Linux Day 2017

28 ottobre

Giornata nazionale a favore della diffusione del software libero e del sistema operativo GNU/Linux

Università degli Studi di Palermo
Viale delle scienze - Edificio 7
Aula Magna di Ingegneria
INGRESSO LIBERO

FREE CIRCLE

A.S.I.

https://linuxday.thefreecircle.org

Mi presento

Girolamo Daniele Bruneo

35 anni, Software Developer e Web Architect.
Da più di 15 anni nell'industria del web.

Appassionato di Linux, della filosofia Open Source e di Cyber Security. sempre pronto a supportare la condivisione e la diffusione della conoscenza.

Fondatore di "*Viral digital strategies*" e membro di Fablab Palermo.

FABLAB PALERMO

fablabpalermo.org

Viral digital strategies get infected

viralds.it

2017
Hacks, Data Breach, Data Leaks e Cyber Warfare

Gli eventi di cyber security
più rilevanti del 2017

(fino ad oggi)

G.D.Bruneo

Hacks

WannaCry

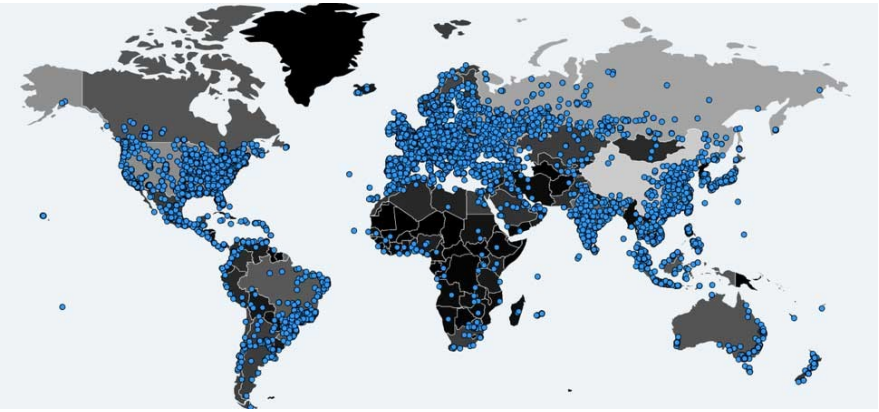
- Attacco massivo di tipo Ramsomware
  - Cripta i file e chiede un riscatto
- Malware di tipo Worm
  - Sfrutta per diffondersi EthernalBlue, una vulnerabilità per Windows trafugata dalla NSA

- Ha infettato i sistemi informatici di numerose aziende e organizzazioni in tutto il mondo, tra cui
  - Portugal Telecom,
  - FedEx, Telefónica,
  - Renault,
  - National Health Service
  - il Ministero dell'interno russo
  - l'Università degli Studi di Milano-Bicocca.

- Fermato grazie a un kill switch basato su un dominio

- 230K computer
- 150 paesi
- Ammontare riscatto: ~ € 300 in bitcoin

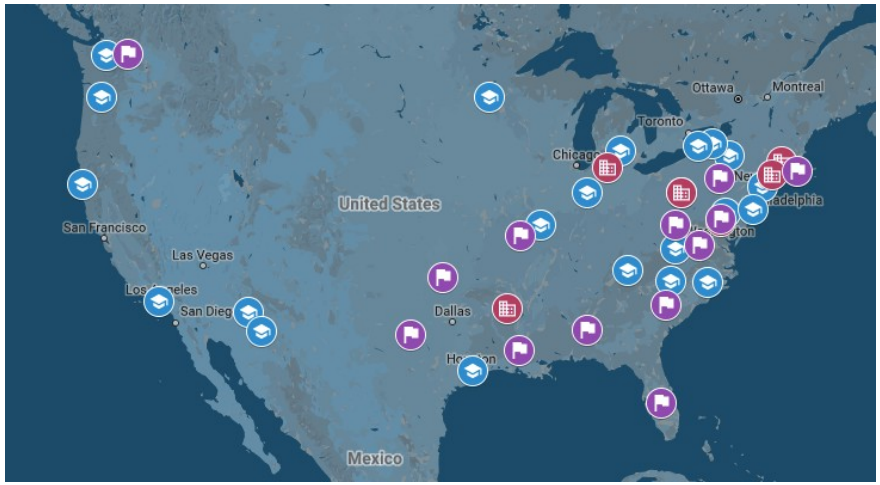
Maggio 2017



Hacker “Rasputin”

L'Hacker Rasputin
penetra in più di 60 database
di università e agenzie governative

- New York University
- University of Cambridge
- the City of Pittsburgh
- the U.S. Department of Housing and Urban Development
- the Fermi National Accelerator Laboratory".



