Dicembre 2018

NEWSLETTER

N°14

Prevenzione della criminalità:

Un'informazione corretta ci preserva da sorprese.

- Internet questo mondo sconosciuto ma ingannevole!

Con questa newsletter ritorniamo ad occuparci di rete, posta elettronica, raggiri e truffe varie che in internet trovano un terreno molto fertile e vario. Chi per motivi vari utilizza questa tecnologia, non è al riparo da tutte quelle situazioni che, anche se non andiamo a cercarle, ci arrivano da differenti posti.

Qualcuno si può chiedere come fanno questi criminali a sapere il nostro indirizzo di posta elettronica o conoscere il nostro profilo social. Innanzitutto dobbiamo confermare che in molti casi siamo noi stessi a fornire questi dati. Pensiamo agli acquisti on line che sicuramente facciamo. La prima informazione che richiedono, dopo l'indirizzo completo, è il nostro numero di cellulare per "essere rintracciabili". Dobbiamo ritenere che molti siti a cui ci iscriviamo per ricevere questo o quel tale articolo, vendono queste liste con i nostri dati a ditte o gruppi di persone che le utilizzano poi in modo fraudolento.

Queste liste vengono pagate dai criminali a peso d'oro poiché contengono una moltitudine di informazioni utili a questi scopi.

Tra le tante attività che possiamo annoverare tra i delinquenti che operano in rete, troviamo quelle che vengono definite “Romantic scam” oppure “love scam”. Queste truffe a sfondo romantico, posso svolgersi in differenti maniere.

La più classica viene avviata tramite i social, Facebook un primis. Questi *scammer* che operano dall’Africa, hanno il compito di contattare una persona ed iniziare il loro lavoro di adescamento digitale. Hanno a disposizione mezzi e materiale adatto per far credere alla vittima che quello che dicono è la verità.

La foto ritrae delle persone che sono ingaggiate da queste bande di criminali in cui il loro scopo è solamente quello di spillare dei soldi per i loro loschi affari.

Troviamo anche gruppi più piccoli che lavorano in questa modalità, il cui scopo comune è sempre quello di estorcere del denaro.

Gli scammer in questione usano le vere identità di soldati americani, giurano amore eterno, chiedono soldi (il più possibile) e poi spariscono. La loro trappola la tessono attorno ad un segreto che vogliono svelarvi e richiedono di non parlarne con nessuno. Arrivano perfino a chiedere di raggiungerli nel paese dove sono stanziati per unisrsi al matrimonio. Questi scammer, con astuzia, entreranno in intimità con la vittima facendole vivere una favola. Stimolano la fantasia delle vittime con frasi sessualmente piccanti.

Il risultato è che la vittima inizia ad inviare ingenti quantità di denaro alla persona (presunta) conosciuta sui social, finche ad un dato momento spariscono e non saranno più rintracciabili.

Una seconda modalità di approccio è molto più diretta. Si riceve sul proprio indirizzo di posta elettronica una mail di una donna oppure di un uomo a dipendenza del titolare dell’indirizzo acquisito illegalmente da questi criminali.
La mail contiene anche degli spunti a sfondo sessuale esplicito, e chiedono di inviargli i nostri dati completi magari anche di codici bancari.

-------- Messaggio originale --------
Da: Trena <contato@transformesorrisos.org.br>
Data: 13/12/18 04:50 (GMT+01:00)
A: @bluewin.ch
Oggetto: Felisa

I am having a coffee close to your place.
Do you want to call me on a date?
I have a lot of free time and I'm interested in new acquaintances.
Send you my location, bloke.
Click the link.

Rispondi Risp. tutti Inoltra Elimina Thread

Traduzione:
Sto bevendo un caffè vicino a casa tua.
Vuoi chiamarmi per un appuntamento?
Ho molto tempo libero e sono interessato a nuove conoscenze.
Ti mando la mia posizione, ragazzo
Clicca il link.

