

## **IV) Fattore Umano e Ingegneria sociale**

**Tipologie criminali più complesse**

**Dal Phishing allo Smishing al Vishing**

**Analisi di casi concreti**

**Cybercrime e settore finanziario italiano**

# Ruolo del fattore umano e dell'ingegneria sociale

- Aumento esponenziale degli attacchi super tecnologici
- Corrispondente miglioramento delle contromisure tecnologiche
- Le contromisure non sono mai sufficienti a garantire una sicurezza adeguata
- In gioco la grande variabile del fattore umano

# Fattore umano e ingegneria sociale

- Gli attaccanti si concentrano sempre più sul fattore umano per raggiungere i loro obiettivi riducendo rischi e investimenti
- Il fattore umano come anello debole “anche” della sicurezza Cyber come di ogni sicurezza
- Il ruolo dell’ingegneria sociale e le intramontabili mail di phishing

## **Più dell'85% delle violazioni nel 2021 ha coinvolto un elemento umano**

Il rapporto Verizon Data Breach Investigations per il 2021 ha rilevato che circa l'85% delle violazioni ha coinvolto un elemento umano e il 61% ha coinvolto l'utilizzo delle credenziali di un dipendente rubate dall'azienda.

Secondo Verizon, nel 2021, la maggior parte degli attacchi proveniva da ingegneria sociale, phishing e attacchi Denial of Service. In particolare, il phishing è diventato una delle minacce più significative durante la pandemia.

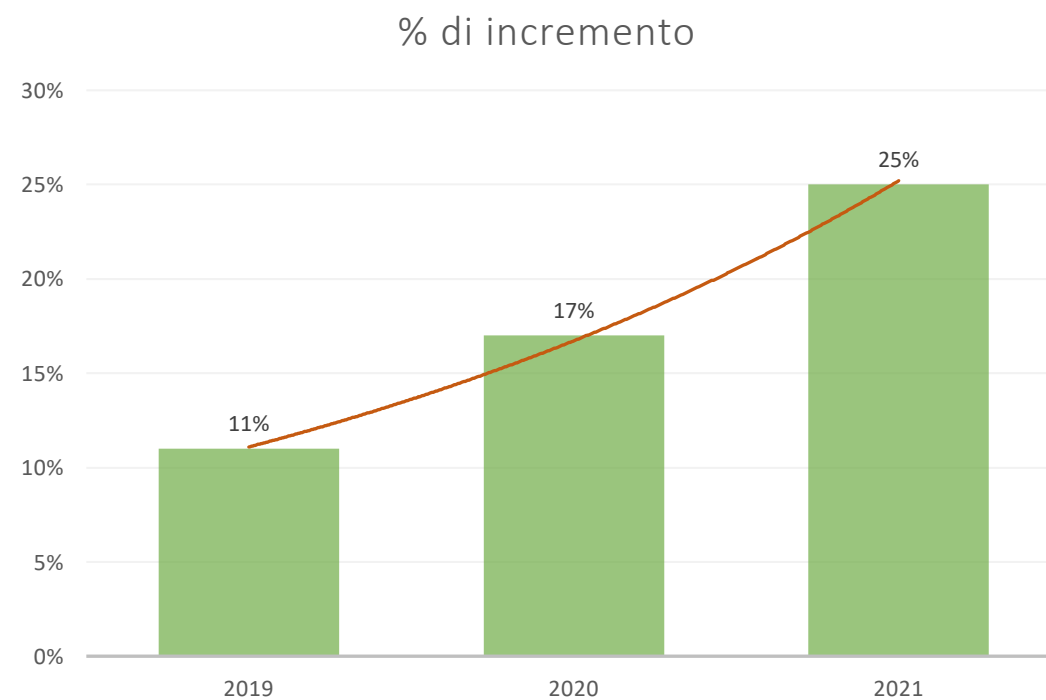
# Ingegneria sociale

Gli attacchi di **phishing, che rimangono tra i più diffusi**, hanno contribuito a compromettere ogni genere di azienda, con un focus globale sul settore manifatturiero e ingegneristico, healthcare, servizi e tecnologia.

Una ricerca di Verizon ha indicato che nel 2021 si sono registrati quasi 30.000 attacchi dovuti per lo più ad attività di social engineering e server exploitation.

Il 25% degli attacchi mappati nel primo semestre del 2021 è stato diretto verso l'Europa. Il dato è interessante perché, secondo il rapporto Clusit, nel 2020 gli attacchi gravi contro l'Europa sono stati il 17% ed erano solo l'11% nel 2019.

# Incremento percentuale attacchi di tipo Social Engineering verso l'Europa anni 2019-2021



# Social engineering

## Attacco a tre fasi

Viene evidenziata la crescita della modalità di **attacco alle aziende** cosiddetta '**a tre fasi**': 1)**invio di una mail di phishing** che include un link a un sito web dannoso o un allegato malevolo; 2) **download del malware** sul Pc dell'utente, in grado di rubare le credenziali di numerose applicazioni; 3)**uso delle credenziali sottratte per futuri attacchi** come l'accesso, ad esempio, a siti web di banche o siti di e-commerce

- Il problema degli utenti che 'aprono' allegati e cliccano su link dannosi, è dunque annoverato tra le principali falle della sicurezza, poiché in questo modo viene data la possibilità ai criminali di introdurre un malware e aprire loro una breccia



# Ingegneria sociale

Il rapporto annuale Clusit sulla sicurezza ICT in Italia denota già dal 2016 **la crescita dell' ingegneria sociale**.

Emblematico tra i dieci attacchi più rappresentativi del 2015 quello riguardante la violazione di una casella mail personale su America on Line (AOL in uso al capo della CIA John Brennan).

Violazione rivendicata da un sedicente gruppo di hacker adolescenti (CWA, Crackers With Attitude) col commento: «**ci sarebbe riuscito anche un bambino di 5 anni**», spiegando di aver utilizzato «**banali tecniche di social engineering**» nei confronti di Verizon (ISP di Brennan) e AOL (provider del servizio di posta) per ottenere l'accesso. Ma, come osservato nel rapporto Clusit, data la natura del target e le modalità professionali con cui gli hacker hanno operato, si fa fatica a credere che si tratti di adolescenti annoiati, come invece alcuni suppongono.

# Ingegneria Sociale

## Annotazioni a margine

A prescindere dal livello di professionalità degli attaccanti, l'utilizzo di «**banali tecniche di social engineering**» è bastato a fare breccia e, allo stato attuale, continua a mietere vittime.

Altro elemento di interesse : l'attacco è stato condotto non direttamente sulla persona oggetto di interesse, ma su terzi detentori dei dati. Questo significa che anche un obiettivo “iper protetto” o “iper attento” può essere raggiunto con tecniche la cui banalità è solo apparente.

## INGEGNERIA SOCIALE : OPZIONI BASICHE DI UTILIZZO

Opzione 1: utilizzare tecniche di IS per saltare tutta la parte di cosiddetto cracking vero e proprio e arrivare direttamente ai risultati che quindi possono diventare subito gli obiettivi prefissati;

Opzione 2: utilizzare tecniche di IS preparatorie di attività di hacking vero e proprio per raggiungere risultati (intermedi) come punti di partenza per ulteriori mirati strumenti di cracking accelerando il raggiungimento dell'obiettivo prefissato e assicurandosi la possibilità di reiterazione delle attività iniziali

# Modelli /percorsi di ingegneria sociale opzione o percorso 1)

## A) L'attacco a RSA (2011).

- Fase 1 Realizzato attraverso una coalizione tra un primo gruppo di criminali che hanno “penetrato” un livello del network di RSA a bassa priorità mediante una campagna di *phishing* a mezzo posta elettronica.
- Fase 2 In seguito altri cyber criminali sono risaliti nel network fino a compromettere la tecnologia di cifratura impiegata sui diffusissimi token di autenticazione SecureID

# Modelli /percorsi di ingegneria sociale

## Modello o percorso 1)

B) Violazione di una casella mail personale su (AOL) in uso all'allora(2015) capo della CIA John Brennan.

L'attacco è stato condotto non direttamente sulla persona oggetto di interesse, ma su terzi detentori dei dati tramite preponderante utilizzo di tecniche di Ingegneria Sociale.

Attacco agli anelli deboli della catena di difesa: anche un obiettivo "iper protetto" o "iper attento" può essere raggiunto con tecniche la cui banalità è solo apparente

# Ingegneria Sociale

## Esempio di PERCORSO 2

A) Attacco Hacker ( Ransomware) all'ASL Napoli Gennaio 2022

Violato in un primo momento il PC di un medico collegato tramite una VPN alla rete dell'ASL.

Obiettivi di secondo livello: il medico e la VPN Obiettivo di primo livello : la rete ASL

# Ingegneria Sociale

## Percorso 2

B) Esempio il caso della articolata frode informatica a una farmacia campana mirata a carpire i codici di accesso al sistema sanitario regionale per falsificare certificati di vaccini anti Covid (Obiettivo principale slide INDICARE XXX).