Rasputin era divenuto famoso nel 2016 per avere avuto accesso al sistema di elezioni americano

Hack: SQL Injection

Autore: Rasputin

Febbraio 2017

Cellebrite – Phone cracking tool

Celebrite

- Compagnia che vende prodotti per accesso a smartphone all'FBI e a governi come:
  - Turchia
  - UAE
  - Russia
- Nota per avere aiutato l'FBI con lo sblocco dell'iPhone nel caso di San Bernandino CA

Hacker prendono possesso di:

- 900 GB di dati
- Databases
- Tool e tecniche per il cracking di iOS

Gennaio 2017

Freedom Hosting II

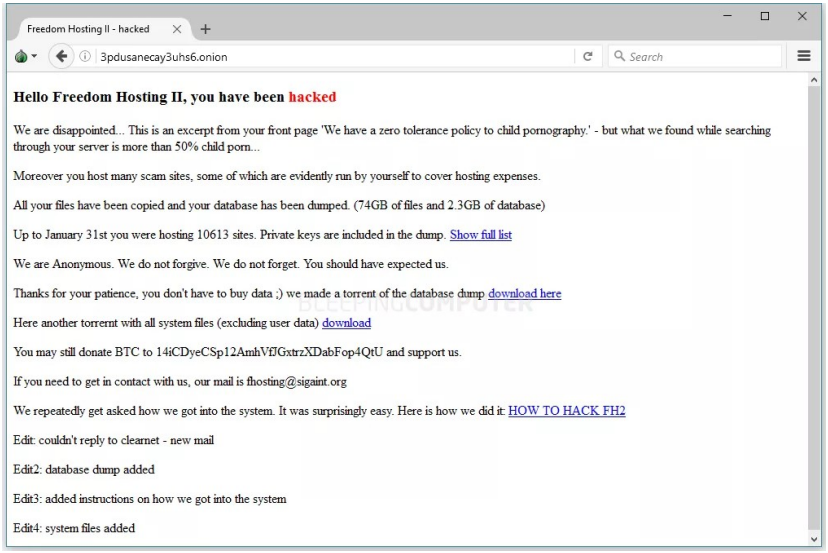
Freedom Hosting II

- Hosting Anonimo su TOR
- 10.000 siti ospitati
- 20% del traffico sul dark web
- 74 GB di dati
- 2.5 GB di database

Hack: Privilege escalation

Autore: Anonymous

Febbraio 2017



Freedom Hosting II - hacked

3pdusanecay3uhs6.onion

Hello Freedom Hosting II, you have been hacked

We are disappointed... This is an excerpt from your front page 'We have a zero tolerance policy to child pornography.' - but what we found while searching through your server is more than 50% child porn...

Moreover you host many scam sites, some of which are evidently run by yourself to cover hosting expenses.

All your files have been copied and your database has been dumped. (74GB of files and 2.3GB of database)

Up to January 31st you were hosting 10613 sites. Private keys are included in the dump. Show full list

We are Anonymous. We do not forgive. We do not forget. You should have expected us.

Thanks for your patience, you don't have to buy data ;) we made a torrent of the database dump download here

Here another torrernt with all system files (excluding user data) download

You may still donate BTC to 14iCDyeCSp12AmhVfJGxtrzXDabFop4QtU and support us.

