Polizia di Stato

Ransomware, Phishing, reati informatici.

Cosa fare ?

Vice Questore

Dott.ssa Lisa Di Berardino

Compartimento Polizia Postale e delle Comunicazioni Lombardia

ARGOMENTI

- Trading on line
- Social engineering
- Malware
- Phishing
- Man in the middle
- Ceo fraud

Polizia di Stato

TRADING ON LINE

Il **trading online** (TOL) è una modalità di investimento in borsa particolarmente diffuso in epoca recente.

Lo si può fare da casa e dal proprio computer e di norma è richiesto di aprire un account presso un broker finanziario.

Fare trading online vuol dire acquistare e vendere titoli finanziari via internet.

E in particolare dal **proprio** computer.

Polizia di Stato

TRADING ON LINE

Il presunto broker opera secondo uno schema comune:

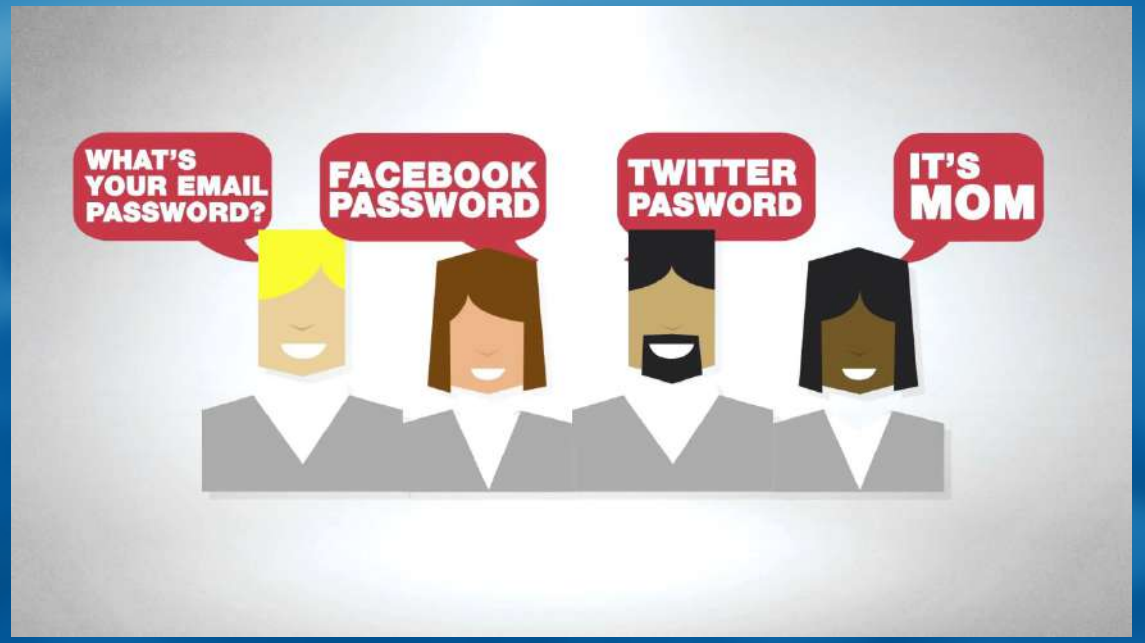
- La vittima viene contattata da una persona che si presenta quale broker operante per conto di una società effettivamente esistente e munita delle apposite autorizzazioni
- I primi contatti hanno natura «esplorativa » e sono volti ad avere notizie in ordine alla disponibilità economica della vittima. Sono seguiti da uno scambio di informazioni via mail (o addirittura tramite sistemi di messaggistica Whatsapp, Telegram, etc.) ove il truffatore sembra utilizzare un account di pertinenza della società regolarmente operante nel settore
- Richiesta di un primo bonifico di una piccola somma, compresa tra i 100 ed i 500 euro
- Seguono richieste di investimenti di portata maggiore, comunque correlate alla situazione finanziaria della vittima secondo le informazioni ottenute inizialmente
- I conti correnti su cui effettuare i bonifici sono generalmente accesi su banche estere
- Nel momento in cui viene richiesto di rientrare dai proprio investimenti, il presunto broker accampa varie scuse quali il blocco delle somme investite o la presenza di vincoli sulle stesse, oppure si rende irreperibile.

TRADING ON LINE
Cosa fare ?

