RANSOMWARE ED ESFILTRAZIONE DATI:

QUANTA PAURA AVETE?

WHO AM I? WHO WE ARE?

Mi chiamo Alessandro, molti mi chiamano “**The Phoenix**”, ho una società di Cybersecurity da 17 anni, opero nel campo dal 1994 e sono uno degli Admin della più grande community d’Italia di Hacking Etico assieme al fondatore Eugenio Fontana ed agli altri 2 moderatori, Francesco Ressa e Davide Pizzuto.

Noi siamo EHI: **ETHICAL HACKER ITALIANI**

La nostra mission? Far crescere il Paese

Operiamo sul campo quotidianamente e passiamo la nostra vita a bucare e proteggere le reti. Ci siamo resi conto da tempo della mancanza di competenze o sensibilità delle Aziende in fatto di security e spesso della lassità o incapacità dei colleghi di innalzare il loro livello di competenze per i più svariati motivi: economici, mancanza di stimoli ecc.

Abbiamo quindi provato a mettere insieme una Community gratuita con un alto filtraggio sui suoi membri (su Facebook) per crescere tutti insieme ed abbiamo creato dei corsi a bassissimo costo, ma di alta qualità, messi sulla nostra piattaforma personalizzata, per cercare di innalzare il livello medio dell'IT italiana. Abbiamo scartato "Guru" mancanti di empatia e ci siamo tenuti chi non si è dimenticato di essere stato niubbo 30 anni fa. Le competenze si trovano ad alto livello, la capacità di trasmettere e l'umiltà, molto meno.

Perchè?

La risposta è semplice: Prima o poi vi bucheranno. Toglietevi dalla testa l'idea di essere immuni. Siete solo fortunati, ma l'onda arriverà. Siete pronti? No. Fidatevi. Non lo siete. Perchè passo una parte del tempo in aziende messe in ginocchio dal ransomware. Le ultime due, sommate, arrivavano a 870MLN di € l'anno di fatturato. Pensate che fossero sprovveduti? NO. Non erano pronti.

Quando vi bloccano oggi, avete 2 problem: sbloccare e ripartire e gestire la Perdita di dati esfiltrati. (che è la cosa peggiore).

Il 95% degli attacchi oggi parte da una mail di phishing.

Le nuove tecniche di phishing

- Usano il Social Engineering
- Simulano interesse
- Usano empatia
- Fanno leva sul «Senso di Urgenza»

- Vengono acquistati domini reali ed a volte omografici quindi le mail che arrivano sono reali e non più spam.