If you need to get in contact with us, our mail is fhosting@sigaint.org

We repeatedly get asked how we got into the system. It was surprisingly easy. Here is how we did it: HOW TO HACK FH2

Edit: couldn't reply to clearnet - new mail

Edit2: database dump added

Edit3: added instructions on how we got into the system

Edit4: system files added

Virgin America

Hacker ottiene accesso
a **3.120 account** della corporate network di Virgin America

- Login
- Password
- Indirizzi
- Email
- Social Security Numbers

Hack: -

Autore: -

Agosto 2017

Edmodo

Edmodo
piattaforma di education

- Hacker accede al database
  e lo mette in vendita sul dark web
- 77 milioni di account
  - Username
  - Email
  - Hashed password

Hack: -

Autore: -

Maggio 2017

Confindustria truffata per 500K

"Sposta subito mezzo milione su questo conto estero".

"Caro Gianfranco, dovresti eseguire un bonifico di mezzo milione di euro su questo conto corrente.
Non mi chiamare perché sono in giro con il presidente e non posso parlare".

Hack: Mail spoofing – Social Engineering

Autore: -

Settembre 2017

Dallas Emergency Sirens System

Hacker prende il controllo e attiva il sistema di sirene di emergenza di Dallas

- Registra il segnale radio e gli basta ripeterlo per attivare il sistema

Hack: Radio signal spoofing

Autore: -

Aprile 2017

IDEAL
MODEL SMALL
STACK 100h
DATASEG
CODESEG
Begin:
MOV AX, @data
MOV DS, AX
MOV DX, OFFSET HW
MOV AH, 09H
INT 21H
MOV AX, 4C00H
INT 21H
END Begin

Data breach

MOV AH,09
INT 21H
POP AX
return sys;
.model small
stack
data
message db "Connecting...

CloudPets

CloudPets

- Internet connected Teddy Bears
- Registrano conversazioni vocali di bambini e adulti

Dati esposti:

- 2 mln di registrazioni vocali
- 800k account (email e password)

Breach: dati accessibili pubblicamente

un database MongoDB era esposto senza alcuna autenticazione o firewall

Febbario 2017

Sogel – Fatture elettroniche

Sistema di trasmissione delle fatture elettroniche all'Agenzia delle Entrate

Una falla ha permesso a chiunque avesse le credenziali per entrare, commercialisti o anche semplici contribuenti, e per non si sa quanto tempo, di consultare liberamente i dati fiscali degli altri cittadini.

Tutti i dati trasmessi all'Agenzia delle entrate, compresi quelli di clienti e fornitori.

Breach: dati accessibili pubblicamente effettuando una ricerca

Settembre 2017

US Voters Data

Deep Root Analytics

- Compagnia di Analisi Dati

Dati esposti:

- Dati su 200 mln di votanti Americani
- 1 TB di dati
  - Nomi
  - Date di nascita
  - Indirizzi
  - Etnia e religione “stimate”

