RSAConference2015

San Francisco | April 20-24 | Moscone Center

CHANGE

Challenge today's security thinking

SESSION ID: ECO-R03

Lie. Cheat. Deceive. How to Practice the Art of Deception at Machine Speed

Jason Bird

Head of EMEA Technical Solutions

CSG Invotas

@securedsensibly

Why continue to do things the way we always have?

- Imagine:
  - Within every aspect of our lives there are rules, legal and moral guidelines that must be followed
  - These tell us what actions are permissible, what responses are appropriate, in short every element of our behaviour
  - Sport clearly illustrate this
    - ~~Football~~, sorry Soccer – 11 people per team, rules govern the time they play, how they play, where they play, each role has it's own set of behavioural rules
  - **Do you really have to follow a set of rules for Cybersecurity?**

USA vs Scotland Match?

USA vs Scotland Match?

So How Do Attackers See Us?

- We are bloated, slow, overworked, underpaid, stressed
  - We are guided by the wrong people
    - Users: “it's too complicated and it doesn’t have a fruit logo on it”
    - Auditor: “Get someone else to do it, and have you documented it?”
    - Procurement: “Choose the lowest bidder”
    - Board: “I don’t understand, why are we doing it?”
- Attackers see us as static, easy to locate, easy to invade, always up, and there’s plenty of people on the inside to rely on for help ☺

In short, we look like this…

Home Field Advantage?

- Over 5000 years of warfare “the defender” has always had the presumed advantage in any fight
  - Required a ratio of 4:1 for the attacker to be “assured” of victory over the defender
    - The defender picks the battlefield
    - The defender can typically move faster
    - The defender begins with forces that are optimally deployed to take advantage of the terrain
  - In cyber, this advantage should be even more pronounced
    - The defender can control what the attacker sees
    - The defender can dictate what they have access to
    - The defender can stop the attack simply by disconnecting
- Why did we give up the natural advantages we have in defending our networks and applications?

The Wrong Mind-set?

- We start with a mindset of losing:
  - The attacker only needs 1 vulnerability while the defender has to defend everything
  - The attacker has infinite time and infinite resources
- We forget that the attacker has to do “abnormal” things
  - Create ***unusual*** traffic
  - Create ***failures***
- Why don’t we catch them in time?

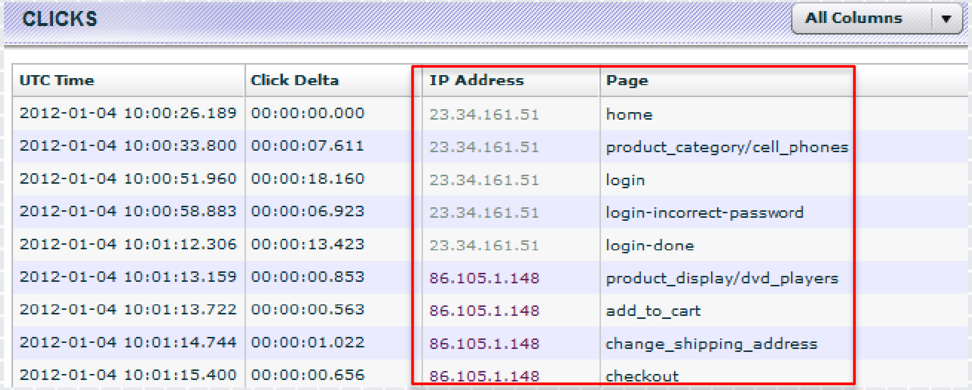
Practice the Art of Deception to Better Defend

- Be less predictable, Be faster, Be more aggressive
  - Lie
  - Cheat
  - Deceive

Change the Game.

Lie – Attackers don’t tell the whole truth!

- Attackers falsify browser headers, spoof IP addresses, use other peoples machines in order to present a false front

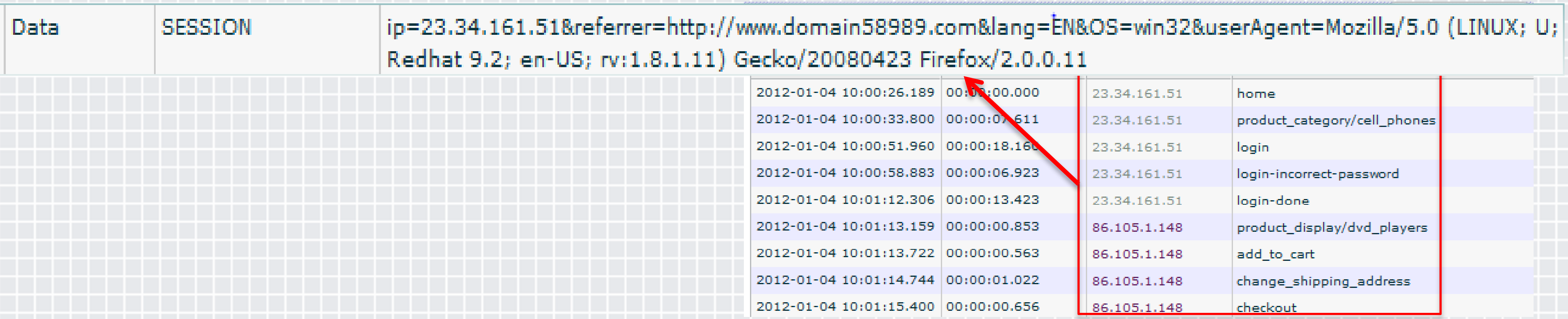


CLICKS

UTC Time	Click Delta	IP Address	Page
2012-01-04 10:00:26.189	00:00:00.000	23.34.161.51	home
2012-01-04 10:00:33.800	00:00:07.611	23.34.161.51	product_category/cell_phones
2012-01-04 10:00:51.960	00:00:18.160	23.34.161.51	login
2012-01-04 10:00:58.883	00:00:06.923	23.34.161.51	login-incorrect-password
2012-01-04 10:01:12.306	00:00:13.423	23.34.161.51	login-done
2012-01-04 10:01:13.159	00:00:00.853	86.105.1.148	product_display/dvd_players
2012-01-04 10:01:13.722	00:00:00.563	86.105.1.148	add_to_cart
2012-01-04 10:01:14.744	00:00:01.022	86.105.1.148	change_shipping_address
2012-01-04 10:01:15.400	00:00:00.656	86.105.1.148	checkout

Lie – Attackers don’t tell the whole truth!

