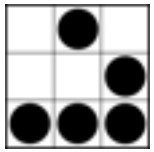


Mobile (in)security

i tuoi dispositivi visti con gli occhi di un hacker

Alessio L.R. Pennasilico - apennasilico@clusit.it

Mobile Business
Treviso, 9 Maggio 2014

Clusit Education

$whois -=mayhem=-

Security Evangelist @ 

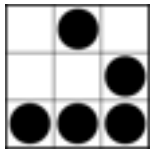
Committed:

AIP Associazione Informatici Professionisti, CLUSIT
AIPSI Associazione Italiana Professionisti Sicurezza Informatica
Italian Linux Society, Sikurezza.org, AIP/OPSI
Hacker's Profiling Project, CrISTAL

Io sono preoccupato

Le informazioni

Le informazioni



Perché occuparsi di security?

Cosa dobbiamo affrontare?

Ogni anno
durante il Security Summit di Marzo a Milano
Clusit presenta un rapporto
su cosa è accaduto nell'anno precedente
e cosa ci si aspetta dall'anno in corso

SECURITY SUMMIT

Io sono preoccupato

Cosa emerge?

Tutti sono un bersaglio

Tutte le piattaforme sono un bersaglio

Le protezioni tradizionali sono inefficaci

Trend?

Aumentano i tentativi di intrusione

Aumentano i tentativi andati a buon fine

Per ogni intrusione perdiamo sempre più denaro

Perché preoccuparsi?

Nel 2013 gli attacchi noti
che hanno prodotto un danno ingente a chi li ha subiti
in termini economici o di immagine
sono aumentati del 245%

Campione 1152 attacchi di cui 35 Italiani

Vettori

Spear Phishing
Siti infetti
Sciacallaggio sulle news
Social APP infette
Mobile APP infetta

Botnet

Una volta infettati i **DEVICE** per fare SPAM, Phishing, DDoS

posso rubare altri dati/identità

posso utilizzarli per produrre altro denaro

Ci attaccano per questo?

ASSET	GOING RATE
1 US CVV (Visa, Master)	2$/cvv
1 US CVV (American Express, Discovery)	4$/cvv
1 UK CVV	5$/cvv
1 UK CVV (American Express, Discovery)	6$/cvv
1 UK CVV with DOB	15$/cvv
1 CA CVV	10$/cvv
1 CA CVV (American Express, Discovery)	15$/cvv
1 EU CVV	10$/cvv
1 EU CVV (American Express, Discovery)	15$/cvv
1 US CVV full info	45$/CVV
1 UK CVV full info	55$/cvv
CVVs from other countries	10$/cvv
SMS Spammer (various options)	60 WMZ, may vary
For every 1,000 Gmail account credentials	up to 10K: $ 12 | from 10K to 100K: $ 10 | from 100K: $ 8
For every 1,000 Hotmail account credentials	up to 10K: $ 12 | from 10K to 100K: $ 10 | from 100K: $ 9
For every 1,000 Blogger.com RU account credentials	up to 10K: $ 30 | from 10K to 100K: $ 25 | from 100K: $ 20
For every 1,000 Blogger.com EN account credentials	up to 10K: $ 30 | from 10K to 100K: $ 25 | from 100K: $ 20

L'approccio al problema...

la Repubblica BOLOGNA.it

Cerca: Archivio

Cerca: Cerca nel Web con G

Martedì 12 Luglio 2011 – Aggiornato Alle 15.56

Home | Cronaca | Sport | Foto | Video | Annunci | Aste-Appalti | Lavoro

Sei in: Repubblica Bologna / Cronaca / Hacker, colpito l'ateneo di Bologna ...

CRONACA

Consiglia 22

Hacker, colpito l'ateneo di Bologna "Diffusi dati non riservati"

I pirati informatici hanno preso di mira molte unievrsità italiane, da Siena a Cagliari, da Bari a Napoli: codici fiscali, email, numeri di telefono di docenti e studenti a disposizione di tutti. L'Alma Mater: "Ma nel nostro caso sono informazioni molto generiche"

L'Alma Mater di Bologna non è stata risparmiata dall'attacco di pirateria informatica che ha preso di mira 18 atenei italiani. Dall'account LulzStorm su Twitter i dati degli studenti e dei professori di diverse università italiane sono a disposizione di tutti.

LEGGI Gravissimo attacco hacker di J.D'ALESSANDRO


Gmail
by Google


amazon.com


ebay


facebook

Identity theft: solo uno scherzo?