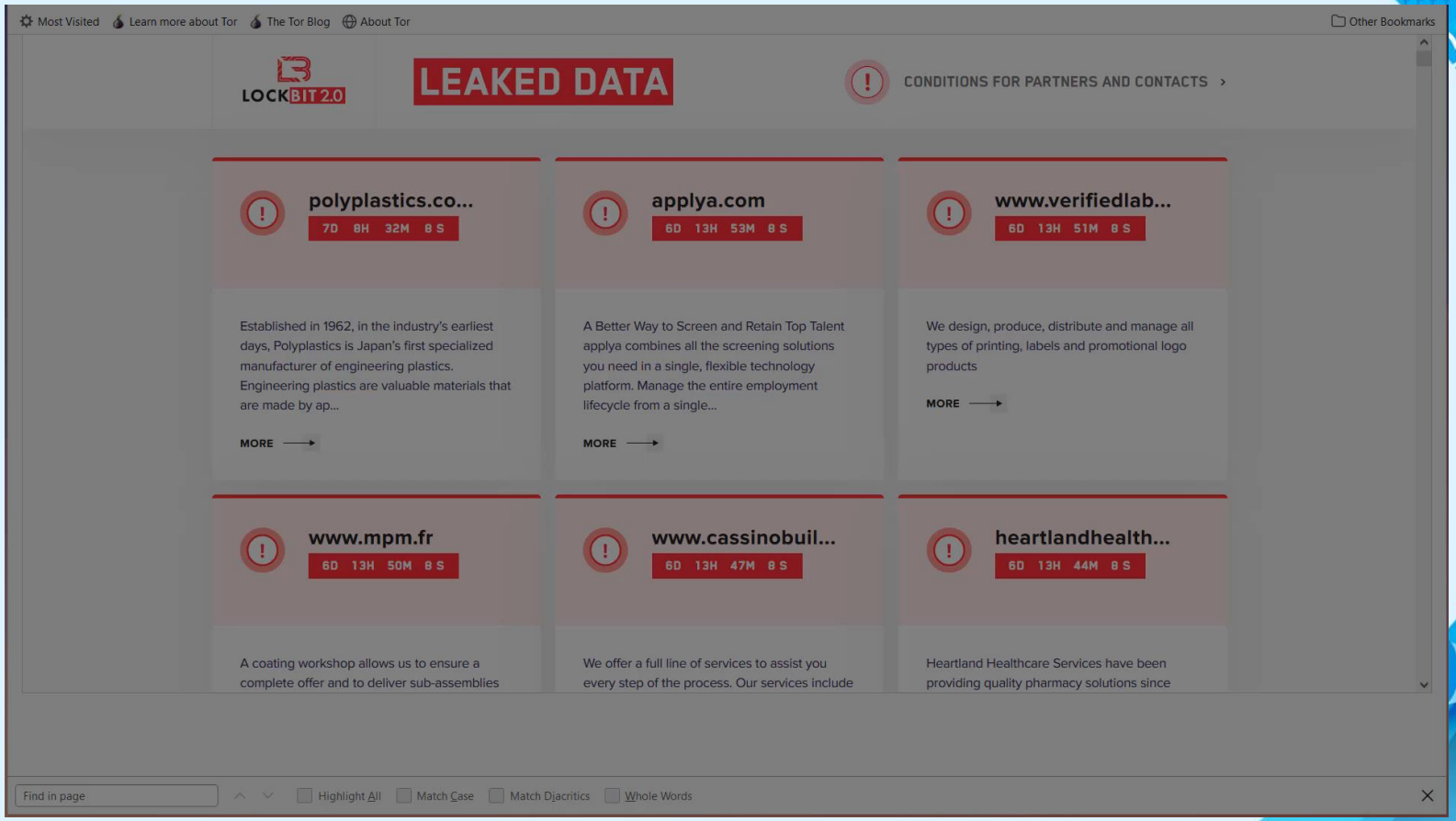
Siete in grado di capire il data breach?

La risposta anche in questo caso è NO. Spesso chi attacca si posiziona all'interno della vostra struttura molto prima dell'attacco. Lo Lancia quando ha preparato tutto. Cancella i log, si crea account amministrativi perfino sui firewall e vi chiede 2 riscatti.

1) per sbloccarvi i dati
2) quando avete pagato, per evitare di pubblicarveli

Se i vostri dati vanno online, come società siete FINITI. Perchè anche se avete comunicato al Garante il breach, i vostri clienti vi faranno inevitabilmente causa.

Una piccola dimostrazione:



Noi siamo come Cassandra

Sindrome di Cassandra? no grazie.

Sembra che gli Hacker Etici, i Blue Teamer e gli esperti di sicurezza siano lì pronti per mettervi paura e per sminuire il Vs operato. Non è così! Non vogliamo crearci lavoro, non lesiniamo problem per vivere! Vorremo un mondo in cui i Black Hat non lavorano più. L'unico modo? Avere un'idea reale di come siete posizionati con la VS Security

E poi c’è quello che non tutti sanno..

