Dall’endpoint al mobile, dall’on premise al cloud, dai rischi agli incidenti

Luca Bechelli

Clusit
Education

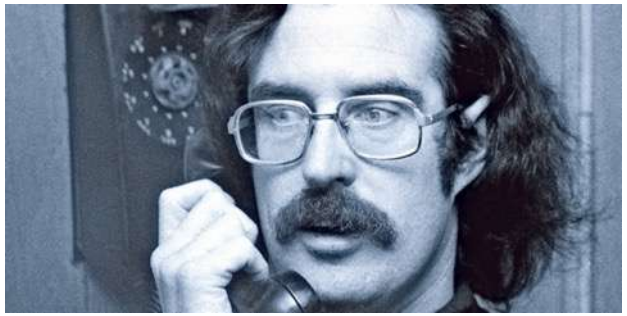
Luca Bechelli

- Practice Leader Information & Cyber Security Advisory Team @ P4I
- Membro del Comitato Direttivo e del Comitato Tecnico Scientifico Clusit Associazione Italiana per la Sicurezza Informatica
- Coordinatore GdL «La valutazione degli impatti del GDPR nelle clausole contrattuali dei fornitori» presso l'Osservatorio «Privacy & Security» del Politecnico di Milano OSSERVATORI.NET digital innovation
- Direttore Didattico Academy Experis per Master in Cybersecurity Experis ManpowerGroup
- Community Clusit - Oracle4Security Oracle Community For Security


TECNOLOGIA
Malware infetta migliaia di PC e gli hacker guadagnano con i Bitcoin
Kaspersky Lab ha scoperto due reti botnet utilizzate dagli hacker per svolgere attività di mining, il sistema che permette di generare la moneta virtuale
LA STAMPA TECNOLOGIA
Se gli hacker trasformano i robot da casa in spie
L'allarme arriva dal collettivo IOActive ma c'è anche il rischio, peggiore, che le macchine possano arrivare a farci del male
AZZETTA DI MODENA
Modena. Attacco hacker a ditta, salvi 78mila euro
«Ci hanno indotti a immettere una nuova password all'home banking: subito partito un bonifico a banca portoghese»
Beppe Grillo (LaPresse)
M5S e gli hacker, autocritica sul blog «Pessima gestione della sicurezza»
L'esperto parla di rischio manipolazione del voto. E non esclude che il pirata sia interno. «Grillo? Non era cosciente dei dispositivi necessari per portare avanti questo tipo di democrazia»
di Alvise Losi
Sicurezza
Instagram, hacker sfrutta falla per 'bucare' i profili delle star
Il social delle foto rassicura: problema risolto, nessun accesso alle password. Negli ultimi giorni era stato forzato l'account di Selena Gomez, dove sono comparse foto osé dell'ex Justin Bieber
FORLITODAY
Cronaca
Gli hacker colpiscono il sito del Forlì calcio
Un hacker ha fatto visita al sito del Forlì Calcio. Il pirata informatico è penetrato nel sito ufficiale della società calcistica
il Giornale.it
mondo
Le elezioni tedesche e la paura degli hacker russi
LA STAMPA MONDO
Attacco a Equifax, a rischio i dati di 143 milioni di consumatori
LA STAMPA MONDO
Aziende dell'energia in Europa e Usa violate da hacker
Il gruppo, Dragonfly, poteva sabotare i sistemi infiltrati, dice Symantec. Ma rischi di blackout non ce ne sono, precisano altri. Pista russa ma dibattuta
la Nuova di Venezia e Mestre
Un hacker gli ruba soldi La banca non risarcisce
Disavventura a Mestre per un cliente dell'istituto che ha saputo dov'erano finiti i suoi soldi, ma la banca
BANCHE
TRUFFE
HACKER
IlFattoQuotidiano.it / Media & Regime
Libero quotidiano offline da giovedì notte: "Siamo sotto attacco hacker"
Il blocco informatico è avvenuto nella notte tra il 7 e l'8 settembre. Il quotidiano diretto da Vittorio Feltri indica come responsabile l'hacker Anonplus e assicura: "Stiamo lavorando per risolvere il problema al più presto".L'attacco è avvenuto all'indomani delle polemiche sulla l'apertura del giornale sulla bambina morta di malaria, che aveva indignato il web
di F. Q. | 8 settembre 2017

«Chi viene a cena stasera?»

