



“The Name of the Rose”

What Statistical Analysis can reveal about the threats hiding behind domain names

Davide **ARIU**
Pluribus **One**

Simone **BONETTI**
CERT
Università di **Bologna**

Luca **PIRAS**, Iginio **CORONA**
Pluribus **One**

Battista **BIGGIO**, Giorgio **GIACINTO**, Fabio **ROLI**
PRALab
Università degli Studi di Cagliari

«Conferenza GARR 2018 - », Cagliari, 3 Ottobre 2018

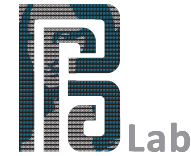


...or even better

- **A (very quick) review of the DNS infrastructure**
 - Main components
 - Working Principles
- **An overview of different kinds of abuses against such infrastructure**, which enable a wide variety of cyber attacks

About me and this work

- Working since 2006 (Ph.D./Post-Doc/Research Assistant) with the **P**attern **R**ecognition and **A**pplications **LAB**oratory (pralab.diee.unica.it) @**U**niversity of **C**agliari
 - Worked on several areas of computer security
- Since August 2015 – CEO and Co-Founder of **Pluribus One** (www.pluribus-one.it)
 - **Company Mission:** To develop safe and explainable machine learning algorithms for Cybersecurity solutions
- This presentation has been developed in the context of several R&D projects, funded through European and regional calls.



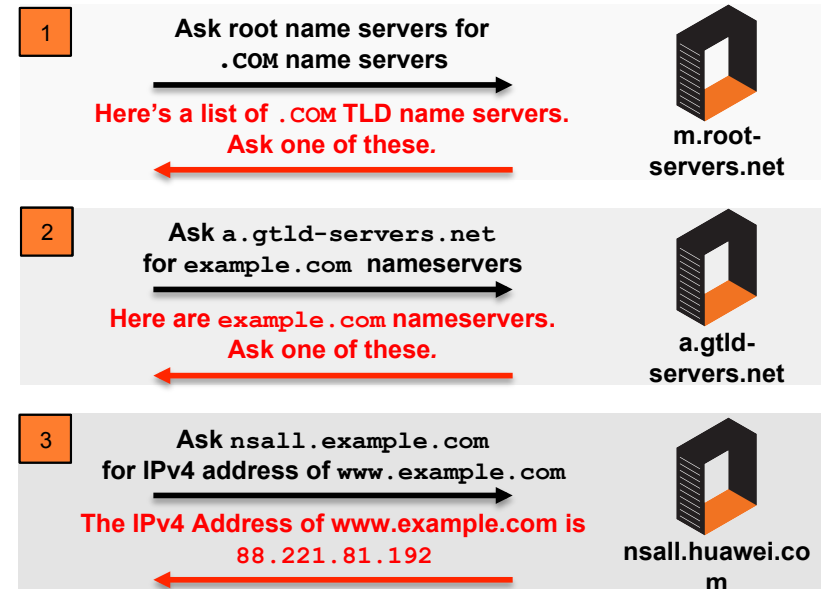
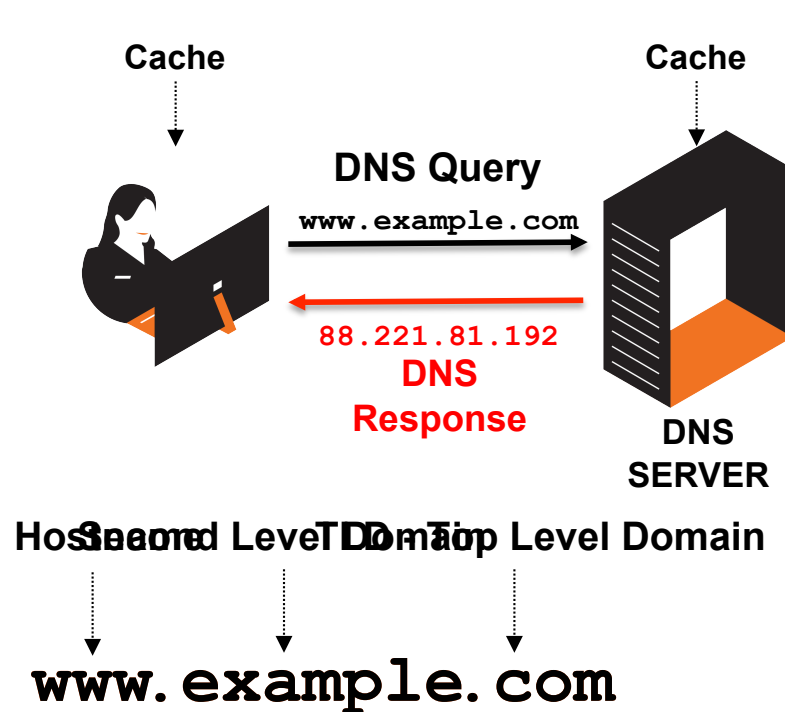
safe DNS project

supported by the Regional Government of Sardinia
and the POR FESR 2014-2020 programme



Domain Name System (DNS) – Principles

- With DNS we generically refer to the *infrastructure* (servers, protocol, resolvers, caches, etc.) which allows to translate (resolve) domain names into IPv(4/6) addresses



- Distributed
- Hierarchical
- Recursive

Role of the DNS in the modern Cyber-attacks

- The DNS has a pivotal role to support a large

1. Phishing.

- Well crafted domain names help to make phishing*¹ campaigns more effective

2. Scams

- Similarly to phishing, other kind of scam by using well-crafted domain names

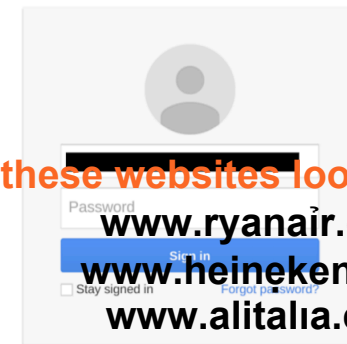
3. Botnets

- To make botnet more resilient, malware writers avoid to hardcode the IP addresses of the C&C servers and dropzones
 - They use domain names** instead
 - Often include into malware algorithms able to generate domain names dynamically → **Domain Fluxing**
 - Often use mechanisms to change frequently the association between domain names and IP addresses → **IP fluxing**

dropboxsupport.servehttp.com

Get the best Dropbox experience on-the-go, for free!

