Malware de Terminales Punto de Venta:

evolución, tipos y características

Ricardo J. Rodríguez
Universidad de Zaragoza

cyber camp
CYBERSECURITY EVENT
2016

GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

incibe_
TRABAJANDO POR LA CONFIANZA DIGITAL

CyberCamp.es

$whoami

- CLS member (2001)
- Ph.D. on Comp. Sci. (2013)
- Assistant Professor at University of Zaragoza
- Research lines:
  - Aspects of theoretical computer science and security
  - Security-(performance/safety-)driven engineering
  - Malware (anti-)analysis
  - RFID/NFC Security
- Not prosecuted ⌣̈
- Speaker/Trainer at NcN, HackLU, RootedCON, STIC CCN-CERT, HIP,

#sinCiencia
no hay futuro

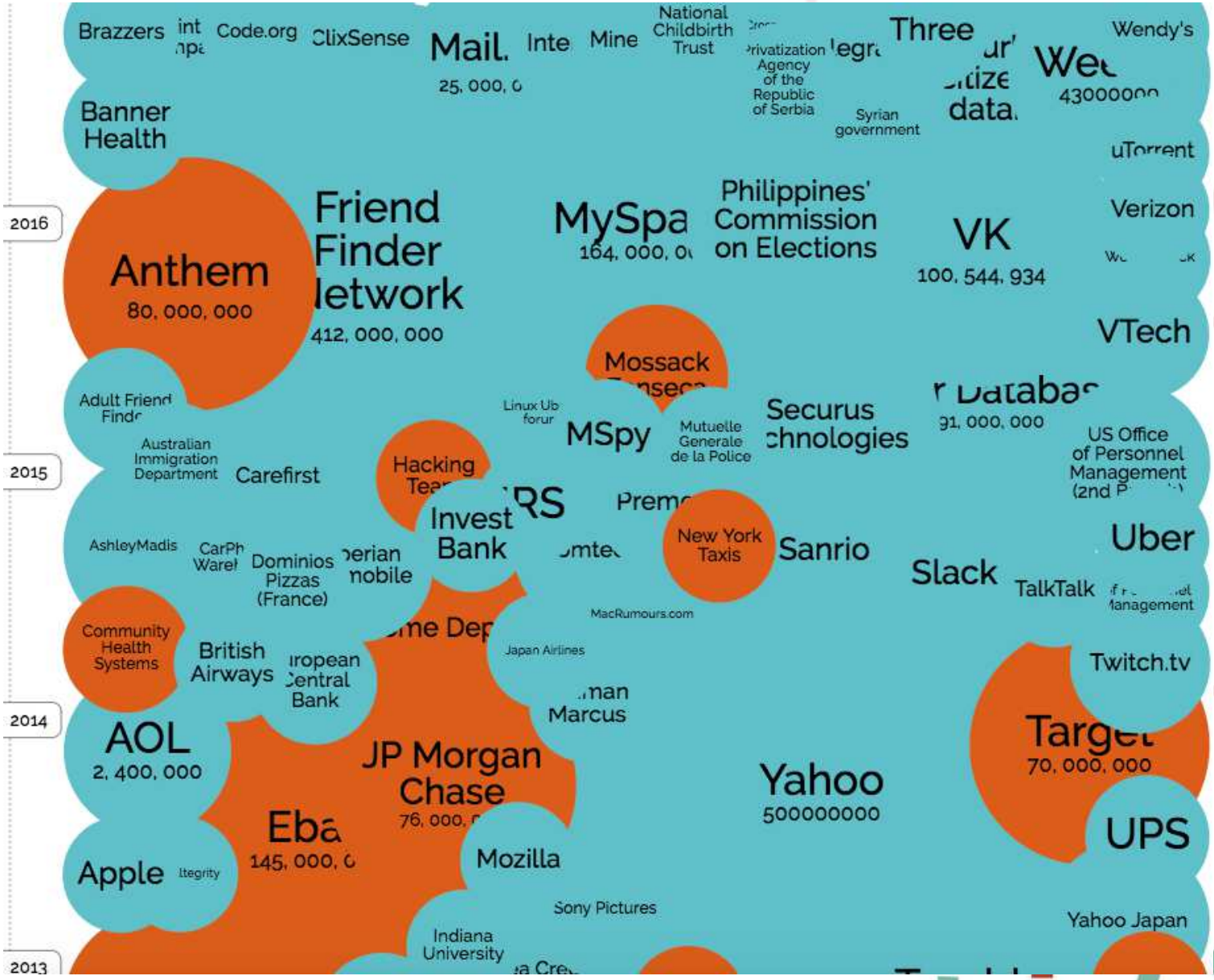
Agenda

1. Introduction
2. POS Card Transaction Flow
3. Ways to Access to Credit Card Data
4. POS RAM Scraping Malware
   - Features
   - Classification and Discussions
5. DEMO
6. Related Work
7. Conclusions

Agenda

1. Introduction
2. POS Card Transaction Flow
3. Ways to Access to Credit Card Data
4. POS RAM Scraping Malware
   - Features
   - Classification and Discussions
5. DEMO
6. Related Work
7. Conclusions

Introduction



Credits: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Introduction

Financial services

- Provides essential services to our society
  - Credit & debit cards are becoming primary payment method
    - Some countries even want to set them as the unique payment method
- Outages mainly caused by intended *events*
  - Increasing trend of (cyber)attacks have been reported

Introduction

Financial services

- Provides essential services to our society
  - Credit & debit cards are becoming primary payment method
    - Some countries even want to set them as the unique payment method
- Outages mainly caused by intended *events*
  - Increasing trend of (cyber)attacks have been reported

Credit & debit card data

- Sought-after items in underground market
  - US credit card data: \$1.5 $\sim$ \$5 – discounts may apply when bulk buying!
  - EU credit card data are expensive (\$5 $\sim$ \$8)
  - Price depends in card type and other data (e.g., US *fullz* data $+$\$20)
- Minimum data needed to complete a payment
  - Cardholder name, expiry date, and credit card number

Introduction

Where are these data coming from, dude?

- Mainly retrieved from Point-of-Sale (POS) devices
  - In-store systems used to pay merchants for good or services
- Summary of publicly known cyberattacks in 2014 reported 36% related to stolen credit card customer data
  - Mostly occurred at retailers and restaurants

Thank you, Windows!

- 88% POS systems are Windows-based environments (in different flavours)
- Increasing trend of attacks: from skimming terminals to network sniffing

Thank you, Windows!

- 88% POS systems are Windows-based environments (in different flavours)
- Increasing trend of attacks: from skimming terminals to network sniffing
  - The TXJ Companies, Inc., 2008: wireless network using WEP ¨‿
    - ≈40M of credit card customer data stolen → do the maths!
    - Albert Gonzalez was found guilty for these felonies and sentenced to 20 years

Thank you, Windows!

- 88% POS systems are Windows-based environments (in different flavours)
- Increasing trend of attacks: from skimming terminals to network sniffing
  - The TXJ Companies, Inc., 2008: wireless network using WEP 😐
    - ≈40M of credit card customer data stolen → do the maths!
    - Albert Gonzalez was found guilty for these felonies and sentenced to 20 years

POS RAM Scrapping malware

- Specially crafted malware to attack these systems
- Currently, their major threat (before it was network sniffing)
- Ad-hoc solutions from numerous vendors

Introduction

Another piece of history...