FIRENZE

LA NAZIONE

ITALIA E MONDO · NOTIZIE LOCALI · SPORT · MULTIMEDIA · Meteo Lavoro

Cronaca Politica Sport Eventi AC Fiorentina Ristoranti Cinema

Rubano l'identità di Tremonti: "Era una burla"

Creano un falso profilo Facebook del ministro e conquistano 5mila amici: ora rischiano un anno di carcere

COMMENTA LA NOTIZIA

facebook

Giulio Tremonti

Governo Italiano

Università degli studi di Pavia

Danni economici
Danni di immagine
Ripercussioni sul credito
Difficile da dimostrare
Strascichi lunghissimi

Io sono preoccupato

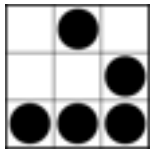
Economia “digitale”

Economia “digitale”

Economia “digitale”

Quel che succede su Internet

Ho conseguenza nel mondo “reale”



Mobile è imprescindibile da Cloud e Social

(ma da Security?)

Clusit

Clusit Education

I social network

I social network

Facebook Hacking

"The social reconnaissance enabled us to identify 1402 employees 906 of which used facebook."

[…]

"We also populated the profile with information about our experiences at work by using combined stories that we collected from real employee facebook profiles."

http://snosoft.blogspot.com/2009/02/facebook-from-hackers-perspective.html

Fiducia

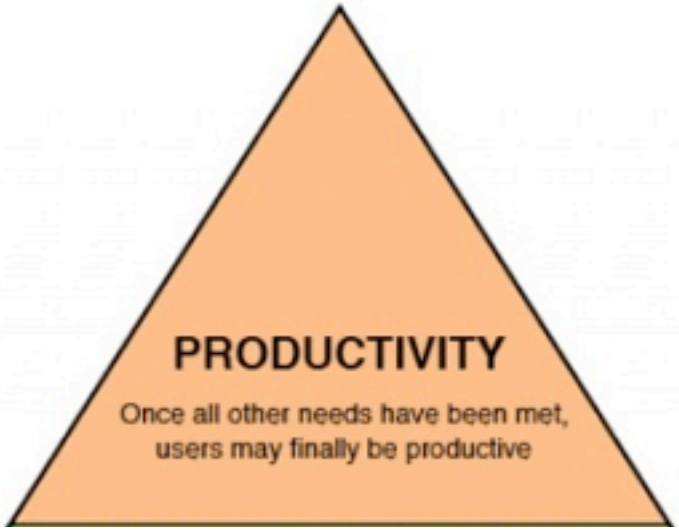
"Upon completion we joined our customer's facebook group. Joining wasn't an issue and our request was approved in a matter of hours. Within twenty minutes of being accepted as group members, legitimate customer employees began requesting our friendship. […] Our friends list grew very quickly and included managers, executives, secretaries, interns, and even contractors."

