UNIVERSITÀ DEGLI STUDI
DI MILANO

Frode informatica

Politecnico di Milano – 17.05.2024

Avv. Davide Zaninetta

Detenzione e diffusione abusiva di codici d'accesso

L'art. **615-quater c.p.** punisce con la reclusione fino a 2 anni e con la multa sino a euro 5.164 «*chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparati, strumenti, parti di apparati o di strumenti, codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo*».

Detenzione e diffusione abusiva di codici d'accesso

La pena è della reclusione da uno a tre anni e della multa da euro 5.164 a euro 10.329 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) al quarto comma dell'art. 617 quater c.p, quindi se il fatto è commesso:

1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;
2) da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;

Detenzione e diffusione abusiva di codici d'accesso

L'art. 615 quater c.p. sanziona, in un'ottica preventiva, l'abusiva acquisizione e diffusione dei mezzi o codici di accesso ad un sistema informatico o telematico, protetto da misure di sicurezza.

La fattispecie incriminatrice si pone in un'ottica anticipatoria della tutela penale anche rispetto a quei reati informatici come la frode informatica, giacché non solo mira ad interdire la diffusione degli strumenti necessari per la relativa commissione, ma non richiede neppure, essendo un reato di pericolo, l'effettivo conseguimento del profitto.

Detenzione e diffusione abusiva di codici d'accesso

Sotto il profilo dell'elemento oggettivo, la norma sanziona la condotta di chi illegittimamente operi su codici di accesso, parole chiave o altri mezzi di accesso a sistemi informatici protetti da misure di sicurezza. Vi rientrano sia gli strumenti «virtuali» di accesso (password e codici) che quelli fisici (chiavi meccaniche e tessere elettroniche).
Per ciò che riguarda l'elemento soggettivo, trattasi di reato a dolo specifico: il soggetto deve agire con la finalità di conseguirne un profitto per sé o per altri o arrecare ad altri un danno. Va richiamata la nozione ampia di profitto secondo cui il vantaggio può essere anche di carattere non patrimoniale (ad es. movente di soddisfazione morale).

Il concorso tra i delitti di cui agli artt. 615-ter e 615-quater

«Il delitto di cui all'art. 615-quater cod. pen. ***non può concorrere con quello, più grave, di cui all'art. 615-ter cod. pen.****, del quale* ***costituisce naturalisticamente un antecedente necessario****, sempre che quest'ultimo, oltre ad essere procedibile, risulti integrato nel medesimo contesto spazio-temporale in cui sia stato perpetrato l'antefatto ed in danno della medesima persona offesa».*

(Cass. Pen., Sez. II, 14 gennaio 2019, n. 21987).

La frode informatica

Art. 640 ter c.p.

*«Chiunque, **alterando** in qualsiasi modo il funzionamento di un sistema informatico o telematico o **intervenendo senza diritto** con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un **ingiusto profitto con altrui danno**, è punito con la reclusione **da sei mesi a tre anni** e con la multa da euro 51 a euro 1.032.»*

La frode informatica: le aggravanti/1

- pena della reclusione da **uno a cinque anni** e della multa da 309 euro a 1.549 euro se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640 (Stato o ente pubblico), **ovvero se il fatto produce un trasferimento di denaro, di valore monetario o di valuta virtuale o è commesso con abuso della qualità di operatore del sistema.**

La frode informatica: le aggravanti/2

- pena della reclusione da **due a sei anni** e della multa da euro 600 a euro 3.000 **se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti.**

La frode informatica: la procedibilità

- Di regola, il delitto punibile a **querela della persona offesa.**

- Se ricorre taluna delle circostanze aggravanti (di cui al secondo e terzo comma) o la circostanza prevista dall'articolo 61, primo comma, numero 5, limitatamente all'aver approfittato di circostanze di persona, anche in riferimento all'età, si **procede d'ufficio.**

Frode informatica e Truffa

- La frode informatica richiama chiaramente quanto disposto dall'art. 640 c.p. in tema di **truffa**.

- Tuttavia, ai fini della configurabilità della frode informatica **non è richiesta l'induzione in errore** della vittima, poiché l'attività fraudolenta investe il sistema informatico.

