New Botnet and Malware Targeted to Industry Sectors

By Roland Cheung
@HKCERT

Agenda

- Malware Trend
- Security Risk on Industry Sector
- Case Study
- Security Mitigations

Malware Trend

Reason

- Fun
- Profit
  - Direct financial gain
  - Sell data, service
- State sponsor
  - Political

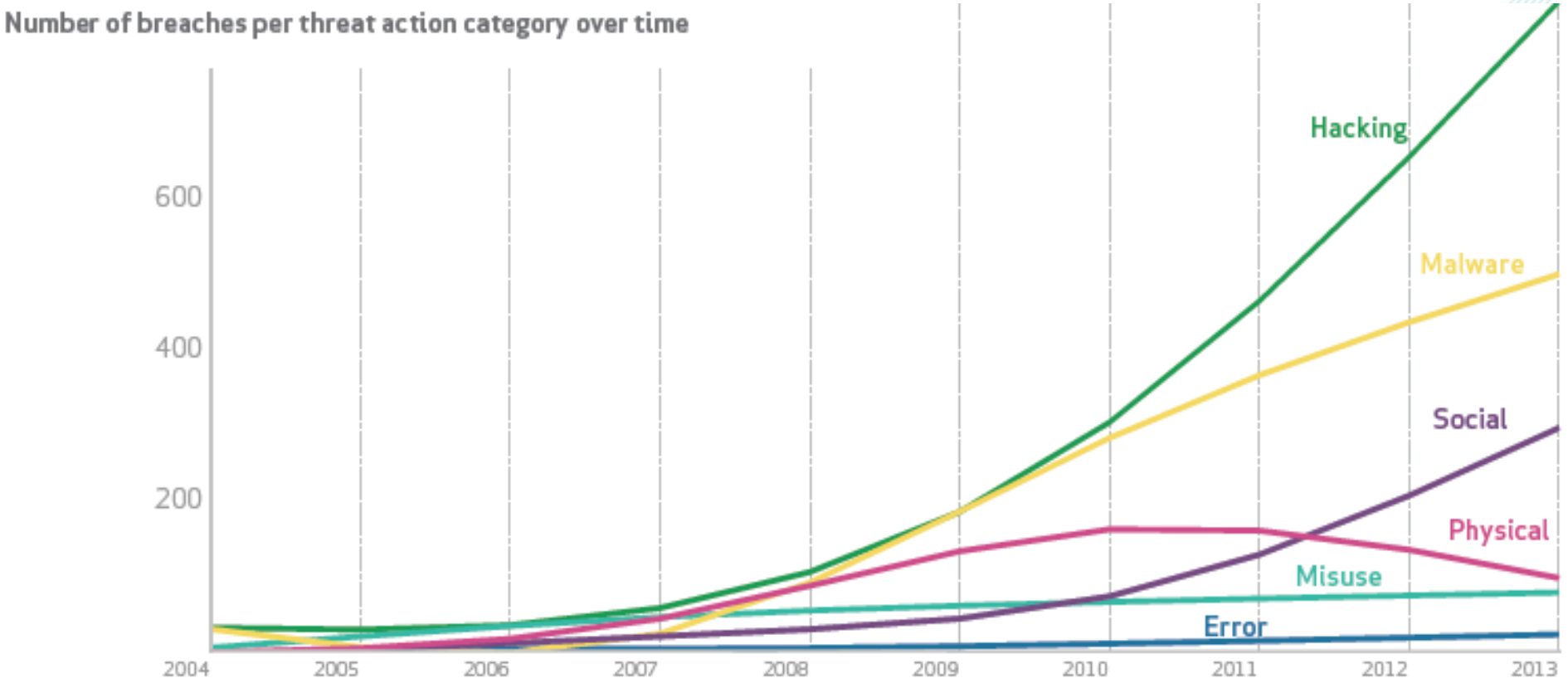
Incident Classification by Industry

INDUSTRY	POS INTRUS-ION	WEB APP ATTACK	INSIDER MISUSE	THEFT/ LOSS	MISC. ERROR	CRIME-WARE	PAYMENT CARD SKIMMER	DENIAL OF SERVICE	CYBER ESPION-AGE	EVERY-THING ELSE
Accommodation [72]	75%	1%	8%	1%	1%	1%	<1%	10%		4%
Administrative [56]		8%	27%	12%	43%	1%		1%	1%	7%
Construction [23]	7%		13%	13%	7%	33%			13%	13%
Education [61]	<1%	19%	8%	15%	20%	6%	<1%	6%	2%	22%
Entertainment [71]	7%	22%	10%	7%	12%	2%	2%	32%		5%
Finance [52]	<1%	27%	7%	3%	5%	4%	22%	26%	<1%	6%
Healthcare [62]	9%	3%	15%	46%	12%	3%	<1%	2%	<1%	10%
Information [51]	<1%	41%	1%	1%	1%	31%	<1%	9%	1%	16%
Management [55]		11%	6%	6%	6%		11%	44%	11%	6%