Risultati

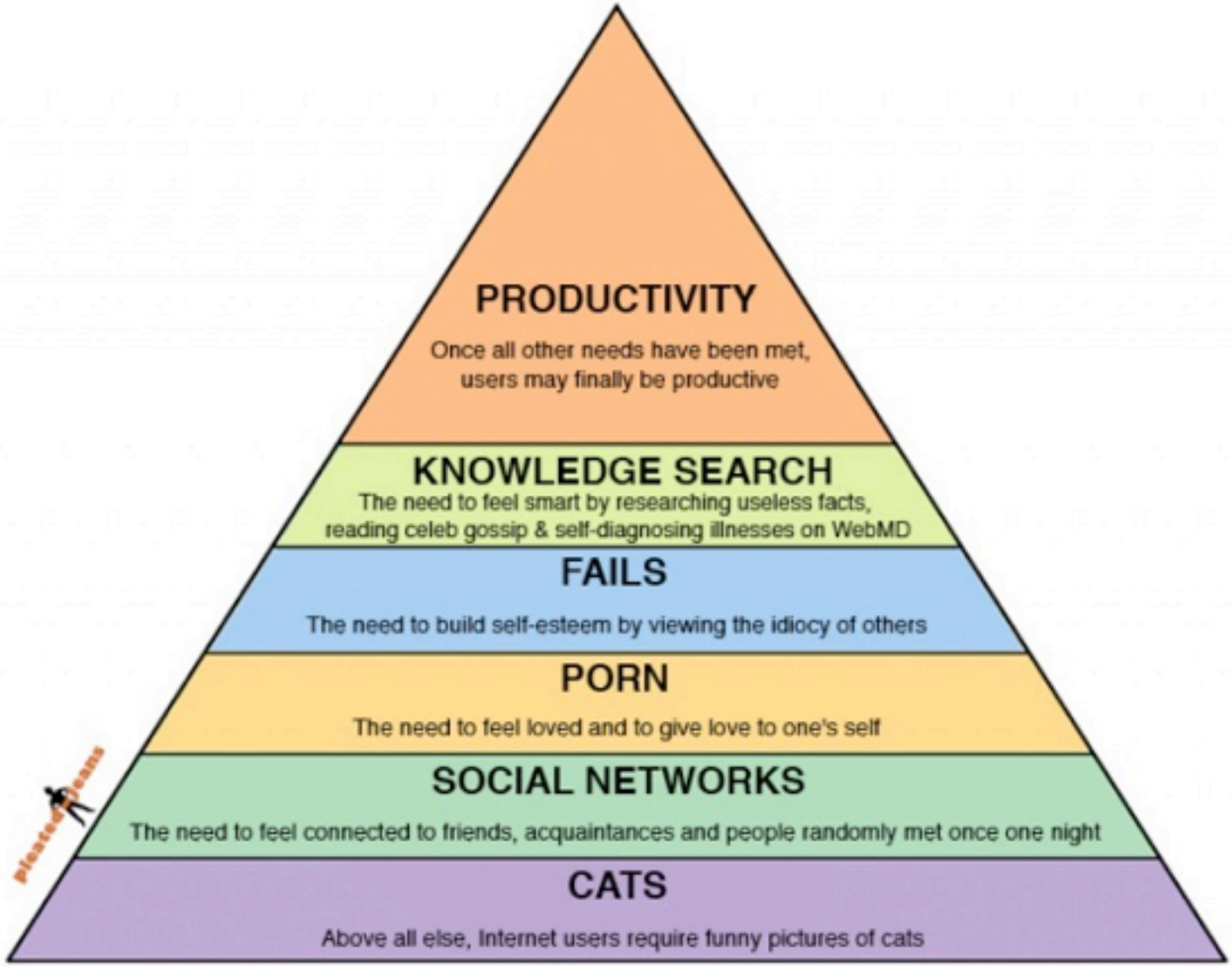
"We used those credentials to access the web-vpn which in turn gave us access to the network. As it turns out those credentials also allowed us to access the majority of systems on the network including the Active Directory server, the mainframe, pump control systems, the checkpoint firewall console, etc."

Io sono preoccupato

Maslow's Hierarchy of Internet Needs



Maslow's Hierarchy of Internet Needs




trudi

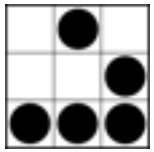
Cosa saprò insegnare?

Sara Amlesù, 36 anni

MILANO - Scrivania addio. La sua storia ricorda quella Kimberley Swann, la teenager inglese che ha definito noioso il proprio lavoro, scrivendolo sulla propria pagina di Facebook senza immaginare le conseguenze del suo gesto. La bacheca di Sara Amlesù è ancora visibile: «Se anche tu, come me, ti svegli al mattino pensando... No, anche oggi in Danieli/ Se anche tu, come me, quando conosci un friulano o un genovese non puoi fare a meno di pensare mal comune mezzo gaudio/ Se anche tu, come me, dopo una giornata in Danieli sogni il barettino a Santo Domingo/ Se anche tu, come me, ringrazi la Danieli solo per gli amici/ Sei il benvenuto».