- Attackers falsify browser headers, spoof IP addresses, use other peoples machines in order to present a false front

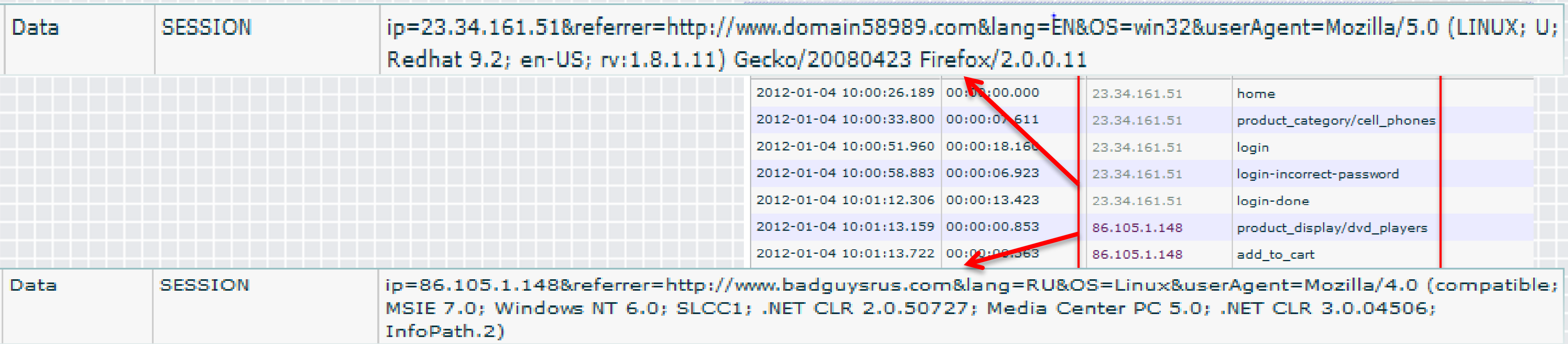


Data	SESSION	ip=23.34.161.51&referrer=http://www.domain58989.com&lang=EN&OS=win32&userAgent=Mozilla/5.0 (LINUX; U; Redhat 9.2; en-US; rv:1.8.1.11) Gecko/20080423 Firefox/2.0.0.11

2012-01-04 10:00:26.189	00:00:00.000	23.34.161.51	home
2012-01-04 10:00:33.800	00:00:07.611	23.34.161.51	product_category/cell_phones
2012-01-04 10:00:51.960	00:00:18.160	23.34.161.51	login
2012-01-04 10:00:58.883	00:00:06.923	23.34.161.51	login-incorrect-password
2012-01-04 10:01:12.306	00:00:13.423	23.34.161.51	login-done
2012-01-04 10:01:13.159	00:00:00.853	86.105.1.148	product_display/dvd_players
2012-01-04 10:01:13.722	00:00:00.563	86.105.1.148	add_to_cart
2012-01-04 10:01:14.744	00:00:01.022	86.105.1.148	change_shipping_address
2012-01-04 10:01:15.400	00:00:00.656	86.105.1.148	checkout

Lie – Attackers don't tell the whole truth!

- Attackers falsify browser headers, spoof IP addresses, use other peoples machines in order to present a false front

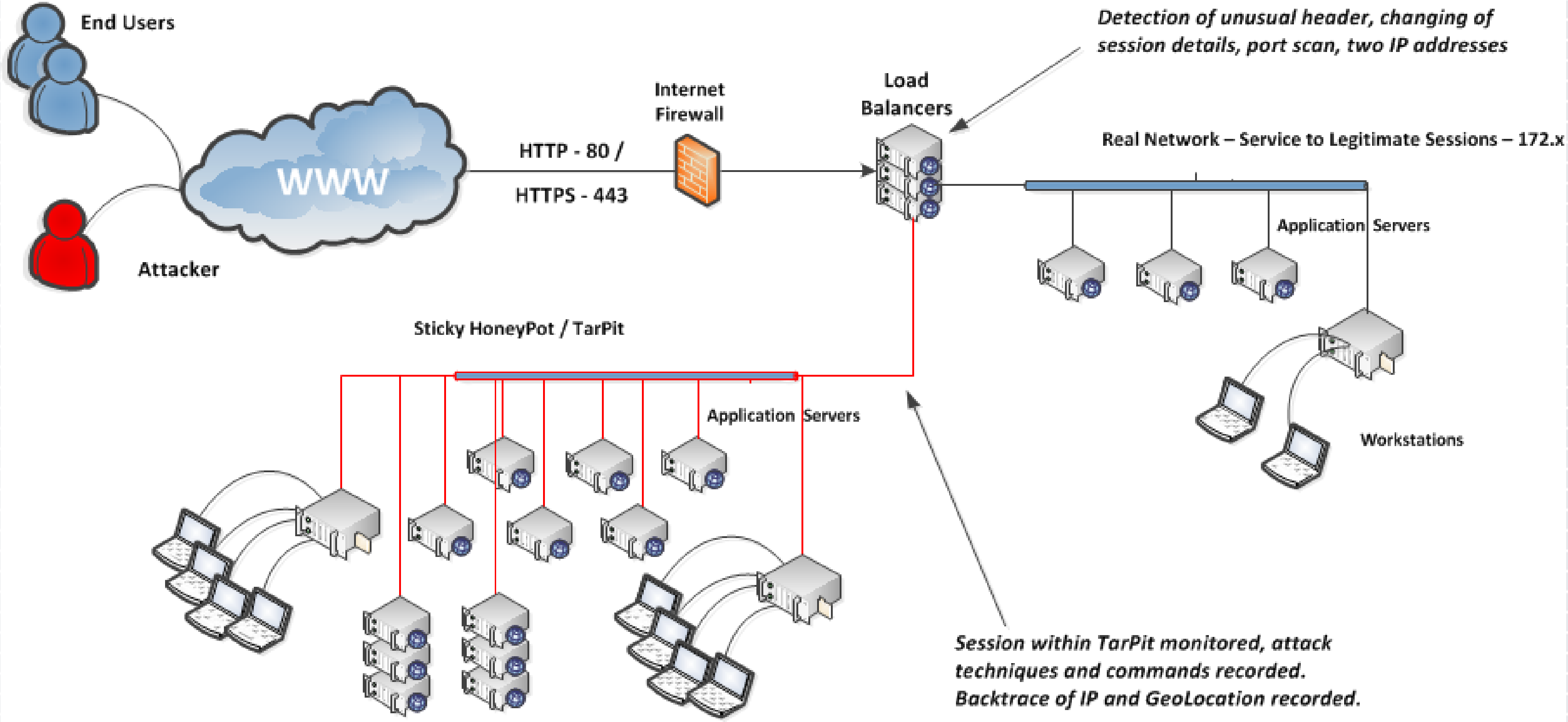


Data	SESSION	ip=23.34.161.51&referrer=http://www.domain58989.com&lang=EN&OS=win32&userAgent=Mozilla/5.0 (LINUX; U; Redhat 9.2; en-US; rv:1.8.1.11) Gecko/20080423 Firefox/2.0.0.11

2012-01-04 10:00:26.189	00:00:00.000	23.34.161.51	home
2012-01-04 10:00:33.800	00:00:07.611	23.34.161.51	product_category/cell_phones
2012-01-04 10:00:51.960	00:00:18.160	23.34.161.51	login
2012-01-04 10:00:58.883	00:00:06.923	23.34.161.51	login-incorrect-password
2012-01-04 10:01:12.306	00:00:13.423	23.34.161.51	login-done
2012-01-04 10:01:13.159	00:00:00.853	86.105.1.148	product_display/dvd_players
2012-01-04 10:01:13.722	00:00:00.563	86.105.1.148	add_to_cart

Data	SESSION	ip=86.105.1.148&referrer=http://www.badguysrus.com&lang=RU&OS=Linux&userAgent=Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; SLCC1; .NET CLR 2.0.50727; Media Center PC 5.0; .NET CLR 3.0.04506; InfoPath.2)

Lie – So Why Should We ?