Manufacturing [31,32,33]		14%	8%	4%	2%	9%		24%	30%	9%
Mining [21]			25%	10%	5%	5%	5%	5%	40%	5%
Professional [54]	<1%	9%	6%	4%	3%	3%		37%	29%	8%
Public [92]		<1%	24%	19%	34%	21%		<1%	<1%	2%
Real Estate [53]		10%	37%	13%	20%	7%			3%	10%
Retail [44,45]	31%	10%	4%	2%	2%	2%	6%	33%	<1%	10%
Trade [42]	6%	30%	6%	6%	9%	9%	3%	3%		27%
Transportation [48,49]		15%	16%	7%	6%	15%	5%	3%	24%	8%
Utilities [22]		38%	3%	1%	2%	31%		14%	7%	3%
Other [81]	1%	29%	13%	13%	10%	3%		9%	6%	17%

For more information on the NAICS codes [shown above] visit: https://www.census.gov/cgi-bin/sssd/naics/naicsrch?chart=2012

Source:
Verizon DBIR 2014

Threat Action Category Trend



Source: Verizon DBIR 2014

Infection Vector

- PC
- Mobile
- USB storage device
- Router
- Network connected device??
  - NAS
  - Smart Home , e.g.Google Nest

Internet of Things (IoT)

- Up to 50 billion things (or devices) will be connected to the Internet by 2020

- Equivalent of 6 devices for every person on the planet.

"**Everything Will Get Hacked**"

