AGID
Agenzia per l'Italia Digitale

FormezPA

Social Engineering e Phishing

La sicurezza informatica nella pubblica amministrazione

Webinar - 25 Novembre 2021

Michele Petito

Indice

1. **Le varie forme social engineering** (phishing, smishing, ecc)
2. **Esempi di attacchi** (suddivise per temi e brand)
3. **Le url di phishing** (come sono strutturate, quali servizi sfruttano, come identificarle)
4. **Security awareness**: presentazione di un tool per la **simulazione di campagne di phishing**

Cos’è il social engineering

- Il **social engineering** rappresenta un insieme di tecniche utilizzate dai cyber criminali per attirare gli ignari utenti ad inviare loro i loro dati riservati, infettare i loro computer tramite malware o aprire collegamenti a siti infetti.
- **Si fa appello alle debolezze dell’essere umano** quali ad esempio l'avidità, la curiosità, il timore nei confronti dell'autorità ecc.
- Gli attacchi richiedono una conoscenza tecnica non avanzata (grazie a toolkit, PhaaS)

Vettori di attacco basati su Social Engineering

- Il **Baiting** (l'attaccante offre qualcosa al fine di consentire il download di un file dannoso)
- lo **Scareware** (l'attaccante spinge l'utente a credere che il proprio computer sia infetto per poi offrire una soluzione con cui infettarlo veramente)
- il **Phishing** (l'attaccante invia una mail realizzata appositamente per favorire l'inserimento di informazioni personali)
  - **Sphear phishing** (forma di phishing mirato ad un settore specifico, ad esempio il phishing bancario)
  - **Business Email Compromise (BEC –** forma di phishing mirato verso aziende specifiche)
- Il **Vishing** (Voice o VoIP phishing)
- lo **Shoulder surfing** (sfrutta l'osservazione diretta "dietro alle spalle" della vittima, per ottenere le informazioni accessibili)
- il **Dumpster diving** (frugare nei cestini della spazzatura per ottenere informazioni riservate)
- Il **Reverse social engineering** (l'attaccante genera un malfunzionamento del sistema e poi si propone per l'assistenza)
- Il **Tailgating** e **Piggybacking** (l'attaccante sfrutta l'accesso riservato del personale dipendente)

Alcune best practice per difendersi da attacchi di social engineering (human based)

- **Non lasciare incustoditi documenti aziendali**
- Conservare i documenti riservati in **scomparti chiusi a chiave**
- Distruggere i documenti con **dispositivi appropriati** quando non servono più
- Utilizzare **policy di sicurezza per l'accesso negli spazi riservati**
- Se noti qualcuno che non conosci all'interno del tuo ufficio, **controlla se dispone di un badge visitatore** o se è autorizzato.
- Le persone esterne all'organizzazione dovrebbero entrare solo previa **identificazione e autorizzazione**. Evitare eccezioni (quali fattorini, elettricisti ecc.) anche se si dimostrano gentili e ben vestiti (**Piggybacking**)
- Non permettere a qualcuno che non riconosci come collega di entrare insieme a te (**Tailgating**) mentre effettui l'accesso ad aree riservate

Canali di comunicazione più utilizzati nei social engineering

Telefono

E-mail

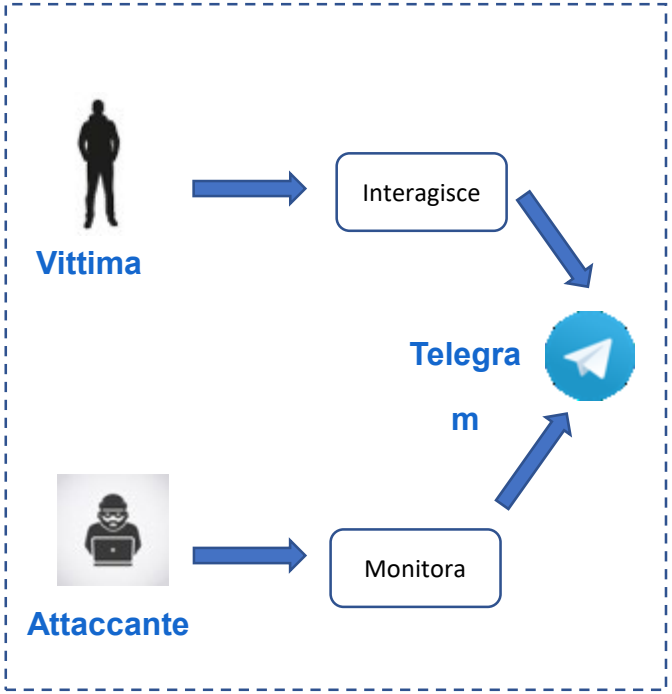
Social

Video

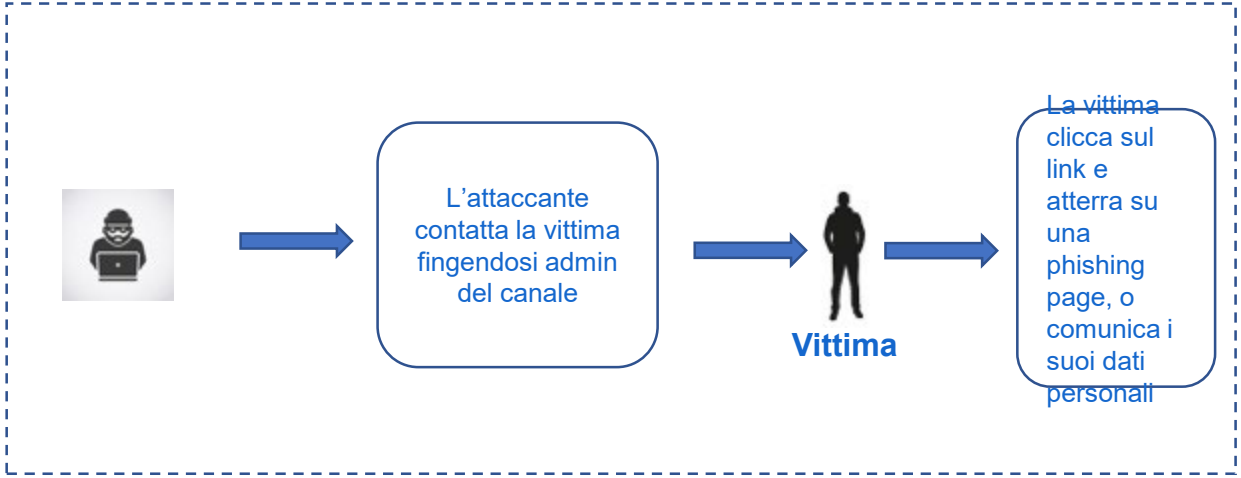
Sms

Attacco via Telegram

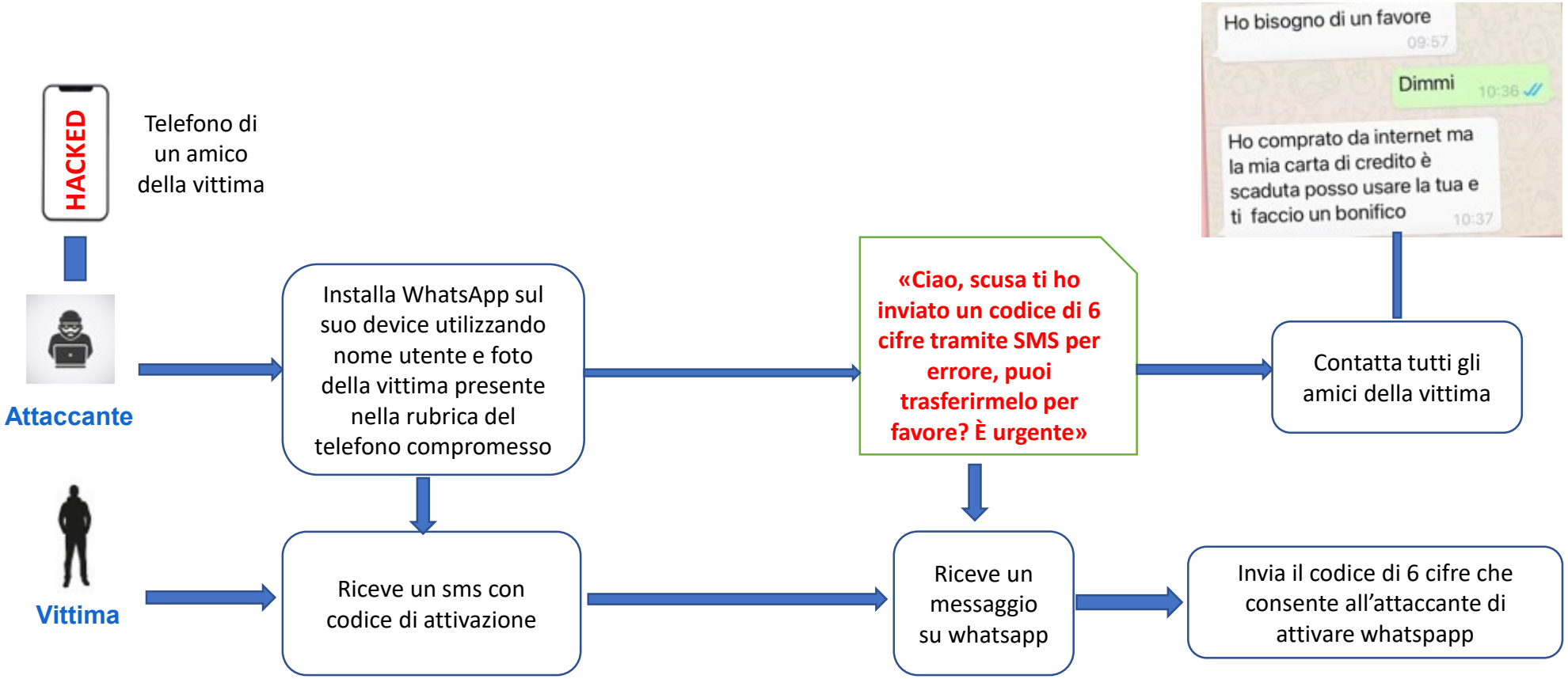
FASE 1 – INFORMATION GATHERING



FASE 2 – ATTACCO



Attacco via Whatsapp



App di messaggistica: come difendersi

- Abilitare la **verifica in due passaggi**
- Se disponibili, preferire l'utilizzo di **app di autenticazione** (es. Google Authenticator e simili) **al posto degli sms** (facilmente aggirabili)
- Non condividere con nessuno il **codice di verifica**
- **In generale, non fidarti di nessuno**, neanche degli amici in rubrica, soprattutto se ti chiedono informazioni personali, codici o password

