

**Tsurikichi Sanpei (il patito del phishing)**  
**[alessandro@bertoldicybersecurity.com](mailto:alessandro@bertoldicybersecurity.com)**

# 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.



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- [redacted] +39 011 [redacted]

[redacted]@intesasanpaolo.com

Follow Intesa Sanpaolo on:



[www.intesasanpaolo.com](http://www.intesasanpaolo.com)



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

# Se non otteniamo risposte dobbiamo verificare se la mail dei destinatari esistono

- 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](mailto:alice@domain1.com)
- RCPT TO:[bob@domain1.com](mailto:bob@domain1.com)

```
Prompt dei comandi
220 mailsrv.domain1.com ESMTP MAIL Service ready at DATE
helo domain1.com
250 mailsrv.domain1.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
```

# 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 ESMTF 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 ESMTF 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 ESMTF 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=FMA64jpvJowVimJSumIy40EyiIPhq6clsLHnBx14/vy=;
b=C0byicz8z513178n9M6Ty6ta1I9Xq0H07s+qYQPXqSAFRkuBdDttwk2iD/eEnO3+AJOJwTQ1
LGOwEV1Sdo/8dUd/1DFr9qqpHWjHwJzE1x0QLXdnIg/+ELqLhYwS6kne6aDuaOcEA1ldgIOHmGZ
KmhSpVEgys7J/8R+nKmxR1ID3iTT+W0N219IcFshv67NmV2RAS/ypPw+9r9w8Jf09r7P4GH7sdeZ
OPsG0KC5G44zV7HzUr+f+t1CcF/yPwMfzEa3Kmla0+QC+uRfDrWu9AgTo4Q8wrJrXHKRqgBkz4W