Sign in to Dropbox



*1 Source: **John Scott-Railton et Alii**, *Nile Phish: Large-Scale Phishing Campaign Targeting Egyptian Civil Society*, CitizenLab.org, 2017

About this presentation

1. What is this presentation about:

- Attacks which can be spotted through (statistical) analysis of the domain names and of information gathered during the resolution process
 - IP Fluxing
 - Domain *Squatting
 - Internationalized Domain Names Abuse
- **Examples taken from real traffic**
 - >3 years of real traffic monitoring
 - ≈ 300.000.000 DNS requests/day
 - ≈ 2.5M domain names/day
 - ≈ 430k unique IPs/day

2. Attacks not covered by the presentation

- Domain Fluxing
- Abuses of the DNS Protocol (Spoofing)
- DDoS Attacks against DNS
- Covert channels over DNS

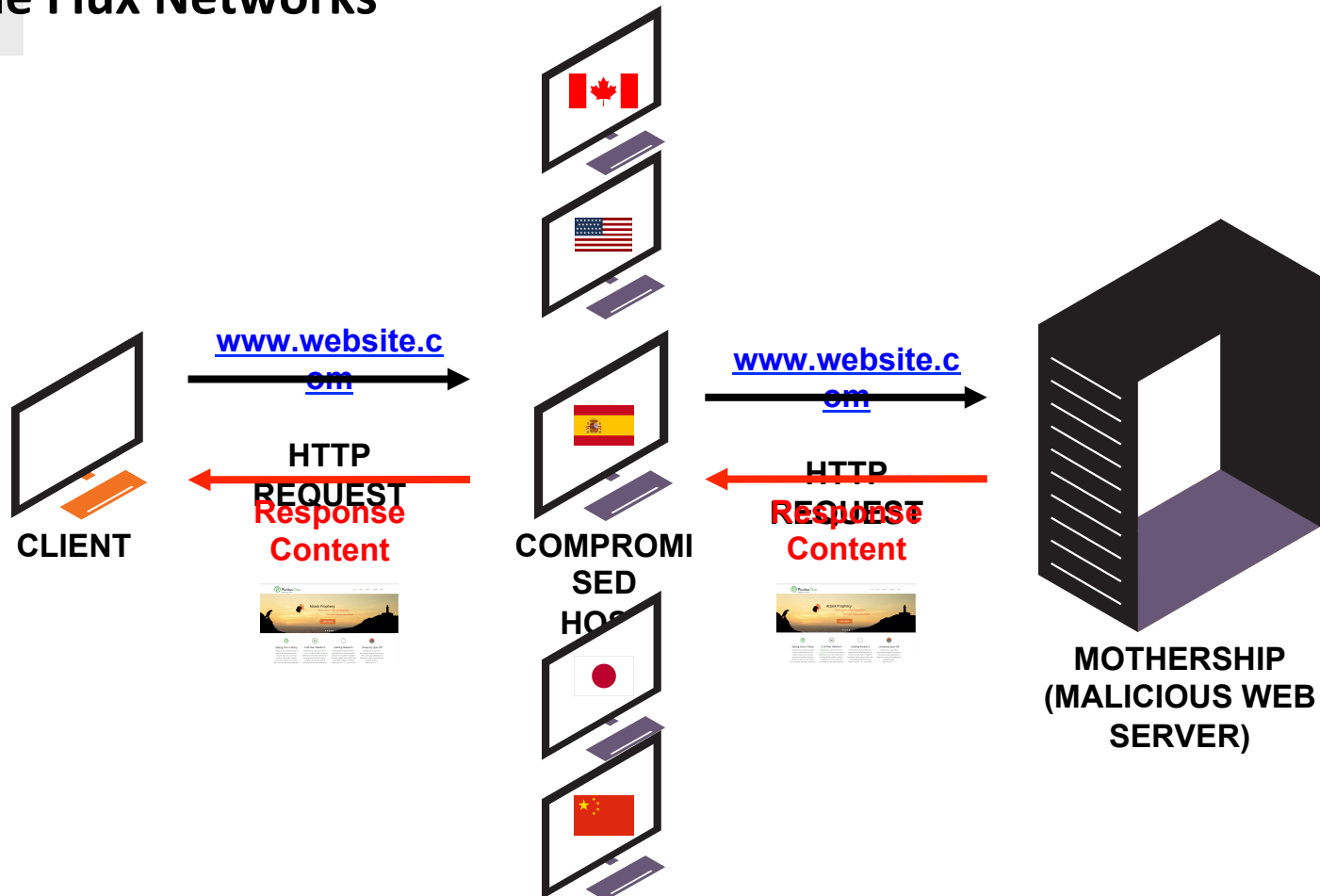


IP Fluxing

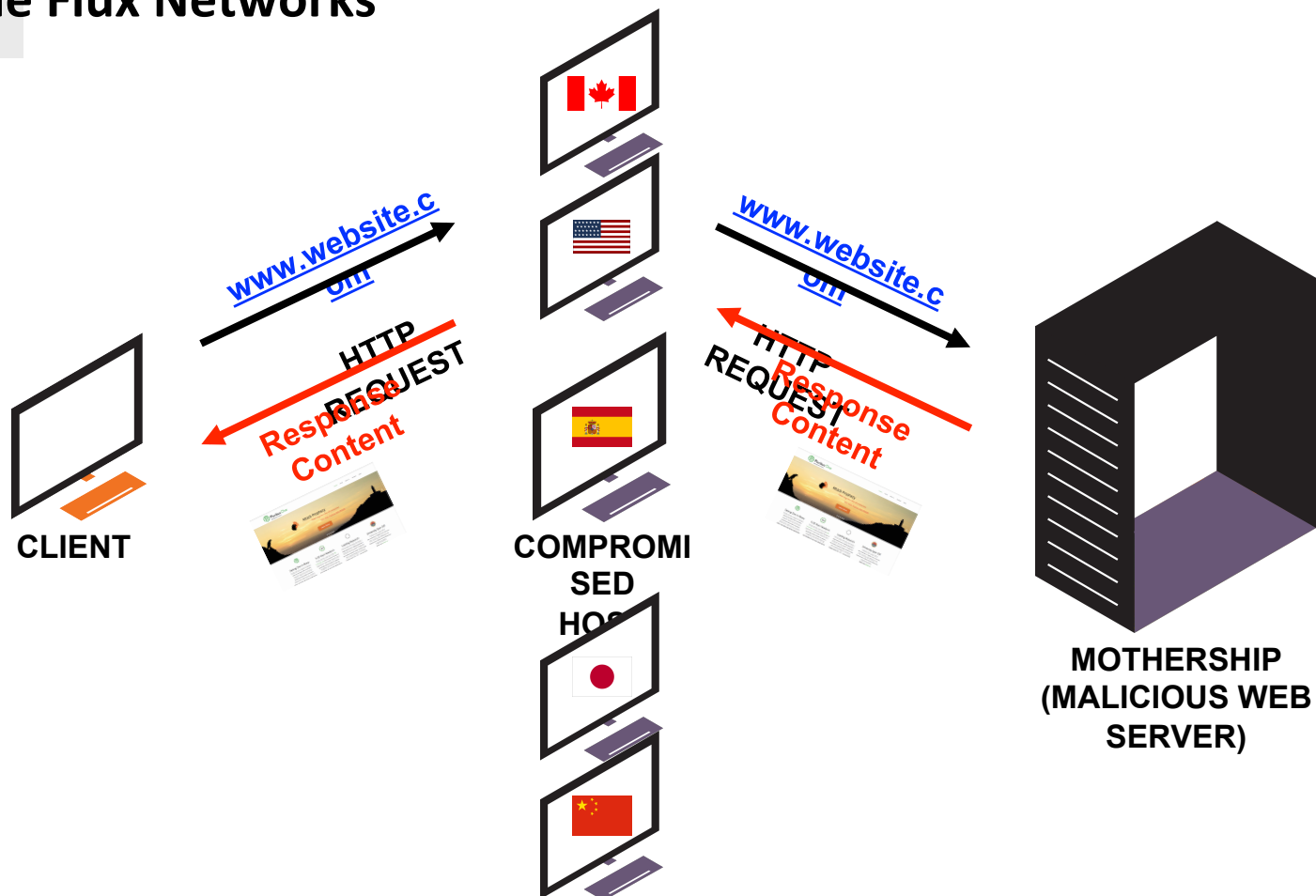
Design of Fast Flux Service Network

- **Fast-Flux Service Networks** exploit an architecture which is conceptually similar to that of **Content Delivery Networks**
- The key idea is to construct **a distributed proxy network on top of compromised machines** that redirects traffic through these proxies to a central site, which hosts the actual content.
 - Taking down any of the proxies does not effect the availability of the central site (**Mothership**)
 - The **attacker always returns a different set of IP addresses for a DNS query** and thus distributes the traffic over the whole proxy network.