John Thomas Draper



"I do it for one reason and one reason only.
I'm learning about a system.
The phone company is a System.
A computer is a System, do you understand?
If I do what I do, it is only to explore a system.

Computers, systems, that's my bag.
The phone company is nothing but a computer"

Gennady Kapkanov

Ci sono cose che non cambiano mai…

OWASP Top ten vulnerabilities 2017

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

Tecniche di attacco (rispetto al 2017)

+39%

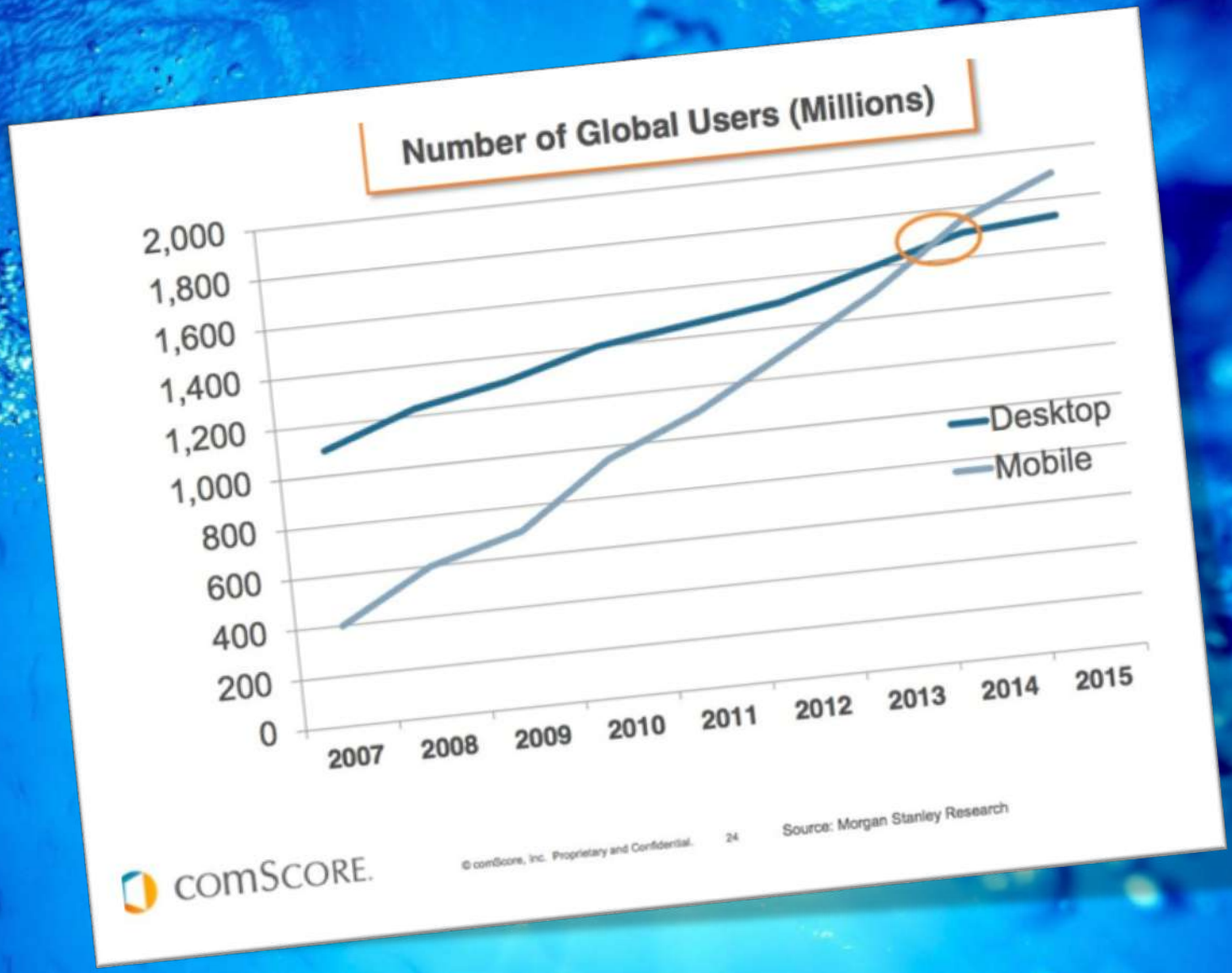
Know Vulnerabilities

Tecniche di attacco (rispetto al 2017)

