radware
availability | performance | security

Turbot

“Catch me if you can”

Itzik Kotler
Ziv Gadot
Security Operation Center (SOC)

Smart Network. Smart Business.

radware

Agenda

Smart Network. Smart Business.

- Introduction
  - What are the existing problems of Botnets communication
  - A new domain for Botnets communication: web services
- Turbot Protocol
- Turbot Demo
- Turbot Analysis
- Summary
- Q&A

Introduction

Smart Network. Smart Business.

In order to understand where Botnets communication is going to we need to understand their existing problems first.

radware | Conficker

Smart Network. Smart Business.

- Conficker
  - Conficker A,B,C : HTTP
    - Domain names are PRNG
  - Conficker D,E : P2P
- Trends
  - Why did it use HTTP first?
    - HTTP blends into common traffic
  - Why was it forced back to P2P?
    - Had a single-point-of-failure in its HTTP protocol

Blend into Common Traffic

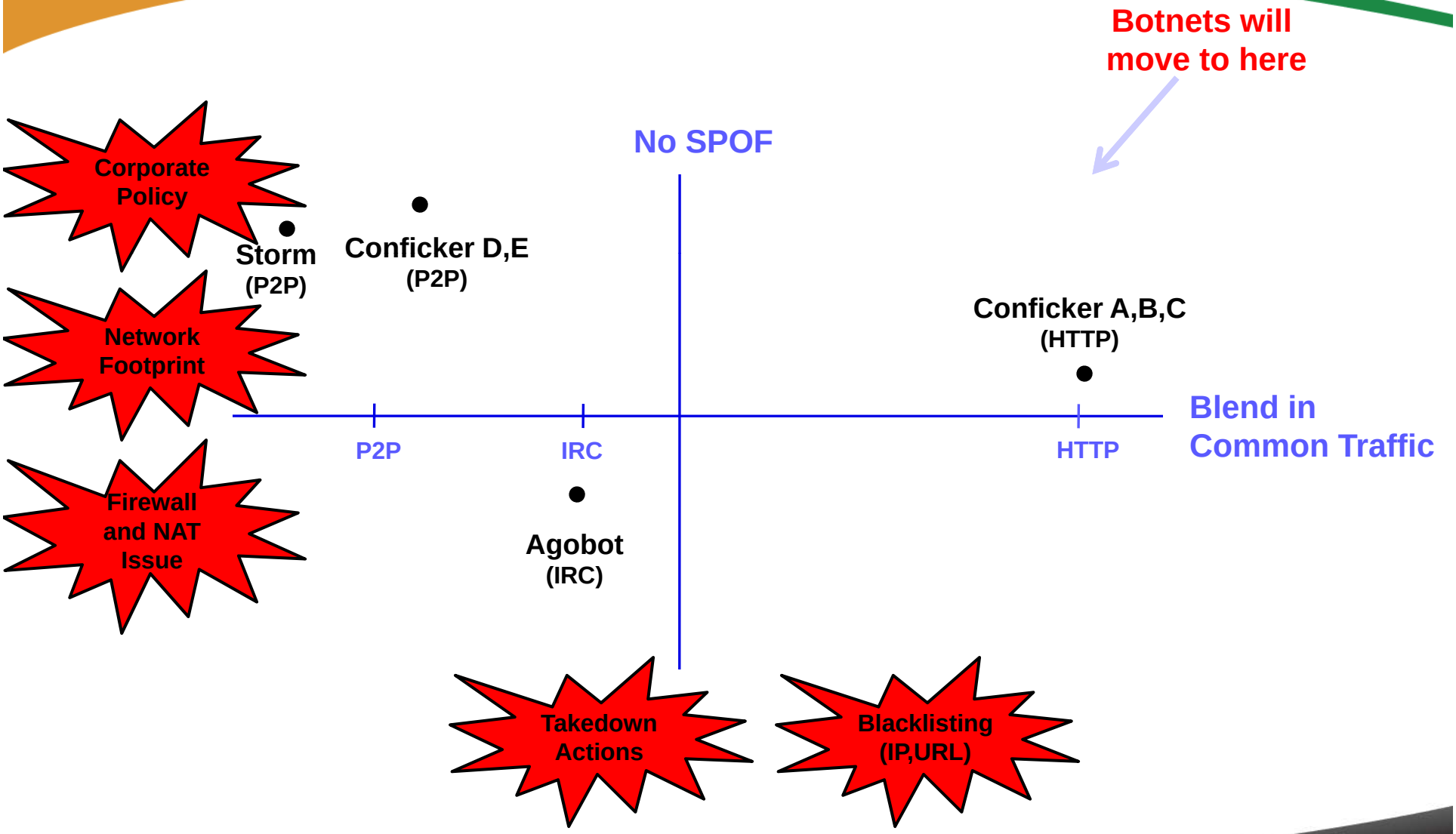
- Advantages
  - Minimizes potential network fingerprint
  - Passes corporate policy
    - HTTP is never blocked, whereas IRC and P2P are
  - Firewall/NAT issues
- Ultimately
  - HTTP/HTML
  - Client initiates requests
  - Legitimate sites

No Single Point of Failure

- Single Point of Failure (SPOF)
  - The ability to block communication by attacking a single set of resources
    - Resource takedown
      - IP, DNS or Site takedown
    - Blacklisting
      - Blocking the known resource
  - Technologies against SPOF
    - P2P (decentralized)
    - Conficker PRNG domain name – failed

radware | SPOF Versus Blend In

Smart Network. Smart Business.



radware | Technology vs. problems

Smart Network. Smart Business.

