Intsights

DETECT . ANALYZE . REMEDIATE

OSINT: The Secret Weapon in Hunting Nation-State Campaigns

Alon Arvatz

alon@intsights.com

+972-545444313

1

What People Think…

True or False?

Threat intelligence is focused on the “reconnaissance” phase

+

Nation-state actors just sit in a secured place collaborating over internal networks

=

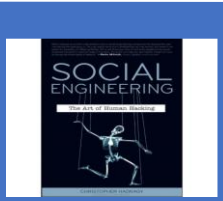
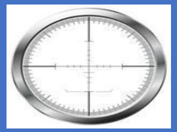
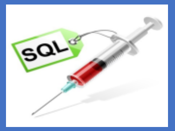
Commercial threat intelligence won’t help me against nation-state attacks

2

Using OSINT to Detect Attacks

How Nation-state Cyber Attacks Unfold?

The Attack Supply Chain

Motive	Targeting	Development	Infrastructure	Recon	Attack
					
		WELCOME TO DARKODE "The best malware marketplace on the net"			

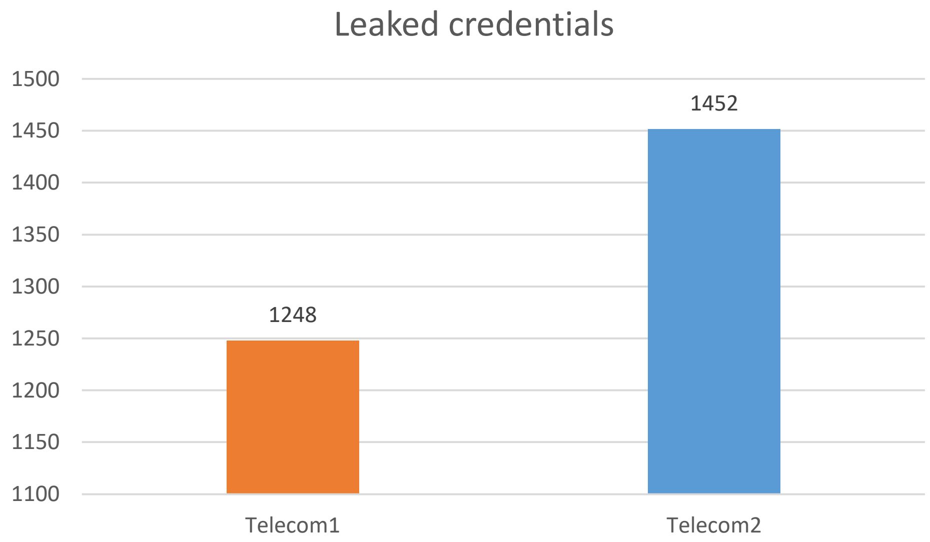
What Does This Mean For You

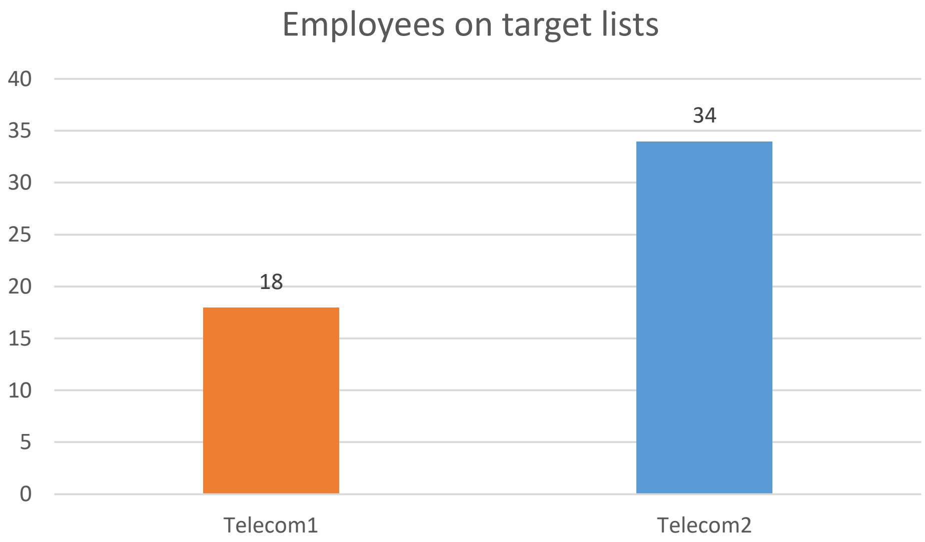
Intsights

Step 1: Outrun Your **Competitor**

- Don’t outrun the bear, outrun your competitor.
- Benchmark your digital footprint.
- Benchmark is a crucial security need!

Benchmark in the telecom industry





Intsights

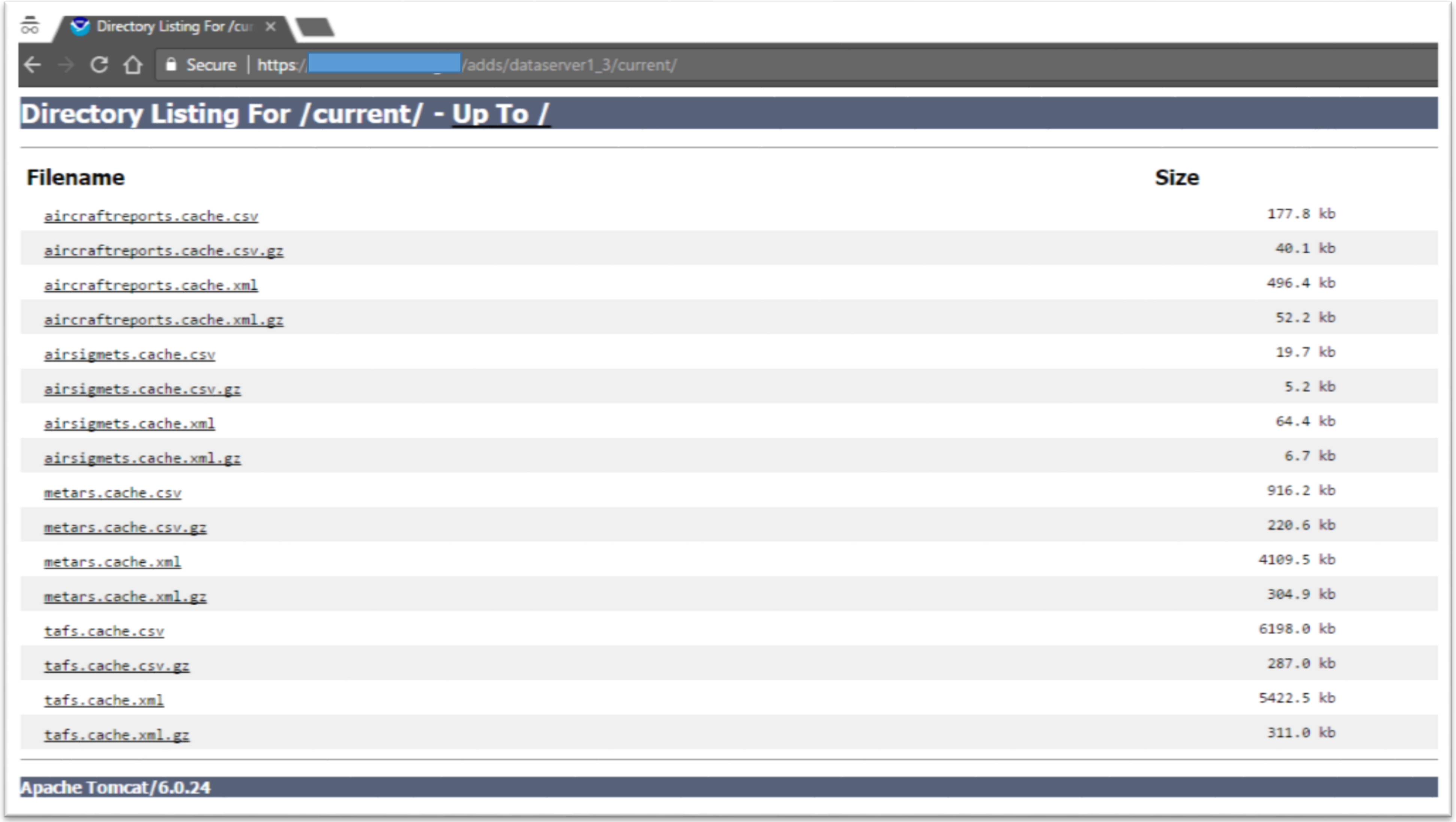
Nation-State Attacks Motivations

- Damage
- Support for Other Efforts
- Intelligence
- Profit (??)

