

# Evidence Based Cybersecurity and its Relevance for Guiding Certificate Authorities Operations



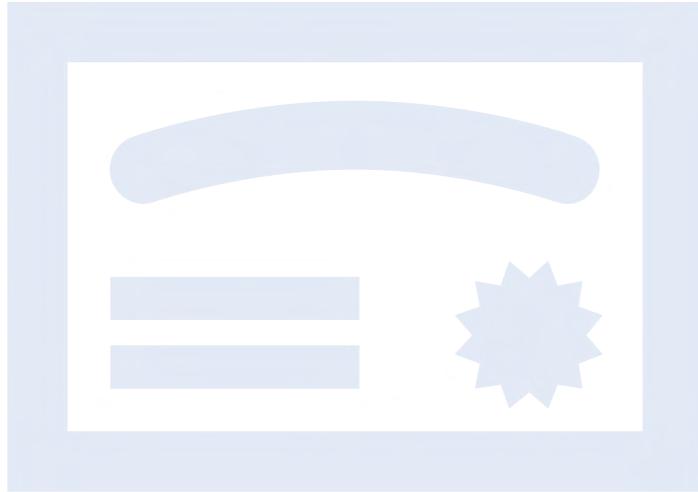
Andrew Young School of Policy  
Criminology and Criminal Justice  
Evidence Based Cybersecurity Research Group





# Outline

- Evidence Based Cybersecurity
- Relevance to Certificate Authorities
  - TLS Certificate sells over underground platforms
  - Website defacement





# RESEARCHING THE HUMAN FACTOR IN CYBERSECURITY

Cybersecurity experts mostly focus on code. Our group is different. We learn from criminals and victims to protect you.



## OUR APPROACH

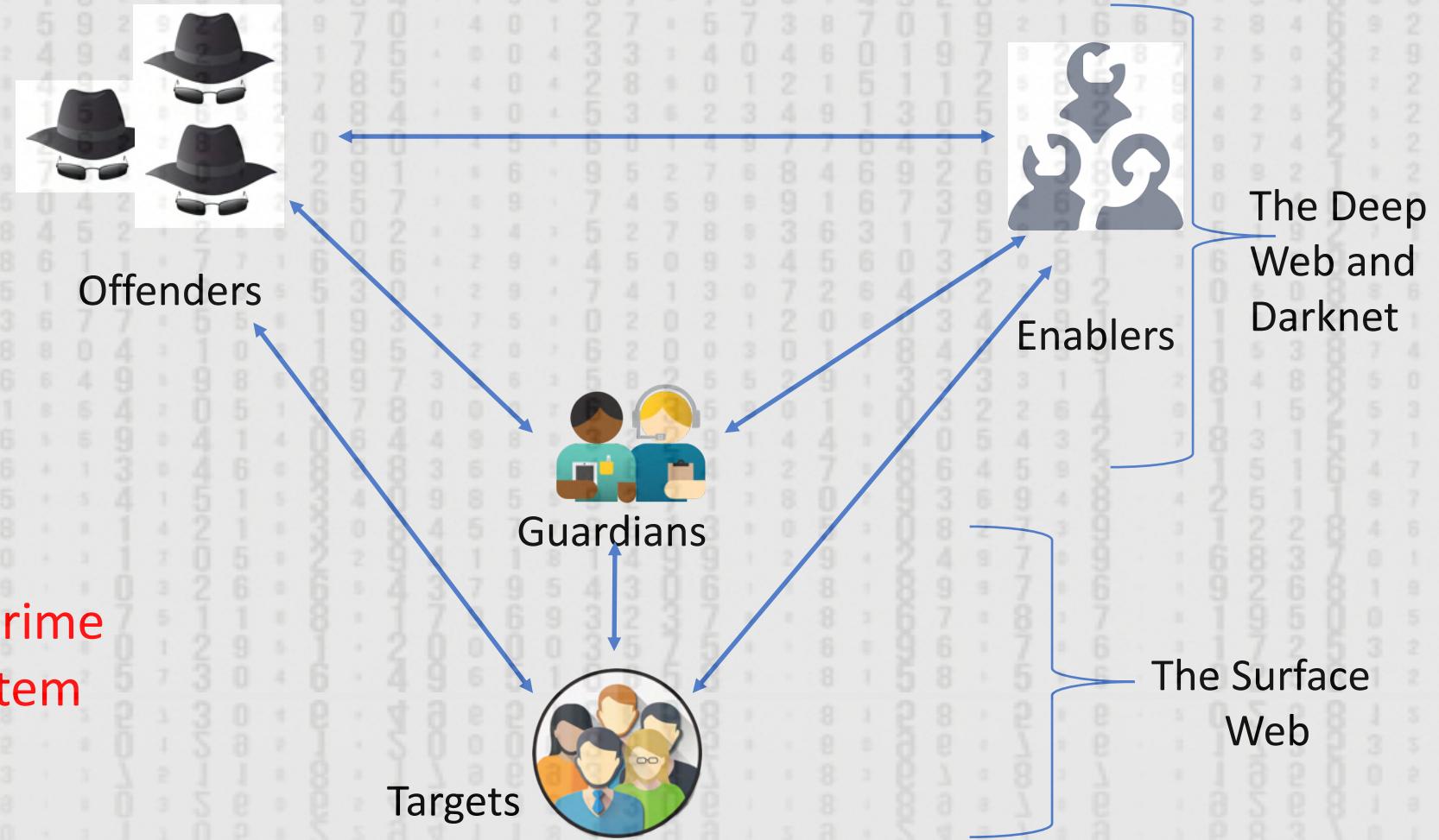
We use science to minimize cyber harm, this involves nudging cybercriminals to reveal themselves on attacked systems and networks, while encouraging legitimate users to take protective actions.

# Evidence-Based Cybersecurity (EBCS)

- Stresses moving beyond decision makers' political, financial, social background and personal experience when making security decision to a model in which tools' adoption and policy enforcements decisions are made based on scientific studies findings.