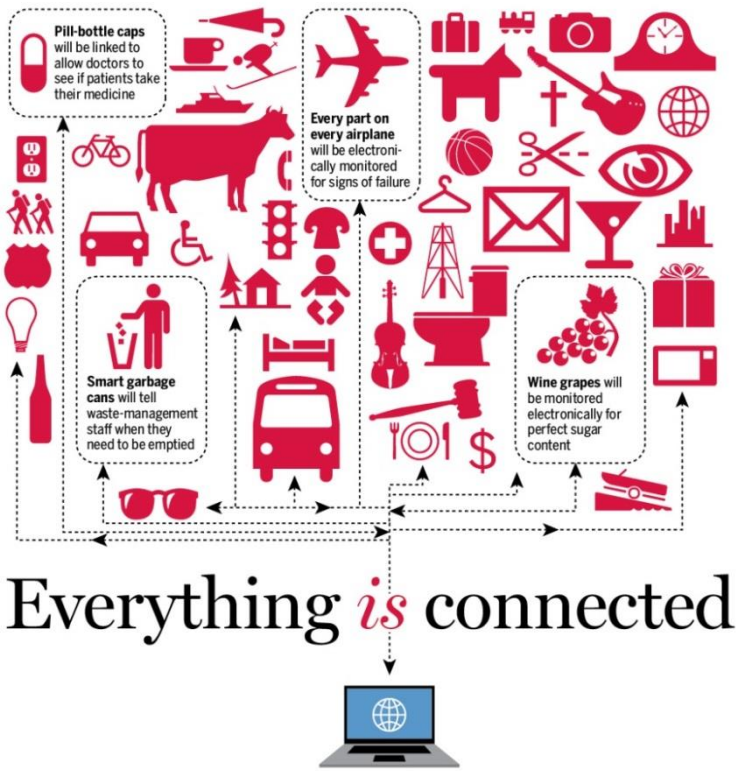
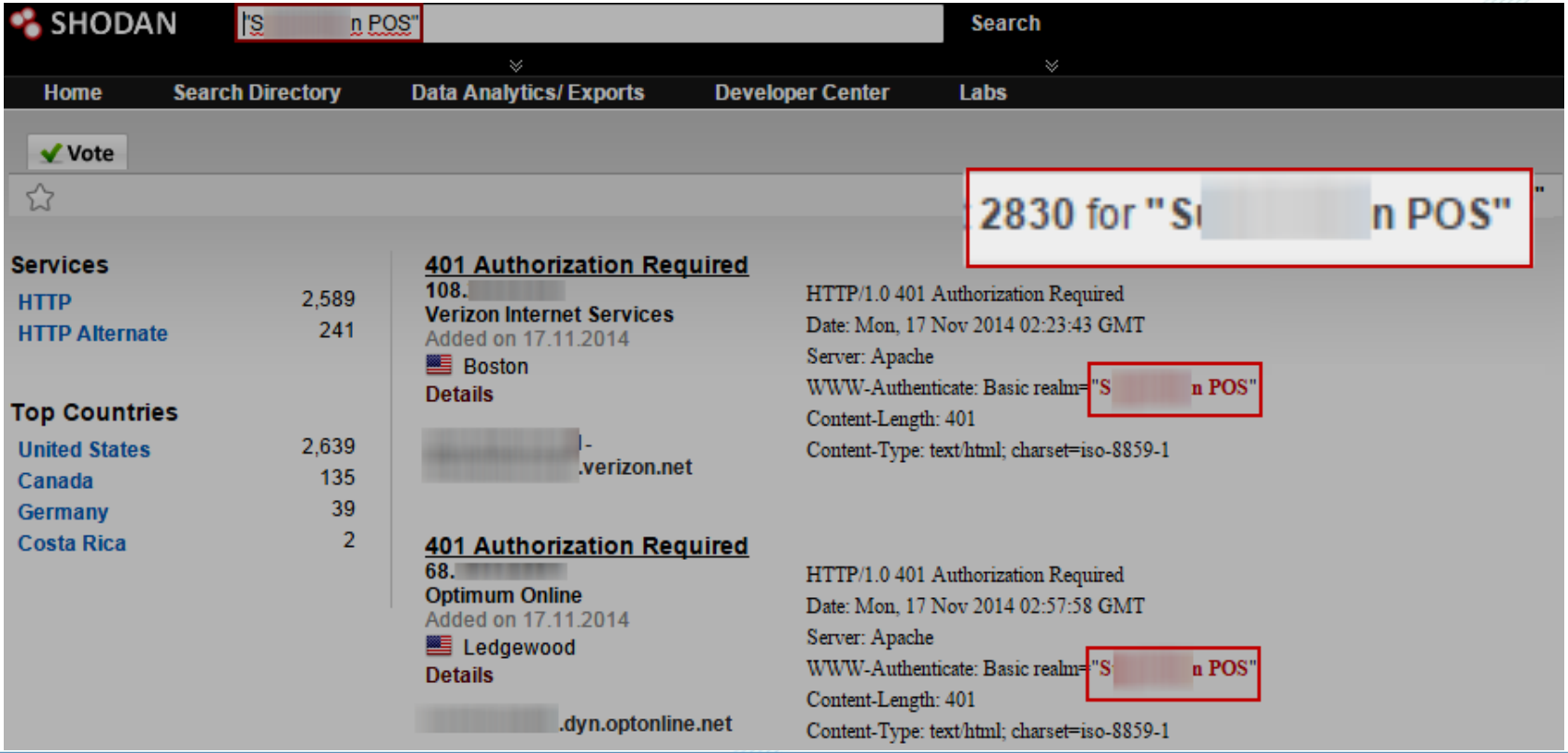


Image source: PAI/BAY AREA NEWS GROUP

Internet of Things (IoT)

- Search “POS name” on Internet



Security Risk on Industry Sector

Banking (ATM)

- 95 % run on versions of Windows XP
- Allow physical access and may connect additional device for hacking
- Insert CDs and USB sticks to upload the malware
- In Macau, connect skimming device to record card data and pins