Step 2: Get Into The Attacker's Shoes

- How does your attacker see you?
- What is your digital footprint?
- 2 steps:
  - Monitor your digital foot print.
  - Clean your digital footprint.

Exploitable Data



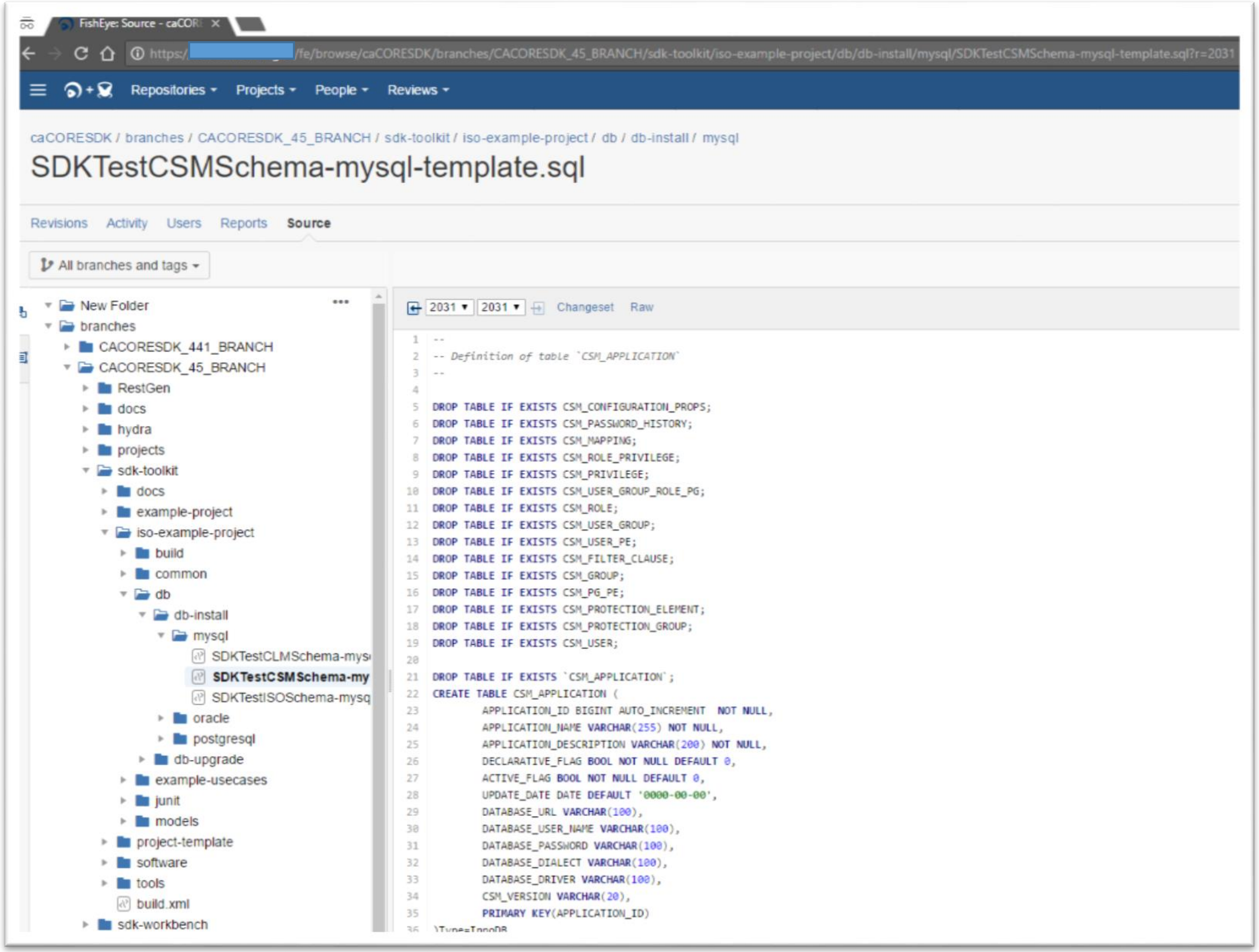
Directory Listing For /cur ×
Secure | https:/[redacted]/adds/dataserver1_3/current/

Directory Listing For /current/ - Up To /

Filename	Size
aircraftreports.cache.csv	177.8 kb
aircraftreports.cache.csv.gz	40.1 kb
aircraftreports.cache.xml	496.4 kb
aircraftreports.cache.xml.gz	52.2 kb
airsigmets.cache.csv	19.7 kb
airsigmets.cache.csv.gz	5.2 kb
airsigmets.cache.xml	64.4 kb
airsigmets.cache.xml.gz	6.7 kb
metars.cache.csv	916.2 kb
metars.cache.csv.gz	220.6 kb
metars.cache.xml	4109.5 kb
metars.cache.xml.gz	304.9 kb
tafs.cache.csv	6198.0 kb
tafs.cache.csv.gz	287.0 kb
tafs.cache.xml	5422.5 kb
tafs.cache.xml.gz	311.0 kb

Apache Tomcat/6.0.24

Exploitable Data



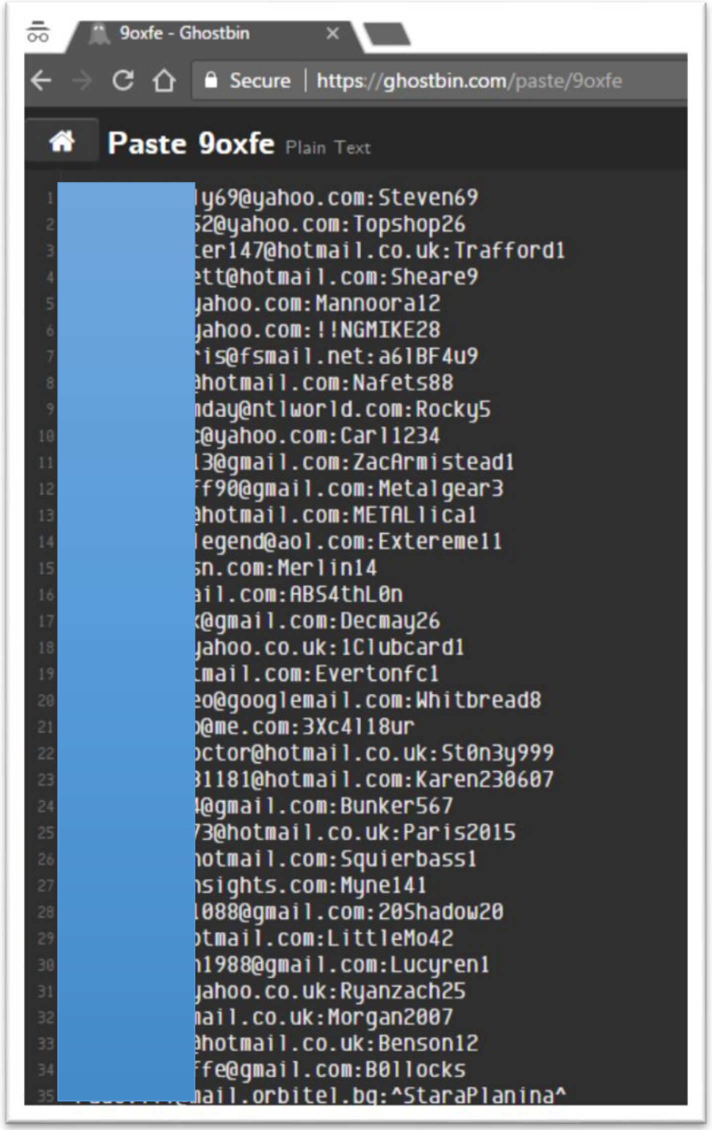
https:/[redacted]/fe/browse/caCORESDK/branches/CACORESDK_45_BRANCH/sdk-toolkit/iso-example-project/db/db-install/mysql/SDKTestCSMSchema-mysql-template.sql?r=2031

caCORESDK / branches / CACORESDK_45_BRANCH / sdk-toolkit / iso-example-project / db / db-install / mysql

