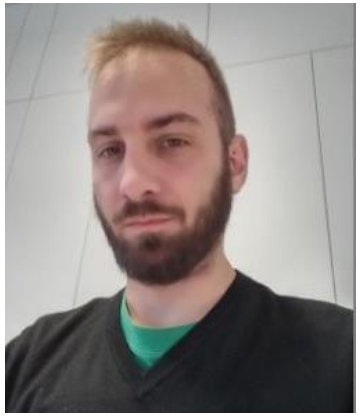
Tecniche di password cracking: quanto è davvero sicura la tua password?

Gianluca Baldi

mediaservice.net
CORPORATE SECURITY & IMAGE

Chi sono



gianluca.baldi@mediaservice.net

- ✓ **Penetration Tester da circa 3 anni presso**

mediaservice.net
CORPORATE SECURITY & IMAGE

- ✓ **5 Anni di esperienza nella Security**
- ✓ **Web Application Security**
- ✓ **Password Craking Addicted ;)**

Agenda

- Introduzione
- Cenni di Crittografia
- Tipi di attacchi alle password
- Come otteniamo gli hash e i data leak
- Introduzione al password cracking (Hashcat)
- Tecniche di Password Cracking
- Piccolo esempio
- Consigli per difendersi
- Domande

Perché sono importanti le password?

Proteggono tutto ciò che usiamo ogni giorno!

- e-mail personale (gmail, yahoo, hotmail, ecc)
- PEC

E-mail

- Facebook
- Instagram
- Linkedin
- Twitter
- …

Social

- Home Banking
- Shopping online
- Paypal
- Bitcoin & Cryptovalute

Denaro & Shopping

- E-mail aziendale
- PC Portatile (Active Directory)
- Intranet aziendale
- Dischi cifrati
- Server…

Lavoro

- Telecamere
- Allarmi
- Router
- Devices IoT
- …

Asset Fisici

- App (videogames, messaggistica, app di fitness con geolocalizzazione..)
- Blog personale
- Molto, Molto altro… !

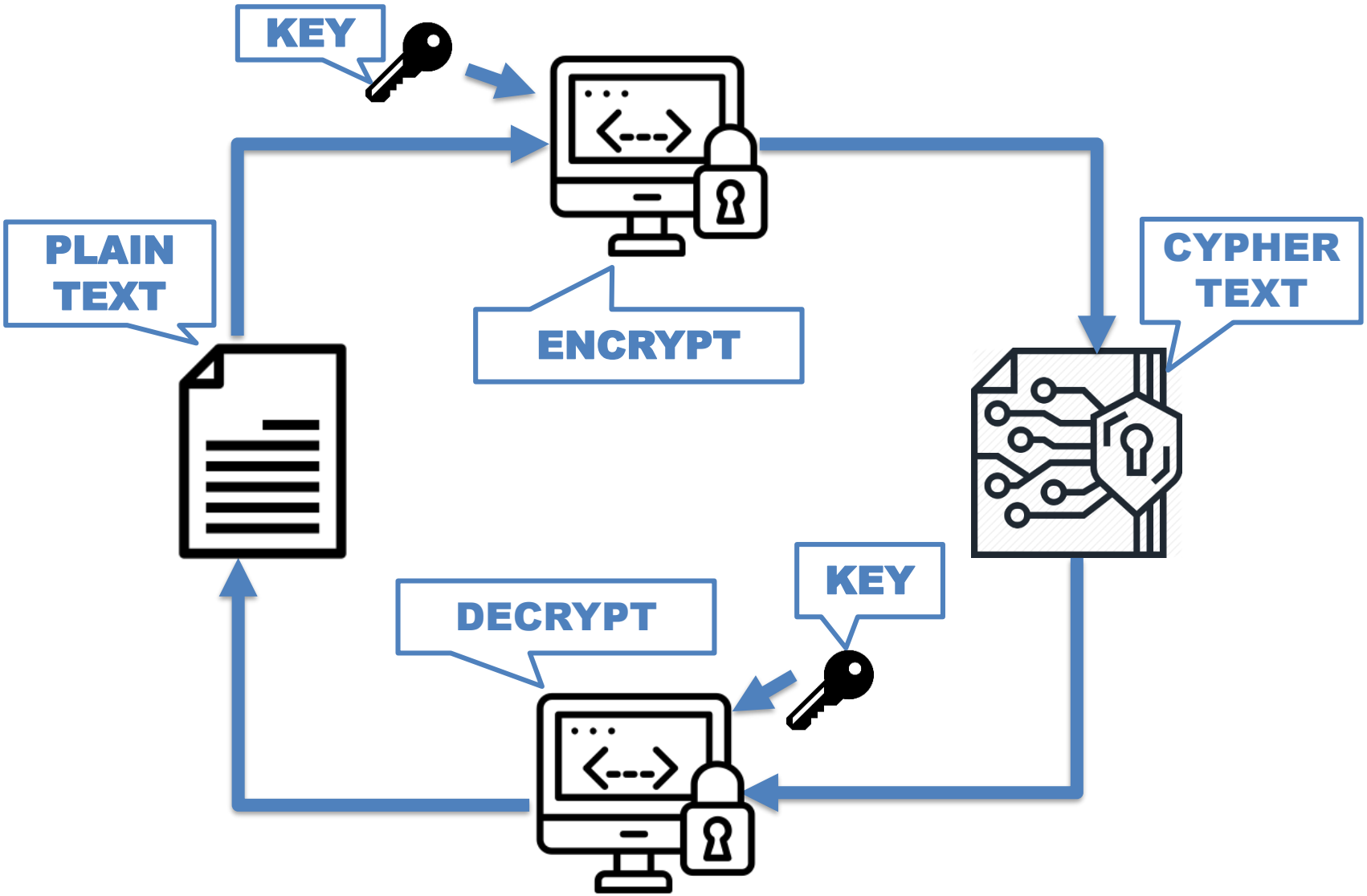
Varie

Perché sono importanti?

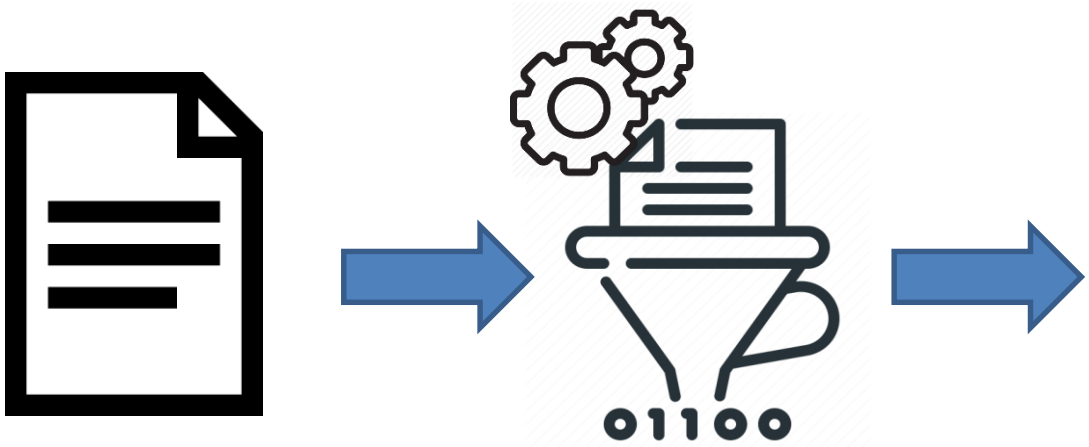
Sono le «chiavi» delle aziende a livello informatico!

