Burning the Lookout

> whoami

- Senior Security Researcher @ CrowdStrike
- Project Director / Intern @ MalShare
- Project Director @ Project 25499

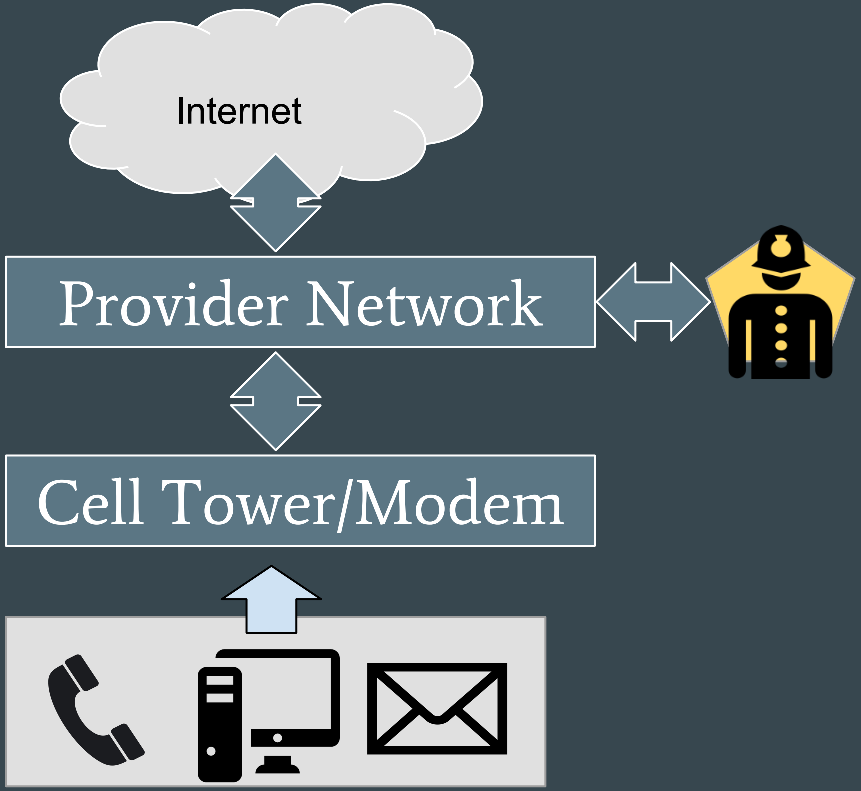
- Twitter: @SilasCutler
- Email: silascutler@riseup.net

Crash course in Lawful Intercept

Crash course on Lawful Intercept

- Process, Tools, Ability for Law Enforcement to collect as part of investigations (*wiretaps*)
  - CALEA (Communications Assistance for Law Enforcement Act)
  - ESTI (European Telecommunications Standards Institute)

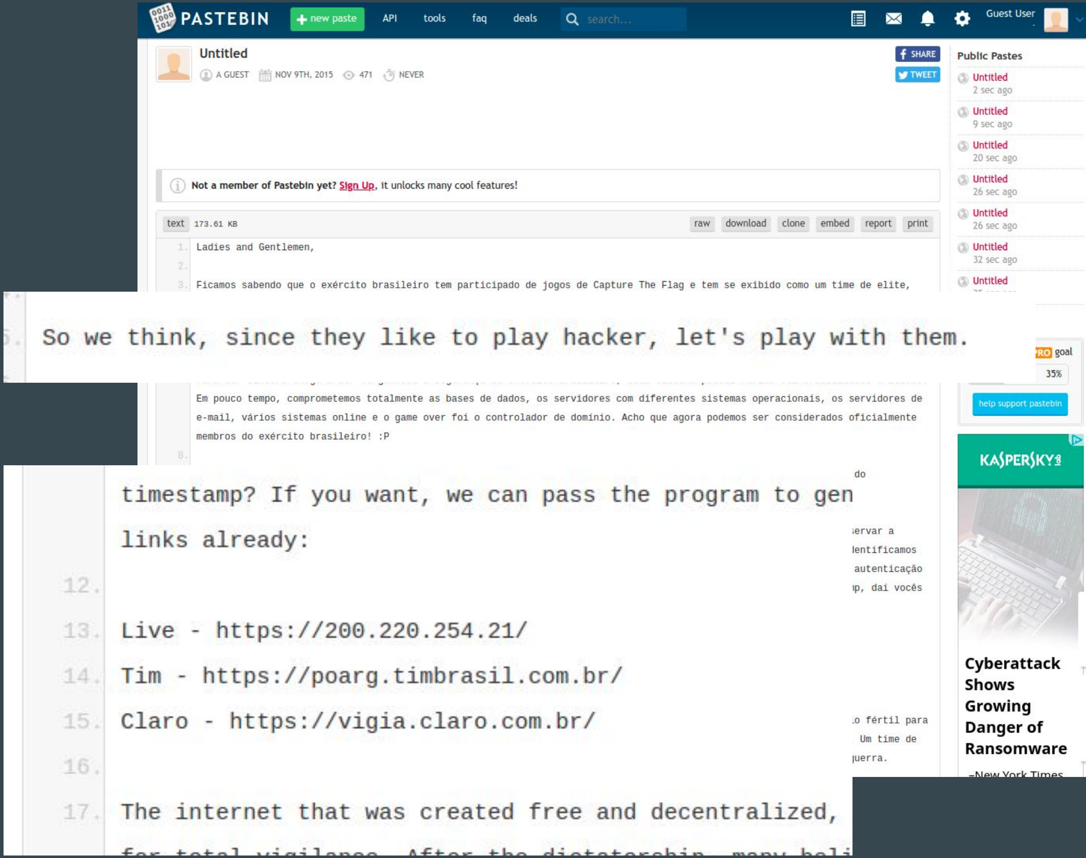
- Standard deployment
  - Intercept Access Point (IAP)
  - Mediation Device
  - Lawful Intercept Administration (LIA)