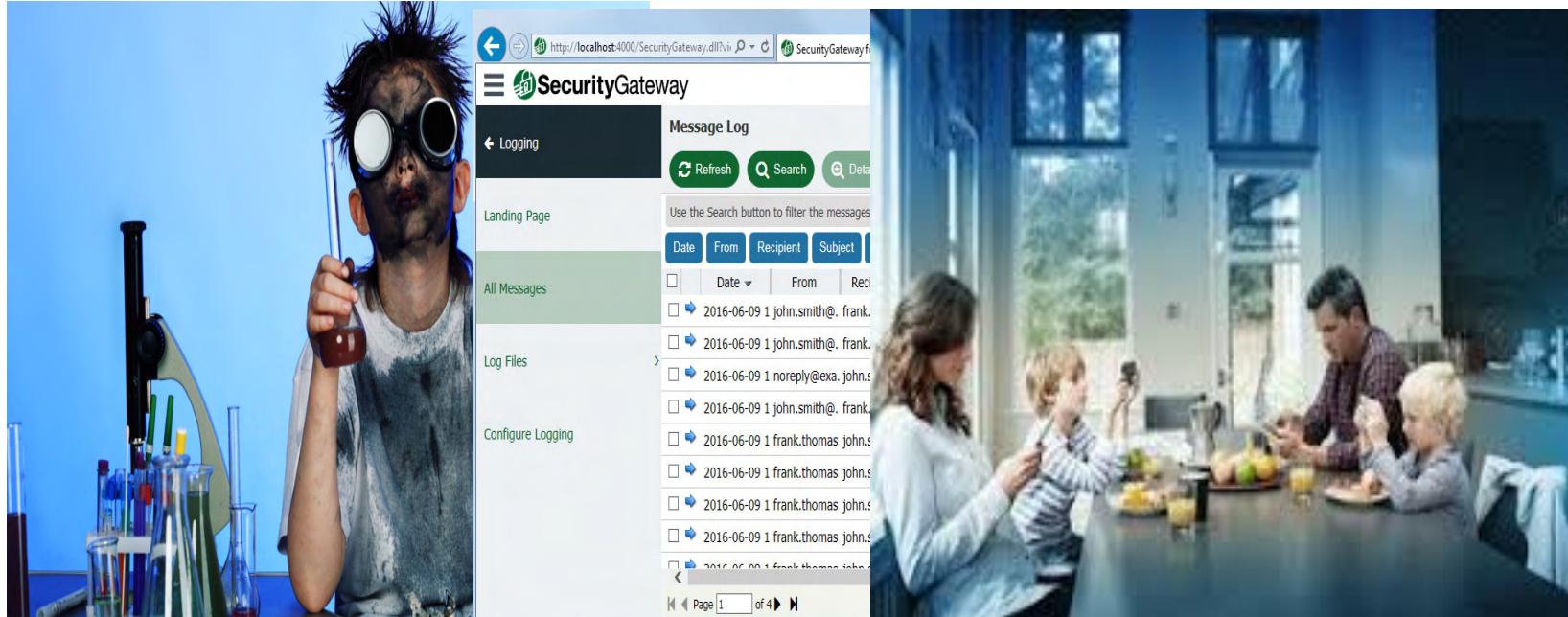


# Cybercrime Ecosystem





# Rigorous Scientific Research Designs



The collage illustrates the integration of scientific research with digital security and everyday life.

- Left Image:** A scientist in a white lab coat and safety goggles holds a test tube containing a red liquid. In the foreground, several other test tubes with different colored liquids are visible on a stand.
- Middle Image:** A screenshot of a web-based "SecurityGateway" application. The title bar shows the URL <http://localhost:4000/SecurityGateway.dll?vi>. The main content area is titled "Message Log" and displays a list of messages from June 9, 2016. The messages are as follows:
  - [checkbox] 2016-06-09 1 john.smith@. frank.
  - [checkbox] 2016-06-09 1 john.smith@. frank.
  - [checkbox] 2016-06-09 1 noreply@exa. john.s
  - [checkbox] 2016-06-09 1 john.smith@. frank.
  - [checkbox] 2016-06-09 1 frank.thomas john.s
  - [checkbox] 2016-06-09 1 frank.thomas john.s
  - [checkbox] 2016-06-09 1 frank.thomas john.s
  - [checkbox] 2016-06-09 1 frank.thomas john.s
- Right Image:** A family of four (two adults and two children) is seated around a dining table in a modern kitchen. They appear to be having breakfast or a meal together. Large windows in the background provide a view of a city skyline.



# Key Principals of the Approach

Generate and employ empirical evidence to:

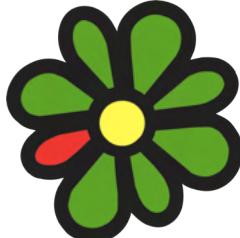
- Identify online threats and vulnerabilities and educate targets of cybercrime
- Support policy development and guardians' efforts to secure cyberspace
- Guide the design and configuration of computing environments that can mitigate effectively the consequences cybercrime events

- The translation of research findings into a format that is accessible and easy to digest for cybersecurity professionals in the field

The screenshot shows the Georgia State University website's navigation bar at the top, featuring links for Georgia State Home, About, Projects, People, Training, Courses, Evidence, Students, Faculty & Staff, Alumni, and a calendar icon. Below the navigation is a section titled "Publications" with a horizontal line and a double arrow icon. Underneath are tabs for Articles, Proceedings, Reports, Presentations, Infographics, and Tools, with "Articles" being the active tab. A list of publications is displayed:

- Deterrence in Cyberspace: An Interdisciplinary Review of the Empirical Literature  
Uploaded: 04/24/20
- Attacking and securing beacon-enabled 802.15.4 networks  
Uploaded: 04/24/20
- Demonstrating the Threat of Hardware Trojans in Wireless Sensor Networks  
Uploaded: 03/30/20
- Learning from the Offenders' Perspective on Crime Prevention  
Uploaded: 02/03/20
- The Offenders' Perspective on Prevention: Guarding Against Victimization and Law Enforcement  
Uploaded: 02/03/20
- Online Deception and Situations Conducive to the Progression of Non-Payment Fraud  
Uploaded: 01/16/20
- Website Defacement and Routine Activities: Considering the Importance of Hackers' Valuations of Potential Targets  
Uploaded: 01/06/20

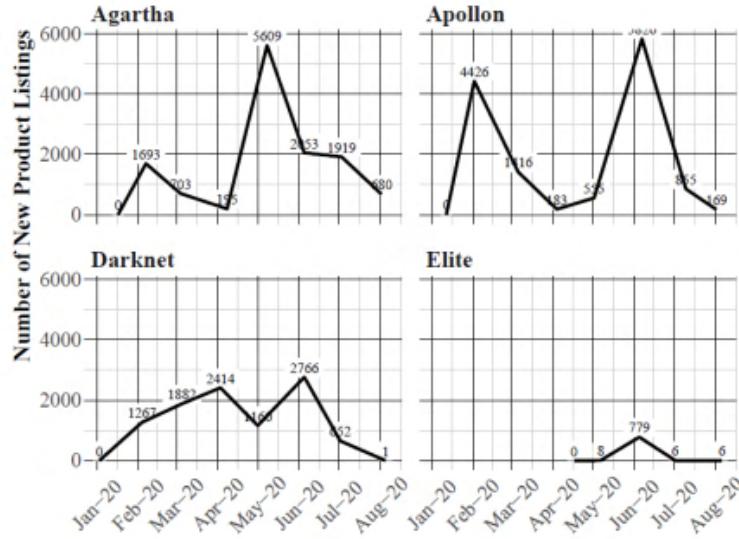
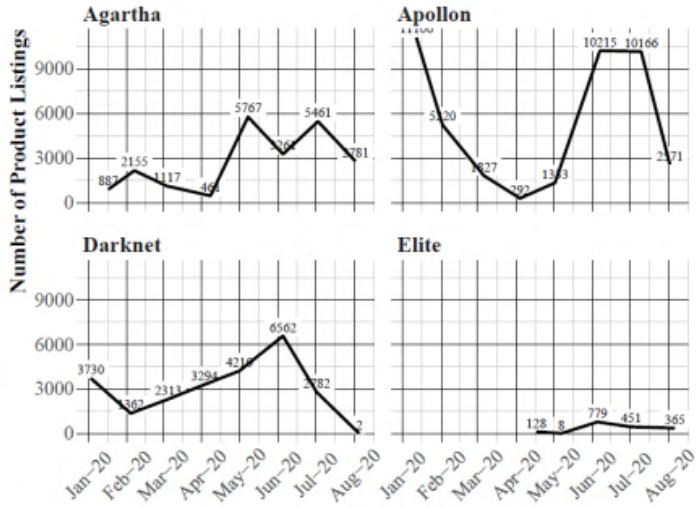
Identify  
Threats  
Trends