 - This leads to an **increased resilience** since taking down such schemes usually needs cooperation with a domain name registrar.
 - The **Mothership** itself becomes really **hard to track**

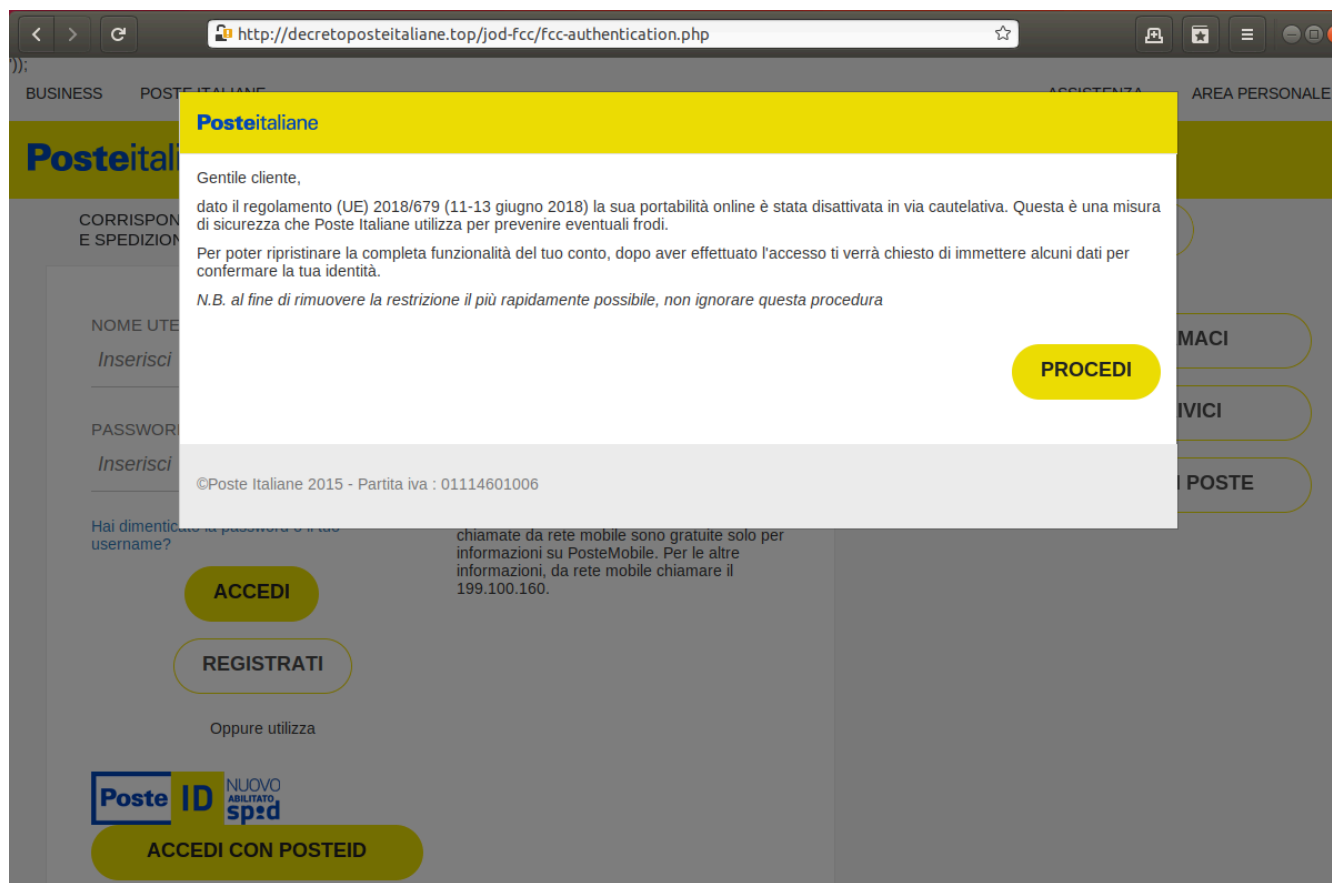
Single Flux Networks



Single Flux Networks



A Fast-Flux Domain – decretoposteitaliane.top



A Fast-Flux Domain – decretoposteitaliane.top

The screenshot shows a web browser window with the address bar displaying `http://decretoposteitaliane.top/jod-fcc/fcc-authentication.php`. The page layout includes a top navigation bar with links for BUSINESS, POSTE ITALIANE, ASSISTENZA, and AREA PERSONALE. Below this is a yellow header with the Posteitaliane logo. A secondary navigation bar lists various services: CORRISPONDENZA E SPEDIZIONI, CONTI CARTE E FINANZIAMENTI, RISPARMIO E INVESTIMENTI, PREVIDENZA E PROTEZIONE, SERVIZI AL CITTADINO, and SERVIZI ONLINE (which is highlighted). The main content area is divided into two columns. The left column contains the login form with fields for 'NOME UTENTE' and 'PASSWORD', both with 'Inserisci' placeholder text. Below these fields are links for 'Hai dimenticato la password o il tuo username?' and buttons for 'ACCEDI' and 'REGISTRATI'. At the bottom of the left column is the 'Poste ID' logo and a button 'ACCEDI CON POSTEID'. The right column contains a section titled 'Hai bisogno di aiuto?' with three buttons: 'CHIAMACI', 'SCRIVICI', and 'VIENI IN POSTE'. A block of text on the right side of the login form provides information about access credentials and contact numbers.