Deep fake

Video: https://bit.ly/deepfakequeen

Software open source utilizzato: https://github.com/iperov/DeepFaceLab

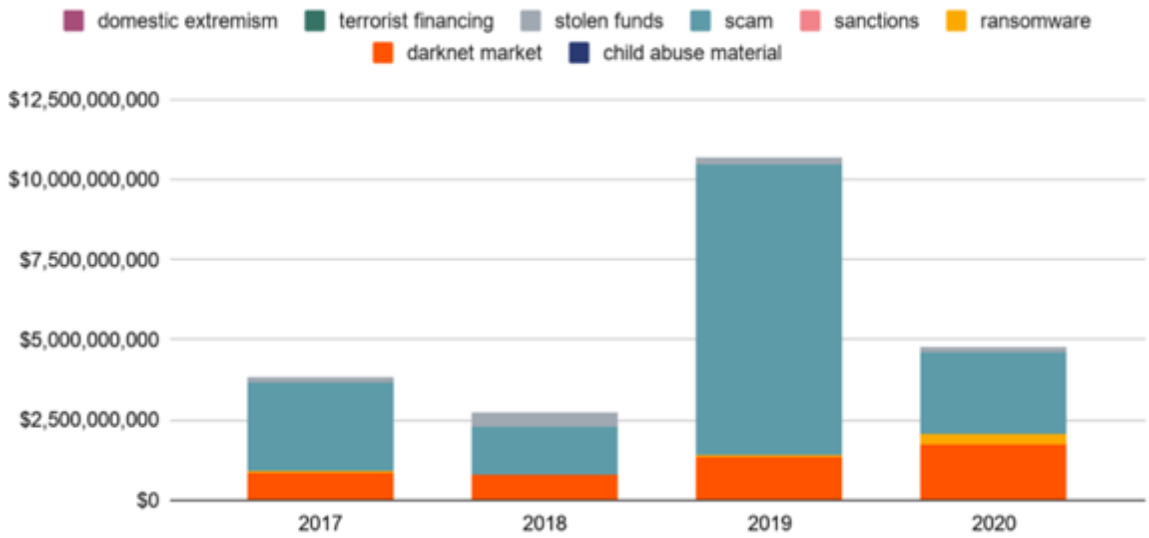
Altri video realizzato con lo stesso software:

- **https://bit.ly/deepfaketomcruise**
- **https://bit.ly/deepfakeeinstein**
- **https://bit.ly/deepfakecarolinewinberg**

Siti scam

- Le tecniche di social engineering spesso vengono utilizzate per eseguire vere e proprie truffe

- Gli scam sfruttano le tecniche del social engineering per convincere gli utenti e si concludono con diversi esiti sia nel web2.0 che nel web3.0:
  - **Web 2.0** → *Exit scam*
  - **Web 3.0** → *Exit scam, Rug pull, Honeypot*



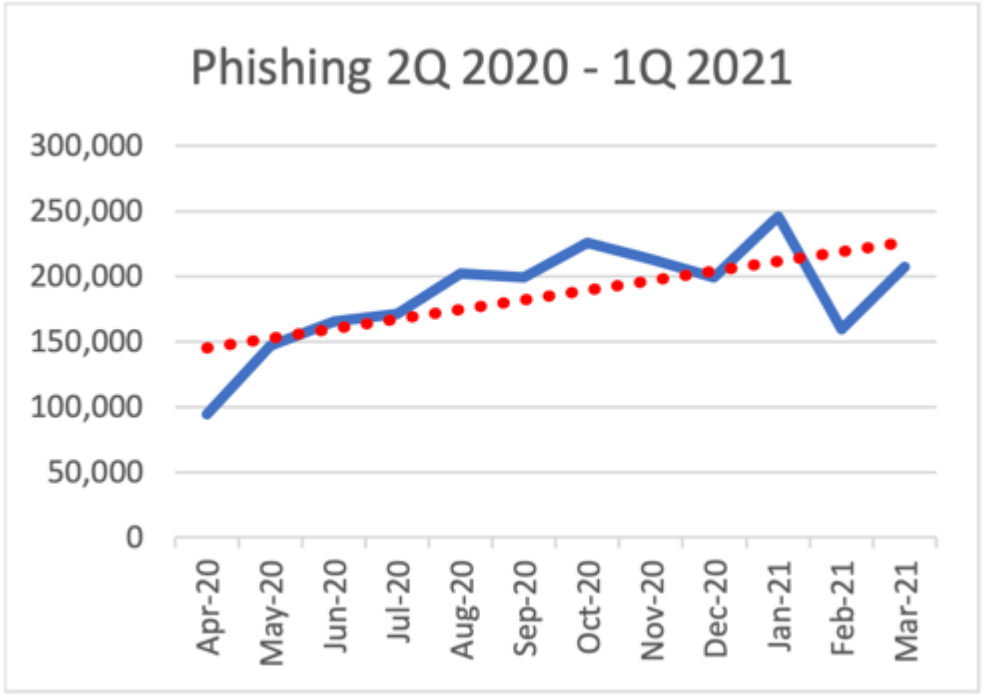
Rif. https://cert-agid.gov.it/news/scam-hack-e-scenari-reali-nel-mondo-delle-criptovalute/

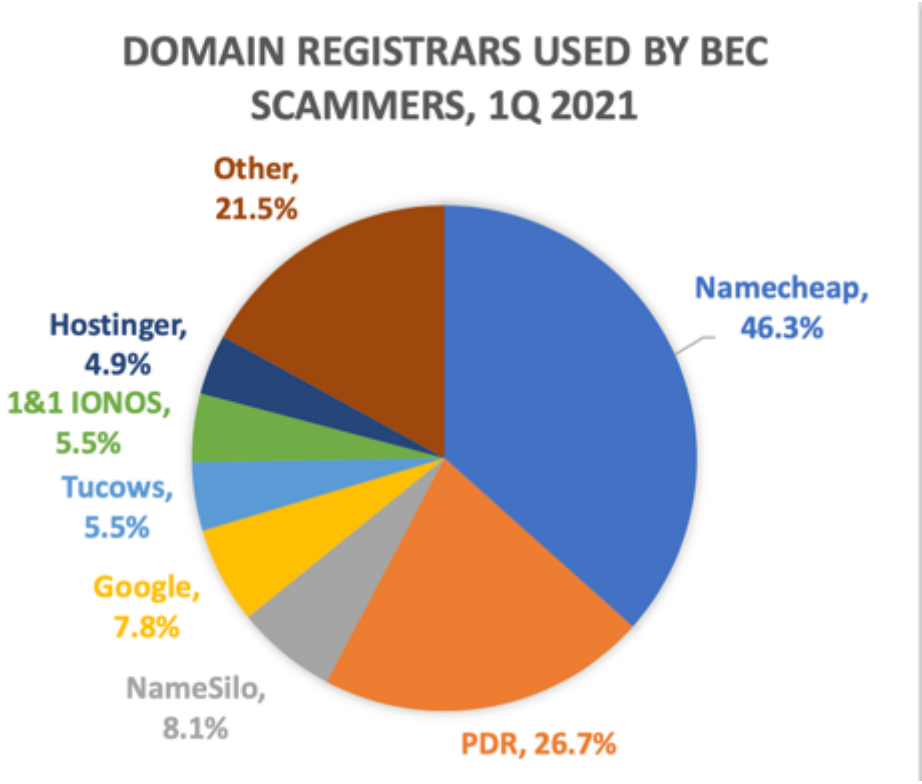
Diffusione del phishing e social engineering

- Secondo il **Rapporto CLUSIT 2021** il "Phishing/Social Engineering" si conferma tra le principali tipologie di attacco
- Tale categoria dopo una crescita del **+81,9%** rispetto al 2018, nel 2021 in base all'ultimo rapporto registra un **calo del -13%.**
- **Maggiore preparazione degli attaccanti** (i criminali si affidano a collaboratori madrelingua e sfruttano gli eventi locali per attacchi contestualizzati)
- Una quota crescente di questi attacchi basati su Phishing si riferisce a **"BEC scams"** che infliggono danni economici sempre maggiori alle loro vittime.

TECNICHE DI ATTACCO PER TIPOLOGIA	2017	2018	2019	2020	2020 su 2019	Trend 2020
Malware	446	585	729	783	7.4%	↑
Unknown	277	408	317	372	17.4%	↑
Known Vulnerabilities / Misconfigurations	127	177	127	184	44.9%	↑
Phishing / Social Engineering	102	160	291	289	-0.7%	↘
Multiple Techniques / APT	63	98	65	95	46.2%	↑
Account Cracking	52	56	86	85	-1.2%	↘
DDoS	38	38	23	34	47.8%	↑
0-day	12	20	30	23	-23.3%	↓
Phone Hacking	3	9	1	3	200.0%	↑
SQL Injection	7	1	1	3	200.0%	↑
TOTALE	1127	1552	1670	1871	+12%	

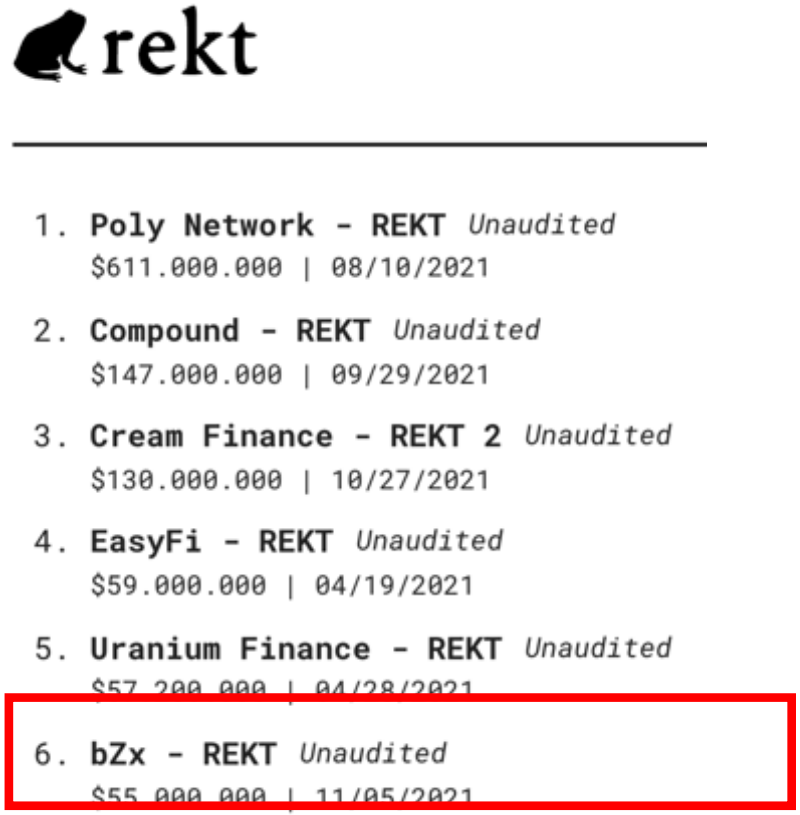
Alcuni dati dell'Anti-Phishing Working Group (APWG)





Phishing da 50 milioni di dollari

- **Il 5 novembre 2021 l'azienda bZx**, che gestisce un protocollo blockchain per il lending e il borrow di criptovalute ha subito un attacco di Phishing
- **L'attacco** ha colpito direttamente lo sviluppatore di bZx che si è visto recapitare una mail di phishing con allegato Word e macro malevola. L'apertura dell'allegato ha avvitato la catena di infezione e provocato la perdita della chiave privata.
- **L'attaccante, grazie alla chiave privata sottratta,** è riuscito a prendere possesso del protocollo, odificare lo smart contract e svuotare tutti i wallet degli utenti