2013 Target.

`BlackPOS` stole ≈40M of records in three weeks

2014 Home Depot.

`FrameworkPOS` (a variant of `BlackPOS`) stole ≈56M of records in a five-month attack

Introduction

Another piece of history...

2013 Target.
`BlackPOS` stole ≈40M of records in three weeks

2014 Home Depot.
`FrameworkPOS` (a variant of `BlackPOS`) stole ≈56M of records in a five-month attack

Evolution and characterization of this kind of malware

RQ1. Functionality and persistence

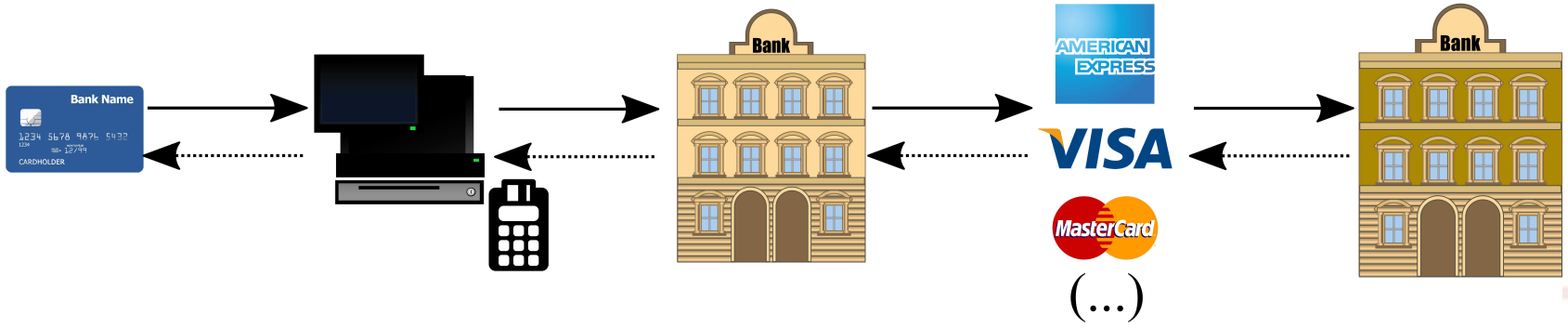
RQ2. Processes search data scrapped

RQ3. Exfiltration of scrapped data

Agenda

1. Introduction
2. POS Card Transaction Flow
3. Ways to Access to Credit Card Data
4. POS RAM Scraping Malware
   - Features
   - Classification and Discussions
5. DEMO
6. Related Work
7. Conclusions

POS Card Transaction Flow



But. . . where data may be accessed?

- Data in memory: in the processing machine while being manipulated
- Data at rest: temporarily or for long-term storing
- Data in transit: following between devices within the system
- Own application running into POS systems

POS Card Transaction Flow

PCI rocks!

Oh. . . wait. . .

POS Card Transaction Flow

PCI rocks!

Oh. . . wait. . .

Payment Card Industries standard

- PCI Data Security Standard (PCI-DSS)
  - Defines how sensitive cardholder data must be protected by the merchants and service providers (acquirer/issuer banks)
- Payment Application Data Security Standard (PA-DSS)
  - Defines software requirements to be fulfilled by payment applications in compliance with PCI-DSS

Agenda

1. Introduction
2. POS Card Transaction Flow
3. Ways to Access to Credit Card Data
4. POS RAM Scraping Malware
   - Features
   - Classification and Discussions
5. DEMO
6. Related Work
7. Conclusions

Ways to Access to Credit Card Data

Physical Data

- Name

Ways to Access to Credit Card Data

Physical Data

- Name
- Expiration date: in “YY/MM” format

Ways to Access to Credit Card Data

Physical Data

- Name
- Expiration date: in “YY/MM” format
- Credit Card Number / Primary Account Number (PAN)

Ways to Access to Credit Card Data

Physical Data

- Name
- Expiration date: in “YY/MM” format
- Credit Card Number / Primary Account Number (PAN)
- Card Verification Value (CVV): 3 to 4-digit value, depends on card manufacturer

Ways to Access to Credit Card Data

Physical Data

- Name
- Expiration date: in “YY/MM” format
- Credit Card Number / Primary Account Number (PAN)
- Card Verification Value (CVV): 3 to 4-digit value, depends on card manufacturer
  - Proves physical access to the card

Ways to Access to Credit Card Data

Magnetic Stripe

- Three tracks, but Track 3 not really used
  - Track 1 & 2: ISO/IEC 7813
  - Track 3: ISO/IEC 4909 (also known as THRIFT)

SS	FC	PAN	FS	CN	FS	ED	SC	DD	ES	LRC

(a) Track 1

SS	PAN	FS	ED	SC	DD	ES	LRC

(b) Track 2

Check this out! `https://youtu.be/UHSFf0Lz1qc`

Ways to Access to Credit Card Data

Chip cards

- Chip-and-PIN / EMV cards
- Unique transaction ID that prevents replay
- Any transaction is previously authorized (theoretically)
- Several flaws reported in literature
  - Nobody fucking care about identity of the POS terminal
- Just remember this: **EMV was created to counterfeiting card fraud, not to protect data confidentiality**

Ways to Access to Credit Card Data

Chip cards

- Chip-and-PIN / EMV cards
- Unique transaction ID that prevents replay
- Any transaction is previously authorized (theoretically)
- Several flaws reported in literature
  - Nobody fucking care about identity of the POS terminal
- Just remember this: **EMV was created to counterfeiting card fraud, not to protect data confidentiality**

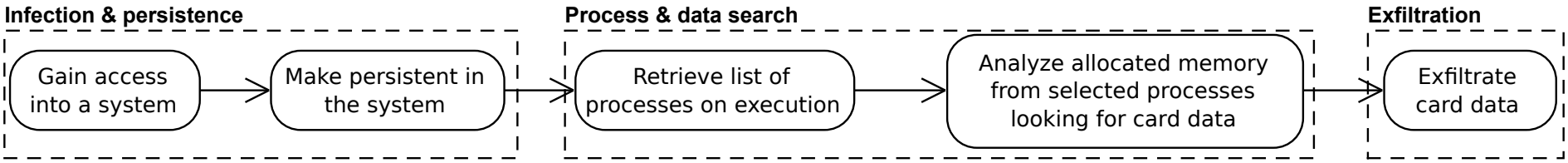
Contactless cards

- Just another door to access to the card content without *any* physical contact
- Payments of limited value (and limited amounts of time)