);

BUSINESS POSTE ITALIANE ASSISTENZA AREA PERSONALE

Posteitaliane

CORRISPONDENZA E SPEDIZIONI CONTI CARTE E FINANZIAMENTI RISPARMIO E INVESTIMENTI PREVIDENZA E PROTEZIONE SERVIZI AL CITTADINO **SERVIZI ONLINE**

NOME UTENTE
Inserisci

PASSWORD
Inserisci

[Hai dimenticato la password o il tuo username?](#)

ACCEDI

REGISTRATI

Oppure utilizza

Poste ID NUOVO ABILITATO **spid**

ACCEDI CON POSTEID

Per accedere al servizio inserisci le tue credenziali oppure registrati.

In caso di mancato accesso o non funzionamento dei servizi è possibile contattare il Call Center al numero verde 803.160 (dal lunedì al sabato dalle ore 8.00 alle ore 20.00) effettuando la scelta "3" per i Servizi Internet.

La chiamata è gratuita da rete fissa; le chiamate da rete mobile sono gratuite solo per informazioni su PosteMobile. Per le altre informazioni, da rete mobile chiamare il 199.100.160.

Hai bisogno di aiuto?

CHIAMACI

SCRIVICI

VIENI IN POSTE

A Fast-Flux Domain – decretoposteitaliane.top

Date: 2018-07-21, Cluster: 67, Sensor: TIS, Nickname: **ecure.decretoposteitaliane.top**

class: **Flux Validated**

Blacklisted IPs

ZEN 4 Blacklisted IP(s)

High IP diversity (entropy of IP /24 prefixes)

44.0 Network Cardinality
147.3 TTL per Domain
10.0 Domains per Network
2.0 Number of domains
0.966697 IP diversity

Time To Live (TTL) << than in legitimate networks

Resolved IP addresses spread over many different Autonomous Systems / Organizations.

5.0 Queries per domain
4.36667 IP Growth Ratio

4.8 IP LAST Growth ratio
4.8 IP Prefixes LAST Growth ratio
8.0 IP LAST Growth ratio (previous clusters)
7.8 IP Prefixes LAST Growth ratio (previous clusters)

High ratio of previously unseen IP addresses (novelty).
The number of IPs as well as the number of networks they do belong tends to grow.

5.0 Novelty 6 Month
6.0 Novelty 1 Month
11.0 Novelty 1 Week

TOP 10 ORGANIZATIONS: (4): AS8708 RCS & RDS SA, (3): AS6830 Liberty Global Operations B.V., (2): AS13124 Blizoo Media and Broadband EAD, (2): AS35141 MEGALAN MOBILTEL EAD, (2): AS8953 Orange Romania SA, (2): AS6821 Makedonski Telekom, (1): AS197769 ET Internet - Ventzislav Dimitrov, (1): AS8448 Telenor Hungary Telecommunications Plc., (1): AS12302 Vodafone Romania S.A., (1): AS31287 AI PI AKT OOD,

DOMAIN NAMES: **secure.decretoprivati.top**, **decretoposteitaliane.top**,

RESOLVED IP Addresses: 151.237.82.2, 176.241.82.11, 88.85.248.252, 185.94.4.228, 190.219.210.37, 103.244.248.94, 46.238.18.157, 81.12.175.59, 213.222.130.75, 155.133.93.30, 37.143.160.70, 87.97.249.2, 188.26.83.210, 190.213.108.96, 46.217.126.201, 90.177.80.171, 93.103.166.70, 46.217.125.85, 66.181.168.248, 84.224.103.179, 213.149.152.120, 80.98.149.20, 93.114.82.80, 197.255.225.249, 186.74.208.84, 86.124.61.73, 188.27.204.20, 109.166.237.170, 46.10.53.233, 95.158.162.200, 109.166.208.203, 78.96.178.214, 46.238.18.241, 103.62.144.18, 188.25.33.204, 200.91.115.40, 151.251.23.210, 197.255.246.6, 37.210.199.164, 158.174.70.91, 77.85.213.209, 86.106.200.105, 188.254.187.254, 124.43.17.103,



Domain Squatting

Cybersquatting

Anticybersquatting Consumer Protection Act – U.S. 1999

- A **person** shall be **liable** in a civil action **by the owner of a mark if [...]**
 - ‘(ii) **registers**, traffics in, or uses **a domain name that—**
 - ‘(I) **in the case of a mark** that is distinctive at the time of registration of the domain name, **is identical or confusingly similar to that mark; [...]**
 - ‘(III) **is a trademark, word**, or name protected by reason of section 706 of title 18, United States Code, or section 220506 of title 36, United States Code.
- **Cybersquatting is used to make cyber-attacks more effective (less noticeable), and in particular:**
 - **Phishing**
 - Well crafted domain names help to make phishing campaigns more effective
 - **Scams**
 - Are vehiculated by using well-crafted domain names
 - Often using social networks and messaging platforms (e.g. Whatsapp)

Squatting Types

Domain Name	Squatting Type
youtube.com	Original Domain
yewtube.com	Homophone-Based Squatting
youtubg.com	Bitsquatting
YOUTUBE.COM	Homograph-Based Squatting
youtubee.com	Typosquatting

- **Typosquatting** generally refers to the practice of registering domains which are minor typographical variations of popular domain names.
- **Possible replacement strategies:**
 - **Missing Dot** → www.youtube.com
 - **Character Omission** → yutube.com
 - **Character Duplication** → youutube.com
 - **Character Permutation** → yuotube.com
 - **Character Substitution** → yoyube.com

Source: P. Kintis et. Al., *Hiding in Plain Sight: A Longitudinal Study of Combosquatting Abuse*, ACM CCS, 2017
Source: Farsight Security, *Global Internationalized Domain Name Homograph Report*, Q2-2018.