La sicurezza di un organizzazione passa anche per la robustezza delle sue password!

Algoritmi di cifratura



Algoritmi di hashing



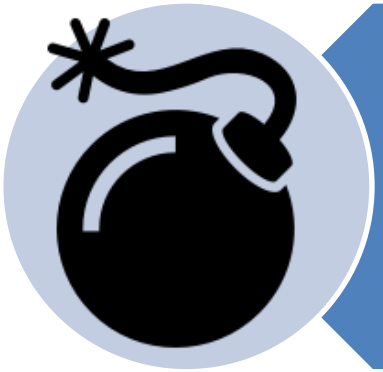
8c980eadcb0e9d
9e1ad4eb7253ef
dc92

Algoritmi di cifratura ed hashing

Hash	Anno	Utilizzato da
MD5	1991	WordPress, MySQL, Joomla , Badoo*
SHA1	1995	Linkedin*,mySpace*, Dropbox*
NTLM (MD4)	1990	Microsoft Active Directory
Sha512 (SHA2)	2001	Linux ultima generazione
Whirlpool	2000-2003	TrueCrypt , VeraCrypt
scrypt	2009	Litecoin, Dogecoin

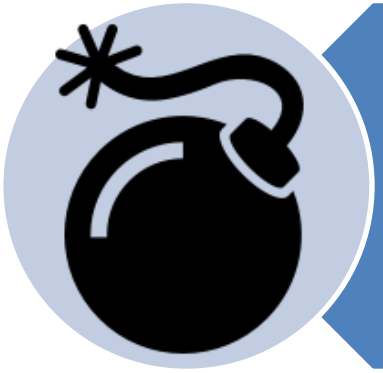
*Data Breach

Attacchi alle password



ONLINE

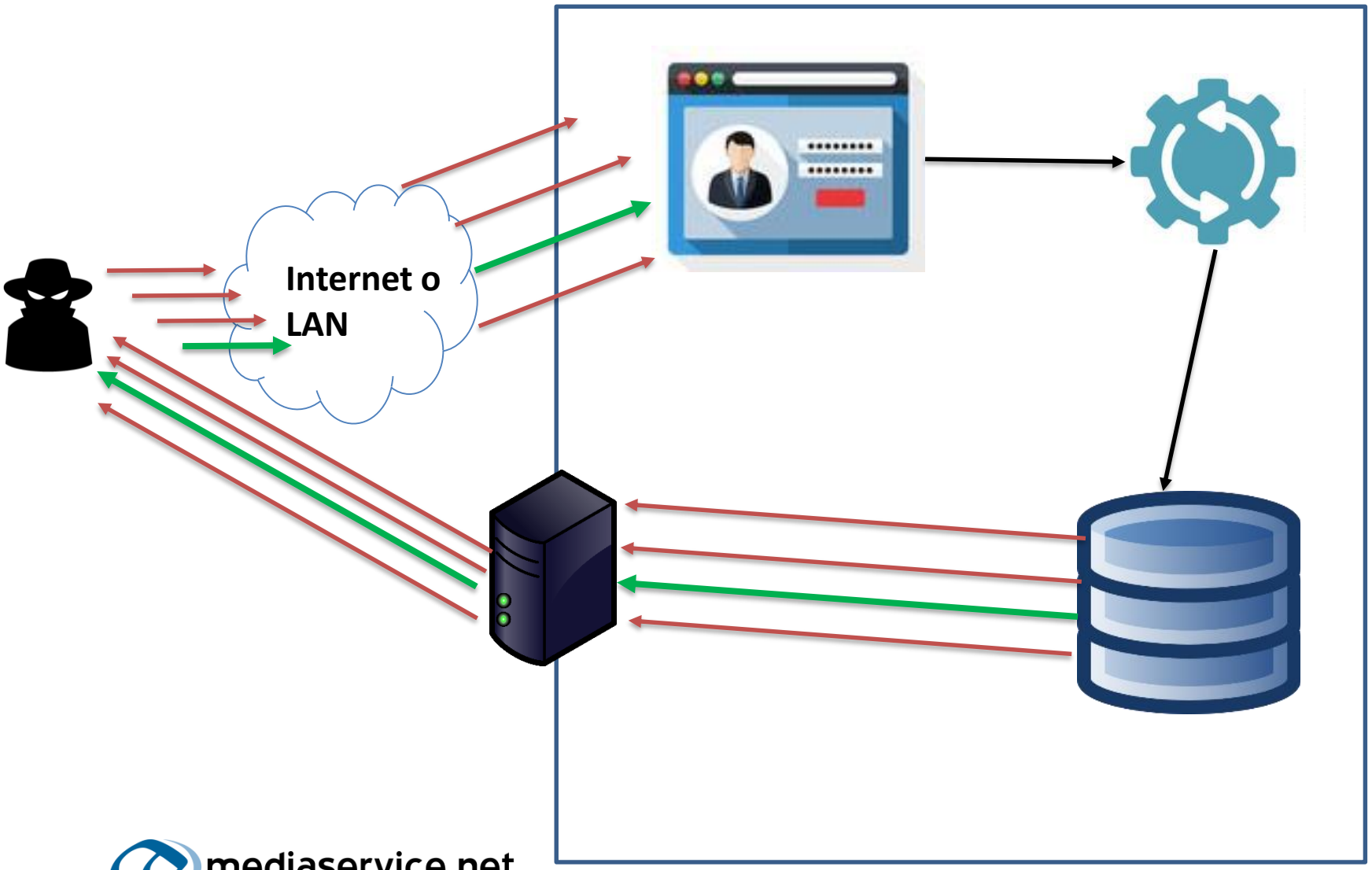
- Password guessing
- Password bruteforce
- Password spraying