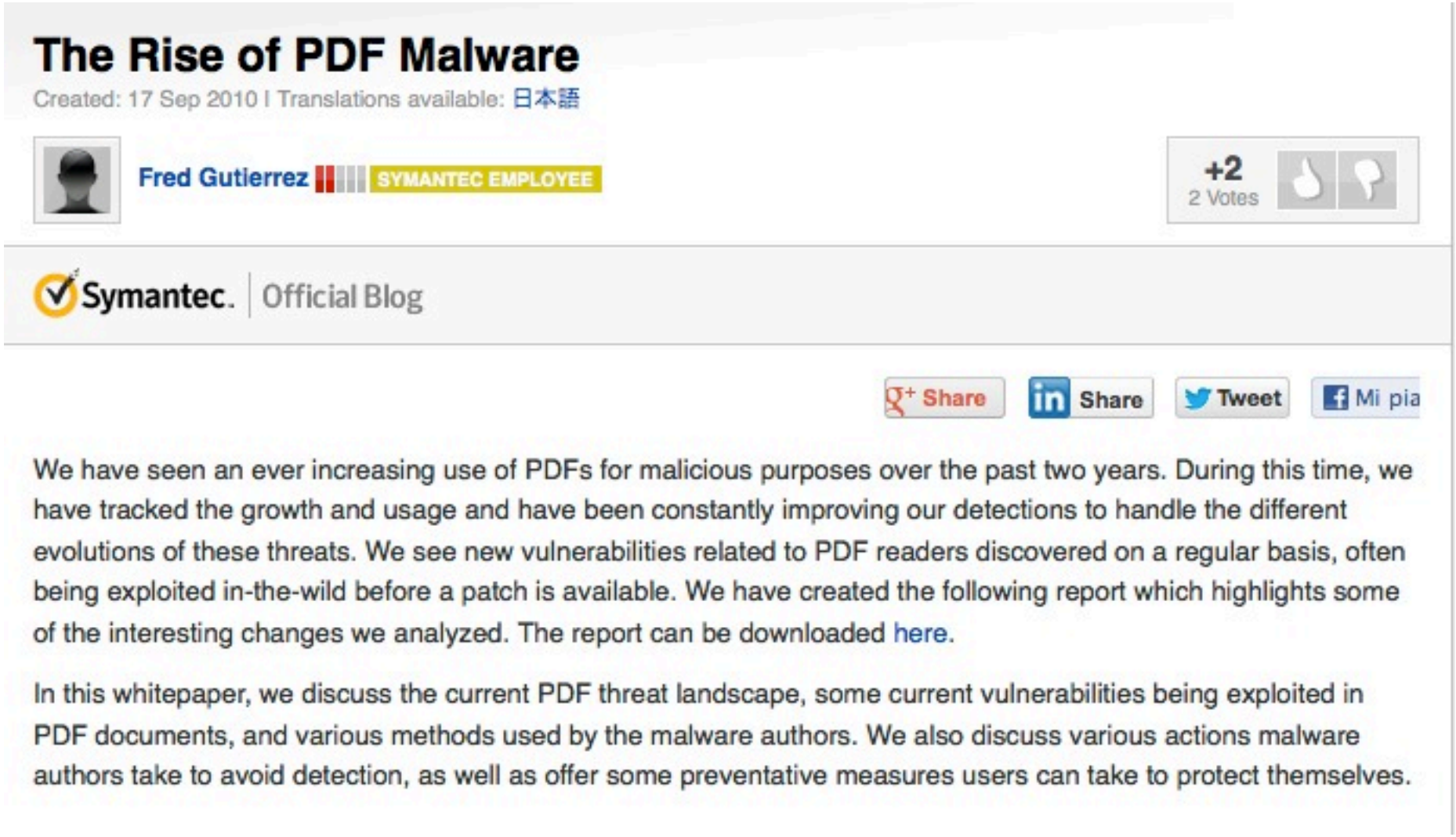

PLEASE ROB ME
Raising awareness about over-sharing
Check out our guest blog post on the CDT website.