Squatting Types – Homoglyph Based Squatting

Domain Name	Squatting Type
youtube.com	Original Domain
yewtube.com	Homophone-Based Squatting
youtubg.com	Bitsquatting
YOUTUBE.COM	Homograph-Based Squatting
youtubee.com	Typosquatting
youtube-login.com	Combosquatting
youṭube.com	Homoglyph-Based Squatting

Homoglyph based squatting

- Attackers abuse Internationalized Domain Names
- **At DNS level, domains are encoded using ASCII characters only**
 - Punycode encoding is used
 - E.g. **youṭube.com** is represented as **xn--youube-k17b.com**
- **Homoglyph Examples**
 - Cyrillic « а »
 - Lating jota « Ĺ »

Source: P. Kintis et. Al., *Hiding in Plain Sight: A Longitudinal Study of Combosquatting Abuse*, ACM CCS, 2017

Source: Farsight Security, *Global Internationalized Domain Name Homograph Report*, Q2-2018.

Copying, reproduction, modification, distribution, display or transmission of any of the contents of this presentation for any purpose without the prior written consent of Pluribus One SRL is strictly prohibited.

Homoglyph Based Squatting – www.alitalia.com



Valido solo per oggi-

Stiamo dando 2 biglietti gratuiti per celebrare il nostro decimo anniversario!

Biglietti rimanenti : Caricamento

Si prega di prendere parte al sondaggio prima:

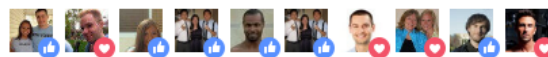
Domanda 1: Hai mai viaggiato con noi ?

☒ Si

☐ Non

☐ Non ricordo

👍 Mi Piace 💬 Commenta ➦ Condividi



e altri 65.059



Rachel Singleton Grazie Alitalia, ora posso andare per la mia luna di miele

Mi Piace · Risposta · 👍 50 · Proprio ora



Julia Schröder Ho appena fatto una prova e mi chiedo, ho ottenuto il mio 2 biglietti gratuiti

Mi Piace · Risposta · 👍 16 · Proprio ora



Michael Drechsler Mi piace volare con loro, sono i migliori

Mi Piace · Risposta · 👍 27 · Proprio ora



Johanna Grunewald Grazie Alitalia.

Mi Piace · Risposta · 👍 18 · Proprio ora



Scrivi un commento...



📖 Maggiori informazioni

* Questa offerta è valida solo per tempo limitato.

Alitalia-2018

Homoglyph Based Squatting – www.ryanair.com



Valido solo per oggi-

Ryanair dà 2 biglietti gratuiti per celebrare il 34 ° anniversario.

Biglietti rimanenti : Caricamento

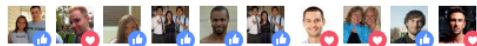
Si prega di prendere parte al sondaggio prima:

Domanda 1: Hai mai viaggiato con noi?

☐ Sì

☐ Non

👍 Mi Piace 💬 Commenta ➦ Condividi



e altri 65.059



Lynse-anne Grazie Ryanair, Ho ottenuto i miei biglietti gratuiti, sono davvero grato a voi



Mi Piace · Risposta · 🗨️ 50 Â · Proprio ora



Julia Schröder Ho ricevuto i miei biglietti gratuiti, grazie, Ryanair

Mi Piace · Risposta · 🗨️ 16 Â · Proprio ora



Michael Drechsler Ho biglietti gratuiti Ryanair

Mi Piace · Risposta · 🗨️ 27 Â · Proprio ora



Johanna Grunewald grazia, Ryanair

Mi Piace · Risposta · 🗨️ 18 Â · Proprio ora



Scrivi un commento...



📖 Maggiori informazioni

* Questa offerta è valida solo per tempo limitato.

Ryanair-2018

Homograph Based Squatting – www.ryanair.com



Valid for today only-

Ryanair donne 2 billets gratuits pour célébrer le 34e anniversaire.

Billets restants : Chargement

S'il vous plaît prendre part à l'enquête d'abord:

Question 1: Avez-vous déjà voyagé avec nous ?

☐ Oui

☐ Non

☐ Ne me souviens pas

Homoglyph Based Squatting – www.ryanair.com

Aktion nur noch heute -

Ryanair gibt 2 Freikarten, um das 34. Jubiläum zu feiern.

Verbleibende flugtickets: *wird geladen*

Bitte nimm zuerst an der Umfrage teil:

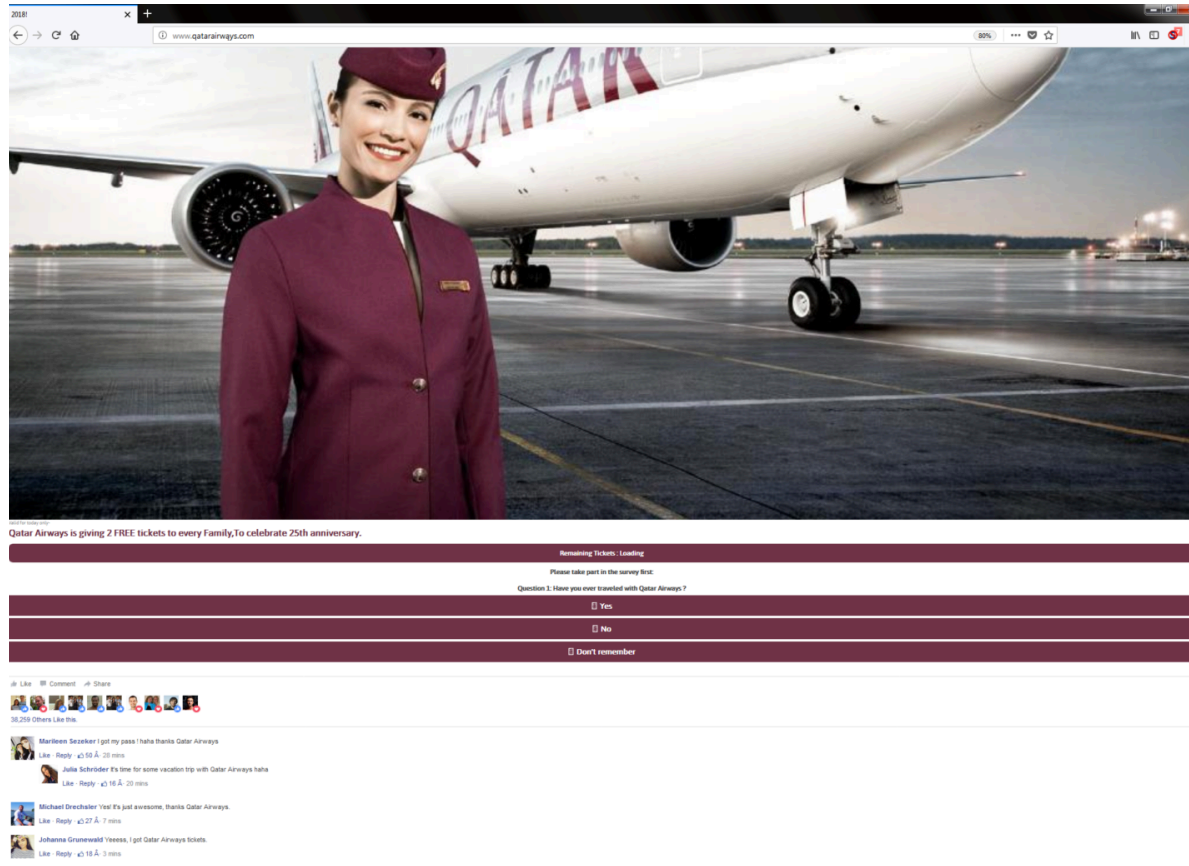
Frage 1: Haben Sie schon einmal mit uns gereist ?