Y9L4uKcWzrDp0gm03YqG15V2kHA9gnJJ7gyw==;
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 InpnPs-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=vRkXFKy6f08/8UMwAueMdtLRnluovw0zQ25nCc2D13QimE0DyymIG0yR35Z30zYbyPEsz7E8TUSjR
SlqFTeZ4teQ041m61mJz41nU5kx0+bEmLLXuvjg6fgox1AeijY9h0kSc549svFNBM+aw4XePxEy74I
H03AH720+8X1kcsdRgHk0L5rVsc/pRv6nMNCYnZTNONTIKOqE6cEND15iJHTU7qA09KJngqW6D0pw
EkoMxyejQ10KFceiwq76z9dDeNfmJxm1a23pfxBES+tbrcQBkx7eQZY8uya+SAV/PVqOkkku4L6k8
ka85yubngnKZJaerBV4kmtuP2AV2+CA==
X-Footer: YmVydG9sZGljeWJlcnNlY3VyaXR5LmNvbQ==
Received: from localhost ([127.0.0.1])
by mail-de-01.intactmail.pro with ESMTFSA
for abertoldi@partner.clouditalia.com;
Sat, 14 May 2022 10:46:19 +0200
Date: Sat, 14 May 2022 10:46:18 +0200
Subject: Test
```

# 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)

# Consultazione DNS del dominio/i target il tool indispensabile



## MX Lookup

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

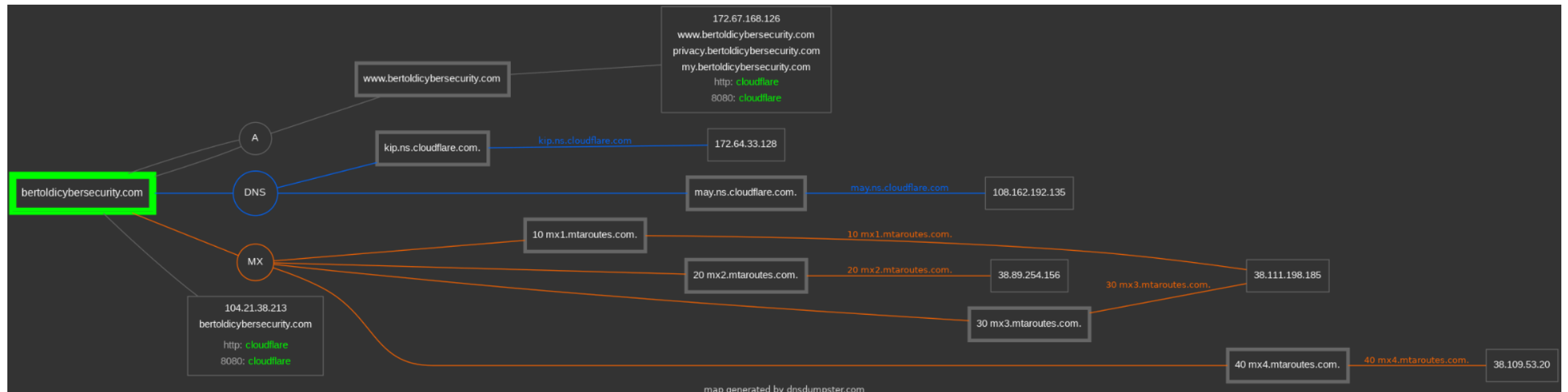
DKIM Lookup (Request for Comments: 6376 → Updated by: 8553, 8616 )

\* 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 )

# 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>



# 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 + - ~ ?



# 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.

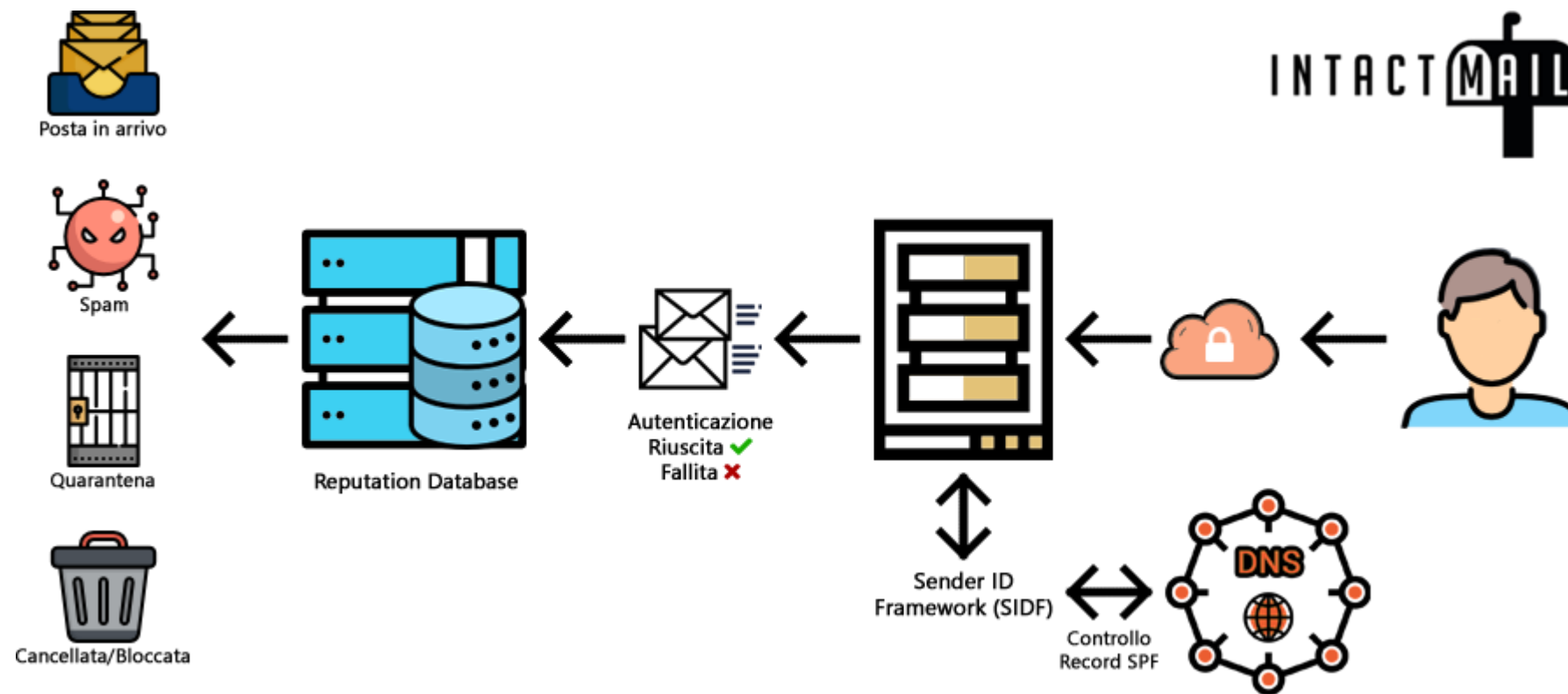
# Esempio di record DNS DMARC (Domain-based Message Authentication, Reporting & Conformance)