+57%

Phishing

Mobilis in mobile



212 BILLION

Total number of available sensor enabled objects by 2020

212B is **28x** the total population of the world

30 BILLION

Sensor enabled objects **connected to networks** by 2020


Mirai botnet, a DDoS nightmare
turning Internet of Things
into Botnet of things

…comunque, ho l'antivirus

Il cloud Azure, a livello mondiale, incontra lo stesso malware

sola volta in più del 97% dei casi

Tecniche di attacco (rispetto al II sem.2017)

+140% 0-day

+48% APT

…e malware, malware, MALWARE!

Un obiettivo interessante…

57%

del traffico internet è generato da dispositivi mobili (Wandera)

2B

Mobile banking users forecasted for 2018

50%

Of global banked population are mobile banking users

$86B

spent in app stores in 2017

2X

growth in two years

>3.1M

Apps on the Google Play Store

>1.9M

Apps on the Apple App Store

Fonte: OneSpan Report

I dispositivi mobili sono davvero sotto attacco?

Dal 2017 al 2018:

+24%

di attacchi verso il mondo mobile

Fonte: ThreatMetrix Report

E in Italia?

TOP 10 countries by share of users attacked by mobile ransomware Trojans:

	Country*	%**
1	USA	1.73
2	Kazakhstan	0.36
3	China	0.14
4	Italy	0.12
5	Iran	0.11
6	Belgium	0.10
7	Switzerland	0.09
8	Poland	0.09
9	Mexico	0.09
10	Romania	0.08

Fonte: Karspesky

…a cosa servirà mai, l'antivirus

Dal 2016 al 2017: **+56%**

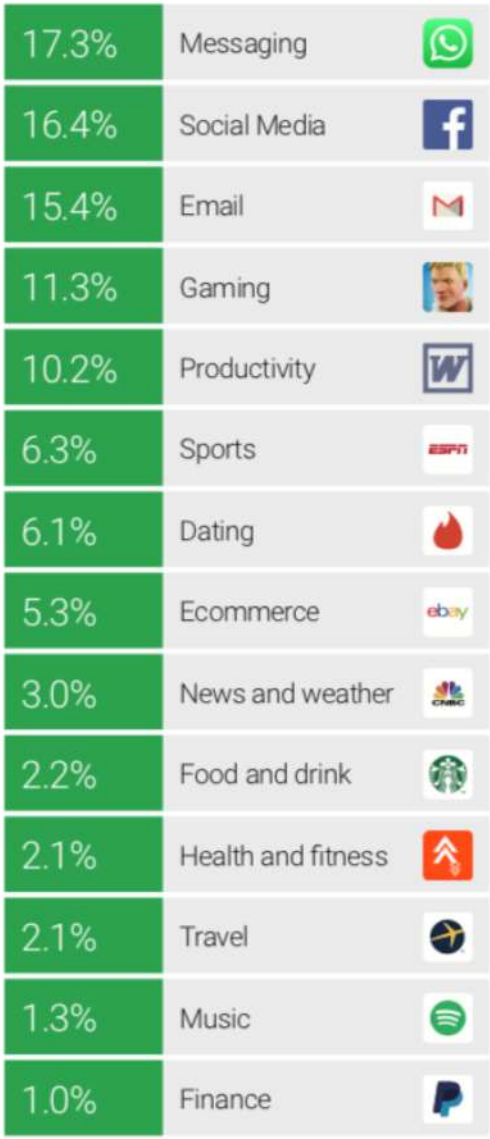
nuovi malware nel mondo mobile

Fonte: Symantec Threat Report

Non esiste la panacea per ogni male…

Affidarsi all'utente…

- **1 su 281** dispositivi personali Android è «rooted» dal proprietario (1 su 1500ca su iOS) (Symantec)
- Solo il **45%** dei dispositivi personali (Android) ha la cifratura del file system attiva (-2% in caso di device aziendali) (Symantec)
- Solo il **20%** dei dispositivi Android ha installata l'ultima release del software. Il **23%** degli iOS è ancora ad una versione precedente (Symantec)
- Gli utenti iOS cadono vittima **18 volte** più di frequente degli attacchi phishing (Wandera)
- Gli utenti «mobile» sono i primi «ad arrivare» in caso di phishing (IBM)
- Gli utenti «mobile», di fronte ad un sito di phishing, hanno una probabilità 3 volte maggiore di inserire le credenziali (IBM)