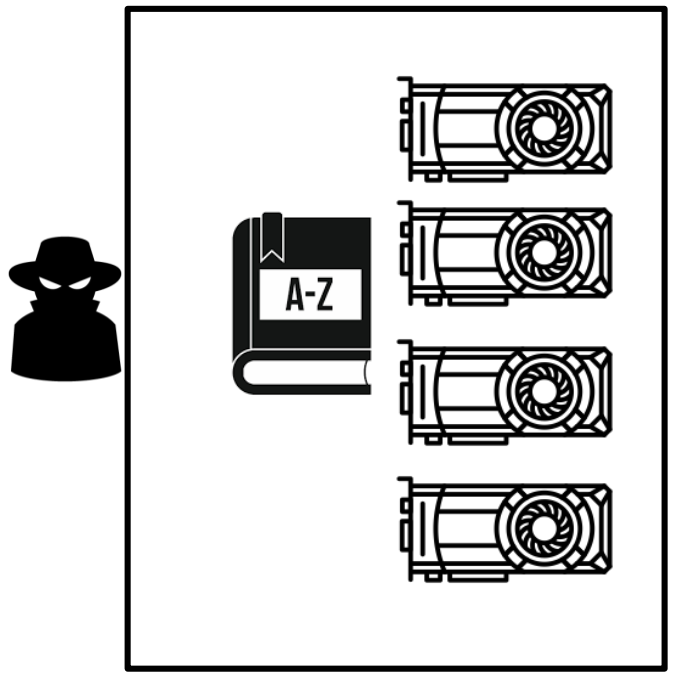
OFFLINE

- **Password Cracking**
- Rainbow Tables

Attacchi alle password: Online



Attacchi alle password: Offline



.....	....
pomodorini	ee2a6a741a3f774cc4f61fefc0ec2dd7
eleonora	7756dad2e8fe14e0b5b64d2b3b3bce32
roserosse	a19e060d7162513cd70c5b90ac9d2dd1
dicembre27	**37e7c35bac2992d7c2f4d1258e87c18a**
alberto17	b0ce1f4cfe3a5dee9ed720e18df4d199
15041956	4b2102e6513bcee8aaa94329bc615846
.....	.....

37e7c35bac2992d7c2f4d1258e87c18a

Come ottenere hash delle password

Compromissione di un sistema

Compromissione Database applicativo

Accesso alla memoria del sistema operativo (mimikatz)

Trasmissione degli hash via rete per autenticazione (rogue SMB server, Responder.py, ecc)

La password di reti Wi-Fi

DIAMO QUINDI PER SCONTATO CHE L'HASH SIA NOTO AD UN ATTACCANTE

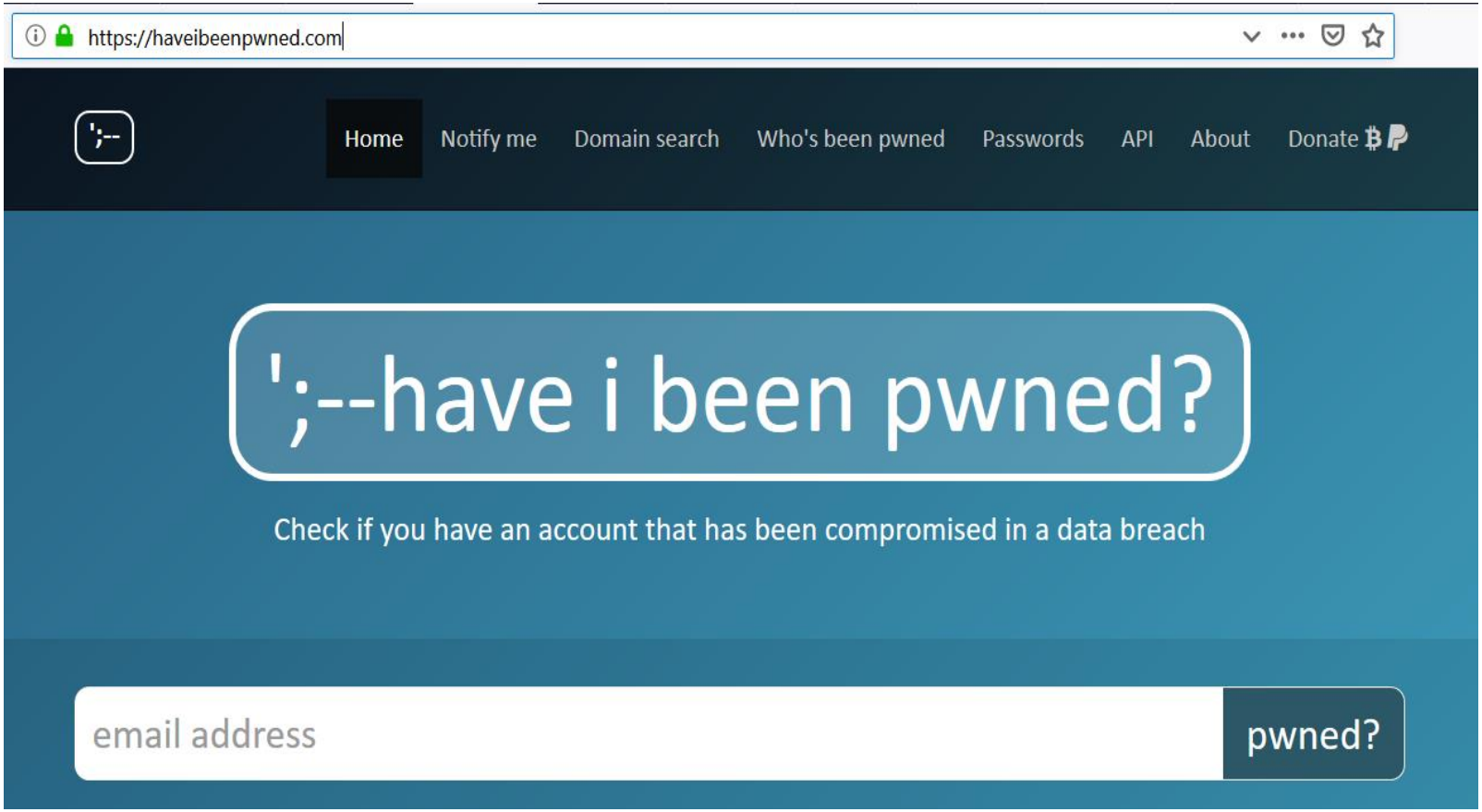
Esempi: I data leak

Compromissioni di aziende importanti, con impatto su numerosi utenti

Azienda	Info	Account Compromessi
MySpace	2008? pubblico nel 2016. (SHA1)	360.000.000
Linkedin	2012, pubblico nel 2016 (SHA1)	164.000.000
Adobe	2013	153.000.000
Ashley Madison	2015? Pubblico nel 2015 (MD5 & bcrypt)	30.000.000

https://en.wikipedia.org/wiki/List_of_data_breaches

Esempi: I data leak



Come craccare un hash - Tools

- Stato dell'arte dei software per cracking delle password
- Ottimizzato per l'utilizzo delle GPU nel password cracking (molto più efficienti delle CPU in fatto di calcolo parallelo)

Calcola gli hash delle password che gli diciamo noi e verifica se sono uguali agli hash che stiamo cercando!

Password hash = 0c88028bf3aa6a6a143ed846f2be1ea4

p1 = ec6ef230f1828039ee794566b9c58adc
p2 = 1d665b9b1467944c128a5575119d1cfd
p3 = 7bc3ca68769437ce986455407dab2a1f
p4 = ….