☐ Ja

☐ Nein

☐ Weiß ich nicht

Homoglyph Based Squatting – www.qatarairways.com



Homoglyph Based Squatting – www.westjet.com

← → ↻ 🏠 www.westjet.com ... 📌 ☆ Cerca

We are giving free 5000 tickets to celebrate our birthday.

Remaining tickets: Loading

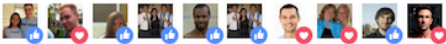
Please answer the questions below first:


Question 1: Do you think WestJet is the best?


Yes


No


👍 Like 💬 Comment ➦ Share

 17,259 Others Like this.

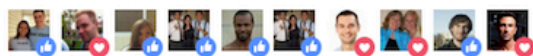
 **Rachel Singleton** Thank you soo much WestJet for tickets! i got mine
Like · Reply · 🗨️ 50 🗨️ 28 mins

 **Julia Schröder** It's time for some good shopping @ WestJet
Like · Reply · 🗨️ 16 🗨️ 20 mins

 **Michael Drechsler** Yes! It's just awesome, thanks WestJet.
Like · Reply · 🗨️ 27 🗨️ 7 mins

 **Johanna Grunewald** Yeeess, I got WestJet coupon.
Like · Reply · 🗨️ 18 🗨️ 3 mins

Look at the winners...



17,259 Others Like this.



Rachel Singleton Thank you soo much WestJet for tickets! i got mine

Like · Reply · 50 Â· 28 mins



Julia Schröder It's time for some good shopping @ WestJet

Like · Reply · 16 Â· 20 mins



Michael Drechsler Yes! It's just awesome, thanks WestJet.

Like · Reply · 27 Â· 7 mins



Johanna Grunewald Yeeess, I got WestJet coupon.

Like · Reply · 18 Â· 3 mins



Marileen Sezeke I got my pass ! haha thanks Qatar Airways

Like · Reply · 50 Â· 28 mins



Julia Schröder It's time for some vacation trip with Qatar Airways haha

Like · Reply · 16 Â· 20 mins



Michael Drechsler Yes! It's just awesome, thanks Qatar Airways.

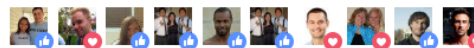
Like · Reply · 27 Â· 7 mins



Johanna Grunewald Yeeess, I got Qatar Airways tickets.

Like · Reply · 18 Â· 3 mins

👍 Mi Piacce · 💬 Commenta · ➦ Condividi



e altri 65.059



Rachel Singleton Grazie Alitalia, ora posso andare per la mia luna di miele

Mi Piacce · Risposta · 50 Â· Proprio ora



Julia Schröder Ho appena fatto una prova e mi chiedo, ho ottenuto il mio 2 biglietti gratuiti

Mi Piacce · Risposta · 16 Â· Proprio ora



Michael Drechsler Mi piace volare con loro, sono i migliori

Mi Piacce · Risposta · 27 Â· Proprio ora

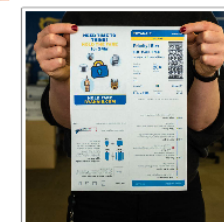


Johanna Grunewald Grazie Alitalia.

Mi Piacce · Risposta · 18 Â· Proprio ora



Lynse-anne Grazie Ryanair, Ho ottenuto i miei biglietti gratuiti, sono davvero grato a voi