L'iter criminale ha consentito di conseguire anche in successivi momenti lucrosi risultati sfruttando le iniziali attività

# ANALISI DI CASI PRATICI DI INGEGNERIA SOCIALE

Si compendiano nella sottrazione di credenziali di utenti di diversi gruppi bancari mediante una combinazione di svariati attacchi di ingegneria sociale

Metodologie tipiche di attacchi tramite ingegneria sociale:

- 1) Phishing 2) Smishing 3) Vishing
- e ... ultimo arrivato il 4) QRishing



# 1) PHISHING

**Phishing:** tipica truffa effettuata tramite invio di email fraudolente per realizzare furti di identità digitali.

Il criminale cerca di ingannare la vittima inducendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un ente affidabile in una comunicazione digitale.

- Il termine phishing è una variante di *fishing* (letteralmente "pescare" in lingua inglese)

## 2) SMISHING I parte

**Il termine** deriva dalla fusione tra “**SMS**”, ovvero il sistema dei messaggi di testo che si inviano tramite cellulare, e “**PHISHING**”.

Il “vettore” della frode, che nel caso del phishing è la e-mail fraudolenta, viene sostituito nello smishing da un SMS via telefono cellulare.

Analogamente ai casi di phishing anche il messaggio di smishing punta a indurre il destinatario ad aprire un allegato contenente malware o ad attivare un link dannoso al prevalente fine di rubare identità digitali e dati utili a sottrarre fraudolentemente denaro.

## 2) SMISHING II parte

I malware contenuti negli allegati malaccortamente aperti potrebbero mascherarsi da app “legittime”, inducendo i destinatari a digitare informazioni confidenziali poi inviate ai cybercriminali.

I link altrettanto ingannevolmente attivati possono aprire siti falsi per acquisire informazioni personali sensibili che i cybercriminali utilizzano per rubare l’ID delle vittime

### 3) VISHING o phishing vocale

Si realizza quando il criminale crea un sistema vocale automatizzato (o manuale) per attivare chiamate vocali verso utenti telefonici e chiedere loro informazioni private.

L'intento fraudolento è lo stesso del phishing e dello smishing.

La chiamata vocale tende sostanzialmente a conferire alla richiesta il carattere di urgenza per accrescere la pressione psicologica sul destinatario e agevolare la rivelazione di informazioni riservate.

## 4) QRISHING

Ultima tendenza invece è il QRishing.

Il distanziamento sociale durante la pandemia ha reso popolari i QR code (Quick-Response) che sono semplici da usare e possono essere piuttosto semplici da generare.

Identificare un messaggio QR falso non è semplice e per tale motivo risulta particolarmente adatto per attività dannose.

Una tattica che è stata osservata consiste nell'incorporare QR code falsi nelle e-mail di phishing inviate da grandi banche europee.

## 4) QRISHING II - parte

Dopo aver scansionato il codice, gli utenti vengono indirizzati a siti Web con pagine di destinazione dall'aspetto realistico, in cui alla vittima potrebbe essere richiesto di accedere per rinnovare le proprie carte di credito.

I codici possono anche indirizzare gli utenti a siti Web in cui è possibile scaricare automaticamente malware.

CASISTICA

# CASO 1.1

Il primo caso di studio riguarda un attacco che coinvolge tutte le tecniche descritte, messa in atto da un organizzazione criminale con impiego di quattro figure ciascuna con un suo ruolo ben preciso.



# CASO 1.2

## RUOLI NELL'ORGANIZZAZIONE

- 1 – **Programmatore o esperto informatico** per l'attivazione di uno spazio web "anonimo" e la creazione di pagine web contraffatte simili alle pagine di noti istituti di credito.
- 2 – **Soggetto che procura numeri di telefono cellulari attivi**, meglio ancora liste «customizzate» di utenti on line di istituti di credito con attivazione di servizio multicanale.  

Di solito le liste di utenti vengono acquisite da Call Center, dalla banca o da operatori telefonici tramite dipendenti infedeli o altri insider
- 3 – **Soggetti con un ottima dialettica** e conoscitori delle tecniche di social engineering
- 4 – **Soggetti senza specifiche competenze** usati per i prelievi agli sportelli.

# CASO 1.3

## Prerequisiti

- **Attivazione di un servizio Voip** con numero chiamante modificabile. Nel caso di specie il numero chiamante era il numero verde utilizzato dall'istituto bancario.
- **Attivazione di un servizio di Bulk Messaging** per l'invio massivo di SMS con mittente artefatto. Nello specifico il mittente era rappresentato da una stringa corrispondente al nome dell'istituto bancario.

# CASO 1.4

## MODUS OPERANDI

Tramite l'emulatore telefono VOIP X-lite i cyber-criminali inviavano molteplici SMS ad una lista precostituita di numeri di telefono reperiti dal **soggetto 2** e scambiati tramite il sito/servizio [www.filestofriends.com](http://www.filestofriends.com) che permette di inviare messaggi mail con allegati fino ad 1 GB in modo anonimo

# CASO 1.5

Gli SMS inviati alle ignare vittime avevano il seguente testo  
*“Gentile cliente, la sua carta è stata bloccata per mancata sicurezza web psd2 antifrode. Verifica e riattiva ora: bit.ly/XXXXXXXXXX-”* dove le X rappresentavano l’istituto di Credito oggetto di frode.

(L’ indirizzo **bit.ly/XXXXXXXXXX** è del tipo TinyUrl\* o shortURL)

---

TinyURL\* è un servizio web che permette di convertire lunghi indirizzi web in brevi URL, accorciandoli quindi in un link di pochi caratteri; l'uso di URL corti permette di semplificare il copia-incolla dei collegamenti multimediali nelle e-mail o nelle conversazioni di messaggistica istantanea.

## CASO 1.6

A tal punto l'ignaro utente che riceveva il messaggio, cliccava sul link e veniva ri-diretto verso un sito web fake (**soggetto 1**), in questo caso verso il servizio gratuito *000webhostapp.com*, con colori e impaginazione simili al sito originale dell'istituto di credito; la vittima compilava i form visualizzati che venivano catturati e registrati su file denominati *login.txt* e visualizzabili dai truffatori tramite un qualsiasi browser.

Il servizio *000webhostapp.com*, offre la possibilità di pubblicare siti web gratuiti; fa capo al servizio *000webhost.com* società avente sede a *Cipro* all'indirizzo: *61 Lordou Vironos Street 6023 Larnaca, Cyprus* Email: [contact@000webhost.com](mailto:contact@000webhost.com) così come descritto nel sito.

## CASO 1.7

Fatto sorprendente, in questa fase non venivano richiesti specifici dati riservati, ma solo nome/cognome e numero di telefono dell'utente.

La richiesta era però propedeutica al successivo attacco Vishing.

Alla fine degli inserimenti sul sito veniva presentata una pagina che informava che a breve un operatore della banca avrebbe ricontattato l'utente per la definizione del problema.

## CASO 1.8

Un sedicente operatore (**Soggetto 3**) di lì a poco, contattava la vittima all'utenza telefonica segnalata dallo stesso sul sito web contraffatto.

Intrattenendo una conversazione con tono affabile e suadente, lo avvisava che a breve gli sarebbe arrivato un codice via SMS che lo stesso malcapitato avrebbe dovuto successivamente comunicargli per consentirgli di sbloccare la carta.

L'acquisizione di quel codice permetteva così al cyber criminale di installare ed attivare su un altro dispositivo mobile l'applicazione fornita dalla banca con i dati della vittima per l'accesso diretto al suo conto

.

## CASO 1.9

Per completare la frode Il finto operatore poco dopo avvisava l'utente che avrebbe potuto utilizzare la carta oramai sbloccata ma non l'applicazione della banca sul proprio terminale che sarebbe stata invece riattivata entro 48 ore (ovviamente falso).



Nel frattempo, avuto pieno accesso al conto bancario tramite l'applicazione installata sul dispositivo mobile, i cyber criminali (**i Soggetti 4**) potevano effettuare bonifici e ricariche avendo anche possibilità di prelevare allo sportello bancario mediante lettura del QR Code (quindi senza carta (prelievo cardless); inoltre potevano effettuare prelievi SOS\*\* presso qualsiasi sportello dello stesso circuito bancario generando un codice temporaneo e temporizzato

---

\*\*È il servizio che, in una situazione di emergenza, ti permette di autorizzare chi vuoi tu a fare prelievi di contante presso tutte le casse veloci automatiche del gruppo bancario

## Caso 1.10

In un solo weekend l'organizzazione aveva prelevato **solo di contante circa 25.000 euro** da diversi conti correnti ma la banda aveva attivato già da più di un anno tale tipo di operazioni.

