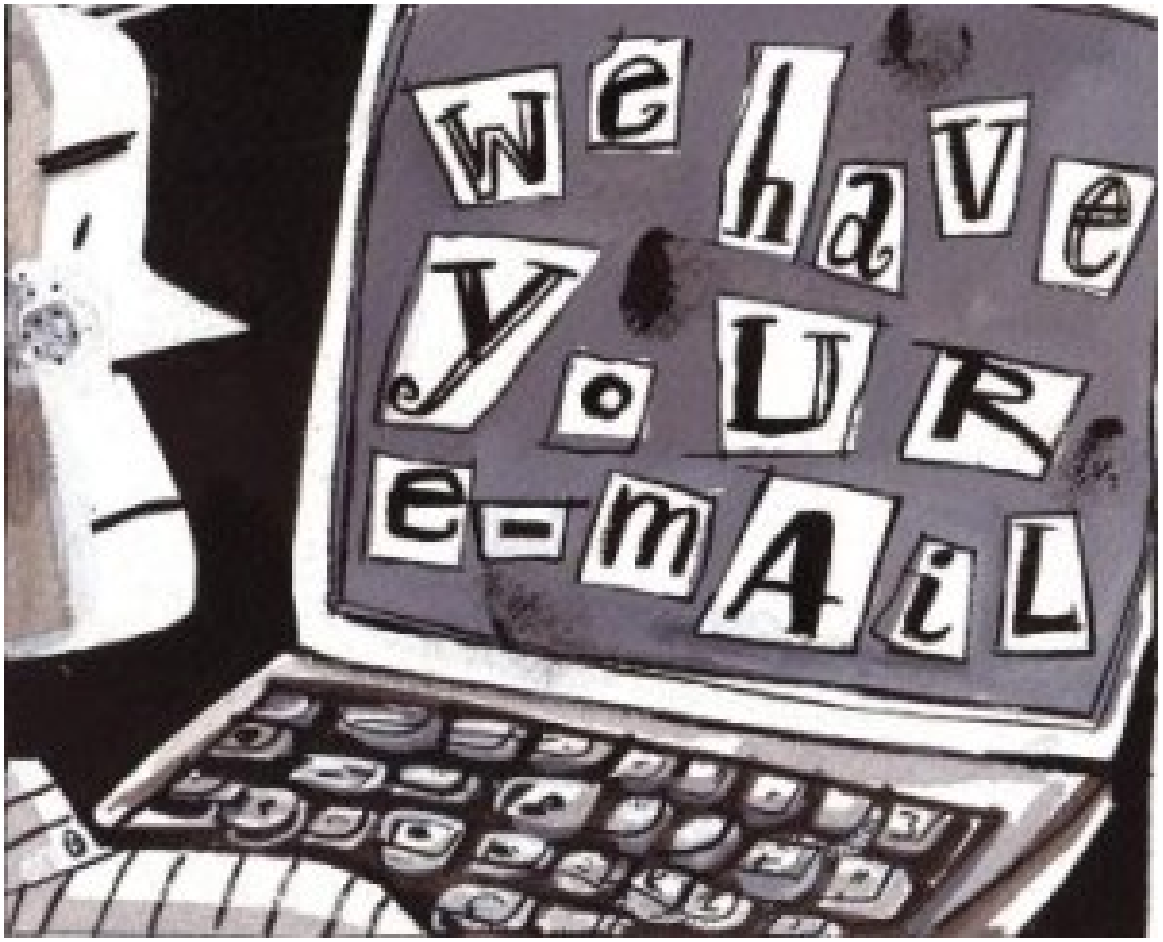
Cyber security: tecnologie, innovazione e infrastrutture



I rischi attuali per le aziende italiane

Milano, 23 marzo 2016

Chi Sono

Davide ‘Rebus’ Gabrini

Per chi lavoro non è un mistero.
Come vedete, non sono qui in divisa.