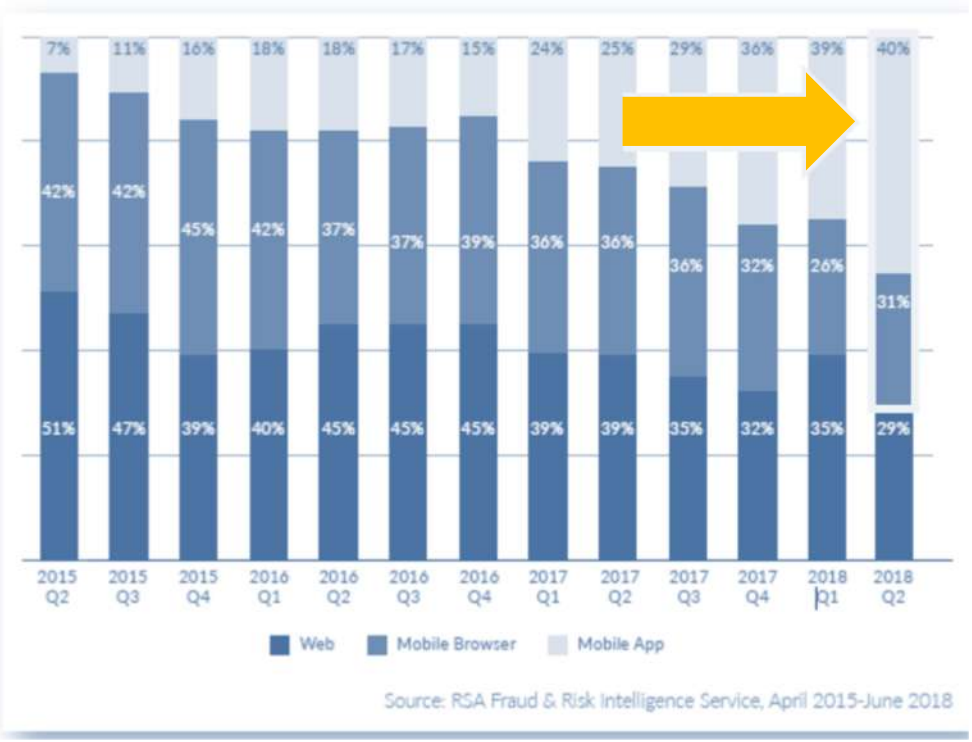


Affidarsi alle App

- Il **48%** degli sviluppatori dichiarano che non hanno tempo sufficiente da investire nella sicurezza
- **+9k rogue App** nel solo II semestre 2018

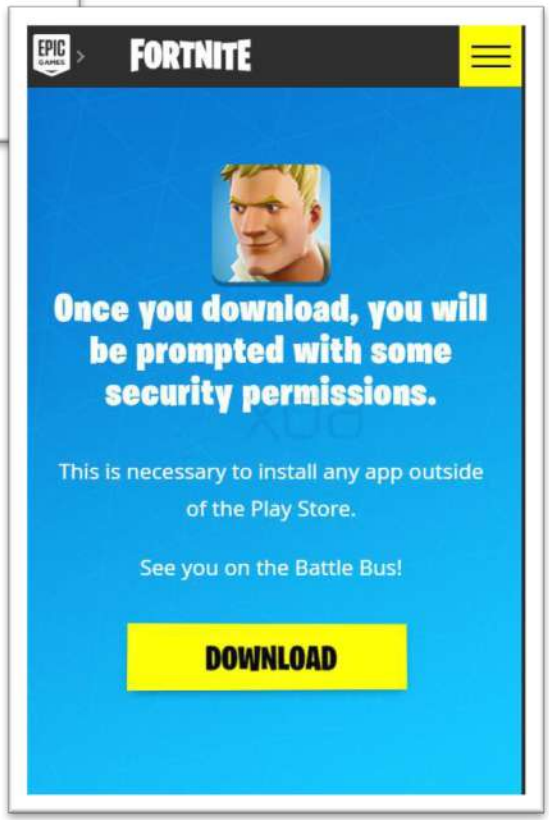
71%

of fraud transactions came from mobile apps & browsers in Q2 2018 (↑ 9% over Q1 & ↑ 16% YOY)