http://krebsonsecurity.com/2014/05/thieves-planted-malware-to-hack-atms/

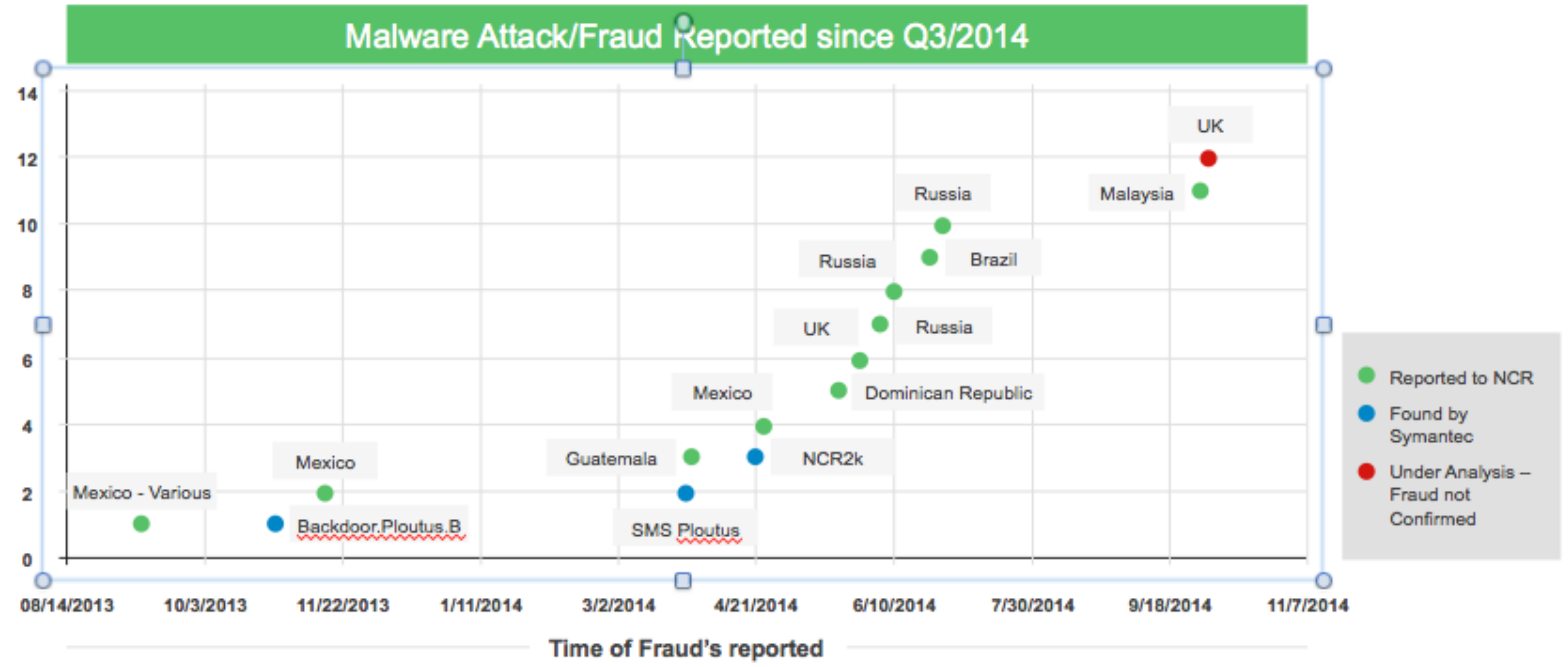
- In Mexico, connect external keyboard or mobile phone to receive command

http://www.symantec.com/connect/blogs/texting-atms-cash-shows-cybercriminals-increasing-sophistication

Banking (ATM)

Rapid rise

In frequency and expansion of logical attacks



Source: http://krebsonsecurity.com/2014/10/spike-in-malware-attacks-on-aging-atms/