- Controllare sul sito della Consob (www.consob.it) che la società che gestisce il broker sia iscritta nell'elenco delle società autorizzate
- Visitare il sito ufficiale e controllare che, in fondo alla pagina, siano presenti tutte le informazioni relative agli enti regolatori ed alle licenze
- Cercare sul web informazioni ed opinioni sul broker e sulla società
- Diffidare di richieste intese ad ottenere versamenti di somme di denaro su conti correnti di banche estere
- Evitare di :
  - fornire i propri dati personali
  - trasmettere documenti attraverso sistemi di messaggistica istantanea
  - scaricare software forniti dal presunto broker

SOCIAL ENGINEERING

Riguarda tutte le azioni che consentono di ottenere informazioni su fonti aperte (social network) o con l'inganno (confidenze, telefonate o mail fake, travestimenti…)



MALWARE

Il *trojan horse* è un programma agganciato ad un software innocuo che una volta installato consente di prendere il controllo parziale o totale del dispositivo target infettato

Funzioni:

- ***Trasformazione del host in bot***
- ***Esecuzione di azioni (script) non controllabili dall'utente***
- ***Key logging***
- ***Screen recording***
- **Intercettazioni ambientali audio-video**

PHISHING

- **Principali forme del phishing:**
  - Deceptive phishing
  - Search-engine Phishing
  - Smishing
  - Vishing
  - Spear Pishing

PHISHING

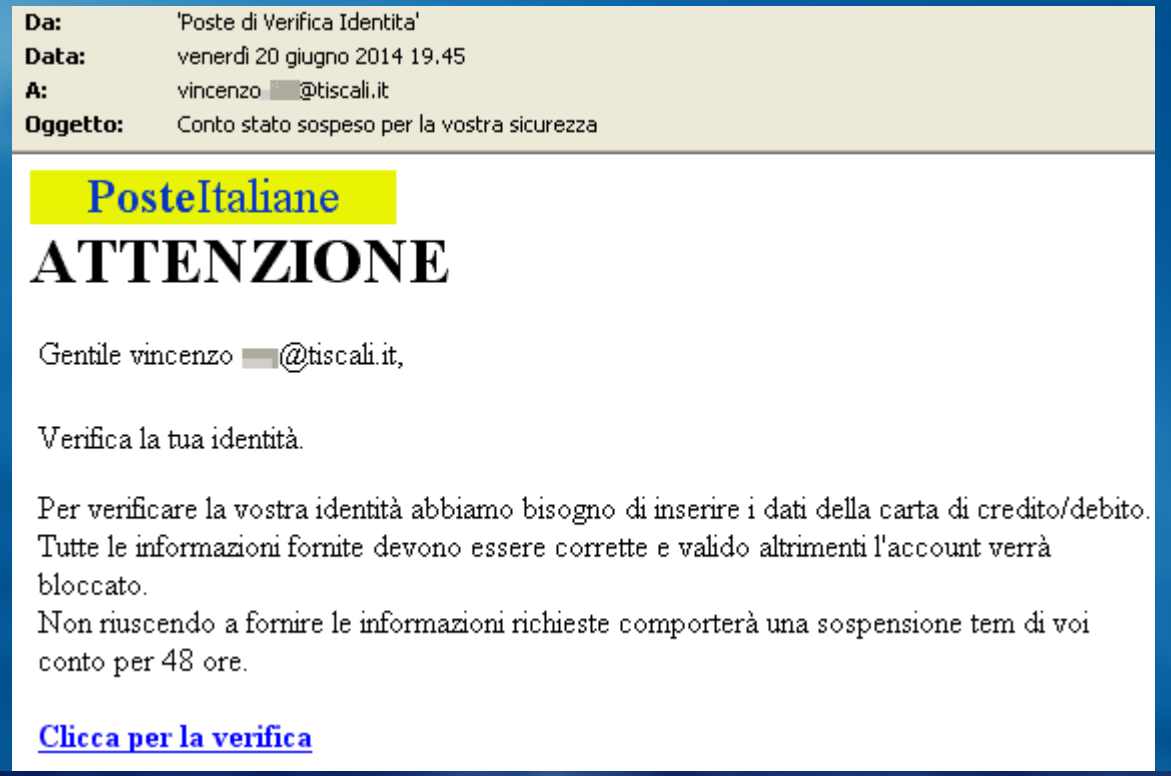
Frode informatica mirata alla sottrazione di dati personali (come le credenziali utente) attraverso l'azione inconsapevole dell'utente, generalmente tramite invio di e-mail fittizie con link che rimandano a un sito clone della banca