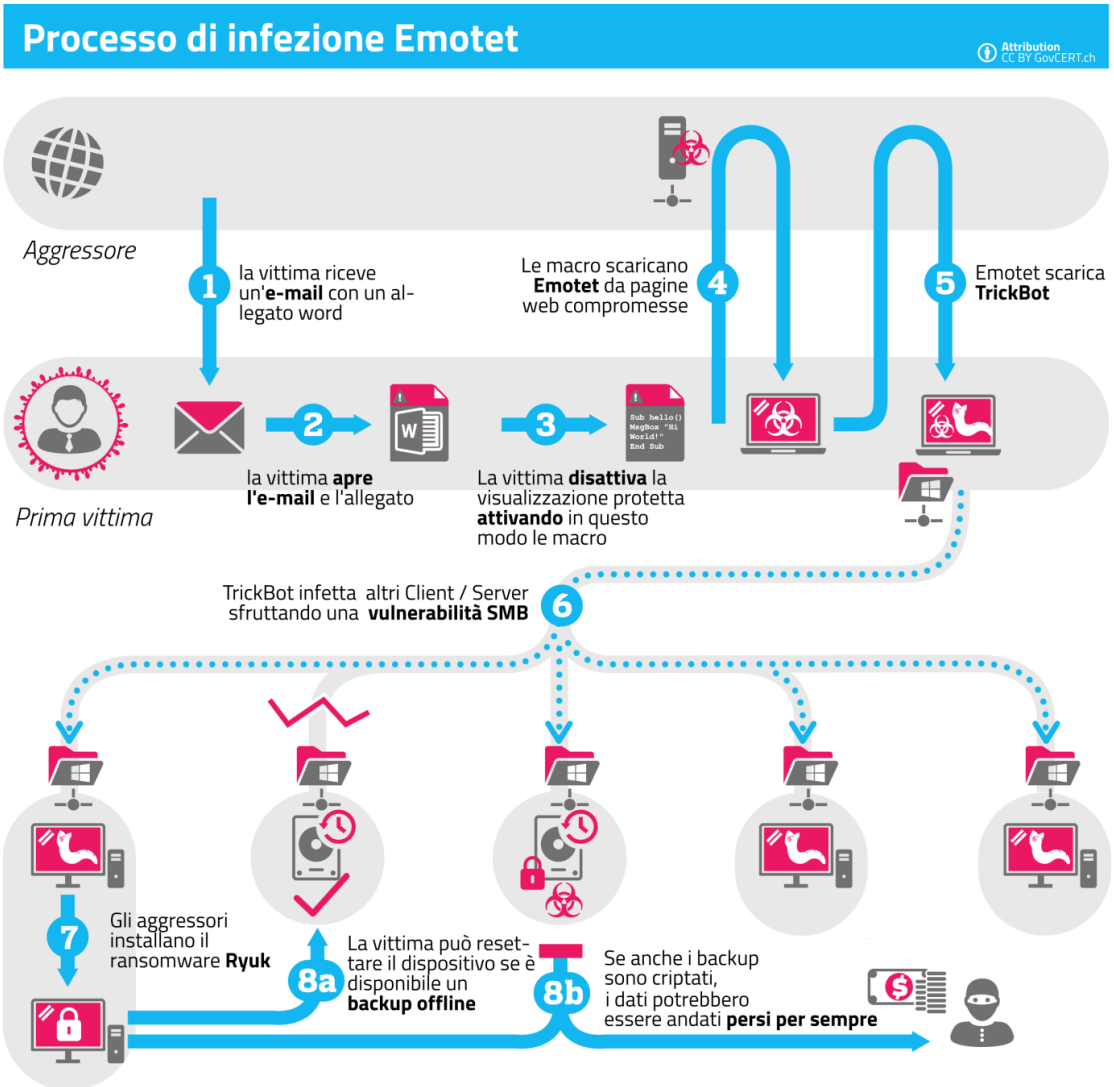
In questa seconda modalità si aprono due concetti. Il primo che cliccando sul link che trovo a fine mail, vado a scaricare un virus o un trojan che mi blocca il computer oppure che prende il suo controllo in remoto.
Seconda possibilità che inizio una conversazione con questa persona, che di fatto non so chi possa essere, e da li scatta una “romantic scam” con le medesime modalità spiegate sopra.