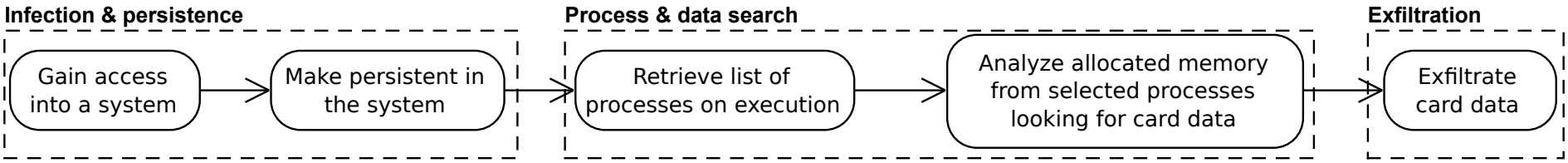
Agenda

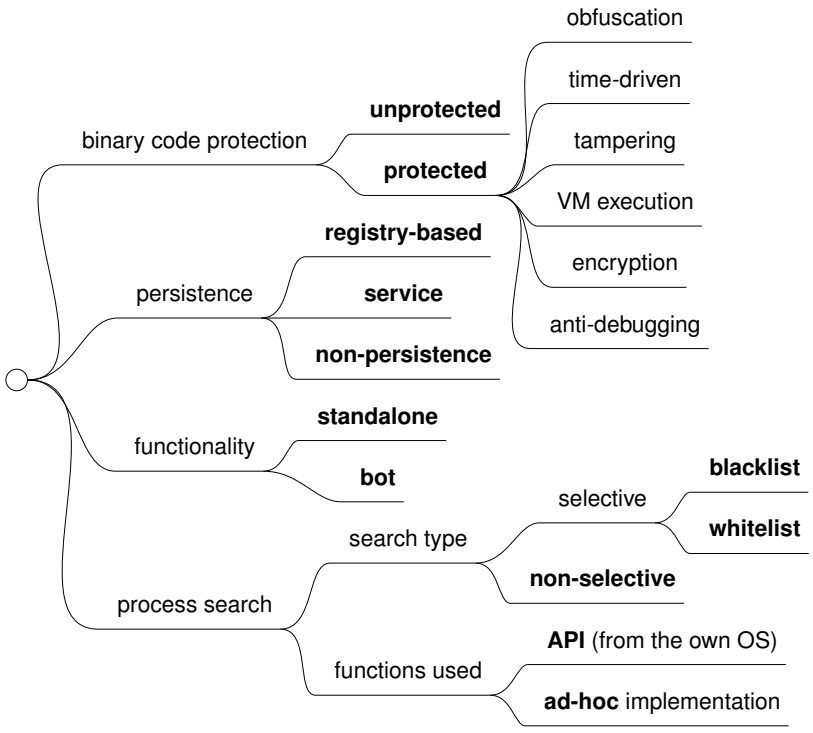
1. Introduction
2. POS Card Transaction Flow
3. Ways to Access to Credit Card Data
4. POS RAM Scraping Malware
   - Features
   - Classification and Discussions
5. DEMO
6. Related Work
7. Conclusions