Fonte: OneSpan Report

Affidarsi all'utente e alle App



- **15M di download e 23 milioni di giocatori dopo 21 giorni di beta testing**

- I dispositivi che scaricano software da siti diversi dagli store ufficiali, hanno una probabilità **9 volte maggiore** di compromissione da malware

Fonte: OneSpan Report

L'importanza dell'infrastruttura…

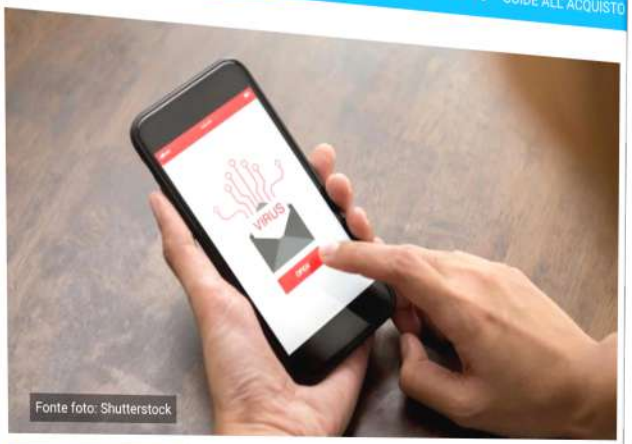
Atm: subito attacco informatico ma sistemi non sono stati violati

Milano, 22 feb. (askanews) – Oggi Atm ha segnalato al Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche (Cnaipic) della polizia postale "un accesso massivo ostile da numerosi indirizzi IP provenienti contemporaneamente da diverse parti del mondo". Si tratta del cosiddetto "Denial of service" (Ddos) che ha sottoposto "i sistemi informatici ad un rallentamento, dovuto ad un sovraccarico della banda e alla saturazione della connessione". Lo ha spiegato la stessa azienda, precisando che "il Ddos è una pratica frequente" e che "i sistemi informatici di Atm non sono mai stati violati da alcun attacco hacker che abbia toccato il sistema centrale o le telecamere delle metropolitane e della security, né tantomeno altri dati sensibili".

LIBERO / TECNOLOGIA

Cerca in Tecnologia

TECH NEWS ANDROID APPLE SOCIAL DIGITAL LIFE APP HOW TO GUIDE ALL'ACQUISTO



Fonte foto: Shutterstock

SICUREZZA INFORMATICA

Connessioni 4G e 5G a rischio: bug permette agli hacker di spiarti

Quali sono i bug che affliggono i dispositivi con connessione 4G e 5G? Ecco le tre falle che potrebbero colpire il tuo smartphone o cellulare