Collecting, Sorting and Analyzing

# Market Trends – New Products



# Mentions Count of Search Performed on December 3<sup>rd</sup>

Web Name	SSL Certificates	TLS Certificates
Dream Market	2912	64
Wall Street	10	4
BlockBooth	3	1
Nightmare	2	0
Galaxy3	16	7

# TLS Certificates Sold along with Web Design Services (Dream Market)

Browse by category	
» Services	6107
» Hacking	738
» IDs & Passports	1491
» Money	1060
» Other	907
» Cash out	1146
<hr/>	
» Digital Goods	62724
» Drugs	84469
Drugs Paraphernalia	465
» Services	6107
» Other	8162
<hr/>	
Onion mirrors	
uhivlt5grqjhad7.onion	verified

eCommerce with Private Host & Domain [+ SSL]

Vendor [REDACTED] (3)

Price [REDACTED]

Ships to Worldwide, Worldwide

Ships from PM

Escrow No



## Product description

We are offering now eCommerce on one of the follower providers:

AbanteCart

PrestaShop

WHMCS

CubeCart

osCommerce

Zen Cart

The Next Cart

## Links

- » Forum
- » Help
- » Conferences
- » Vendor application
- » Earn money

## ฿ Exchange

BTC	1.0
mBTC	1000.0
BCH	28.3
» USD	3618.5
EUR	3191.2
GBP	2868.9
CAD	4888.9
AUD	5048.5
mBCH	28366.0
BRL	14210.5
DKK	23828.9
NOK	31644.2
SEK	32863.2
TRY	19373.9
CNH	25019.2
HKD	28408.3
RUB	244192.9
INR	254676.1
JPY	40810.2

## News

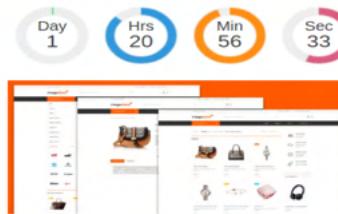
» Downtime & Recovery  
13/09/2017

» Deposit delays  
27/10/2016

» Forum under  
maintenance  
12/08/2016

» Earn money by finding

# TLS Certificates Sold along with Web Design Services (Bitify)



Available QTY

Buy Now

8 items

\$100.00 (Reference Only)

0.011910 BTC

Buy Now

Seller:  
Feedback: 10 0 2  
Rating: 83.3% (12)  
Member Since: Jan 3rd, 2019

Item ID

#2133851

Reserve

Reserve price met.

Condition

Brand New

Ending

9/27/2019, 8:37:30 AM

+ Watch

Category:

Misc (Digital Goods)

Location:

USA

Viewed:

63 times

Contact Seller

Report Listing

## Item description

I will provide you with professional looking Custom made E-commerce Webstores! I've made thousands of websites and I know exactly what you need.

These websites can be used for ANY payment processor (PAYPAL+STRIPE+SQUARE+BRAINTREE)

You will only provide me with merchant details and I will connect it to the ecommerce website. And Bam you're ready to go!

## What you will have:

- ✓ Aged domain
- ✓ Guaranteed satisfaction
- ✓ Ready to use E-commerce webstore
- ✓ Low-risk products
- ✓ professionally designed
- ✓ Hosting and Domain will be within the package

# EV Certificates of USA Companies- NO Doc or verification required

Last Scrapped: 3 hours ago [Update now](#)

## USA Company + EV SSL + D-U-N-S All in one(No Document Required)

Product Rating: (0)  
Price: 1,300.00 USD  
[View in OpenBazaar](#)

Sold by: [bulkaccounts](#) (3)  
New York  
Last Online: 6 months ago  
Product Last Modified: 4 months ago

Large Gallery (NoScript Detected)

## Description

This all in one package is suitable for all type of online business

## Description

This all in one package is suitable for all type of online business

You will get Your company registered in USA with Comodo EV SSL for your domain with D-U-N-S number.

What you will get?

- Complete Company Documents
- D-U-N-S Number
- EV SSL (Comodo)

No Documents required from you. You will stay completely anonymous.

We provide Hyp Manager Script + Perfectmoney Verified Account, AdiCash Verified Account, Payeer Verified Account, OKPay Verified Account, Payza Verified Account, PayPal Verified Account.

We also provide SSL from companies below

- Symantec
- GoDaddy
- GlobalSign
- DigiCert
- StartCom
- Geotrust
- Trustwave

We also provide security seals from Steckel, McAfee, Truste, Trust-Guard, VeriSign, Trustwave.

If you need any other EV SSL rather then Comodo or need any other services listed above please contact me.

Tags - USA Company, USA Company registration, ev ssl, ssl, us company, DUNS, D-U-N-S, db, company formation

Contact Detail:

Skype : [live.ly/1c8cas28123a1c2f](https://live.ly/1c8cas28123a1c2f)

Telegram : <https://t.me/globalexpert>

Email : [\[email protected\]](mailto:[email protected])

## Terms And Conditions

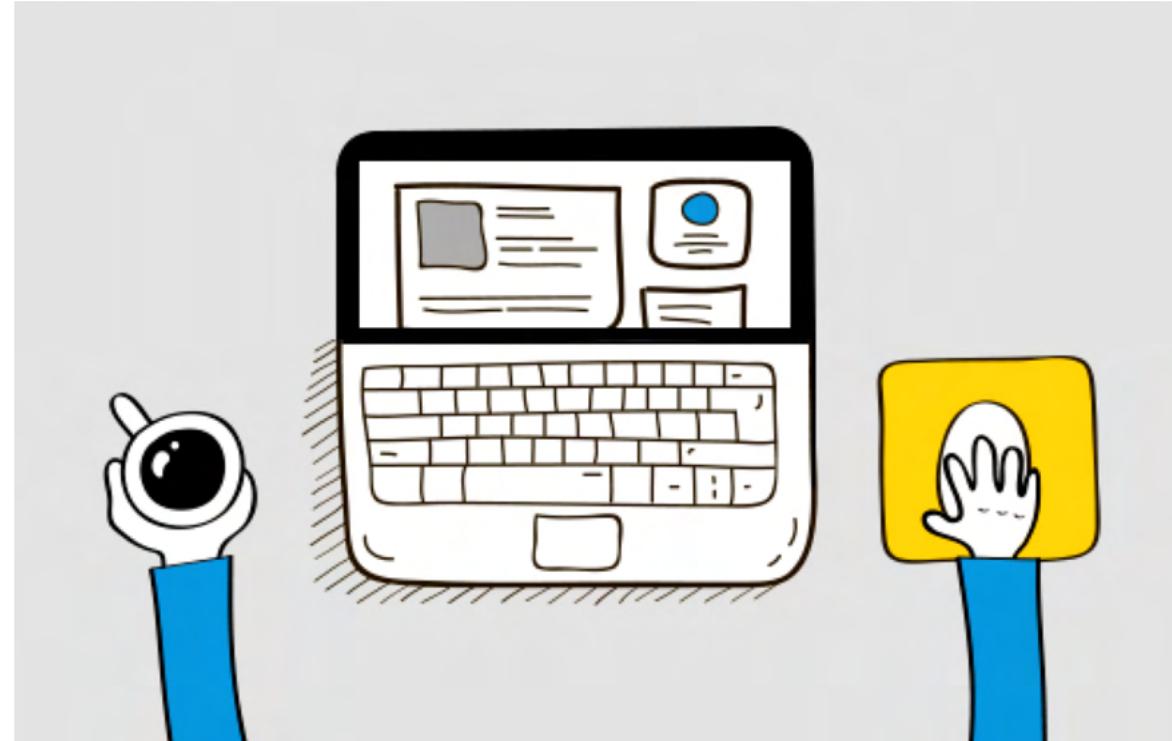
Please do Not Try To Change Account password or any Other Detail If you do there will be no account replacement. For Account Replacement you should leave 5 star rating. If you did not do so then we will not replace your account.