Benchmarck: SHA1, NTLM , scrypt

```
Hashmode: 1000 - NTLM

Speed.#1.........: 16157.9 MH/s (66.00ms) @ Accel:128 Loops:1024 Thr:256 Vec:1
Speed.#2.........: 23106.9 MH/s (63.46ms) @ Accel:128 Loops:1024 Thr:256 Vec:1
Speed.#3.........: 16158.3 MH/s (66.01ms) @ Accel:128 Loops:1024 Thr:256 Vec:1
Speed.#4.........: 16158.5 MH/s (66.01ms) @ Accel:128 Loops:1024 Thr:256 Vec:1
Speed.#*.........: 71581.6 MH/s
```

```
Hashmode: 100 - SHA1

Speed.#1.........:  2961.3 MH/s (90.10ms) @ Accel:128 Loops:256 Thr:256 Vec:1
Speed.#2.........:  4236.6 MH/s (86.66ms) @ Accel:128 Loops:256 Thr:256 Vec:1
Speed.#3.........:  2961.4 MH/s (90.10ms) @ Accel:128 Loops:256 Thr:256 Vec:1
Speed.#4.........:  2961.4 MH/s (90.10ms) @ Accel:128 Loops:256 Thr:256 Vec:1
Speed.#*.........: 13120.7 MH/s
```

```
Hashmode: 8900 - scrypt (Iterations: 1)

Speed.#1.........:   152.5 kH/s (181.90ms) @ Accel:16 Loops:1 Thr:16 Vec:1
Speed.#2.........:   135.1 kH/s (578.70ms) @ Accel:16 Loops:1 Thr:16 Vec:1
Speed.#3.........:   150.2 kH/s (180.91ms) @ Accel:16 Loops:1 Thr:16 Vec:1
Speed.#4.........:   123.2 kH/s (140.48ms) @ Accel:16 Loops:1 Thr:16 Vec:1
Speed.#*.........:   561.0 kH/s
```

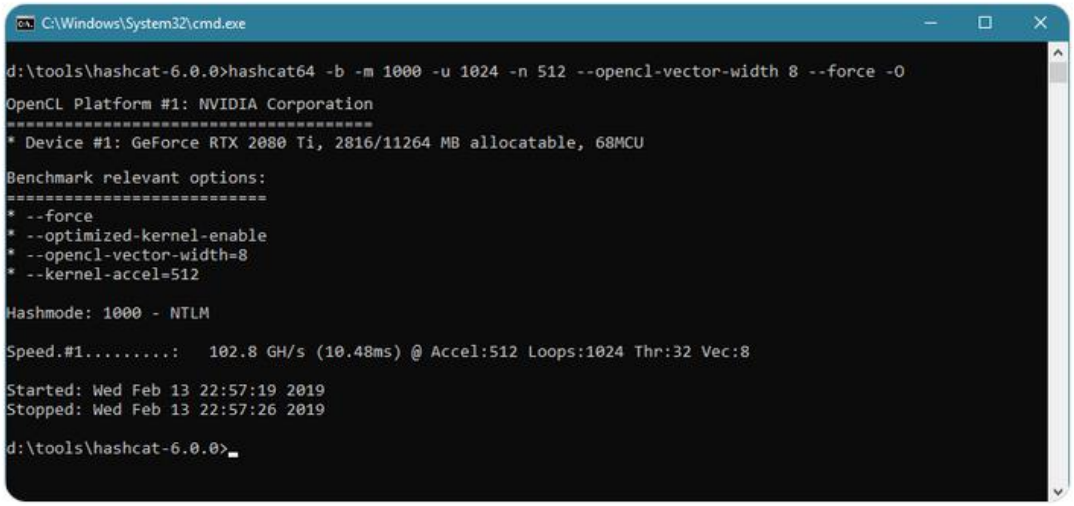
Benchmark: 100 GH/s

hashcat
@hashcat

Following

hand-tuned hashcat 6.0.0 beta and 2080Ti (stock clocks) breaks NTLM cracking speed mark of 100GH/s on a single compute device

Traduci il Tweet



14:08 - 13 feb 2019

Tecniche di password cracking

Tecniche

1- Bruteforce

2 - Attacco a dizionario

3 - Rules

4 - Mask

5 - Attacchi combinati

Bruteforce

È il «provo tutte le combinazioni»:

aaaaaaa, aaaaaab,aaaaaac … AAAAAAAA,AAAAAAB…. ZZZZZZZ !

- **Pro:**
  - è «infallibile»
- **Contro:**
  - Computazionalmente infattibile oltre certi limiti
  - «Spreco tempo» a provare un sacco di password inutili (non reali)
  - Fortemente dipendente dal tipo di hash che vogliamo crackare

Bruteforce

N° Char	[0-9]	[a-z]	[A-Z]	[!@?*, # ….]	Combinazioni	Tempo (100 GH/s)
8	X				100.000.000 (10^8)	0,1 s
8		X			200.000.000.000 (~10^11)	2 s
8	X	X			~10^12	10 s
8	X	X	X		~10^14	16 min
8	X	X	X	X	~10^15	2.7 h
10	X	X	X	X	~10^20	31 y
15	X	X			~10^23	31.709 y
15	X	X	X	X	~10^29	3*10^10 y

10^23= 100.000.000.000.000.000.000.000

10^20 < numero di granelli di sabbia sulla Terra <10^24

10^80 Particelle dell' universo visibile…

mediaservice.net
CORPORATE SECURITY & IMAGE

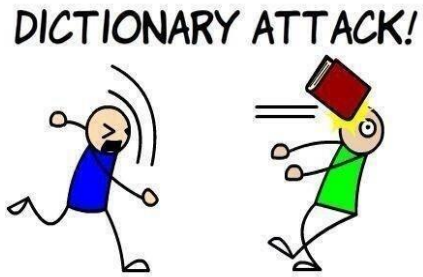
Attacco a dizionario:

Prendo un dizionario (wordlist) e vedo se la password è contenuta lì dentro.

- **Pro:**
  - Sono parole o password reali quelle del dizionario, non «spreco tempo»
  - Trovo immediatamente le password più deboli
  - Molto più rapido di un bruteforce (molti meno tentativi e più «mirati»)
- **Contro**
  - La rapidità dell'attacco è proporzionata alla dimensione e alla «qualità» del dizionario (importante crearlo ad hoc!)
  - L'input avviene da file (la lettura da disco è un collo di bottiglia)
  - Posso trovare solo password che conosco già (devono essere presenti nel dizionario!)

Attacco a dizionario:

Dizionario	Dimensione	Tempo (20MH/s)
Dizionario italiano (282000 parole):	~ 3.2 MB	< 1s
Top 1.000.000 Password (2018):	~ 8.2 MB	< 1s
Tutta Wikipedia (2009 - caratteri latini)	~ 6.4 GB	~ 1 min
hashes.org database (2018)	~ 4.1 GB	~ 30 s



Tecniche avanzate: Rules

Si applicano regole di sostituzione/modifica alle parole di un dizionario/wordlist!