Breach: dati accessibili tramite web storage Amazon S3 esposto al pubblico

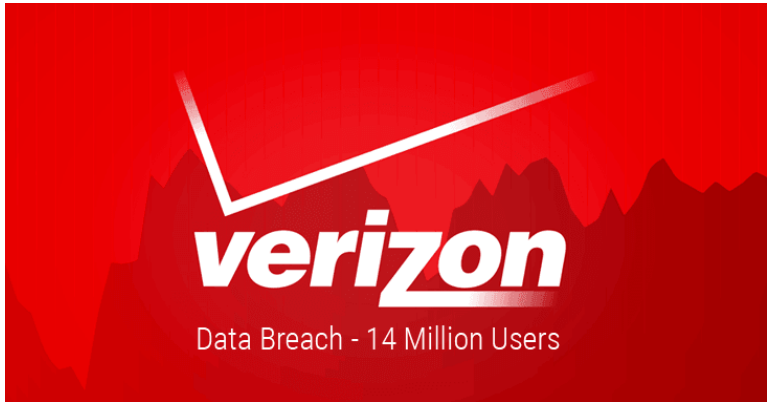
Giugno 2017

RNC_RegID	State	2012ObamaVoter_DRA_12_16	2012RomneyVoter_DRA_12_16	2016ClintonVoter_DRA_12_16	2016TrumpVoter_DRA_12_16	AmericaFirstForeignPolicy_agree_DRA_...	AmericaFirstForeignPolicy_disagree_DR...	AutoCompaniesShipJobsOver
{-4846-9310-B219917E9098}	AK	0.063016	0.571314	0.053027	0.551194	0.602687	0.169557	0.464875
{>4988-A7E9-E33CA7ID52BE}	AK	0.053668	0.707244	0.050368	0.710313	0.481612	0.177465	0.331644
-4E64-81DC-AF1047EFF0D5}	AK	0.084698	0.366629	0.084682	0.501998	0.377841	0.204837	0.318368
{>463D-9033-FFFB4469279*}	AK	0.055057	0.806223	0.04669	0.744124	0.479264	0.167188	0.35108
{^94B1-A9B7-4CFC3E94A585}	AK	0.066218	0.469906	0.061771	0.603631	0.484545	0.155052	0.408957
{-4D8E-93BF-2A2B31F47617}	AK	0.270389	0.145265	0.263194	0.260338	0.322196	0.187472	0.29259
{-4CBD-89C6-3A85C741E7E7}	AK	0.310231	0.17945	0.277853	0.265422	0.44298	0.244778	0.376611
{-4E91-9E58-DED971C380F6}	AK	0.703669	0.053965	0.708858	0.08392	0.313643	0.307473	0.29446
{^42F3-8C8C-47B65E58C9C0}	AK	0.369552	0.120109	0.377402	0.24179	0.443629	0.294659	0.383681
{^49F9-A32A-7F63A60A1B84}	AK	0.05925	0.797582	0.052514	0.773824	0.501335	0.168872	0.343528
{-444D-8652-5029581AC85A}	AK	0.055432	0.706105	0.051108	0.755157	0.505331	0.179509	0.41664
8-4483-AA10-EC4A4C0ED468}	AK	0.058641	0.708128	0.048693	0.703338	0.506371	0.172593	0.321626
-4CA5-A710-190A66391A42}	AK	0.052957	0.790685	0.051408	0.763825	0.51226	0.17224	0.341513
-47C8-BF61-92AC63AAF52A}	AK	0.364036	0.110677	0.355915	0.16711	0.365308	0.303395	0.328733
{-4FC7-93F0-E7A9A52B5927}	AK	0.082728	0.543524	0.077666	0.532271	0.503128	0.170274	0.343845
{-46FF-AB03-4FEA5185E6ID}	AK	0.722743	0.059612	0.708182	0.090227	0.335643	0.340255	0.414711
{>4163-B982-E6DFA1016AF4}	AK	0.053129	0.76351	0.049686	0.675581	0.515356	0.165555	0.288988
-4D3A-A963-1BE9F3539285}	AK	0.735015	0.058311	0.695729	0.090247	0.291987	0.416227	0.379467
r41D3-B6F2-6F474CFFB1C2}	AK	0.373483	0.116215	0.366706	0.186676	0.45696	0.235871	0.37697
-4104-4A8A-275270A853F9}	AK	0.263161	0.139569	0.241241	0.190559	0.343729	0.270333	0.385123
{-45DB-8D71-8736ZEB1DC2A}	AK	0.199837	0.233243	0.190505	0.437843	0.499198	0.167191	0.396062
{-4E8A-B577-391978E95255}	AK	0.279332	0.171205	0.254128	0.246832	0.31401	0.289612	0.294014
{-4A7A-813C-F7DB3A44AF17}	AK	0.064943	0.493935	0.059796	0.616545	0.495759	0.181181	0.378552
{-41D2-958C-F5C5F0B901B7}	AK	0.084982	0.485015	0.080543	0.545057	0.468451	0.178103	0.374171
{>4256-A5B5-E9AC7380C4B}	AK	0.110371	0.254286	0.121428	0.343682	0.459141	0.262414	0.37164
{>4F4E-A8A4-8F5AAD8E2DE5}	AK	0.481394	0.082207	0.469467	0.140254	0.336325	0.234048	0.389701
{^4394-B6D8-20E57DAA58B8}	AK	0.80217	0.06407	0.692983	0.088118	0.273626	0.261091	0.328082
-41D9-BCC7-7985ID4D7E69}	AK	0.053448	0.769965	0.050236	0.65751	0.5501	0.171422	0.347657
-446B-B95F-4852FA6C0FEA}	AK	0.067747	0.467848	0.101971	0.509767	0.420752	0.198149	0.29413
{-4047-82BE-5D9C7B24FAD4}	AK	0.178756	0.266768	0.155978	0.312251	0.46878	0.204695	0.338451
-4985-B1B8-2408241FB8C}	AK	0.075435	0.635886	0.072049	0.674178	0.475957	0.168529	0.357108
{-4CEA-8D4D-82842224488B}	AK	0.23698	0.524954	0.204902	0.292266	0.414051	0.212404	0.369967
-42DA-8F78-EC468BA14AF4}	AK	0.057559	0.73754	0.05013	0.605205	0.493792	0.170646	0.296392
-4661-6D6F-E98FFFA85743}	AK	0.067158	0.72232	0.054613	0.593721	0.451352	0.182517	0.27888
{>4B1B-A646-998B261321591}	AK	0.057108	0.729993	0.053337	0.632087	0.488812	0.165229	0.279291
{>4B21-8D70-877621694163}	AK	0.090304	0.318752	0.096251	0.339416	0.509206	0.161856	0.403844
{-4E04-A2FC-C3DF8F0C3DD3}	AK	0.055334	0.792398	0.052621	0.76517	0.467659	0.175858	0.274614
{-48DC-6448-8F6461585740}	AK	0.707157	0.176567	0.197694	0.31981	0.564353	0.245346	0.328487