Impact and Loss

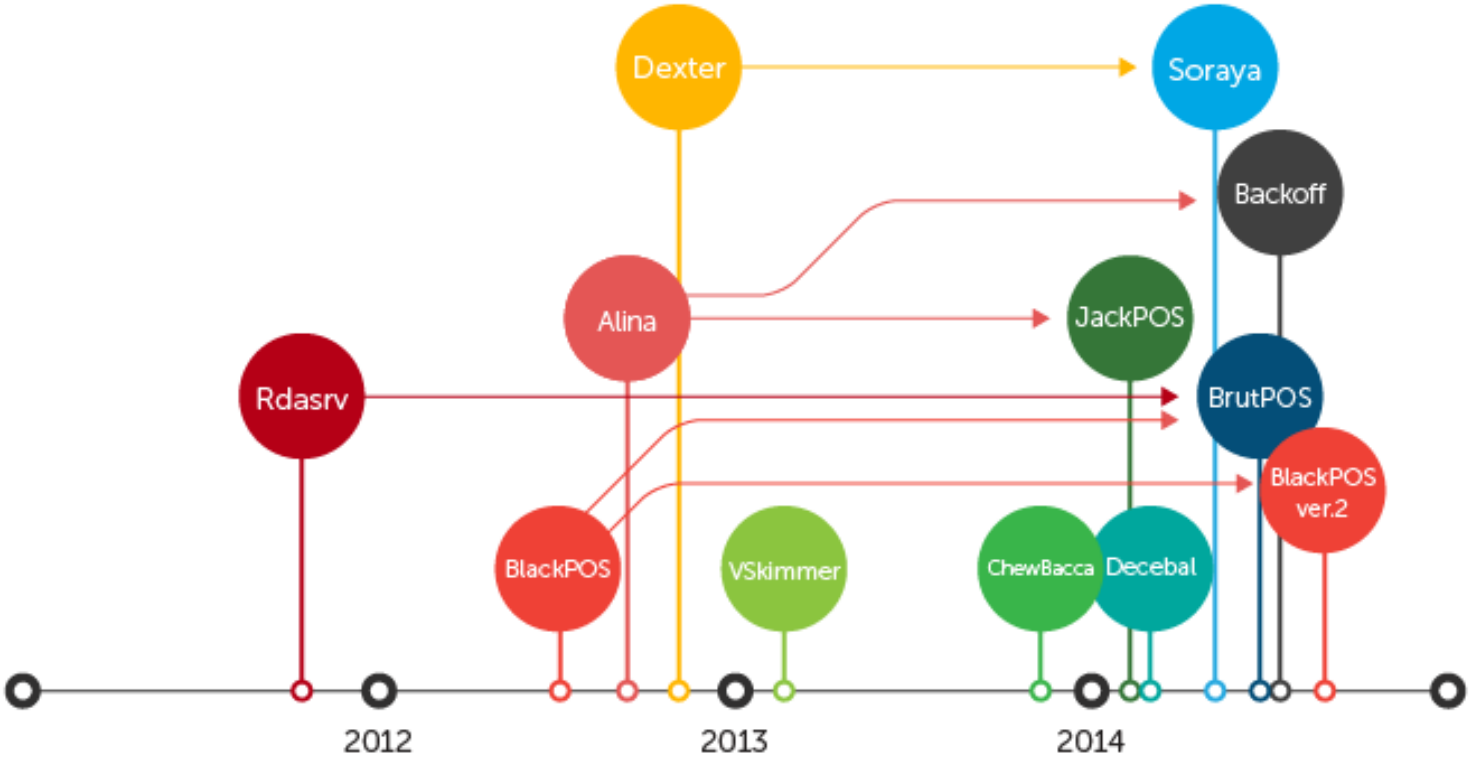
- ATM malware
  - USD $1 million loss (from 18 ATMs) reported in Malaysia
  - EAST Estimated 20 incidents of ATM in 1H2014
  - Overall ATM related fraud losses of €132 million (~USD $158 million), 7% Up

Source: http://european-atm-security.eu/files/ATM-Malware-reaches-Western-Europe-For-release-to-the-media-on-14th-October-2014.pdf

Retail (Point of Sales)

- Support various payment methods and increase attack surfaces
- Support various business needs and not only store financial data but also personal data
- Connected to corporate network through the Internet
- Low adoption rate of EMV chips in US compare with other region
- RAM (memory) scraping malware

Retail (Point of Sales)



Source: http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-evolution-of-pos-ram-scraper-malware

Impact and Loss

- POS malware

Target data breach

Nov 2013

  - 40 millions cards leaked
  - Sell USD20-45 per card

HomeDepot data breach

Sep 2014)

  - 56 millions cards leaked

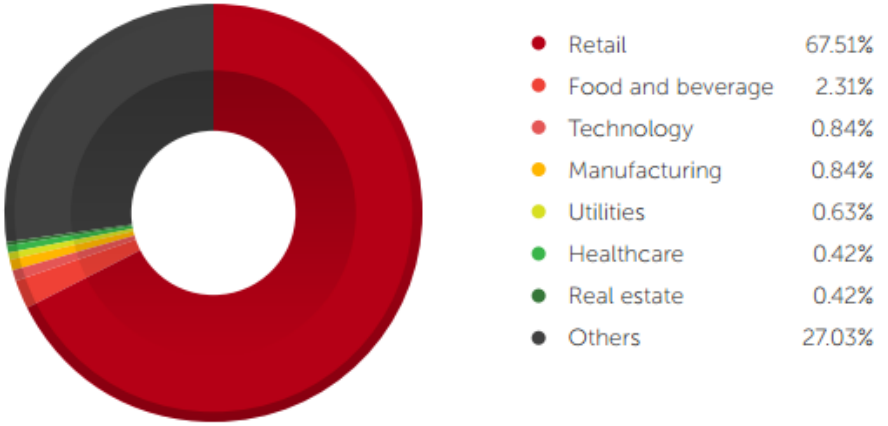


Figure 47: PoS RAM scraper detection distribution by industry

Source: http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-evolution-of-pos-ram-scraper-malware

Others

- Critical Infrastructure
  - ICS, SCADA malware
- Shipping and Logistics
- HealthCare