Vigia

Backstory

- Pastebin 2015
- Poster claimed to have hacked Brazilian Army after they did a CTF
- Post included:
  - 7000 Credentials
  - 3 Websites



Untitled

A GUEST NOV 9TH, 2015 471 NEVER

Not a member of Pastebin yet? Sign Up, it unlocks many cool features!

text 173.61 KB

```
Ladies and Gentlemen,

Ficamos sabendo que o exército brasileiro tem participado de jogos de Capture The Flag e tem se exibido como um time de elite,
```

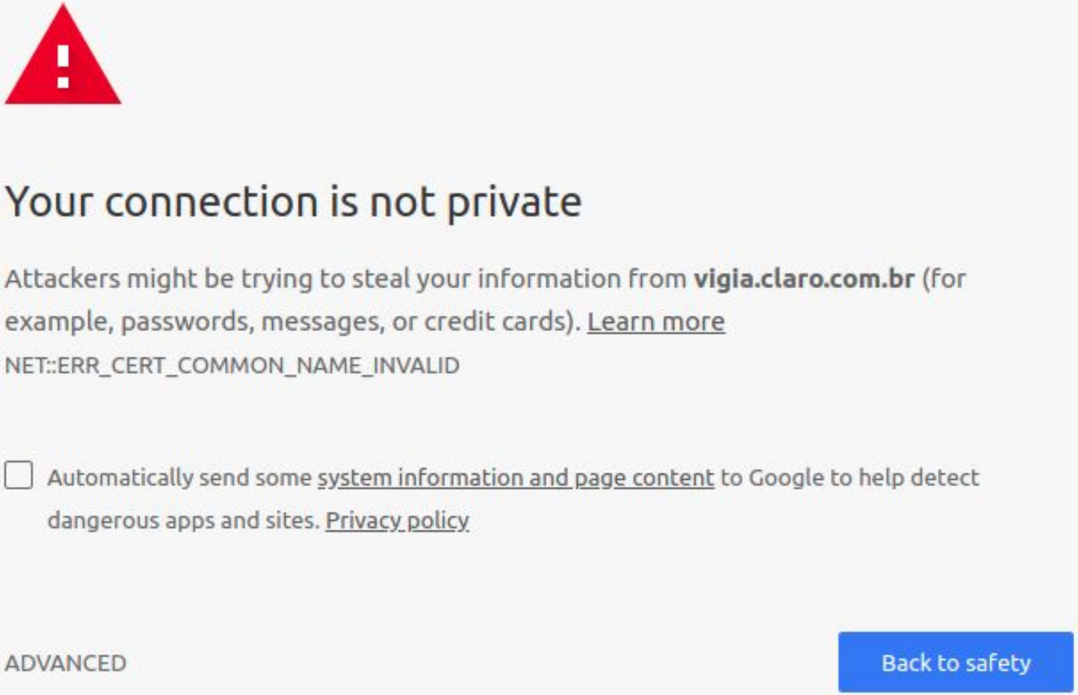
```
So we think, since they like to play hacker, let's play with them.
```

```
Em pouco tempo, comprometemos totalmente as bases de dados, os servidores com diferentes sistemas operacionais, os servidores de
e-mail, vários sistemas online e o game over foi o controlador de dominio. Acho que agora podemos ser considerados oficialmente
membros do exército brasileiro! :P
```

```
timestamp? If you want, we can pass the program to gen
links already:

Live - https://200.220.254.21/
Tim - https://poarg.timbrasil.com.br/
Claro - https://vigia.claro.com.br/

The internet that was created free and decentralized,
```