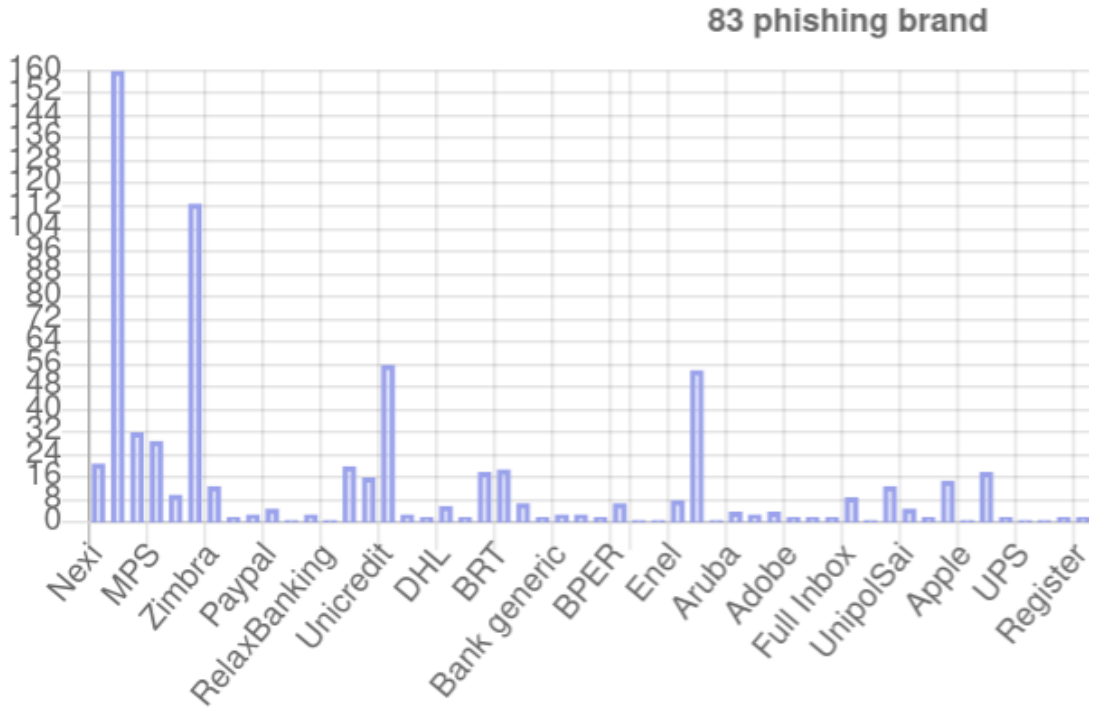
Fonte: https://rekt.news/bzx-rekt/

Campagne di Phishing rilevate dal Cert-AgID

(da 1-1-2021 al 5-11-2021)

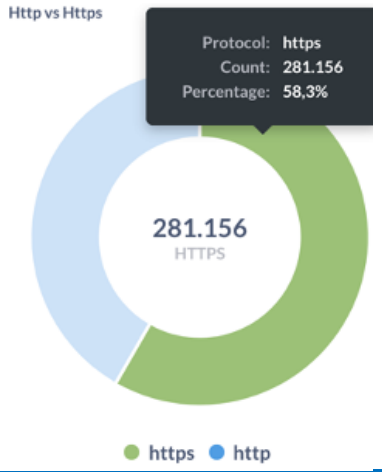
Numero totale campagne di Phishing:
764

1. **Intesa SanPaolo**: 161
2. **Poste Italiane**: 113
3. **Unicredit**: 56
4. **Ing Direct**: 54
5. **Webmail generica**: 32
6. **Monte dei Paschi di Siena**: 29
7. **Nexi**: 21
8. **Microsoft**: 20
9. **BRT corriere**: 19
10. **Findomestic e Amazon**: 18



PhishStats: analisi URL Phishing per https/http

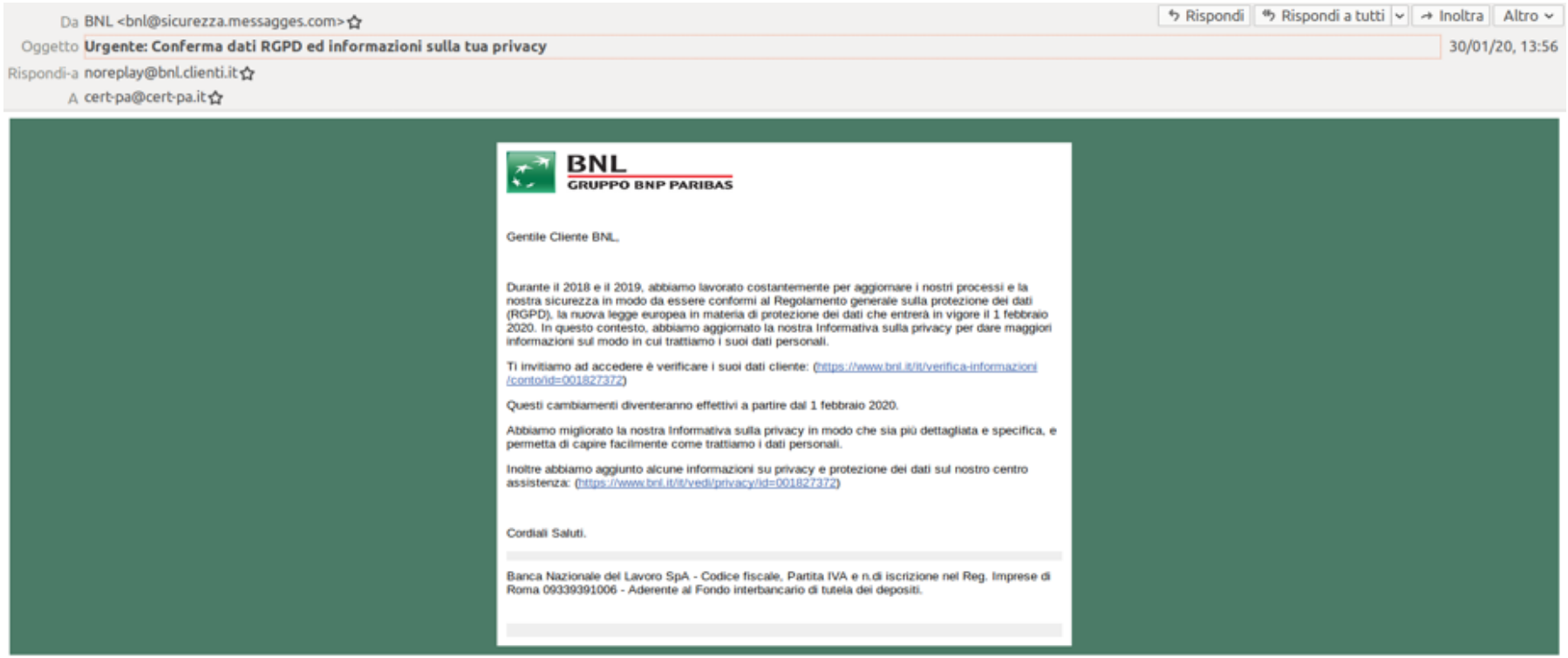
Periodo analizzato**: gennaio - novembre 2021**



- Dal **2017** in poi le pagine di phishing iniziano a spostarsi verso **l'https**
- Il **2020** è l'anno del «**sorpasso**»
- Ad oggi il **58,3% delle pagine utilizza domini con certificati SSL/TLS** installati
- IL **36,2%** di questi certificati sono stati emessi da **Let's Encrypt** (fonte: PhishLabs)

Esempi di pagine di phishing

Esempio di phishing a tema banking (1.1)



Da BNL <bnl@sicurezza.messagges.com>
Oggetto **Urgente: Conferma dati RGPD ed informazioni sulla tua privacy**
Rispondi-a noreplay@bnl.clienti.it
A cert-pa@cert-pa.it

Rispondi | Rispondi a tutti | Inoltra | Altro
30/01/20, 13:56

BNL
GRUPPO BNP PARIBAS

Gentile Cliente BNL,

Durante il 2018 e il 2019, abbiamo lavorato costantemente per aggiornare i nostri processi e la nostra sicurezza in modo da essere conformi al Regolamento generale sulla protezione dei dati (RGPD), la nuova legge europea in materia di protezione dei dati che entrerà in vigore il 1 febbraio 2020. In questo contesto, abbiamo aggiornato la nostra Informativa sulla privacy per dare maggiori informazioni sul modo in cui trattiamo i suoi dati personali.

Ti invitiamo ad accedere è verificare i suoi dati cliente: (https://www.bnl.it/it/verifica-informazioni/conto/id=001827372)

Questi cambiamenti diventeranno effettivi a partire dal 1 febbraio 2020.

Abbiamo migliorato la nostra Informativa sulla privacy in modo che sia più dettagliata e specifica, e permetta di capire facilmente come trattiamo i dati personali.

Inoltre abbiamo aggiunto alcune informazioni su privacy e protezione dei dati sul nostro centro assistenza: (https://www.bnl.it/it/vedi/privacy/id=001827372)

Cordiali Saluti.

Banca Nazionale del Lavoro SpA - Codice fiscale, Partita IVA e n.di iscrizione nel Reg. Imprese di Roma 09339391006 - Aderente al Fondo interbancario di tutela dei depositi.

Esempio di phishing a tema banking (1.2)

Esempio di phishing a tema «casella piena»

Rispondi | Rispondi a tutti | Inoltra | Altro

Da Amministratore IT/Supporto <[redacted]@comune.[redacted]>

Oggetto **Cordiali saluti: importante** 02/11/21, 05:59

Gentile utente di posta elettronica,

La Sua casella di posta elettronica ha quasi raggiunto la sua capacità massima di archiviazione; quindi, non può ricevere nuove e-mail in arrivo e tutte le e-mail in uscita non saranno consegnate.

È necessario aggiornare la Sua casella di posta per aumentare lo spazio di archiviazione.

