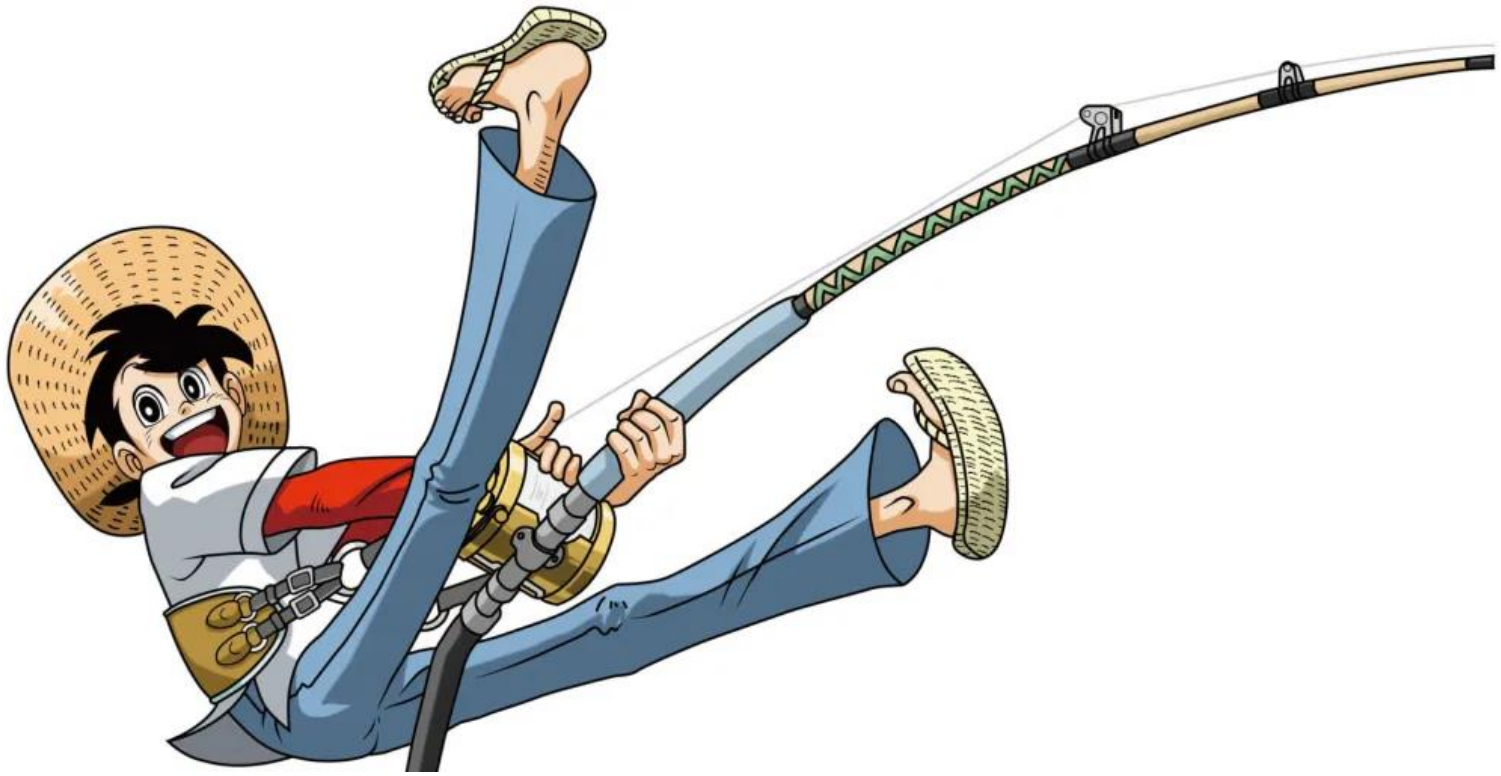
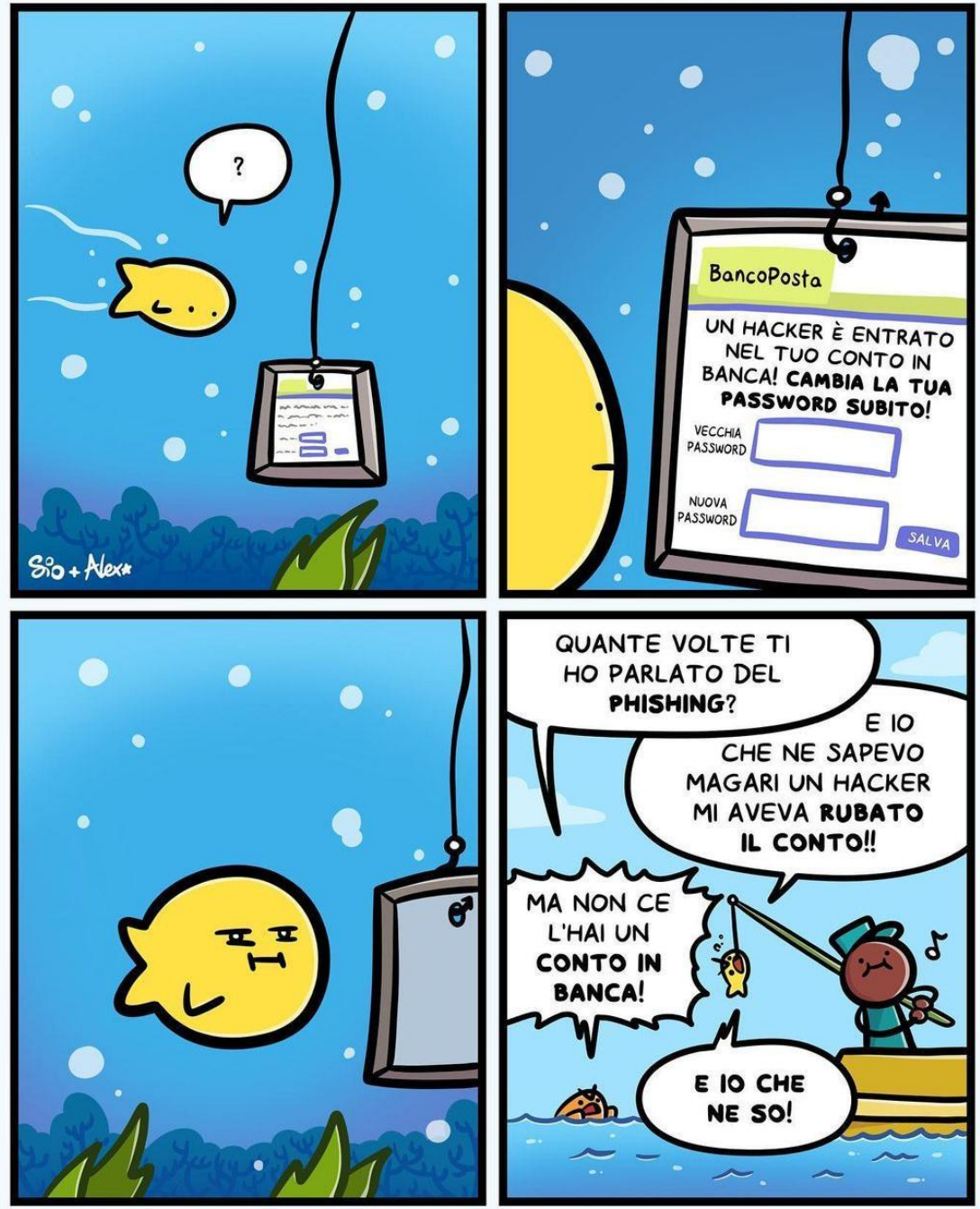


Tsurikichi Sanpei (il patito del phishing)

alessandro@bertoldicybersecurity.com


?
Sio + Alex
BancoPosta
UN HACKER È ENTRATO NEL TUO CONTO IN BANCA! CAMBIA LA TUA PASSWORD SUBITO!
VECCHIA PASSWORD
NUOVA PASSWORD
SALVA
QUANTE VOLTE TI HO PARLATO DEL PHISHING?
E IO CHE NE SAPEVO MAGARI UN HACKER MI AVEVA RUBATO IL CONTO!!
MA NON CE L'HAI UN CONTO IN BANCA!
E IO CHE NE SO!

