

2016 RECAP

Rivediamo insieme alcuni degli eventi
digitali dell'anno passato

Liceo Serpieri, 14 febbraio 2017

Pietro Albini

Liceo Serpieri, 5H scienze applicate

www.pietroalbini.org

pietro@pietroalbini.org

[@pietroalbini](#) su Telegram

Tante cose sono successe
nel 2016

Alcuni eventi però non hanno
ricevuto abbastanza attenzione

L'iPhone di S. Bernardino

2 dicembre 2015

Attacco terroristico a S. Bernardino, in California

L'attentatore aveva un iPhone,
e l'FBI voleva il contenuto

Problema:
gli iPhone sono criptati

Problema più grave:
alcuni si resettano se sbagli PIN

L'FBI aveva anche disattivato il
backup online per sbaglio

Una corte ordina ad Apple di
decrittare il contenuto

Apple si rifiuta

La giustizia americana è basata
sul precedente

Se Apple decrypta quello
smartphone, allora è legale farlo

È come obbligare
un costruttore di lucchetti
a sbloccare una serratura

Questo avrebbe creato un
precedente enorme

Un giudice di New York aveva
dichiarato di voler decriptare
altri 140 iPhone

Una corte avrebbe potuto
ordinare a qualsiasi azienda di
decriptare i loro prodotti

Questo significa legalizzare le
backdoor

Quale migliore occasione di un
attentato terroristico?

Cos'è una backdoor?

Una backdoor è qualcosa che
permette di aggirare
i meccanismi di sicurezza

Una backdoor è creata per
essere usata teoricamente solo
da certe persone

teoria \neq pratica

\$8 key opens NYC to terror

Subways, elevators vulnerable

By SUSAN EDELMAN

Master keys for every elevator in the city, major construction sites, subways and skyscrapers are being freely sold online, despite a city law that makes it illegal for unauthorized persons to possess them.

A New Jersey-based lock company is peddling an unlimited supply of New York City's "1620" fire service keys on eBay at \$15.50 for two.

Access to the Big Apple keys is sharply restricted. It's unlawful for anyone other than firefighters, law-enforcement personnel, elevator contractors or inspectors and building owners to have them.

But a Post reporter bought two keys to the city with no questions asked from UltimateSecurityDevices.com, an online arm of Northeast Lock Corp. in Clifton, N.J.

The keys unlocked elevator control panels in a Midtown high-rise.

"It's kind of scary," said the building's fire-safety director.

A veteran firefighter called the sale of a potential terrorist tool "disturbing."

"That key gives access to elevator banks. Someone could take over the elevators in a high-rise building. In the wrong hands, you can see the problem," he said.

The key could be used to trap people in a skyscraper by sending all the elevators to the lobby and out of service, experts say. It can also be used to control any individual elevator. Every elevator in the city is required to be fitted with a lock for the 1620 key.

In addition, the keys open lock boxes at construction sites and other buildings, leaving them open to theft, vandalism and sabotage. The lock boxes contain other keys to the site — such as ones to open gates and entrances — to give firefighters access in an emergency.

They also open subway entrance gates. The FDNY issues 1620 keys to all firefighters. "If you lose it, there's paperwork. It's like losing your ID card — it's a serious thing," one said. "When you

leave or retire, you hand it back in."

UltimateSecurityDevices offers 1620 keys at \$7.40 each for up to nine, and \$6.66 each for 10 or more. Any order over \$249 comes with a 10 percent discount.

A request for comment from City Hall was not answered.

The City Council amended local law in 2013 to make it illegal for unauthorized people to possess the 1620 or "citywide standard key."

"If you're selling it, it's in your possession for an unlawful reason," said City Councilmember Elizabeth Crowley, chairwoman of the Fire and Criminal Justice committee. "I can't see a real locksmith [being] willing to jeopardize his career and the safety of others for a few bucks."

Kevin McCallen, owner of Northeast Lock and UltimateSecurityDevices, did not return messages.

susan.edelman@nypost.com



Le backdoor sono pericolose,
e non vanno create

Una volta che diventano
pubbliche, è impossibile inibirle

Domande?

AlphaGo

9-15 marzo 2016

AlphaGo batte Lee Sedol 4-1

AlphaGo è un software
creato da Google

Grazie alle reti neurali, è riuscito
a battere uno dei campioni
mondiali di Go **senza handicap**

Questo è un evento storico

Il Go è uno tra i giochi da tavola
più complessi mai creati

Creato in Cina 2500 anni fa

Il gioco si svolge su una
scacchiera 19x19, con "pietre"
bianche e nere

L'obiettivo è controllare la
maggior parte della scacchiera

In Cina, Giappone e Corea è
quasi sport nazionale

Esistono scuole in cui i bambini
per decenni si allenano

Perché è complesso che un computer vinca a questo gioco?

Ci sono **troppe** possibili mosse
da analizzare

Una mossa può avere effetti
anche 100 turni dopo

Ci sono più partite possibili che
atomi nell'universo conosciuto

Com'è possibile che AlphaGo
abbia vinto?