4998 MB **5000 MB**

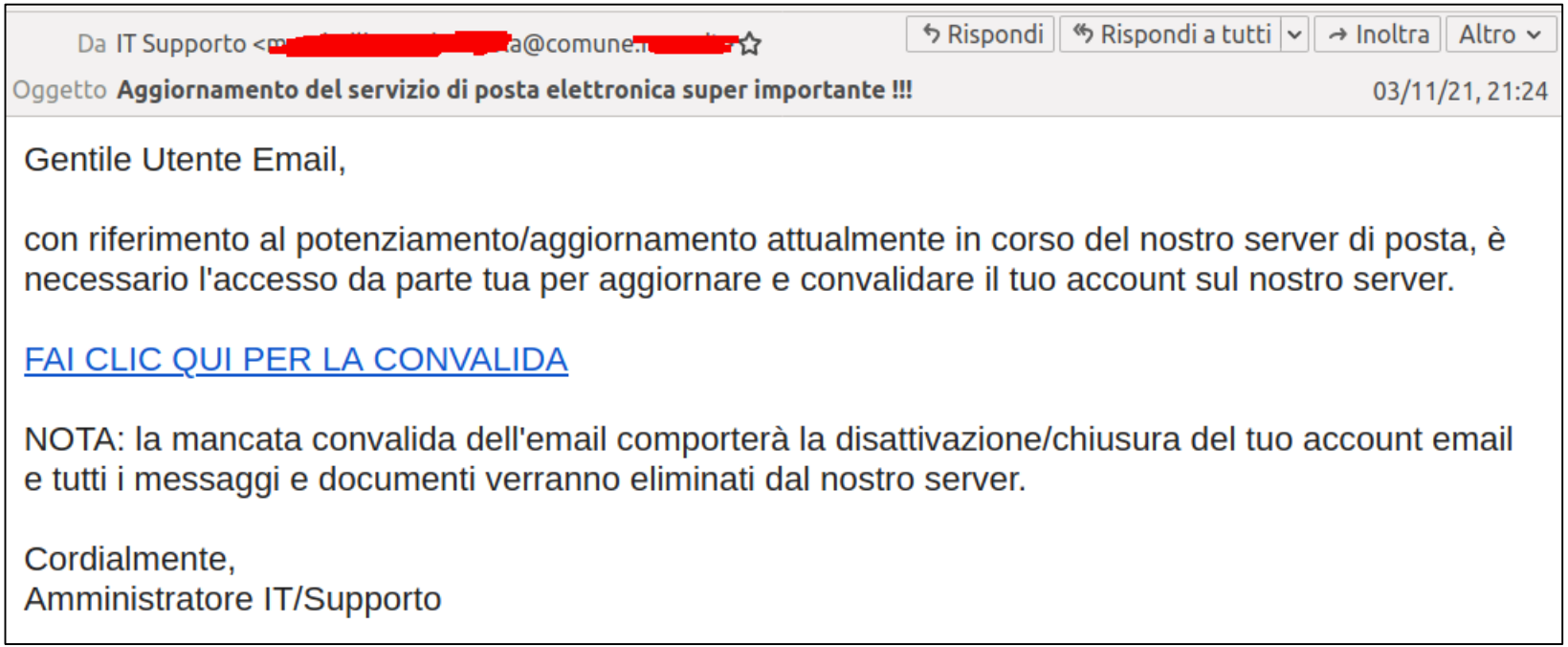
AGGIORNA LO SPAZIO DI ARCHIVIAZIONE DELLA CASELLA DI POSTA QUI

Nota: Il mancato aggiornamento implica che la Sua casella di posta sarà chiusa/disattivata per ridurre al minimo il tempo di inattività del nostro server.

Cordialmente,

Amministratore IT/Supporto

Esempio di phishing a tema «aggiornamenti»



Da IT Supporto <[redacted]a@comune.[redacted]>

Rispondi | Rispondi a tutti | Inoltra | Altro

Oggetto **Aggiornamento del servizio di posta elettronica super importante !!!**

03/11/21, 21:24

Gentile Utente Email,

con riferimento al potenziamento/aggiornamento attualmente in corso del nostro server di posta, è necessario l'accesso da parte tua per aggiornare e convalidare il tuo account sul nostro server.

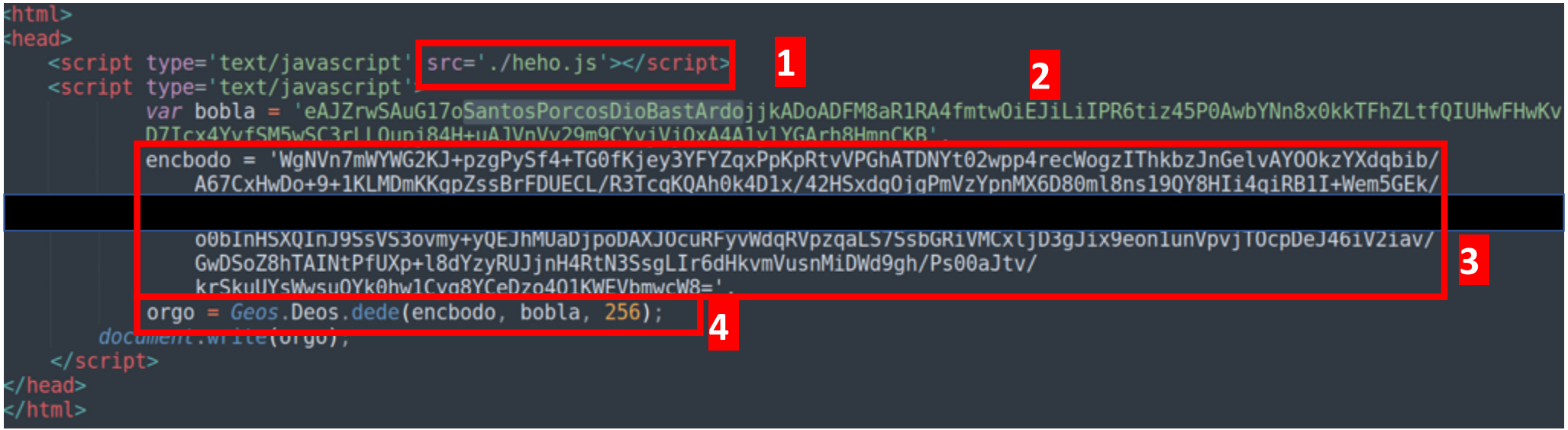
FAI CLIC QUI PER LA CONVALIDA

NOTA: la mancata convalida dell'email comporterà la disattivazione/chiusura del tuo account email e tutti i messaggi e documenti verranno eliminati dal nostro server.

Cordialmente,
Amministratore IT/Supporto

Phishing a tema «aggiornamenti»: ANALISI (1.1)

Con gli «Strumenti per sviluppatori» di Chrome (o l'analogo in Firefox o altro browser)




```
<html>
<head>
    <script type='text/javascript' src='./heho.js'></script>
    <script type='text/javascript'>
        var bobla = 'eAJZrwSAuG17oSantosPorcosDioBastArdojjkADoADFM8aR1RA4fmtwOiEJiLiIPR6tiz45P0AwbYNn8x0kkTFhZLtfQIUHwFHwKv
        D7Tcx4YvfSM5wSC3rLLQupi84H+uAJVnVv29m9CYviViQxA4A1vlYGArh8HmnCKB'
        encbodo = 'WgNVn7mWYWG2KJ+pzgPySf4+TG0fKjey3YFYZqxPpKpRtvVPGhATDNYt02wpp4recWogzIThkbzJnGelvAYOOkzYXdqbib/
            A67CxHwDo+9+1KLMDmKKgpZssBrFDUECL/R3TcqKQAh0k4D1x/42HSxdgOjgPmVzYpnMX6D80ml8ns19QY8HIi4qiRB1I+Wem5GEk/
            o0bInHSXQInJ9SsVS3ovmy+yQEJhMUaDjpoDAXJOcuRFyvWdqRVpzqaLS7SsbGRiVMCxljD3gJix9eon1unVpvjTOcpDeJ46iV2iav/
            GwDSoZ8hTAINtPfUXp+l8dYzyRUJjnH4RtN3SsgLIr6dHkvmVusnMiDWd9gh/Ps00aJtv/
            krSkuUYsWwsuOYk0hw1Cvq8YCeDzo4O1KWEVbmwcW8='.
        orgo = Geos.Deos.dede(encbodo, bobla, 256);
        document.write(orgo);
    </script>
</head>
</html>
```

(1) - Script Javascipt per decodifica AES

(2) - Password

(3) - Body cifrato in AES

(4) - Funzione di decifratura

Phishing a tema «aggiornamenti»: ANALISI (1.2)

https://ufficiocliente.com/heho.js   120%

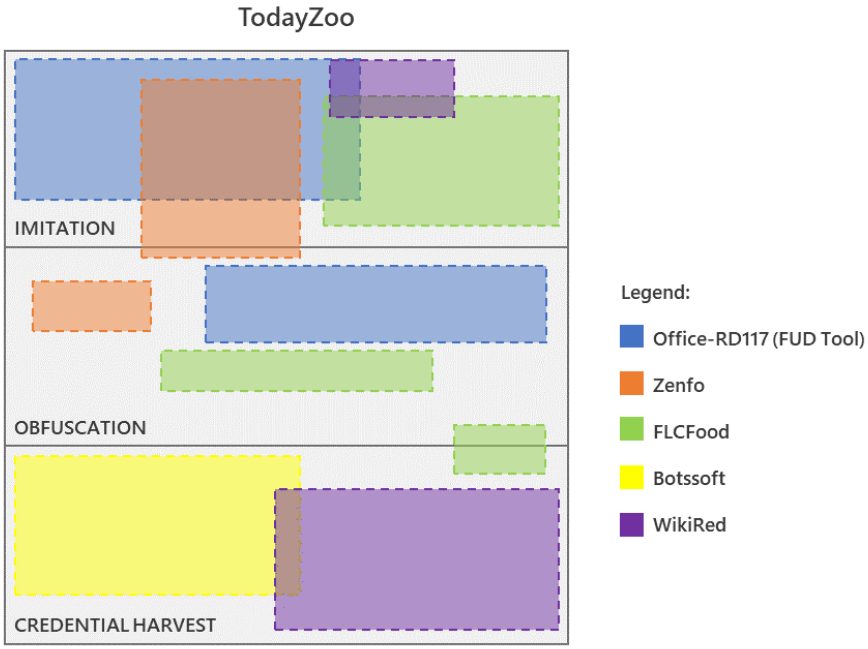
```
/* - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - */
/*  AES implementation in JavaScript                     (c) Chris Veness 2005-2014 / MIT Licence */
/* - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - */

/* jshint node:true *//* global define */
'use strict';


/**
 * AES (Rijndael cipher) encryption routines,
 *
 * Reference implementation of FIPS-197 http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.
 *
 * @namespace
 */
var Geos = {};


/**
 * Decrypt a text encrypted by AES in counter mode of operation
 *
 * @param   {string} ciphertext - Cipher text to be decrypted.
 * @param   {string} password - Password to use to generate a key for decryption.
 * @param   {number} nBits - Number of bits to be used in the key; 128 / 192 / 256.
 * @returns {string} Decrypted text

 * @example
 *   var decr = Geos.Deos.decrypt('lwGl66VVwVObKIr6of8HVqJr', 'pÄ ÅŸÄ¡ÄµÅ Ä™Ä'', 256); // 'big secret'
 */
Geos.Deos.dede = function(ciphertext, password, nBits) {
```

Parametri

Routine

Kit di Phishing

- La maggior parte degli attacchi di Phishing si avvale di **kit pronti all'uso**
- Uno dei più recenti usato ai danni di Microsoft è **TodayZoo** che riutilizza codice di altri precedenti kit (vedi box colorati)
- I kit di phishing sono formati da tre parti:
  1. **Imitation** (parte di presentazione, contenente html, immagini, loghi del sito target)
  2. **Obfuscation** (rendono più difficile la lettura del codice html/css, forniscono quindi la funzionalità di anti detection)
  3. **Credential Harvest** (si occupano della raccolta delle credenziali).