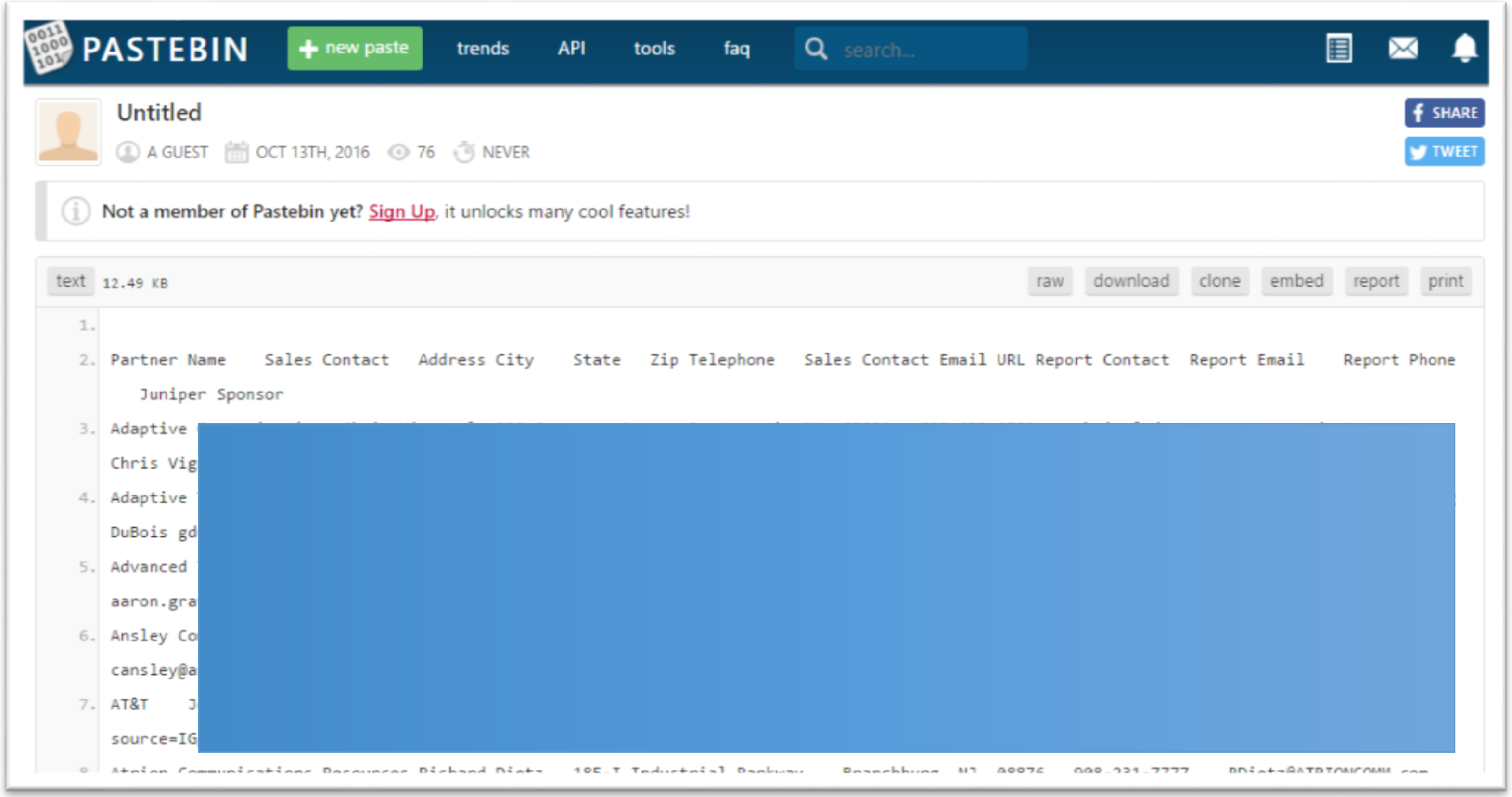
SDKTestCSMSchema-mysql-template.sql

```
--
-- Definition of table `CSM_APPLICATION`
--

DROP TABLE IF EXISTS CSM_CONFIGURATION_PROPS;
DROP TABLE IF EXISTS CSM_PASSWORD_HISTORY;
DROP TABLE IF EXISTS CSM_MAPPING;
DROP TABLE IF EXISTS CSM_ROLE_PRIVILEGE;
DROP TABLE IF EXISTS CSM_PRIVILEGE;
DROP TABLE IF EXISTS CSM_USER_GROUP_ROLE_PG;
DROP TABLE IF EXISTS CSM_ROLE;
DROP TABLE IF EXISTS CSM_USER_GROUP;
DROP TABLE IF EXISTS CSM_USER_PE;
DROP TABLE IF EXISTS CSM_FILTER_CLAUSE;
DROP TABLE IF EXISTS CSM_GROUP;
DROP TABLE IF EXISTS CSM_PG_PE;
DROP TABLE IF EXISTS CSM_PROTECTION_ELEMENT;
DROP TABLE IF EXISTS CSM_PROTECTION_GROUP;
DROP TABLE IF EXISTS CSM_USER;

DROP TABLE IF EXISTS `CSM_APPLICATION`;
CREATE TABLE CSM_APPLICATION (
        APPLICATION_ID BIGINT AUTO_INCREMENT  NOT NULL,
        APPLICATION_NAME VARCHAR(255) NOT NULL,
        APPLICATION_DESCRIPTION VARCHAR(200) NOT NULL,
        DECLARATIVE_FLAG BOOL NOT NULL DEFAULT 0,
        ACTIVE_FLAG BOOL NOT NULL DEFAULT 0,
        UPDATE_DATE DATE DEFAULT '0000-00-00',
        DATABASE_URL VARCHAR(100),
        DATABASE_USER_NAME VARCHAR(100),
        DATABASE_PASSWORD VARCHAR(100),
        DATABASE_DIALECT VARCHAR(100),
        DATABASE_DRIVER VARCHAR(100),
        CSM_VERSION VARCHAR(20),
        PRIMARY KEY(APPLICATION_ID)
)Type=InnoDB
```

Clean Your Digital Footprint



```
[redacted]
ly69@yahoo.com:Steven69
52@yahoo.com:Topshop26
ter147@hotmail.co.uk:Trafford1
ett@hotmail.com:Sheare9
yahoo.com:Mannoora12
yahoo.com:!!NGMIKE28
ris@fsmail.net:a61BF4u9
@hotmail.com:Nafets88
nday@ntlworld.com:Rocky5
c@yahoo.com:Carl1234
13@gmail.com:ZacArmistead1
ff90@gmail.com:Metalgear3
@hotmail.com:METALlical
legend@aol.com:Extereme11
sn.com:Merlin14
ail.com:ABS4thL0n
k@gmail.com:Decmay26
yahoo.co.uk:1Clubcard1
tmail.com:Evertonfc1
eo@googlemail.com:Whitbread8
o@me.com:3Xc4118ur
octor@hotmail.co.uk:St0n3y999
31181@hotmail.com:Karen230607
4@gmail.com:Bunker567
73@hotmail.co.uk:Paris2015
hotmail.com:Squierbass1
nsights.com:Myne141
1088@gmail.com:20Shadow20
otmail.com:LittleMo42
n1988@gmail.com:Lucyren1
yahoo.co.uk:Ryanzach25
mail.co.uk:Morgan2007
@hotmail.co.uk:Benson12
ffe@gmail.com:B0llocks
mail.orbitel.bg:^StaraPlanina^
```