Problem		Technology		
		IRC	P2P	HTTP
Blend in common traffic	Corporate-policy blocking	X	X	OK
	Network footprint detection	OK	X	OK
	Firewall and NAT issues	OK	X	OK
SPOF	Takedown Actions	X	OK	X
	Blacklisting (IP,URL)	OK	OK	X

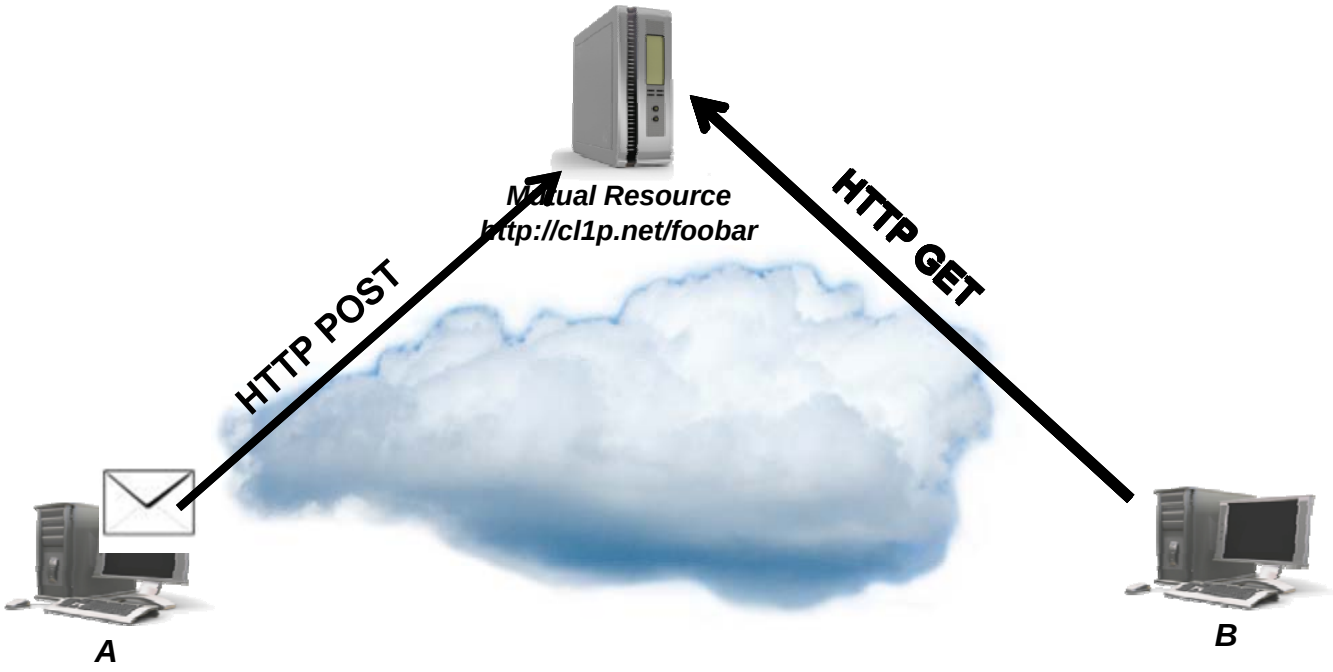
- We assume a real fight against Botnets !
  - Full deployment of mitigation equipment.
  - Binaries are fully analyzed (protocol is fully known).
  - Security vendors (***security agent***) are resourceful and determined.

Turbot Protocol

Smart Network. Smart Business.

- Passing a message using web services is very easy (and obvious)
  - Open any writable mutual resource and send message in the form of new entries:
    - E-mail
    - Blog
    - Online documents
    - Wiki site
- Botnet (in particular the bots) cannot use many of them
  - No CAPTCHA or login please
    - Internet clipboards
    - Disposable email address
    - UGC (User Generated Content)

- Once A and B agree on a mutual resource they can
  - Monitor the resource for a new messages
  - Send new messages to that resource



Internet Clipboard

- Functionality
  - Copies any data to a specific URL to later paste in a different host
  - Also supports files and pictures
- Examples
  - www.cl1p.net
  - www.padfly.com
  - www.pastebin.com
- Accessibility
  - No CAPTCHA no login, since service needs to be quick

Disposable E-mail Addressing (DEA)