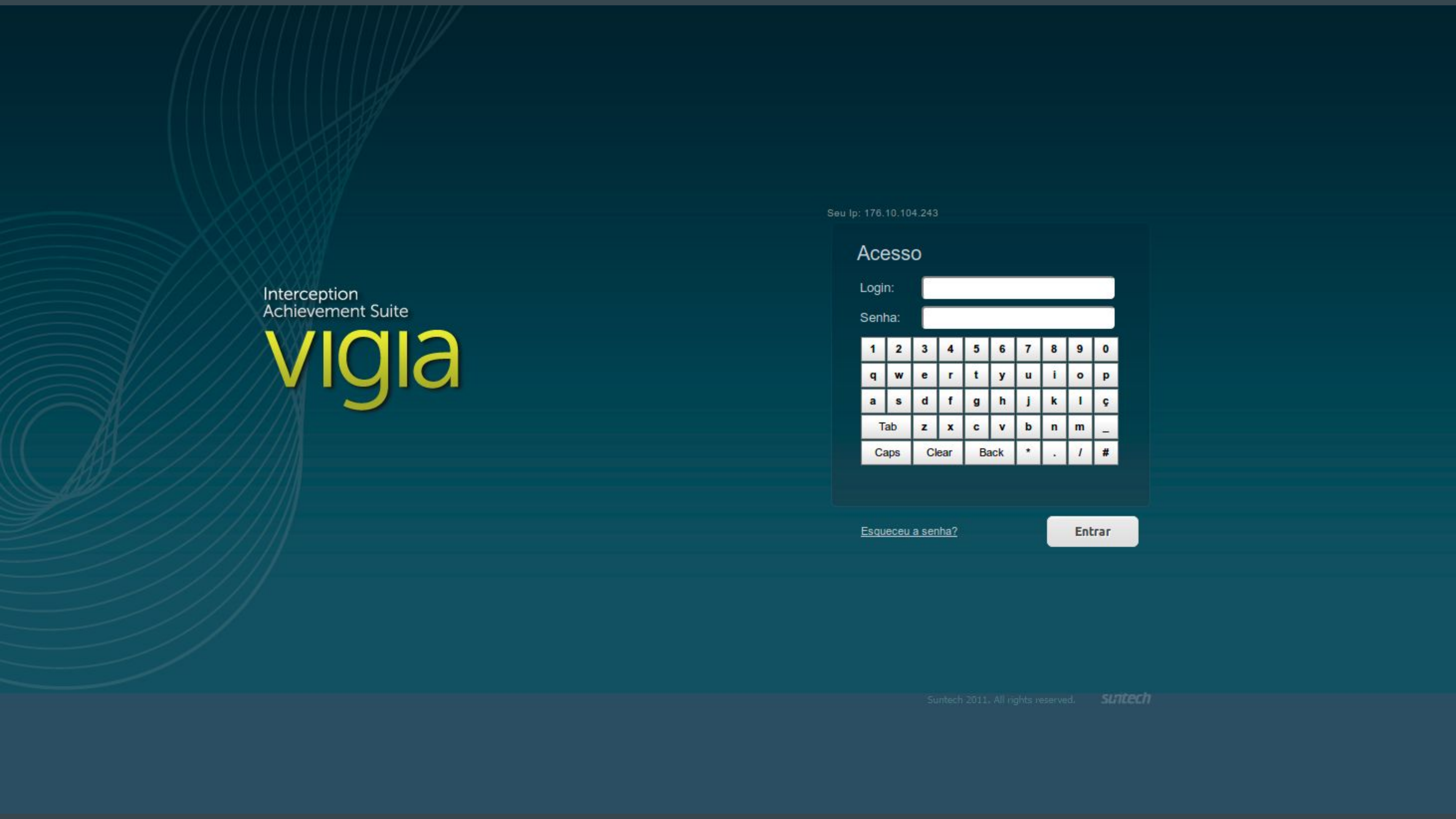


Your connection is not private

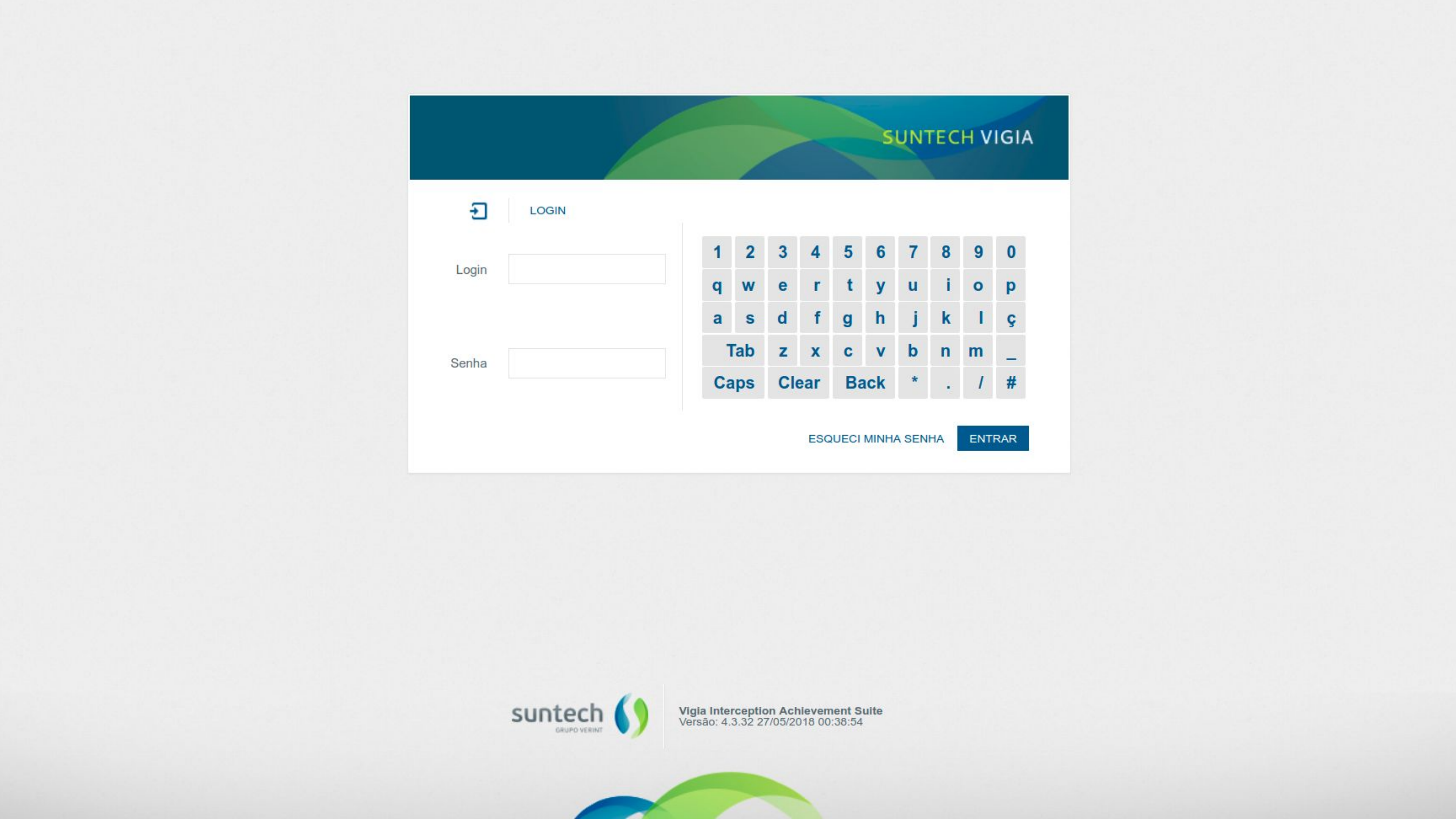
Attackers might be trying to steal your information from **vigia.claro.com.br** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_COMMON_NAME_INVALID