Ricognizione:
Studio del criterio indirizzi del target

- Serve per capire la struttura degli indirizzi e-mail in modo tale da ricostruire quella del target.
- Le scelte più comuni sono: nome.cognome@nomedominio.ext oppure inizialenome.cognome@nomedominio.ext **(nelle aziende più strutturate solitamente gli indirizzi e-mail corrispondono ai nomi utente di Ldap o dei servizi di Directory)**
- Utilizzando https://it.linkedin.com/ , https://pipl.com/ , https://hunter.io/ , ecc. ci viene indicato il modello usato per costruire gli indirizzi e spesso le mail di nostro interesse per l'attacco.

Verifica del criterio indirizzi del target

- Utilizzando callback verification “RCPT TO” tramite Telnet (**se vogliamo rimanere anonimi** utilizziamo Telnet su TAILS con Torsocks)
- torsocks telnet mail.server.ext 25
- helo domain1.com
- MAIL FROM:alice@domain1.com
- RCPT TO:bob@domain1.com
- Se otteniamo la risposta **“Recipient OK”** l’indirizzo esiste

```
Prompt dei comandi
220 mailsrv.domain1.com ESMTP MAIL Service ready at DATE
helo domain1.com
250 mailsrv.domain.com Hello [IP.IP.IP.IP]
MAIL FROM:<alice@domain1.com>
250 2.1.0 Sender OK
RCPT TO:<bob@domain1.com>
250 2.1.5 Recipient OK
DATA
354 Start mail input; end with <CRLF>.<CRLF>
From: Alice <alice@domain1.com>
Subject: Messaggio di spoofing da telnet
Date: Thu, 04 Oct 2028 10:25:36 +0200
To: bob@domain1.com

Messaggio di test inviato a bob@domain1.com da un hacker utilizzando
l’indirizzo alice@domain1.com senza averne le credenziali.

.

250 2.0.0 OK: Message accepted
QUIT
221 2.0.0 Bye
```

Ricognizione: Spedizione di un E-Mail al target

- Recuperare per quanto possibile i loghi e le firme (sia che siano di dominio, che del singolo utente) per poi riutilizzarli nel modello della mail di spoofing.

[redacted]

Responsabile Cybersecurity Projects Delivery
Head of Cybersecurity Projects Delivery
Cybersecurity and Business Continuity Management
Area Chief IT, Digital and Innovation Officer

Intesa Sanpaolo Group Services S.c.p.a.
Corso Savona, 58 10024 Moncalieri (TO)
☎ +39011[redacted] +39- +39 011[redacted]
[redacted]@intesasanpaolo.com

Follow Intesa Sanpaolo on:

www.intesasanpaolo.com

LEONARDO
CYBER SECURITY

[redacted]
Cyber and Digital Competence Center
Head of Cyber Security Design&Build

Leonardo – Società per azioni
Via Laurentina, 760 – Roma - 00143 - Italy
Tel: +39 06[redacted]
Mob: +39[redacted]
[redacted]@leonardocompany.com

Sorgente del messaggio di una mail di risposta: lista elementi importanti che è possibile individuare

- E’ possibile ricostruire l’intero percorso* della mail dal punto di partenza a noi, individuando eventuali livelli di protezione (mail gateway e servizi di filtraggio) a monte del server MTA
- Visualizzare l’indirizzo del server di posta (a meno che sul server di posta non si sia stata abilitata l’opzione: Hide local IP in Received headers, in tal caso sul sorgente del messaggio si visualizzerà 127.0.0.1)*
- Visualizzare l’indirizzo IP Pubblico di chi invia (molto utile anche per una scansione delle porte o per risalire all’internet provider della sede)
- Visualizzare il client di posta di chi invia (User-Agent)

