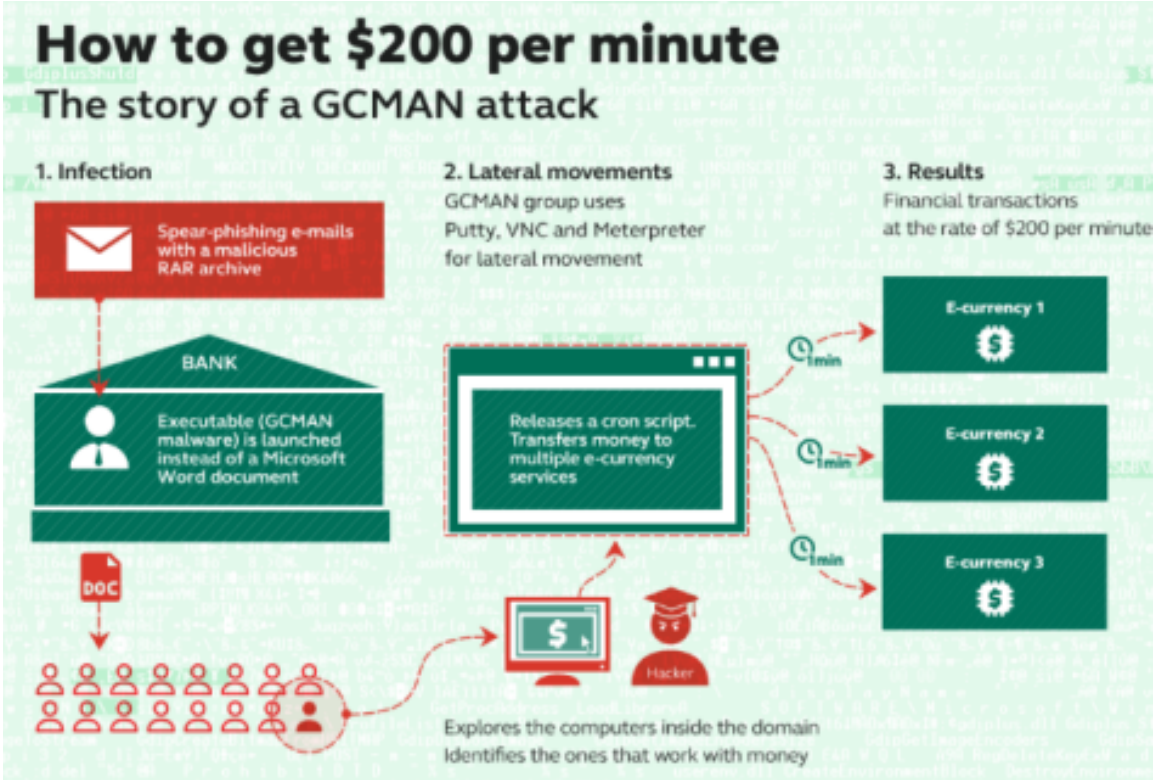


KASPERSKY lab

METEL – TRANSACTIONS ROLLBACK

KASPERSKY lab

GCMAN – 200$ PER MINUTE AUTOSCRIPT



200 USD PER MINUTE

```
root@payments ~ #
root@payments ~ # crontab -l
# crontab for root
* * * * * /bin/snitch_some_money

root@payments ~ #
```