Frode informatica e Truffa

- Le due norme sono poste in **rapporto di specialità** ed è pertanto **escluso il concorso** tra le due fattispecie.

- Ciò significa che se oltre all'alterazione del sistema informatico si registri anche **l'induzione in errore della persona**, tipica della truffa, allora prevale quest'ultima.

Frode informatica e Truffa

- il delitto di frode informatica (art. 640 ter c.p.) «*ha la medesima struttura ed i medesimi elementi costituitivi della truffa, dalla quale si differenzia solamente perché l'attività fraudolenta dell'agente investe* ***non la persona, di cui difetta l'induzione in errore,*** *bensì* ***il sistema informatico di pertinenza*** *(…)*».

Cass. Pen., sez. II, 05 febbraio 2020, n. 10354

Frode informatica e Accesso abusivo

- Il delitto di accesso abusivo «*può concorrere con la frode informatica, **diversi essendo i beni giuridici tutelati e le condotte sanzionate***».
- **L'accesso abusivo** tutela il domicilio informatico sotto il profilo dello «ius excludendi alios»;
- la **frode informatica** contempla l'alterazione dei dati immagazzinati nel sistema al fine della percezione dell'ingiusto profitto.

Cass. Pen., sez. II, 29 maggio 2019, n. 26604

Il «Phishing»

- Tra gli attacchi informatici che possono essere commessi mediante *malware* rientra anche il c.d. ***phishing***.
- Il *phishing* o «spillaggio dei dati» è un'attività illegale che sfrutta una tecnica di ingegneria sociale mediante l'utilizzo delle comunicazioni elettroniche (soprattutto messaggi e-mail fasulli o messaggi istantanei) ed è utilizzata per ottenere l'accesso a informazioni personali o riservate **con la finalità del furto d'identità**.

Il «Phishing»

- Grazie a messaggi che imitano grafico e logo di siti istituzionali, l'utente è ingannato e portato a rivelare i propri dati personali, come dati di accesso ai sistemi aziendali, numero di conto corrente, numero di carta di credito, codici *home banking*.

Il c.d. «Nigerian scam»

- Truffa risalente ai primi anni ’90, nella quale si veniva contattati via mail per contribuire, mediante pagamento di determinate somme, allo «sblocco» di un’ingente quantità di denaro.

Il c.d. «Nigerian scam»

- Il copione era il seguente: prima venivano chiesti **soldi per la parcella** di un notaio, poi altro denaro per l'avvocato ed infine si era invitati ad un incontro personale nella loro nazione (di solito la Nigeria, da cui il nome della truffa);

- arrivati nel luogo dell'appuntamento o il truffato veniva accolto in modo opulento per dare credibilità e **proseguire la truffa**, oppure veniva **rapinato**.

Un attacco di phishing: come funziona

- Di solito la frode inizia con un invio causale di e-mail ad un elevato numero di destinatari, facendo in modo che la mail appaia provenire da un **destinatario attendibile** (es. datore di lavoro, Ente Pubblico);
- tali messaggi solitamente segnalano presunti problemi tecnici tali da richiedere che l'utente si colleghi ad una determinata pagina web per inserire i propri codici e consentire fantomatiche verifiche.

Problemi di traduzione

- Fino a qualche anno fa, le e-mail truffa erano scritte spesso in inglese o in un pessimo italiano, favorendo così la facile intuizione circa la truffa stessa.

- Recentemente non si è più rilevato il problema della pessima traduzione, rendendo più difficile l'identificazione della truffa.

Le fasi di un attacco di phishing

Un attacco di phishing si compone di regola di **n. 6** fasi:

1- Planning

2- Setup

3- Attack

4- Collection

5- Fraud

6- Post attack

1 - Planning

- Rappresenta la fase «**preliminare**» nella quale si decide chi colpire, quali tecniche utilizzare e quali dati sottrarre.

- Nel caso in cui si voglia raccogliere una buona quantità di dati personali ed e-mail, basterà utilizzare un forum o una mailing list.

- In questa fase si decide inoltre di creare all'occorrenza un sito falso.

2 - Setup

- Mediante questa fase si configurano i **meccanismi per sferrare l'attacco** e si procacciano i contatti e le informazioni sulle vittime.