Features of POS RAM Scraping Malware

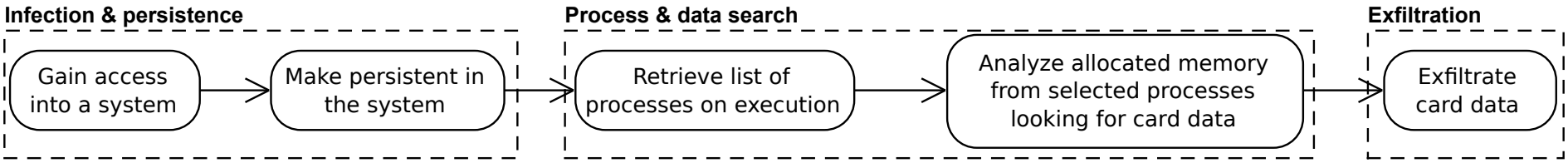


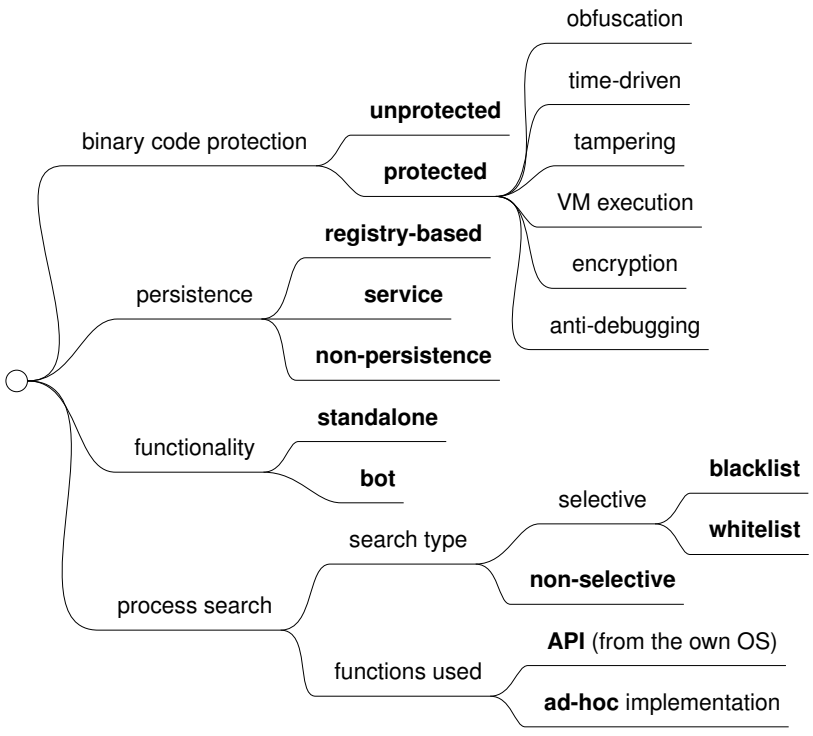
Features of POS RAM Scraping Malware

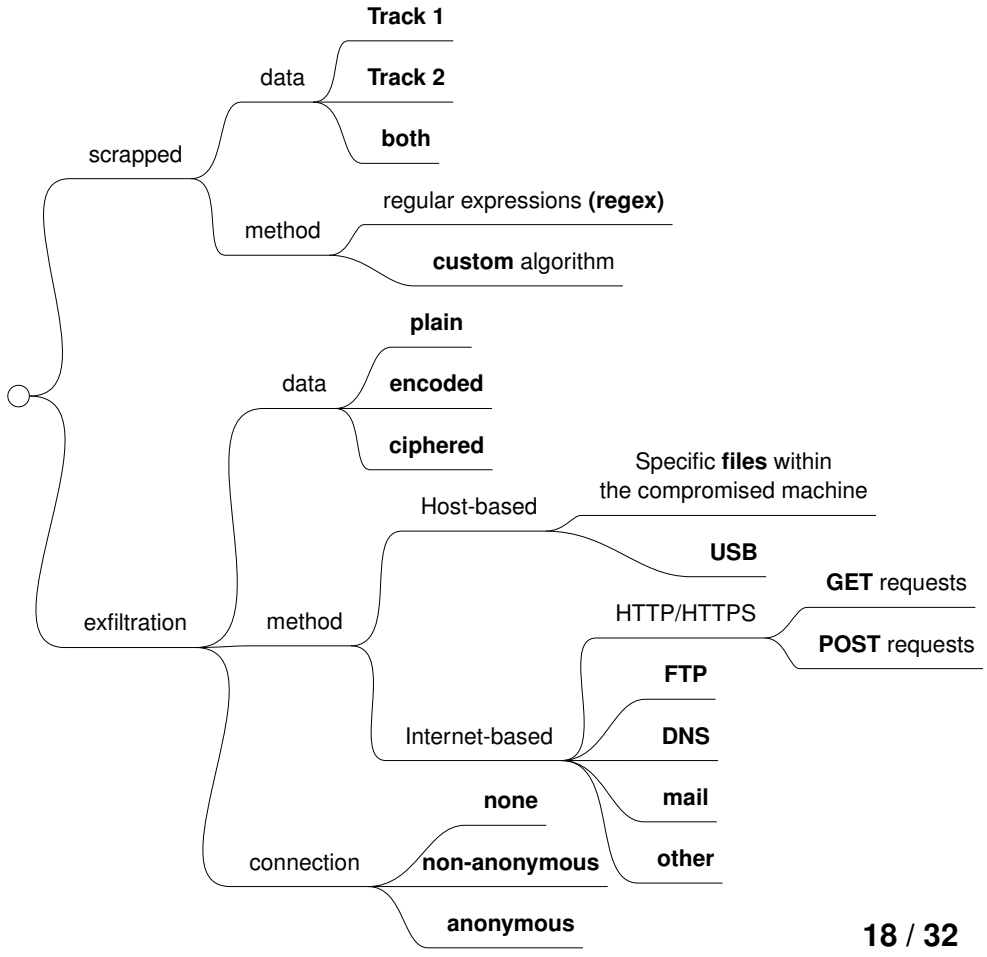




Features of POS RAM Scraping Malware







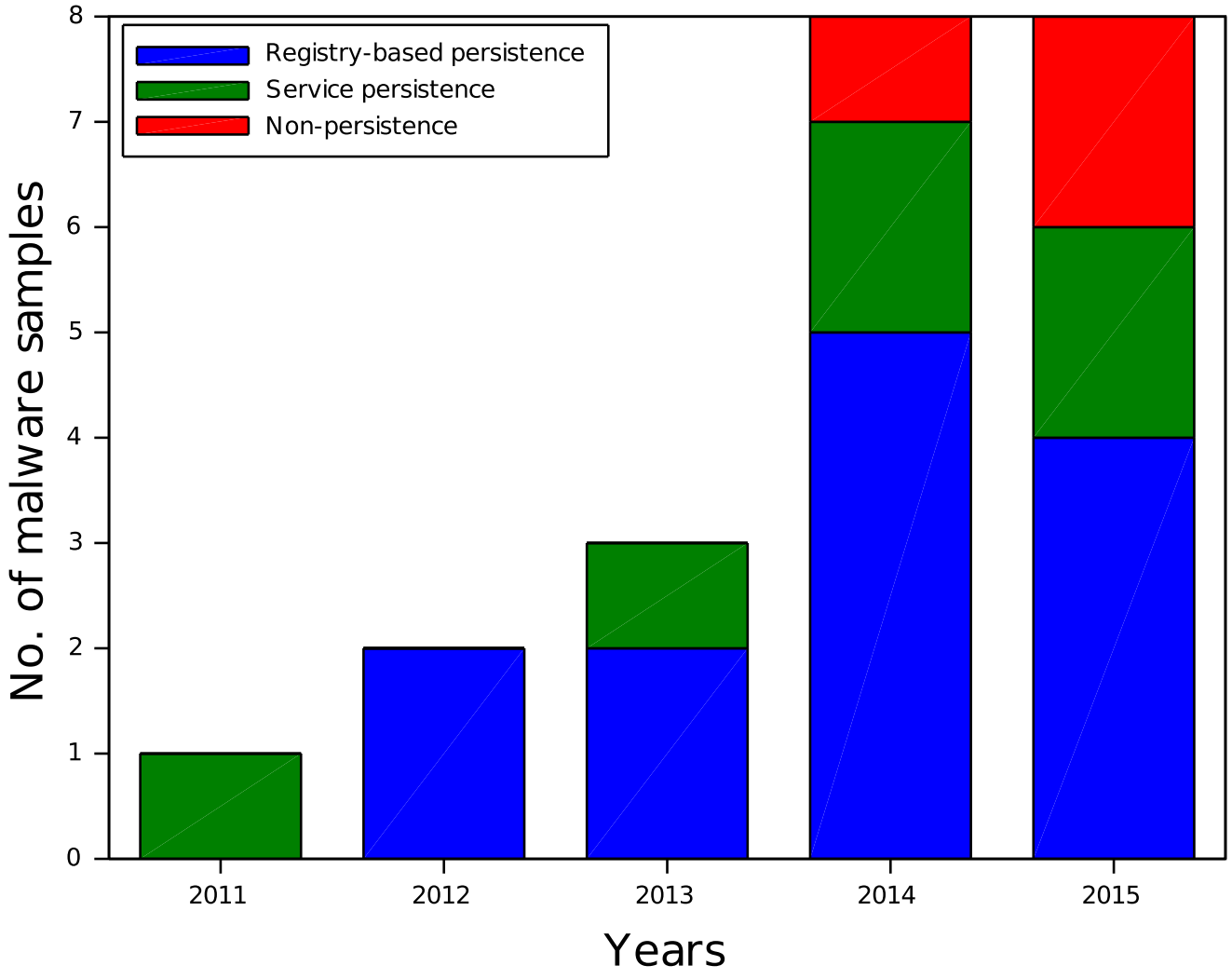
Classification and Discussions

- 144 samples from 22 known families
- Sample with highest VT ratio selected as most representative

Malware family	Other names	Discovery date	Selected sample	VT ratio
rdasrv		2011 (Q4)	516cef2625a822a253b89b9ef523ba37	47 out of 52
ALINA		2012 (Q4)	1efeb85c8ec2c07dc0517ccca7e8d743	46 out of 55
Dexter		2012 (Q4)	70feec581cd97454a74a0d7c1d3183d1	50 out of 54
vSkimmer		2013 (Q1)	dae375687c520e06cb159887a37141bf	48 out of 55
BlackPOS	KAPTOXA, Reedum	2013 (Q2)	d9cc74f36ff173343c6c7e9b4db228cd	45 out of 52
FYSNA	Chewbacca	2013 (Q4)	21f8b9d9a6fa3a0cd3a3f0644636bf09	47 out of 55
Decebal		2014 (Q1)	d870d85e89f3596a016fdd393f5a8b39	41 out of 55
JackPOS		2014 (Q1)	75990dde85fa2722771bac1784447f39	41 out of 52
Soraya		2014 (Q2)	1483d0682f72dfefff522ac726d22256	43 out of 55
BackOff	PoSeidon, FindPOS	2014 (Q3)	17e1173f6fc7e920405f8dbde8c9ecac	49 out of 56
BrutPOS		2014 (Q3)	95b13cd79621931288bd8a8614c8483f	42 out of 53
FrameworkPOS	BlackPOS v2	2014 (Q3)	b57c5b49dab6bbd9f4c464d396414685	45 out of 56
GetmypassPOS		2014 (Q4)	1d8fd13c890060464019c0f07b928b1a	35 out of 56
LusyPOS		2014 (Q4)	bc7bf2584e3b039155265642268c94c7	47 out of 56
LogPOS		2015 (Q1)	af13e7583ed1b27c4ae219e344a37e2b	44 out of 56
Punkey		2015 (Q2)	b1fe4120e3b38784f9fe57f6bb154517	44 out of 56
FighterPOS		2015 (Q2)	b0416d389b0b59776fe4c4ddeb407239	43 out of 57
NitlovePOS		2015 (Q2)	6cdd93dcb1c54a4e2b036d2e13b51216	47 out of 56
MalumPOS		2015 (Q2)	acdd2cffc40d73fdc11eb38954348612	36 out of 56
BernhardPOS		2015 (Q3)	e49820ef02ba5308ff84e4c8c12e7c3d	43 out of 56
GamaPOS		2015 (Q3)	58e5dd98015164b40de533e379ed6ac8	43 out of 55
AbbaddonPOS		2015 (Q4)	46810f106dbaaff5c3c701c71aa16ee9	39 out of 56