Untitled

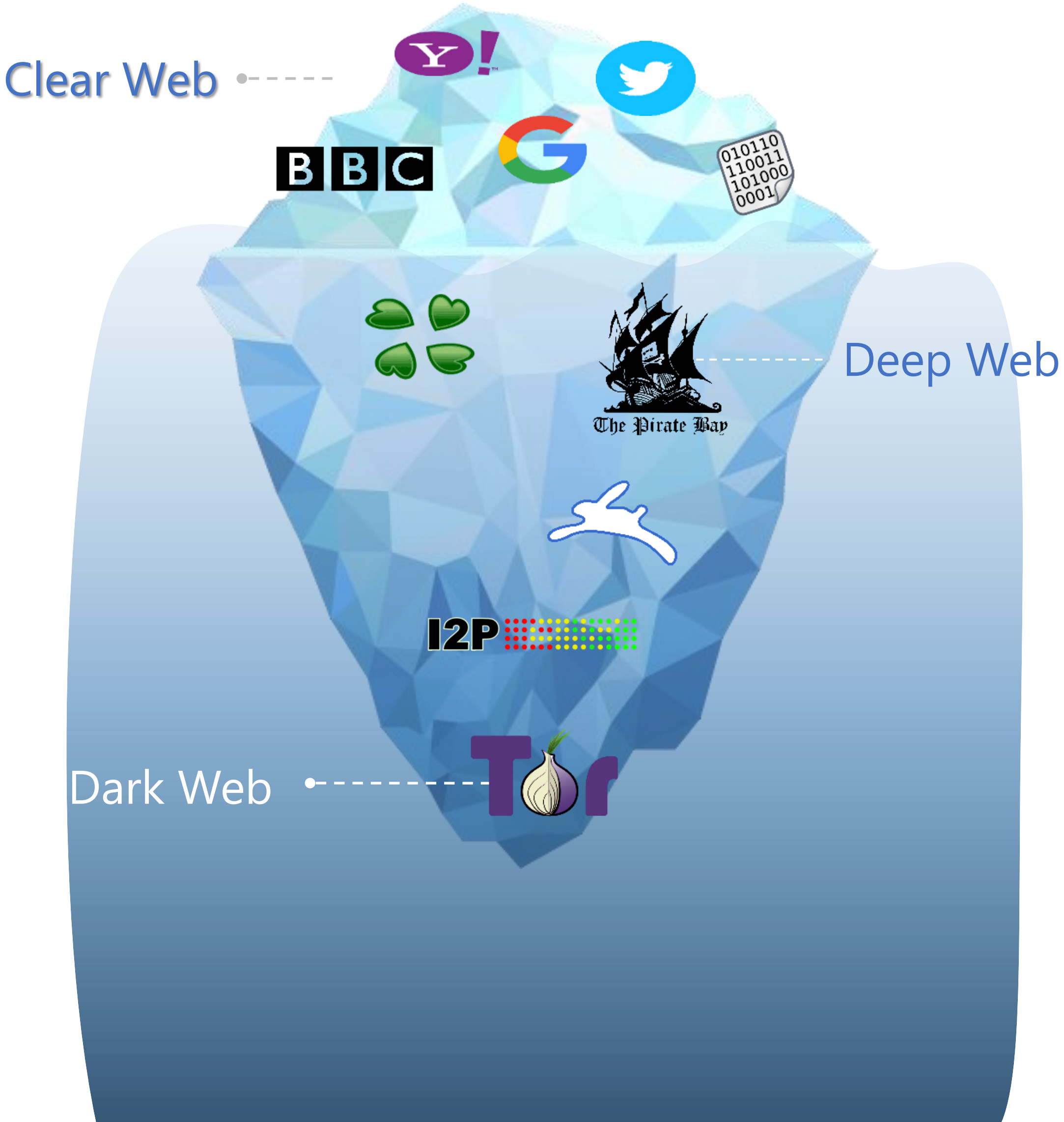
A GUEST   OCT 13TH, 2016   76   NEVER

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

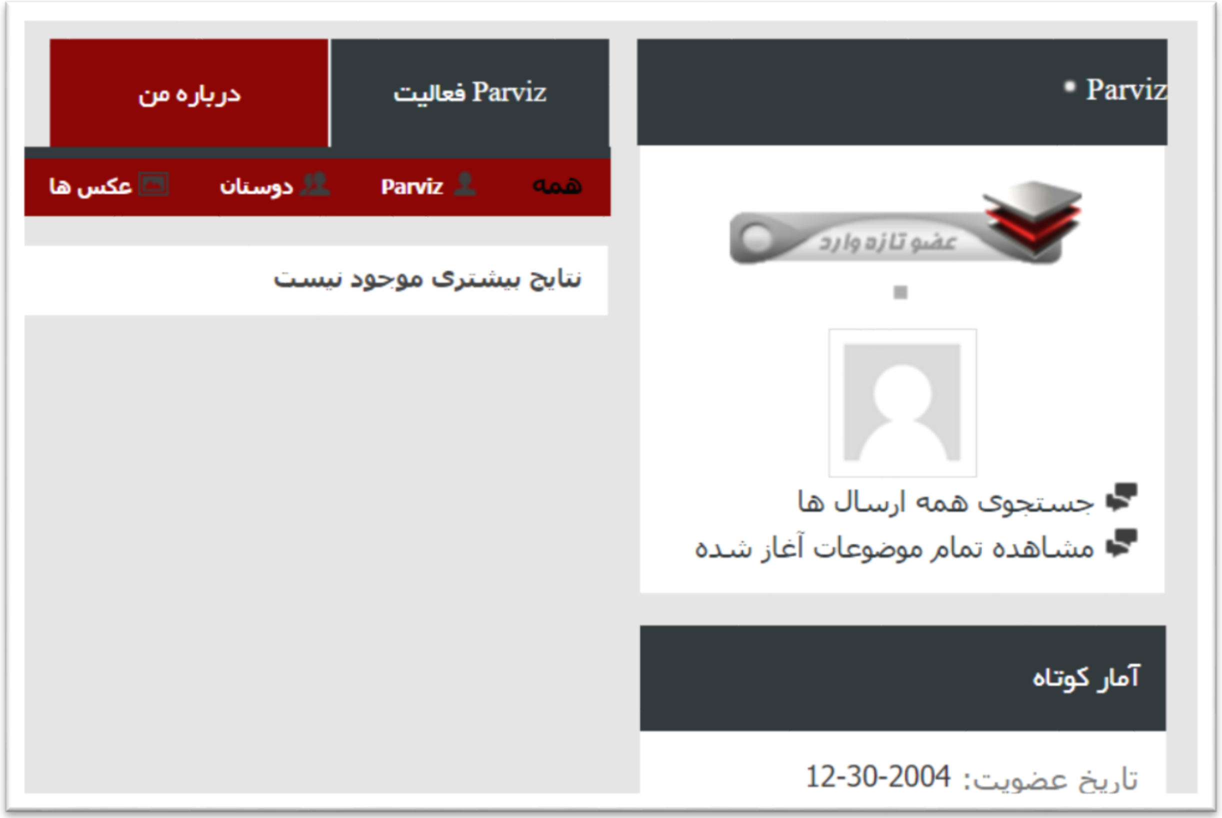
```

Partner Name    Sales Contact   Address City    State   Zip Telephone   Sales Contact Email URL Report Contact  Report Email    Report Phone
   Juniper Sponsor
Adaptive [redacted]
Chris Vig
Adaptive
DuBois gd
Advanced
aaron.gra
Ansley Co
cansley@a
AT&T    J
source=IG
Atrion Communications Resources Richard Dietz   185-J Industrial Parkway    Branchburg  NJ  08876   908-231-7777    RDietz@ATRIONCOMM.com
```

Step 3: Monitor The Dark Web

- What is the Dark Web?
- Hackers #1 interest – Anonymity.