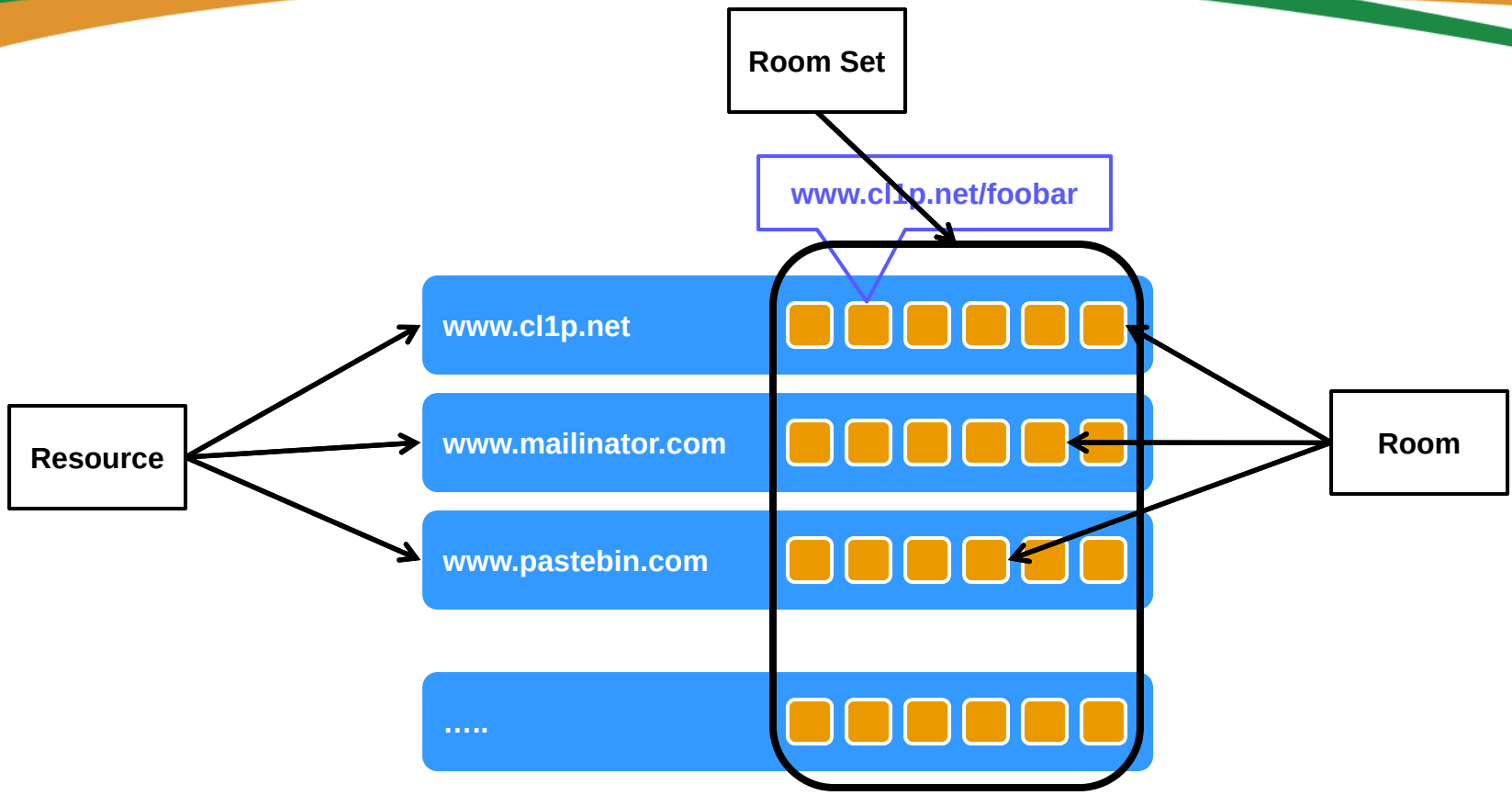
- Functionality
  - A disposable e-mail address used to avoid spamming
  - The user can choose any e-mail address within given domains, provide it, and later fetch e-mail messages
- Examples
  - www.mailinator.com
  - www.guerrillamail.com
  - www.spamex.com
- Accessibility
  - CAPTCHA, if at all, only when deleting a message
  - Sending the e-mail message can also be done by Web services (mostly offering to send large attachments easily)