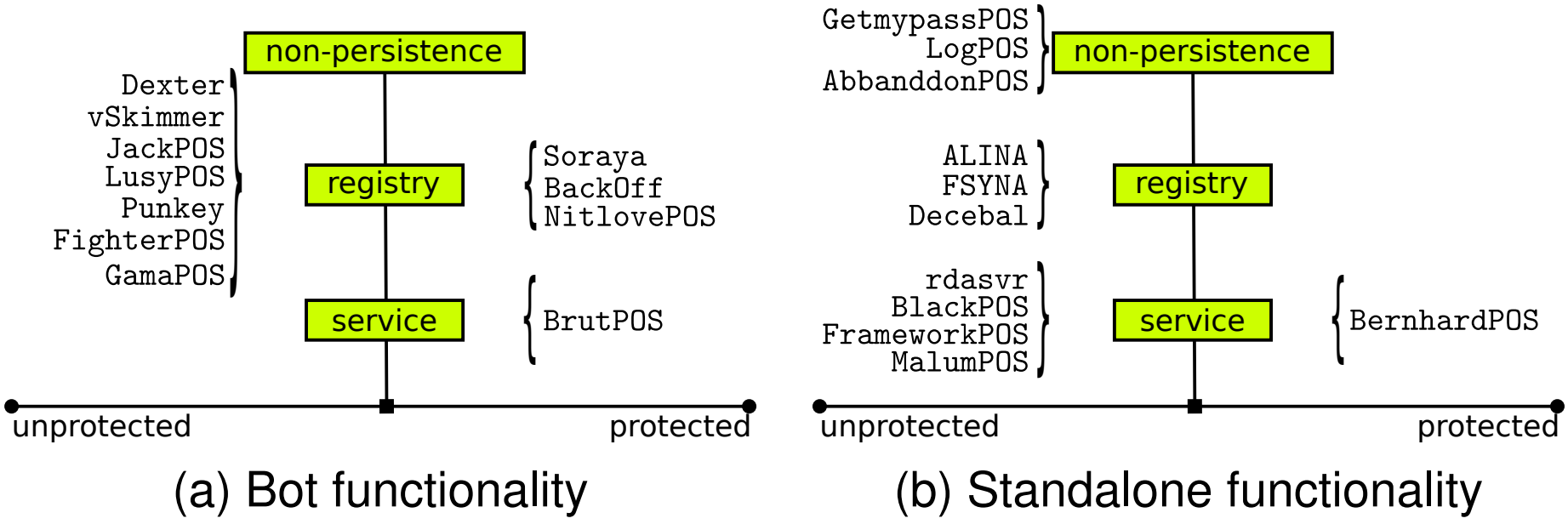
Classification and Discussions

On Evolution



Classification and Discussions (III)

On Infection and Persistence



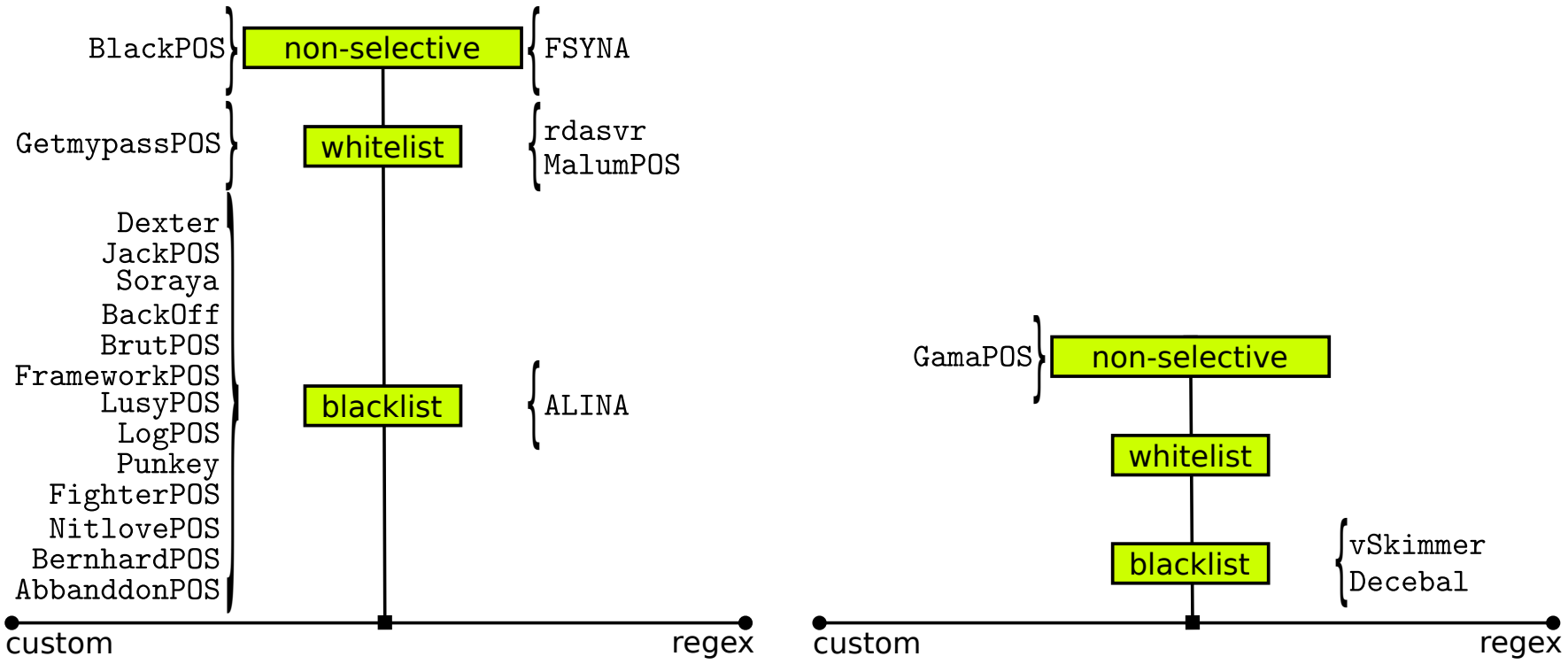
(a) Bot functionality

(b) Standalone functionality

- Mainly C++ and Delphi binaries
  - `GamaPOS` is .NET
- UPX and custom packer (5 out of 22)
  - Only three families use anti-analysis tricks
- Mostly registry-based persistence
  - `NitlovePOS` uses NTFS ADS

Classification and Discussions

On Process and Data Search (1)