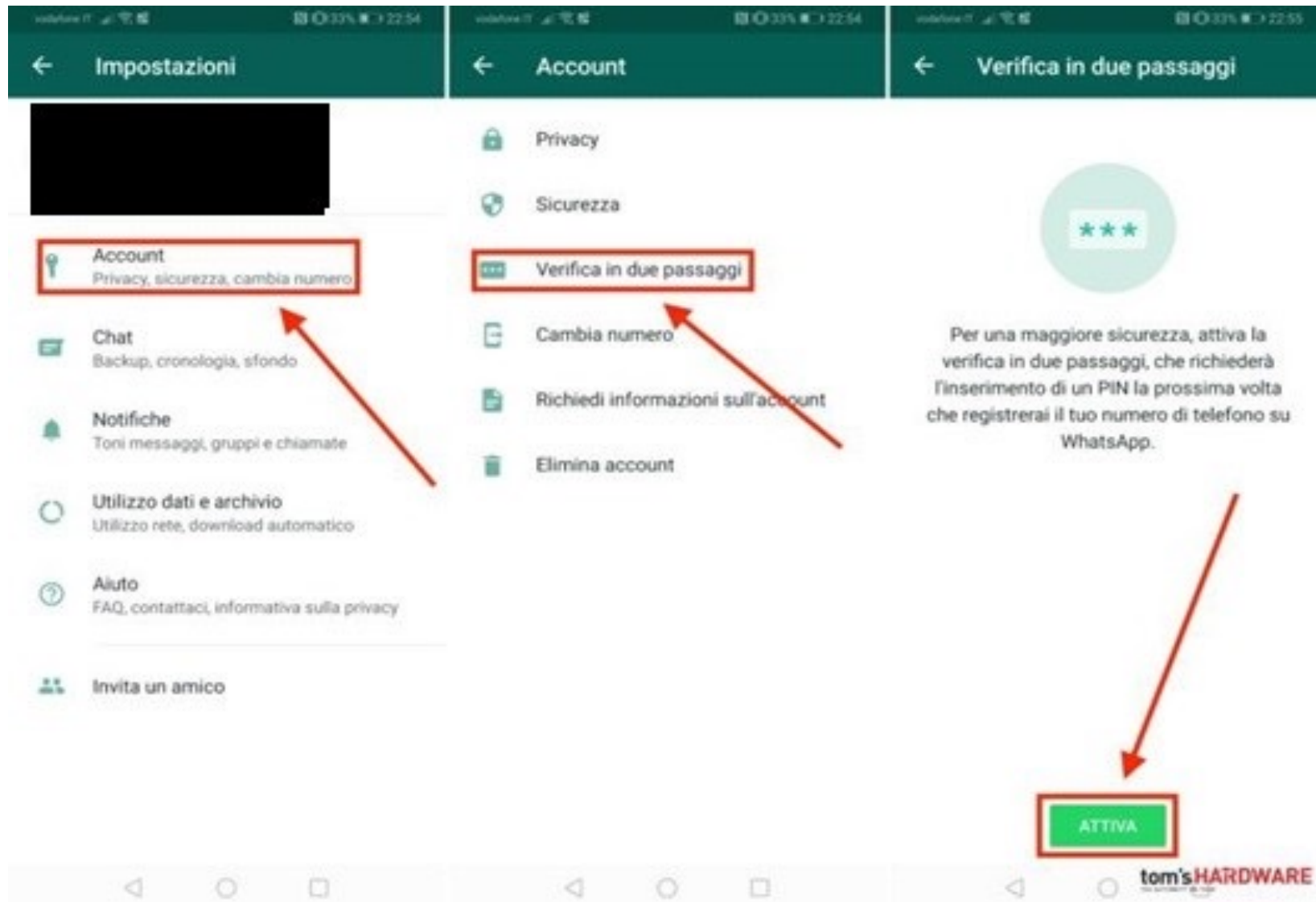
# CASO 2.1

Attacco finalizzato alla sottrazione di account  
WhatsApp

Anche in questo caso tramite attacchi di ingegneria sociale i cybercriminali puntano a carpire il codice di attivazione inviato tramite SMS per abbinare l'applicazione WhatsApp ad un dispositivo mobile.

In questo contesto però, la procedura opzionale di autenticazione a 2 fattori (un codice aggiuntivo scelto dall'utente proprietario dell'account) per aumentare il livello di sicurezza risulta anche essere il tallone di Achille per la sicurezza dell'applicazione

# Caso 2.2



# CASO 2.3

## Modus Operandi

Inizialmente, con svariate tecniche di ingegneria sociale, i cybercriminali sottraggono un primo account ad un utente e attivano quindi l'applicazione su un altro dispositivo.

Successivamente abilitano anche l'autenticazione a 2 fattori in modo che il proprietario a cui sia stato sottratto l'account non possa più ripristinarlo sul proprio dispositivo, non conoscendone il codice.

Sempre tramite l'applicazione WhatsApp contattano quindi tutti gli utenti compresi nei gruppi delle chat associati a tale account.. Spacciandosi per l'utente proprietario (anche perché registrato in rubrica e quindi associato ad una persona conosciuta) cercano di propagare l'attacco convincendo altri utenti vittima a farsi inviare il codice ricevuto tramite SMS.

## Caso 2.4

La richiesta è fatta tramite invio di messaggi del tipo *“scusa mi sono confuso, potresti reinviarmi il codice che ti è arrivato tramite SMS?”*

L’ignaro utente invia il codice, anche perché il messaggio proviene da un numero presente in rubrica o comunque da appartenente a gruppi di conoscenti.

Una volta in possesso del codice il cybercriminale attiva l’applicazione WhatsApp impedendone l’accesso dal terminale del proprietario.

## CASO 2.5

- La società Facebook proprietaria di WhatsApp ha implementato una procedura che dopo 7 giorni permette di reinstallare l'applicazione sulla specifica utenza telefonica anche senza conoscere il secondo codice di autenticazione. Ovviamente per 7 giorni il cybercriminale può usare il profilo dell'utente per le più svariate operazioni: dal proseguire l'attacco per sottrarre altri account al pretendere una somma di danaro come riscatto per restituire l'account al legittimo proprietario fino ad effettuare truffe o altri reati, impersonando il legittimo utilizzatore

# WA Le tutele

- Nelle ultime versioni di Whatsapp l'installazione dell'applicazione su un nuovo dispositivo è cambiata in alcuni passaggi in modo da migliorarne la sicurezza e dare un controllo maggiore all'utente utilizzatore dell'applicazione (utente vittima).
- Quando il dispositivo dell'utente è acceso e collegato alla rete e l'applicazione Whatsapp è attiva, se un attaccante prova ad installare l'applicazione su un altro dispositivo, il codice di attivazione viene inviato dal servizio WA mediante messaggio "push" sull'applicazione dell'utente (non tramite SMS).



# WA Le tutele

- Questa funzionalità protegge, anche dall'attacco mediante SIM Swap. (associazione della numerazione telefonica ad una nuova scheda SIM).
- Se invece il dispositivo utente è spento e quindi l'applicazione Whatsapp non è connessa alla rete, il messaggio col codice di verifica viene inviato via SMS all'utenza target (o dove è inserita la sim abbinata all'utenza mobile) ovvero l'utenza/dispositivo su cui sta per essere installata l'applicazione Whatsapp.

# CASO 3.1

## Malware per Android – Flu Bot

Google ha recentemente pubblicizzato con grande risalto il rafforzamento dei sistemi di protezione per i servizi di Google Play Store e per i dispositivi Android tramite utilizzo di tecnologie avanzate di apprendimento automatico.

Il sistema di protezione però non si estende alle App acquisite al di fuori del Play Store e dei telefoni che le installano.

E' l'esempio del malware FluBot che si è diffuso rapidamente.

## CASO 3.2

- Dall' inizio del 2021 a tutt'oggi si stanno intensificando denunce relative alla ricezione di SMS inoltrati da utenti, conosciuti e non, contenenti nel testo un link.
- Non si tratta del classico richiamato smishing (phishing via sms), attraverso il quale cliccando sul link viene richiesto di immettere le credenziali o gli estremi del conto corrente, ma di una vera e propria campagna malevola per veicolare un malware di tipo *infostealer* (specifico per dispositivi Android) mirato in particolare anche al furto dei dati di carta di credito e credenziali 2FA (2 Factor Authentication) utilizzate per l'home banking.

## CASO 3.3

Si tratta di un attacco mirato verso paesi europei tra cui: Italia, Spagna, Germania, Ungheria, Polonia con esclusione, al momento, dei paesi dell'ex URSS.

Questo può indurre a ritenere che sia stato creato proprio in quel contesto geografico

La pervasività e la pericolosità del malware hanno destato l'allarme di tutte le Polizie dell'EU e in particolare di Europol che in maggio 2022 è riuscita a smantellare i server olandesi presso cui era ospitato Flu Bot.

Al momento non si evidenziano sue ulteriori propagazioni ma non si esclude un suo potenziale «ritorno»

## CASO 3.4

Le campagne Flu Bot italiane, sempre impostate sull'invio massivo di SMS, hanno interessato prevalentemente noti corrieri di spedizione **“DHL”**, **“UPS”** o **“Amazon”** e altri ancora.