- In particolare, **si forgiano le e-mail ingannevoli**, si acquisisce una *botnet* per l'invio delle stesse e si cercano siti che contengano grandi quantità di dati personali.

3 - Attack

- In questa fase l'attaccante **instaura il contatto** con le potenziali vittime mediante diversi strumenti informatici o telematici.

- Il caso più ricorrente è quello della mail truffaldina, ma vi sono casi di *phishing* perpetrato via SMS (c.d. *smishing*), via VoIP (c.d. *vishing*) o via QR Code (c.d. *quishing)*.

4- Collection

- In questa fase vengono **sottratte e raccolte** le varie credenziali d'accesso.

- Scopo di chi commette questo reato è, infatti, possedere il **maggior numero di di credenziali possibili** per utilizzarle o per rivenderle su forum specifici.

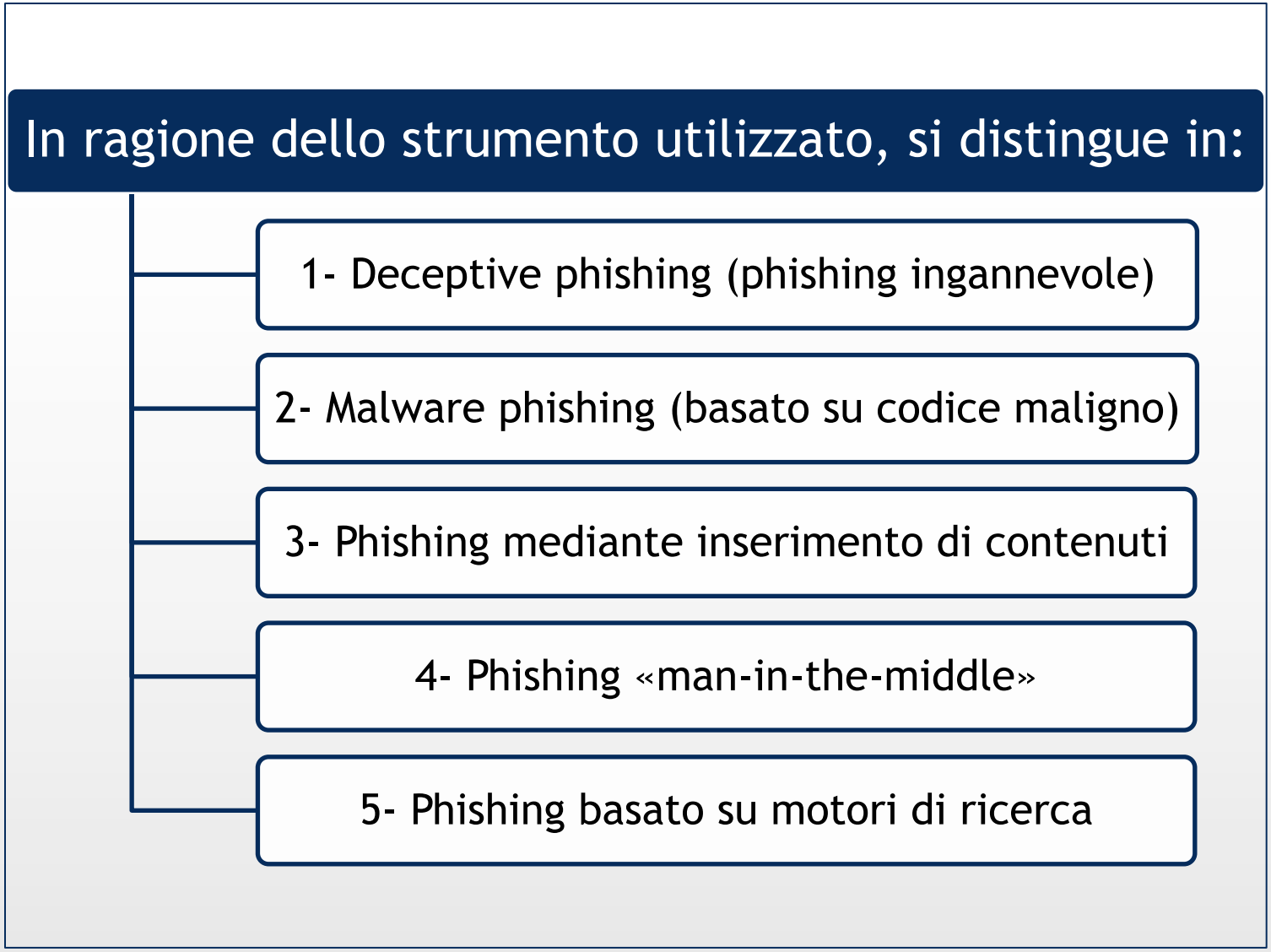
5- Fraud

- In questa fase l'attaccante commercia, vende o usa direttamente le credenziali per scopi fraudolenti.

6- Post attack

- Nell'ultima fase, l'attaccante «smonta» l'apparato predisposto per il *phishing*, cancella le sue tracce eventualmente conservate sui server dove erano ospitati i siti e analizza le reazioni conseguenti all'attacco.

I vari tipi di phishing



1 – Deceptive phishing

- E’ lo schema tradizionale coesistente nell’invio di una mail con un «invito all’azione», ossia l’invito a cliccare il link contenuto nella mail per essere poi reindirizzato al sito fraudolento.

2 – Malware phishing

- Questo tipo di phishing presuppone che l'attaccante sia riuscito ad eseguire un software malevolo sul computer dell'ignara vittima.

3 –Phishing con inserimento di contenuti

- Questa tecnica consiste nell'inserire contenuti malevoli in un sito legittimo.

- Mediante tali contenuti, ad esempio, si potrà essere reindirizzati verso siti fraudolenti o si potrà installare un malware all'interno del sistema «vittima».

Le finestre Pop-up

- La tecnica delle finestre di popup è senza dubbio la scelta che garantisce il migliore rendimento per il «*phisher*»; infatti mentre in *background* è presente il vero sito, una finestra priva di barra degli indirizzi, degli strumenti ed in alcuni casi anche con il tasto destro disabilitato richiede informazioni riservate al malcapitato utente.