Suggerimenti:

Le banche non chiedono dati via mail

Il linguaggio è impreciso

Il tono è intimidatorio



Da: 'Poste di Verifica Identita'
Data: venerdì 20 giugno 2014 19.45
A: vincenzo [redacted]@tiscali.it
Oggetto: Conto stato sospeso per la vostra sicurezza

PosteItaliane

ATTENZIONE

Gentile vincenzo [redacted]@tiscali.it,

Verifica la tua identità.

Per verificare la vostra identità abbiamo bisogno di inserire i dati della carta di credito/debito.
Tutte le informazioni fornite devono essere corrette e valido altrimenti l'account verrà bloccato.
Non riuscendo a fornire le informazioni richieste comporterà una sospensione tem di voi conto per 48 ore.

Clicca per la verifica

DECEPTIVE PHISHING

Il «**Deceptive Phishing**» (*phishing ingannevole*) è una tecnica che consiste in una fase iniziale di *spamming* di posta elettronica verso innumerevoli destinatari, inducendo questi ultimi a cliccare su un link contenuto nel messaggio per visualizzare così una pagina web identica o quasi a quella originale, di cui se ne replica l'impostazione grafica, loghi, etc.

Non appena l'utente inserisce le proprie credenziali di accesso sulla pagina «*fake*», il phisher è in grado di recuperare le informazioni per sottrarre denaro, stipulare contratti, o in generale per procurarsi un vantaggio economico, ad esempio vendendo i dati in un mercato secondario.

SEARCH-ENGINE PHISHING

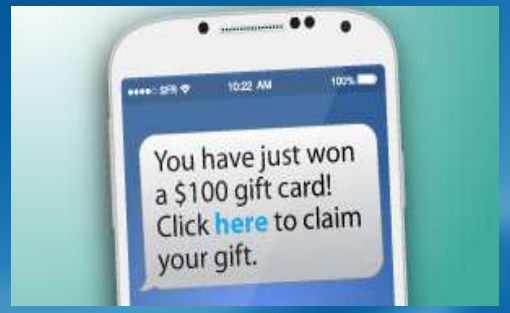
Il «**Search-engine phishing**» (*phishing basato sui motori di ricerca*) è una tecnica con la quale l'attaccante pone in essere l'attacco mediante la creazione di pagine web dedicate a prodotti fittizi, che vengono poi indicizzate sui motori di ricerca (es. Google, Yahoo!, etc) cosicchè gli utenti, facendo un ordine di acquisto o disponendo trasferimenti di denaro, forniranno al phisher le credenziali di accesso ai conti correnti.

Un esempio di tale attacco può essere un sito web e-commerce, contenente prodotti a prezzi particolarmente vantaggiosi, che compare nei risultati di ricerca di Google: l'utente procede ad effettuare l'acquisto, i dati di pagamento vengono sottratti e il denaro viene quindi prelevato indebitamente.

.

SMISHING

E’ il phishing realizzato tramite l’invio di sms



L’invio massiccio di sms tramite gsm-box e relativo software, utilizzando schede telefoniche di gestori esteri, acquistate su mercatini on-line, gia’ attive