# Transport Layer Security (TLS) Certificates

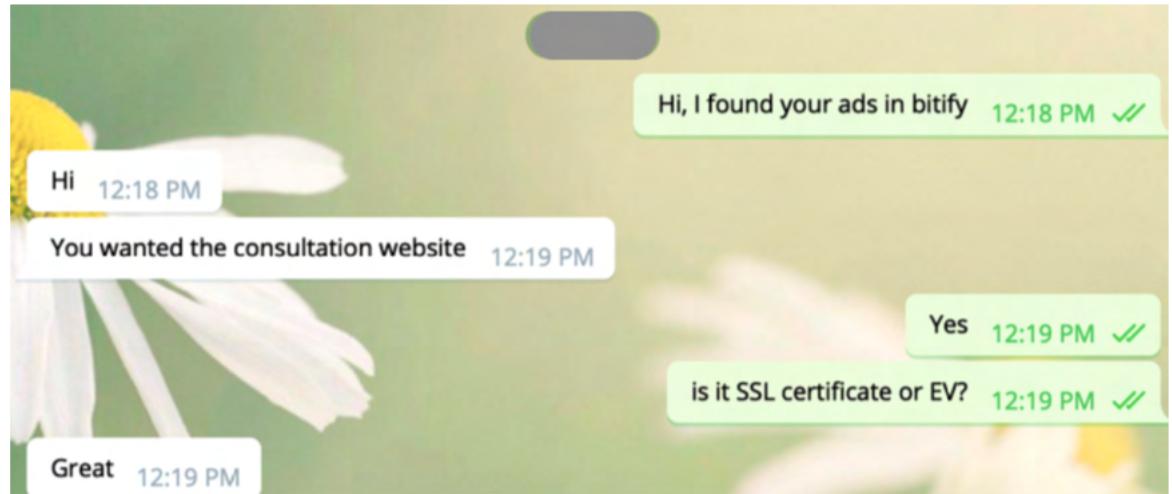


**https://www.**

EV SSL CERT  
ADVERTISED AS  
PART OF WEB  
DESIGN  
SERVICE



# Approaching a Vendor over Telegram



Website  
Designed by  
Darknet Vendor  
and Delivered to  
Research Team

The screenshot shows a website interface with a header bar containing a search bar, a 'Call us:' field, and navigation links for Shopping Cart, My Account, and a shopping cart icon. Below the header is a main banner with a large image of a woman in a dark, layered dress. The banner text reads 'Designer Bags' and 'LATEST COLLECTION'. To the right of the banner are two smaller images: one showing several perfume bottles and another showing a close-up of pink lingerie.

Call us: [REDACTED]