In precedenza in ambito EU il malware aveva interessato altri marchi quali «Fedex» e «Orange»

## CASO 3.5

Cliccando da un dispositivo Android sul link presente nell'SMS veniva presentata alla vittima una pagina con i loghi, ad esempio di DHL, UBS o altri, e proposto il download di un APK (Applicazione Android)

# Caso 3.6

Non sicuro | [alborzdates.ir/track/?sl7stnqltsed](http://alborzdates.ir/track/?sl7stnqltsed)



Scarica la nostra applicazione per rintracciare il tuo pacco



**Scaricare l'applicazione**  
[Come si installa?](#)

1. Quando scarichiamo un file .apk, sarà l'applicazione da cui lo facciamo ad avvisarci che il processo è bloccato.
2. Nella parte inferiore dello schermo vedremo un avviso che indica che "non è possibile installare applicazioni da fonti sconosciute" e ci invita a entrare nelle "Impostazioni".
3. All'interno dell'applicazione cerchiamo la sezione "Installare applicazioni sconosciute" e attiviamo la casella di controllo.
4. Da quel momento in poi, quell'applicazione ha i permessi per installare applicazioni esterne.

# Caso 3.7



## Track your package

This package is linked to your phone number and can only be tracked with our app.

If a window appears preventing the installation, select "settings" and enable the installation of unknown apps.

[Download App](#)



## CASO 3.8

Una particolarità di questo “virus” è che si sostituiva ad applicazioni valide.

Ad esempio il gestore dell'SMS poteva quindi catturare SMS in arrivo, manipolandoli o nascondendoli.

FluBot era in grado di auto-diffondersi tramite l'invio di SMS malevoli alla lista di contatti della vittima con l'obiettivo di infettare quanti più dispositivi possibile.

## CASO 3.9

Questa particolare caratteristica accomunava FluBot alla maggior parte dei malware per Android che **non sfruttano falle nel sistema operativo o nel dispositivo della vittima** per acquisire privilegi elevati, ma riescono a prenderne il controllo abusando del “servizio di accessibilità” tipicamente utilizzato per assistere gli utenti in attività come la lettura dello schermo per i non vedenti o nell’interazione con il dispositivo (ad esempio, mediante il clic assistito per gli utenti diversamente abili).

# CASO 3.10

Una volta installato il malware poteva attivare diversi comandi pericolosi sul telefono Android.

Da alcune analisi è emerso che **Flu Bot** era in grado di:

Esportare la rubrica

Inviare SMS malevoli

Disabilitare Google Play Protect

Attivare servizi come la deviazione delle chiamate

Disattivare l'[autenticazione a due fattori](#)

Aprire URL

Esportare SMS

Disinstallare un'app

Bypassare pertanto i sistemi di sicurezza sia del dispositivo che delle applicazioni utilizzate per accesso a dati riservati.

**L'8 Marzo 2021 in Spagna è stata smantellata una delle organizzazioni i cui membri erano promotori e utilizzatori di questo malware.**

# Caso nr. 4.1

Un ulteriore (anche se vecchio fenomeno ma con diverse varianti) si è riverificato negli ultimi mesi ed è tuttora attivo sulla rete.

L'attacco combina varie tecniche di ingegneria sociale inducendo le ignare vittime a rivelare codici di accesso, pin, password.

La banda in questione era costituita da varie figure simili a quelle del primo caso, ma con un capo carismatico, vera mente di tutta l'organizzazione, esperto in informatica e con capacità avanzate nella gestione di varie piattaforme.

Il sodalizio criminale era specializzato in diversi settori, dalle frodi bancarie, all'accesso abusivo a sistemi informatici e telematici, nonché al rilascio di falsi certificati vaccinali per il Covid-19 e relativi green pass.

## Caso n 4.2

Tutto aveva inizio dalla segnalazione di una farmacia che riceveva e-mail di phishing che evidenziavano guasti o malfunzionamenti dei portali utilizzati per l'inserimento dell'esito dei tamponi eseguiti sui propri clienti.

Alla risposta a tale email da parte del personale della farmacia faceva seguito la telefonata di un sedicente impiegato dell'Ufficio Tecnico del Sistema Sanitario Regionale che si diceva pronto a fornire l'aiuto del caso per risolvere direttamente il problema tecnico

## CASO 4.3

In tal contesto convinceva il personale medico, inesperto e colto di sorpresa dalle insolite richieste, ad installare, se non già presente, un sistema di remotizzazione del tipo Teamviewer o Anydesk

Fatto ciò il tecnico richiedeva al farmacista l'ID per la connessione del terminale della farmacia alla piattaforma della struttura sanitaria.

## CASO 4.4

Inizialmente il (finto) tecnico chiedeva all'operatore le credenziali di accesso al portale vaccinazioni/registrazioni tamponi della Sanità Regionale

Solitamente gli operatori non ricordano mai le credenziali, preferendo memorizzarle nel portachiavi custodito dal browser che consente di visualizzarle solo ad utente loggato o dietro immissione della password di accesso al sistema (nel caso di specie Windows).

## CASO 4.5

Ottenuto tale accesso il falso tecnico copiava/rubava tutte le credenziali per i vari siti/portali presenti nel portachiavi del browser, molte volte anche codici di accesso ad email usate come recupero credenziali, codici di accesso a siti bancari e/o altri dati sensibili.



## CASO 4.6

Venuto in possesso di tali dati il falso tecnico poteva così connettersi direttamente alle piattaforme sanitarie regionali per l'immissione di dati di pazienti per ottenere il codice utile per effettuare il download di green pass temporanei (rilasciati con tampone negativo).

Con la stessa tecnica sono stati compromessi anche diversi centri vaccinali per il rilascio di falsi green pass per le note tre dosi progressive mai somministrate

Costo dei servizi illeciti resi : orientativamente 20 euro per tamponi negativi e 150 euro per un greenpass.

## CASO 4.7

Questo era comunque solo uno degli introiti della banda e forse anche tra quelli di minore importo.

Il principale guadagno era infatti ricavato dallo svuotamento di conti correnti di ignari risparmiatori.

## CASO 4.8

Metodologia principale d'attacco per aggressioni ai conti bancari on line.

Social Engineering : con l'ausilio di servizi disponibili in rete e usati per la creazione di siti di phishing e l'invio massivo di messaggi di phishing ad utenti possessori di conti correnti bancari. Vedi caso 1)

## CASO 4.9

Servizio utilizzato originariamente era lufix.to ora sostituito da altri equivalenti

Piattaforme che mettono a disposizione degli acquirenti, spazi web o macchine compromesse e controllabili mediante tools o applicativi web di facile utilizzo (tipo cPanel o altri simili)

Lufix consentiva di procurarsi per qualche decina di euro spazi su cui “appoggiare” siti di phishing di vari Istituti bancari per memorizzare i dati forniti dagli utenti raggirati tramite invio di mail fraudolente o di messaggi mirati apparentemente provenienti dalla propria banca

## CASO 4.10

Il sito rivendicava apertamente : “At Lufix.to You can Buy Spamming Tools, SSH, Shells, RDP, Cpanel, Mailer, SMTP, Leads, Email:password, Combo, FULLZ”.

Nel caso specifico Lufix veniva usato per acquistare macchine compromesse su cui memorizzare le pagine del sito phishing dell’istituto di credito che si voleva riprodurre;

Lufix veniva utilizzato anche per l’acquisto di server di posta relay per l’invio massivo di mail di spam.

# Caso 4.11

LuFix Store

Search

Home

Request Products New

LuFix Services New

Hosts 14885

Shells 7748

cPanels 5820

Rdps 1221

SSH/WHM 196

Send 56359

Leads 7861

Cards 95

WebMails 37309

Accounts 1194

Others

You have 1 Pending Orders.

You have 0 Pending [Service Orders](#).

**Note:** You can only **report a bad tool** within **12 hours** (except [Cards within 1 hour], [RDP within the guaranteed time] or [SSH/WHM within 24 hours]) by clicking on **Report** button, Otherwise we can't give you refund or replacement.

After order is completed, you will not be able to report it again.

Orders

Show: 25 Item Type: All Status: All Bookmarks: All Search:

ID	Item Type	Item	View	Seller	Price	Purchased On	Status	Actions
39456	cPanel	Https://fundochincher	<a href="#">#View Details</a>	Seller111	6.00	2021-12-13 15:34	Pending	<a href="#">Report</a>
38468	cPanel	Https://solar.goclevere	<a href="#">#View Details</a>	Seller200	6.00	2021-12-07 13:39	Completed	<a href="#">View Report</a>
38272	cPanel	Https://urbandynamite	<a href="#">#View Details</a>	Seller33	9.00	2021-12-06 15:32	Completed	<a href="#">View Report</a>
38215	cPanel	Https://artemkashavri	<a href="#">#View Details</a>	Seller47	5.00	2021-12-06 09:59	Completed	<a href="#">View Report</a>
37625	cPanel	Https://teambiffit.com	<a href="#">#View Details</a>	Seller18	5.00	2021-12-02 10:45	Completed	<a href="#">View Report</a>
37624	cPanel	Https://aucutepuppies	<a href="#">#View Details</a>	Seller292	7.00	2021-12-02 10:44	Completed	<a href="#">View Report</a>
37618	cPanel	Https://artemka2807st	<a href="#">#View Details</a>	Seller47	5.00	2021-12-02 09:44	Completed	<a href="#">View Report</a>
37265	cPanel	Https://customer.therm	<a href="#">#View Details</a>	Seller86	6.50	2021-11-30 11:45	Completed	<a href="#">View Report</a>
37046	cPanel	Https://peakfitnessnw	<a href="#">#View Details</a>	Seller228	6.00	2021-11-29 15:27	Completed	<a href="#">View Report</a>
36612	cPanel	Https://waynedefranc	<a href="#">#View Details</a>	Seller57	8.00	2021-11-26 12:37	Completed	<a href="#">View Report</a>
35965	cPanel	Https://loveofdoggies	<a href="#">#View Details</a>	Seller30	6.00	2021-11-22 13:08	Completed	<a href="#">View Report</a>
35955	cPanel	Https://askbobbyd.com	<a href="#">#View Details</a>	Seller30	6.00	2021-11-22 11:45	Completed	<a href="#">View Report</a>


# Caso 4.12


Esempio di messaggio inviato agli utenti vittima con servizio di messaggistica massiva con spoofing del telefono chiamante.