□ Automatically send some system information and page content to Google to help detect dangerous apps and sites. Privacy policy



Seu Ip: 176.10.104.243



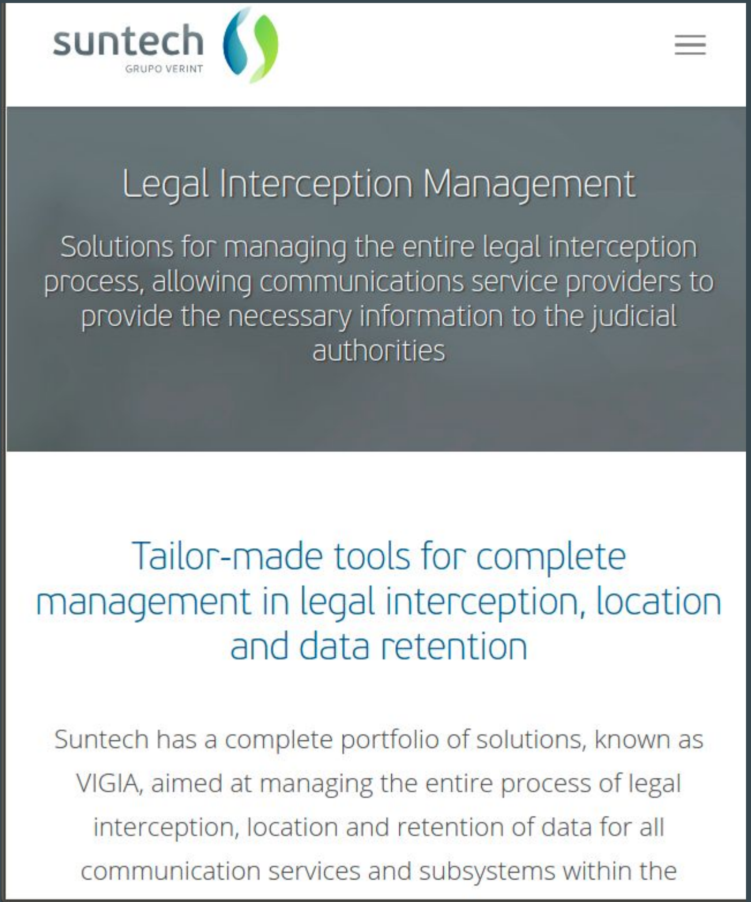
Vigia Interception Achievement Suite
Versão: 4.3.32 27/05/2018 00:38:54

Vigia

- *Lawful Intercept Suite* developed by SunTech Brazil

- (Mediation Device)
    - View intercepted data from service providers
    - Add new surveillance targets

- Where's it used?



Legal Interception Management

Solutions for managing the entire legal interception process, allowing communications service providers to provide the necessary information to the judicial authorities

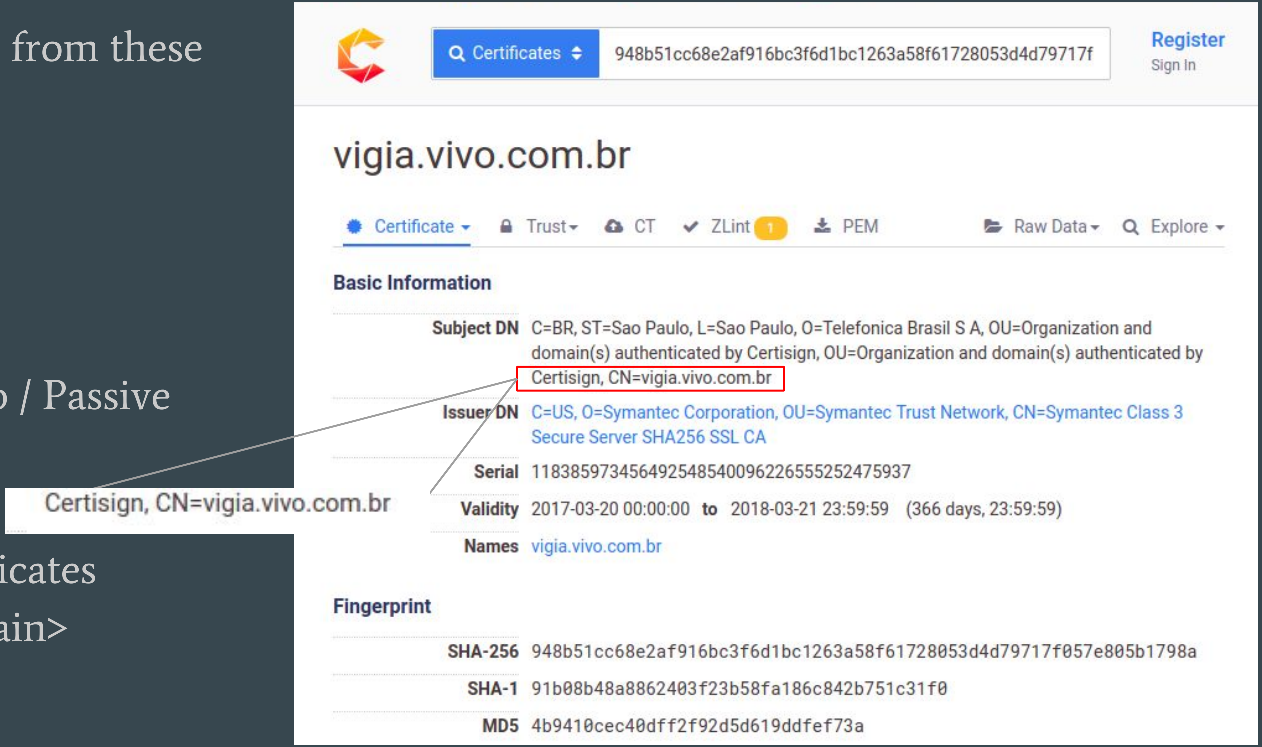
Tailor-made tools for complete management in legal interception, location and data retention