Shopping Cart My Account

CART

Home Lingerie Bags Perfumes Promotions

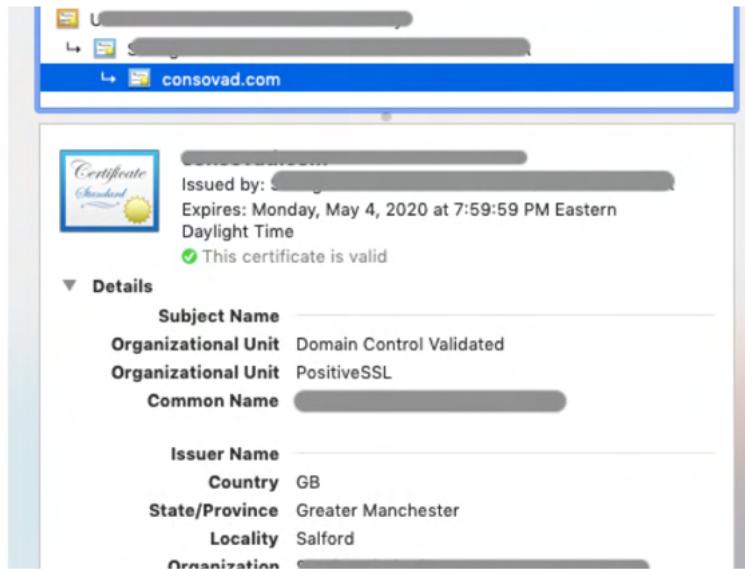
SHOP NOW Contact

Designers

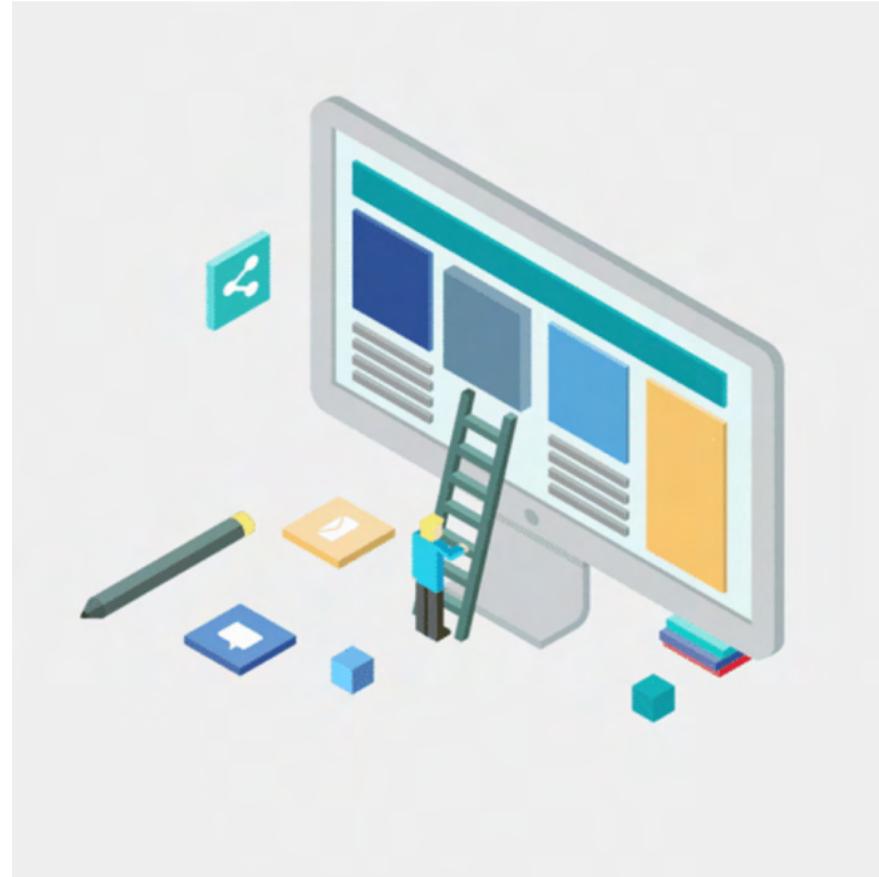
Designer Bags

LATEST COLLECTION

# DV Certificate Installed on the Website Designed by a Darknet Vendor



EV SSL Cert  
Advertised as a  
Standalone  
Service



# Financial Institution





We make it  
easy to get  
your money

Get as much as £5000

[APPLY TODAY WITH OUR SECURE FORM](#)

# Certificates of Incorporation and Registration Documents for a UK Based Financial Institution



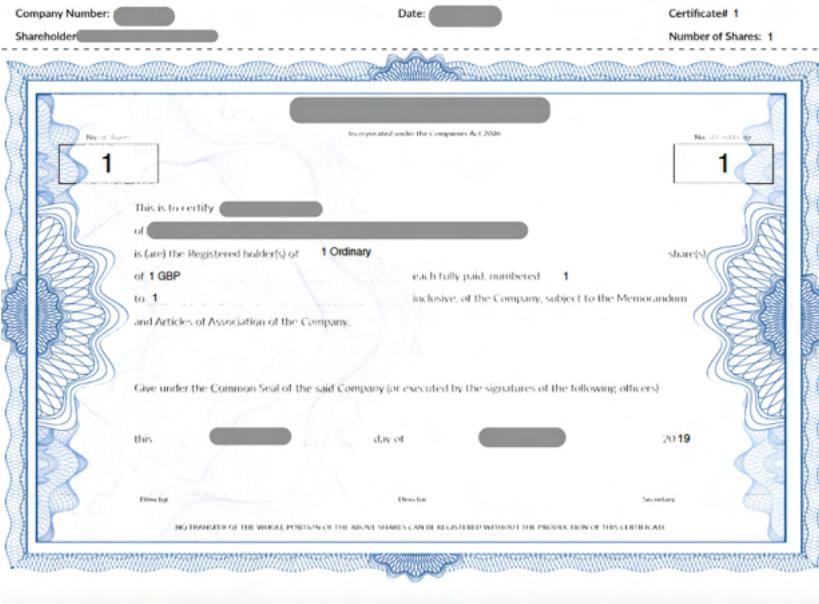
## CERTIFICATE OF INCORPORATION OF A PRIVATE LIMITED COMPANY

Company Number [REDACTED]

The Registrar of Companies for England and Wales, hereby certifies that  
[REDACTED]

is this day incorporated under the Companies Act 2006 as a private company, that the company is limited by shares, and the situation of its registered office is in England and Wales.

Given at Companies House, Cardiff, on [REDACTED]



# Registration of UK Based Financial Institution on Dun and Bradstreet's Website



Perspectives ▾

Solutions ▾

Products ▾

About Us ▾

---



LONDON E11 4HH

GB

Registration No: 1 [redacted]

# Conformation Email from CA for the Receival of an EV Certificate Request to be Installed on a UK Based Financial Institution

From: [REDACTED]  
To: [REDACTED]  
Sent: March 20, 2010 8:00 AM  
Subject: S [REDACTED]: Approve Certificate Request for [REDACTED] (Order # [REDACTED])  
Hello,

We've received a [REDACTED] certificate request for [REDACTED]

Order info:

Domain name: [REDACTED]

Order number: 10500455

Ordered on: 2010-03-20

Contact: Norman Wilson [normin@borezovs.com](mailto:normin@borezovs.com)

Certificate type: EV

Organization name: BOREZOVYS RESTAURANT LIMITED

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

DS

Reply-To: [REDACTED]

---

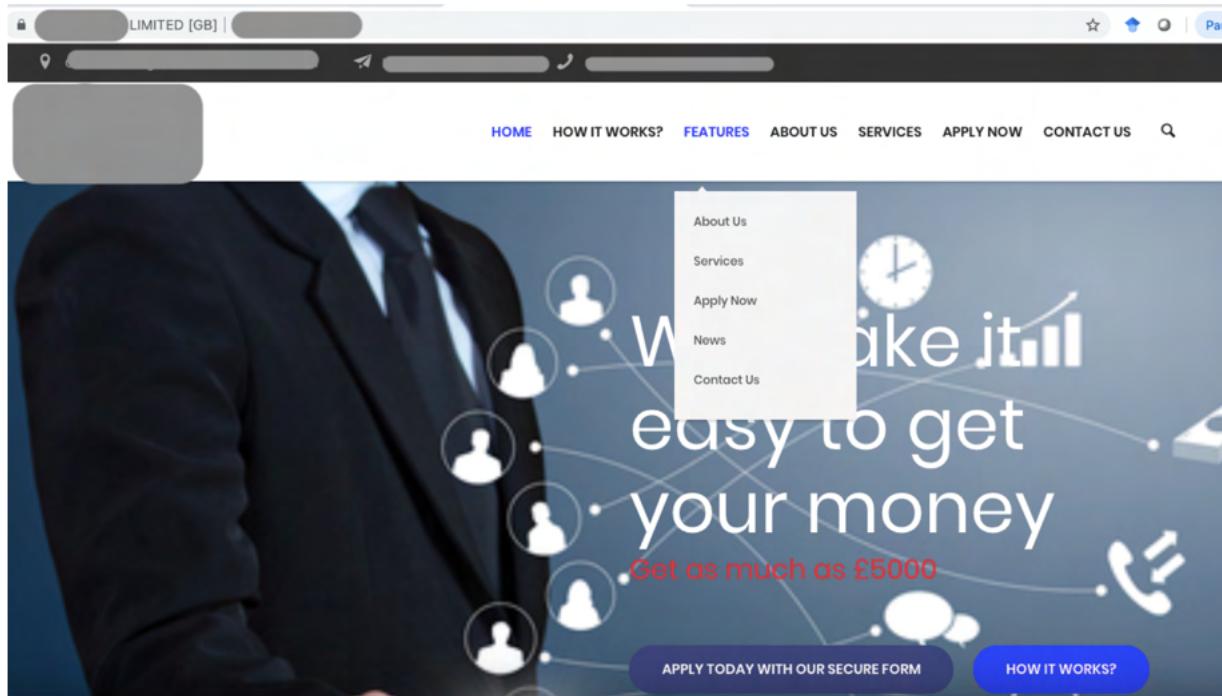
Dear [REDACTED],

Your certificate for [REDACTED] has been issued. It is attached in a ZIP file to this email, and it is also available for download in your account at [REDACTED]