INTERNET E TELEFONO MOBILE HOSTING E DOMINI ALTRI SERVIZI NEGOZI TISCALI MY

Internet, Icann: in corso in tutto il mondo massicci attacchi informatici

Condividi 3 Tweet

di *Askanews*

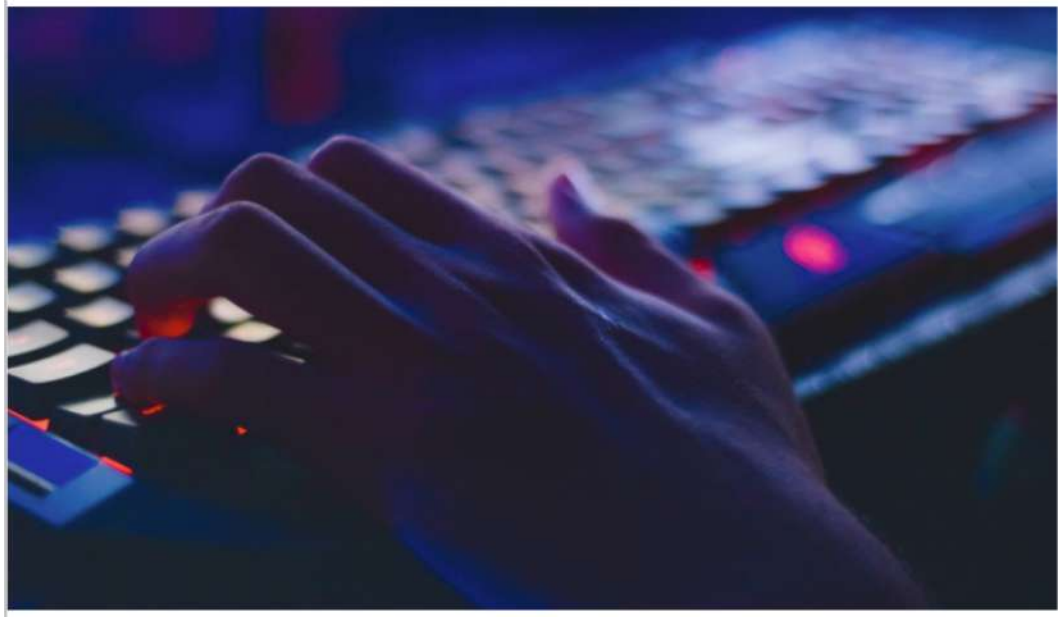
Roma, 22 feb. (askanews) - L'organizzazione internazionale che assegna gli indirizzi Internet (ICANN) ha reso noto che in tutto il mondo sono in corso massicci attacchi informatici contro i domini Internet. Questi attacchi informatici consistono nell'"apportare modifiche non autorizzate" agli indirizzi e nel "sostituire gli indirizzi dei server autorizzati" con indirizzi di macchine controllate dagli aggressori", ha dichiarato

…degli strumenti più diffusi…

SLASHGEAR

Hackers stole 6TB of data from Citrix breach – FBI is investigating

Adam Westlake - Mar 10, 2019, 7:01 am CDT



Software maker Citrix has revealed that it's been the target of a data breach, resulting in international hackers making off with a large amount of data. The company states that it was contacted by the FBI last week and warned that its network was likely compromised by an Iran-linked hacker group, which stole between 6TB and 10TB of business documents.

…e dei servizi ad uso massivo…

HUFFPOST

CITTADINI 19/11/2018 19:12 CET | Aggiornato 19/11/2018 19:12 CET

Attacco hacker alle pec, violate 500mila caselle di posta

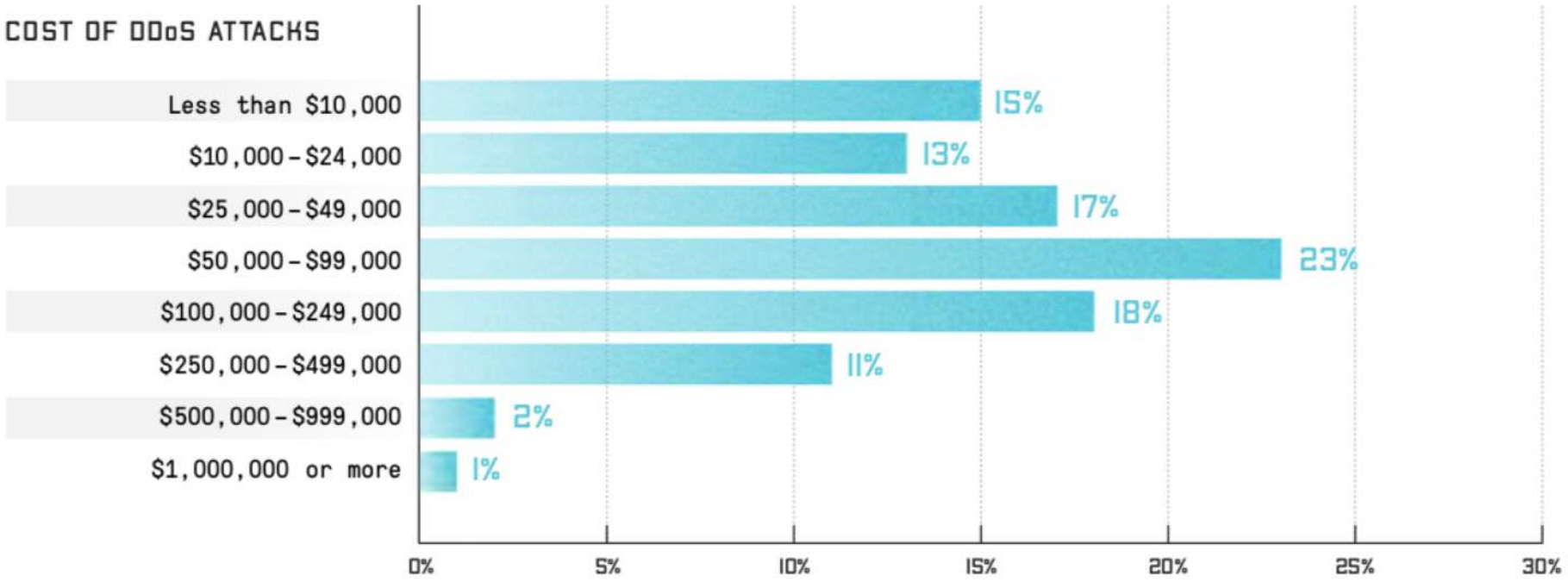
Quasi 100mila sono della Pubblica Amministrazione