Phishing-as-a-service (PhaaS)

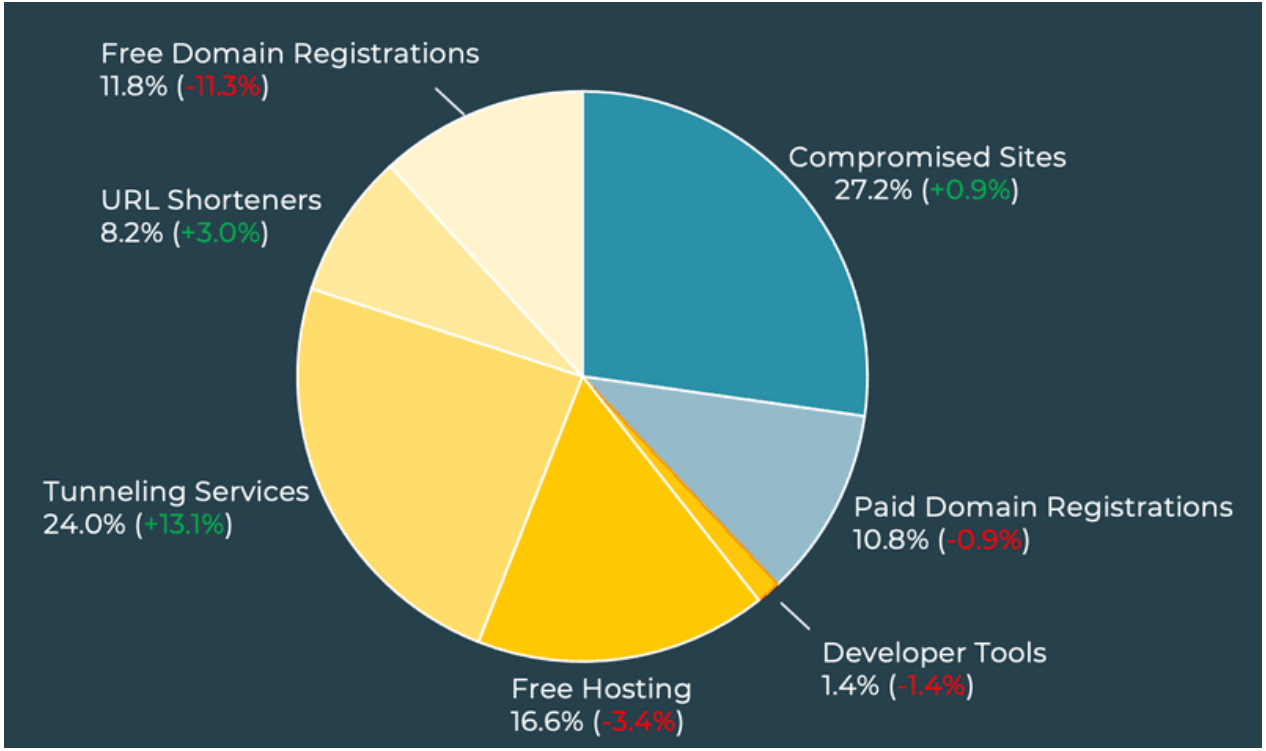
- **Il 21 settembre 2021 Microsoft** rileva **BulletProofLink**, un'evoluzione dei kit di phishing in modalità **PHaaS** che ha permesso agli attaccanti la creazione di 300.000 domini in una singola esecuzione.
- Il servizio **attivo dal 2018** viene venduto sul dark web con **abbonamenti una tantum o mensili** e fornisce
- **BulletProofLink** fornisce ai suoi «clienti» più di **100 template** di pagine di phishing legati ai brand più noti
- I prezzi vanno da **$80 a $100** e sono disponibili sullo store anche tutorial per aiutare i clienti nell'utilizzo del servizio
- **il phishing-as-a-service**, come per il modello software-as-a-service, **fornisce un servizio «chiavi in mano»**: l'attaccante deve solo avviare la campagna e attendere la ricezione delle credenziali, senza preoccuparsi del registrazione del dominio, hosting, invio delle mai e raccolta delle credenziali.

	Phishing kits	Phishing-as-a-Service (PhaaS)
Payment	One-time	Subscription-based *(Available weekly, bi-weekly monthly, or annual)*
Email templates	✓	✓ *(Optional)*
Site templates	✓	✓
Email delivery		✓ *(Optional)*
Site hosting		✓
Credential theft		✓
Credential redistribution		✓
"Fully undetected" links/logs		✓

URL di Phishing

Servizi utilizzati nelle campagne di phishing

- In base all'ultimo report di **PhishLabs** (secondo trimestre 2021), l'**11,1%** delle URL di phishing ha utilizzato **domini a registrazione gratuita** contro **l'10,8%** ha utilizzato **servizi a pagamento**
- Un altro **26,3%** delle URL ha utilizzato **siti compromessi** mentre il
- Aumenta lo sfruttamento dei servizi di **URL shortner** (**dal 5,2% al 8,2%** nell'ultimo report)
- Incrementano invece i **servizi di Tunneling** (dal 10,9% al)

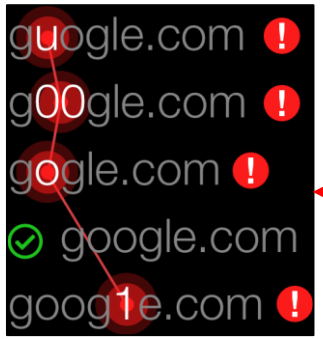


Fonte: PhishLabs/

Domini di phishing

Domini di phishing italiani

- portale-**psd2**.com
- info-sblocco-**posteitaliane**-com.preview-domain.com
- portaleweb1-**Intesasanpaolo**.xyz
- **protocollo**-dati2021.com



Typesquatting

Top 10 TLDs Abused

TLD	TYPE	% PHISH	+/-
.COM	Legacy gTLD	39.7%	-7.2%
.ORG	Legacy gTLD	5.9%	+1.0%
.CA	ccTLD	4.1%	+3.5%
.IO	ccTLD	3.7%	-2.4%
.NET	Legacy gTLD	3.2%	+1.2%
.MX	ccTLD	2.8%	+2.7%
.CO	ccTLD	2.4%	+1.8%
.UZ	ccTLD	2.4%	+2.4%
.MONSTER	New gTLD	2.2%	+2.2%
.AE	ccTLD	2.1%	+2.1%

Fonte: PhishLabs QTTI Report Ago 2021

Struttura di URL di phishing

URL: https://poste-italiane.it-pagamenti.domain.mx/directapp/55320

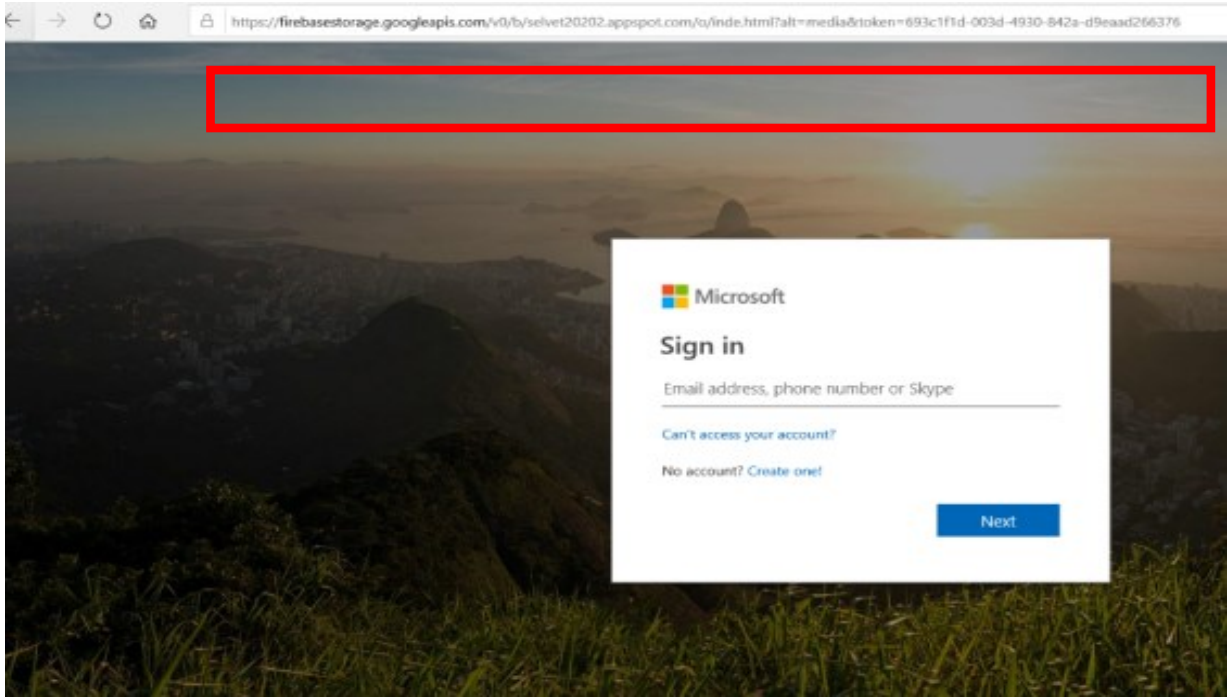
- Protocollo
- Nome del dominio
- Sottodominio2
- Sottodominio1
- Dominio di primo livello (TLD)
- Path

Esempi di URL di phishing che sfruttano domini leciti (1)