Complotti? ma quali complotti, i nostri dati sono VERAMENTE disponibili

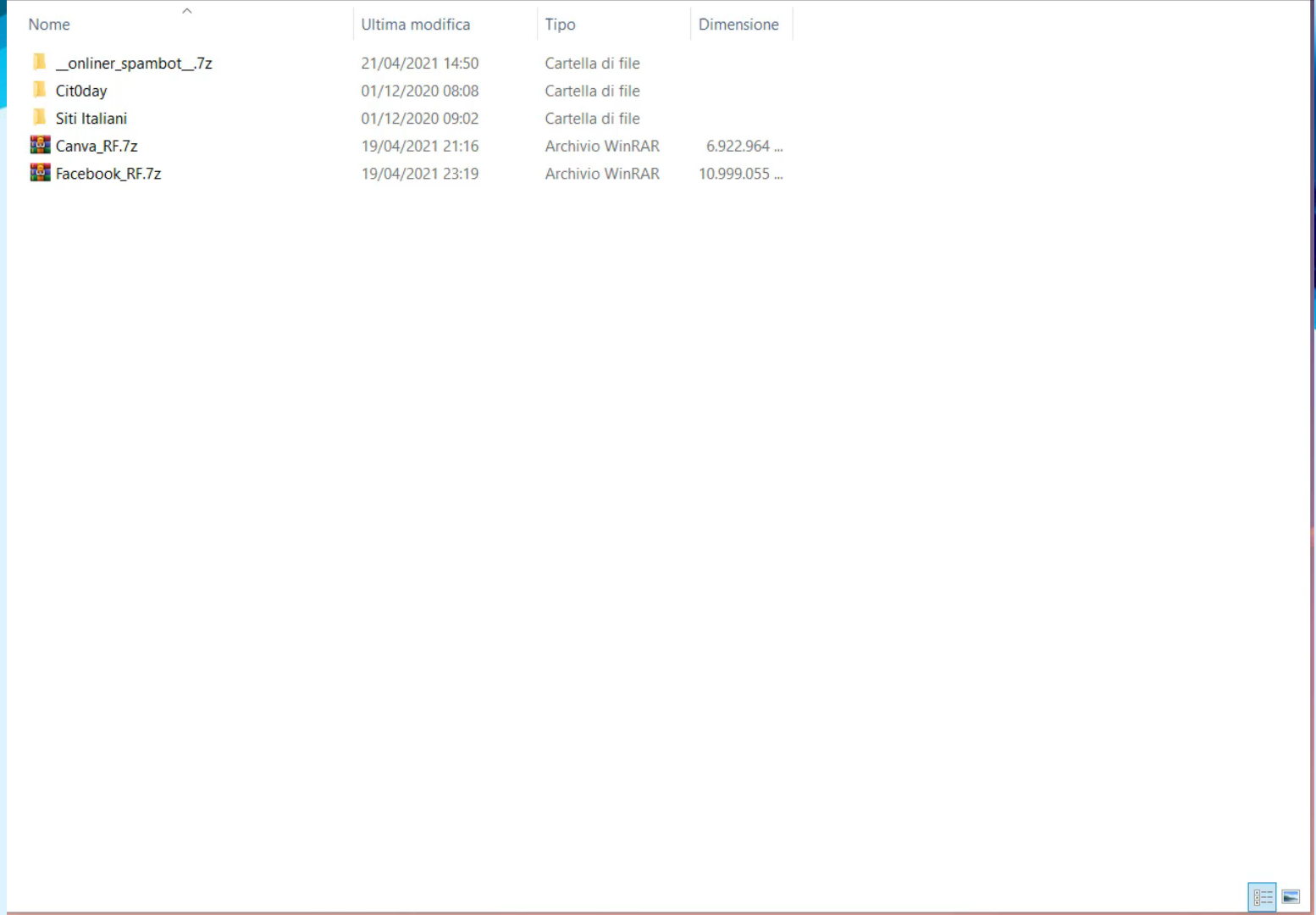
A Novembre 2020

23.000 Databases
13 Miliardi di Utenti
266 Milioni di Password

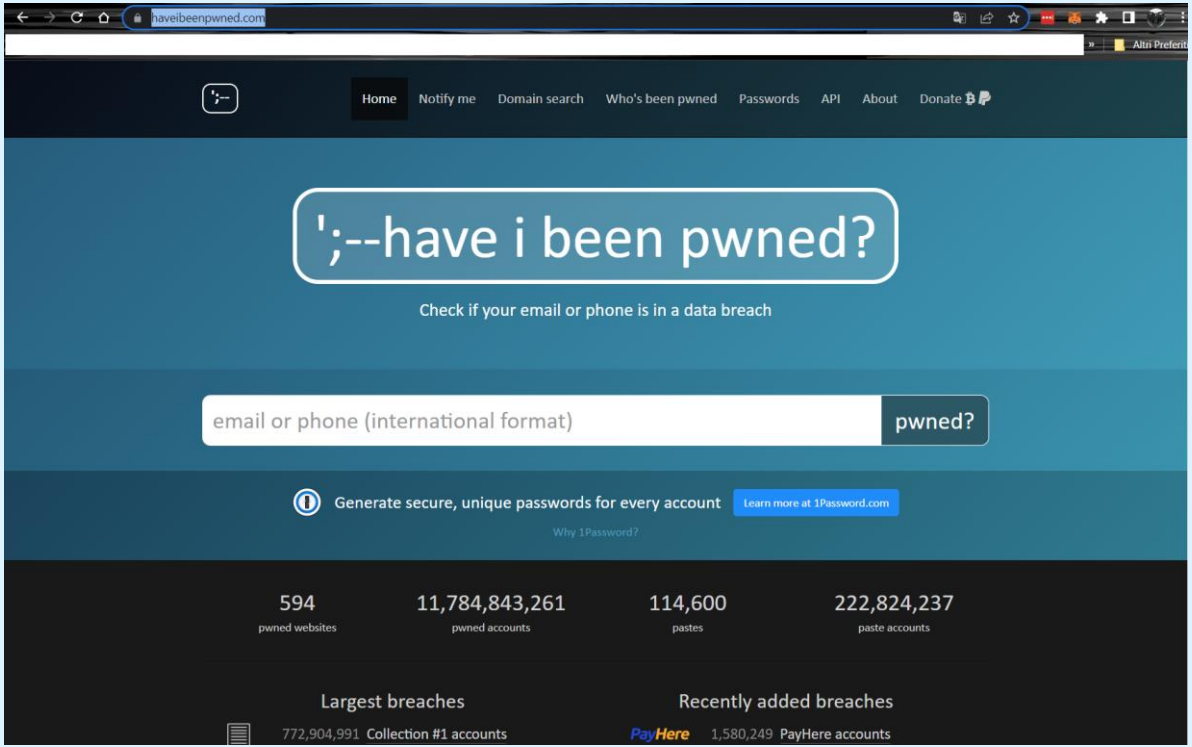
Piccolo esempio pratico?

Il cit0day

- https://www.troyhunt.com/inside-the-cit0day-breach-collection/
- https://gist.github.com/gvolluz/dd0df2ba2400c4891f95d05de3dde1da

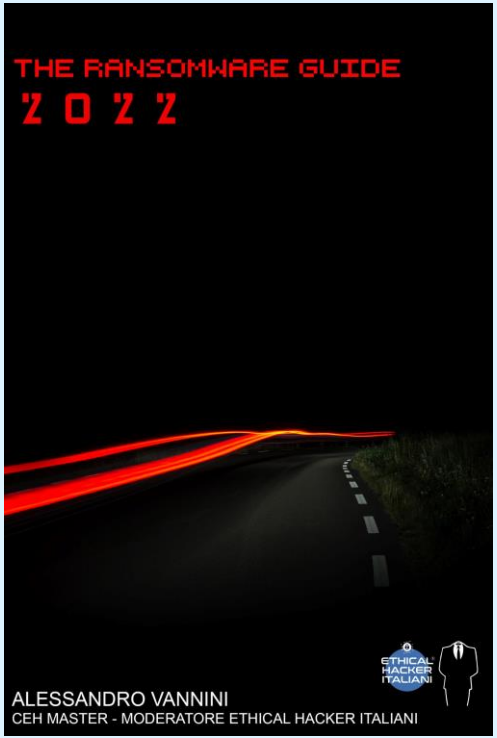

Nome
Ultima modifica
Tipo
Dimensione
__onliner_spambot__.7z
21/04/2021 14:50
Cartella di file
Cit0day
01/12/2020 08:08
Cartella di file
Siti Italiani
01/12/2020 09:02
Cartella di file
Canva_RF.7z
19/04/2021 21:16
Archivio WinRAR
6.922.964 ...
Facebook_RF.7z
19/04/2021 23:19
Archivio WinRAR
10.999.055 ...

https://haveibeenpwned.com/



Siete stati violati? Al 99% la vostra mail lo sarà per forza di cose. E allora? controllo e cambio le password!

Vi lasciamo un piccolo aiuto..



La Guida RANSOMWARE 2022!

L’ho appena aggiornata, chiedetela agli organizzatori!

Volete un consiglio? un parere? Crescere in autonomia?
Venite sulla nostra Community!

https://www.facebook.com/groups/160773531196286

Sul Canale Youtube

https://www.youtube.com/channel/UCabO9wlI3dBygaqhngn-5tA

O sulla nostra Piattaforma di Learning!

https://ethicalhackeritaliani.it

..se invece ci volete «professionalmente», scriveteci a info@ethicalhackeritaliani.it

Gr4z1€!
D3l|4 V05tR4
4Tt3nz10N3!