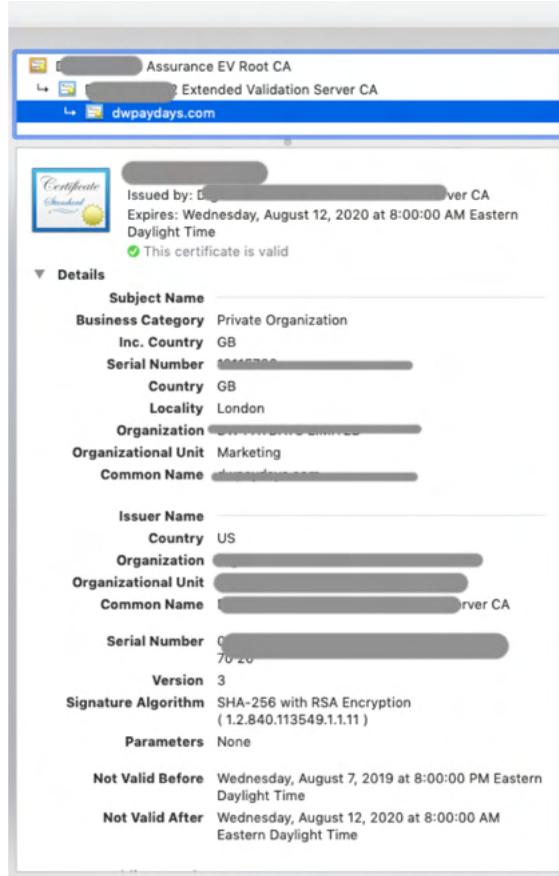
**Where can I find installation instructions?**

---

## UK Based Financial Institution Website Appearance after the Installation of an EV Certificate



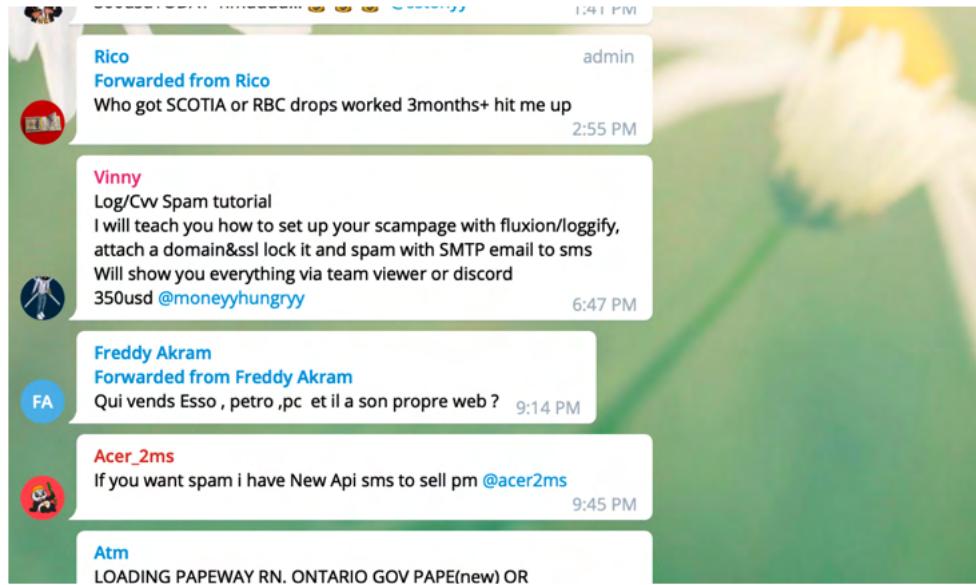
# Details of EV Certificate as Appeared on UK Based Financial Institution Website



# Street View from UK Based Financial Institutions' Address Submitted to CA by Vendor



# Recent Trend



Dedicated  
Channels

# OV vs EV Code Signing Certificate

Understanding the Difference

В наличии есть ОV сертификат с грастом Microsoft SmartScreen.

Т.е. сертификат выполняют одну из главных особенностей EV сертификата (обход SmartScreen по дефолту).  
Перед АВ и всячими сервисами сертификат чист.

Цена - 1500 \$.

Т.к это все же ОV сертификат, то цена ниже чем на EV, но больше чем за обычный ОV.

Обычные ОV сертификаты все так же делаю, актуально.

Цены ниже чем у конкурентов.

В jabber много спама приходит, поэтому **only Telegram**:

@ildmitriy

Оплата: (Bitcoin, Bitcoin Cash, Ethereum Ltc)

(<https://msng.link/o/?ildmitriy=tg>)

↑ Всем доброго времени суток хочу представить вам  
свои услуги ↑

Good day to all who know me and who are not yet!  
I want to introduce you to my services that were not there before!

↑ 17 11:55 PM

В наличии есть несколько EV сертификатов, которые  
хранил долгое время для оптовика, но он временно  
отказался от сертификатов, поэтому продаю их.

There are several EV certificates in stock that I  
kept for a long time for a wholesaler, but he  
temporarily refused certificates, so I sell them.

Цена на 1 сертификат - 3000 \$.

22 edited 11:56 PM

June 2

Global search results

FAKE

ildmitriy [CodeSigning]

@ildmitriy

ildmitriy

@ildmitriy

Есть в наличии как ОV, так и EV сертификаты.

OV and EV certificates are available.

12 edited 1:48 AM

В наличии есть OV сертификат с трастом Microsoft SmartScreen.  
Т.е. сертификат выполняют одну из главных особенностей сертификата (обход SmartScreen по дефолту).  
Перед AB и всякими сервисами сертификат чист.

Цена - 1500 \$.  
Т.к это все же OV сертификат, то цена ниже чем на EV, но больше чем за обычный OV.

Обычные OV сертификаты все так же делаю, актуально.  
Цены ниже чем у конкурентов.

В jabber много спама приходит, поэтому **only Telegram**:  
[@ildmitriy](https://t.me/ildmitriy)

Оплата: ([Bitcoin](#), [Bitcoin Cash](#), [Ethereum Ltc](#))

<https://msng.link/o/?ildmltriy=tg>

Всем доброго времени суток хочу представить вам  
свои услуги

Good day to all who know me and who are not yet!  
want to introduce you to my services that were not there before

## Translation

- OV certificate with Microsoft SmartScreen trust is available. Those certificates fulfill one of the main features of an EV certificate (bypassing SmartScreen by default). Before AB and all sorts of services, the certificate is clean. Price - \$ 1500. Since this is still an OV certificate, the price is lower than for EV, but more than for a regular OV. I still do the usual OV certificates, it's up to date. Prices are lower than those of competitors. Jabber receives a lot of spam, so only Telegram: [@ildmitriy](https://t.me/ildmitriy)

# Customers' Reviews

-TMT-

байт



Платная регистрация

● 0

18 публикаций

Регистрация

21.05.2019 (ID: 93 034)