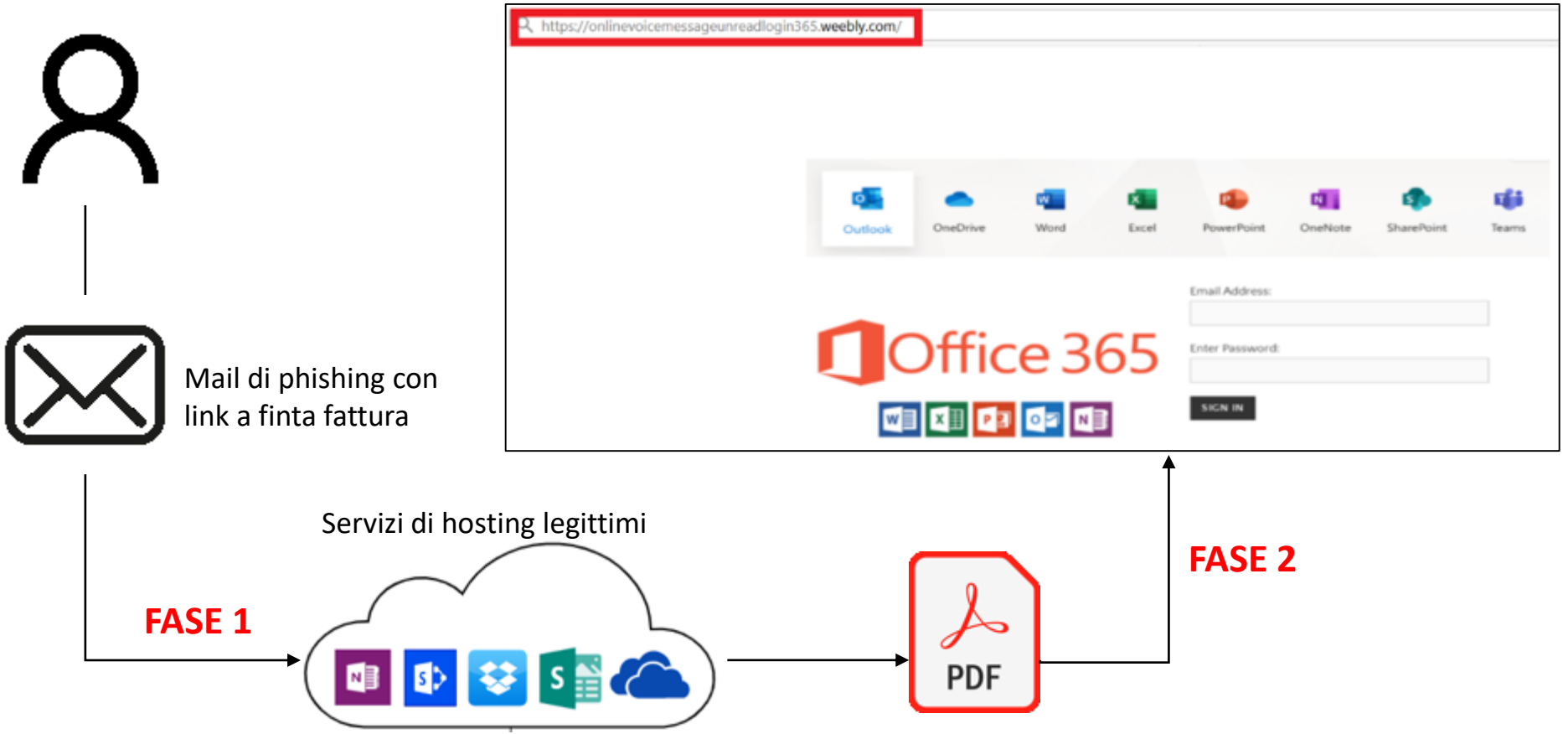
- **Pagine di phishing che sfruttano servizi di Short URL**
  - hXXps://**bit.ly**/3w8Ru6G
  - hXXps://**tinyurl.com**/wjrh8r6u
  - hXXps://**ow.ly**/37Cx30rFY7u
  - hXXps://**rb.gy**/xwhkst
  - hXXps://**cutt.ly**/6R07zpk
  - hXXps://**tinyurl.com**/3u5emycj
- **Servizi Google**
  - hXXps://**sites.google.com**/**view**/orange-bank-france-/accueil
  - hXXps://**docs.google.com**/**forms**/d/e/1FAIpQLSc-xysoGoHjSbzmcnodeD8OoAR2Gz1c5ZxoBGk8EnVh3jBPow/viewform
- **Servizio Amazon S3**: hXXps://outlook-password-expiring-object-storage-static-web-hosting-ln3.**s3.eu-de.cloud-object-storage.appdomain.cloud**/index.html

Esempi di URL di phishing che sfruttano servizi leciti (2)

- **Servizio: Google Firebase**
- **Dominio: firebasestorage.googleapis.com**
- Google Firebase è una piattaforma di sviluppo per applicazioni web e mobile
- Attraverso le API di Firebase è possibile archiviare la pagina di Phishing e i dati carpiti in un bucket di Google Cloud
- Servizi simili:
  - phishingdomain.**weebly.com**
  - phishingdomain.**wixsite.com**



Pagina di phishing multifase



Best practices

- Quando ricevi un'email presta la massima attenzione, verifica che la mail sia autentica**, guarda bene chi è il mittente e pensaci due volte prima di cliccare** su eventuali link o allegati

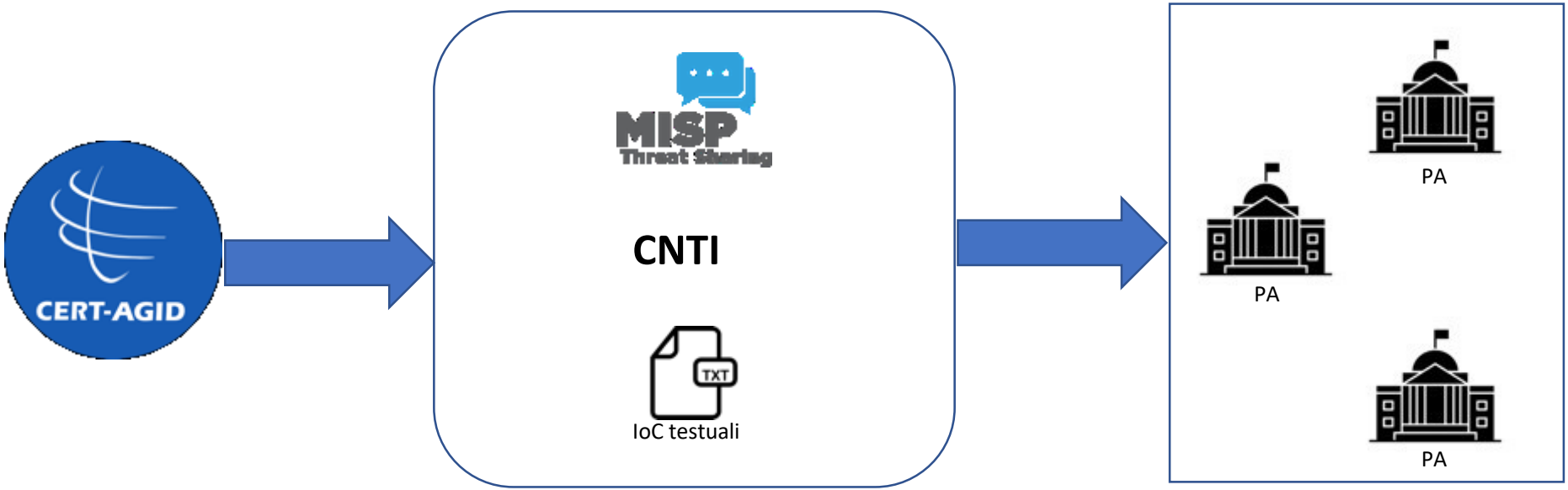
- **Controlla bene le URL**, in particolare se:
  - **Il dominio non è correlato con l'azienda** che ha inviato il messaggio
  - **Il dominio** è **molto lungo** (vedi esempi precedenti)
  - **Il dominio** contiene molti ' **-** ' (es. https://intesa**-**san**-**paolo-accesso**-**conto.dominio**-**fake.com)
  - Il **dominio** contiene molti '.' (es. sub-domain2.subdomain3.sub-domain4.mcomerce.com)
  - Il dominio contiene molti numeri
  - **il nome del brand** è contenuto **nel path** (http://108.179.216.140/**intesasanpaolo**
  - **è presente una mail** (http://**username@hotmail.com.fddcol.com**)
  - **il nome del dominio è codificato** (es. https://www**.%64isc%72%65%74%2done-%6ei%67h%74.%63o%6d**)
  - la **presenza di un IP** o **indirizzo IP codificato** (es. http://**0x42.0x1D.0x25.0xC2**)
  - **simboli provenienti da altre lingue** simili all'alfabeto latino

- Se non sei sicuro che una richiesta e-mail sia legittima **non rispondere** o **prova a verificarla contattando direttamente l'azienda mittente**, tramite i contatti abituali.

Strumenti

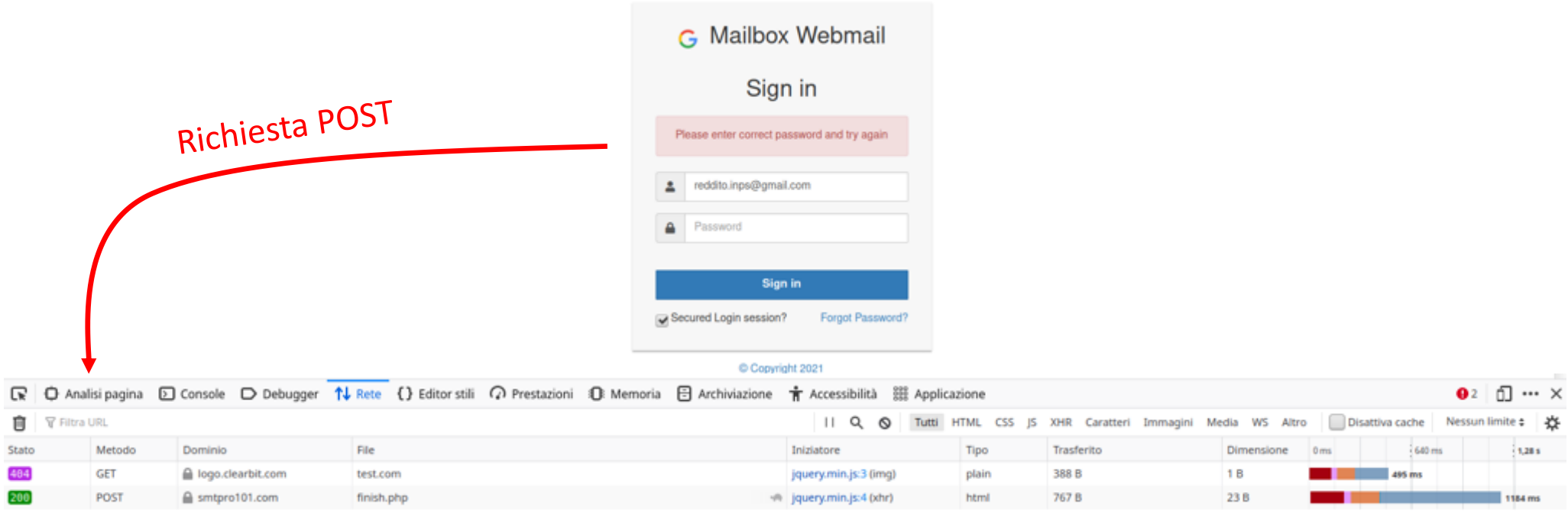
Servizio di condivisione IoC del Cert-AgID

- **Il CERT-AGID eroga un servizio di IoC** tramite i classici canali offerti via **MISP** e **CNTI** alle Pubbliche Amministrazioni accreditate
- Le Pubbliche Amministrazioni possono anche utilizzare un flusso di Indicatori in **formato testuale** per innalzare la protezione delle proprie macchine in maniera semplice, magari anche tramite un firewall di rete. Per accedere al flusso seguire le indicazioni scritte in https://cert-agid.gov.it/scarica-il-modulo-accreditamento-feed-ioc/