Suntech has a complete portfolio of solutions, known as VIGIA, aimed at managing the entire process of legal interception, location and retention of data for all communication services and subsystems within the

Hunting for Vigia

- What are distinct artifacts from these systems?
    - SSL
    - DNS
    - Page Content

- Censys / Shodan / Scans.io / Passive DNS for static patterns
    - /vigia/ or /suntech/ present in SSL certificates
    - vigia.<provider domain>



vigia.vivo.com.br

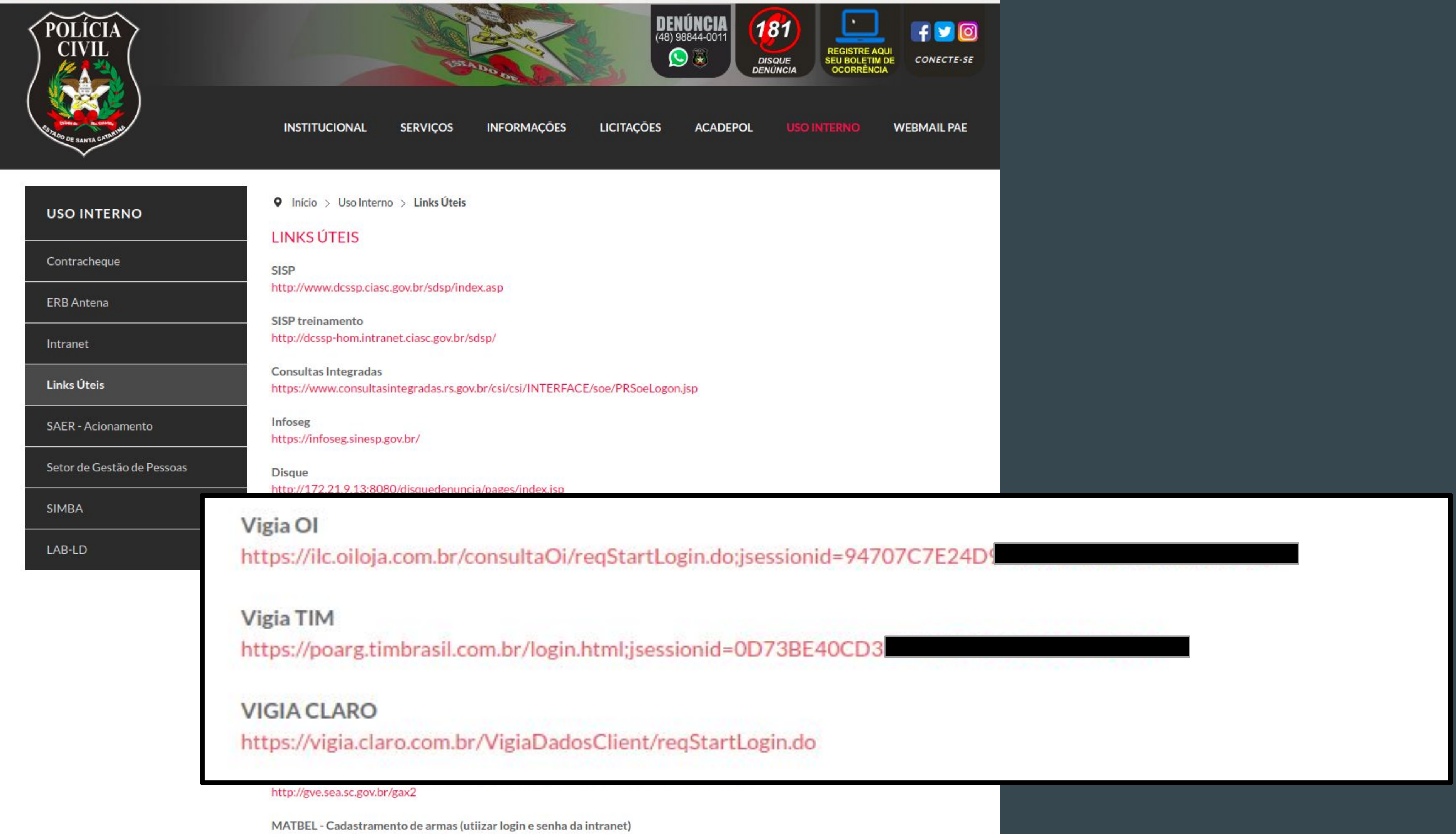
Basic Information

Subject DN	C=BR, ST=Sao Paulo, L=Sao Paulo, O=Telefonica Brasil S A, OU=Organization and domain(s) authenticated by Certisign, OU=Organization and domain(s) authenticated by Certisign, CN=vigia.vivo.com.br
Issuer DN	C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 Secure Server SHA256 SSL CA
Serial	118385973456492548540096226555252475937
Validity	2017-03-20 00:00:00 **to** 2018-03-21 23:59:59 (366 days, 23:59:59)
Names	vigia.vivo.com.br