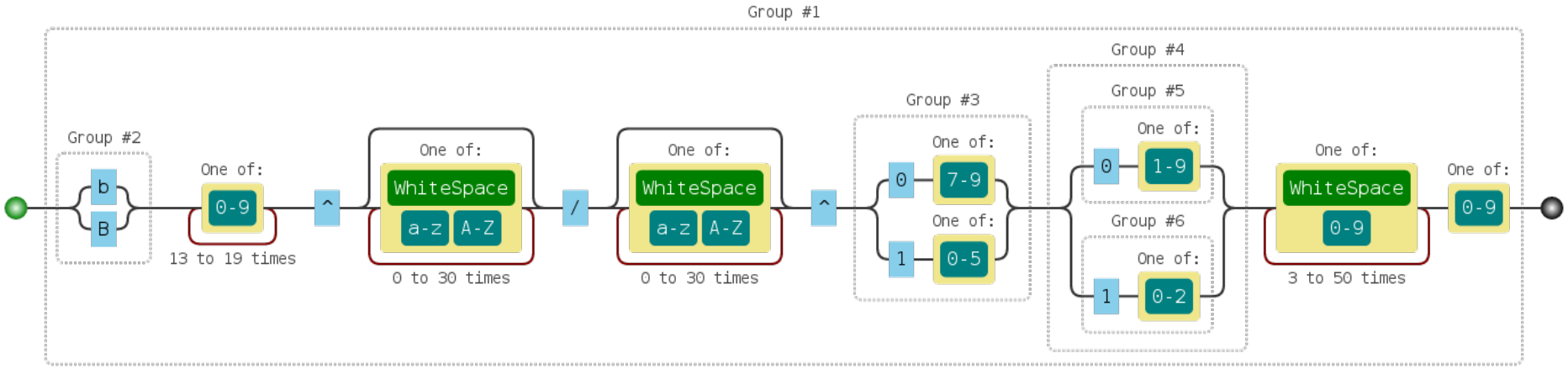
Classification and Discussions

On Process and Data Search (2)

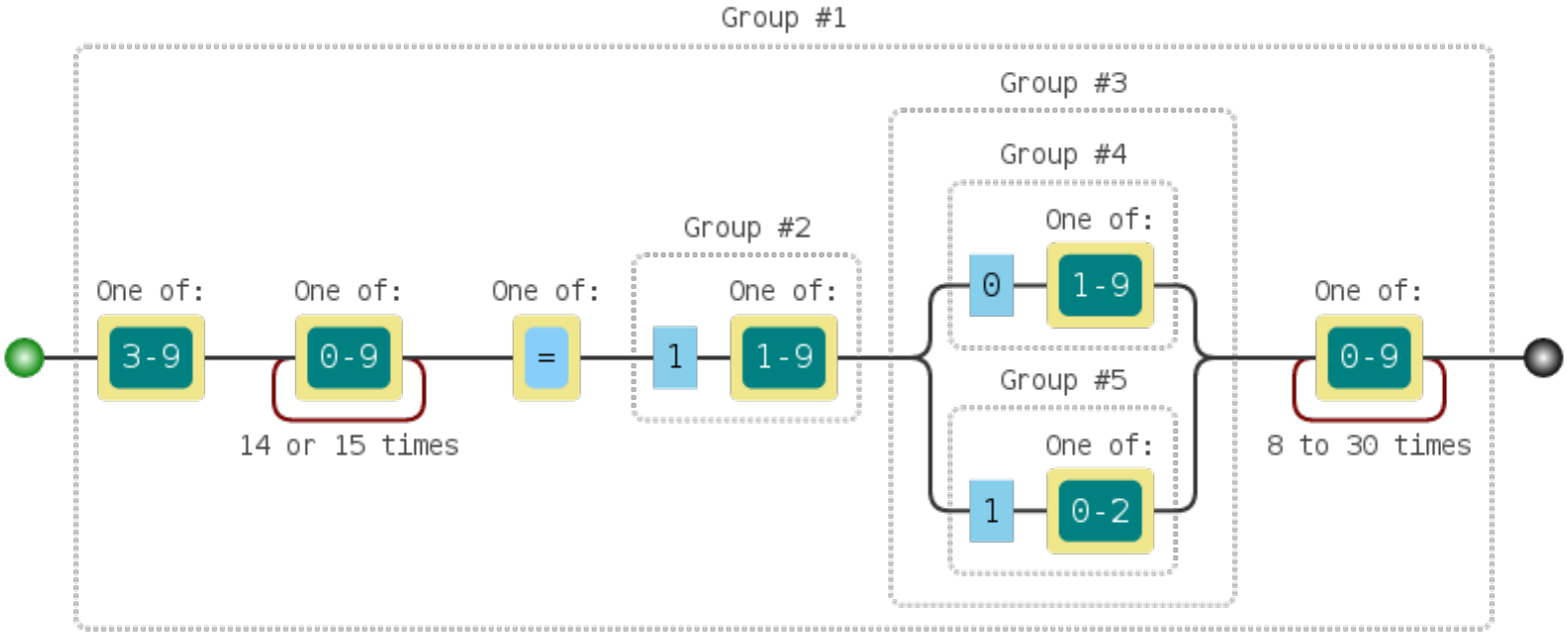
- Mostly process blacklisting
  - `AbbanddonPOS` only excludes itself ⌣̈
  - 3 out of 22 search for particular processes
  - The same number analyze any process on execution
- Windows APIs for collecting processes
  - *CreateToolhelp32Snapshot*
  - *EnumProcesses*
  - *ZwQuerySystemInformation* (`BernhardPOS`)
- Read of process memory from the malware itself
  - `BernhardPOS`, `LogPOS`: inject the reading process into the victim's process ⌣̈
- Some samples include a custom implementation of Luhn formula
- Track 1 & Track 2, or Track 2 only. None looks only for Track 1 data.

Classification and Discussions

RegExp: /((b|B)[0-9]{13,19}\^[A-Za-z\s]{0,30}\/[A-Za-z\s]{0,30}\^(0[7-9]|1[0-5])((0[1-9])|(1[0-2]))[0-9\s]{3,50}[0-9]{1})/