4- Phishing «man-in-the-middle»

- Mediante questo attacco, il *phisher* si interpone nella comunicazione tra l'utente e il sito legittimo, catturando tutti i dati in transito.

- Tali attacchi sono praticamente **impossibili da scoprire lato utente**.

- L'unica soluzione consiste nel non affidare mai credenziali riservate se non su canali cifrati.

5- Phishing basato su motori di ricerca

- In alcuni casi, il *phisher* crea pagine web clonate da istituti bancari o dedicate a finti prodotti venduti a prezzi estremamente vantaggiosi e, mediante apposite tecniche, fa in modo che queste pagine siano indicizzate con rating elevati nei motori di ricerca.

5- Phishing basato su motori di ricerca

- L’utente generalmente non va oltre i primi 5 risultati del motore di ricerca.

- Nel momento in cui si crede di comprare un determinato prodotto o di collegarsi alla propria banca, si consegnano le credenziali al phisher.

Alcuni casi celebri: indagine Phish & Chip

- Nel 2007 viene effettuato un massiccio attacco di phishing ai danni di Poste Italiane.

- In particolare, si sono registrate diverse transazioni fraudolente verso due carte *postepay* attivate il giorno precedente.

Phish & Chip: le indagini

- Tutte la mail partivano da un unico *provider;*
- Vennero pertanto acquisiti i *log* dal *provider;*
- Da tali *log* si giunge ad un'utenza cellulare che viene intercettata;
- Mediante pedinamenti viene individuato l'utilizzatore del numero di cellulare intercettato e si scopre dell'esistenza di un complice che creava la mail fraudolente, anche mediante una rete estera.

Phish & Chip: l'anello debole

- Una delle leggerezze commesse è stata quella di ricaricare le carte *postepay* intestate a soggetti persone fisiche;

- Il procedimento portò all'emissione di ordinanze cautelari nei confronti di n. 26 soggetti ed alla scoperta che nel frattempo era in atto una truffa analoga nei confronti dei clienti di Banca Intesa

UNIVERSITÀ DEGLI STUDI
DI MILANO

Grazie per l'attenzione!