Fingerprint

SHA-256	948b51cc68e2af916bc3f6d1bc1263a58f61728053d4d79717f057e805b1798a
SHA-1	91b08b48a8862403f23b58fa186c842b751c31f0
MD5	4b9410cec40dff2f92d5d619ddfef73a

Certisign, CN=vigia.vivo.com.br



LINKS ÚTEIS

SISP
http://www.dcssp.ciasc.gov.br/sdsp/index.asp

SISP treinamento
http://dcssp-hom.intranet.ciasc.gov.br/sdsp/

Consultas Integradas
https://www.consultasintegradas.rs.gov.br/csi/csi/INTERFACE/soe/PRSoeLogon.jsp

Infoseg
https://infoseg.sinesp.gov.br/

Disque
http://172.21.9.13:8080/disquedenuncia/pages/index.jsp

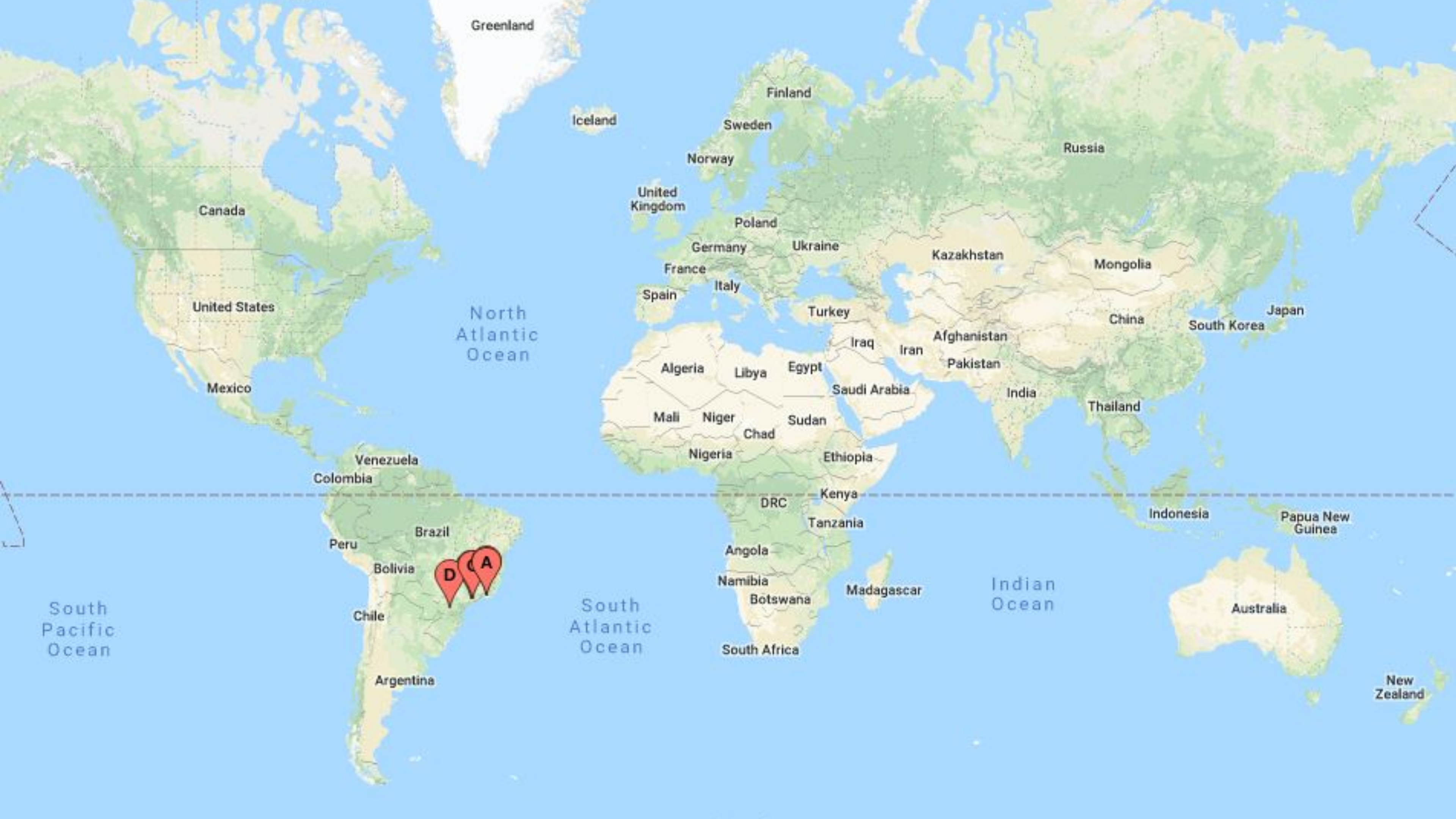
Vigia OI
https://ilc.oiloja.com.br/consultaOi/reqStartLogin.do;jsessionid=94707C7E24D[redacted]