Trojan Emotet

In questi ultimi tempi si assiste alla comparsa in diverse ondate di e-mail infette con un allegato word. Si tratta di un trojan ormai noto da tempo di nome Emotet (oppure Heodo). L’apertura di questo allegato word, a cui è associata una serie di macro, installa sul nostro computer dei programmi che cifrano i dati per poi passare a chiedere il pagamento per poter rientrare in possesso dei dati.

Maggiori informazioni si possono trovare sul link riportato sotto.

https://www.melani.admin.ch/melani/it/home/dokumentation/bollettino-d-informazione/Trojaner_Emotet_greift_Unternehmensnetzwerke_an.html



Fenomeno in continua evoluzione

Per evitare spiacevoli sorprese, la Polizia cantonale invita la popolazione a prestare particolare attenzione quando naviga in internet, e si raccomanda di seguire queste semplici precauzioni:

- Diffidate delle e-mail ricevute senza sollecitazione. Solitamente il mittente sfrutta indirizzi riconducibili a ditte degne di particolare fiducia.
- Diffidate delle e-mail di cui non conoscete l'indirizzo del mittente ed evitate di rispondere.
- Usate prudenza se ricevete e-mail che sollecitano un'azione da parte vostra e vi minacciano altrimenti di conseguenze (perdita di denaro, querela penale, blocco del conto, occasione mancata, disgrazia)
- In caso di e-mail sospette non aprite allegati, link, file eseguibili (.exe).
- Mantenete costantemente aggiornati il sistema operativo e le applicazioni presenti sui vostri dispositivi (ad es. antivirus).

Per ovviare a problemi legati a virus o programmi malevoli, bisogna avere un rigore in quelle che sono le azioni di protezione del proprio computer. Il sito Melani - Centrale d'annuncio e d'analisi per la sicurezza dell'informazione troviamo delle regole molto valide per mantenere la protezione dei computer alta. Posso anche inoltrare delle segnalazioni che poi verranno vagliate.

https://www.melani.admin.ch/melani/it/home.html

Melani consiglia anche altre regole per evitare che questi programmi si insinuino nei vari computer.

- effettuate regolarmente una copia di backup dei dati. La copia di backup deve essere archiviata offline, cioè su un supporto esterno, ad esempio un disco rigido esterno. Assicuratevi pertanto di scollegare il supporto su cui si sta eseguendo il backup dal computer o dalla rete dopo l'operazione di backup. In caso contrario, i dati sul supporto di backup potrebbero venir criptati e resi inutilizzabili in caso di infezione ransomware;
- sia il sistema operativo sia tutte le applicazioni installate sul computer e sul server (ad es. Adobe Reader, Adobe Flash, Oracle Java, ecc.) devono essere costantemente aggiornati. Se disponibile, è meglio utilizzare la funzione di aggiornamento automatico;
- segmentate la rete in base a diverse zone di fiducia, aree di applicazione e/o regioni (separazione delle reti client/server/ e controller di dominio così come delle reti di produzione, ciascuna con amministrazione isolata);
- rispettate il principio dell'assegnazione minima dei diritti, in particolare per i drive di rete (nessun utente dovrebbe avere accesso a tutti i dati se non ne ha bisogno);
- utilizzate dispositivi dedicati con accesso a internet assente o limitato per la gestione dei sistemi e per effettuare pagamenti.

Buona navigazione in sicurezza.

Appuntamento alla prossima newsletter.

Polizia Cantonale
Addetto alla prevenzione

Sgtm c **Claudio Ferrari**

Mail to: polizia@polca.ti.ch