They Are On The Dark Web!



نتایج بیشتری موجود نیست

جستجوی همه ارسال ها

مشاهده تمام موضوعات آغاز شده

آمار کوتاه

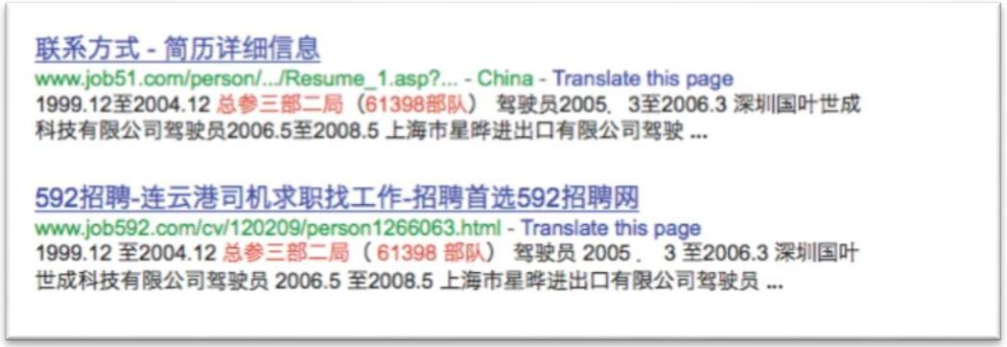
تاریخ عضویت: 12-30-2004

*OpCleaver, Cylance

What are they doing on the Dark Web?

- Recruiting/Hiring.
- 0days.
- Staying up-to-date.

Recruiting



[联系方式 - 简历详细信息](www.job51.com/person/.../Resume_1.asp?...)

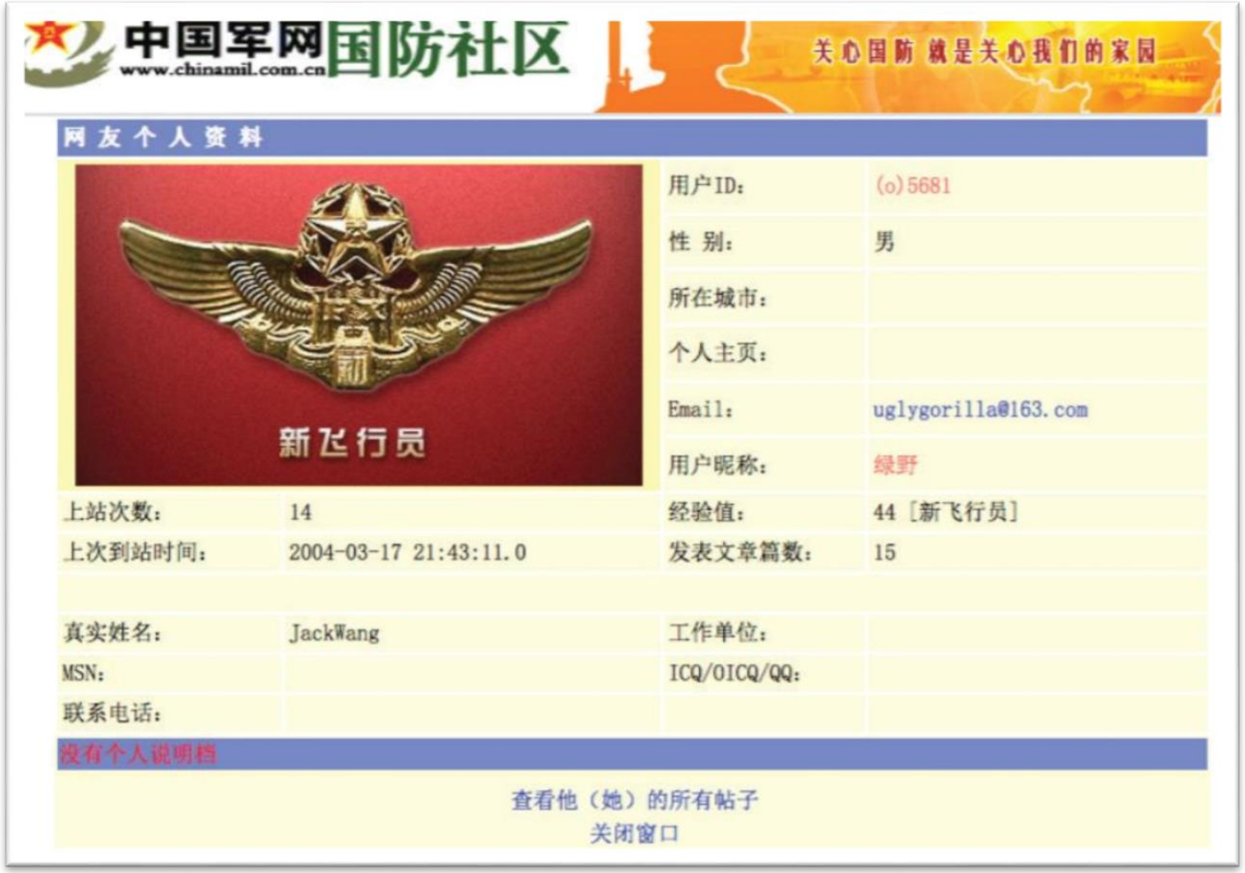
www.job51.com/person/.../Resume_1.asp?... - China - Translate this page

1999.12至2004.12 总参三部二局（61398部队） 驾驶员2005. 3至2006.3 深圳国叶世成科技有限公司驾驶员2006.5至2008.5 上海市星晔进出口有限公司驾驶 ...

[592招聘-连云港司机求职找工作-招聘首选592招聘网](www.job592.com/cv/120209/person1266063.html)

www.job592.com/cv/120209/person1266063.html - Translate this page

1999.12 至2004.12 总参三部二局（61398 部队） 驾驶员 2005． 3 至2006.3 深圳国叶世成科技有限公司驾驶员 2006.5 至2008.5 上海市星晔进出口有限公司驾驶员 ...



中国军网 www.chinamil.com.cn 国防社区

关心国防 就是关心我们的家园

网友个人资料

新飞行员

		用户ID:	(o)5681
		性 别:	男
		所在城市:	
		个人主页:	
		Email:	uglygorilla@163.com
		用户昵称:	绿野
上站次数:	14	经验值:	44 [新飞行员]
上次到站时间:	2004-03-17 21:43:11.0	发表文章篇数:	15
真实姓名:	JackWang	工作单位:	
MSN:		ICQ/OICQ/QQ:	
联系电话:			