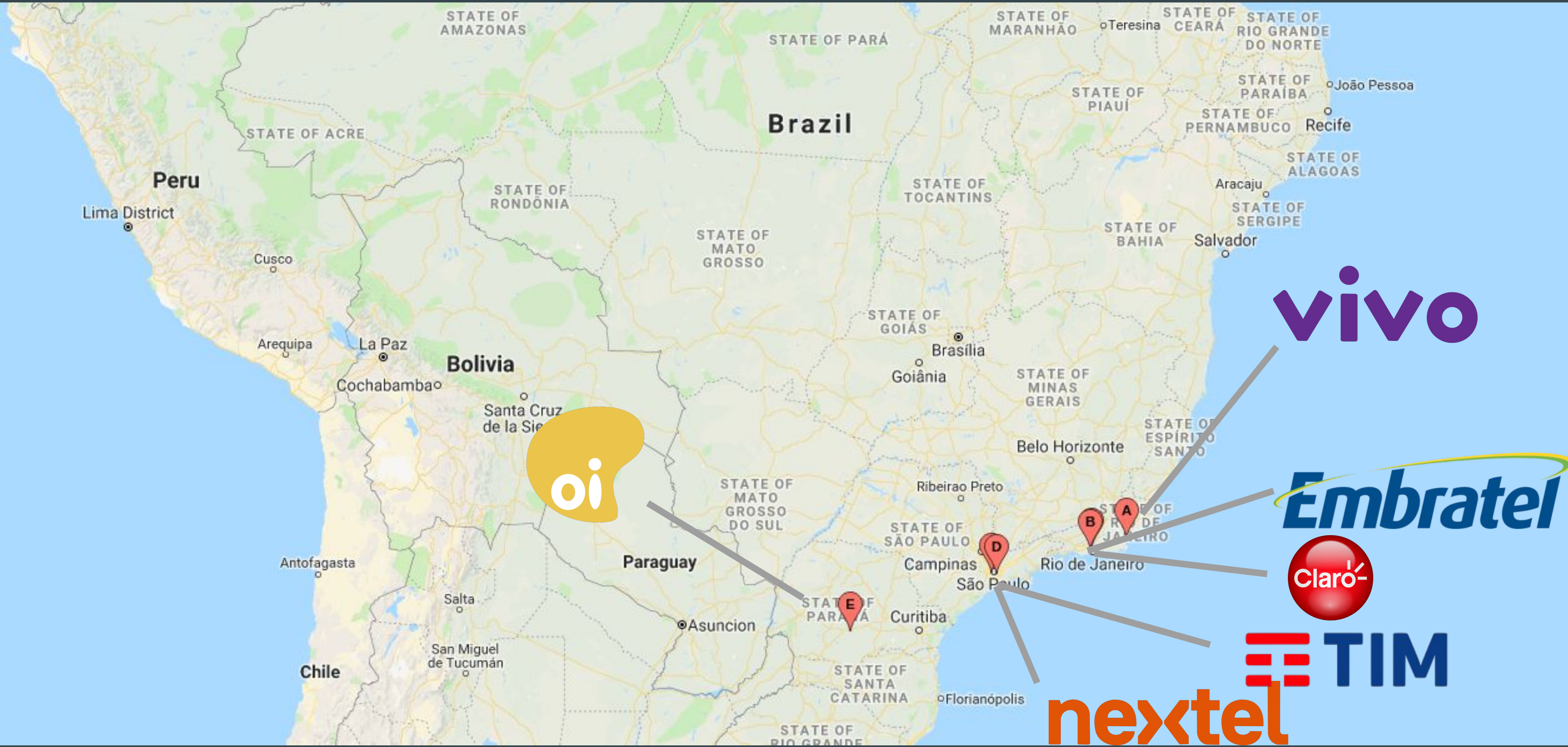
Vigia TIM
https://poarg.timbrasil.com.br/login.html;jsessionid=0D73BE40CD3[redacted]