Oltre a ciò:

- Perito informatico
- Consulente tecnico e Perito forense
- Collaboratore del Laboratorio di Informatica Forense UniPV
- Docente di sicurezza informatica e digital forensics per privati e P.A.
- Certificazioni CIFI, ACE, AME
- Socio IISFA, DEFTA, Tech&Law fellow
- Socio fondatore di Italia Gr.A.P.P.A.
- Sensei Zanshin Tech

I trend dominanti nel cybercrime

RANSOMWARE

BUSINESS EMAIL COMPROMISE

RANSOMWARE

Ransomware

- Dalla prima pagina del Rapporto Clusit 2016: «*E poi c'è la modalità di attacco che più di ogni altro ha fatto parlare del tema nel corso del 2015: i ransomware . Vera e propria estorsione informatica la cui diffusione, e la conseguente capacità di generare denaro, non conosce limiti.*»
- Una minaccia così nuova che il primo ransomware è del 1989, ma il reboot in chiave moderna è del 2012 con Reveton (il «malware della polizia») e dal 2013 con Cryptolocker

Ransomware

Attenzione!!!

È stata rivelata un'attività illegale. Il sistema operativo è stata bloccata per una violenza delle leggi della Repubblica Italiana!

È stata fissata una seguente violazione: Dal tuo indirizzo IP "1337" era eseguito un accesso alle web-pagine contenenti la pornografia, la pornografia minorile, zoofilia, nonché la violenza dei bambini. Nel tuo computer sono stati trovati video-file contenenti la pornografia, elementi di violenza e la pornografia minorile.

Dalla posta elettronica era effettuato anche la distribuzione dello spam con un senso recondito terroristico.
Il bloccaggio di computer serve per troncare l'attività illegale dalla parte tua.

I tuoi dati: **IP:1337**
Posizione: Moon
ISP: SpaceTelecom

Per togliere il bloccaggio devi pagare una multa di 100 euro. Hai due seguenti varianti di pagamento:

1) Effettuare il pagamento tramite l'Ukash.

Per questo inserisci il numero ricevuto nella colonna di pagamento, dopodiché premi OK (se hai più numeri, allora inseriscili uno dopo l'altro, dopodiché premi OK)

Se il sistema segnalerà un errore, allora dovrai mandare il numero per la posta elettronica deposito@cyber-gdf.net.

2) Effettuare il pagamento tramite il Paysafecard:

Per questo inserisci per favore il numero ricevuto (nel caso di necessità insieme con la password) nella colonna di pagamento, dopodiché premi OK (se hai più numeri, allora inseriscili uno dopo l'altro, dopodiché premi OK).

Se il sistema segnalerà un errore, allora dovrai mandare il numero per la posta elettronica deposito@cyber-gdf.net

Ukash Dove passo trovare Ukash?

Puoi richiedere e ottenere Ukash presso migliaia di punti vendita, edicole, stazioni di servizio, bar e tabacchi e negozi di telefonia mobile dotati di terminale **Epay**, **Epipoli**.

Recati presso il punto vendita dotato di terminale **Epay**, **Epipoli** a te piu vicino. Richiedi un voucher in contanti al negoziante. Il negoziante dovra stampare e consegnarti un voucher Ukash con codice PIN da 19 cifre.

epay - Voucher Ukash sono disponibili da migliaia di negozi con un terminal epay.
Epipoli - Voucher Ukash sono disponibili da migliaia di negozi con un terminal Epipoli.

OK

paysafecard Dove passo trovare Paysafecard?

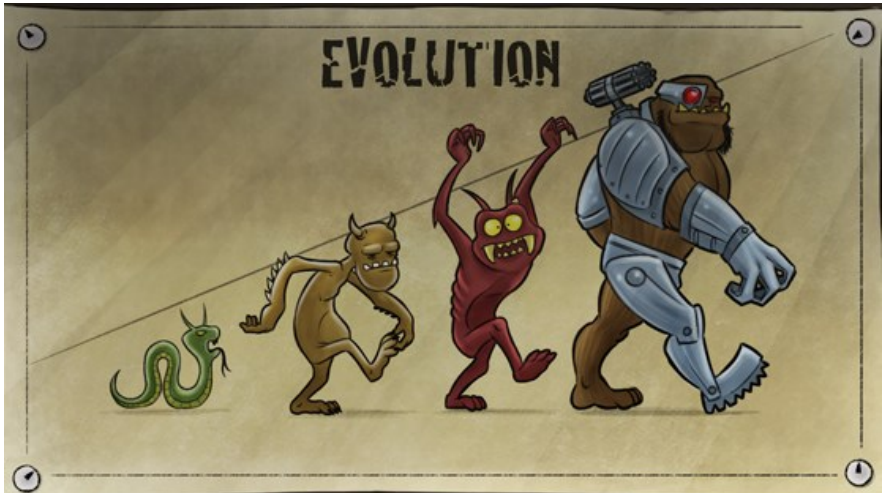
paysafecard è disponibile in tutta sicurezza vicino a te in Italia, ad esempio presso numerose edicole, bar, tabaccai anche nei negozi Sisal e Penny.