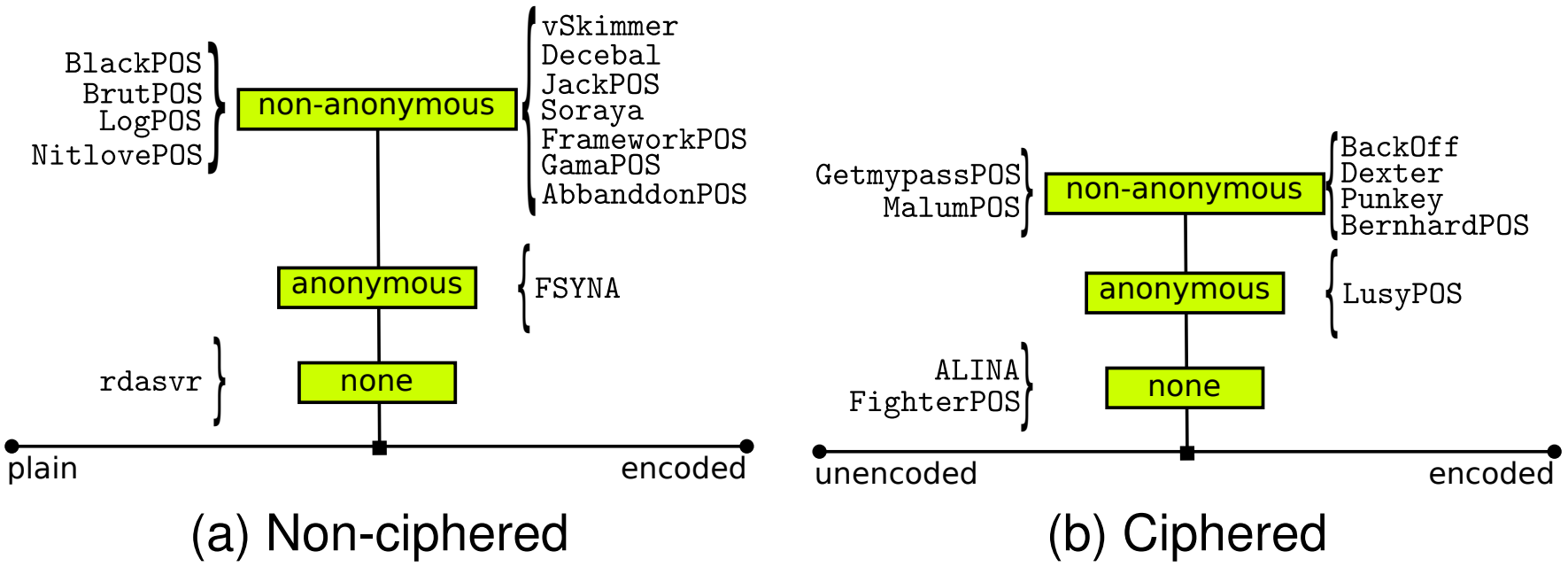


RegExp: /([3-9]{1}[0-9]{14,15}[=](1[1-9])((0[1-9])|(1[0-2]))[0-9]{8,30})/



Classification and Discussions (VI)

On Exfiltration



- Mainly, data encoded or/and ciphered
- HTTP POST (commonly)
  - 3 out of 22 generate files in the compromised machine
  - DNS requests and specific USB drives (e.g., `vSkimmer`)
- Non-anonymous communication
  - `FSYNA`, `LusyPOS` use TOR network

Agenda

1. Introduction
2. POS Card Transaction Flow
3. Ways to Access to Credit Card Data
4. POS RAM Scraping Malware
   - Features
   - Classification and Discussions
5. DEMO
6. Related Work
7. Conclusions

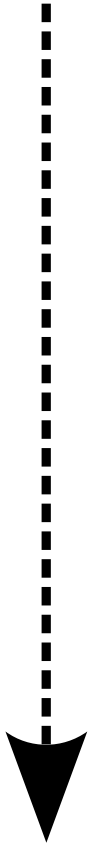
The PinAPIhook tool

What is DBI?

Dynamic Binary Instrumentation (DBI)

- Analyze the runtime behavior of a binary
- Executes arbitrary code during normal execution of a binary

- Arbitrary code insertion during binary code execution



Running code

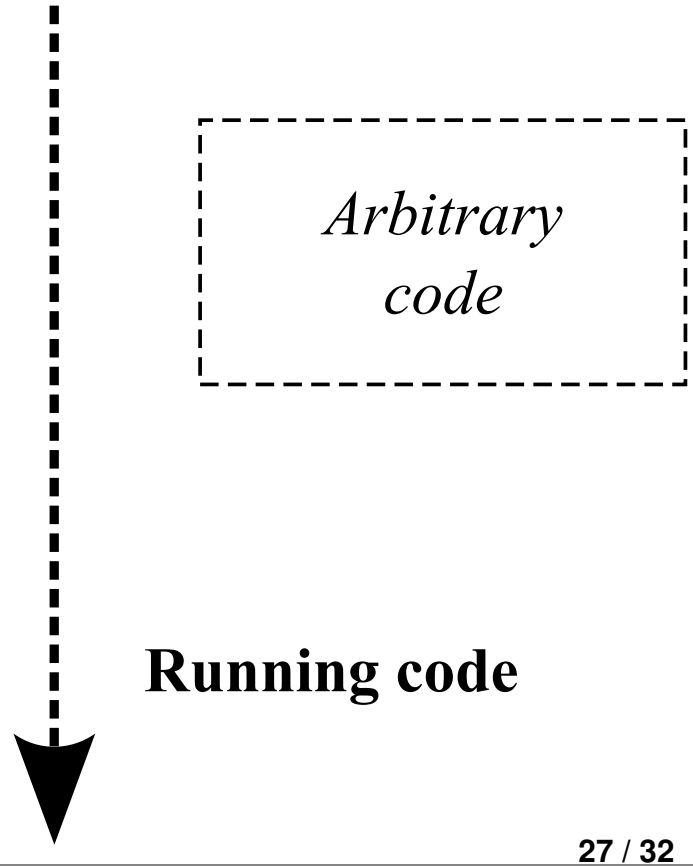
The PinAPIhook tool

What is DBI?

Dynamic Binary Instrumentation (DBI)

- Analyze the runtime behavior of a binary
- Executes arbitrary code during normal execution of a binary

- Arbitrary code insertion during binary code execution
- What do I insert? → instrumentation function



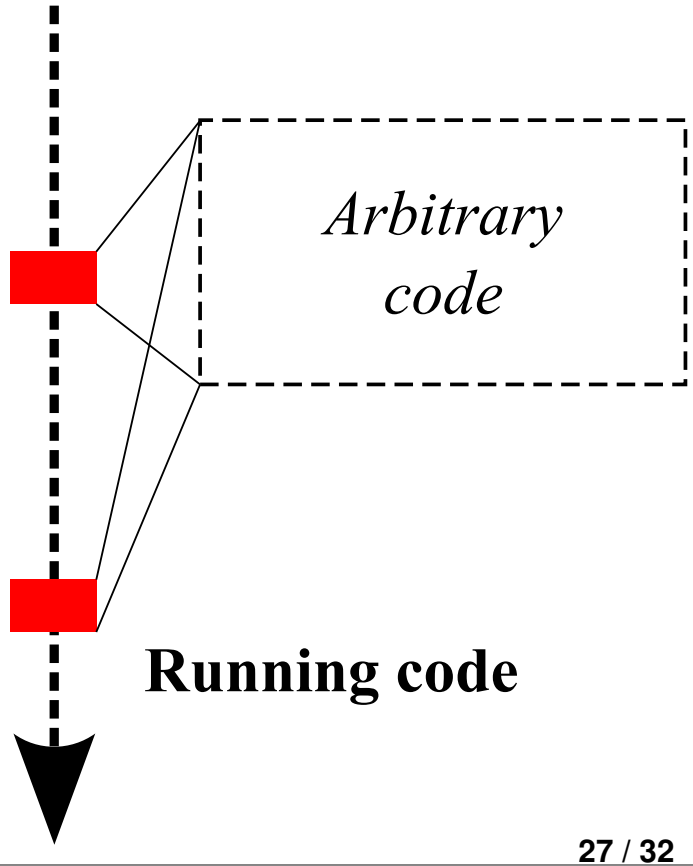
The PinAPIhook tool

What is DBI?