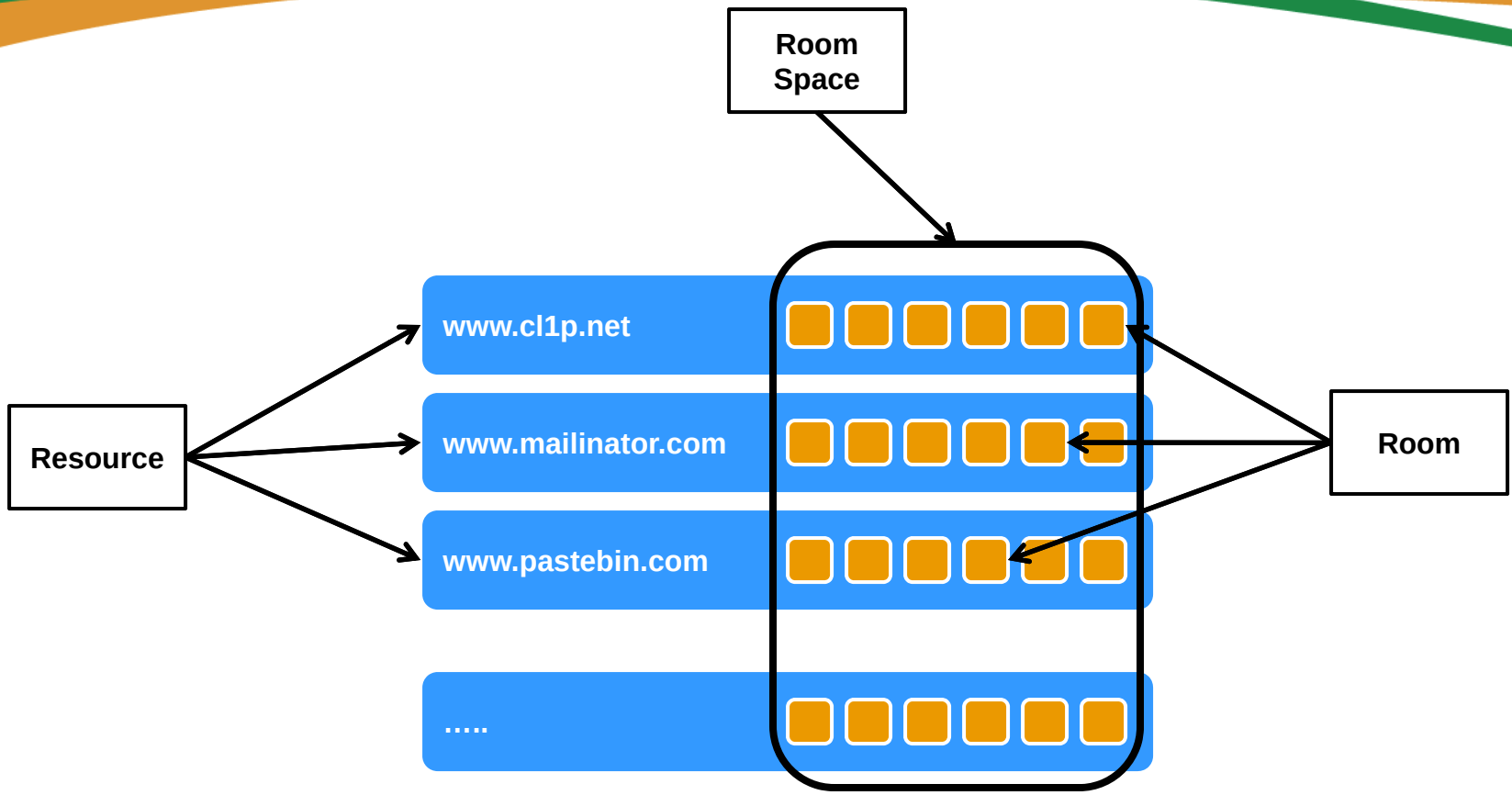
User Generated Content

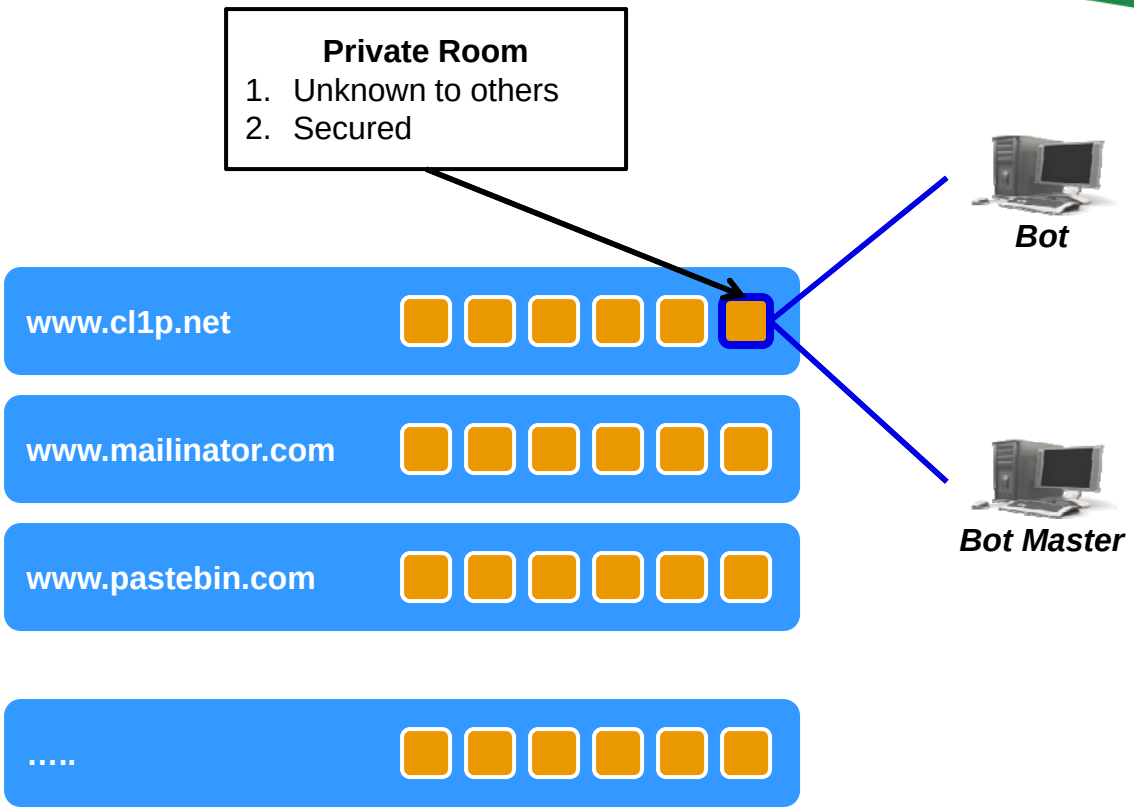
- Functionality
  - User comments mostly in news sites and blogs
- Examples
  - www.moconews.net
  - www.sofiaecho.com
- Accessibility
  - Many services are protected with CAPTCHA, login or active moderation; however, a significant number are not protected.
  - It is expected that the comment be relevant to its location
    - The message can be encoded in the User **S**ite field (if supported), or it can be encoded in a link within the message.