Mi Piacce · Risposta · 50 Â· Proprio ora



Julia Schröder Ho ricevuto i miei biglietti gratuiti, grazie, Ryanair

Mi Piacce · Risposta · 16 Â· Proprio ora



Michael Drechsler Ho biglietti gratuiti Ryanair

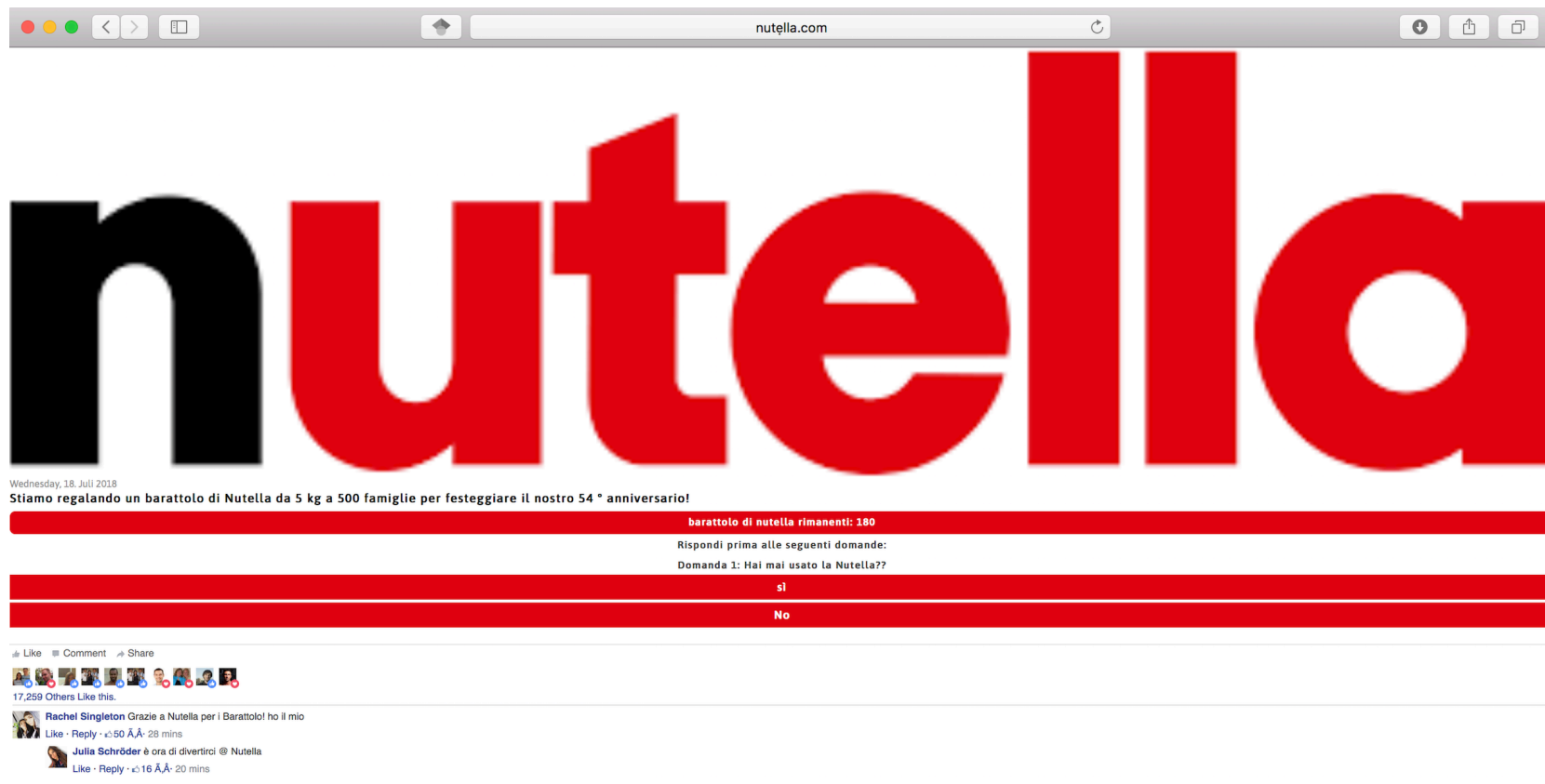
Mi Piacce · Risposta · 27 Â· Proprio ora



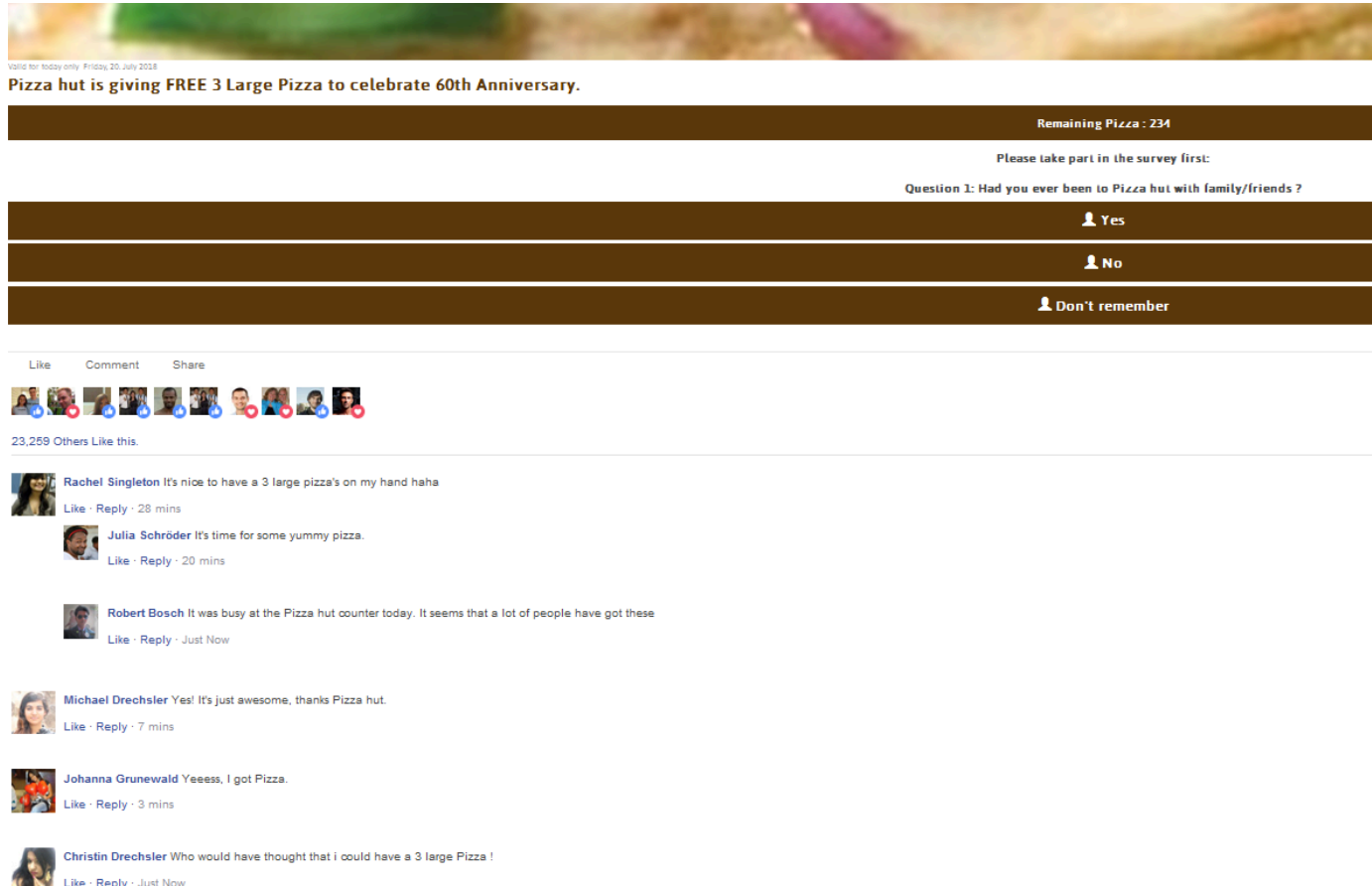
Johanna Grunewald grazia, Ryanair

Mi Piacce · Risposta · 18 Â· Proprio ora

Homoglyph Based Squatting – www.nutella.com



Homoglyph Based Squatting – www.p1zzahut.online



Valid for today only - Friday, 20 July 2018

Pizza hut is giving FREE 3 Large Pizza to celebrate 60th Anniversary.