Sorgente del messaggio di una mail di risposta: si possono estrarre elementi utilissimi per il nostro lavoro

```
Return-Path: alessandro@bertoldicybersecurity.com
Received: from rmcv-zcs-mta01.clouditalia.com (LHLO
 rmcv-zcs-mta01.clouditalia.com) (10.24.28.132) by
 rmcv-zcs-mbs01.clouditalia.com with LMTP; Sat, 14 May 2022 10:46:31 +0200
 (CEST)
Received: from localhost (localhost [127.0.0.1])
    by rmcv-zcs-mta01.clouditalia.com (Postfix) with ESMTP id 8D77F144F3E
    for <abertoldi@partner.clouditalia.com>; Sat, 14 May 2022 10:46:31 +0200 (CEST)
X-Spam-Flag: NO
X-Spam-Score: -0.599
X-Spam-Level:
X-Spam-Status: No, score=-0.599 tagged_above=-10 required=4
    tests=[BAYES_05=-0.5, DKIM_SIGNED=0.1, DKIM_VALID=-0.1,
    DKIM_VALID_AU=-0.1, HTML_MESSAGE=0.001] autolearn=ham
Authentication-Results: rmcv-zcs-mta01.clouditalia.com (amavisd-new);
    dkim=fail (2048-bit key) reason="fail (bad RSA signature)"
    header.d=bertoldicybersecurity.com header.b=C0byicz8;
    dkim=pass (2048-bit key) header.d=bertoldicybersecurity.com
    header.b=vRKXfkY6
Received: from rmcv-zcs-mta01.clouditalia.com ([127.0.0.1])
    by localhost (rmcv-zcs-mta01.clouditalia.com [127.0.0.1]) (amavisd-new, port 10024)
    with ESMTP id rfHxlOWicZ_q for <abertoldi@partner.clouditalia.com>;
    Sat, 14 May 2022 10:46:31 +0200 (CEST)
Received: from out1-94.antispamcloud.com (out1-94.antispamcloud.com [185.201.16.94])
    by rmcv-zcs-mta01.clouditalia.com (Postfix) with ESMTPS id 48184144EA9
    for <abertoldi@partner.clouditalia.com>; Sat, 14 May 2022 10:46:31 +0200 (CEST)
DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/relaxed;
    d=bertoldicybersecurity.com; s=mail; h=Content-Type:MIME-Version:To:From:
    Message-ID:Subject:Date:reply-to:sender:cc:bcc:in-reply-to:references:
    content-transfer-encoding; bh=FMA64jpVjowVimJ5umIy4OEyiIPhq6clsLHnBx14/vY=;
     b=C0byicz8z5131J7Bn9M6Ty6ta1I9Xq0HQ7s+qYQPXq5AFRKuBdDttwk2iD/eEnO3+AJOjIwtQi
    LGOWEVlSdo/BdUd/1DFr9qqpHWjHWjEz1x0QLXDnIg/+ELqQLhywSH6kne6aDuaOcEA1LdgIOHmGZ
    Kmh5pVEgys7J/8R+nKmxR1ID3iTT+W0N219IcFshv67Nmv2RAs/ypPW+9r9wBJf09r7P4GH7sdeEz
    OPsG0KC5G44GzY7HzuIrf+tlCcF/yPwMfzEa3KmlaO+QC+uRfDrWMu9AgTo4QBwrJrXHkRUqBkz4W
    Y9L4uKCwZrDP0gmO3YqGl5V2kHA9gnjJJ7gyw==;
Received: from mail-de-01.intactmail.pro ([54.36.235.115])
    by mx7.antispamcloud.com with esmtpsa (TLSv1.3:TLS_AES_256_GCM_SHA384:256)
    (Exim 4.92)
    (envelope-from <alessandro@bertoldicybersecurity.com>)
    id 1npnPs-0001X1-9v
    for abertoldi@partner.clouditalia.com; Sat, 14 May 2022 10:46:30 +0200
DKIM-Signature: v=1; a=rsa-sha256; c=simple/simple;
    d=bertoldicybersecurity.com; s=mail;
    h=from:subject:date:message-id:to:mime-version:content-type;
    bh=urQj9khEEIyEBGa471TmNwvIbQmgVKXSyBbs4mM7qog=;
    b=vRKXfkY6f0/8UMWAueMdtLRnluovWOzQ2SnCq2Di3QimE0DyymiGOyR35Z30zYbyPEsz7E8TUsSjR
     SlqFTeZ4teQ041m61mJz4lnU5kx0+bEmLLXuvjg6fgoxlAeijV9h0kSc549svFNBM+aw4XePxEy74I
     HO3AH720+8X1kcsdRgHk0L5rVsxc/pRv6nMNCYnZTNONTIKOqE6cENDl5iJHTu7qA09KJngqW6DOpw
     EKoMxyeJQl0KFecWwq76z9dDeNfmJxm1aZ3pfxbEs+tbrcQKBwx7eQZY8uya+SAV/PYqOkkku4L6X8
     ka8SyubngrKZJaerBV4kmtuP2AV2+CA==
X-Footer: YmVydG9sZGljeWJlcnNlY3VyaXR5LmNvbQ==
Received: from localhost ([127.0.0.1])
    by mail-de-01.intactmail.pro with ESMTPSA
    for abertoldi@partner.clouditalia.com;
    Sat, 14 May 2022 10:46:19 +0200
Date: Sat, 14 May 2022 10:46:18 +0200
Subject: Test
```

Ricognizione:
Consultazione DNS del dominio/i target
il tool indispensabile

https://mxtoolbox.com/

MX Loookup

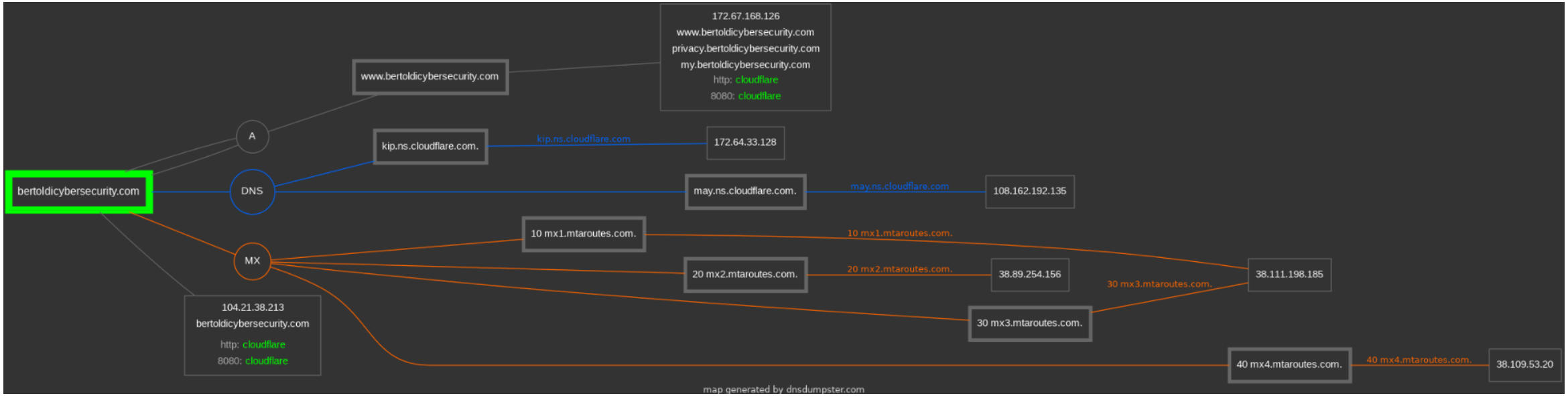
SPF Record Lookup (**Request for Comments: 7208** → Updated by: 8553, 8616)

DKIM Lookup (**Request for Comments: 6376** → Updated by: 8553, 8616)
* per trovare questo campo su MX TOOLBOX ci serve il selettore ad esempio “bertoldicybersecurity.com:mail”

DMARC Lookup (**Request for Comments: 7489** → Updated by: 8553, 8616)

Ricognizione:

Consultazione DNS di dominio: rappresentazione grafica del sistema di posta o almeno in parte….dove è il server di posta?



https://dnsdumpster.com/static/map/bertoldicybersecurity.com.png

Scopriamo quali sono i segreti dei DNS
leggerli per saper attaccare
e integrarli per proteggersi dallo spoofing.

- **SPF – DKIM – DMARC**
- **MTA-STS**
- **DANE**
- **BIMI**

Esempio di record DNS SPF (Sender Policy Framework)

- v=spf1 include:spf.mtaroutes.com include:servers.mcsv.net –all

Meccanismi del record SPF:

v=spf1 Versione di SPF. Questo tag è obbligatorio e deve essere il primo tag del record.

Così si possono autorizzare gli host ad utilizzare "MAIL FROM" ed il comando SMTP HELO/EHLO