KASPERSKY lab

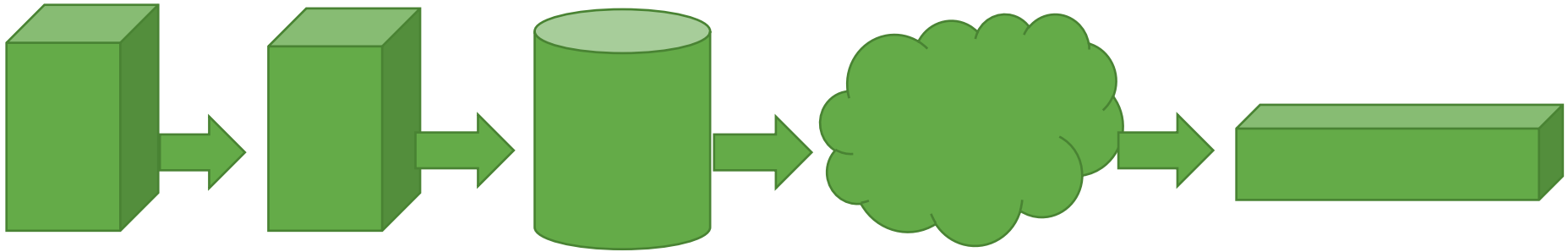
1.5 YEARS

- 70 internal hosts
- 56 accounts
- 139 attack sources:

  TOR and home routers

KASPERSKY lab

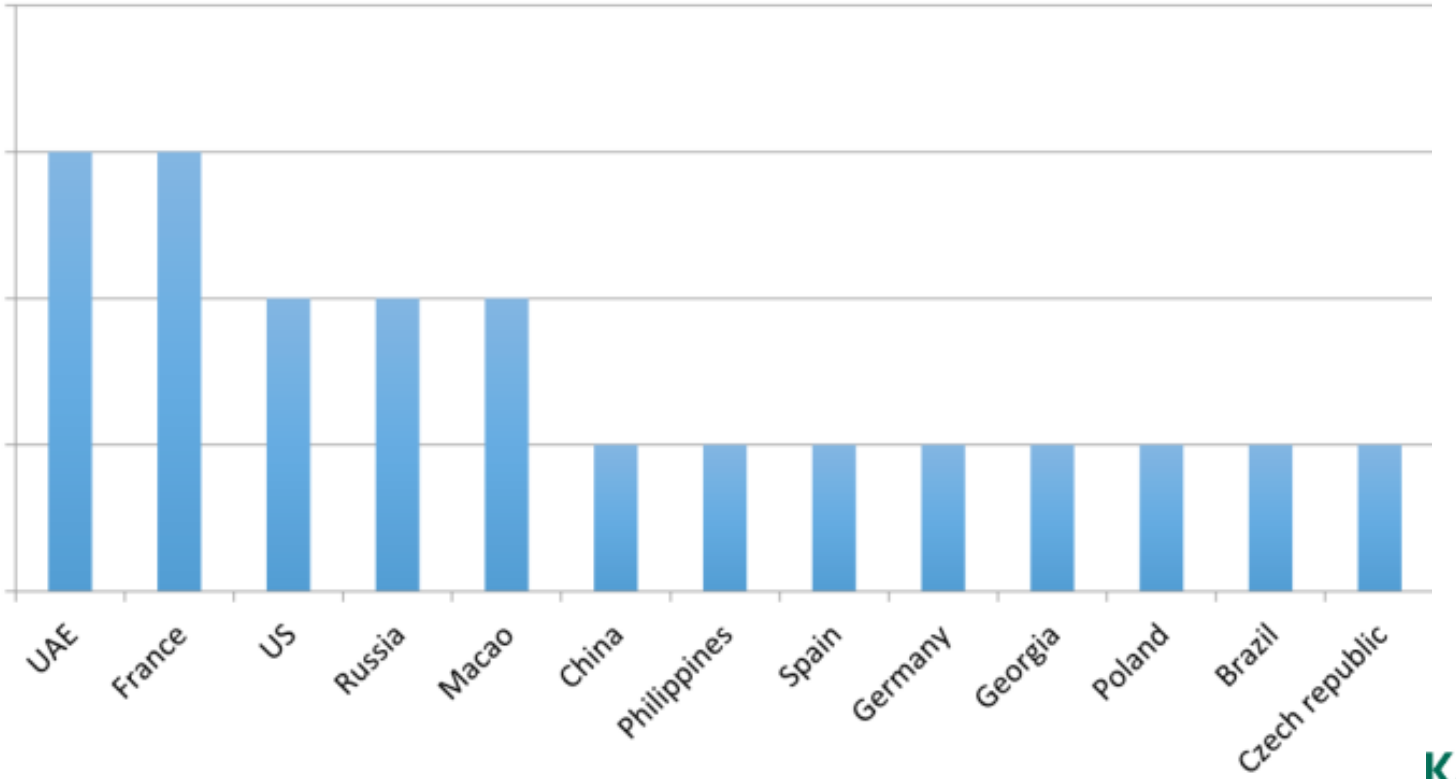
GCMAN ATTACK



Ads Web Server	Corporate online banking webserver	Online banking DB	Admin's Workstations	Processing Connection Server