Detection of unusual header, changing of session details, port scan, two IP addresses

Session within TarPit monitored, attack techniques and commands recorded. Backtrace of IP and GeoLocation recorded.

Cheat – There's A Whole Army Against You

- Botnet armies give them superior power
  - Zeus EuroGrabber – Stole $47million from 30,000 customers through mobile devices
  - ZeroAccess Botnet Network globally an estimated 1,000,000 devices
    - Mining bitcoin and other banking credentials, its estimated it generates $100,000 per day for its operators

ZeroAccess Botnet Network (Europe)

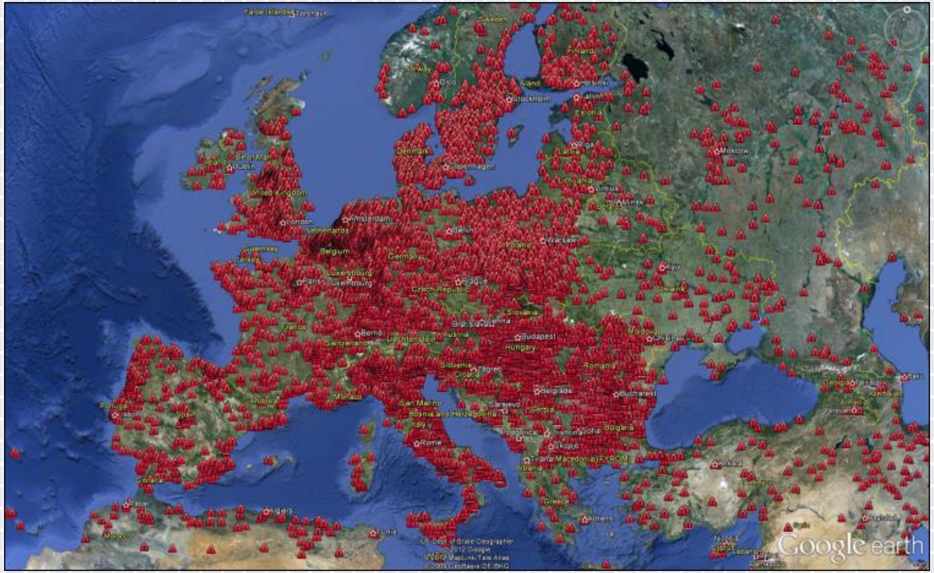
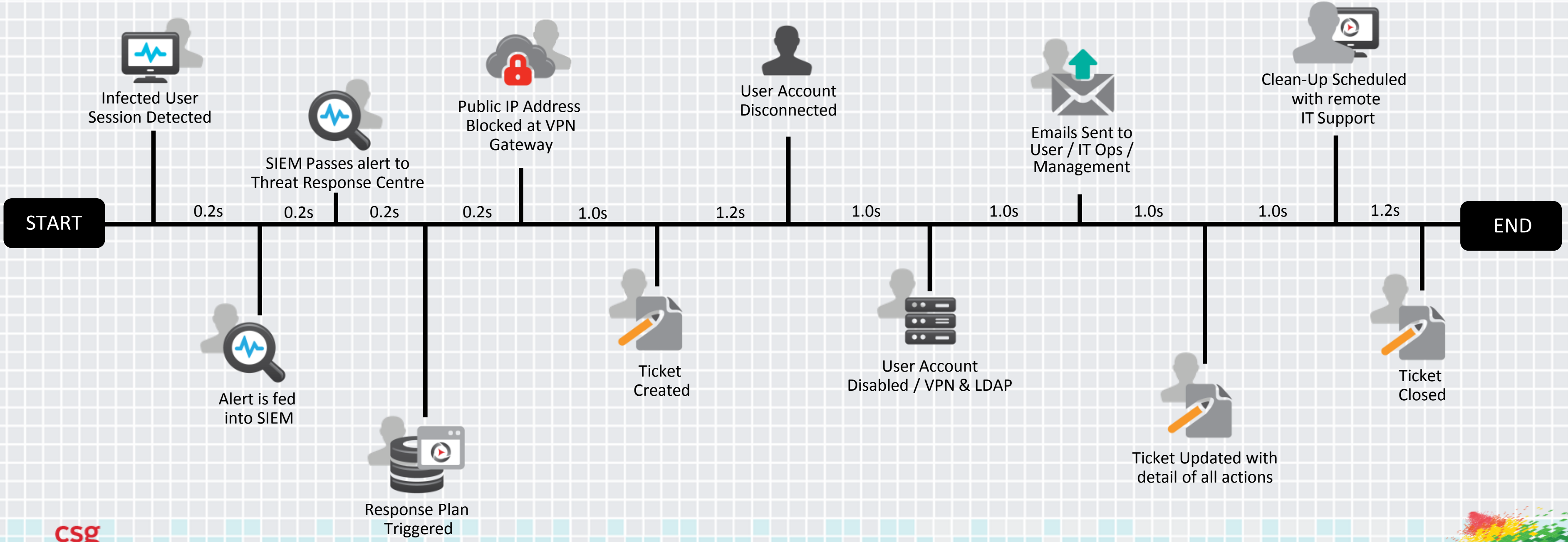


Image source – TechnologyReview.com

Cheat – Multiply Forces, Coordinate Response

- Automate defensive capabilities internally, so you now have an army of analysts battling for you:



START

Infected User Session Detected

0.2s

Alert is fed into SIEM

0.2s

SIEM Passes alert to Threat Response Centre

0.2s

Response Plan Triggered

0.2s

Public IP Address Blocked at VPN Gateway

1.0s

Ticket Created

1.2s

User Account Disconnected

1.0s

User Account Disabled / VPN & LDAP

1.0s

Emails Sent to User / IT Ops / Management

1.0s

Ticket Updated with detail of all actions

1.0s

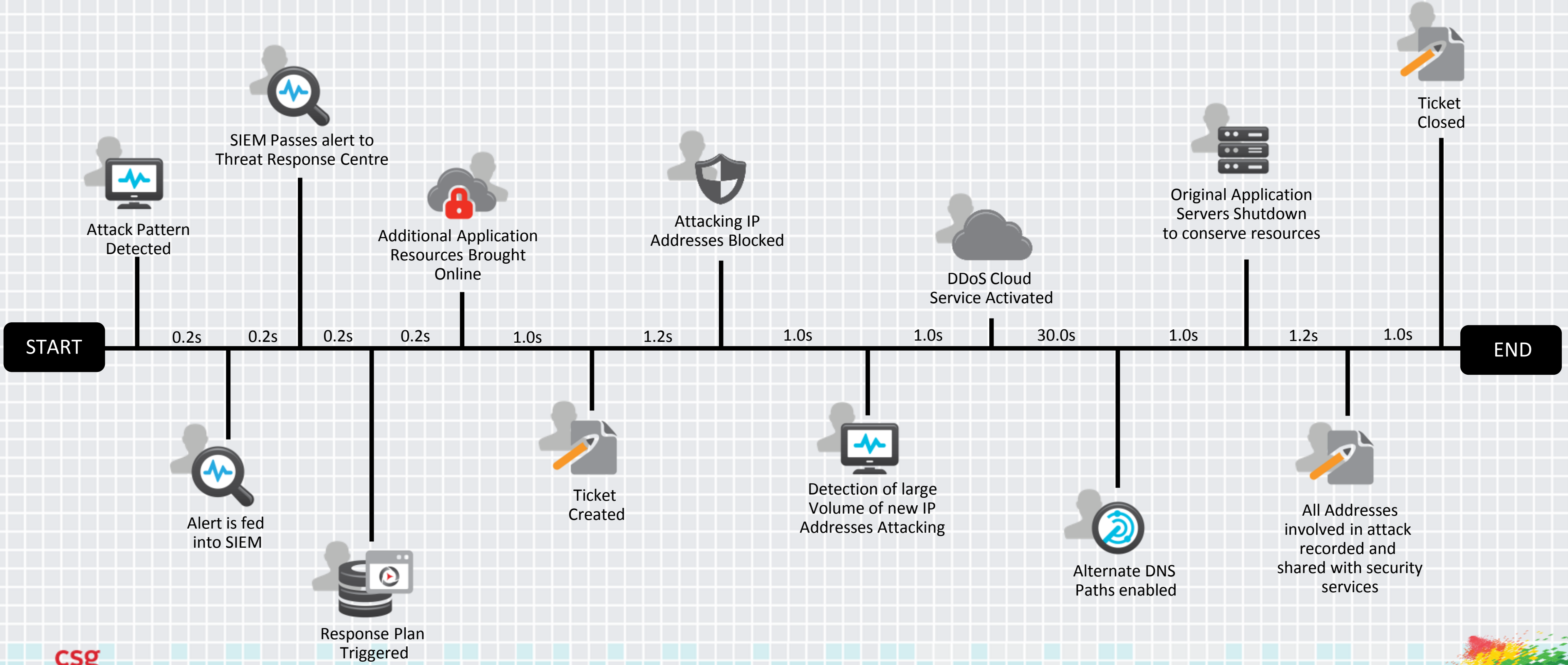
Clean-Up Scheduled with remote IT Support

1.2s

Ticket Closed

END

Cheat – Fight Fire with Fire



START

Attack Pattern Detected

0.2s

Alert is fed into SIEM

0.2s

SIEM Passes alert to Threat Response Centre

0.2s

Response Plan Triggered

0.2s

Additional Application Resources Brought Online

1.0s

Ticket Created

1.2s

Attacking IP Addresses Blocked

1.0s

Detection of large Volume of new IP Addresses Attacking

1.0s

DDoS Cloud Service Activated

30.0s

Alternate DNS Paths enabled

1.0s

Original Application Servers Shutdown to conserve resources

1.2s

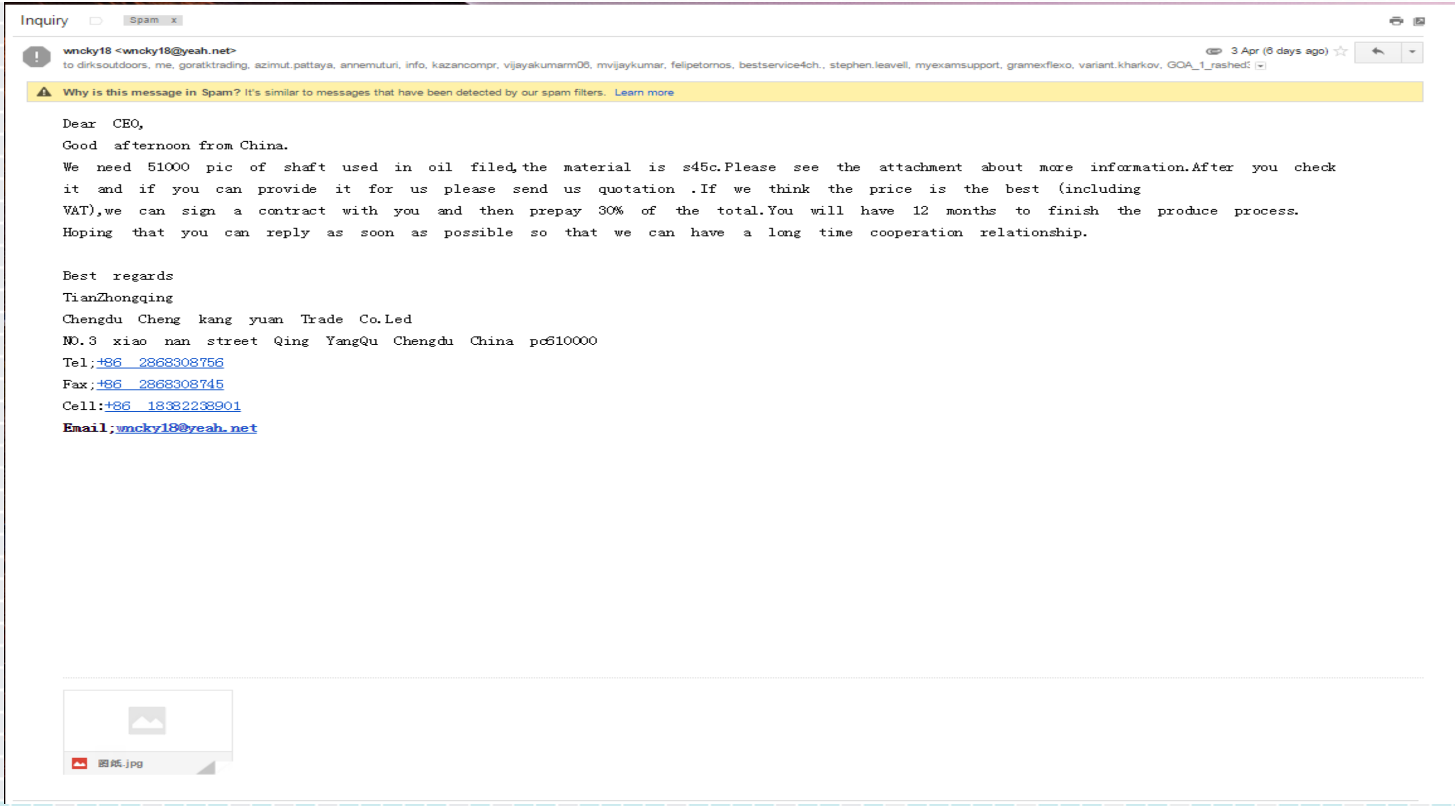
All Addresses involved in attack recorded and shared with security services

1.0s

Ticket Closed

END

Deceive – Spear Phishing Attack (Infiltration)



Inquiry Spam x

wncky18 <wncky18@yeah.net>
to dirksoutdoors, me, goratktrading, azimut.pattaya, annemuturi, info, kazancompr, vijayakumarm06, mvijaykumar, felipetornos, bestservice4ch., stephen.leavell, myexamsupport, gramexflexo, variant.kharkov, GOA_1_rashed:

3 Apr (6 days ago)

Why is this message in Spam? It's similar to messages that have been detected by our spam filters. Learn more

Dear CEO,

Good afternoon from China.

We need 51000 pic of shaft used in oil filed,the material is s45c.Please see the attachment about more information.After you check it and if you can provide it for us please send us quotation .If we think the price is best (including VAT),we can sign a contract with you and then prepay 30% of the total.You will have 12 months to finish the produce process.