ip4 ip4:198.0.2.1 oppure ip4:198.0.2.0/24

Ip6 ip6:3FFE:0000:0000:0001:0200:F8FF:FE75:50DF oppure ip6:2001:db8:1234::/48

a a:mail.intactmail.pro

mx mx:mx1.mtaroutes.com

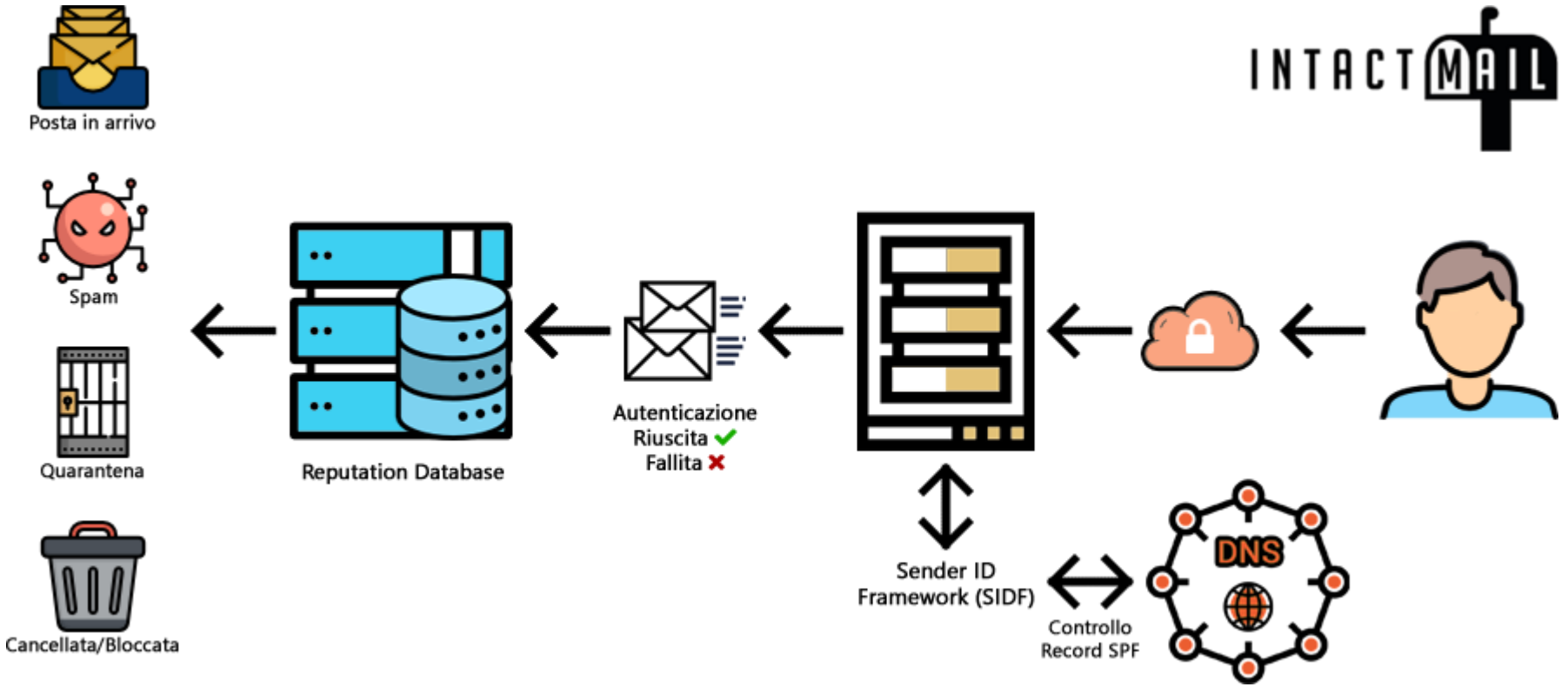
include include:servers.mcsv.net

---

all

finale indica che tutti i messaggi sono corrispondenti, deve essere definito con relativo valore qualificatore + - ~ ?

Capire Sender Policy Framework (SPF)



Esempio di record DNS DKIM (DomainKeys Identified Mail)

v=DKIM1;p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0Qb+FDCF10y
phcWHps6JzTf48koMSe/jpc67Aa1VkIDhrxFrj+ywlmrE8SsYvQ1ZBONOg70+2kdHtd8l
mKN2IYnxv3+GGJOtdaoi7jXX2UsDyMvR4CZp68JjCcfcg1iGJn2+sMEZXCjlskUff2b/icM
8RYluF2r/q0ZKe1tqZhNp38APMxsiwwk02yq0dgD9P0npNphtDVikC/2TUgWUsqx2eR
tRBoGoa4UCyHwwyGgBL1OS6QrX6pp1HGugoQGvPci7u8JoSBhelm+MuE0qUPcUA1
Txj393FSfdUHvS56BwfAowULRpkjuLI6X40npT2IHkCO51H0lurQ490FV7sQIDAQAB

DKIM, o DomainKeys Identified Mail, è un protocollo di autenticazione e-mail che viene utilizzato per verificare l'autenticità delle e-mail in uscita. Il processo comporta l'utilizzo di una chiave crittografica privata generata dal tuo server di posta che firma ogni messaggio di posta in uscita ed una chiave pubblica pubblicata come record di testo sui tuoi DNS di dominio.

Capire DKIM


Posta in arrivo
Chiave Pubblica e
Privata combaciano
La E-Mail viene firmata
con la Chiave Privata
INTACT MAIL
La Chiave Pubblica
viene inviata al
Server di posta ricevente
DNS
La Chiave Pubblica
viene inviata
ai Server DNS

Esempio di record DNS DMARC (Domain-based Message Authentication, Reporting & Conformance)

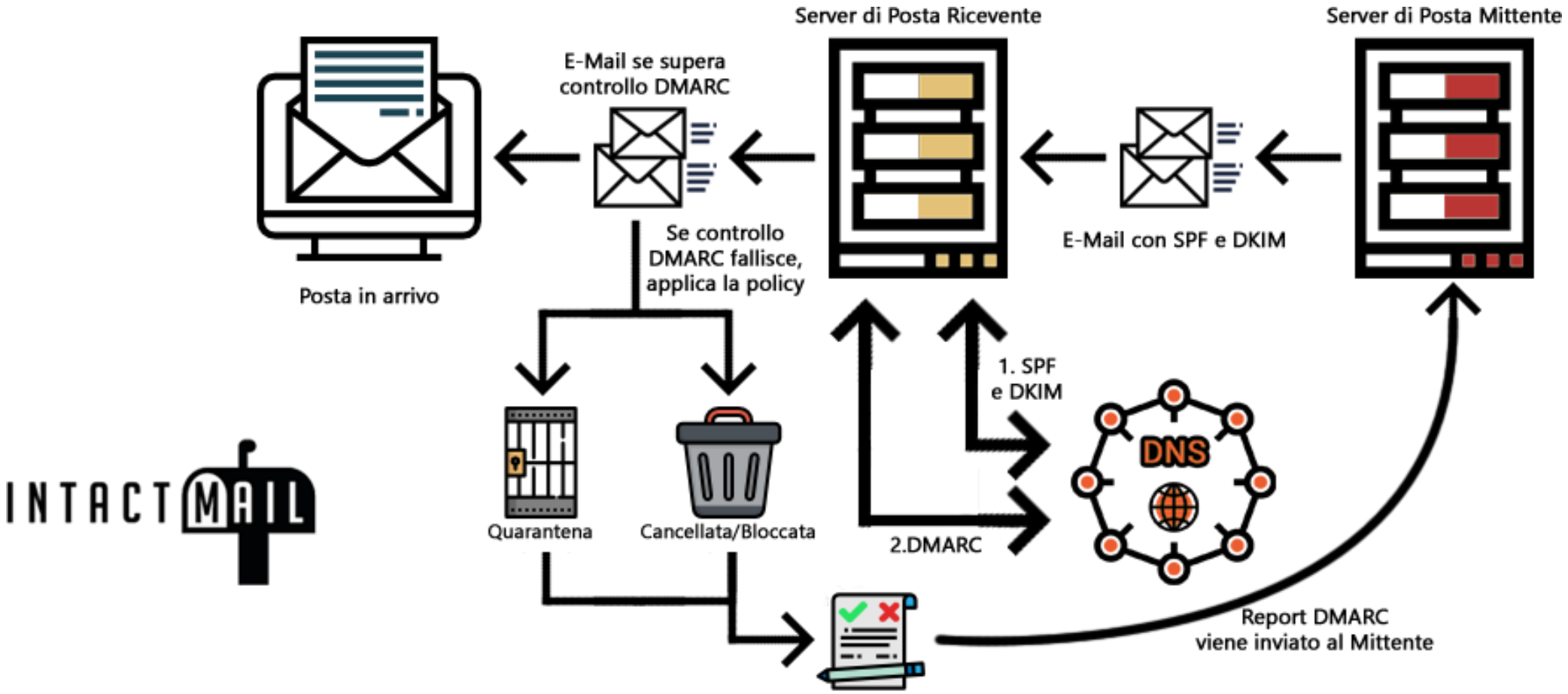
v=DMARC1; p=reject; sp=reject; adkim=s; aspf=s; pct=100; fo=1; rf=afrf; ri=86400; rua=mailto:dmarc_rua@bertoldicybersecurity.com,mailto:b929c56e0d9f086@rep.dmarcanalyzer.com; ruf=mailto:dmarc_ruf@bertoldicybersecurity.com