URL Shortening

- Functionality
  - Takes a long URL and generates a short one to replace it. Purposes:
    - To prevent broken links in e-mail
    - To send links in Twitter
- Examples
  - www.tinyurl.com
  - www.dwarfurl.com
  - www.snipurl.com
- Alternative usability
  - Compression service—a long message encoded as a URL is compressed to very short URL.

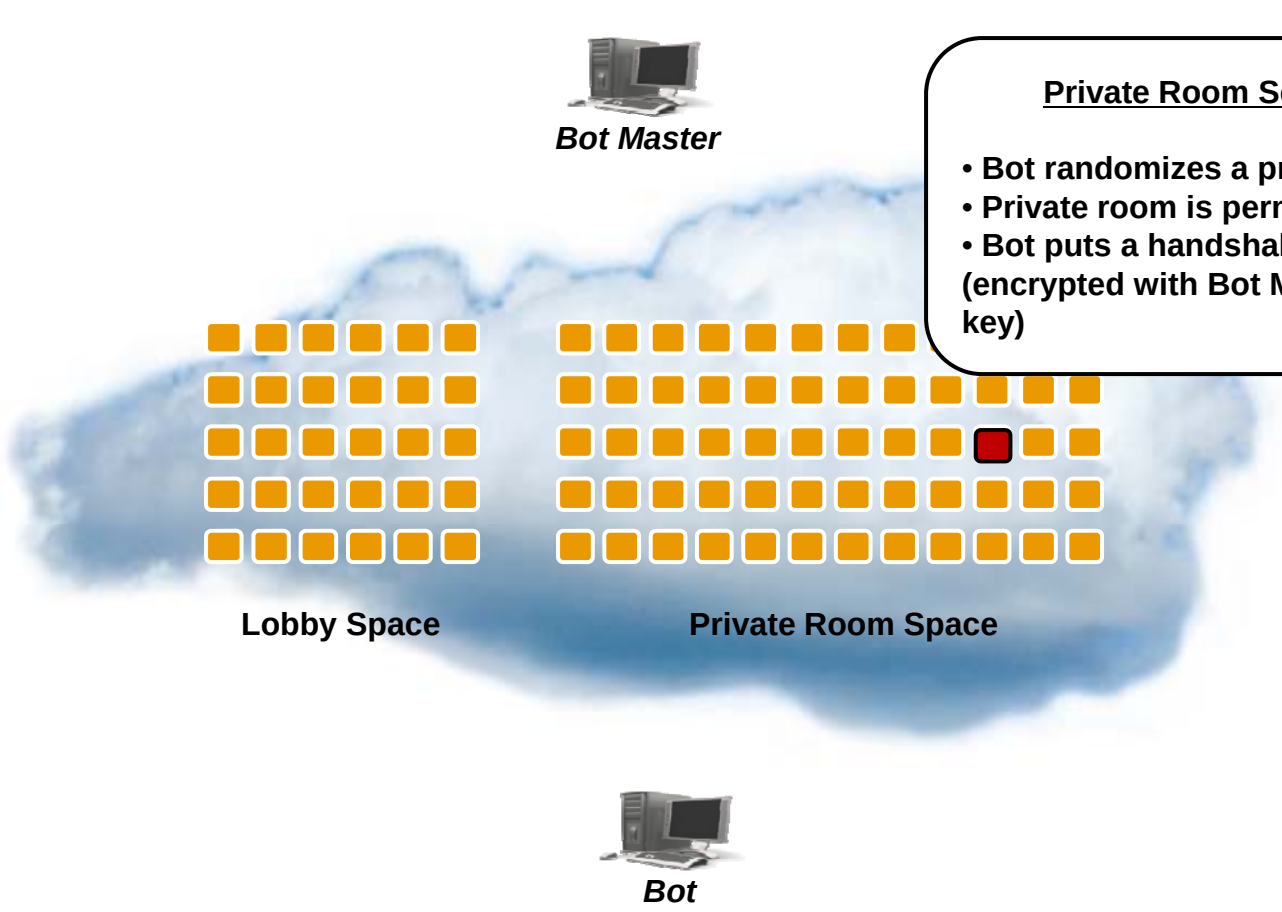

Room Set
www.cl1p.net/foobar
www.cl1p.net
www.mailinator.com
www.pastebin.com
.....
Resource
Room


Room Space
www.cl1p.net
www.mailinator.com
www.pastebin.com
.....
Resource
Room


Private Room
1. Unknown to others
2. Secured
www.cl1p.net
www.mailinator.com
www.pastebin.com
.....
Bot
Bot Master

Private Room Space and Lobby Space

- Private Room space
  - Is a room space
  - Very large
  - The more resources the better