Verizon

Verizon

- Compagnia di telecomunicazioni
- Più di 150 mln di clienti



Dati esposti:

- Dati su 14 mln di account
  - Numeri di telefono
  - Nomi
  - Codici PIN

Breach: dati accessibili tramite web

a causa di una configurazione di sicurezza errata
uno storage Amazon S3 è stato esposto al pubblico

Giugno 2017

Cloudbleed

Cloudflare

- Servizio di CDN
- Serve più di 5mln di siti web
- Uber, Zendesk, OkCupid, 4chan...

Dati esposti:

- 3 mln di richieste HTTP
- Potenzialmente:
  - Password
  - Messaggi privati
  - Sessioni private

Breach: dati accessibili tramite web sessioni private sono state cachate inavvertitamente a causa di un bug

Febbraio 2017

Sabre – Reservation System

Sabre System

- Reservation Software Company
- Usata da Hotel e Compagnie Aree
- Compagnie come Hard Rock Hotel, Google e proprietà di Trump.

Dati esposti:

- Dati di Carte di credito non criptati
- Dettagli di prenotazioni
- 15% delle prenotazioni sono state spiate

Breach: dati accessibili tramite web senza autenticazione

Agosto 2016 - Marzo 2017

TigerSwan – CV mercenari

TigerSwan
Compagnia di mercenari USA

TigerSwan
Solutions to Uncertainty®

Dati esposti:

- Curriculum di migliaia di mercenari
  - Indirizzi
  - Numeri di telefono
  - Email
  - Passaporti
  - Social Security number
  - Contatti di alte cariche militari

Breach: dati accessibili tramite web storage Amazon S3 esposto al pubblico

Luglio 2017

Objective:

To obtain Employment with: TigerSwan

Personal information:

Steven [redacted]

Address
[redacted]
United States

Phone: (801) [redacted]
[redacted]@us.army.mil
[redacted]

Job Title: Close Quarters Battle Instructor, Advisor [redacted]
US Citizen: yes
Veteran's Preference: No

Civilian Education:

[redacted]
Continuing education with [redacted] 29 Semester Hours
General Education

Work Experience:

US. Army November [redacted] to Present
Military Occupational Specialties held
[redacted]

Leaks

Vault 7 – CIA leaks

Wiki leakes pubblica documenti segreti sull'arsenale informatico della CIA

Strumenti per accedere a:

- Smart TV
- Automobili
- Web Browsers (tutti)
- OS (tutti)
- Mobile OS (tutti)