---

DMARC si basa su SPF e DKIM (può funzionare anche con solo SPF)

e definisce cosa accade alla mail in base alla configurazione della sua policy

Connecting the dots
capire DMARC



<cheat sheet> del record SPF
ci spiega cosa accade alla mail inviata in base al valore

Valore	Azione	Note
+all	Pass	Valore opzionale, il controllo spf verrà sempre superato.
-all	Fail	Se il controllo SPF fallisce, l'email non sarà consegnata al server di destinazione.
~all	SoftFail	Se il controllo SPF fallisce, l'email sarà consegnata al server di destinazione ma verrà contrassegnata come spam.
?all	Neutral	Il controllo SPF sarà ignorato.

<cheat sheet> del record DMARC
ci spiega cosa accade alla mail inviata in base al valore

Tag	Valore	Note
v=	DMARC1	Valore obbligatorio, deve essere il primo tag del record DMARC, mentre gli altri tag non sono case sensitive, questo deve essere obbligatoriamente maiuscolo con il valore v=DMARC1.
p=	Può assumere uno dei seguenti valori: **none** :Nessun avviso specifico sarà dato al server di posta di destinazione **quarantine** :Avvisa il server di posta di destinazione di trattare qualsiasi email che fallisce il test DKIM e/o SPF come sospetta ed esegue controlli aggiuntivi **reject** :Avvisa il server di posta di destinazione di rifiutare qualsiasi email che fallisce il test DKIM e/o SPF	Valore obbligatorio, deve essere il secondo tag del record DMARC. Definisce le regole con le quali i server di posta di destinazione tratteranno le email.
sp=	Stessi valori di p= (reject, quarantine, none)	Valore opzionale, se il tag sp **non è** presente, il tag p coprirà il dominio principale e tutti i suoi sottodomini. Se il tag sp invece è presente indica le regole da applicare a tutti i sottodomini del dominio principale. In questo caso il dominio principale rimane sempre coperto dal tag p.

<cheat sheet> del record DMARC
ci spiega le modalità di allineamento restrittive

adkim=	r (relaxed – default) oppure s (strict)	Valore opzionale, se il tag viene omesso il valore di default sarà adkim=r. Specifica la “modilità di allineamento” per la firma DKIM.
aspf=	r (relaxed) oppure s (strict)	Valore opzionale, se il tag viene omesso il valore di default sarà aspf=r. Specifica la “modalità di allineamento” per il controllo SPF.

<cheat sheet> del record DMARC
ci spiega le % di applicazione e la generazione report

pct=	Valore compreso tra 0 e 100	Valore opzionale, definisce la percentuale di email alle quali le regole del DMARC sono applicate. Se il valore viene omesso il valore di default sarà pct=100, quindi tutte le email saranno sottoposte ai controlli DMARC.
fo=	Può assumere uno dei seguenti valori: **0** : Genera il report al server di posta mittente se tutti i controlli falliscono. Se è utilizzata solo la DKIM come sistema di sicurezza ed il test DKIM fallisce, il report sarà inviato. Se è utilizzata solo l'SPF come sistema di sicurezza ed il test SPF fallisce, il report sarà inviato. Se sono utilizzati sia DKIM che SPF, e l'SPF fallisce ma il test DKIM passa il report non sarà inviato **1** : Genera il report al server di posta mittente se almeno 1 controllo fallisce. Se è utilizzata solo la DKIM come sistema di sicurezza ed il test DKIM fallisce, il report sarà inviato. Se è utilizzata solo l'SPF come sistema di sicurezza ed il test SPF fallisce, il report sarà inviato. Se sono utilizzati sia DKIM che SPF, e l'SPF fallisce ma il test DKIM passa il report sarà inviato **d** : Genera il report se il test DKIM fallisce **s** : Genera il report se il test SPF fallisce	Valore opzionale, se il valore viene omesso il valore di default sarà fo=0. Definisce le regole per quando deve essere generato il report DMARC.

<cheat sheet> del record DMARC ci spiega i parametri del report

rf=	Può assumere uno dei seguenti valori: **afrf** : Il formato del messaggio per il report degli errori (Abuse Report Format) è definito dall'RFC 5965 **iodef** : Il formato del messaggio per il report degli errori (Incident Object Description Exchange Format) è definito dall'RFC 5070	Valore opzionale, se il valore viene omesso il valore di default sarà rf=afrf. Definisce il formato del report DMARC.
ri=	Definisce l'intervallo di tempo dei report in secondi	Valore opzionale, se il valore viene omesso il valore di default sarà ri=86400, cioè 1 giorno. Definisce l'intervallo di tempo in secondi tra l'invio di un report DMARC e l'altro.
rua=	Definisce l'elenco delle email alle quali viene inviato il report aggregato	Valore opzionale, se il valore non è presente i report aggregati non saranno inviati. L'email deve avere il formato mailto:user@example.com
ruf=	Definisce l'elenco delle email alle quali viene inviato il report forense	Valore opzionale, se il valore non è presente i report forensi non saranno inviati. L'email deve avere il formato mailto:user@example.com

Next level dell’ e-mail security contro MITM: MTA-STS

Come agisce MTA-STS?

- MTA-STS è un meccanismo che indica a un server SMTP che la comunicazione con l'altro server SMTP deve essere crittografata e che il certificato deve essere valido.
  La policy indica cosa fare quando non è possibile negoziare un canale crittografato e descrive inoltre come vengono inviati i report.
- https://datatracker.ietf.org/doc/html/rfc8461

- https://datatracker.ietf.org/doc/html/rfc8460
  (SMTP TLS Reporting)

Next level dell’ e-mail security contro MITM: DANE/TLSA

- DANE e MTA-STS hanno lo stesso scopo, ma DANE richiede DNSSEC per l'autenticazione DNS, mentre MTA-STS si basa su autorità di certificazione.

- https://datatracker.ietf.org/doc/html/rfc7672

Next level dell’ e-mail security DANE vs MTA-STS

- DANE è superiore a MTA-STS.
  Il problema è che non tutti vogliono adottare DNSSEC perché, in alcune situazioni, questo è indesiderabile o poco pratico. Tuttavia, MTA-STS è progettato per non interferire con le distribuzioni DANE quindi si possono implementare entrambi.