Деятельность

хакинг / hacking

good certificates  
honest seller  
worked without a guarantor  
recommend

Опубликовано: 26 января

хорошие серты  
честный селлер  
сработали без гаранта  
рекомендую



Цитата

⌚ 12 11:51 PM

learnfast123

байт



Пользователь  
● 0  
18 публикаций  
Регистрация  
04.01.2016 (ID: 66 368)  
Деятельность  
другое / other



Опубликовано: 11 июля 2020

wow its cool, i really like to get one for my new project



Цитата

f13rk3n

байт



Платная регистрация  
● 0  
3 публикации  
Регистрация  
19.02.2020 (ID: 100 610)  
Деятельность  
хакинг / hacking



Опубликовано: 30 июля 2020

I bought a certificate, got it shortly afterwards.  
everything is good)



Цитата



⌚ 11 11:49 PM

# Guide Policy





# Guide Policy Development and Guardians' Efforts

- A more proactive approach for cyber-security is desired by defenders
  - Prevent novice hackers' initiation into a criminal life course trajectory
  - Collection and production of strategic cyber-intelligence, which could lead to termination of cyber-attacks before they occur

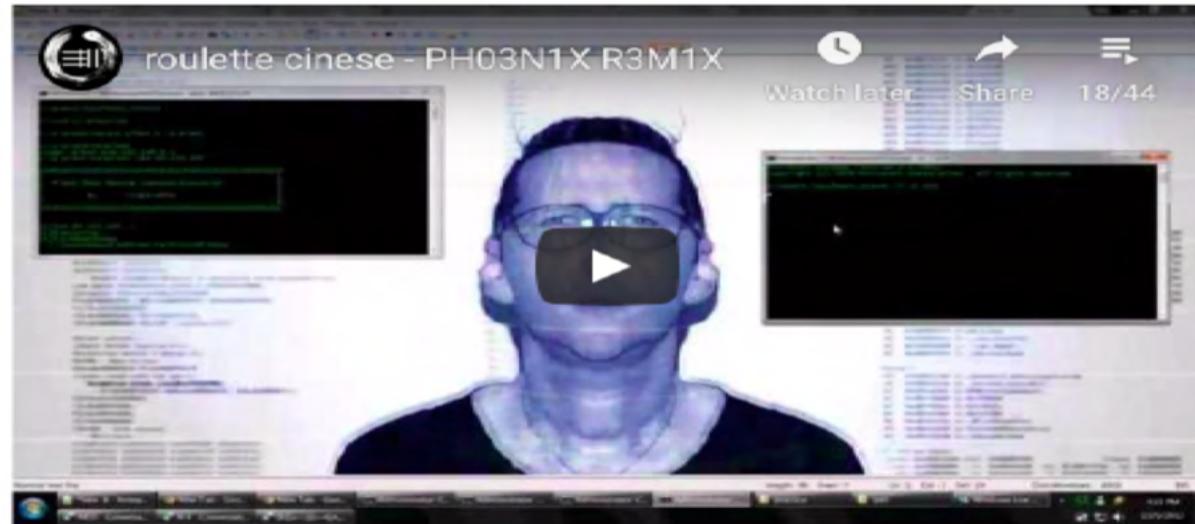


## Dedicated to all the hackers - Pho3nix (Roulette Cinese)

24/03/2014 Written by Roberto SyS64738 Preatoni

We finally concluded the Hacker Visual Contest through which we collected videoclips and artwork from the hacker world which we used to assemble the official videoclip for the song "Pho3nix" (Roulette Cinese) dedicated to the hacker world. I feel obliged to thank all of the participants, credits are added at the end of the clip with a special mention to Christian Milani for the outstanding remix, to Roberto "SyS64738" Preatoni for promoting the idea throughout the hacker world and to Gianluca Zenone aka Alex Dreiser for the videoclip realization. Thanks again to all of you and... enjoy the clip.

Joe Raggi (Roulette Cinese)  
(for what is worth: <https://itunes.apple.com/it/artist/roulette-cinese/id286575097>)



[Read more](#)

## The Virtual Graffiti Project

03/02/2014 Written by Todd Hopkins

## ZONE-H In Numbers

News: **4.738**

Admins: **4**

Registered Users: **147.795**

Early Warning subscriptions: **7570**

Digital Attacks: **13.822.723**

Attacks On Hold: **363.821**

Online Users: **90**

## Login

Login :

Password :

[Sign on](#) [Lost password ?](#)

## Events

< August 2019 >

M	T	W	T	F	S	S
				1	2	3
5	6	7	8	9	10	11
12	13	14	15	16	17	18
<b>19</b>	20	21	22	23	24	25
26	27	28	29	30	31	

[\[ENABLE FILTERS\]](#)

Total notifications: 229,437 of which 91,442 single ip and 137,995 mass

## Legend:

H - Homepage defacement

M - Mass defacement (click to view all defacements of this IP)

R - Redefacement (click to view all defacements of this site)

L - IP address location

★ - Special defacement (special defacements are important websites)

Date	Notifier	H	M	R	L	★ Domain
2017/09/03	./VOTR			R		★ sipp.pacitank
2017/09/03	Santi boy	H				★ www.difatiza
2017/09/03	chinafans					★ lpasme.gob.v
2017/09/03	TUNOVATO	H				★ www.chavim
2017/09/03	Santi boy	H	M	R		★ www.munita
2017/09/03	Santi boy	H	R			★ www.munibellavistajaen.gob.pe
2017/09/02	Shade			R		★ pn-tebingtinggl.go.id/sh.txt
2017/09/02	TeaM_CC	H	M	R		★ ebanoslp.gob.mx
2017/09/02	Moroccan Revolution		M			★ salecliviche.comune.talamona.so...
2017/09/02	Moroccan Revolution		M			★ percorsoarcheologico.comune.br...
2017/09/02	Dr.S4mom			R		★ www.ltarema.ce.gov.br/404.php
2017/09/01	Cyb3r-Shla		M	R		★ sooko.ponorogo.go.id/IQ.htm
2017/09/01	Cyb3r-Shla		M	R		★ sukorejo.ponorogo.go.id/IQ.htm
2017/09/01	Cyb3r-Shla		M	R		★ umum.ponorogo.go.id/IQ.htm
2017/09/01	Cyb3r-Shla			R		★ slahung.ponorogo.go.id/IQ.htm
2017/09/01	Cooldsec	H	M	R		★ camarahidrolandia.ce.gov.br

zone-h  
concentrated information

Home News Events Archive Archive II OnHold Notify Stats Register Login Search...