  - Private rooms are chosen from this space
- Lobby space
  - Is a room space
  - Medium size
  - The more resources the better
  - Use as common place to negotiate private rooms



1

Private Room Selection

- **Bot randomizes a private room**
- **Private room is permanent**
- **Bot puts a handshake message (encrypted with Bot Master public key)**

Invitation publish

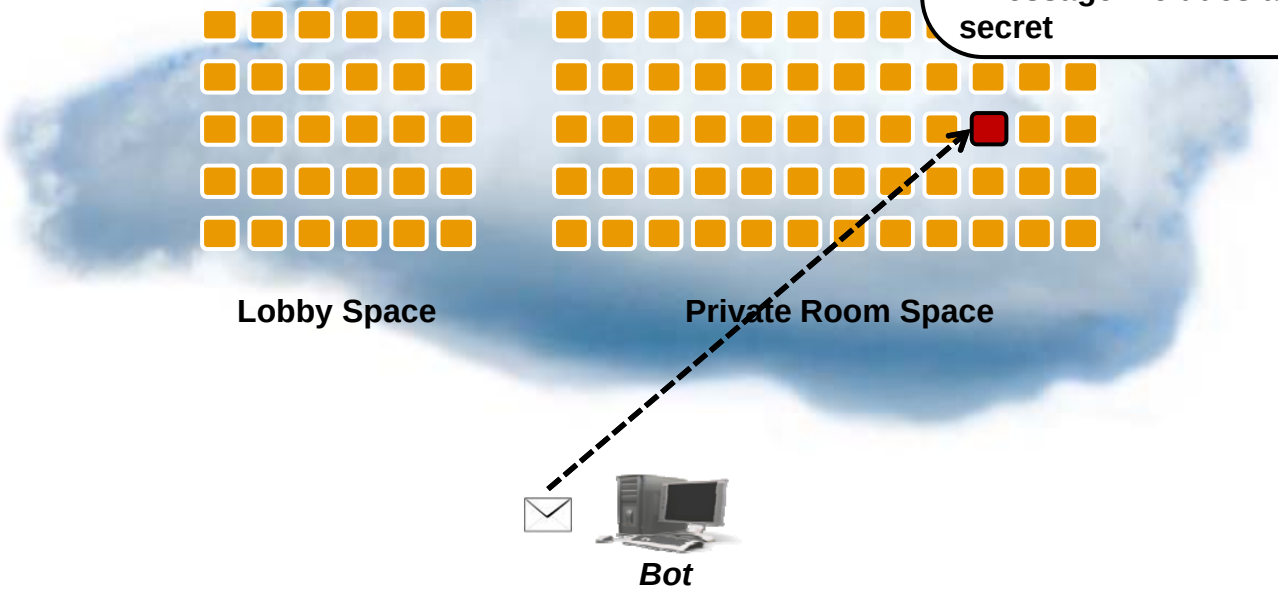
2

- Bot prepares an invitation
  - Includes private room ID
  - Encrypted with Bot Master private key
- Bot publish invitation in the lobby
  - Periodically the Bot ranodomize a room in the lobby
  - Publish the invitation in that room

Private Room Selection

1

- Bot randomizes a private room
- Private room is permanent
- Bot puts a handshake BOT HELLO message (encrypted with Bot Master public key)
- Message includes a common secret