Servizi esterni per il monitoraggio dei report RUA, RUF e SMTP TLS Reporting

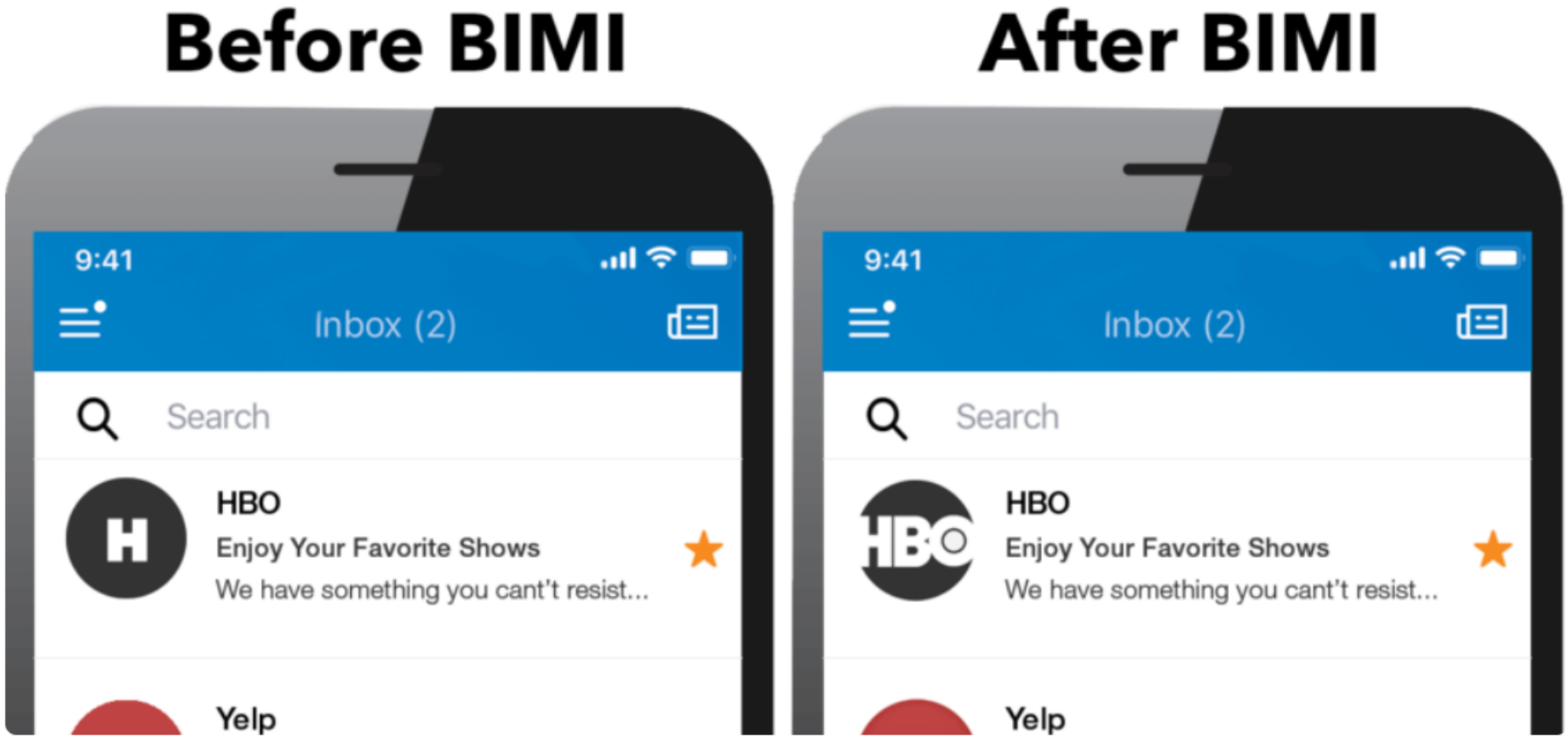
- DMARCIAN
  https://dmarcian.com

- DMARC ANALIZER
  https://www.dmarcanalyzer.com/

Next level dell’ e-mail security standard BIMI

- BIMI (Brand Indicators for Message Identification) è uno standard email che ti consente di aggiungere il logo di un brand ai messaggi autenticati inviati dal tuo dominio. I client di posta che lo supportano mostrano il logo del tuo brand accanto al tuo messaggio nella Posta in arrivo.
- Con BIMI, i loghi e la proprietà dei brand sono verificati tramite i certificati di marchio verificato (VMC), pertanto i destinatari possono essere sicuri che i loghi mostrati nella propria Posta in arrivo siano legittimi.
- https://support.google.com/a/answer/10911320?hl=it#:~:text=BIMI%20(Brand%20Indicators%20for%20Message,messaggio%20nella%20Posta%20in%20arrivo
- https://bimigroup.org/
- https://datatracker.ietf.org/doc/html/draft-blank-ietf-bimi-02

Next level dell’ e-mail security standard BIMI



E-mail spoofing how-to
falsificazione dell'intestazione 'MAIL FROM' (condizioni ideali)

- SPF inesistente, oppure SPF con valore "?all", "+all"
- DKIM inesistente
- DMARC inesistente
- Sistema di filtraggio inesistente

E-mail spoofing how-to
falsificazione dell'intestazione 'MAIL FROM'
(condizioni meno ideali)

- SPF "~all" o "-all"
- DKIM (irrilevante)
- DMARC inesistente
- Sistema di filtraggio inesistente

E-mail spoofing how-to
falsificazione dell'intestazione 'MAIL FROM'
(condizioni sfavorevoli)

- SPF -all
- DKIM (irrilevante)
- DMARC presente con policy non configurata
- Sistema di filtraggio inesistente o esistente

E-mail spoofing how-to falsificazione dell’intestazione‘MAIL FROM’ (condizioni negative)

- SPF -all
- DKIM presente
- DMARC presente con policy configurata correttamente
- Sistema di filtraggio della posta presente

PGP

- Quando non hai la DMARC policy configurata e qualcuno fa mail spoofing iniziando a scambiare chiavi PGP con gli utenti di dominio…
  A meno che non si usi un server che richiede l'autenticazione per inviare le chiavi PGP pubbliche dell'organizzazione
  https://github.com/mailvelope/keyserver

Come falsificare l’intestazione della mail

- Mozilla Thunderbird + Header Tools Lite

https://addons.thunderbird.net/it/thunderbird/addon/header-tools-lite/
Ovviamente la mail di base configurata deve avere le seguenti caratteristiche:

SPF inesistente, oppure SPF con valore “?all”, “+all”

DKIM inesistente

DMARC inesistente

(E non essere riconducibile a voi!)

- Phishing attack con (SET) Social Engineering Toolkit

Individuazione del sistema di filtraggio tramite la lettura dei record MX oppure sfruttando le caratteristiche del sistema di filtraggio.

proofpoint.