Dynamic Binary Instrumentation (DBI)

- Analyze the runtime behavior of a binary
- Executes arbitrary code during normal execution of a binary

- Arbitrary code insertion during binary code execution
- What do I insert? → instrumentation function
- Where? → addition places

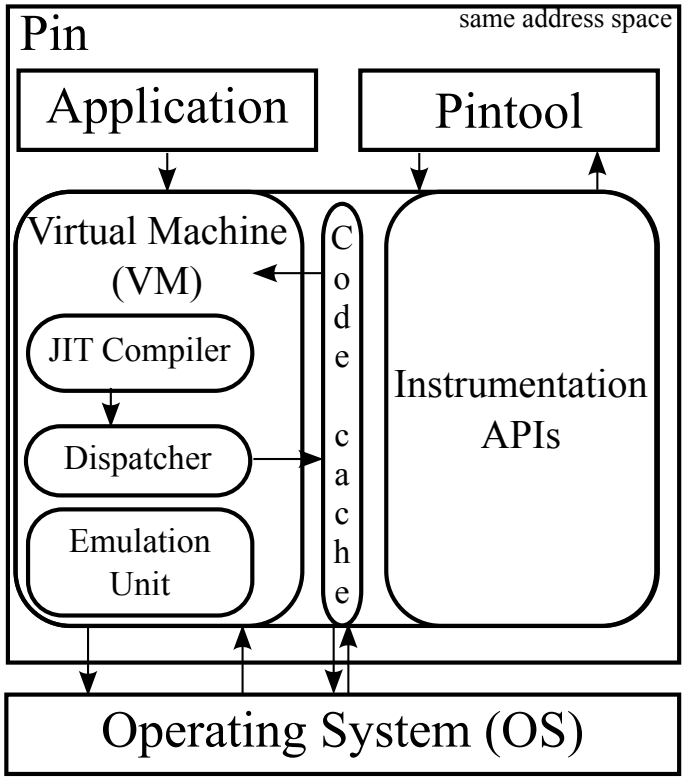


The PinAPIhook tool

Pin

What is Pin?

- Framework designed by Intel
- Allows to build easy-to-use, portable, transparent and efficient instrumentation tools (DBA, or Pintools)
- Recall: instrumentation enables the execution of arbitrary code during run-time of a binary



PinAPIhook

- APIs intercepted: **files, registry, processes, network**
- We intercept when a program *calls* any API to inspect parameters and execution result
  - Note that we could fake the return result

Live Demo

MD5: `0de9765c9c40c2c2f372bf92e0ce7b68`

(slightly patched for demo)

Agenda

1. Introduction
2. POS Card Transaction Flow
3. Ways to Access to Credit Card Data
4. POS RAM Scraping Malware
   - Features
   - Classification and Discussions
5. DEMO
6. Related Work
7. Conclusions

Related Work

Regarding taxonomies

- Computer worms
- Advanced Persistent Threats
- Analysis-aware malware
- Botnet structures
- Software packers (based on run-time complexity)

Related Work

Regarding taxonomies

- Computer worms
- Advanced Persistent Threats
- Analysis-aware malware
- Botnet structures
- Software packers (based on run-time complexity)

Others...

- Tool to identify credit card data in commercial payment systems
  - Scraps the network packets
- Security analysis of audio MSRs for mobile devices

Agenda

1. Introduction
2. POS Card Transaction Flow
3. Ways to Access to Credit Card Data
4. POS RAM Scraping Malware
   - Features
   - Classification and Discussions
5. DEMO
6. Related Work
7. Conclusions

Conclusions

- RAM scraping is the major threat at the moment
- POS RAM scraping malware workflow
  1. Make persistence

Conclusions

- RAM scraping is the major threat at the moment
- POS RAM scraping malware workflow
  1. Make persistence
  2. Retrieve list of processes on execution

Conclusions

- RAM scraping is the major threat at the moment
- POS RAM scraping malware workflow
  1. Make persistence
  2. Retrieve list of processes on execution
  3. Scan its memory looking for credit card data

Conclusions

- RAM scraping is the major threat at the moment
- POS RAM scraping malware workflow
  1. Make persistence
  2. Retrieve list of processes on execution
  3. Scan its memory looking for credit card data
  4. When found, exfiltrate it (somehow)

Conclusions

- RAM scraping is the major threat at the moment
- POS RAM scraping malware workflow
  1. Make persistence
  2. Retrieve list of processes on execution
  3. Scan its memory looking for credit card data
  4. When found, exfiltrate it (somehow)
- Samples of 22 families analyzed based on their workflow

Conclusions

- RAM scraping is the major threat at the moment
- POS RAM scraping malware workflow
  1. Make persistence
  2. Retrieve list of processes on execution
  3. Scan its memory looking for credit card data
  4. When found, exfiltrate it (somehow)
- Samples of 22 families analyzed based on their workflow

Take-home messages

- Few families use analysis-aware tricks

Conclusions

- RAM scraping is the major threat at the moment
- POS RAM scraping malware workflow
  1. Make persistence
  2. Retrieve list of processes on execution
  3. Scan its memory looking for credit card data
  4. When found, exfiltrate it (somehow)
- Samples of 22 families analyzed based on their workflow

Take-home messages

- Few families use analysis-aware tricks
- Detectable persistence methods (mainly registry-based)

Conclusions

- RAM scraping is the major threat at the moment
- POS RAM scraping malware workflow
  1. Make persistence
  2. Retrieve list of processes on execution
  3. Scan its memory looking for credit card data
  4. When found, exfiltrate it (somehow)
- Samples of 22 families analyzed based on their workflow

Take-home messages

- Few families use analysis-aware tricks
- Detectable persistence methods (mainly registry-based)
  - One of them uses NTFS ADS

Conclusions

- RAM scraping is the major threat at the moment
- POS RAM scraping malware workflow
  1. Make persistence
  2. Retrieve list of processes on execution
  3. Scan its memory looking for credit card data
  4. When found, exfiltrate it (somehow)
- Samples of 22 families analyzed based on their workflow

Take-home messages

- Few families use analysis-aware tricks
- Detectable persistence methods (mainly registry-based)
  - One of them uses NTFS ADS
- Process blacklisting

Conclusions

- RAM scraping is the major threat at the moment
- POS RAM scraping malware workflow
  1. Make persistence
  2. Retrieve list of processes on execution
  3. Scan its memory looking for credit card data
  4. When found, exfiltrate it (somehow)
- Samples of 22 families analyzed based on their workflow

Take-home messages

- Few families use analysis-aware tricks
- Detectable persistence methods (mainly registry-based)
  - One of them uses NTFS ADS
- Process blacklisting
- Data exfiltration thru. encoded data and non-anonymous channels

Conclusions

- RAM scraping is the major threat at the moment
- POS RAM scraping malware workflow
  1. Make persistence
  2. Retrieve list of processes on execution
  3. Scan its memory looking for credit card data
  4. When found, exfiltrate it (somehow)
- Samples of 22 families analyzed based on their workflow

Take-home messages

- Few families use analysis-aware tricks
- Detectable persistence methods (mainly registry-based)
  - One of them uses NTFS ADS
- Process blacklisting
- Data exfiltration thru. encoded data and non-anonymous channels
  - DNS, specific USB drives

Conclusions

- RAM scraping is the major threat at the moment
- POS RAM scraping malware workflow
  1. Make persistence
  2. Retrieve list of processes on execution
  3. Scan its memory looking for credit card data
  4. When found, exfiltrate it (somehow)
- Samples of 22 families analyzed based on their workflow

Take-home messages

- Few families use analysis-aware tricks
- Detectable persistence methods (mainly registry-based)
  - One of them uses NTFS ADS
- Process blacklisting
- Data exfiltration thru. encoded data and non-anonymous channels
  - DNS, specific USB drives
  - Two samples use TOR network to exfiltrate!

Gracias por su atención

cyber camp
CYBERSECURITY EVENT
2016

GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

incibe_
2006-2016
TRABAJANDO POR LA CONFIANZA DIGITAL