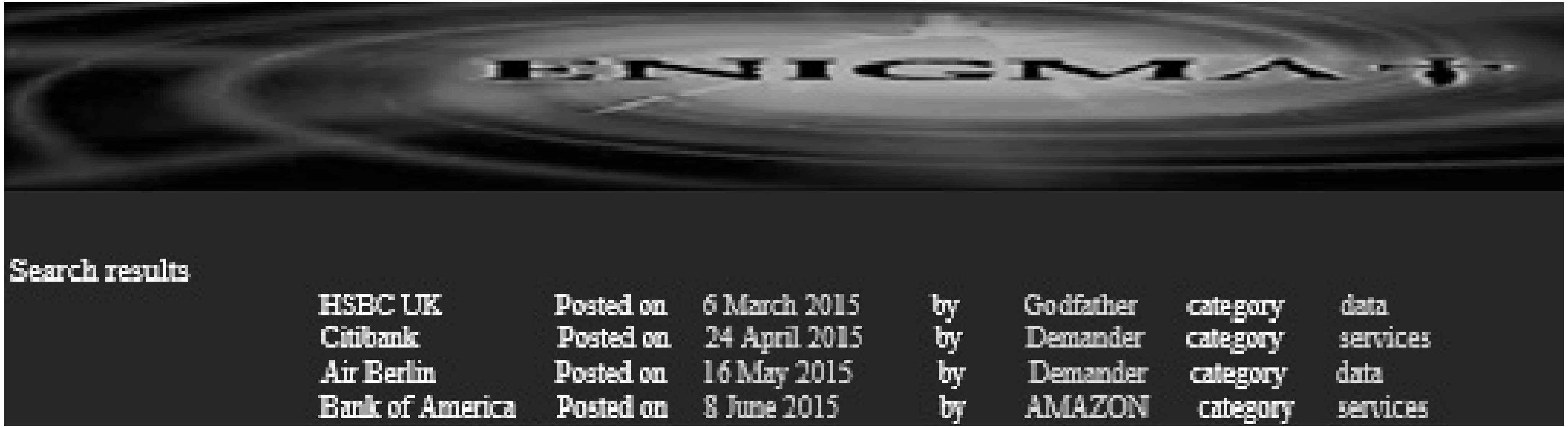
没有个人说明档

查看他（她）的所有帖子

关闭窗口

*APT1, Exposing one of China’s Cyber Espionage Units, Mandiant

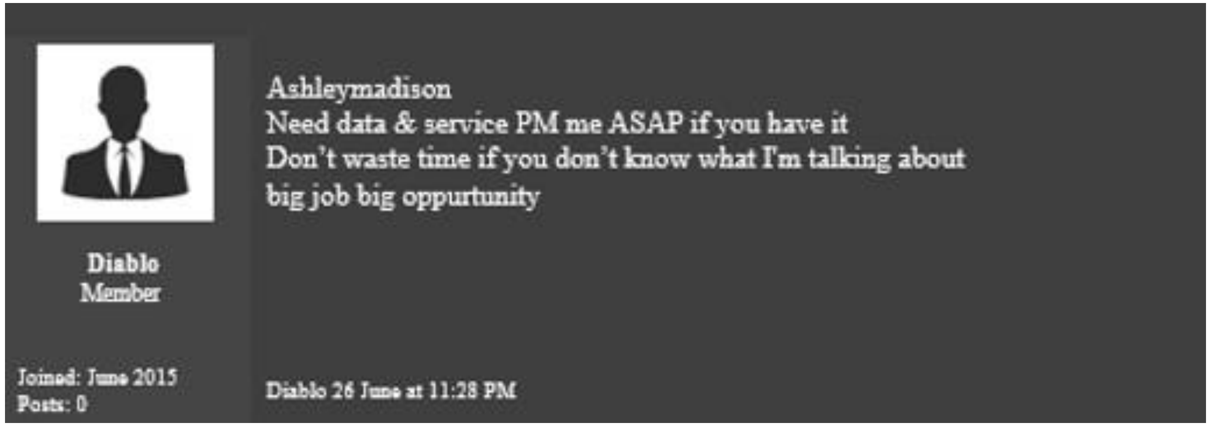
Outsourcing



ENIGMA

Search results

HSBC UK	Posted on	6 March 2015	by	Godfather	category	data
Citibank	Posted on	24 April 2015	by	Demander	category	services
Air Berlin	Posted on	16 May 2015	by	Demander	category	data
Bank of America	Posted on	8 June 2015	by	AMAZON	category	services



Ashleymadison
Need data & service PM me ASAP if you have it
Don't waste time if you don't know what I'm talking about
big job big oppurtunity

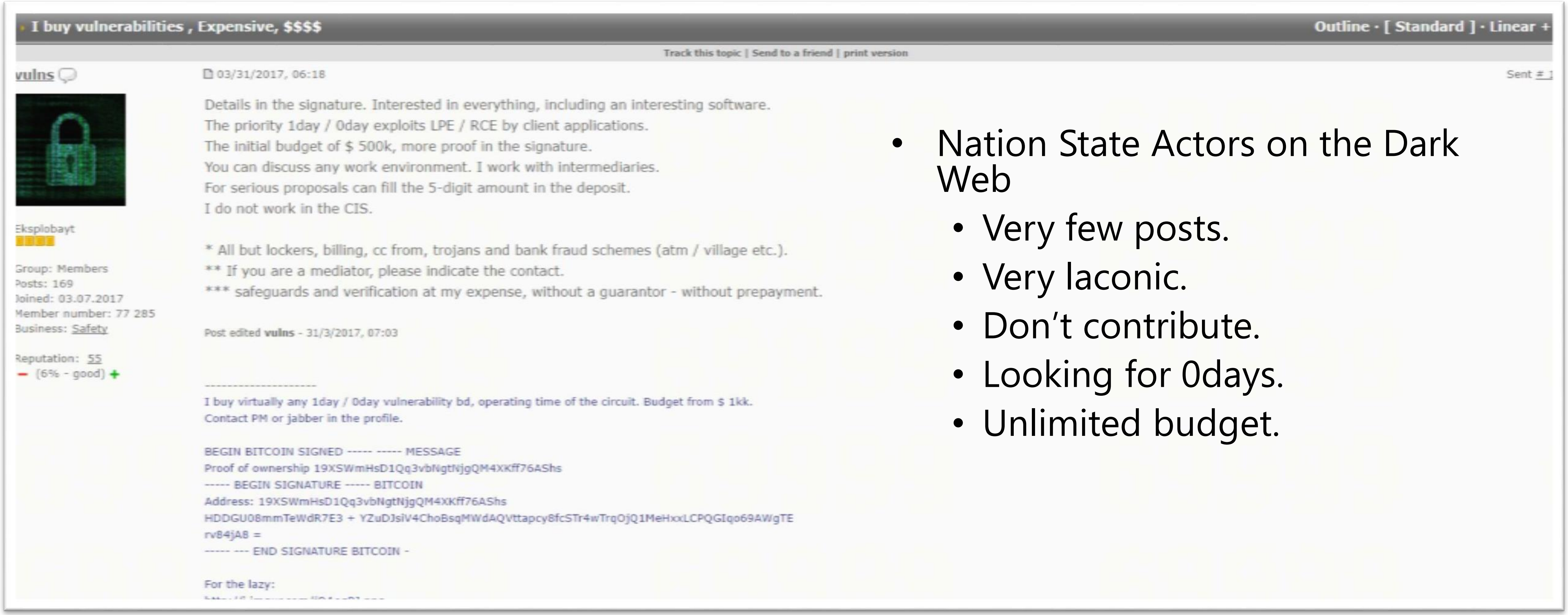
Diablo
Member

Joined: June 2015
Posts: 0

Diablo 26 June at 11:28 PM

*Exposed by Noam Jolles, Diskin Advanced Technologies

How Can They Be Detected?



I buy vulnerabilities , Expensive, $$$$

Outline · [Standard] · Linear +

Track this topic | Send to a friend | print version

vulns

Eksplobayt

Group: Members
Posts: 169
Joined: 03.07.2017
Member number: 77 285
Business: Safety

Reputation: 55
− (6% - good) +

03/31/2017, 06:18

Sent # 1

Details in the signature. Interested in everything, including an interesting software.
The priority 1day / 0day exploits LPE / RCE by client applications.
The initial budget of $ 500k, more proof in the signature.
You can discuss any work environment. I work with intermediaries.
For serious proposals can fill the 5-digit amount in the deposit.
I do not work in the CIS.

* All but lockers, billing, cc from, trojans and bank fraud schemes (atm / village etc.).
** If you are a mediator, please indicate the contact.
*** safeguards and verification at my expense, without a guarantor - without prepayment.