Sophos Email Security

mimecast™

N-ABLE™ SpamExperts™

TREND MICRO | Trend Micro Email Security

By-pass sistema di filtraggio

- Il server di posta accetta connessioni solo dal sistema di filtraggio o anche dall'esterno? Come verificarlo?
  Fare risolvere l'indirizzo del server di posta di destinazione (target) **direttamente dal file Host** del sistema operativo dove è installato il nostro server di posta ed inviare al (target) una mail **con conferma di recapito**; se riceveremo la mail di notifica della conferma di recapito il sistema di filtraggio sarà bypassato ovvero il server di destinazione oltre a ricevere dal sistema di filtraggio riceve anche dall'esterno.
  Oppure verificandolo via Telnet.
- Bug noti (sessione telnet aperta nei tool per i clienti N-ABLE Spam Expert, nessuna autenticazione SMTP per molte piattaforme cloud condivise ovvero possibilità di invio mail lecite tra i clienti della stessa piattaforma)
- Attacco alle whitelist (previo OSINT)
  ed invio di mail con contenuto lecito ma ugualmente efficaci e meno individuabili.

Configurazione ottimale server di posta con sistema di filtraggio per la sicurezza.

- Posta in arrivo:

  (record MX puntano a Sistema di filtraggio) Sistema di filtraggio/Mail Gateway → Firewall → Server di posta

  Tutta la posta arriva sul Sistema di filtraggio/Mail Gateway
  Il server di posta per la ricezione della posta grazie al firewall intermedio accetta connessioni solo dagli indirizzi IP dal Sistema di filtraggio/Mail Gateway

  La parte webmail è protetta dalla CDN (sistemi tipo Cloudflare)

Configurazione ottimale server di posta con sistema di filtraggio per la sicurezza.

- Posta in uscita:

- Server di posta → Sistema di filtraggio/Mail Gateway

  Il sistema di filtraggio/Mail Gateway è in grado di isolare una casella compromessa da Virus

  Il pool di IP del servizio SMTP costantemente monitorato ed aggiornato del sistema di filtraggio/Mail Gateway
  permette al vostro dominio di non entrare in Black List Spam se compromesso.

Configurazione ottimale server di posta con sistema di filtraggio per la sicurezza.

- Configurazione DNS:

- SPF
- DKIM
- DMARC (con policy attivata e monitoraggio)
- MTA-STS (con monitoraggio)

Configurazione ottimale server di posta con sistema di filtraggio per la sicurezza.

- Configurazione 2FA:

- 2FA abilitata per accesso al sistema di filtraggio/mail gateway a tutti gli utenti e amministratori

- 2FA abilitata per accesso al server di posta a tutti gli utenti e amministratori e ad eventuali app.

Configurazione ottimale server di posta con sistema di filtraggio per la sicurezza.

- Configurazione sistema invio/ricezione:

- Richiede connessioni crittografate.
- Scelta delle versioni TLS supportate
- L'utente deve autenticarsi per spedire messaggi dal dominio locale
- Rigetta messaggi con indirizzi del dominio locale 'spoofed'
- Blocca indirizzi IP sospettati di 'password guessing'
- Blocca utenti che sono obiettivo di 'password guessing'
- Aggiornamenti/patch

Mail phishing weaponizing

- Tramite mail spoofing possiamo cercare di compromettere i processi aziendali semplicemente chiedendo a personale e stakeholders di intraprendere delle azioni (bonifici-giroconti-acquisti-vendite-appuntamento di un tecnico)
  In questo caso non utilizzeremo nessun allegato o link verso malware, quindi la possibilità di successo è molto alta e dipende dalla precisione dell'analisi e dalla perfezione grafica, l'attacco per essere maggiormente credibile può essere integrato da tecniche di Vishing e Smishing

(Consigliato in quanto i sistemi di sicurezza aziendali sono facilmente bypassabili)

Mail phishing weaponizing

- Esegui un attacco di spear-phishing con SET (Social Engineering Toolkit)
- Creare un malware che permetta di controllare il pc/esfiltrare files.

(Sconsigliato in quanto il malware si scontrerebbe con i sistemi di sicurezza aziendale)

Mail phishing weaponizing

- Links leciti per i sistemi di filtraggio da inserire all'interno delle mail
- Riprodurre un sito raggiungendolo tramite link ingannevole (dominio costruito come: dominioattaccante.com/nomedominioaziendale
- Scopo recuperare dati dell'utente dal sito falso oppure fargli caricare files sul sito falso.
- Muraena phishing tool
- https://github.com/muraenateam/muraena
  https://www.youtube.com/watch?v=glzq5yL8LCE


BONUS TRACK

Come sfruttare il bug typo su Exchange: La mail è lecita!

- Acquistare il dominio con i al posto della L
- Acquistare una più caselle di Exchange e configurarle come le e-mail originali es. nome.cognome@bertoidicibersecurity.com per spedire al dominio vero nome.cognome@bertoldicibersecurity.com
- Utilizzare la **I maiuscola = l minuscola** in Outlook al momento della composizione delle e-mail
- Assicurarsi che il destinatario utilizzi Exchange (sia che appartenga al dominio falsificato sia che appartenga agli stakeholders del proprietario del dominio falsificato)
- Configurare le nuove caselle per la massima deliverability controllare su https://www.mail-tester.com/

Ricerca dominio libero - Bug typo su Exchange: Exchange visualizza le lettere maiuscole! La partita potrebbe essere vinta

Bug Typo su Exchange: possibili controindicazioni

- Black list su sistemi di filtraggio
- Non funziona se chi riceve utilizza GMAIL / Google Workspace
- Individuabile trasponendo l’indirizzo su un foglio di Word e convertendo in «tutto minuscolo»

Ho trovato un problemino riguardo alle mail su iOS ma anche su Gmail e Samsung mail….

Ho trovato un problemino riguardo alle mail su iOS ma anche su Gmail e Samsung mail….

[11:30, 20/8/2022] GM: Ho trovato un problemino riguardo alle mail su iOS, Gmail per Android e Samsung Mail (forse anche altri? Immagino di si') che riguarda IMAP/POP3 e SMTP. Non succede su Outlook mobile (perche' non fa modificare le impostazioni)

[11:30, 20/8/2022] GM: Niente di serio, ma non saprei come valutarlo

[11:32, 20/8/2022] GM: Mi sono accorto che se cambio il server di destinazione non dimentica la password e quindi sono riuscito a leggerle proxando o sniffando.

[11:32, 20/8/2022] GM: Adesso, non e' il problema del secolo, ma in teoria quella password una volta inserita non dovresti piu' poterla leggere

[11:32, 20/8/2022] GM: E la modifica va un po' contro quello

[11:33, 20/8/2022] GM: E' una modifica manuale che va fatta nelle impostazioni, quindi niente di drammatico, pero' esiste

Ho trovato un problemino riguardo alle mail su iOS ma anche su Gmail e Samsung mail….