By Huffington Post

BLUEBAY2014 VIA GETTY IMAGES

Tremila tra soggetti pubblici e privati, oltre 30 mila domini e mezzo milione di caselle email, 98 mila delle quali della pubblica amministrazione. E' Roberto Baldoni, vicedirettore del Dis responsabile del cyber a fornire i numeri dell'attacco hacker ad un fornitore di servizi di posta elettronica certificata che ha avuto, tra le sue conseguenze, il blocco dei tribunali italiani.

Non è un problema IT



Fonte: NETSCOUT's 14th Annual Worldwide Infrastructure Security Report

Beneath the surface of a cyberattack
A deeper look at business impacts

Deloitte.

Summary of the impact factors

	Impact factor	Term	Cost (in millions)	% Total cost
Above the surface	Cybersecurity improvements	1 year	13.00	0.40%
	Attorney fees and litigation	5 years	11.00	0.35%
	Public relations	1 year	1.00	0.03%
	Technical investigation	9 weeks	1.00	0.03%
	Customer breach notification	Not applicable	-	0.00%
	Post-breach customer protection	Not applicable	-	0.00%
	Regulatory compliance	Not applicable	-	0.00%
Beneath the surface	Value of lost contract revenue	5 years	1,600.00	49.11%
	Operational disruption	2 years	1,200.00	36.83%
	Devaluation of trade name	5 years	280.00	8.59%
	Loss of intellectual property	5 years	151.00	4.63%
	Insurance premium increases	1 year	1.00	0.03%
	Increased cost to raise debt	Not applicable	-	0.00%
	Lost value of customer relationships	Not applicable	-	0.00%
	Total		**$3,258.00**	**100.00%**


ACCEDI
CORCOM
CYBERSECURITY
Maxi attacco hacker al big dell'alluminio, ferme in tutto il mondo le fabbriche di Norsk Hydro
Home > Cyber Security
Condividi questo articolo
Presi di mira i sistemi IT del gruppo utilizzando un ransomware: parte degli stabilimenti costretta a operare manualmente, chiusi molti degli impianti di estrusione. L'azienda: "Ripercussioni difficili da valutare"
19 Mar 2019

Dietro ogni problema c'è un'opportunità

(Galilei)

WhatsApp, Fb e Instagram down: «Ma non è un attacco hacker»

Mercoledì 13 Marzo 2019

Whatsapp, Facebook e Instagram down in tutto il mondo per 15 ore. Fb spiega: «Non è stato un attacco informatico»

sky tg24 HOME VIDEO CRONACA ED. LOCALI POLITICA ECONOMIA MONDO SPORT

XI JINPING IN ITA

SOFTWARE-APP 14 marzo 2019

WhatsApp, Telegram guadagna 3 milioni di utenti durante il down

Anche quando non si raggiunge la X

AGI > Cronaca

Cosa sappiamo dell'ultimo attacco informatico sventato da Unicredit

Nella seconda metà di gennaio, numerosi clienti della banca si sono visti recapitare per posta una lettera con la quale venivano informati di un tentativo di violazione dei loro dati. Ecco cosa è successo, e cosa fare

di **RAFFAELE ANGIUS**
25 gennaio 2019,07:56

GRAZIE!

Luca Bechelli
Comitato Scientifico Clusit
luca@bechelli.net
www.bechelli.net
https://twitter.com/luca_bechelli
https://www.facebook.com/bechelli.luca
http://www.linkedin.com/in/lucabechelli