Servizio utilizzato per l'invio massivo di SMS  
presi da una lista presente in un file TXT  
<https://dashboard.affiliate-sms.com>


# Caso 4.13


 [NEWS](#) [SETTINGS](#) [PRICES](#) [BALANCE](#)


  
Dashboard

  
Send message

  
Campaigns report

  
Messages report

  
General statistics

  
Contact list

### Campaign list

ID

Status

-- select --

Creation date from / to

13.12.2021 00:00:00 - 16.12.2021 00:00:00

Start date from / to

-

Clicks (Short links)

-- select --

Find

Total: 13

< Back

1 2

Next >

Add

ID	Message type	Date of creation, start, done	Total / Sent
Name	Sender		Delivered / Undelivered
1090784	SMS	13.12.2021 19:37:13	3000 / 3000
13.12.2021 19:36:18	Gruppo ISP	13.12.2021 19:36:18	2789 (92.97%) / 178
1090765	SMS	13.12.2021 18:48:04	3000 / 3000
13.12.2021 18:47:02	Gruppo ISP	13.12.2021 18:47:02	2925 (97.5%) / 42
1090762	SMS	13.12.2021 18:44:38	3000 / 2558
13.12.2021 18:44:23	Gruppo ISP	13.12.2021 18:44:23	2297 (89.8%) / 31



## CASO 4.14

L'utente indotto a cliccare sul link presente all'interno dell'SMS veniva dirottato su un sito di phishing memorizzato previo acquisto su Lufix e su cui poi venivano catturati i seguenti dati digitati dall'ignaro utente

# Caso 4.15

-----  
IP: 151.43. [REDACTED]  
Date: 2021-12-13 22:11:39  
Codice Titolare: [REDACTED]  
PIN: [REDACTED]  
Codice Fiscale  
Telefono: 331 [REDACTED]  
-----

IP: 151.43. [REDACTED]  
Date: 2021-12-13 22:11:40  
Codice Titolare: [REDACTED]  
PIN: [REDACTED]  
Codice Fiscale  
Telefono: 331 [REDACTED]  
-----

IP: 151.61 [REDACTED]  
Date: 2021-12-14 09:52:56  
Codice Titolare: [REDACTED]  
PIN: 12143  
Codice Fiscale  
Telefono: 331 [REDACTED]  
-----

IP: 151.61. [REDACTED]  
Date: 2021-12-14 13:11:13  
Codice Titolare: [REDACTED]  
PIN: 12143  
Codice Fiscale  
Telefono: 331 [REDACTED]  
-----

IP: 151.61 [REDACTED]  
Date: 2021-12-14 13:12:18  
Codice Titolare: [REDACTED]  
PIN: 12143  
Codice Fiscale  
Telefono: 331 [REDACTED]  
-----

IP: 151.35. [REDACTED]  
Date: 2021-12-15 08:36:03  
Codice Titolare: [REDACTED]  
PIN: [REDACTED]  
Codice Fiscale  
Telefono: 33 [REDACTED]  
-----

## CASO 4.16

Particolare importante: oltre alle prime credenziali di accesso, la frode consentiva di rilevare anche il numero di telefono successivamente utilizzato dagli attaccanti per contattare la vittima mediante attacco Vishing per carpire ulteriori dati sensibili come in precedenza indicato (caso 1)

# SIM Card SWAP

- **Attacco SIM swapping: cos'è e come funziona**
- Come il nome suggerisce, **tutto gira intorno alla SIM card del nostro gestore di telefonia mobile**. La SIM ci connette al network telefonico e dati dell'operatore, che associa la SIM fisica con il nostro numero di telefono.
- In altre parole, viene creata una corrispondenza univoca tra la nostra “identità fisica” (la SIM) e la nostra “identità digitale” (il numero di telefono).
- La terminologia “SIM swapping” si riferisce all'atto di **trasferire da una SIM card a un'altra questa corrispondenza** con il nostro numero di telefono

# SIM Card Swapping

Sim Card Swapping « legittima »

Sim Card Swapping «**illegittima**» :

- riuscire a portare a termine un'operazione di SIM swapping illegittima significa **ottenere accesso al numero di telefono del legittimo (e ignaro) proprietario** di tale numero, con tutto ciò che ne consegue.
- **Il criminale si fa dare una sim, con il numero della vittima, dall'operatore tramite un negozio o con modalità online.**

# SIM Card Swapping

- Questo obiettivo, di norma, viene raggiunto dai *criminal hacker* in vari modi:
  - tramite tecniche di [social engineering](#), così da indurre gli operatori di telefonia mobile a emettere una nuova SIM card;
  - oppure, corrompendo chi lavora presso uno store o presso il customer care dei provider (la Silicon Valley REACT Task Force spiega bene con la frase “if you’re working at a mobile phone store and making \$12 an hour and suddenly someone offers you \$400 to do a single SIM Swap, that can seem like a pretty sweet deal”).
  - o anche con un documento falso.
- Ma anche, più semplicemente, può capitare che l’utente ottenga una SIM senza che gli venga richiesto un documento di identità.

# SIM Card Swapping

- **Attacco di SIM swapping: perché è così pericoloso**
- Da quanto detto finora è evidente che un attacco di tipo SIM swapping è pericoloso perché **rappresenta il primo passo verso la violazione degli account online della vittima**, in quanto il numero di telefono è spesso utilizzato come uno dei fattori necessari in scenari di **autenticazione a due fattori (2FA)**.
- E come detto un account online può essere anche qualcosa di molto importante come **un conto corrente, un wallet bitcoin, un profilo Facebook, una mail (controllando la quale si possono fare anche altre truffe e sottrazioni di password di altri servizi), un backup cloud.**

.

# SIM Card Swapping. Pericoli

- L'autenticazione a due fattori è infatti basata sulla necessità di essere in possesso di due credenziali differenti per potersi autenticare a un determinato servizio.
- Nei casi di token fisico, i due fattori sono la conoscenza (di una password) e il possesso fisico (di un token): “something you know & something you have”.
- Nel caso di token inviato via SMS, i due fattori sono la conoscenza della password principale e la possibilità di ricevere l'SMS sul proprio numero di telefono



# SIM Card Swapping

- La SIM Card Swapping è una tecnica criminale vecchia di anni
- Recentemente ha però avuto **un forte «ritorno di fiamma»**
- Uno dei motivi principali è stato **l'avvento delle criptovalute**, in quanto garantirsi l'accesso a un wallet corposo può significare avere la possibilità di rubare molti milioni di euro con una sola operazione.
- Ripetuti sono in tal senso gli «alert» dell'FBI
- I sintomi di allarme di attacchi di questo tipo e i rimedi

# SIM swap (o SIM swapping)

## Le attenzioni dell'AGCOM

Il fenomeno osservato da Agcom prende il nome di **SIM swap (o SIM swapping)** e si realizza quando un malintenzionato riesce a ottenere dal nostro operatore telefonico una copia della nostra SIM.

La tecnica usata dai truffatori per clonare una SIM consiste nel conoscere il numero di telefono della vittima e riuscire ad avere (magari con la complicità di un addetto al punto vendita) una copia dei suoi documenti. A quel punto basta chiedere alla compagnia telefonica una SIM sostitutiva e il gioco è fatto.

# Attivazione e cambio di SIM card

## Nuove procedure

- Per **l'attivazione o il cambio di una SIM telefonica** non bisogna più presentare i documenti, ma **basta avere SPID**. È quanto ha stabilito l'Agcom, con una decisione che consente agli operatori telefonici di identificare i soggetti richiedenti tramite l'identità digitale.
- Questa novità rappresenta una **misura di sicurezza** che manda in pensione la classica identificazione dei clienti, che obbligava le compagnie a procedure macchinose fatte di fotocopie, scansioni o, nel migliore dei casi, inquadrature video di carte d'identità e codici fiscali.