Case Study

Banking (ATM) - Tyupkin

- Discovered in 2014
- ATM Jackpotting Malware
- Active on more than 50 ATMs

at banking institutions in Eastern Europe

- Spread to several other countries,

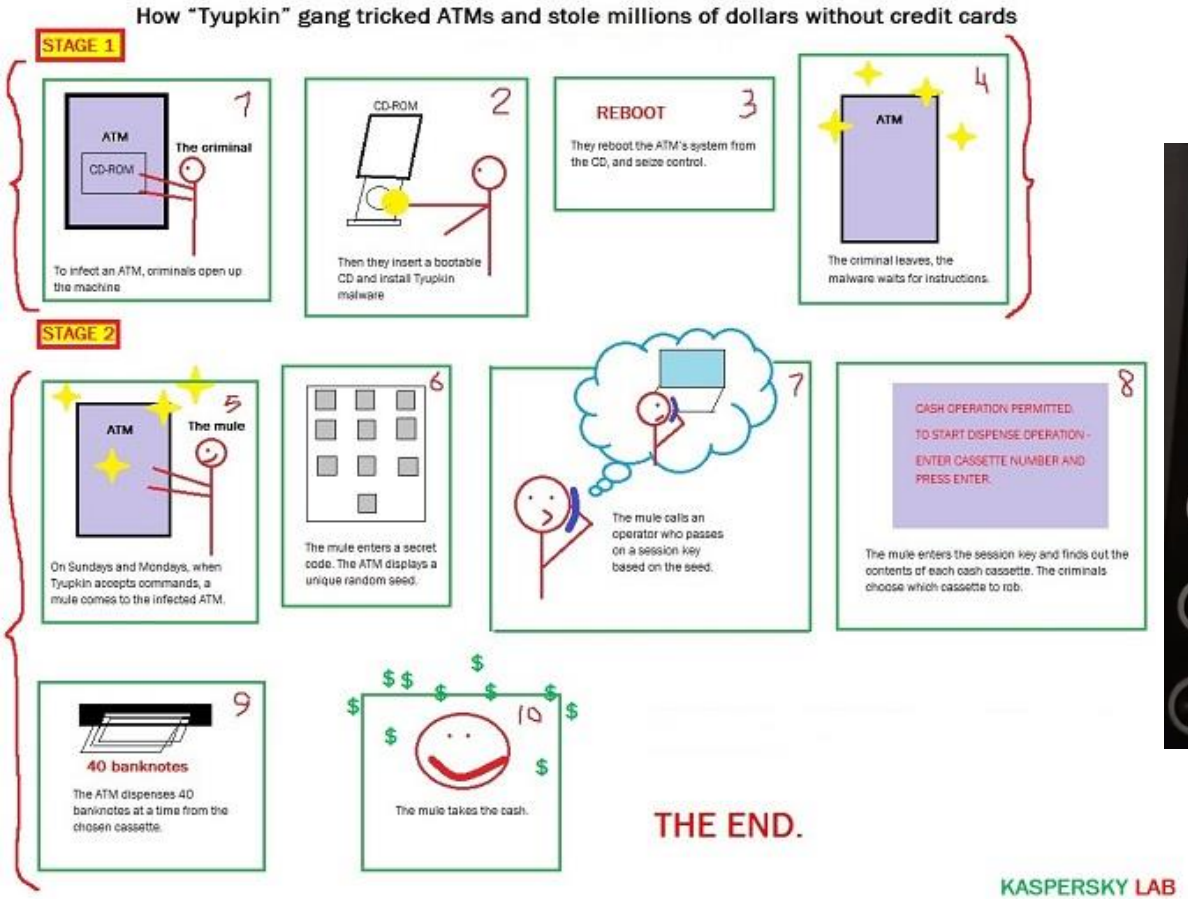
including the U.S., India and China.