- **Ci basiamo sull'assunzione (statistica!!) che le persone tendono a riutilizzare le stesse password, modificandole semplicemente di qualche carattere per facilitarne la memorizzazione!**
- **Risolve il problema dell'attacco a dizionario normale: scopriamo nuove password usando lo stesso dizionario!**
- **È statisticamente l'attacco che ha più successo in termini di tempo/risultato!**

Tecniche avanzate: Rules

Word	Trasformazioni con rules
password	Password,PASSWORD,password?,P@$$w0rd, ….
luca88	Luca , luca87, *luca91, Luc@8800 ...
tomcat	tomcat2019, TOMCAT, 2019TOMCAT# , 20TACMOT18…

Le password identificate ci daranno indizi su altre password con pattern simili!

Ad esempio «Microsoft2019»: con questo criterio, riuscirò a craccare tutte quelle simili (microsoft2019!, microSoft2019, MiCr0sOfT ecc) inserendola nel mio dizionario!

Tecniche avanzate: MASK

Bruteforce «intelligente»: ci concentriamo solo su pattern reali, che sappiamo portare a qualcosa!

- **Limitando il numero di tentativi, rendiamo possibile il bruteforce su password molto più lunghe!**
- **Tipicamente, prima proviamo un attacco a dizionario o con rules, individuiamo i pattern e usiamo questo attacco.**

Tecniche avanzate: MASK

Pattern	#Char	Esempio	Tempo (100GH/s)
?u?l?l?l?l?l?l?s	8	Alberto$, Napoli!, Sehnsucht7	3 s
?u?l?l?l?l?l?l?l?s	9	Password! , Federico@ , Giappone* , Superman$	1 min
?u?l?l?l?l?l?l?l?l?s	10	Microsoft+ , Comobella$, Jkxohwyop&	30 min
?u?l?l?l?l?l?l?d?d	8	Andrea68 , Summer15 , Ubuntu86	< 1 sec
?d?d?d?d?d?d?d?d?d?d	10	Numeri di telefono!	< 1 sec
?u?l?l?l?l?l?l?d?d?d?d?s	12	Napoli2018!, Firenze2000$	7 h

?l = abcdefghijklmnopqrstuvwxyz

?u = ABCDEFGHIJKLMNOPQRSTUVWXYZ

?d = 0123456789

?s = «space»!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~

mediaservice.net
CORPORATE SECURITY & IMAGE

Tecniche avanzate: combinazioni

- **Dizionario + mask**
  - Ad ogni parola del dizionario, aggiungiamo o prima o dopo una mask su cui fare bruteforce!
  - **es: parola + ?d?d?d?d: Microsoft0000 ….. Microsoft2017, Microsoft2018, Microsoft2019 …**

- **Dizionario + dizionario:**
  - Combiniamo tutte le password del primo con quelle del secondo: posso cracckare passphrase in questo modo!
  - Fattibile con dizionari realtivamente piccoli
  - Posso creare un dizionario che sia la combinazione di altri due e poi concatenarlo ad un 3 dizionario! (solo dizionari molto piccoli**)**
  - **Es: ludo02fabri89, pastoreaustraliano, tiamostellina73, newyorkroma1 …**

Caso Reale

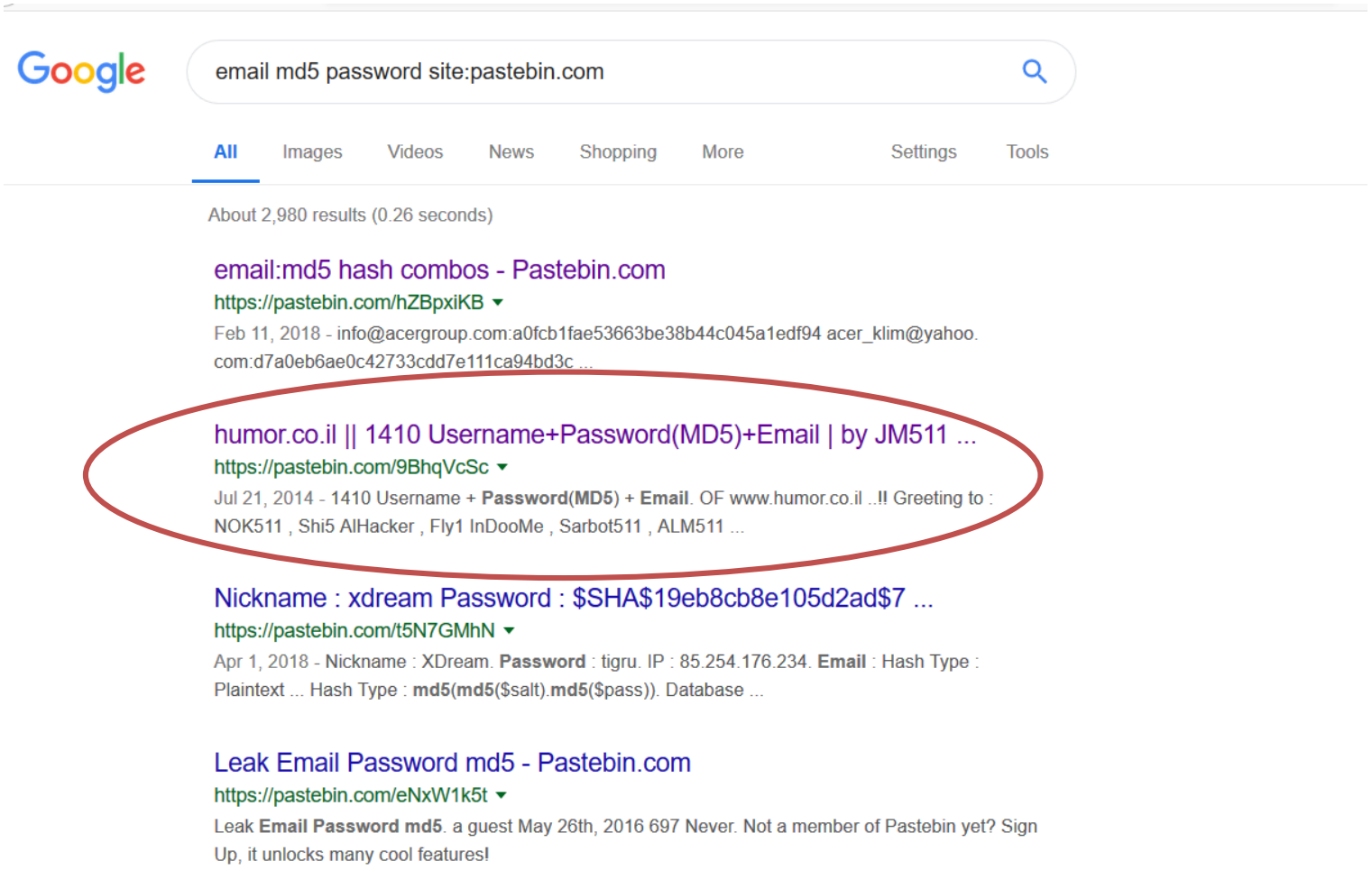
- **Dizionario**
  - **Top 1.000.000 Password 2018 (8MB)**: 598/5970 (10.02%) in < 1s
  - **Wordlist hashes.org 2018 (4.1 GB)** : 2105/5970 (**35.26%**) in 27s
- **Rules**
  - **Top 1.000.000 Password 2018 + best64 rule:** 1230/5970 (20.60%) < 2s
  - **Wordlist hashes.org 2018 + Best64 rules:** 2968/5970 (**49.72%**) <(**1min**)
  - **Wordlist hashes.org 2018 + OneRuleToRuleThemAll** :4540/5970 (**76.05%**) (**40min)**
- **Mask**
  - **?d?d?d?d?d?d?d?d:** 235/5970 (3.94%) in < 1 sec
  - **?l?l?l?l?l?l?l?l:** 222/5970 (3.72%) in 4 sec
  - **?l?l?l?l?l?l?l?d?d:** 294/5970 (4.92%) in 20 sec
  - **?l?l?l?l?l?l?d?d:** 178/5970 (2.98%) in 2 sec