Post edited **vulns** - 31/3/2017, 07:03

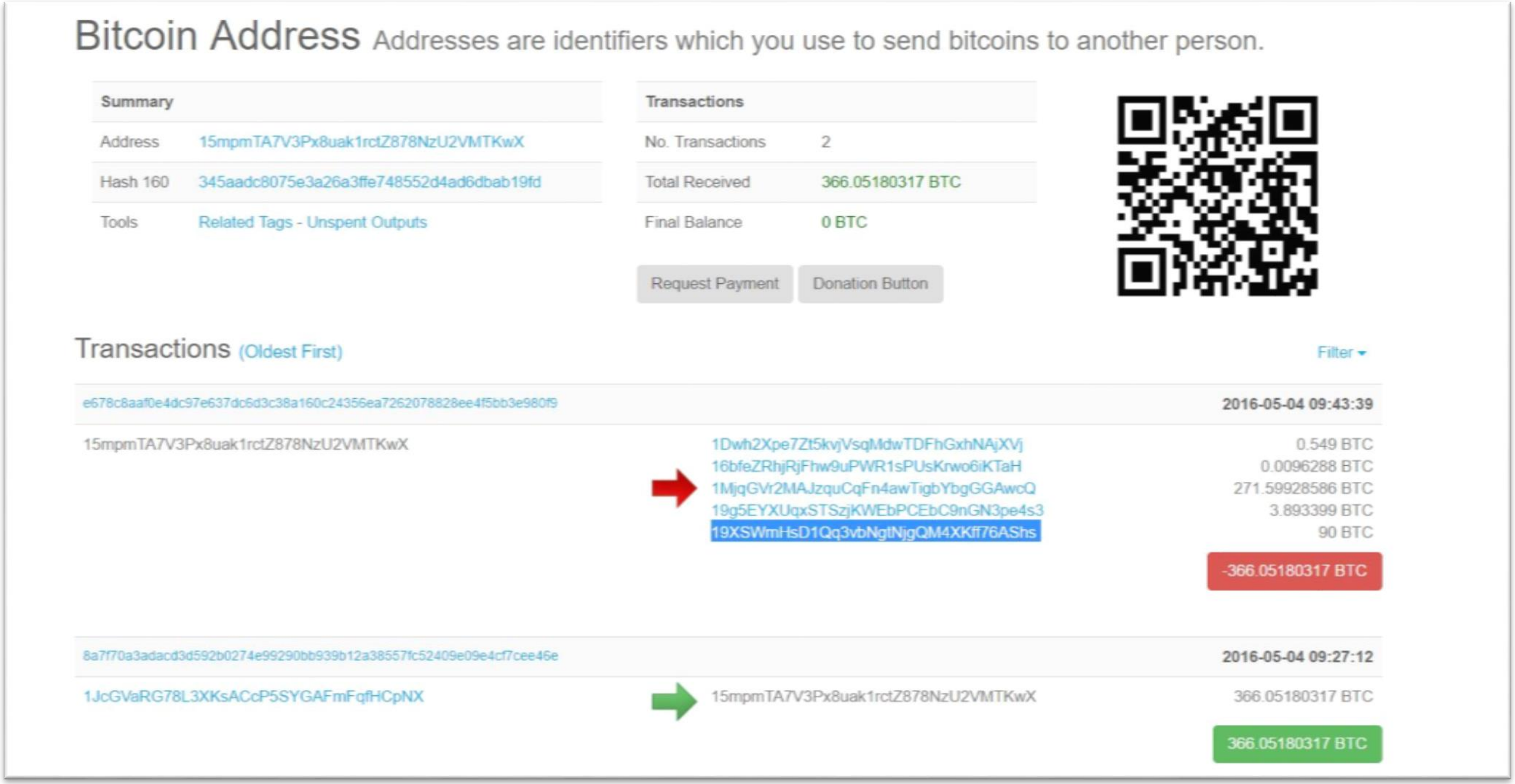
I buy virtually any 1day / 0day vulnerability bd, operating time of the circuit. Budget from $ 1kk.
Contact PM or jabber in the profile.

```
BEGIN BITCOIN SIGNED ----- ----- MESSAGE
Proof of ownership 19XSWmHsD1Qq3vbNgtNjgQM4XKff76AShs
----- BEGIN SIGNATURE ----- BITCOIN
Address: 19XSWmHsD1Qq3vbNgtNjgQM4XKff76AShs
HDDGU08mmTeWdR7E3 + YZuDJsiV4ChoBsqMWdAQVttapcy8fcSTr4wTrqOjQ1MeHxxLCPQGIqo69AWgTE
rv84jA8 =
----- --- END SIGNATURE BITCOIN -
```

For the lazy:

- Nation State Actors on the Dark Web
  - Very few posts.
  - Very laconic.
  - Don’t contribute.
  - Looking for 0days.
  - Unlimited budget.

How Can They Be Detected?



Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary	
Address	15mpmTA7V3Px8uak1rctZ878NzU2VMTKwX
Hash 160	345aadc8075e3a26a3ffe748552d4ad6dbab19fd
Tools	Related Tags - Unspent Outputs

Transactions	
No. Transactions	2
Total Received	366.05180317 BTC
Final Balance	0 BTC

Transactions (Oldest First)

e678c8aaf0e4dc97e637dc6d3c38a160c24356ea7262078828ee4f5bb3e980f9 2016-05-04 09:43:39

15mpmTA7V3Px8uak1rctZ878NzU2VMTKwX →

1Dwh2Xpe7Zt5kvjVsqMdwTDFhGxhNAjXVj 0.549 BTC
16bfeZRhjRjFhw9uPWR1sPUsKrwo6iKTaH 0.0096288 BTC
1MjqGVr2MAJzquCqFn4awTigbYbgGGAwcQ 271.59928586 BTC
19g5EYXUqxSTSzjKWEbPCEbC9nGN3pe4s3 3.893399 BTC
19XSWmHsD1Qq3vbNgtNjgQM4XKff76AShs 90 BTC

-366.05180317 BTC

8a7f70a3adacd3d592b0274e99290bb939b12a38557fc52409e09e4cf7cee46e 2016-05-04 09:27:12

1JcGVaRG78L3XKsACcP5SYGAFmFqfHCpNX → 15mpmTA7V3Px8uak1rctZ878NzU2VMTKwX 366.05180317 BTC