Io sono preoccupato



E’ necessario un nuovo approccio

PDF come vettore



The Rise of PDF Malware

Created: 17 Sep 2010 | Translations available: 日本語

Fred Gutierrez SYMANTEC EMPLOYEE

+2
2 Votes

Symantec. | Official Blog

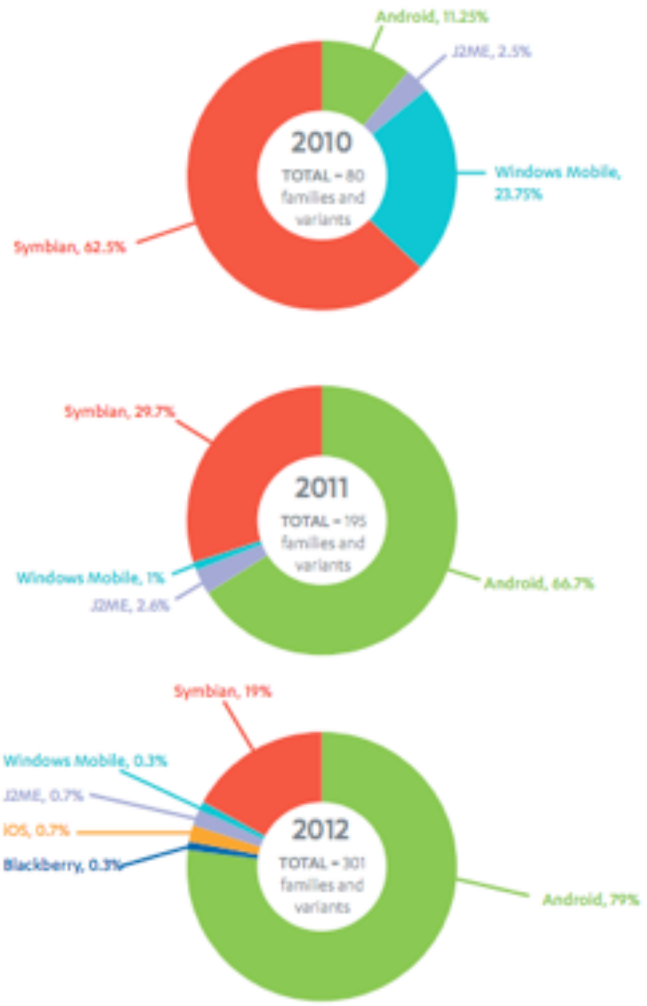
Share Share Tweet Mi pia

We have seen an ever increasing use of PDFs for malicious purposes over the past two years. During this time, we have tracked the growth and usage and have been constantly improving our detections to handle the different evolutions of these threats. We see new vulnerabilities related to PDF readers discovered on a regular basis, often being exploited in-the-wild before a patch is available. We have created the following report which highlights some of the interesting changes we analyzed. The report can be downloaded here.

In this whitepaper, we discuss the current PDF threat landscape, some current vulnerabilities being exploited in PDF documents, and various methods used by the malware authors. We also discuss various actions malware authors take to avoid detection, as well as offer some preventative measures users can take to protect themselves.

Dalla carta...

FIGURE 2: THREAT FAMILIES AND VARIANTS BY PLATFORM,2010–2012



Botnet di Smartphone create anche da volantini cartacei...

... alle App ...

Thread Tools | Search this Thread | Display Modes

22nd March 2010, 08:52 AM #1

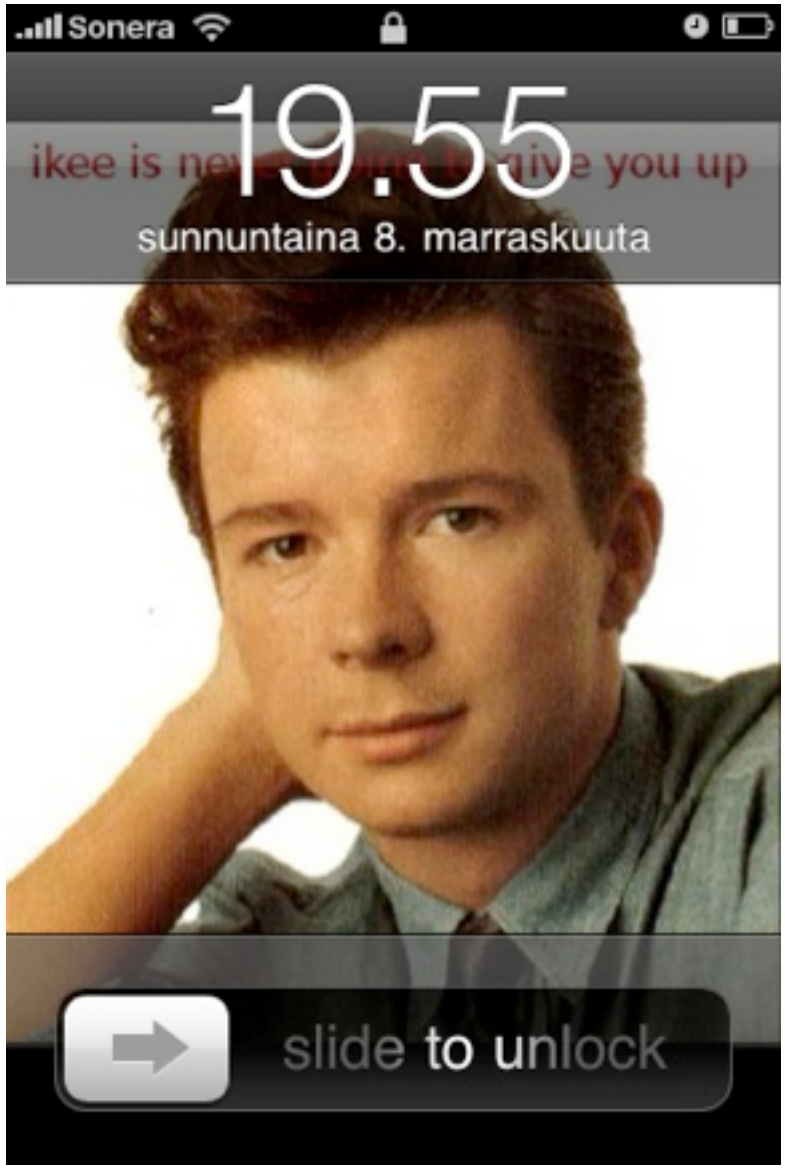
smudgelab [OP]
Member

Join Date: Jan 2010
Posts: 38

Phone dialled out internaionally without permission!