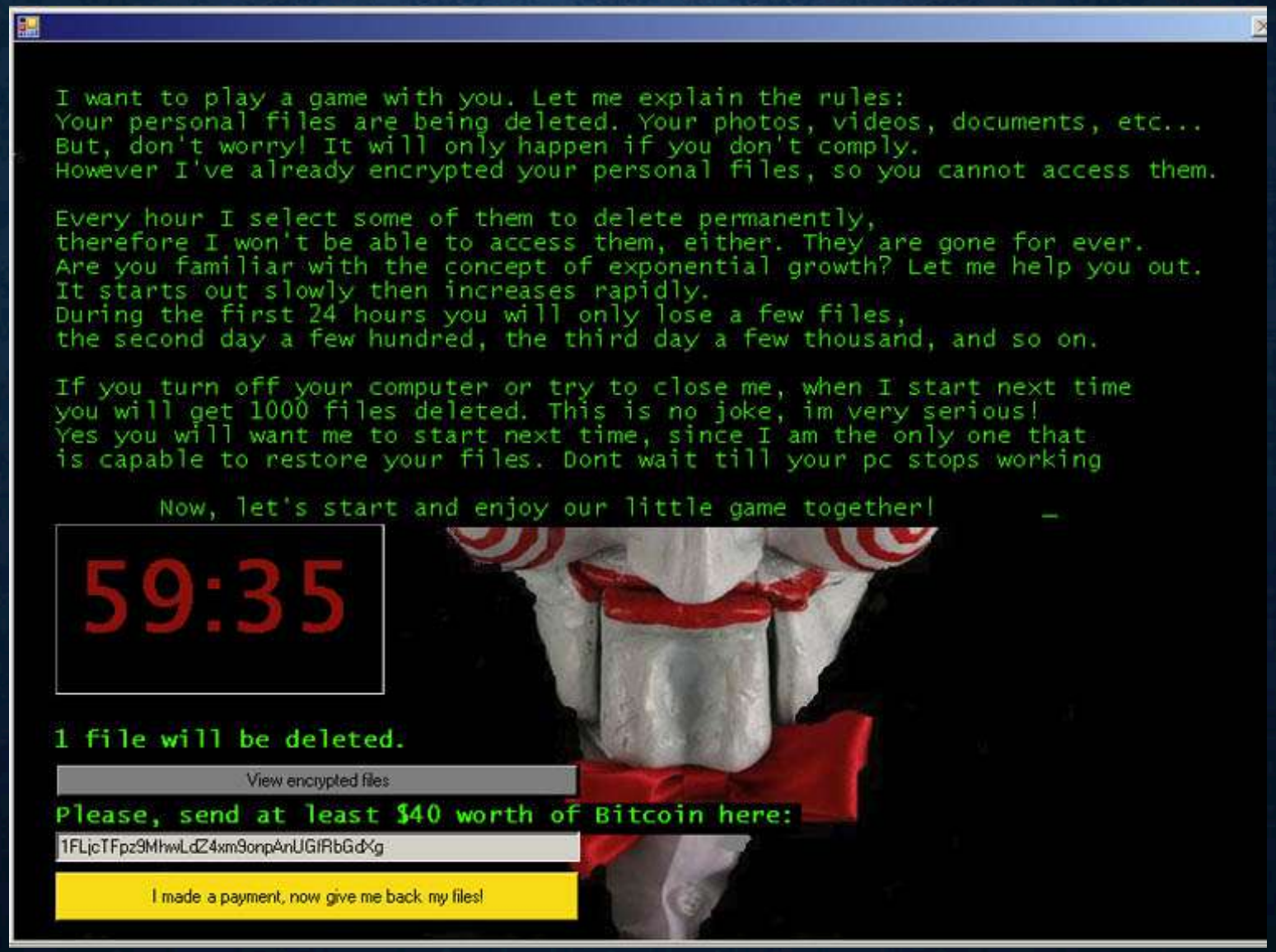
Polizia di Stato

CRYPTOLOCKER
MODALITÀ D'INFEZIONE

- Quale che sia la modalità d'infezione, il danno provocato è molto simile. Nello specifico:
- **Vengono crittografati i file utente degli hard disk del computer** (le estensioni dei files.variano a seconda della tipologia di virus, sono comunque colpite le estensioni più diffuse come: .DOC,.DOCX,.XLS, .XLSX, .PDF, .JPG, .MDB, .PST).
- **Vengono crittografati i file presenti in hard disk o pennette USB connessi all computer al momento dell'infezione o successivamente**,
- **Vengono crittografati i file dell'utente presenti in cartelle di rete condivise da altri computer.**

Polizia di Stato

CRYPTOLOCKER: ESEMPIO DI MESSAGGIO



CRYPTOLOCKER
Cosa fare ?