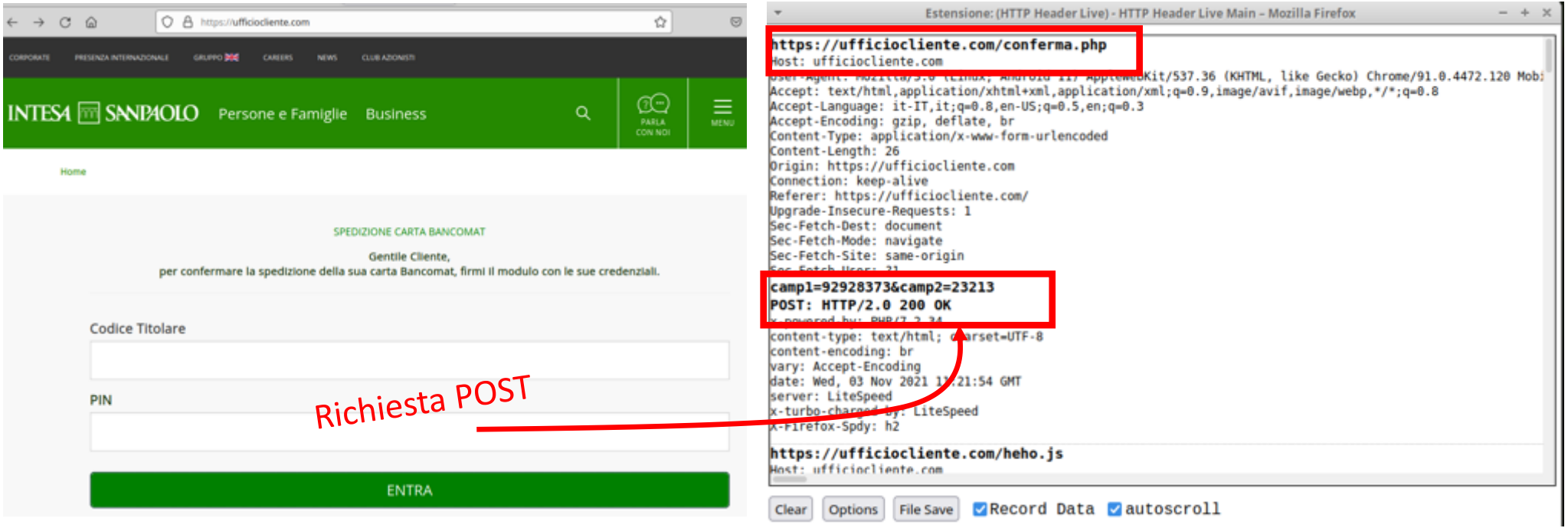
Analisi delle richieste POST di un URL di phishing (1)

«Strumenti per sviluppatori» di Chrome
(o l'analogo in Firefox o altro browser)



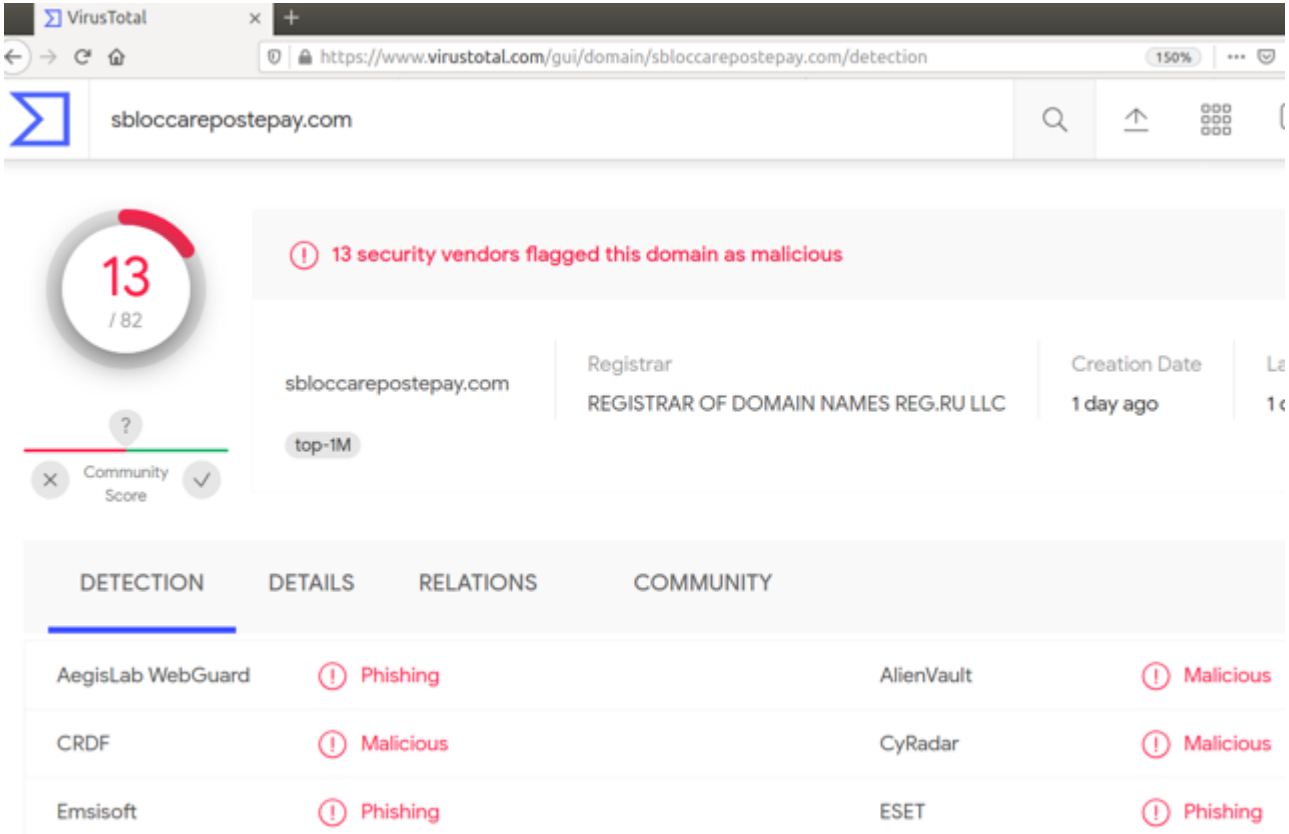
Analisi delle richieste POST di un URL di phishing (2)

HTTP Header Live
(estensione per Firefox)



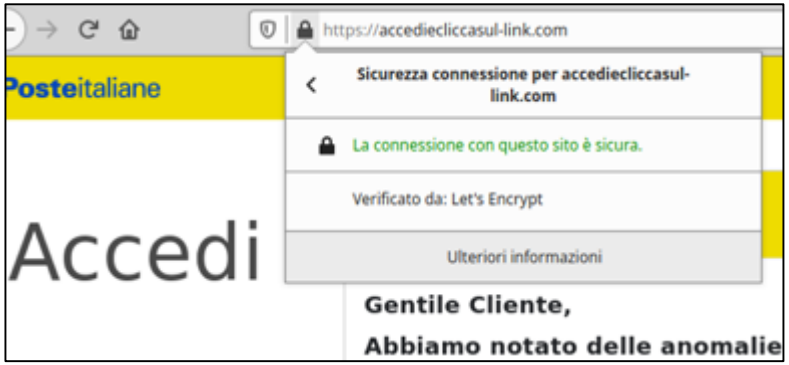
Fonte: https://addons.mozilla.org/it/firefox/addon/http-header-live/

VirusTotal

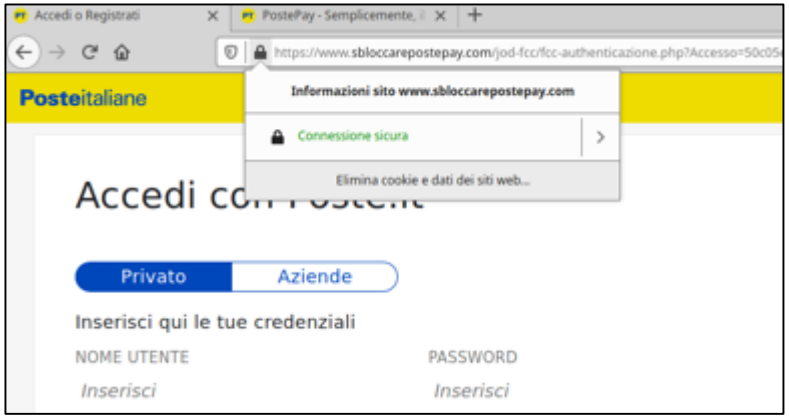

VirusTotal
https://www.virustotal.com/gui/domain/sbloccarepostepay.com/detection
150%
sbloccarepostepay.com
13
/ 82
13 security vendors flagged this domain as malicious
sbloccarepostepay.com
Registrar
REGISTRAR OF DOMAIN NAMES REG.RU LLC
Creation Date
1 day ago
top-1M
Community Score
DETECTION
DETAILS
RELATIONS
COMMUNITY
AegisLab WebGuard
Phishing
AlienVault
Malicious
CRDF
Malicious
CyRadar
Malicious
Emsisoft
Phishing
ESET
Phishing

Verifica del certificato

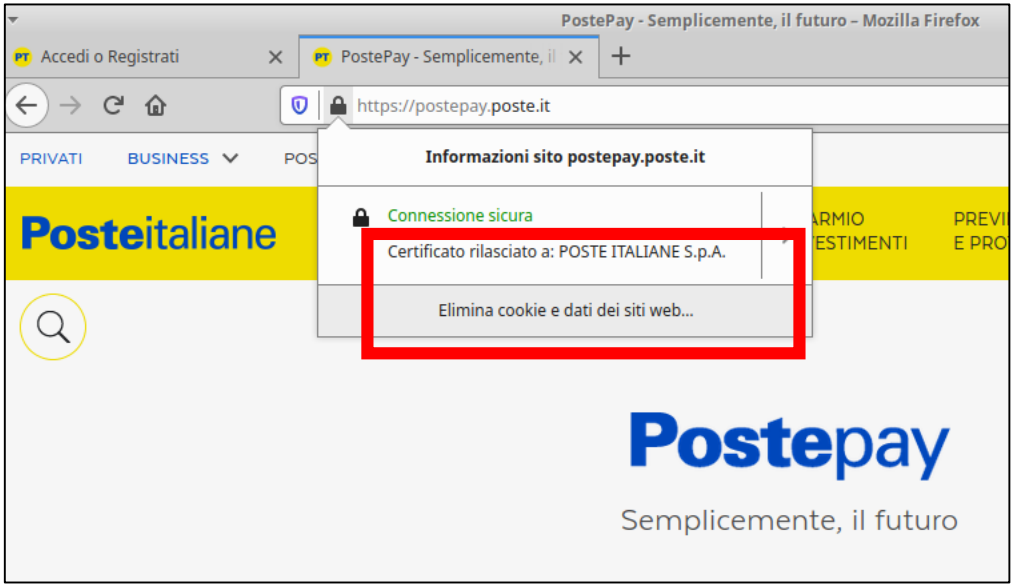
Sito Fake



Sito Fake



Sito legittimo



Security awarness

La miglior difesa è la formazione

- Secondo il report **Threat Landscape 2021** di Enisa, il dipendente aziendale sarebbe responsabile dell'**84% delle compromissioni del perimetro informatico**

- Il **National Institute of Standards and Technologies (NIST)** classifica le minacce informatiche che provengono dal personale interno all'azienda come Insider Threats e sottolinea l'importanza della presa di coscienza della minaccia come primo passo necessario per la mitigazione del rischio informatico