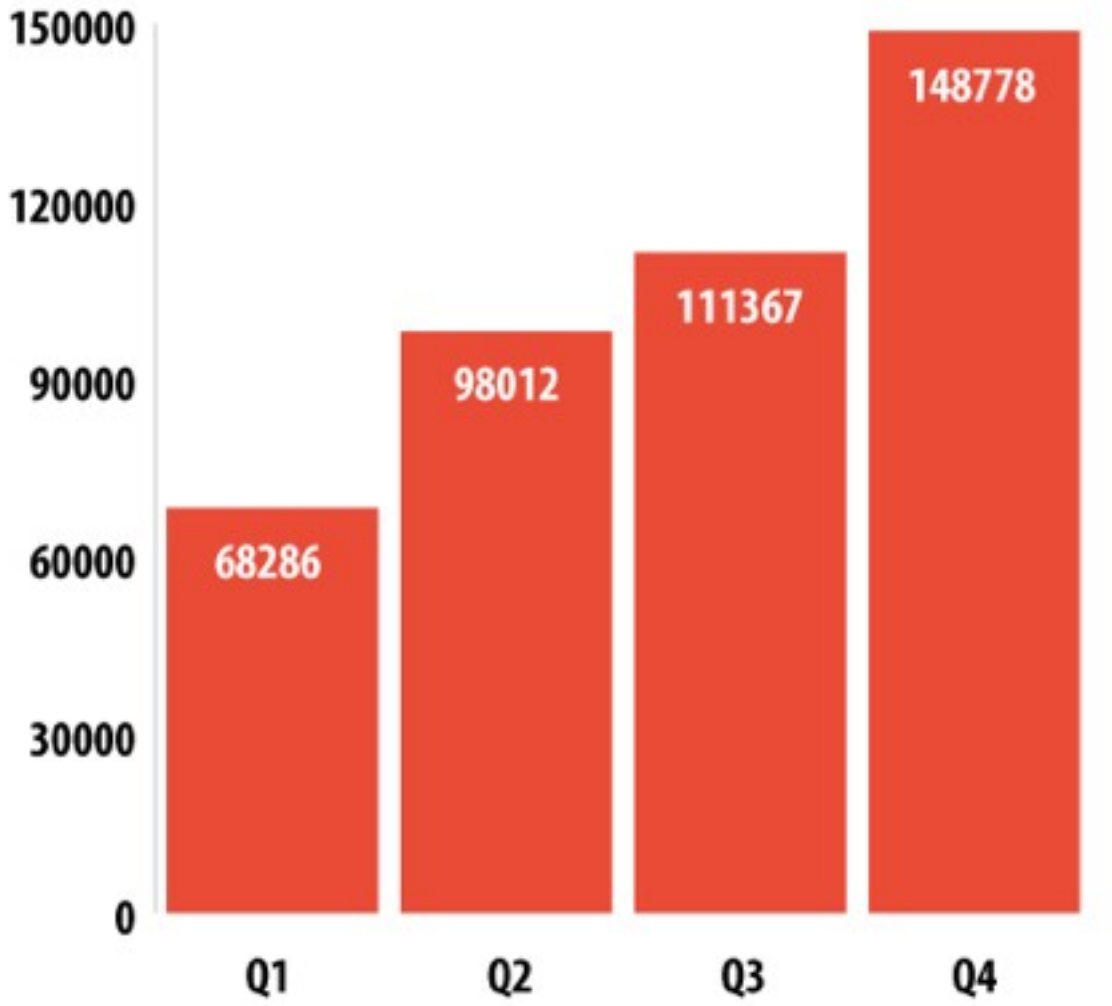
Really wierd one this. Last night, I was woken by a repetitive voice telling me that "International dialling is not currently permitted from this device". As this was at aprox' 02.40 on Suday AM, it fair shook me out of a deep sleep! On checking the phone I found the following call history:
+88213213214 @ 02:44
+88213213214 @ 02:36
+1(767)503-3611 @ 02 36
+1(767)503-3611 @ 02:36
+1(767)503-3611 @ 02:36
+8823460777 @ 02:35
I have absolutely no idea who or what these numbers are for (Google suggests +882 may be something to do with satellite phones(!?) & +1767 appears to be a Dominican country code(!!??) but it was very unnerving to see my phone has been trying to ring these without any input from me. I'll be onto Virgin mobile later to see if they can help but thought I'd try the collective wisdom of you guys first. Virus / dialler maybe? Do these even exist for win mo phones? Any help wil be very much appreciated. Thank you.

... agli script ...



Jailbreak di iPhone:
qualcuno cambia
la password di root?