# Identità digitale per contrastare le frodi

- La [decisione dell'Agcom](#) arriva dopo che in precedenza l'Autorità Garante per le Comunicazioni aveva registrato un aumento preoccupante di segnalazioni di casi di sostituzione SIM all'insaputa del titolare della SIM.
- La richiesta di SIM sostitutive veniva fatta giustificandola con la volontà di passare ad altro operatore o con presunti furti, smarrimenti o malfunzionamenti. La clonazione delle SIM card veniva realizzata ovviamente a scopo fraudolento.

# Chi può chiedere il cambio della SIM

- La **richiesta di cambio SIM**, in caso di passaggio ad altro operatore con portabilità del numero, furto o smarrimento della SIM originale, può essere fatta **solo dal titolare** del numero di telefono.
- In caso di furto, smarrimento o malfunzionamento della propria SIM, la nuova SIM può essere chiesta **solo al proprio operatore telefonico**.
- In tali circostanze, la richiesta di portabilità può essere effettuata solo dopo aver sostituito la SIM e, pertanto, disponendo di una SIM funzionante.

# Chi deve identificare il soggetto per cambio SIM

- Anche con il passaggio alla nuova procedura che prevede l'uso di [SPID, CIE o CNS](#), l'identificazione della persona che chiede una SIM deve essere svolta **sempre dall'operatore telefonico**.
- Mentre prima l'identificazione avveniva acquisendo una fotocopia di documento d'identità, codice fiscale, vecchia SIM o (in caso di furto o smarrimento) della relativa denuncia, oggi con le nuove disposizioni basterà verificare la coincidenza tra i dati raccolti durante l'emissione della nuova SIM con quelli che vengono fuori dal processo di autenticazione digitale fatta dall'utente.

# SIM Card Swapping e conseguenze civilistiche

- La vittima avrà il diritto di ottenere dalla propria banca la restituzione dell'importo subito dopo aver disconosciuto l'operazione ai sensi dell'art. 11 del D.lgs. 11/2010, fatto salvo il diritto della banca di "riprendersi" la somma rimborsata nel caso dimostri che l'operazione era stata autorizzata;
- La vittima **non avrà diritto alla restituzione** da parte della banca e/o dell'operatore telefonico **qualora l'evento dannoso discenda da suo errore o trascuratezza** (Es. smarrimento della propria carta d'identità poi utilizzata dal malvivente, omessa tempestiva contestazione dell'operazione illecita ecc.)
- La banca, risarcito il cliente, potrà «surrogarsi» nei confronti dell'operatore telefonico **qualora non abbia adottato le misure di sicurezza imposte dal contratto o dalla diligenza richiesta** e in particolare l'obbligo di identificare il richiedente della Sim Card fraudolenta

# La steganografia ... «un ritorno di fiamma criminale»

Emerso recentemente a seguito di analisi iniziali di ESET confermate da AVAST, aziende di sicurezza informatica.

Un gruppo hacker («WOROC») ha ideato una tecnica per occultare frammenti di virus all'interno di immagini PNG (file di rilevanti dimensioni di largo uso nella progettazione grafica) così da poter compromettere un sistema senza innescare nessun allarme



## ... Steganografia

Attacchi portati contro bersagli di alto profilo tra cui realtà governative nel Medio Oriente, in Sud Est asiatico e in Africa.

In sostanza le immagini PNG sono utilizzate come vettori di attacco.

Utilizzando tecniche di steganografia il codice dannoso viene nascosto all'interno dei file PNG, in particolare nei pixel d'immagine, così che esse appaiono come tali quando visualizzate con strumenti ordinari

# La steganografia ... «un ritorno di fiamma criminale»

Emerso recentemente a seguito di analisi iniziali di ESET confermate da AVAST, aziende di sicurezza informatica.

Un gruppo hacker («WOROC») ha ideato una tecnica per occultare frammenti di virus all'interno di immagini PNG (file di rilevanti dimensioni di largo uso nella progettazione grafica) così da poter compromettere un sistema senza innescare nessun allarme

## ... Steganografia

Attacchi portati contro bersagli di alto profilo tra cui realtà governative nel Medio Oriente, in Sud Est asiatico e in Africa.

In sostanza le immagini PNG sono utilizzate come vettori di attacco.

Utilizzando tecniche di steganografia il codice dannoso viene nascosto all'interno dei file PNG, in particolare nei pixel d'immagine, così che esse appaiono come tali quando visualizzate con strumenti ordinari

# Cybercrime e settore finanziario italiano

Lo stato dell'arte

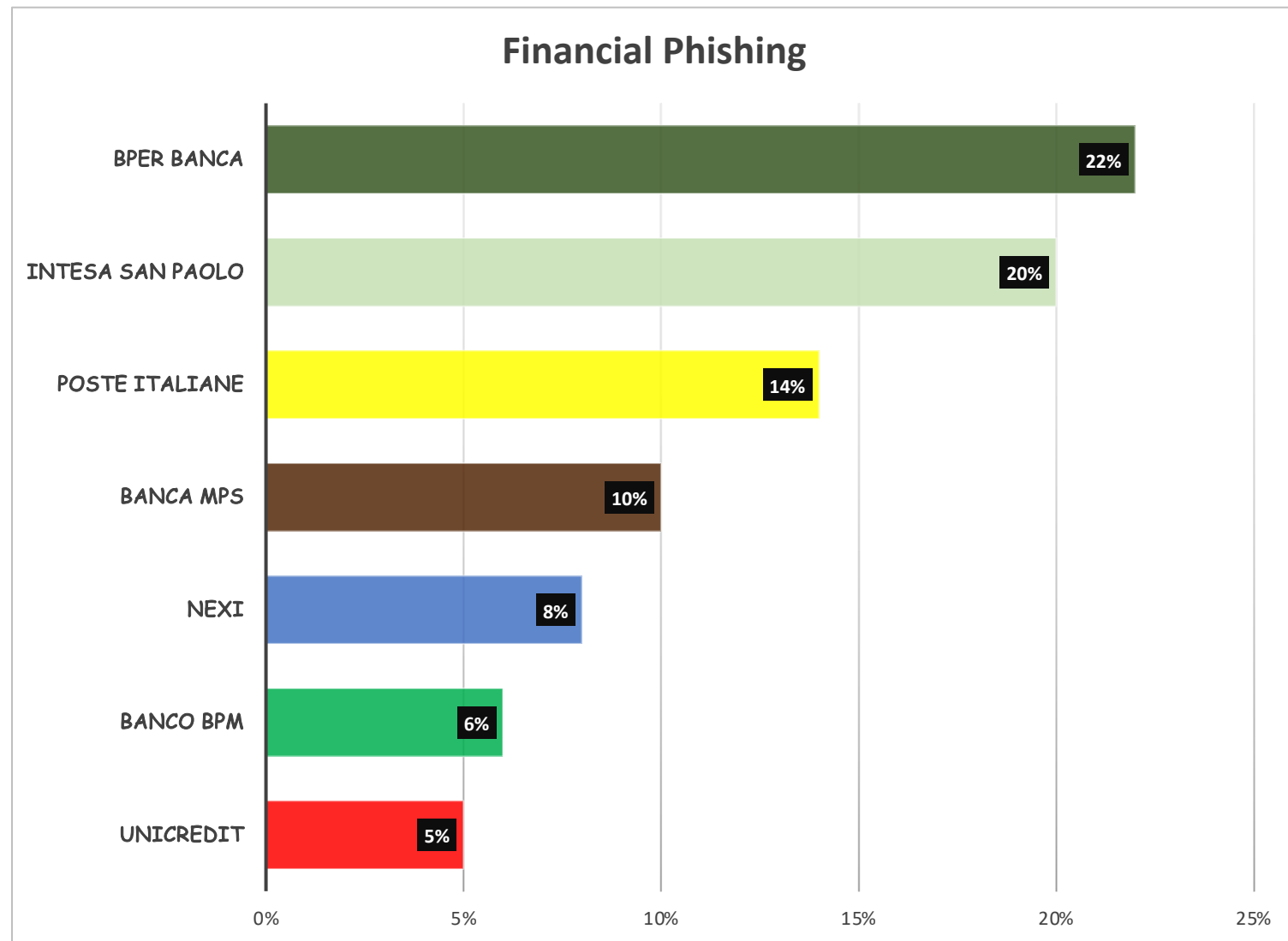
# Cybercrime e settore finanziario (in prospettiva IBM)

Il financial fraud, frode bancaria o finanziaria, passa quasi sempre attraverso il furto delle credenziali di accesso ai sistemi bancari o di pagamento e riutilizzate per transazioni fraudolente all'insaputa del titolare

# Cybercrime nel settore finanziario

Principali vettori di attacco nel 2022 in ambito europeo

- phishing per il credential theft spesso combinato con una successiva interazione con un finto operatore per il furto dei fattori di autenticazione forte
- malware per credential theft o multifactor authentication
- hacking del dispositivo mobile tramite SIM Swap o emulazione software dello smartphone
- in misura inferiore, attacco all'infrastruttura finanziaria



Financial Phishing – Brands più colpiti in Italia anno -2022

# Cybercrime verso il settore finanziario italiano

- Spunto di riflessione :
- Il 97% delle URL di phishing usa il protocollo HTTPs, il cosiddetto HTTP sicuro, che invece non può più essere considerata una indicazione attendibile.
- Come noto la veridicità di una connessione HTTPs dovrebbe essere invece legata alla validazione del dominio.