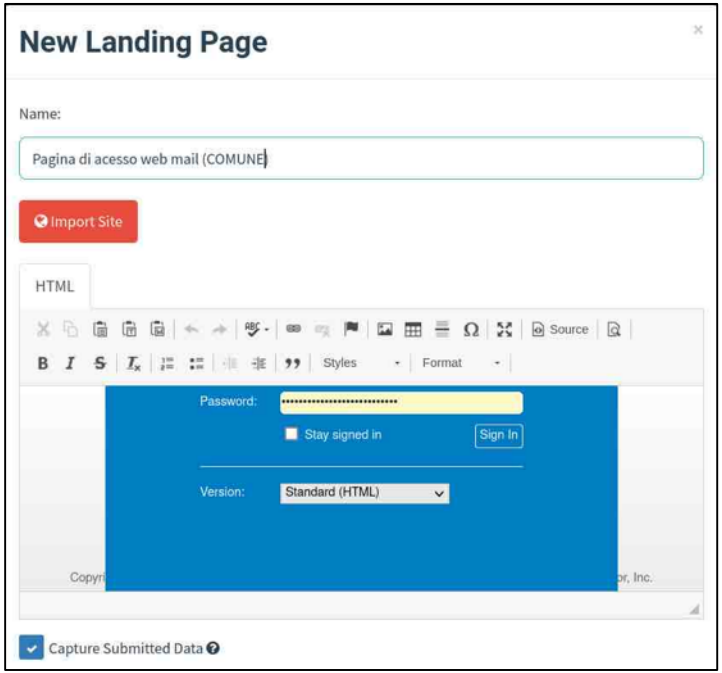
- **Kevin Mitnick**: «Si possono investire milioni di dollari per i propri software, per l'hardware delle proprie macchine e per dispositivi di sicurezza all'avanguardia ma se c'è anche solo un unico dipendente della nostra azienda che può essere manipolato con un attacco di ingegneria sociale, tutti i soldi investiti saranno stati inutili»

Simulazione di campagne phishing nella PA

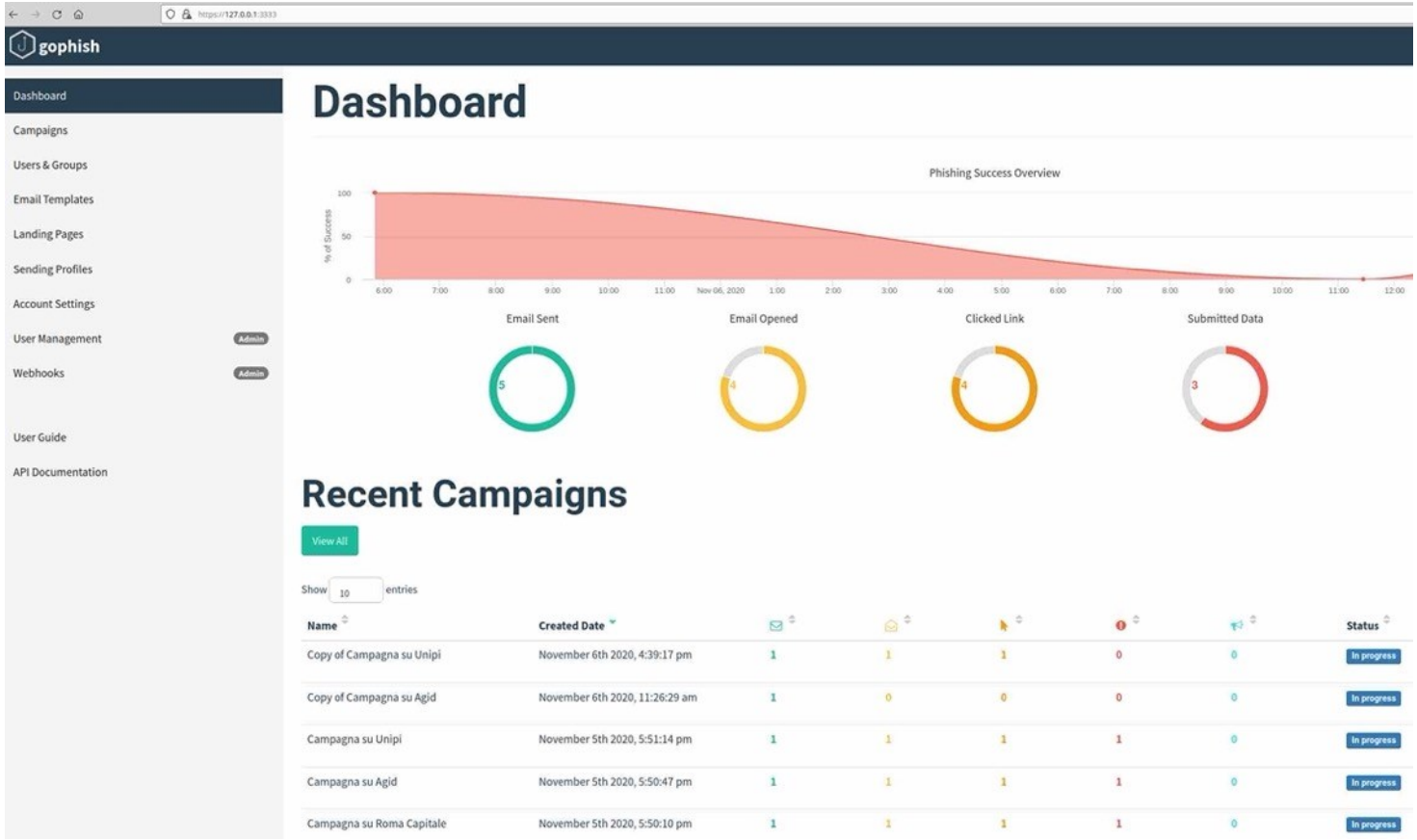
- **Gophish** è un phishing framework **Open Source** che **permette di simulare campagne di Phishing**;
- **Consente l'invio delle email fraudolente**, la creazione della landing page e il monitoraggio della campagna.
- Gophish è uno strumento **multi piattaforma**, sviluppato in Go, utilizzabile su Linux, MacOS e Windows.
- Ottimo per simulare all'interno della propria organizzazione una campagna di Phishing e di **misurare il livello di security awareness della singola organizzazione**
- Nel rispetto della riservatezza dei lavoratori, i dati raccolti dovranno subire un processo di **anonimizzazione e aggregazione**.

Creare una campagna di phishing in 5 step con OpenPhish

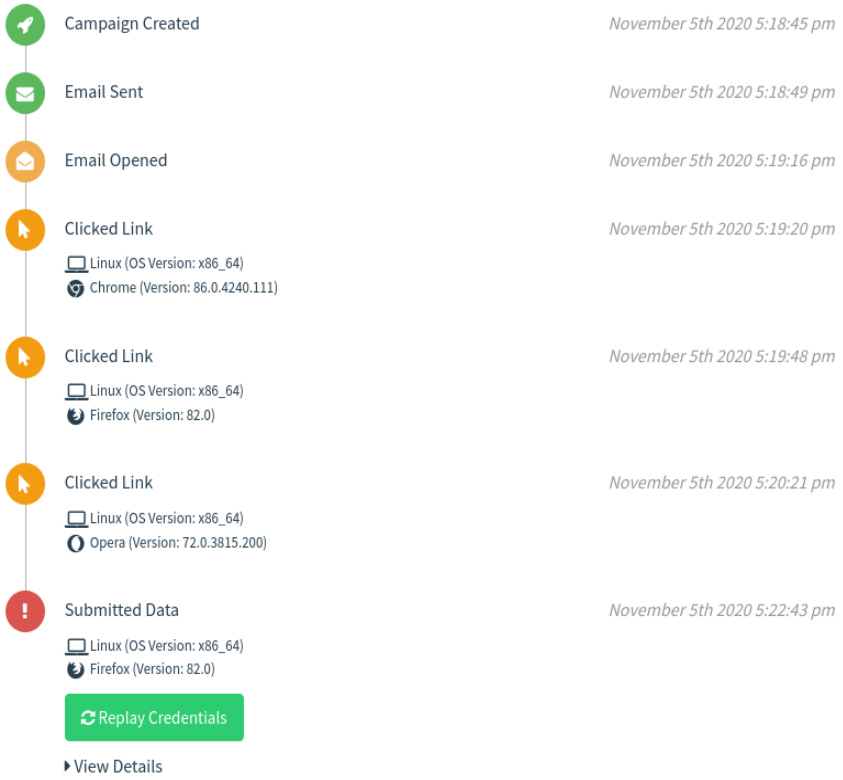
- **STEP 1**: configurazione di un account mittente (SMTP server)
- **STEP 2**: creazione il modello di phishing mail
- **STEP 3:** creazione il modello di **landing page**
- **STEP 4:** definizione target e avvio della campagna
- **STEP 5**: monitoraggio real-time e report finale

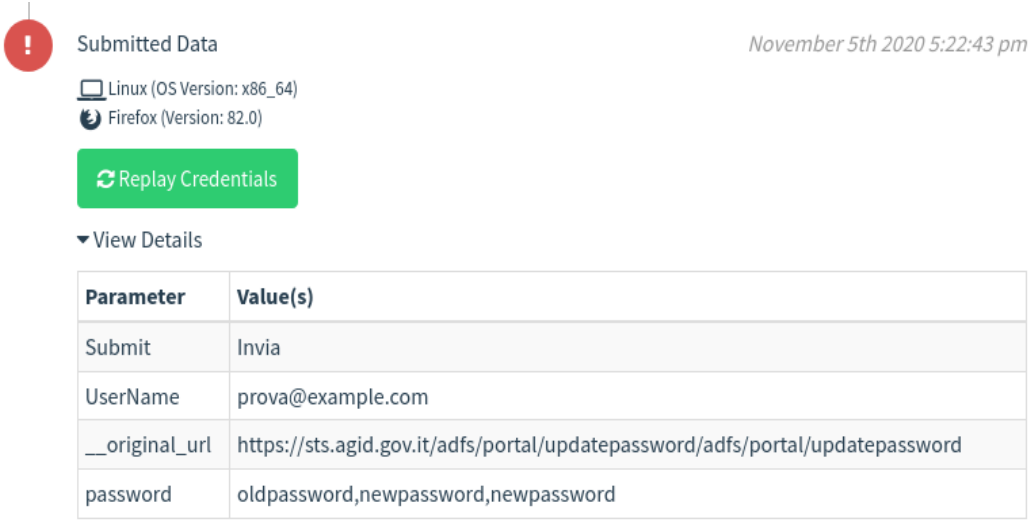


Monitoraggio della campagna



Monitoraggio dei risultati





I benefici

Maggiore consapevolezza dei dipendenti sui rischi cyber legati al phishing

Riduzione della superficie d'attacco

Valutazione del livello attuale di **security awareness** della PA

Riduzione dei costi: le PA possono condurre questi test in totale autonomia senza ricorrere a costosi servizi esterni

UNIONE EUROPEA
Fondo sociale europeo
Fondo Europeo di Sviluppo Regionale

Agenzia per la Coesione Territoriale

Presidenza del Consiglio dei Ministri
Dipartimento della Funzione Pubblica

PON GOVERNANCE E CAPACITÀ ISTITUZIONALE 2014-2020

AGID | Agenzia per l'Italia Digitale

GRAZIE PER L'ATTENZIONE!

petito@agid.gov.it