Hoping that you can reply as soon as possible so that we can have a long time cooperation relationship.

Best regards
TianZhongqing
Chengdu Cheng kang yuan Trade Co.Led
NO.3 xiao nan street Qing YangQu Chengdu China pc610000
Tel;+86 2868308756
Fax;+86 2868308745
Cell:+86 18382238901
Email;wncky18@yeah.net

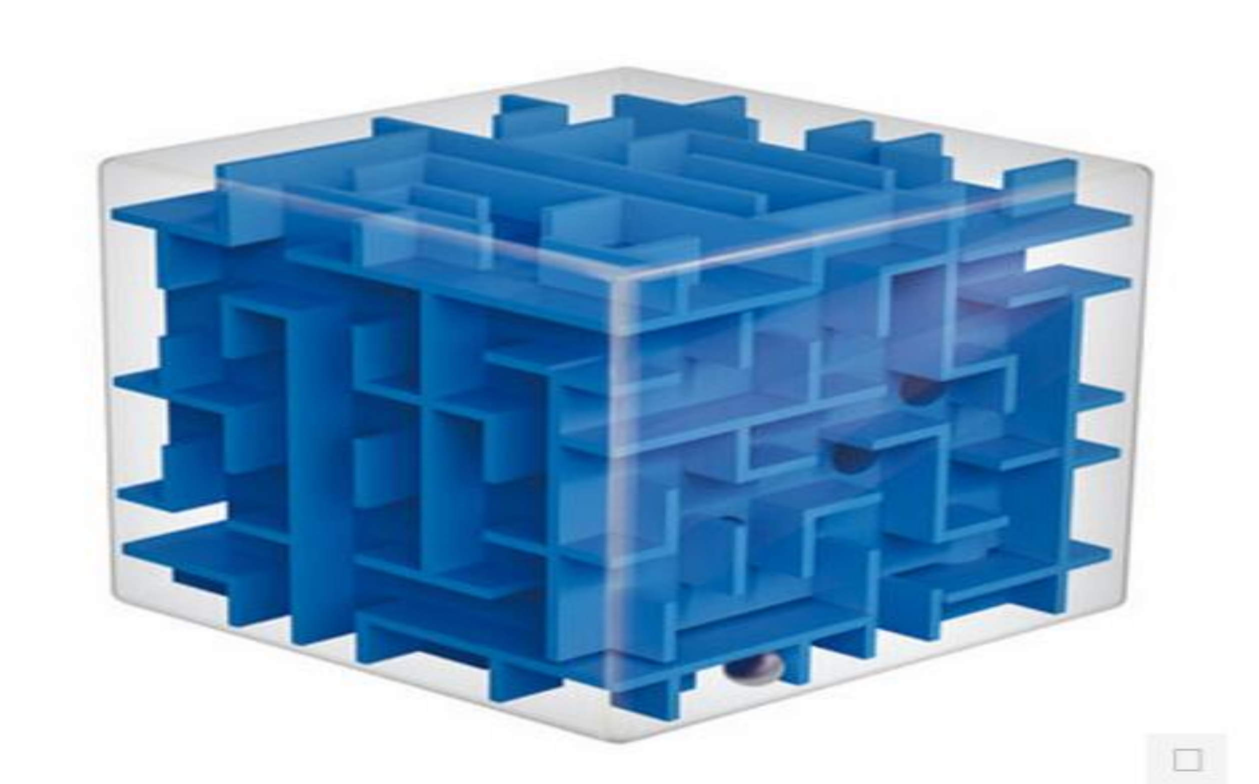
图纸.jpg

Deceive – Ever Played 3 Cups ?

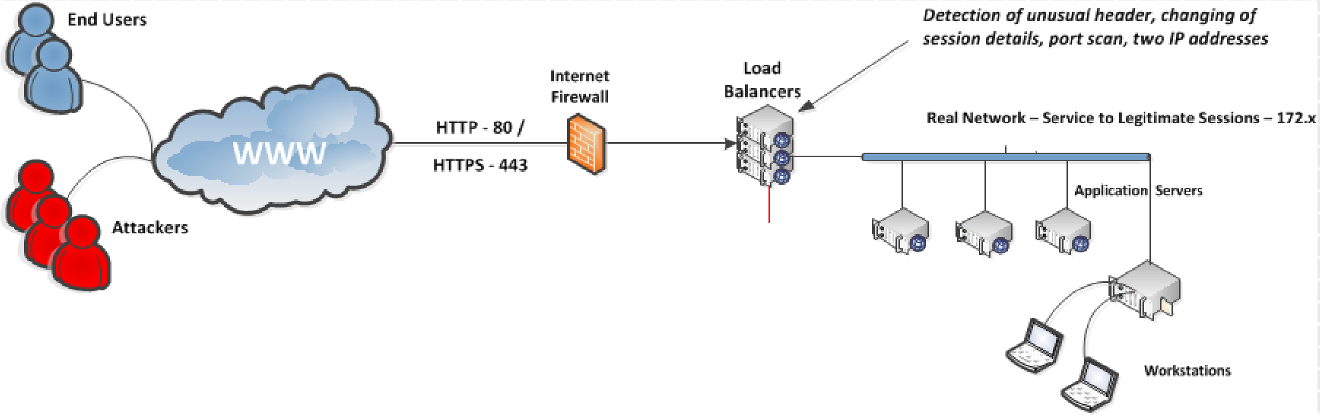
Deceive – Ever Played 3 Cups ?

Ever Played when there is no winning cup?

Deceive – Today's 3 Cup: Maze

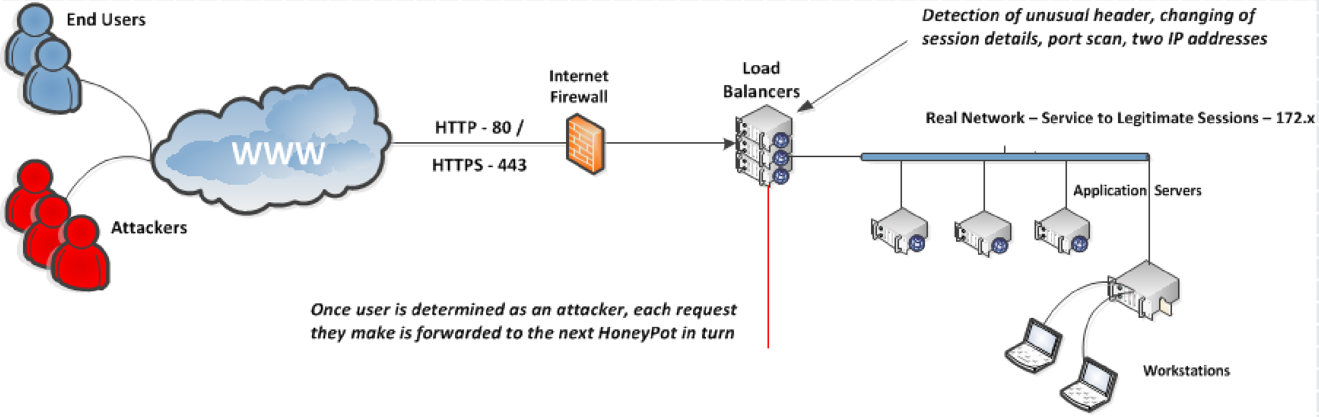


Deceive – Three Way Honeypot



Detection of unusual header, changing of session details, port scan, two IP addresses