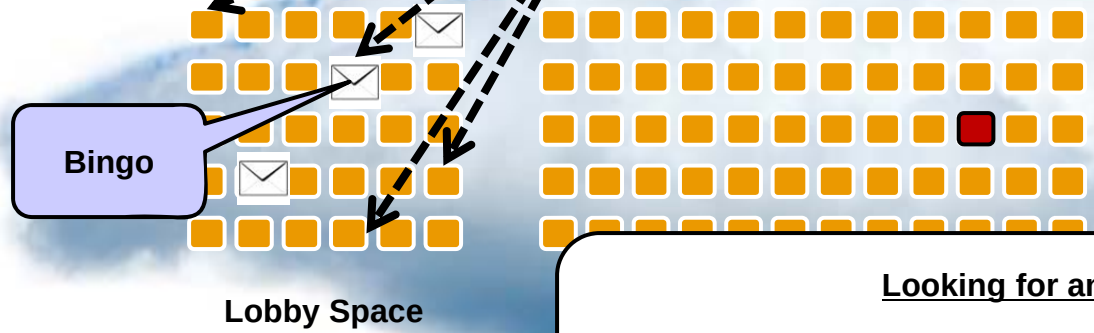


2

Invitation publish

- Bot prepares an invitation
  - Invitation includes private room ID
  - Encrypted with Bot Master private key
- Bot publish invitation in the lobby
  - Periodically the Bot ranodomize a room in the lobby
  - Publish the invitation in that room

Bot Master



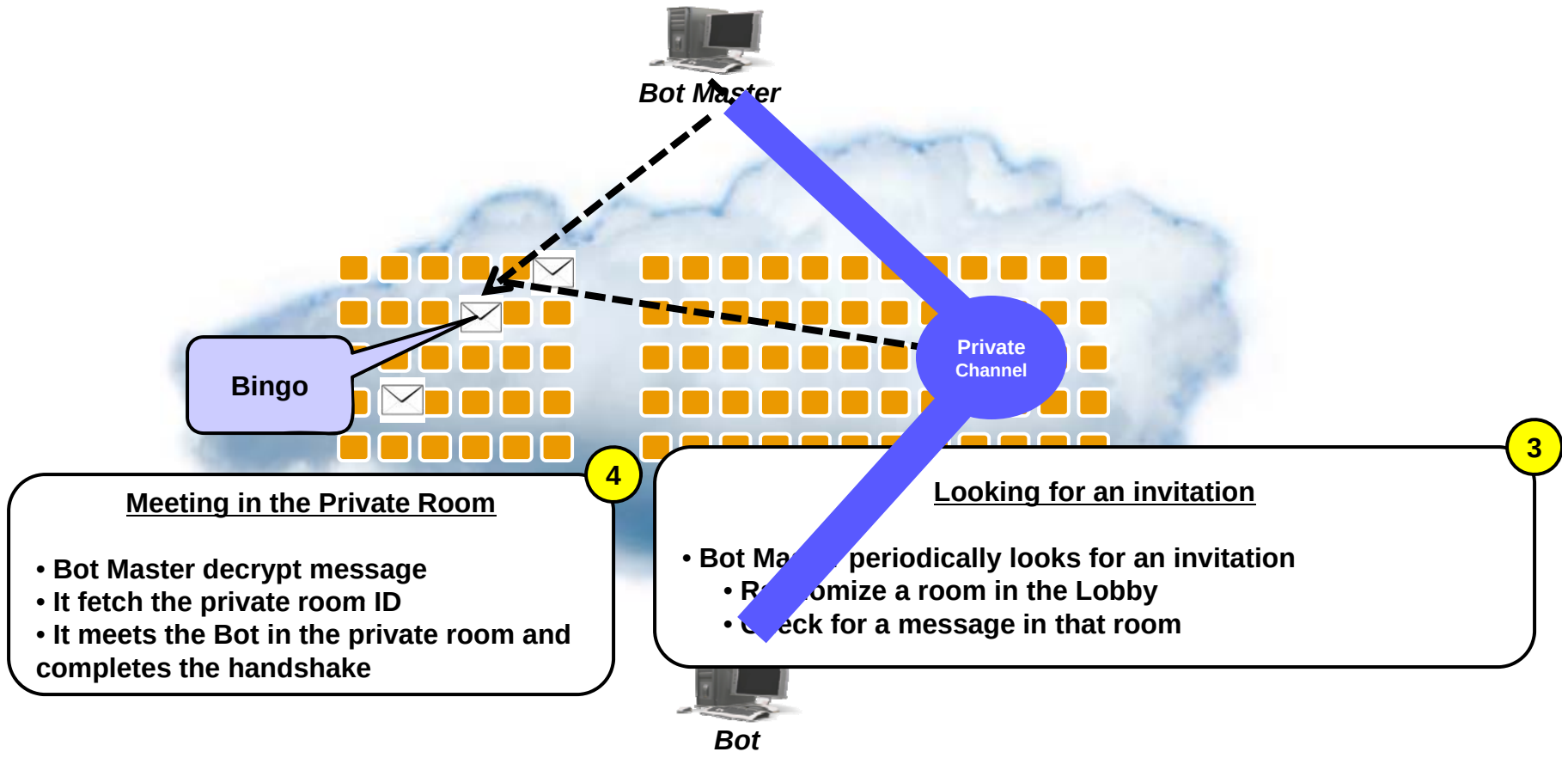
Lobby Space

3

Looking for an invitation

- Bot Master periodically looks for an invitation
  - Randomize a room in the Lobby
  - Check for a message in that room

Bot



Meeting in the Private Room

- Bot Master decrypt message
- It fetch the private room ID
- It meets the Bot in the private room and completes the handshake

4

Looking for an invitation

- Bot Ma periodically looks for an invitation
  - R omize a room in the Lobby
  - C eck for a message in that room

3

Turbot Demo

Smart Network. Smart Business.