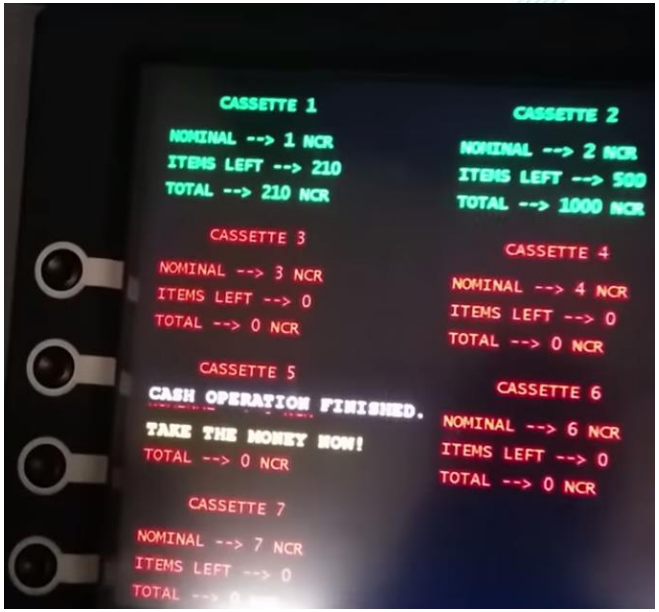
- Only affect Microsoft Windows

32bits version

- Only active at a specific time at night

Banking (ATM) - Tyupkin





Demo
https://www.youtube.com/watch?v=QZvdPM_h2o8

Source: Kaspersky Lab

PoS - BackOff

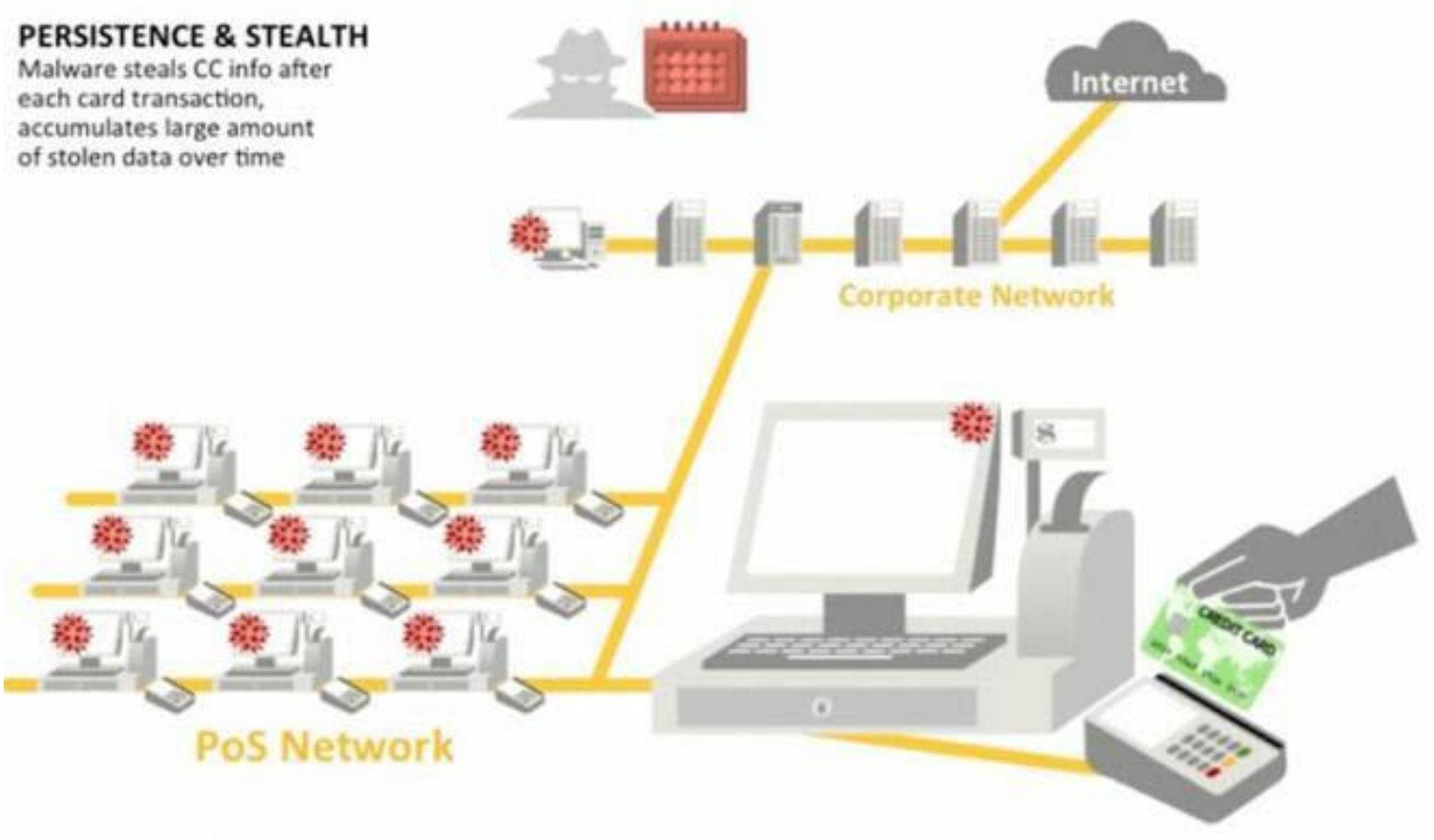
- Discovered in 2014
- 7 PoS system providers/vendors affected
- Estimated more than 1,000