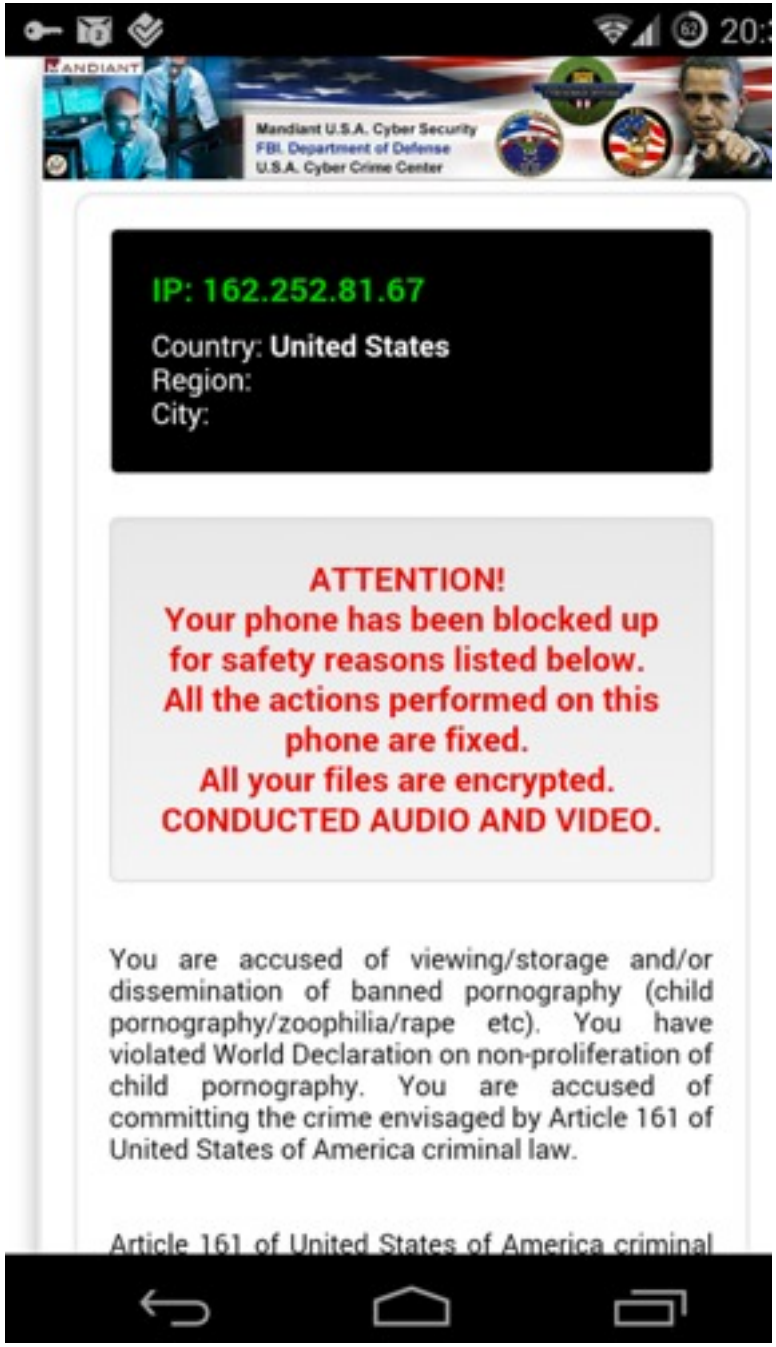
(Novembre 2009)



https://www.securelist.com/en/analysis/204792318/Kaspersky_Security_Bulletin_2013_Overall_statistics_for_2013

Ransomware

Ti cripto tutti i dati
e chiedo il riscatto per dati la chiave
per poterli consultare di nuovo



http://arstechnica.com/security/2014/05/your-android-phone-viewed-illegal-porn-to-unlock-it-pay-a-300-fine/

17 Novembre 2013

The UK's National Crime Agency has given out an urgent national alert that a mass spamming event targeting 10 million UK based email users with a piece of malware called **CryptoLocker** that encrypts your files and then demands a ransom money to restore access.

http://thehackernews.com/2013/11/Cryptolocker-Ransomware-spam-emails-campaign-ten-million-users.html

22 Novembre

The CryptoLocker Malware continues to spread, infected more than 12,000 U.S computers in one week and threatening millions of computers in the UK.

Just last week, The UK National Crime Agency urge people afflicted by CryptoLocker not to pay ransom, not least because there is no guarantee that they will even receive an unlock key.

http://thehackernews.com/2013/11/us-police-department-pays-750-ransom-to.html

5% di 10.000.000 x $ 750 = $ 37.500.000

12.000 infetti x $ 750 = $ 900.000

Chi vuole le informazioni?