Servizi Online

- **Esistono servizi gratuiti di cracking Online:**
  - hashkiller.co.uk
  - hashes.org
  - crackstation.net
  - ….
- **Se preferiamo il «fai da te»:**
  - AMAZON EC2
  - Microsoft Azure NC
  - **Es: p3.16xlarge (Tesla V100-SXM2-16GB x 8 - 633 GH/s) $24.48/ h !**

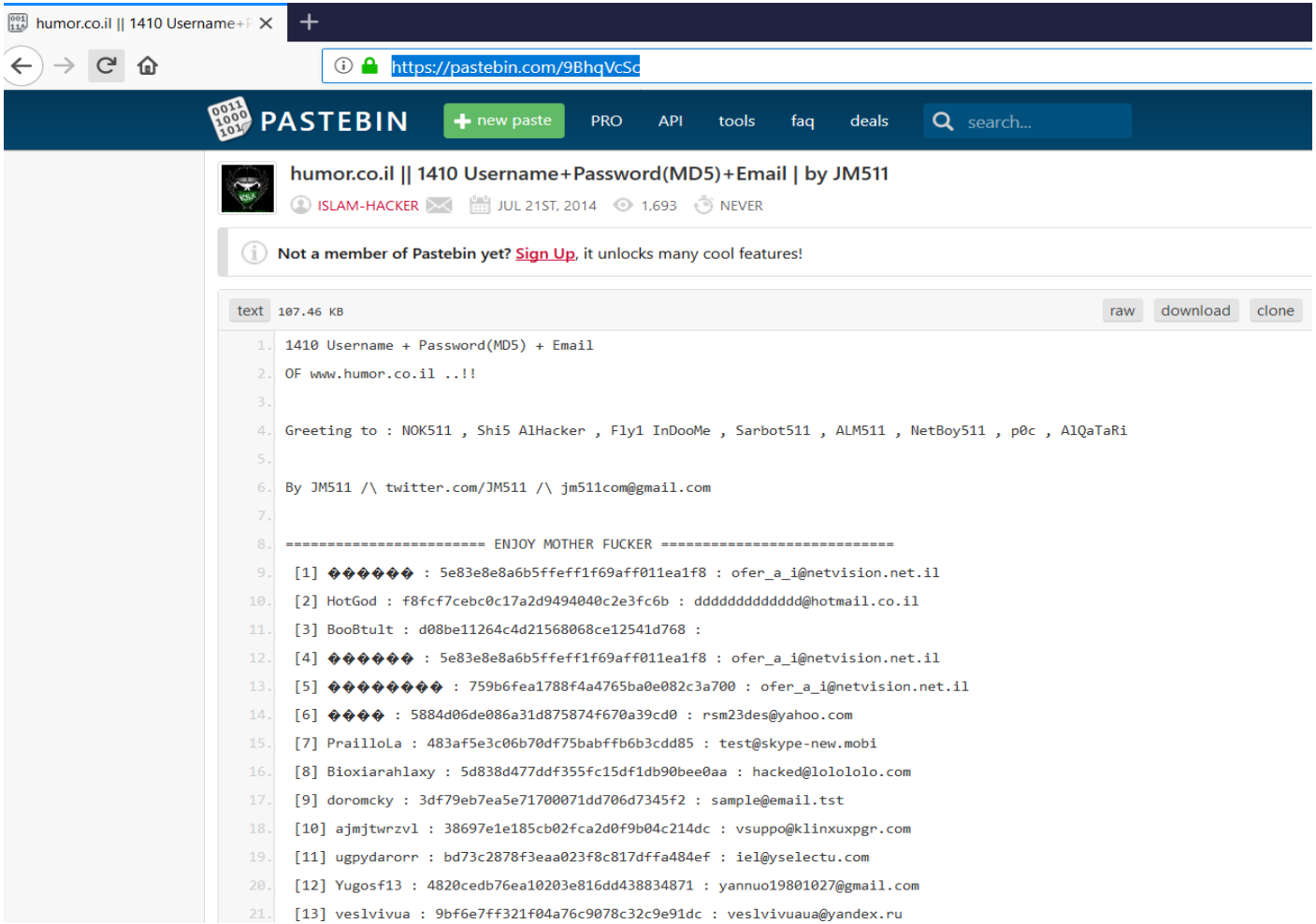
Un agenzia governativa (o chiunque non abbia problemi di budget o sufficiente motivazione) potrebbe comprarsi alcune istanze per qualche settimana o mese – bisogna tenerne conto quando scegliamo le nostre password!

Esempio:

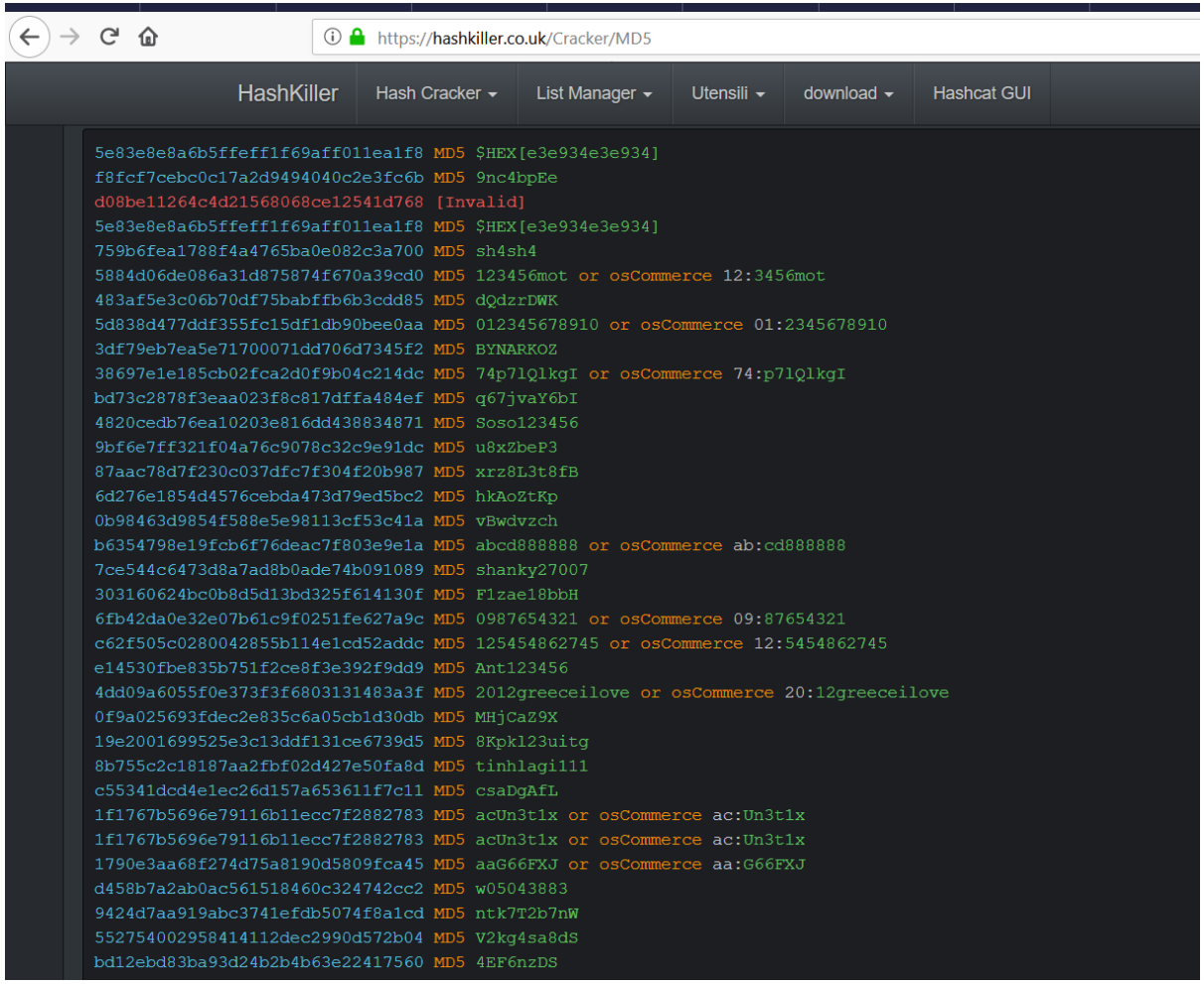


mediaservice.net
CORPORATE SECURITY & IMAGE

Esempio:


humor.co.il || 1410 Username+P
https://pastebin.com/9BhqVcSc
PASTEBIN
+ new paste
PRO
API
tools
faq
deals
search...
humor.co.il || 1410 Username+Password(MD5)+Email | by JM511
ISLAM-HACKER
JUL 21ST, 2014
1,693
NEVER
Not a member of Pastebin yet? Sign Up, it unlocks many cool features!
text 107.46 KB
raw
download
clone
1410 Username + Password(MD5) + Email
OF www.humor.co.il ..!!
Greeting to : NOK511 , Shi5 AlHacker , Fly1 InDooMe , Sarbot511 , ALM511 , NetBoy511 , p0c , AlQaTaRi
By JM511 /\ twitter.com/JM511 /\ jm511com@gmail.com
========== ENJOY MOTHER FUCKER ==========
[1] ������ : 5e83e8e8a6b5ffeff1f69aff011ea1f8 : ofer_a_i@netvision.net.il
[2] HotGod : f8fcf7cebc0c17a2d9494040c2e3fc6b : ddddddddddddd@hotmail.co.il
[3] BooBtult : d08be11264c4d21568068ce12541d768 :
[4] ������ : 5e83e8e8a6b5ffeff1f69aff011ea1f8 : ofer_a_i@netvision.net.il
[5] ��������� : 759b6fea1788f4a4765ba0e082c3a700 : ofer_a_i@netvision.net.il
[6] ���� : 5884d06de086a31d875874f670a39cd0 : rsm23des@yahoo.com
[7] PrailloLa : 483af5e3c06b70df75babffb6b3cdd85 : test@skype-new.mobi
[8] Bioxiarahlaxy : 5d838d477ddf355fc15df1db90bee0aa : hacked@lolololo.com
[9] doromcky : 3df79eb7ea5e71700071dd706d7345f2 : sample@email.tst
[10] ajmjtwrzvl : 38697e1e185cb02fca2d0f9b04c214dc : vsuppo@klinxuxpgr.com
[11] ugpydarorr : bd73c2878f3eaa023f8c817dffa484ef : iel@yselectu.com
[12] Yugosf13 : 4820cedb76ea10203e816dd438834871 : yannuo19801027@gmail.com
[13] veslvivua : 9bf6e7ff321f04a76c9078c32c9e91dc : veslvivuaua@yandex.ru

Esempio:


https://hashkiller.co.uk/Cracker/MD5
HashKiller
Hash Cracker
List Manager
Utensili
download
Hashcat GUI
5e83e8e8a6b5ffeff1f69aff011ea1f8 MD5 $HEX[e3e934e3e934]
f8fcf7cebc0c17a2d9494040c2e3fc6b MD5 9nc4bpEe
d08be11264c4d21568068ce12541d768 [Invalid]
5e83e8e8a6b5ffeff1f69aff011ea1f8 MD5 $HEX[e3e934e3e934]
759b6fea1788f4a4765ba0e082c3a700 MD5 sh4sh4
5884d06de086a31d875874f670a39cd0 MD5 123456mot or osCommerce 12:3456mot
483af5e3c06b70df75babffb6b3cdd85 MD5 dQdzrDWK
5d838d477ddf355fc15df1db90bee0aa MD5 012345678910 or osCommerce 01:2345678910
3df79eb7ea5e71700071dd706d7345f2 MD5 BYNARKOZ
38697e1e185cb02fca2d0f9b04c214dc MD5 74p7lQlkgI or osCommerce 74:p7lQlkgI
bd73c2878f3eaa023f8c817dffa484ef MD5 q67jvaY6bI
4820cedb76ea10203e816dd438834871 MD5 Soso123456
9bf6e7ff321f04a76c9078c32c9e91dc MD5 u8xZbeP3
87aac78d7f230c037dfc7f304f20b987 MD5 xrz8L3t8fB
6d276e1854d4576cebda473d79ed5bc2 MD5 hkAoZtKp
0b98463d9854f588e5e98113cf53c41a MD5 vBwdvzch
b6354798e19fcb6f76deac7f803e9e1a MD5 abcd888888 or osCommerce ab:cd888888
7ce544c6473d8a7ad8b0ade74b091089 MD5 shanky27007
303160624bc0b8d5d13bd325f614130f MD5 F1zae18bbH
6fb42da0e32e07b61c9f0251fe627a9c MD5 0987654321 or osCommerce 09:87654321
c62f505c0280042855b114e1cd52addc MD5 125454862745 or osCommerce 12:5454862745
e14530fbe835b751f2ce8f3e392f9dd9 MD5 Ant123456
4dd09a6055f0e373f3f6803131483a3f MD5 2012greeceilove or osCommerce 20:12greeceilove
0f9a025693fdec2e835c6a05cb1d30db MD5 MHjCaZ9X
19e2001699525e3c13ddf131ce6739d5 MD5 8Kpkl23uitg
8b755c2c18187aa2fbf02d427e50fa8d MD5 tinhlagi111
c55341dcd4e1ec26d157a653611f7c11 MD5 csaDgAfL
1f1767b5696e79116b11ecc7f2882783 MD5 acUn3t1x or osCommerce ac:Un3t1x
1f1767b5696e79116b11ecc7f2882783 MD5 acUn3t1x or osCommerce ac:Un3t1x
1790e3aa68f274d75a8190d5809fca45 MD5 aaG66FXJ or osCommerce aa:G66FXJ
d458b7a2ab0ac561518460c324742cc2 MD5 w05043883
9424d7aa919abc3741efdb5074f8a1cd MD5 ntk7T2b7nW
5527540029584141l2dec2990d572b04 MD5 V2kg4sa8dS
bd12ebd83ba93d24b2b4b63e22417560 MD5 4EF6nzDS