U.S. businesses were affected by the malware, including Dairy Queen, SUPERVALU and UPS

- Use remote desktop applications, such as

Microsoft, Apple and Chrome Remote Desktop on infected machine

PoS - BackOff



Source: Forbes.com

PoS - BackOff

- Scan the Internet facing remote desktop application
- Brute force the login credentials of the remote desktop and gain Admin and privileged access accounts
- Install the malware and extract data by memory scraping
- Parse *Track 1* (IATA) and *Track 2* (ABA) data
- Connect to C&C to upload discovered data

Logistics – Zombie Zero

- Discovered in 2014 by TrapX
- Chinese factory responsible for selling a proprietary hw/sw scanner application used in shipping and logistics company
- Identified 8 victims

Logistics – Zombie Zero

- Embedded in a version of WindowsXP

installed on hardware or software version update

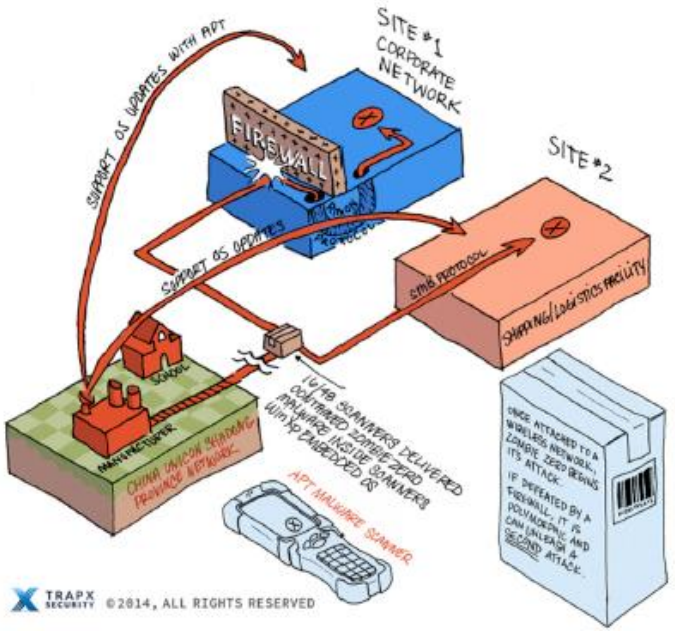
- Found in 16 out of 48 scanners
- Looked for “finance”

related server in the network

- Sent the collected financial and

ERP data to Hacker's CnC server

in China



Source: http://www.trapx.com/wp-content/uploads/2014/07/TrapX_ZOMBIE_Report_Final.pdf

Security Migitation

Banking (ATM)

Physical Protection

- Ensure the ATM is in an open, well-lit environment that is monitored by visible security cameras.
- Regularly check the ATM for signs of attached third-party devices (skimmers).
- Consider filling the ATM with just enough cash for a single day of activity.
- ATMSWG - Best practice for physical ATM security

http://www.link.co.uk/AboutLINK/site-owners/Pages/Security-for-ATMs.aspx

Banking (ATM)

System Protection

- Locking down the BIOS to prevent booting from unauthorized media, such as CD ROMs or USB sticks
- Use disk encryption to avoid tampering
- Upgrading to a supported operating system such as Windows 7

PCI ATM security guidelines

https://www.pcisecuritystandards.org/pdfs/PCI_ATM_Security_Guidelines_Info_Supplement.pdf

Retail (POS)

- Segregate your networks.
- Limit the applications allowed on your POS computers.
- Review firewall configurations and only allow access from authorized source and provide required port/service.
- If your anti-virus has a Live Protection service, make sure it is on and working.

Source: https://nakedsecurity.sophos.com/2014/08/25/secret-service-says-backoff-malware-hit-1000-businesses-6-tips/

Retail (POS)

- Review remote access policies and procedures.
- Consider requiring the use of a Virtual Private Network (VPN) with two-factor authentication(2FA) support.
- Enable logging of events and make sure there is a process to monitor logs on a daily basis.

Microsoft Windows Hardening Guide

http://download.microsoft.com/documents/en-us/Protecting_Point_of_Sale_Devices-April_2014.pdf

Conclusion

Criminals looking for the weakest link

- Physical protection
- Network Access Control
- Password policy
- Secure Remote Access
- Auditing

Thank You

Q & A

HKCERT
Website: www.hkcert.org
Email: hkcert@hkcert.org
Tel: 81056060