Remaining Pizza : 234

Please take part in the survey first:

Question 1: Had you ever been to Pizza hut with family/friends ?

☐ Yes

☐ No

☐ Don't remember

Like Comment Share

23,259 Others Like this.

Rachel Singleton It's nice to have a 3 large pizza's on my hand haha
Like · Reply · 28 mins

Julia Schröder It's time for some yummy pizza.
Like · Reply · 20 mins

Robert Bosch It was busy at the Pizza hut counter today. It seems that a lot of people have got these
Like · Reply · Just Now

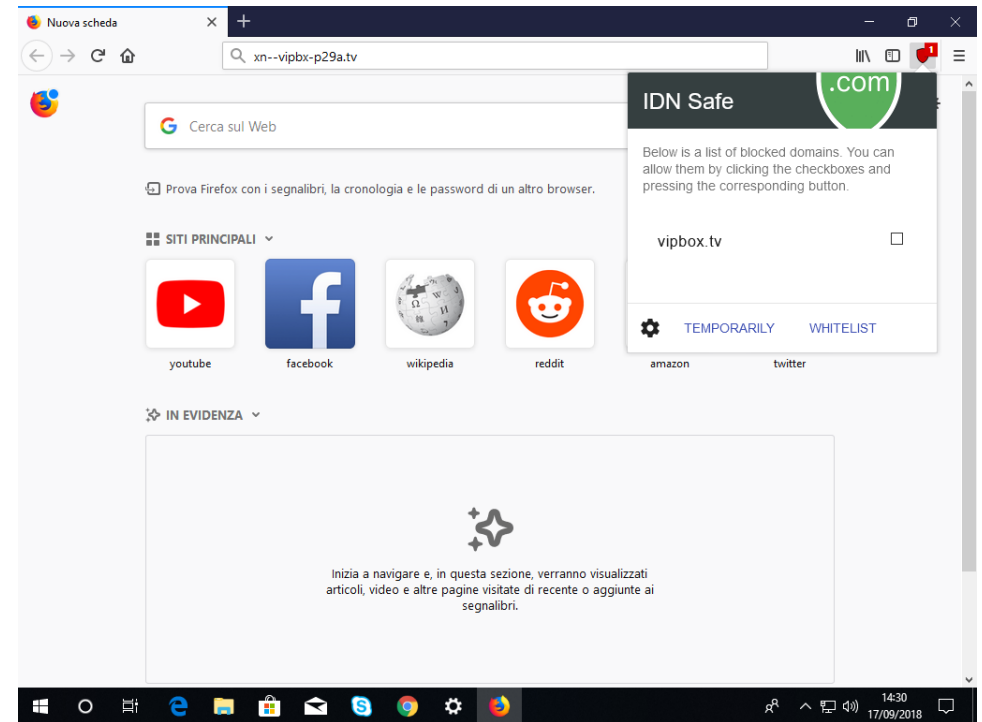
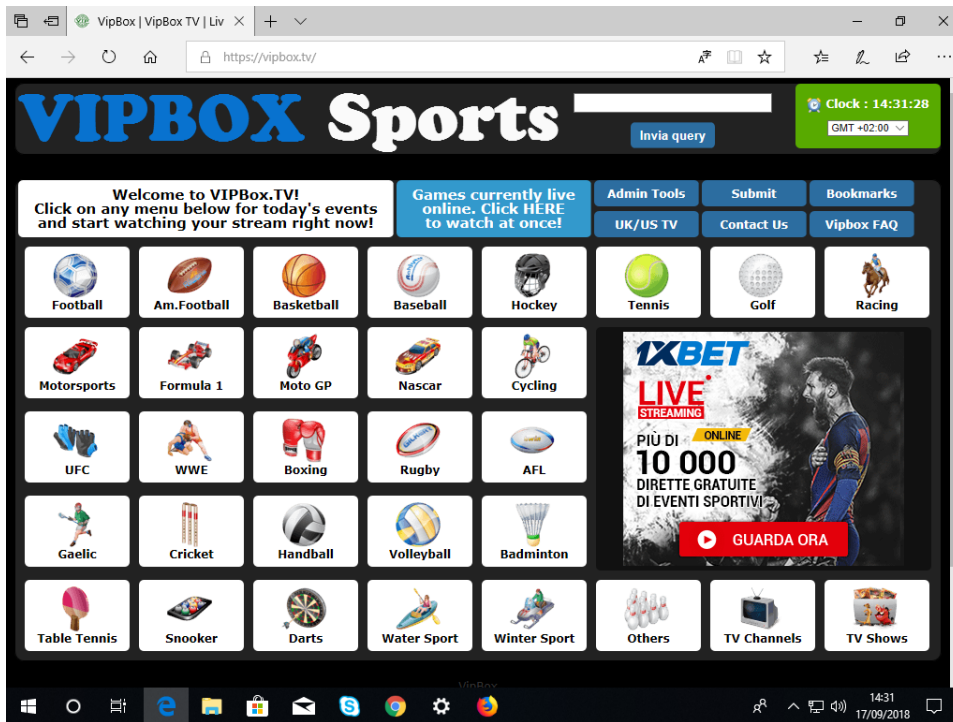
Michael Drechsler Yes! It's just awesome, thanks Pizza hut.
Like · Reply · 7 mins

Johanna Grunewald Yeeess, I got Pizza.
Like · Reply · 3 mins

Christin Drechsler Who would have thought that I could have a 3 large Pizza !
Like · Reply · Just Now

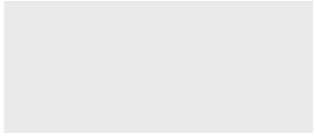
Homoglyph Based Squatting to Evade Blacklisting –

www.vipbpx.tv



Lessons Learned

- The DNS traffic is a primary source of information regarding what is happening on the network
 - **Always worth to look at it!**
- The analysis should be done on site:
 - External blacklisting services are really effective only against large scale campaigns:
 - Short-lived domains can easily evade them
 - **You should monitor and analyse your own traffic!**
- Challenges
 - Ad-hoc detection algorithms for every specific threat
 - Many multi-faceted threats to face
 - Validation of the results



Thanks!!

Questions?



davide.ariu@pluribus-one.it



<https://www.linkedin.com/in/davideariu/>



@davideariu



Contact us!



Pluribus One S.r.l.

Via Vincenzo Bellini 9, Cagliari (CA), Italy

Via Emilio Segrè, 17, Elmas (CA), Italy

info@pluribus-one.it

www.pluribus-one.it