Mirror saved on: 2017-10-25 20:23:15  
Notified by: ErrOr SquaD Domain: http://www.maechangmu.go.th/index.html  
System: Win 2012 Web server: IIS/8.5  
This is a CACHE (mirror) page of the site when it was saved by our robot on 2017-10-25 20:23:15

IP address: 119.59.122.46  
[Other sites](#)

Hacked By Legion BOmb3r  
Bangladeshi Hacker Arrived  
Security is just an illusion to us Cause We are Unbeatable  
We are ErrOr SquaD

Just because we are silent and we don't react  
doesn't mean We didn't notice

Contact @Legion BOmb3r

Home News Events Archive Archive II OnHold Notify Stats Register Login Disclaimer Contact  
Attribution-NonCommercial-NoDerivs 3.0 Unported License



# Collection of OSINT from Social Media Platforms

[ENABLE FILTERS]

Total notifications: 229,437 of which 91,442 single ip and 137,995 mass defacements

Legend:

H - Homepage defacement

M - Mass defacement (click to view all defacements of this IP)

R - Redefacement (click to view all defacements of this site)

L - IP address location

★ - Special defacement (special defacements are important websites)

Date	Notifier	H M R L ★ Domain	OS	View
2017/09/03	NOTD	R ★ sipp.pacitankab.go.id/root.html	Linux	mirror
2017/09/03	Sandi boy	H ★ www.difatizapan.gob.mx	Linux	mirror
2017/09/03	chinfrans	R ★ www.pasme.gob.pe/o.htm	Unknown	mirror
2017/09/03	TUNOVATO	H ★ www.chavimochic.gob.pe	Win 2003	mirror
2017/09/03	Santi boy	H M R ★ www.munitabaconas.gob.pe	Linux	mirror
2017/09/03	Santi boy	H R ★ www.munibellavistajaen.gob.pe	Linux	mirror
2017/09/02	Shade	R ★ pn-tebingtinggi.go.id/sh.txt	Linux	mirror
2017/09/02	TeaM_CC	H M R ★ ebansip.gob.mx	Linux	mirror
2017/09/02	Moroccan Revolution	M ★ www.salciviche.comune.talamona.so...	Linux	mirror
2017/09/02	Moroccan Revolution	M ★ www.corporoarqueologico.comune.br...	Linux	mirror
2017/09/02	Dr.S4mom	R ★ www.tarema.ce.gov.br/404.php	Linux	mirror
2017/09/01	Cyb3r-Shia	M R ★ suko.ponorogo.go.id/IQ.htm	Linux	mirror
2017/09/01	Cyb3r-Shia	M R ★ sukorejo.ponorogo.go.id/IQ.htm	Linux	mirror
2017/09/01	Cyb3r-Shia	M R ★ umum.ponorogo.go.id/IQ.htm	Linux	mirror
2017/09/01	Cyb3r-Shia	R ★ slahung.ponorogo.go.id/IQ.htm	Linux	mirror
2017/09/01	Coldsec	H M R ★ camarahidrolandia.ce.gov.br	Linux	mirror

The screenshot shows a Facebook page for 'Santi Boy' (@santiboy.official). The page has 30 likes and 32 people following it. A post on the timeline features two men wearing yellow hard hats and safety vests, smiling. The caption of the post reads: "ciente, cómoda y segura". Below the post, there are links to 'Movilidad Futura SAS - Sistema estratégico de Transporte público de Pasajeros de Popayán' and 'Movilidad Futura SAS - Sistema de Transporte público de Pasajeros'. The post has 1 like, 0 comments, and 0 shares. The status bar at the bottom of the page indicates: 'April 29 · 4h · Municipalidad de Potosí · Municipio de Potosí · 2001.htm · Police National of Peru · Perú · La Municipalidad Provincial de Atalaya · https://www.munipatalaya.gob.pe · 2017/09/03 · http://www.zone-h.org/mirrorid/31125472 · http://www.zone-h.org/mirrorid/31098722 · http://www.zone-h.org/mirrorid/31098728 · Rest of the server · http://www.zone-h.org/archive/ip=144.217.188.133 · See Translation'. The image below the post shows a close-up of a person's face, possibly a victim or a related image.

# Intelligence and Disruption

---

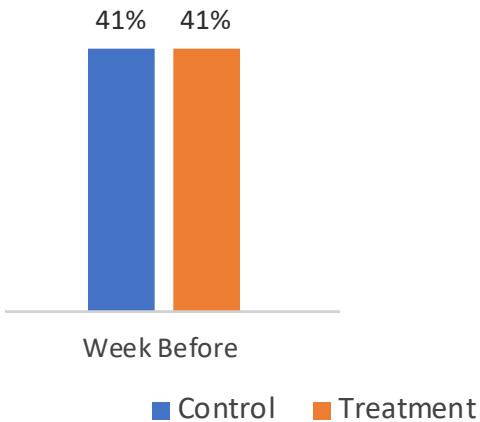


Jakarta Paranoid

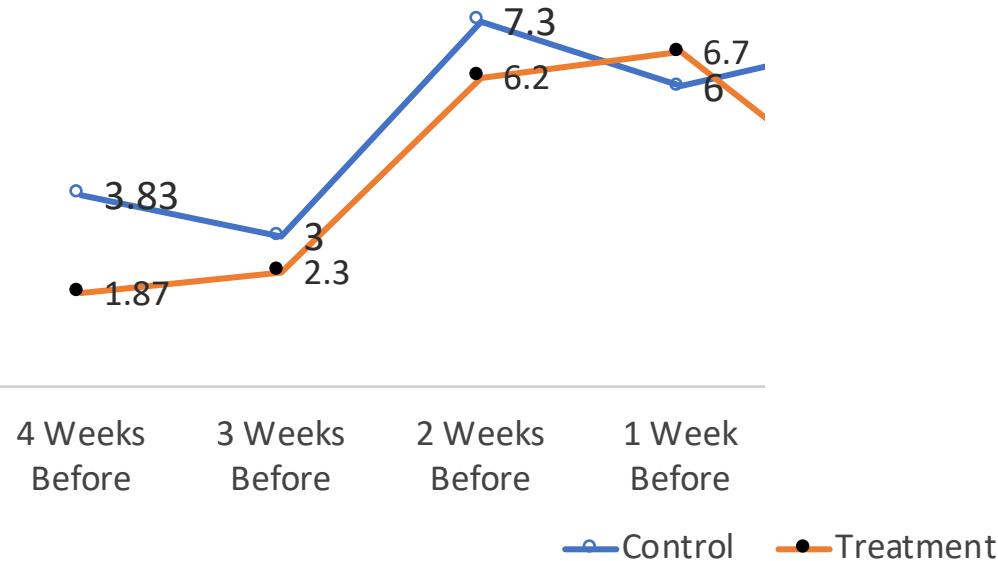


Jakarta Paranoid wanted  
to let u no federal  
authorities raided my  
house with a search  
warrant today(20 agents  
drawn)cause they  
believe I knocked down  
blue-  
[print.com.ar/asu.htm](http://print.com.ar/asu.htm)  
They said punishment  
could range between 1  
to 5 years in prison! U  
may want 2 lay low in  
the next week.

# Proportion of Hackers Reporting Website Defacement the Week and Month Before and After the Administration of Gossip Message over a Private Facebook Channel



## Average Number of Website Defacement Attacks Reported One Month Before and One Month After the Administration of Gossip Message over a Private Facebook Channel



# In conclusion,

We recommend certificate authorities to embrace an Evidence-Based approach in their effort to deploy security tools and policies in the context of their important work

David Maimon  
Email: [dmaimon@gsu.edu](mailto:dmaimon@gsu.edu)  
Website: [ebcs.gsu.edu](http://ebcs.gsu.edu)  
Twitter: [@david\\_maimon](https://twitter.com/david_maimon)