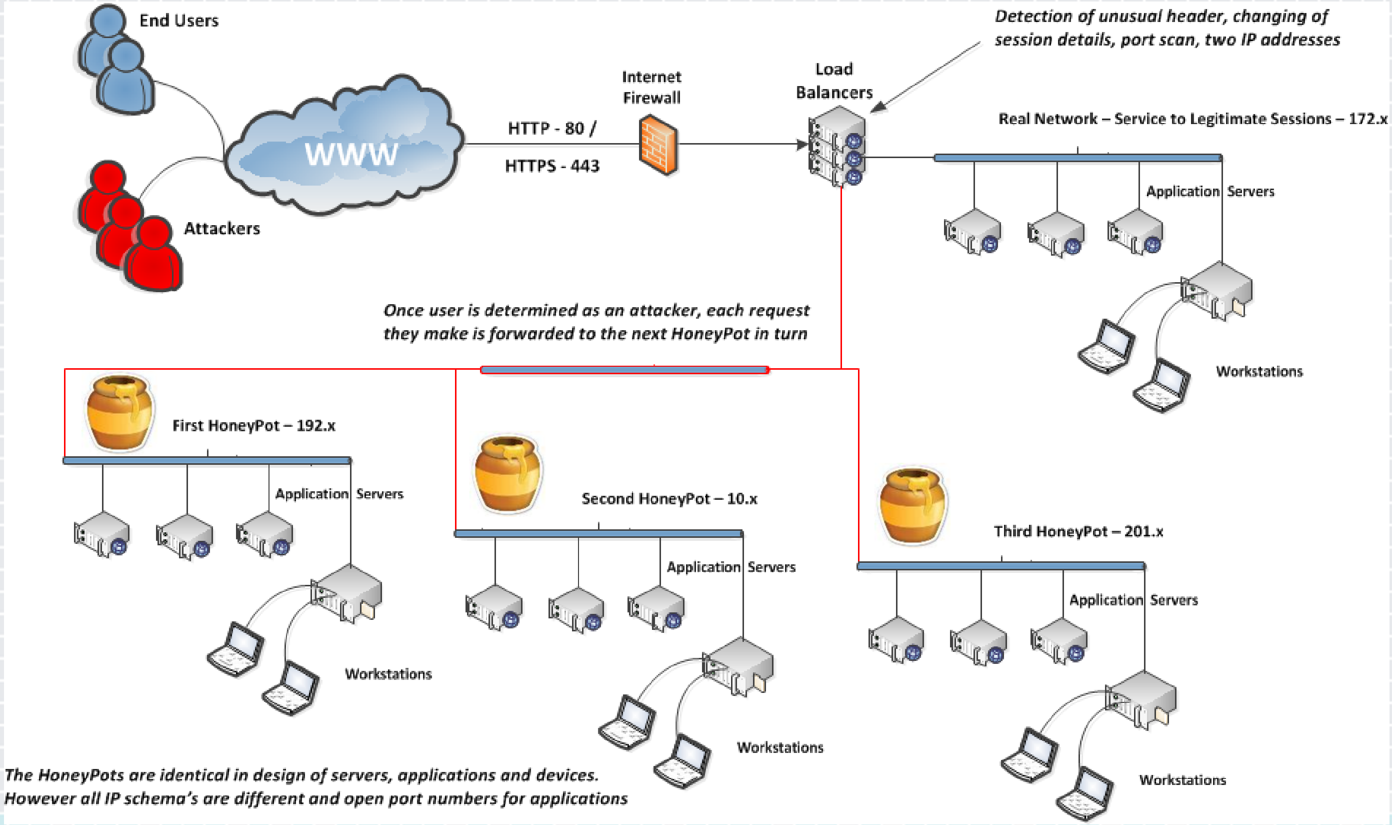
Deceive – Take Back Home Field Advantage



Detection of unusual header, changing of session details, port scan, two IP addresses

Once user is determined as an attacker, each request they make is forwarded to the next HoneyPot in turn

Deceive – Change the Battle Field

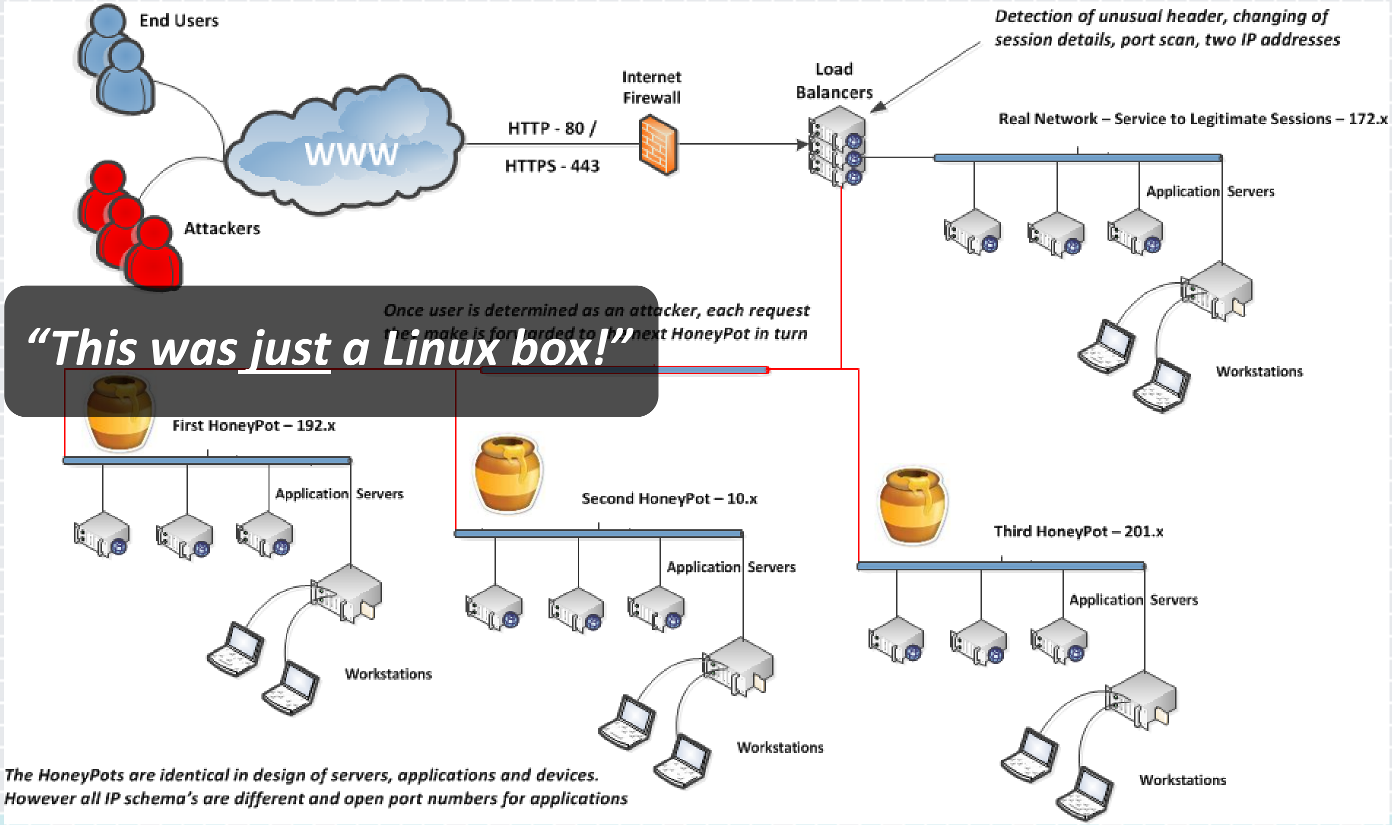


Detection of unusual header, changing of session details, port scan, two IP addresses