Reti neurali

Software che, simulando la struttura del cervello umano, sono in grado di apprendere

AlphaGo ha imparato vedendo
milioni di partite di Go, poi
giocando contro se stesso

Questo gli permette di valutare
le mosse come farebbe un
giocatore professionista

Questa è una pietra miliare nella
storia dell'informatica

Domande?

Ashley Madison

Ashley Madison è un sito per
persone insoddisfatte

I dati che salva devono essere
tenuti sicuri, perché sono
leggermente compromettenti

18-20 agosto 2016

Il database di Ashley Madison
viene pubblicato

Questo è un fatto sconvolgente
per la vita degli utenti del sito

Mogli e mariti potevano sapere
di esser stati traditi

In America, ci sono stati più
suicidi causati da questo evento

Ma cosa è stato trafugato?

Tutti i profili degli iscritti

Nomi utenti e password

Questa password può essere
usata per compromettere altri
account

Tutto ciò non succede solo su
Ashley Madison

Ogni anno, decine di siti
importanti subiscono attacchi
che rubano tutti i dati

Non puoi impedire che
succeda a te

L'unico modo è essere pronti

Non iscriversi a siti del genere
con i propri dati

Usare password diverse
per ogni sito

Usare un password manager
lastpass.com/it

Iscrivarsi a
Have I Been Pwned

Have I Been Pwned permette di
verificare se il proprio indirizzo
email è tra le vittime

[Home](#)[Notify me](#)[Domain search](#)[Who's been pwned](#)[Pastes](#)[API](#)[About](#)[Donate](#)  

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

pietro@pietroalbini.org

pwned?

Good news — no pwnage found!

No [breached accounts](#) and no [pastes](#) ([subscribe](#) to search sensitive breaches)



Notify me when I get pwned



Donate



Permette anche di ricevere email
quando accadono nuovi furti

Domande?

Bug bounties

5 luglio 2016

Ragazzo invitato al Pentagono
per aver hackerato i suoi siti

Non dovrebbe essere
condannato?

No, perché ha partecipato
a un bug bounty

Ogni sistema ha delle falle

Queste falle vengono trovate

Fino a qualche anno fa,
cosa si poteva fare
dopo averle trovate?

Rivenderle a criminali/nazioni

Dimenticare di averle trovate

Segnalarle all'azienda, e
rischiare la denuncia

Cosa faceva la gente?

Per questo sono nati i
bug bounty

Programmi in cui le aziende
permettono di testare
i loro siti web

E prevedono una ricompensa
dopo la segnalazione

Diverse aziende ne hanno
aperti quest'anno

Se trovi una vulnerabilità grave
su Google, ti ricompensano con
decine di migliaia di dollari

E ti permettono di pubblicare un
blog post sull'accaduto

Tornando alla notizia, anche il
Pentagono ha aperto
un bug bounty

Questo ragazzo è stato uno delle
centinaia di persone partecipanti

E ci sono stati centinaia di altri
bug trovati e segnalati

Ne ho trovato uno anch'io!



Gandi security vulnerability: two factor authentication bypass

Written on October 2, 2016.

[Gandi](#) is a French domain name registrar I use for all my domains, which also supports the volunteers behind some FLOSS projects. On Tuesday 27 september 2016 I found a flaw in their login form which allowed to completely bypass two factor authentication (2FA), after you inserted the right handle and password.

It all starts with a broken phone

The day before I found this vulnerability, my phone fell and hit the ground with the corner. The display is now fully cracked and the touch screen doesn't work anymore. I was very frustrated about this, because the other phone I have at home is an old, crappy Android phone (which doesn't work perfectly).

Everything on the phone was backed up, except one thing: the seeds of my 2FA tokens. For most of the sites I have the backup codes saved in my password manager, but Gandi doesn't provide those, and I was worried to be locked out of my account.

A vulnerability discovered out of frustration

I knew my Gandi account had 2FA enabled so, the day after, I went to their website looking for a way to access my account.

Domande?

Mirai

21 ottobre 2016

Mezzo internet smette di
funzionare

Attacco dei russi?

No, qualche centinaia
di migliaia di webcam

Adesso c'è la moda dei
dispositivi connessi a internet

Questi dispositivi sono **insicuri**

Mirai è un virus creato da un
americano per infettare questi
dispositivi

Esso crea una rete di dispositivi
controllati dal creatore di Mirai

E il 21 ottobre Mirai ha effettuato
un attacco ad uno dei nodi
centrali di internet

1.2Tbps di dati inviati da Mirai,
ogni secondo e non amplificati

Prima di Mirai, il record era
intorno a 400Gbps, amplificati

Mirai ha anche attaccato il blog
di un giornalista informatico con
600Gbps di dati

Come funziona?

Mirai scansiona tutto internet
alla ricerca di
dispositivi non protetti

Se ne trova uno, lo infetta e lo
rende sicuro, per impedire
infezioni di concorrenti

Una volta dato il comando, tutti i dispositivi inondano di richieste un sito internet

Questo sito internet non ha la
capacità di reggere il traffico

Mirai ha perso forza, ma tutti i
dispositivi insicuri venduti
peggiorano solo la situazione

Domande?

Grazie!

pietroalbini.org/talks/latest