Marzo 2017

Shadow Brokers – NSA leaks

Il gruppo Shadow Brokers pubblica per quasi un anno set di exploit della NSA:

- Zero Day Exploits per Windows
- Fra cui Ethernal Blue
- Verrà utilizzato da WannaCry per diffondersi in maniera esplosiva

Agosto 2016 – Maggio 2017

Cyber Warfare

Australian Signals Directorate (ASD)

- **Dati su F-35 e altri sistemi militari**
  - F-35 del programma Joint Strike Fighter,
  - i velivoli con capacità anti-sottomarino e anti-nave Boieng P-8 Poseidon,
  - l'aereo da trasporto Lockheed-Martin C-130
  - le bombe guidate JDAM
  - altri dati su vari vascelli

Hack: Vulnerabilità di sistemi non aggiornati e password deboli utilizzati da un contractor della difesa vittima dell'attacco

Autore: -

Ottobre 2017

Attacco avvenuto nel 2016

Difesa della Corea del Sud

- **Hacker di Pyongyang penetrano nella difesa Sudcoreana**
  - 235 GB di dati
  - Piani di risposta militare di USA e Sud Corea
  - Piani di interventi preventivi contro Kim
  - Piani di sorveglianza di Kim e dei suoi generali

- Pyongyang ha un esercito di 6000 hacker al suo servizio, il Bureau 121

Ottobre 2017

Attacco avvenuto nel 2016

Kasperky Lab Antivirus

L'antivirus Kasperky Lab viene bandito dai computer governativi USA.

La compagnia è accusata di collaborare col Cremlino
e di essere coinvolta nei leaks di documenti della NSA.

Settembre 2017

US Army e DARPA – Plan X

La US Army e la DARPA collaborano alla realizzazione di Plan X

- In sviluppo dal 2013 entra in funzione quest'anno
- Piattaforma inter-dipartimento per consentire all'esercito di controllare operazioni di Cyber Warfare and defense
- Interfaccia tattica e user-friendly per consentire al personale militare di operare secondo concetti loro familiari

EU CYBRID 2017, cyber war game

I minsitri della difesa EU partecipano a una simulazione di Cyber Warfare

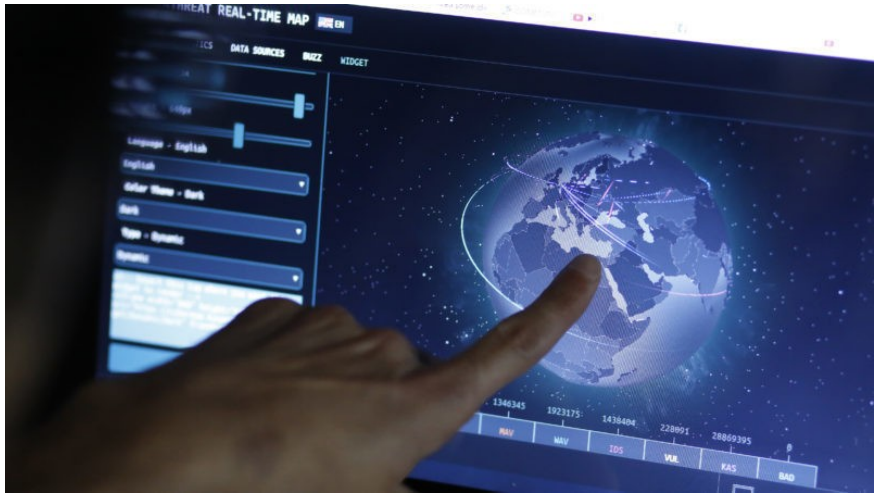
- Attacchi informatici
- Campagne di Fake News

- **Tallin, Estonia**

  Teatro della Web War I nel 2007

"Dobbiamo essere molto più preoccupati per gli attacchi all'integrazione dell'informazione dei nostri sistemi che sono stati manomessi"

Settembre 2017



Ottobre
Mese della cyber sicurezza

EUROPEAN
CYBER
SECURITY
MONTH

TRUST NO ONE

Arrivederci
e Grazie