# OSSERVAZIONI CONCLUSIVE SUL FENOMENO DEL PHISHING

- Il dato che più di ogni altro impone severe riflessioni è che il 91.2% delle URL di phishing usa il protocollo HTTPs, il cosiddetto HTTP “sicuro”, instaurando un canale protetto mediante cifratura.
- Tecnologie come HTTPS e l'SSL/TLS sono progettate per proteggere le comunicazioni tra client e server, tuttavia l'icona del lucchetto nella barra indirizzi del browser può creare la falsa l'illusione che un sito web possa essere considerato attendibile.

# ... sempre a proposito di phishing(1)

Tutto questo richiede la massima attenzione in merito alle indicazioni che le organizzazioni forniscono ai propri clienti, relativamente alla presenza di un lucchetto chiuso e dalla dicitura “**https://**” nella barra degli indirizzi come elementi per distinguere una pagina sicura da una non sicura.

Se l’uso di una connessione HTTP di tipo semplice (http://) sicuramente non fornisce nessuna garanzia sulla controparte, l’uso del protocollo HTTPS, senza successive verifiche sul tipo di certificato, su chi e per quali scopi lo ha emesso, ancora una volta non può darci nessuna indicazione di sicurezza.

**La valutazione sulla veridicità di una connessione HTTPS dovrebbe essere legata alla validazione del dominio. Nella totalità dei casi i phisher usano domini con certificati di tipo Domain Validation (DV), la forma più semplice di validazione e quella proposta dai siti di web hosting per qualche euro o addirittura gratuitamente**

## ... a proposito di phishing (2)

I certificati di tipo Domain Validation, malgrado siano in grado di garantire comunicazioni criptate e sicure attraverso connessioni HTTPS, **poco o nulla dicono sulla autenticità di chi possiede il sito web al quale sono collegati**. Questa ambiguità viene sfruttata dai phisher quando usano comunicazioni HTTPS. Non esiste nessuna forma di controllo sull'entità o sulla persona che richiede un certificato SSL/TLS per abilitare un sito al protocollo HTTPS.

## ... a proposito di phishing (3)

Si controlla in automatico solo che chi richiede il certificato abbia il controllo del dominio in questione, cosa ovvia.

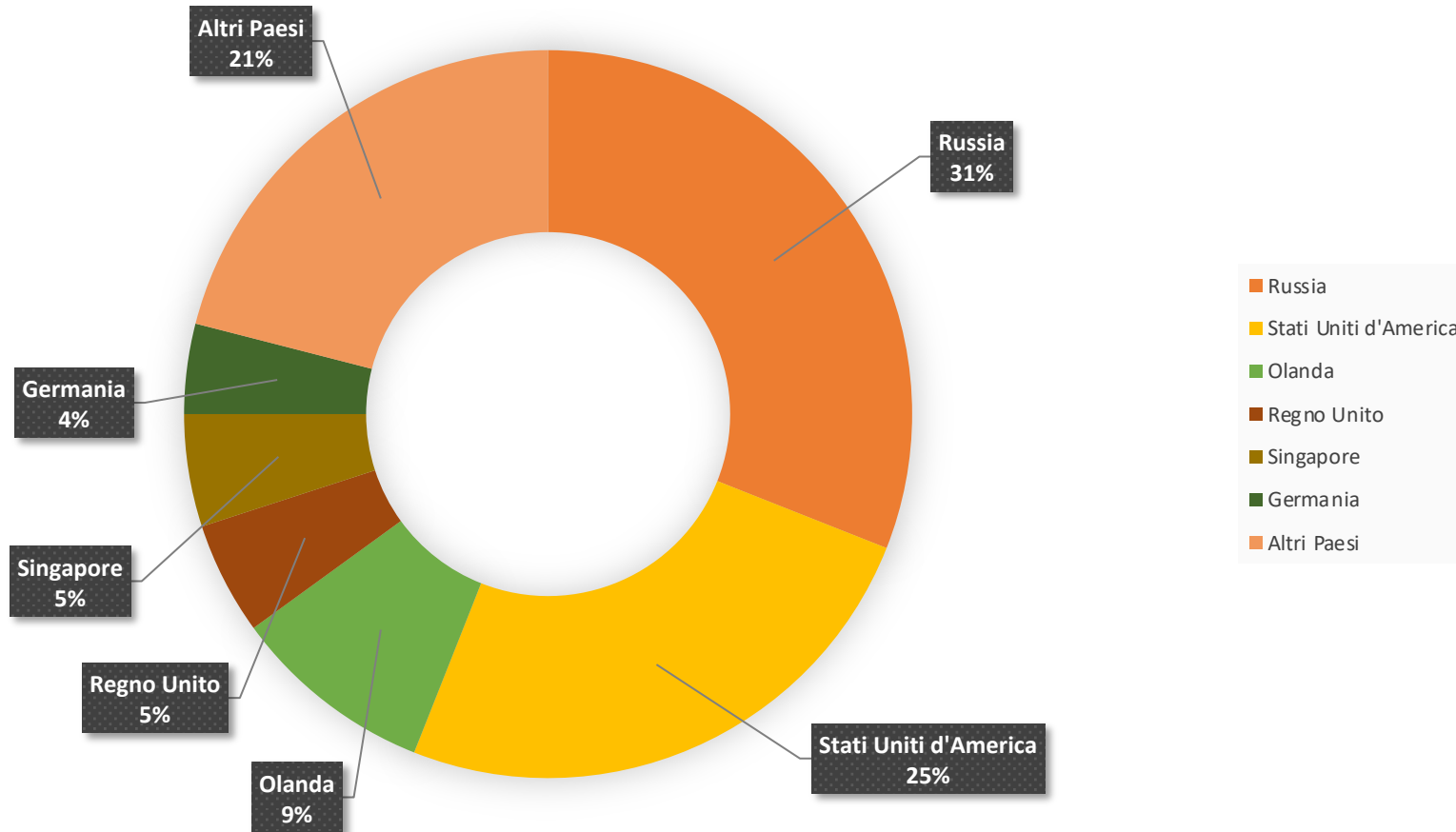
**I siti reali di banking italiani, purtroppo ancora con qualche grave eccezione, usano quasi sempre certificati di tipo Organization Validated (OV), o meglio ancora, Extended Validation (EV).**

Quest' ultimo tipo di validazione del certificato, il cui rilascio è articolato e subordinato a numerosi controlli anche di natura legale sull'entità che lo richiede, fornisce le maggiori garanzie sulla controparte.

# Siti di phishing mirati verso il settore finanziario italiano

## Localizzazione

## Financial Malware hosting countries - 2020



*Andamento dei cyber attacchi nel periodo 2018 - 22*

- Collocazione geografica dei malware
- Nel 31% dei casi il malware era ospitato su provider russi, nel 25 % su provider USA
- La collocazione geografica indica solo dove è stato inizialmente caricato il malware e non fornisce indicazioni precise sui cd threat actors
- I cybercriminali noleggiavano spesso spazi presso provider oppure compromettono siti internet già esistenti, non aggiornati o non ben configurati spesso all'insaputa degli stessi proprietari anch'esse vittime