Once user is determined as an attacker, each request they make is forwarded to the next HoneyPot in turn

The HoneyPots are identical in design of servers, applications and devices. However all IP schema's are different and open port numbers for applications

Deceive – Frustrate Your Attacker



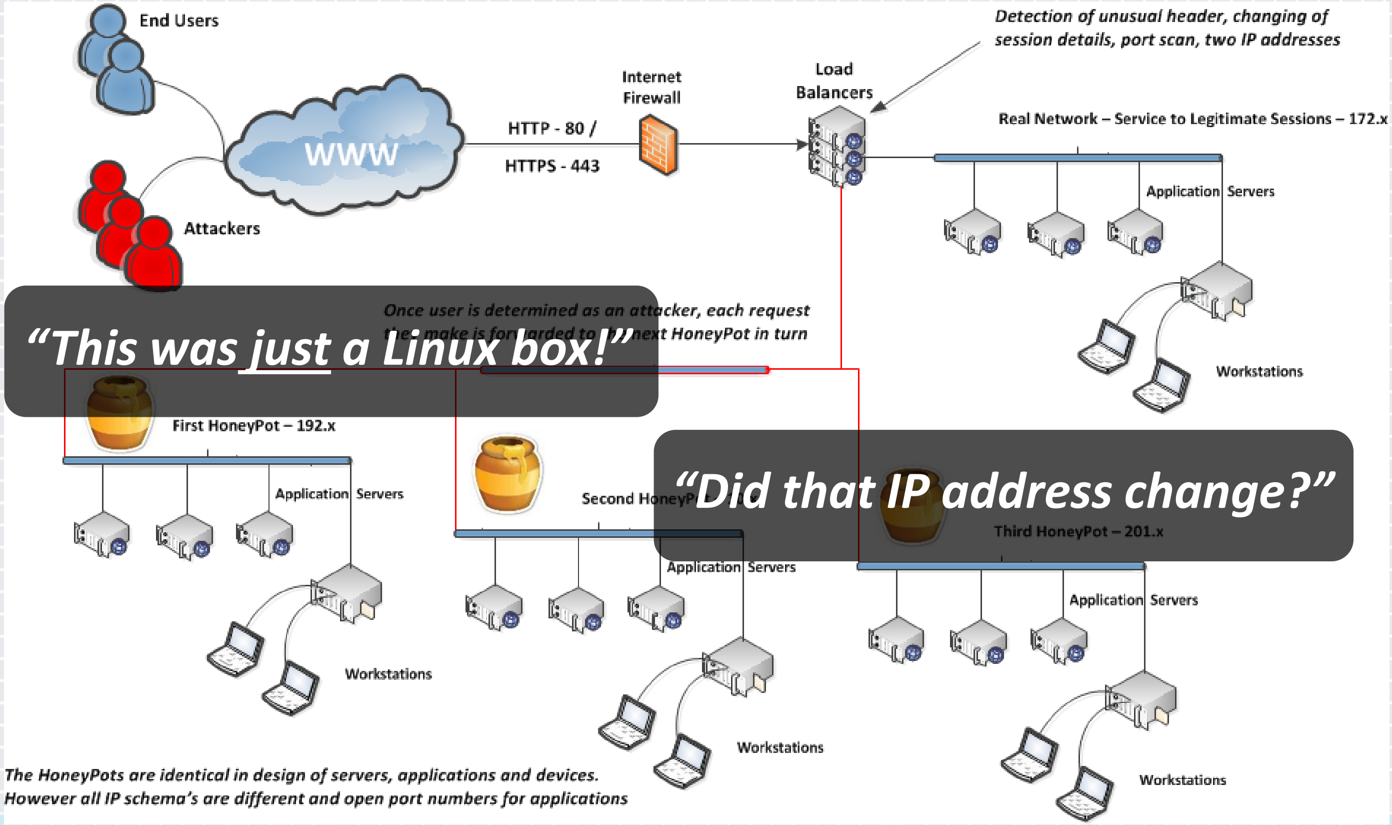
Detection of unusual header, changing of session details, port scan, two IP addresses

Once user is determined as an attacker, each request they make is forwarded to the next HoneyPot in turn

The HoneyPots are identical in design of servers, applications and devices. However all IP schema's are different and open port numbers for applications

"This was __just__ a Linux box!"

Deceive – Frustrate Your Attacker



Detection of unusual header, changing of session details, port scan, two IP addresses

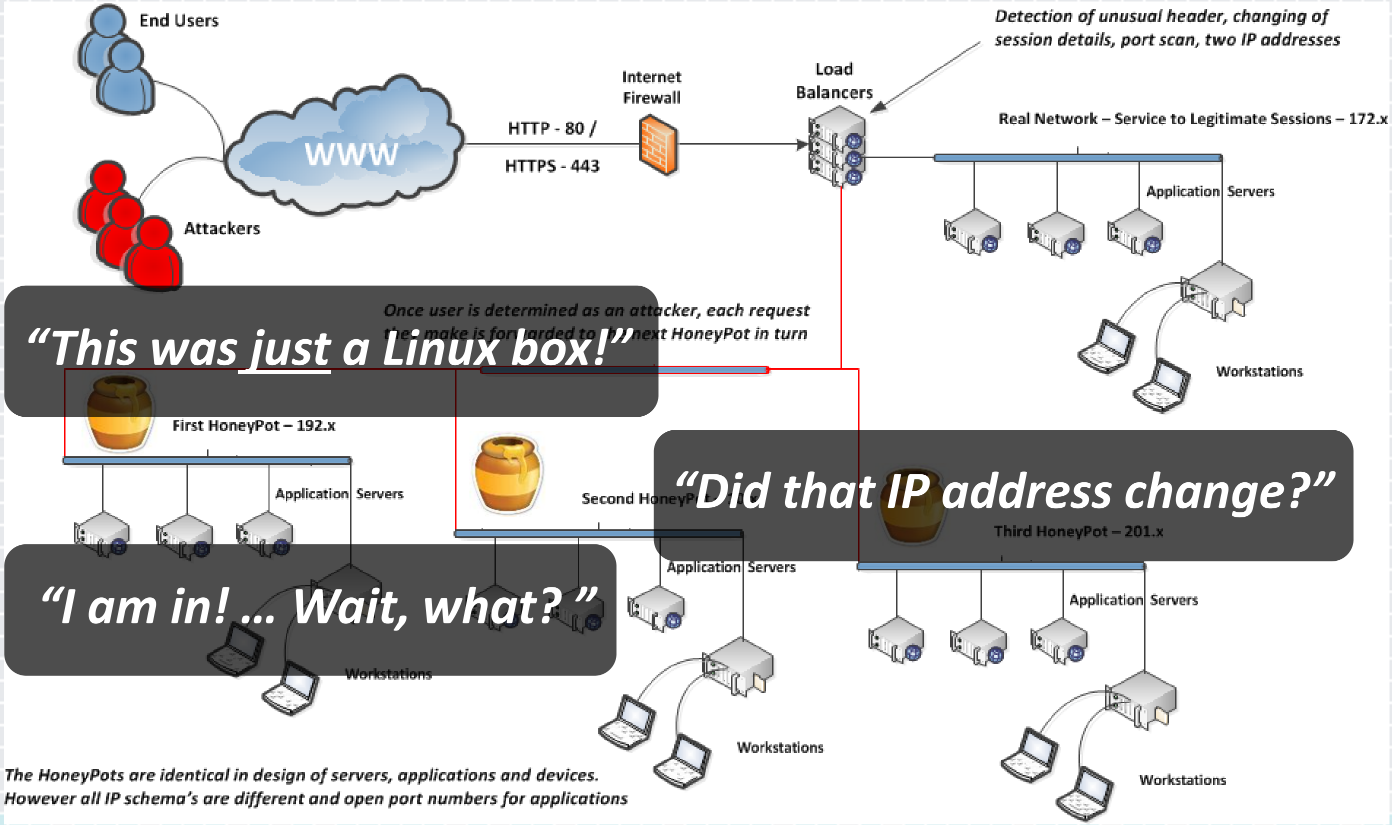
Once user is determined as an attacker, each request they make is forwarded to the next HoneyPot in turn