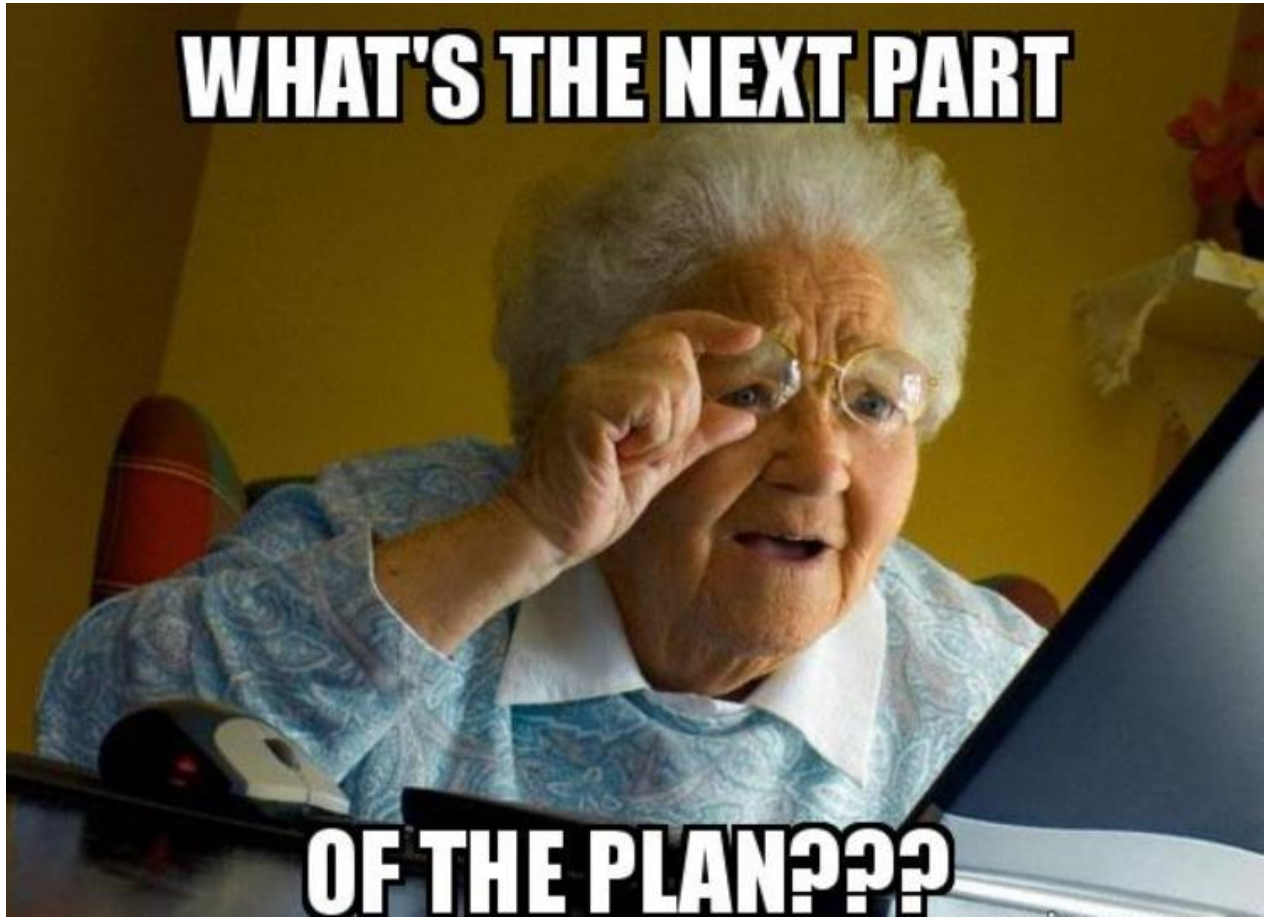
La 2FA non serve a nulla perche’ su IMAP passa la «Password dispositivo»

Ci vogliono meno di 30 secondi (cronometrati) per cambiare quell’impostazione

Si puo’ fare anche di peggio: si potrebbe costruire un proxy che si mette in tra il dispositivo e il server di destinazione, questo permetterebbe di alterare la posta che il dispositivo riceve e invia

Tutto questo indipendentemente da SSL/TLS.

Famoso provider di posta disclosure o responsible disclosure?



Famoso provider di posta disclosure o responsible disclosure?

PEC del 29/06/2022:

Gentilissimi,

volevo segnalarvi una problematica di sicurezza sull'erogazione del vostro servizio di posta elettronica.

Una volta autenticati al vostro servizio di posta elettronica con un qualsiasi vostro account (anche gratuito), si possono spedire e-mail "tecnicamente lecite" da parte di qualsiasi altro indirizzo XXXXXXXX o da parte di qualsiasi altro indirizzo appartenente a domini ospitati sul vostro servizio di posta, ovvero si ottiene una sorta di "open relay" per conto di tutti gli indirizzi presenti sul vostro servizio di posta ordinaria.

E' possibile sfruttare questa problematica di sicurezza semplicemente sostituendo il campo FROM del mittente sul client di posta che spedisce la mail, ove è stato configurato per l'invio un account appartenente al vostro servizio di posta.

Famoso provider di posta disclosure o responsible disclosure?

Ovviamente a causa del problema è possibile spedire e-mail tra domini diversi ospitati sul servizio di posta XXXXXXXX e da domini diversi ospitati sul servizio di posta XXXXXXXX, sia facendole girare sul server di posta XXXXXXXX che inviandole verso l'esterno.

Questa problematica apre imponenti problemi di sicurezza tra tutte le PA, PMI ed il loro fornitori di sicurezza che utilizzano il servizio di posta XXXXXXXX.

A mero titolo di esempio la classica e-mail che chiede alla segretaria del CEO di eseguire il bonifico, la classica e-mail che chiede ai tecnici l'accesso con TeamViewer a server / end point, ed infine l'email che in qualsivoglia modo attacchi i processi aziendali.

Famoso provider di posta disclosure o responsible disclosure?

Il problema presumo derivi dal fatto che sul servizio di posta XXXXXXXX non esiste una policy che stabilisce quanto segue:

L'utente deve autenticarsi per spedire messaggi da un dominio locale.

Il server di posta deve rigettare i messaggi con spoofed local domain sender identity tranne che per i seguenti oggetti ove consentiti per l'utente autenticato per i seguenti possibili casi:

I loro rispettivi indirizzi di posta di dominio.

Gli indirizzi dei gruppi di dominio di cui fanno parte.

Gli alias dei loro indirizzi.

Gli alias delle cartelle pubbliche di cui fanno parte.

Gli indirizzi degli utenti che gli hanno garantito delega.

Famoso provider di posta disclosure o responsible disclosure?

Ora anche ammesso che XXXXXXXX rilasci una DKIM diversa per ogni dominio, come fanno Microsoft365, Google Workspace, (funzionalità che al momento XXXXXXXX non prevede, vedi per poi bloccare lo spoofing con DMARC Policy; suppongo non risolverebbe il problema, perché nel momento in cui ci si presenta al server di posta con quello specifico campo FROM modificato credo che il server rilascerebbe la DKIM del dominio che legge nel campo FROM stesso, ovvero il problema sta a monte perché XXXXXXXX ha già autorizzato quello specifico utente.

Famoso provider di posta disclosure o responsible disclosure?

Inoltre (problema nel problema) non vengono eseguiti controlli all'atto della registrazione di un nuovo account XXXXXXXX, infatti è possibile registrare un account XXXXXXXX con dati falsi ad esempio provenienti da (https://www.fakenamegenerator.com), quindi un possibile attaccante utilizzando una VPN senza log per la registrazione rimarrebbe anonimo, ottenendo in seguito tramite la modifica del campo FROM la capacità di scrivere per conto di indirizzi che utilizzano il servizio di posta XXXXXXXX.

Cordialità

Alessandro Bertoldi

Grazie per l'attenzione!
Sono a vostra disposizione per domande e risposte