## Financial phishing hosting countries 2022

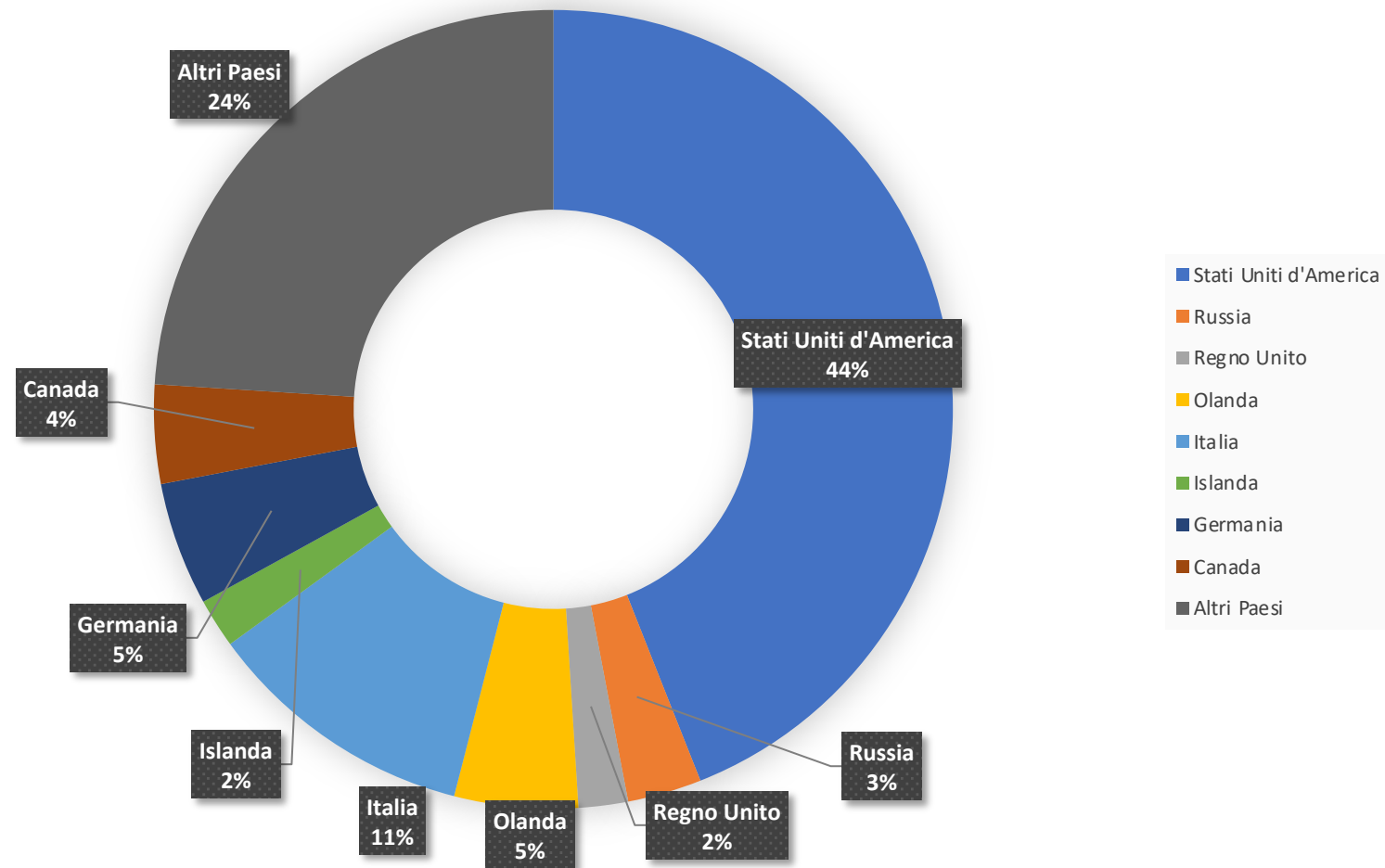


Fig.7 pag. 141



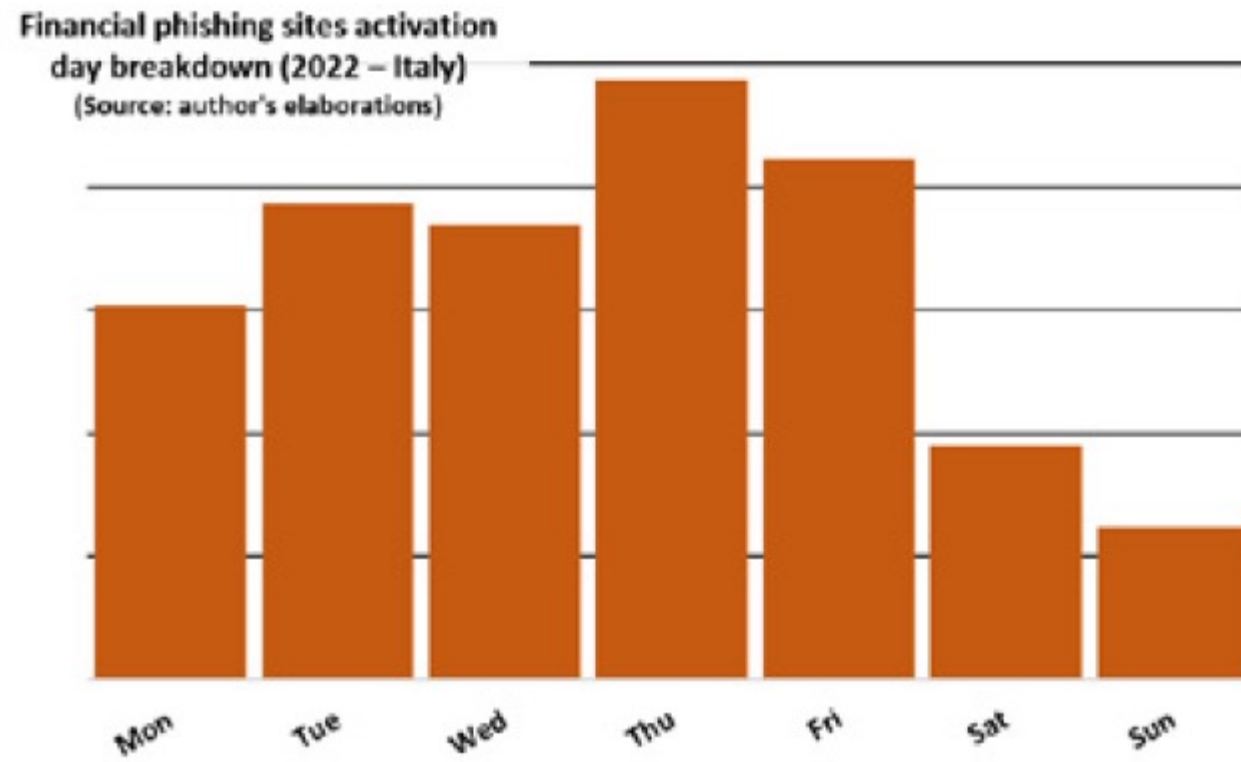
# Siti di phishing verso il settore finanziario italiano Localizzazione

Nel 2022 il 44% dei siti era negli USA mentre nel 2021 il 36%. Tra essi il provider «Namecheap» leader mondiale di web hosting con oltre 10 milioni di siti gestiti

L'11% delle pagine di phishing finanziario italiano era nel 2022 presso provider italiani, dato quasi raddoppiato rispetto a quello del 2021

# La collocazione dei siti di phishing

E' ipotizzabile che la collocazione e la scelta del provider siano da attribuirsi alla combinazione della facilità di creare domini, anche in maniera automatica e pagando in criptovaluta, o addirittura usando offerte di siti web gratuiti assieme agli scarsi controlli del provider



Attivazione dei siti di phishing riferimento ai giorni settimanali anno 2022

# Cybercrime verso il settore finanziario

- Il fenomeno delle phishing factory
- Vere e proprie fabbriche di phishing con i cybercriminali che registrano e attivano una grande quantità di domini di phishing anche verso target diversi nel giro di poche ore
- Evoluzioni del phishing verso il vishing e lo smishing

# Cybercrime verso il settore finanziario italiano

- Il furto o la compromissione delle credenziali è stato il vettore di attacco nel 19% dei data breach del 2022 (fonte : IBM Security Cost of Data Breach Report 2022 July 2022 prodotto da Ponemon Institute)
- **Il phishing** in tutte le sue forme, inclusi allegati e link, è stato **nel 2022 il principale vettore di attacco nel 41% degli incidenti gestiti. Nel 2020 era il 33%** con una percentuale di aumento di 8 punti in due anni (fonte : IBM X-Security Force, February 2023)
- Il furto di credenziali attraverso il phishing non costituisce un attacco ma è il primo passo verso molti schemi di attacco più complessi in base allo specifico obiettivo secondo i collaudati schemi di social engineering.

# Il phishing

## Esempi

- il phishing bancario usa le credenziali delle vittime per effettuare operazioni finanziarie dai conti delle vittime
- Il phishing verso provider usa le false credenziali per attivare servizi Internet, ad esempio spazio web, strumentali a costruire nuovi attacchi
- Il phishing verso servizi di webmail serve a costruire attacchi più realistici inserendosi in conversazioni reali della vittima (MITM, BEC)
- Il phishing verso clienti di aziende di recapito serve a indurre pagamenti per la ricezione di spedizioni

# Furti di credenziali e resistenza al phishing

- La Direttiva EU PSD2 ha introdotto dal 2019 la cd Strong Customer Authentication (SCA) del cliente tramite il noto sistema della OTP tramite SMS, o notifiche push con un numero o codice da inserire in un form spesso tramite app di autenticazione
- Tutti questi sistemi sono vulnerabili al phishing
- Sempre di più quindi si stanno diffondendo sistemi di MFA resistenti al phishing (Phishing-Resistant Multi Factor Authentication) per rilevare e impedire la divulgazione di credenziali di autenticazione verso una applicazione o sito web mascherato da sistema legittimo anche tramite utilizzo di token ( FIDO/WebAuth o standard FIDO2 o basati su Public key infrastructure –PKI)

# Cybercrime verso il settore finanziario italiano

## Nuove difese

- Le nuove forme di Threat Intelligence stanno evidenziando sempre più attacchi unici e fileless (senza file, che si sviluppano per lo più interamente in memoria)
- Di qui il ricorso agli EDR (Endpoint Detection and Response) che intervengono dove gli antimalware non riescono più ad arrivare attraverso una analisi comportamentale dei file durante l'esecuzione in memoria (behavioural analysis) pronta a bloccare comportamenti anomali
- In tutto questa area il Machine Learning può essere estremamente efficace