OK

CryptoLocker

Evoluzione

- Blocco del PC all'avvio
- Cifratura dei file locali
- Cifratura dei file locali e degli share di rete
- Cifratura di file e cancellazione sicura
- Cifratura di file e backup (VSC, Time Machine, cloud…), wiping
- Allargamento a più piattaforme, ai dispositivi mobili, in direzione IoT



Ransomware

- Tra i malware più facili da debellare: si pulisce la macchina e si ripristina il backup. E invece…
- Europol, 2013: «si stima che il 2% degli utenti infetti abbia ceduto al pagamento dando vita ad un business illegale da 1 milione di dollari annuo»
- FBI, 2015: in un anno, ricevute circa 1000 denunce relative a CryptoWall, con un totale di perdite di circa 18 milioni di dollari.
- Cisco, 2015, dopo aver debellato una campagna legata ad Angler Exploit Kit:
  - Circa 3600 utenti erano colpiti ogni giorni dal ransomware
  - Il 3% di essi ha pagato il riscatto richiesto
  - Si stima che la campagna abbia generato una rendita annuale di oltre 34 milioni di dollari

Pagare non è un'opzione

- Pagare il riscatto significa finanziare la criminalità organizzata
- Rende il business dell'estorsione redditizio e favorisce il proliferare delle minacce
- Produce un danno sociale per «riparare» ad una propria inadeguatezza
- Non risolve né riduce i propri problemi di sicurezza
- Non dà garanzia di risultato: stiamo parlando di criminali!

Business Email Compromise

Business Email Compromise (BEC)

- È una truffa sofisticata che colpisce gli account aziendali, usati abitualmente per gestire contatti e pagamenti con i fornitori.
- Lo scopo è ottenere indebiti trasferimenti di fondi, dirottando pagamenti reali o falsificando nuovi ordini.
- Secondo FBI, le truffe BEC hanno già causato negli USA danni per 740 milioni di dollari, in meno di due anni.

https://www.fbi.gov/news/stories/2015/august/business-e-mail-compromise

BEC

- La compromissione può avvenire in vari modi:
  - Violazione della piattaforma
  - Utilizzo di password deboli
  - Procedura di recupero delle credenziali debole
  - Utilizzo di keylogger
  - Phishing
- Una volta ottenuto accesso, è possibile spiare i contenuti a tempo indeterminato
  - Rubrica contatti
  - Comunicazioni pregresse
  - Monitoraggio in tempo reale

BEC

- Presa cognizione della corrispondenza, è possibile attuare diversi attacchi:
  - Impersonare l'account violato per disporre pagamenti o notificare a clienti e fornitori nuove coordinate bancarie
  - Inviare messaggi di *spear phishing* perfettamente calibrati
  - Impersonare il destinatario di un pagamento reale per dirottare i fondi
  - Sostituirsi a entrambi gli interlocutori per ottenere il pieno controllo delle comunicazioni (*man in the mail*)

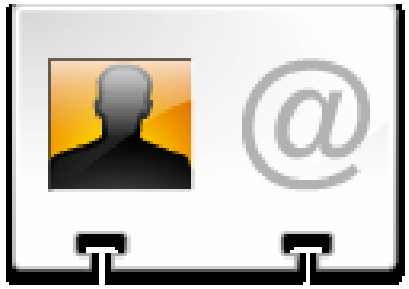
Principale causa di Ransomware e BEC

Teniamoci in contatto...

Davide Rebus Gabrini

e-mail: rebus@tipiloschi.net

GPG Public Key: www.tipiloschi.net/rebus.asc
KeyID: 0x176560F7



facebook.com/gabrini

twitter.com/therebus

it.linkedin.com/in/rebus

Queste e altre cazzate su **http://www.tipiloschi.net**