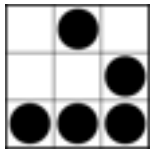
La criminalità organizzata mondiale
ha capito da tempo che
con "*quelli dei computer*"
è possibile gestire truffe
estremamente redditizie

Alpitour, Francorosso, Viaggidea, Villaggi Bravo

12 settembre

Gli account delle diverse pagine Facebook del Gruppo Alpitour sono stati sottratti da cyber criminali egiziani, che hanno iniziato a pubblicare a nome dell'Azienda link malevoli, al fine di redirigere gli utenti su pagine infette da malware (Zeus) . Il malware tentava di infettare i sistemi e di effettuare il furto di credenziali bancarie delle vittime . L'attacco è durato almeno 48h prima di essere risolto, con il recupero del controllo delle pagine Facebook

http://www.lastampa.it/2013/09/15/italia/cronache/alpitour-cyberattacco-via-facebook-false-offerte-per-rubare-dati-agli-utenti-6XHELfHFLlVuGq5RfstdMO/pagina.html



Conclusioni

Io sono preoccupato

Cosa dobbiamo affrontare?

Rischi

reali, concreti
semplici da trasformare in incidenti
alta probabilità di conversione in incident
grande impatto sul business

Rischi

facili da prevenire
difficili da mitigare a posteriori

Io sono preoccupato

IT Security...

Un inutile impedimento
che rallenta le comuni operazioni
e danneggia il business?

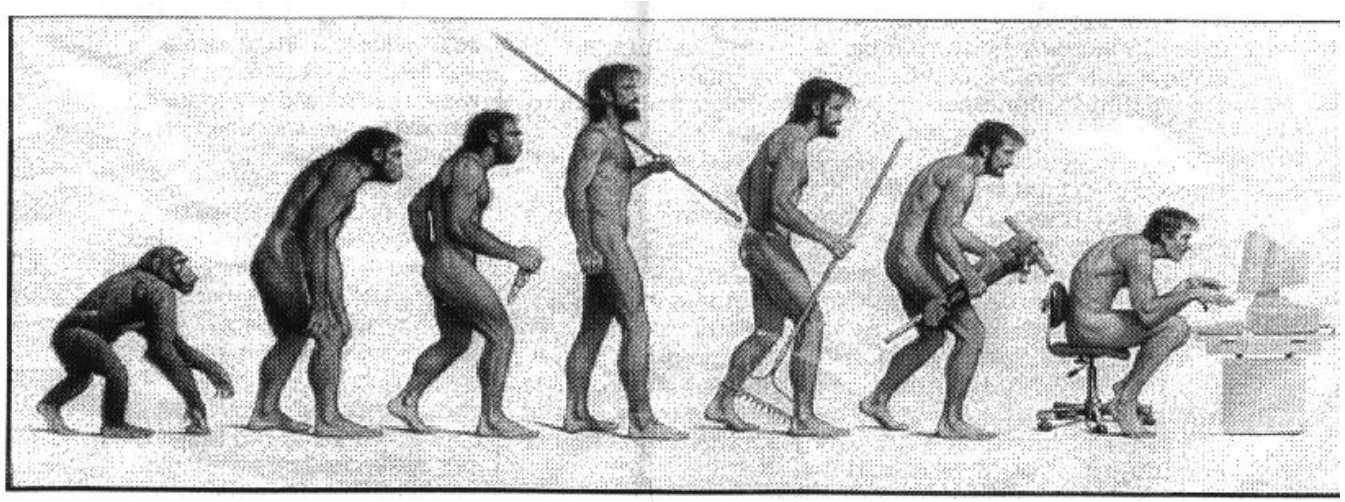
IT Security...

O prevenzione e risposta ad eventi che danneggerebbero il business in modo peggiore?

Io sono preoccupato

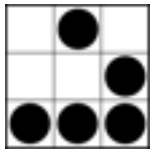
Evoluzione

La tecnologia si evolve…



Somewhere, something went terribly wrong

… e con essa anche le minacce!

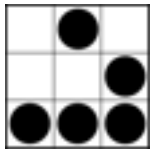


Alessio L.R. Pennasilico - apennasilico@clusit.it
facebook:alessio.pennasilico - twitter:mayhemspp - linkedin:alessio.pennasilico

Clusit

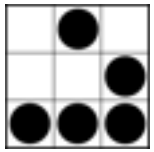
Mobile Business
Treviso, 9 Maggio 2014

Clusit Education



Grazie dell’attenzione!

Alessio L.R. Pennasilico - apennasilico@clusit.it
facebook:alessio.pennasilico - twitter:mayhemspp - linkedin:alessio.pennasilico



Domande?

Alessio L.R. Pennasilico - apennasilico@clusit.it
facebook:alessio.pennasilico - twitter:mayhemspp - linkedin:alessio.pennasilico