366.05180317 BTC

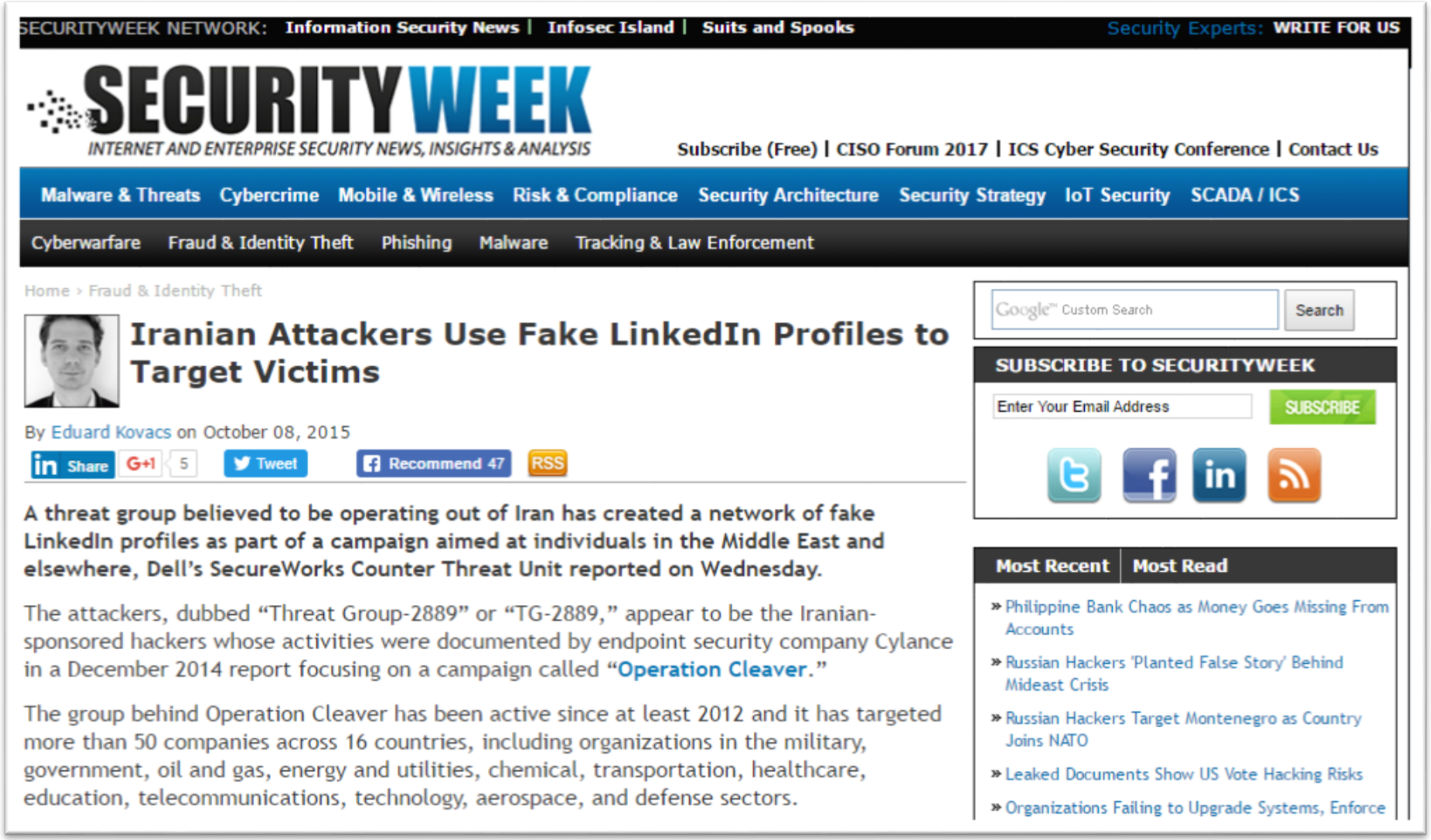
Step 4: Weapon Deployment

- States collaborate on closed networks but organizations are on the surface.
- In order to attack, states have to reach the surface, and that leaves them exposed.

TI can help detect:

- **Phishing attacks**- fake domain registration.
- **Malicious mobile applications**
- **Fake social media profiles**

Fake Social Media Profiles


SECURITYWEEK NETWORK: Information Security News | Infosec Island | Suits and Spooks
Security Experts: WRITE FOR US
SECURITYWEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS
Subscribe (Free) | CISO Forum 2017 | ICS Cyber Security Conference | Contact Us
Malware & Threats
Cybercrime
Mobile & Wireless
Risk & Compliance
Security Architecture
Security Strategy
IoT Security
SCADA / ICS
Cyberwarfare
Fraud & Identity Theft
Phishing
Malware
Tracking & Law Enforcement
Home › Fraud & Identity Theft
Google™ Custom Search
Search
SUBSCRIBE TO SECURITYWEEK
Enter Your Email Address
SUBSCRIBE
Most Recent
Most Read
» Philippine Bank Chaos as Money Goes Missing From Accounts
» Russian Hackers 'Planted False Story' Behind Mideast Crisis
» Russian Hackers Target Montenegro as Country Joins NATO
» Leaked Documents Show US Vote Hacking Risks
» Organizations Failing to Upgrade Systems, Enforce
in Share
G+1
5
Tweet
Recommend 47
RSS

Iranian Attackers Use Fake LinkedIn Profiles to Target Victims

By Eduard Kovacs on October 08, 2015

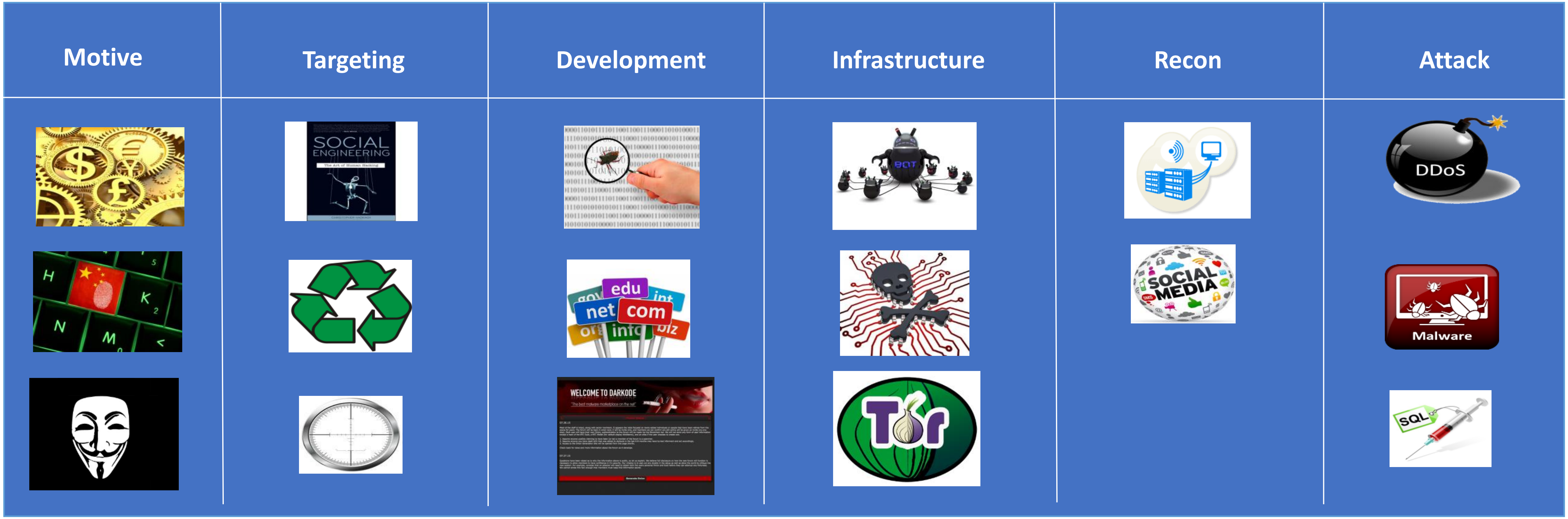
A threat group believed to be operating out of Iran has created a network of fake LinkedIn profiles as part of a campaign aimed at individuals in the Middle East and elsewhere, Dell's SecureWorks Counter Threat Unit reported on Wednesday.

The attackers, dubbed "Threat Group-2889" or "TG-2889," appear to be the Iranian-sponsored hackers whose activities were documented by endpoint security company Cylance in a December 2014 report focusing on a campaign called "**Operation Cleaver**."

The group behind Operation Cleaver has been active since at least 2012 and it has targeted more than 50 companies across 16 countries, including organizations in the military, government, oil and gas, energy and utilities, chemical, transportation, healthcare, education, telecommunications, technology, aerospace, and defense sectors.

How Nation-state Cyber Attacks Unfold?

The Attack Supply Chain



Motive	Targeting	Development	Infrastructure	Recon	Attack
	Benchmark Exploitable Data Data Leakage	Dark Web monitoring	Phishing domains Malicious mobile apps Fake social media profiles	Exploitable Data Data Leakage	

Conclusion: OSINT Is Critical

Eliminates Blind Spots

1. Optimized risk picture with an aggregated and coordinated view across internal and external threats.
2. Context to effectively scope alerts or gauge the severity of a threat.

Enable Proactive Security

1. Connect external threats with your enterprise before they attack.
2. Capture early warning signals.

Operational Efficiency

1. Actionable visibility
2. Automate remediation for internal and external systems
3. Metrics and visibility showcasing security's impact.

Thank You

Alon Arvatz

alon@intsights.com

+972-545444313