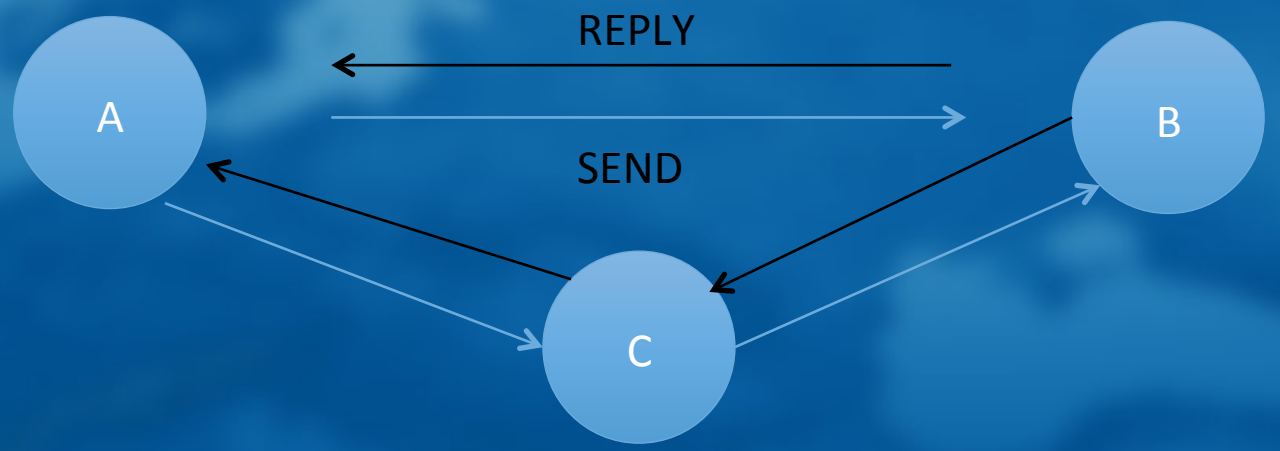
- Porre particolare attenzione alle mail che giungono da mittenti sconosciuti ed ai relativi allegati : la mail è ancora il veicolo maggiormente utilizzato per inoculare nel sistema file indesiderati
- Aggiornare costantemente il sistema operativo
- Dotarsi di sistemi antivirus che siano efficaci e costantemente aggiornati
- Programmare un backup giornaliero dei dati così da poter recuperare i file oggetto dell'attacco
- Predisporre il sistema affinché almeno una copia del backup venga memorizzata su hardware non configurato sulla rete, così da non possa essere fisicamente raggiungibile dal malware

MAN IN THE MIDDLE
Business Email Compromise

Attraverso il furto dell'identità digitale l'*hacker* si impossessa della casella di posta di un dipendente aziendale, oppure tramite tecniche di *social engineering* apprende che è in essere una corrispondenza elettronica di carattere commerciale tra due utenze.

MAN IN THE MIDDLE
Business Email Compromise

In entrambi i casi l'*hacker* si intromette nella comunicazione osservando, intercettando o replicando verso un'altra destinazione prestabilita, i messaggi inviati dai due interlocutori.



MAN IN THE MIDDLE
CEO Fraud

1) L’hacker impersonifica il CEO (AD) e contatta il CFO (contabilità) o un suo dipendente ordinandogli il trasferimento di denaro a saldo di un pagamento dovuto per il perfezionamento di un contratto.

2) Il dipendente viene contattato da un sedicente avvocato internazionale per i dettagli

3) La pressione psicologica esercitata dalle figure autorevoli e l’urgenza di concludere il «deal» inducono il collaboratore ad effettuare il bonifico

MAN IN THE MIDDLE e CEO FRAUD
Cosa fare ?

- **Management**

- Protocolli di sicurezza e classificazione per il trattamento di dati e documenti che devono rimanere riservati
- Procedure di risk assesment e risk management, con gestione e mitigazione degli incidenti di sicurezza
- Monitoraggio della rete e predisposizione di apparati di sicurezza interna e perimetrale, sia fisica che logica
- Training costante del personale e rigide policy relative alla comunicazione all'esterno di informazioni interne su ruoli e competenze

MAN IN THE MIDDLE e CEO FRAUD
Cosa fare ?

- **Personale**

- Diffidare di telefonate, visite, messaggi o e-mail non attese con richieste di informazioni su dipendenti ed organizzazione
- Non fornire mai dati bancari via mail o attraverso link che rimandano a siti web
- Controllare header e dominio delle email
- Evitare di aprire allegati sospetti e comunque utilizzare misure di sicurezza (antivirus, firewall) possibilmente gestiti centralmente
- Verificare la reale identità del mittente contattando telefonicamente la sua azienda

Grazie per l’attenzione

Polizia di Stato

SUB LEGE LIBERTAS

polizia delle comunicazioni