Cosa possiamo fare per difenderci?

Utenti

NON RIUTILIZZARE LE PASSWORD

Impostare password molto lunghe (15+ caratteri)

Abilitare, dove possibile, l'autenticazione a due fattori

Sistemisti, utenti VIP, account privilegiati ecc:

Usare password generate, di almeno 20 caratteri, diverse per ogni sistema

Preferire sistemi di autenticazioni differenti dalla password ove possibile (es: chiavi ssh, smartcard, ecc)

Un password manager sicuro è d'obbligo!

Considerate l'uso di caratteri non ASCII! (Unicode 65535 caratteri vs 255)
ES: à,è,è,ì,ò,ù per noi italiani (sono già sulla tastiera ☺)
Purtroppo non sono sempre accettati ☹

mediaservice.net
CORPORATE SECURITY & IMAGE

Cosa possono "fare" per difenderci

Sistemisti

Forzate password policy strong ai vostri utenti (15+ caratteri meglio, ma mai sotto i 12) con complessità (caratteri speciali, numeri e lettere)

Security

Periodicamente, programmate un Assessment delle password di dominio o dei sistemi critici per individuare eventuali credenziali deboli e segnalatele!

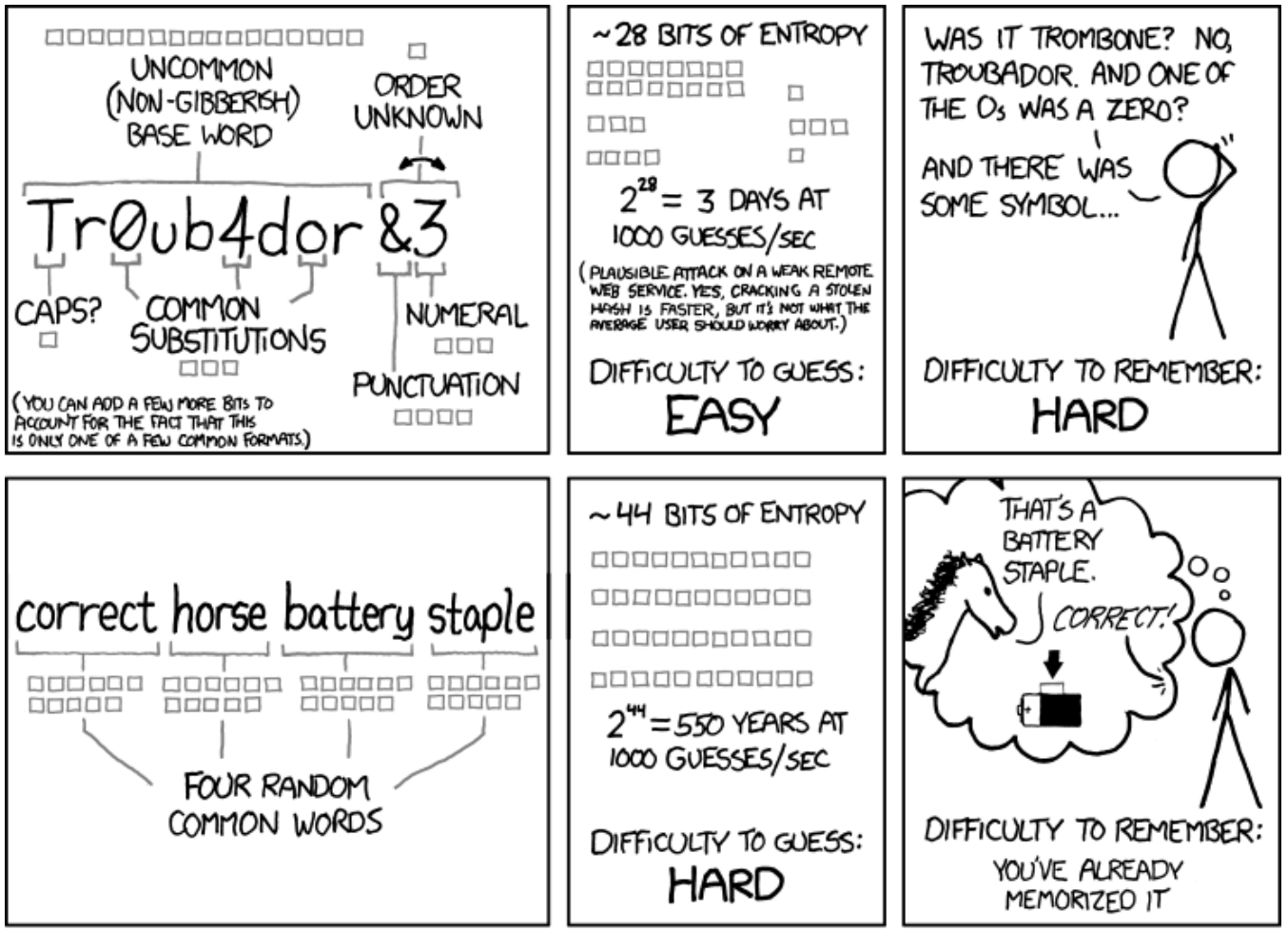
Sviluppatori, designer ecc:

Nelle vostre applicazioni, permettete il range di caratteri più ampio possibile (Unicode!) e lunghezza a 255 (perché limitarla?).

Usate algoritmi di cifratura strong! (es: blowfish, scrypt….).

mediaservice.net
CORPORATE SECURITY & IMAGE

Domande?


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor&3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS:
EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER:
HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS:
HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER:
YOU'VE ALREADY MEMORIZED IT
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.