The HoneyPots are identical in design of servers, applications and devices. However all IP schema's are different and open port numbers for applications

"This was __just__ a Linux box!"

"Did that IP address change?"

Deceive – Frustrate Your Attacker



Detection of unusual header, changing of session details, port scan, two IP addresses

Once user is determined as an attacker, each request they make is forwarded to the next HoneyPot in turn

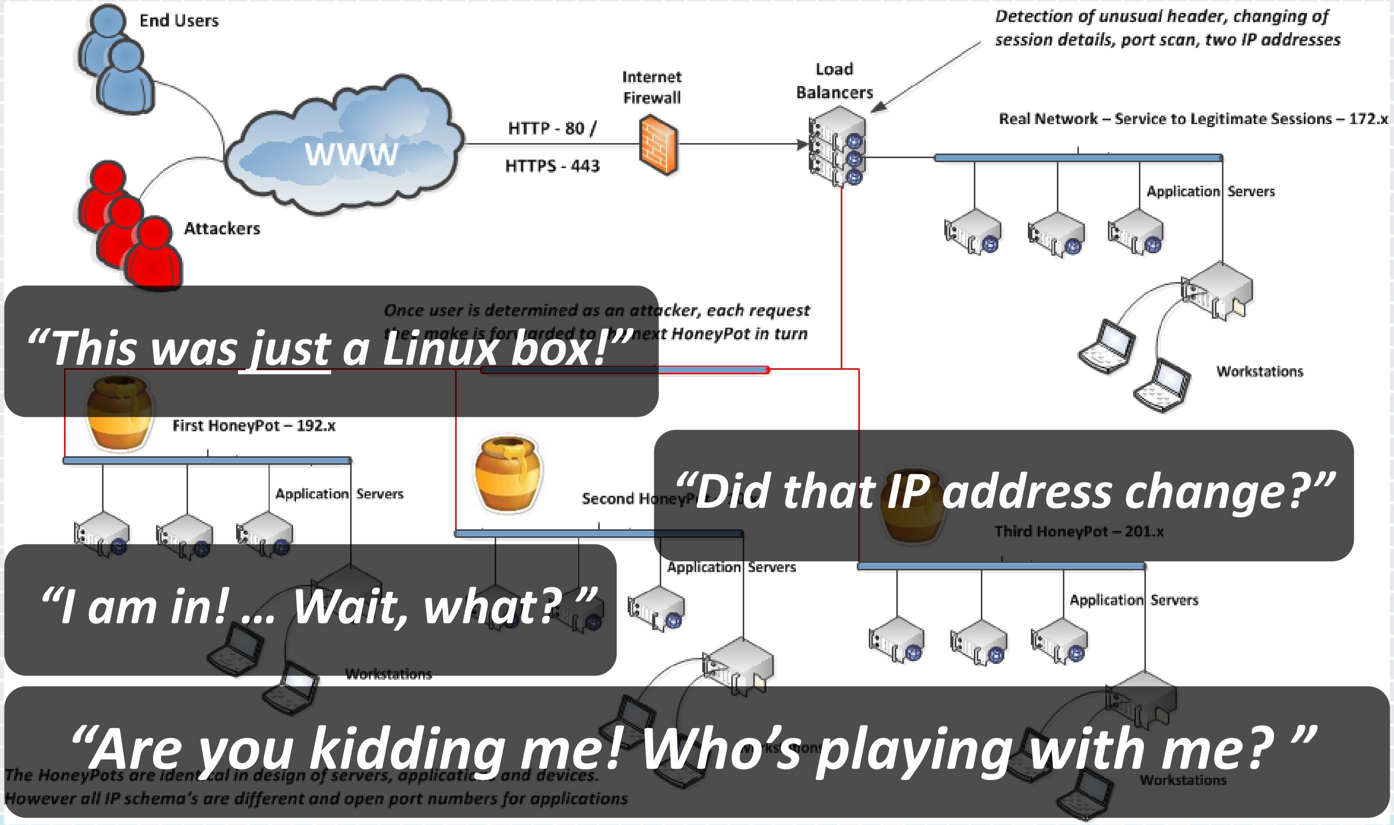
The HoneyPots are identical in design of servers, applications and devices. However all IP schema's are different and open port numbers for applications

"This was just a Linux box!"

"Did that IP address change?"

"I am in! … Wait, what? "

Deceive – Frustrate Your Attacker



Detection of unusual header, changing of session details, port scan, two IP addresses

Once user is determined as an attacker, each request they make is forwarded to the next HoneyPot in turn

The HoneyPots are identical in design of servers, applications and devices. However all IP schema's are different and open port numbers for applications

"This was just a Linux box!"

"Did that IP address change?"

"I am in! … Wait, what? "

"Are you kidding me! Who's playing with me? "

Break the Rules

Don't

- Become An Economical Target
- Be predictable
- Be passive
- Be transparent
- Constrain Your Team

Do

- ◆ Multiple forces through automation
- ◆ Switch network conditions
- ◆ Pre-approve Mitigation Actions
- ◆ Encode asset names
- ◆ Lead a team strategy

Apply

- What’s a Single Simple Action that you can change next week?
  - Design your team strategy
  - Research automation capabilities
- In the next three months, what can you do?
  - Encode names for critical assets
  - Plan network changes
  - Identify and pre-approve known, frequent mitigations