VIGIA CLARO
https://vigia.claro.com.br/VigiaDadosClient/reqStartLogin.do

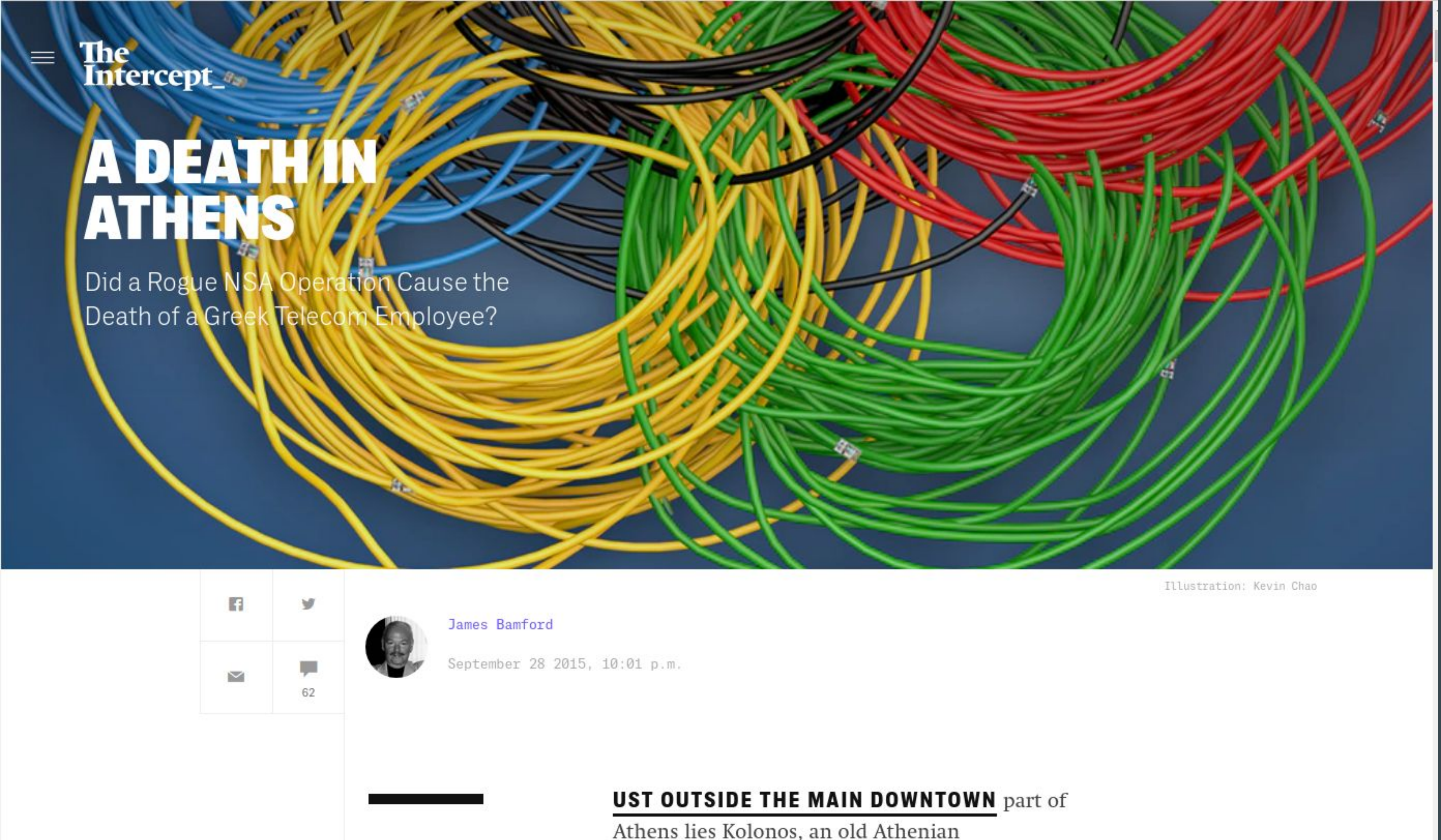
http://gve.sea.sc.gov.br/gax2

MATBEL - Cadastramento de armas (utiizar login e senha da intranet)


Greenland
Iceland
Finland
Sweden
Norway
Russia
United Kingdom
Poland
Canada
Germany
Ukraine
Kazakhstan
Mongolia
France
Italy
Spain
United States
North Atlantic Ocean
Turkey
China
South Korea
Japan
Iraq
Afghanistan
Iran
Pakistan
Algeria
Libya
Egypt
Mexico
Saudi Arabia
India
Thailand
Mali
Niger
Sudan
Chad
Nigeria
Ethiopia
Venezuela
Colombia
Kenya
DRC
Indonesia
Papua New Guinea
Tanzania
Brazil
Peru
Angola
Bolivia
D
A
Namibia
Madagascar
Indian Ocean
Botswana
South Pacific Ocean
Chile
South Atlantic Ocean
Australia
South Africa
Argentina
New Zealand


STATE OF AMAZONAS
STATE OF PARÁ
STATE OF MARANHÃO
Teresina
STATE OF CEARÁ
STATE OF RIO GRANDE DO NORTE
STATE OF PARAÍBA
João Pessoa
STATE OF PIAUÍ
STATE OF PERNAMBUCO
Recife
Brazil
STATE OF ACRE
Peru
Lima District
STATE OF RONDÔNIA
STATE OF TOCANTINS
STATE OF ALAGOAS
Aracaju
STATE OF SERGIPE
STATE OF BAHIA
Salvador
STATE OF MATO GROSSO
Cusco
STATE OF GOIÁS
Brasília
Goiânia
Arequipa
La Paz
Bolivia
Cochabamba
Santa Cruz de la Sie
STATE OF MINAS GERAIS
STATE OF ESPÍRITO SANTO
Belo Horizonte
oi
vivo
STATE OF MATO GROSSO DO SUL
Ribeirao Preto
Embratel
A
B
STATE OF RIO DE JANEIRO
STATE OF SÃO PAULO
D
Campinas
São Paulo
Rio de Janeiro
Claro
Antofagasta
Paraguay
Salta
STATE OF PARANÁ
E
Curitiba
Asuncion
TIM
San Miguel de Tucumán
Chile
STATE OF SANTA CATARINA
Florianópolis
nextel
STATE OF RIO GRANDE

Why it matters



The Intercept_

A DEATH IN ATHENS

Did a Rogue NSA Operation Cause the Death of a Greek Telecom Employee?

Illustration: Kevin Chao

James Bamford

September 28 2015, 10:01 p.m.

62

UST OUTSIDE THE MAIN DOWNTOWN part of Athens lies Kolonos, an old Athenian

Why it matters

- Potential for unauthorized eavesdropping
- Previous targeting by foreign and *domestic* attackers
- Likely other similar systems in the wild

211,046,525

Questions

Thank you // Fin