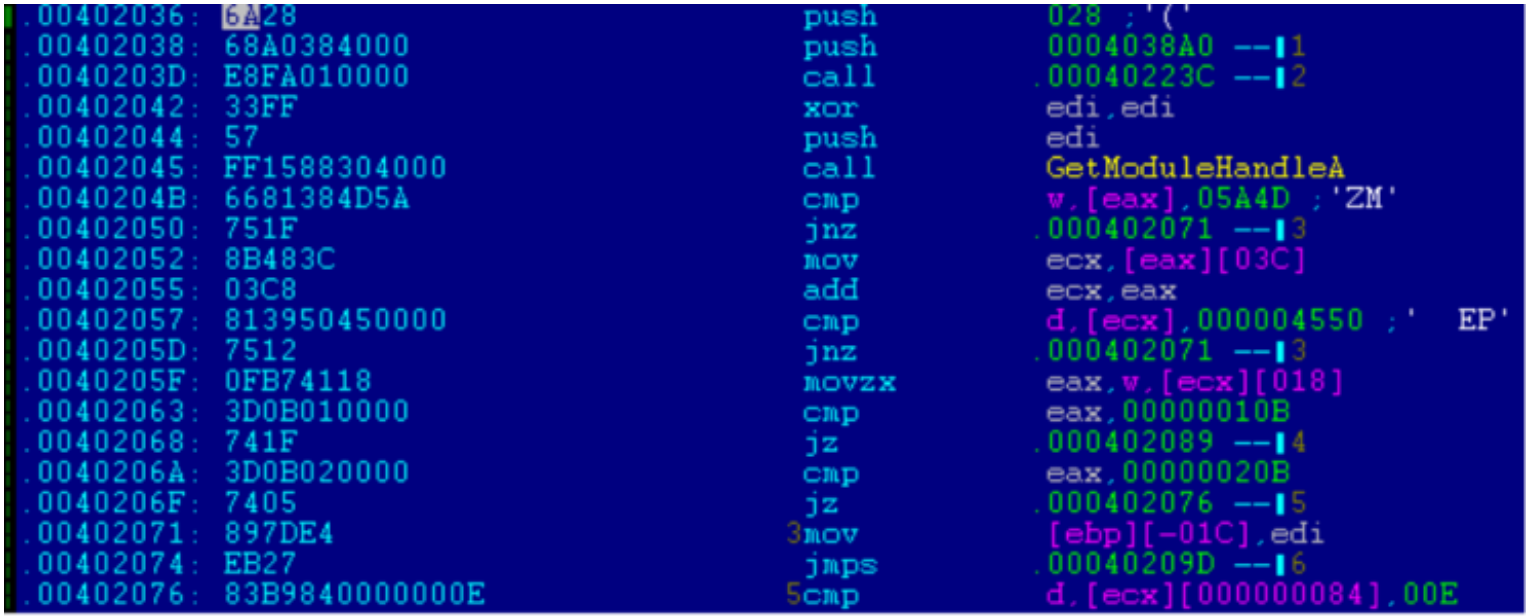
KASPERSKY lab

ATM INFECTOR



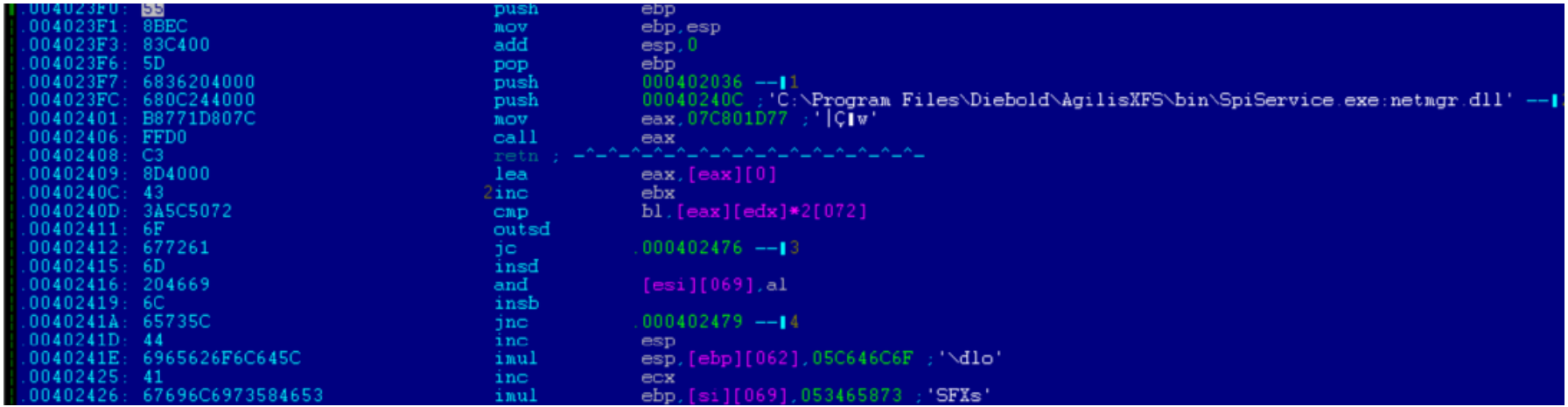
KASPERSKY lab

ATM INFECTOR –XFS SERVICE PATCH



KASPERSKY lab

ATM INFECTOR – SPISERVICE PATCHED

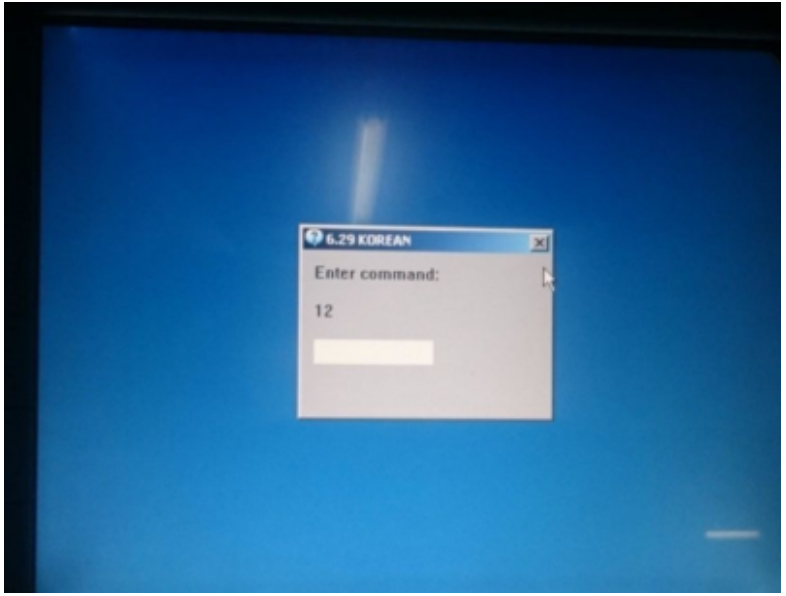


KASPERSKY lab

ATM INFECTOR –MAGIC CARD

CARD 1 – INTERFACE COMMANDS

CARD 2 – TRACK 2 HARDCODED



KASPERSKY lab

THANK YOU!

Sergey Lozhkin
Senior Security Researcher
Kaspersky Lab

KASPERSKY lab