Turbot Analysis

Smart Network. Smart Business.

radware | Technology vs. Problems

Smart Network. Smart Business.

Problem		Technology			
		IRC	P2P	HTTP	**Turbot**
Blend in common traffic	Corporate-policy blocking	X	X	OK	
	Network footprint detection	OK	X	OK	
	Firewall and NAT issues	OK	X	OK	
SPOF	Takedown Actions	X	OK	X	
	Blacklisting (IP,URL)	OK	OK	X	

Technology vs. Problems

radware | Smart Network. Smart Business.

Problem		Technology			
		IRC	P2P	HTTP	**Turbot**
Blend in common traffic	Corporate-policy blocking	X	X	OK	
	Network footprint detection	OK	X	OK	
	Firewall and NAT issues	OK	X	OK	
SPOF	Takedown Actions	X	OK	X	
	Blacklisting (IP,URL)	OK	OK	X	
	Efficiency				
	Interrupting communication				

- Assuming:
  - Each Bot posts 1 invitation per hour
  - Bot-Master scans for 1 room per minute
  - Botnet size is 10,000
  - Lobby size is 100,000
- Then
  - Each bot posts 720 message per month, 7,200,000 posts
  - The Bot-master will add new Bot every minunte, ~10,000 per week.
- Calculation/Simulation
  - Will be presented in the future

Corporate-Policy Traversal

- HTTP is always open
- Turbot does not use HTTPS
- Turbot does not use problematic sites (for example, anonymizers)
- No corporate-policy issues are expected

Network Footprint

- The usage of HTTP and HTML makes each message a very common one.
- Even so, it is possible that the Turbot HTTP implementation will have unique footprints.
  - Example: send “Turbot 1.0” in the “User-Agent” header
- Solution:
  - Turbot should use common libraries such as IE and FF

Firewall and NAT Issues

- Turbot doesn’t open a port
- Turbot always initiate the connection
- HTTP is the most supported and reliable protocol
- No firewall or NAT issues are expected

- There is no single site that can be taken down
  - Both Lobby-space and Private-room-space are as large as desired
  - The access to the Lobby is randomized.

Blacklisting

- Turbot spans over many resources.
- If at all, whole domains of legitimate services will have to be blocked in order block the botnet.
- The percent of organizations that can do so is very small.

- Security agents can delete message in the Lobby
- The Security agents is competing with
  - Botnet size – usually more powerful than legitimate network
  - Birthday paradox – 1 successful message is enough!
- Future
  - Exact figures
  - Simulation

radware | Technology vs. Problems

Smart Network. Smart Business.

Problem		Technology			
		IRC	P2P	HTTP	**Turbot**
Blend in common traffic	Corporate-policy blocking	X	X	V	V
	Network footprint detection	V	X	V	V
	Firewall and NAT issues	X	X	V	V
SPOF	Takedown Actions	X	V	X	V
	Blacklisting (IP,URL)	V	V	X	V
	Efficiency				V
	Interrupting communication				V

- Message time
  - Messages are fetched by recipient by pulling from a common resource.
  - Time depends on the pulling frequency and is not instant.
  - Workarounds
    - Each message will contain a “next message time”

- Adding CAPTCHA or Login to Web services

Summary

Smart Network. Smart Business.

Questions & answers

Smart Network. Smart Business.

Appendix

Smart Network. Smart Business.

Appendix Content

- Additional Features
  - Indirect Access
  - Handle Bogus Bots
- Additional Analysis
  - Private Channels

Indirect Access

- Problem
  - Slaves accessing the Web leave their identity
- Solution
  - Indirect access using online site translation services
    - Examples: Google Translate, Yahoo Bubblefish, Windows Live Translator

Handle Bogus Bots

- The attack
  - Security vendors can create numerous virtual bots to slow down communication.
- Solution
  - Require each bot to perform an action that will distinguish the majority of the real zombies from the bogus ones.
    - Computational work in the form of solving a cryptologic puzzle.
    - Legal complication – ask the bot to take some verifiable illegal action which will complicate it. Security vendors cannot allow this.

- Turbot is unique in having private channels
- Pros
  - The main reason: part of the no SPOF requirement.
  - Better control of the Botnet especially when selling/renting.
- Cons
  - Bot-master has to invest labor in the C&C
    - Broadcast over Unicast can be simulated