```
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:b929c56e0d  
9f086@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

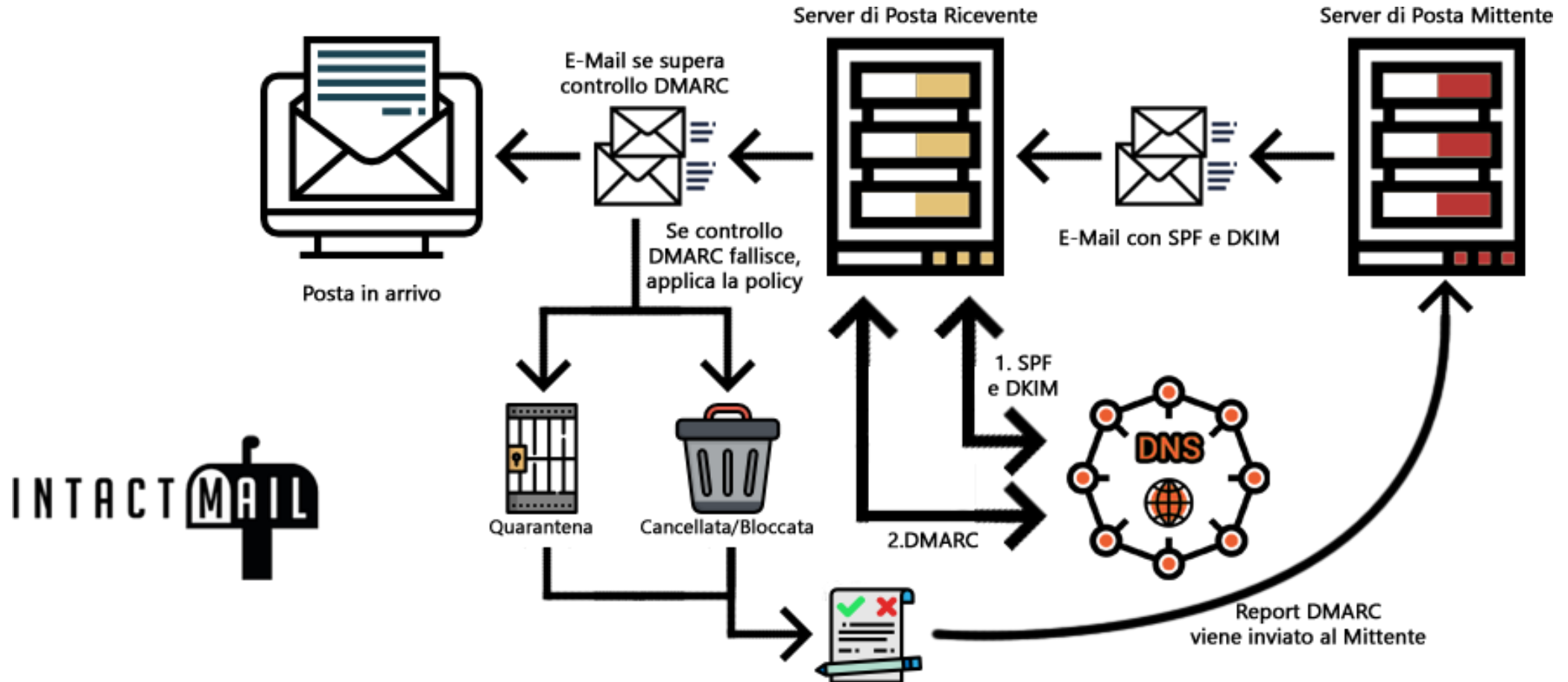
# Capire Sender Policy Framework (SPF)



# Capire DKIM



# 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=	<p>Può assumere uno dei seguenti valori:</p> <p><b>none</b> :Nessun avviso specifico sarà dato al server di posta di destinazione</p> <p><b>quarantine</b> :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</p> <p><b>reject</b> :Avvisa il server di posta di destinazione di rifiutare qualsiasi email che fallisce il test DKIM e/o SPF</p>	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 <b>non è</b> 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 omissso il valore di default sarà adkim=r. Specifica la “modalità di allineamento” per la firma DKIM.
aspf=	r (relaxed) oppure s (strict)	Valore opzionale, se il tag viene omissso 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	<p>Valore opzionale, definisce la percentuale di email alle quali le regole del DMARC sono applicate.</p> <p>Se il valore viene omissso il valore di default sarà pct=100, quindi tutte le email saranno sottoposte ai controlli DMARC.</p>
fo=	<p>Può assumere uno dei seguenti valori:</p> <p><b>0</b> : Genera il report al server di posta mittente se tutti i controlli falliscono.</p> <p>Se è utilizzata solo la DKIM come sistema di sicurezza ed il test DKIM fallisce, il report sarà inviato.</p> <p>Se è utilizzata solo l'SPF come sistema di sicurezza ed il test SPF fallisce, il report sarà inviato.</p> <p>Se sono utilizzati sia DKIM che SPF, e l'SPF fallisce ma il test DKIM passa il report <u>non sarà</u> inviato</p> <p><b>1</b> : Genera il report al server di posta mittente se almeno 1 controllo fallisce.</p> <p>Se è utilizzata solo la DKIM come sistema di sicurezza ed il test DKIM fallisce, il report sarà inviato.</p> <p>Se è utilizzata solo l'SPF come sistema di sicurezza ed il test SPF fallisce, il report sarà inviato.</p> <p>Se sono utilizzati sia DKIM che SPF, e l'SPF fallisce ma il test DKIM passa il report <u>sarà</u> inviato</p> <p><b>d</b> : Genera il report se il test DKIM fallisce</p> <p><b>s</b> : Genera il report se il test SPF fallisce</p>	<p>Valore opzionale, se il valore viene omissso il valore di default sarà fo=0.</p> <p>Definisce le regole per quando deve essere generato il report DMARC.</p>

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

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

# 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/>

# 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

# 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**<sup>TM</sup>

 **TREND**  
MICRO | Trend Micro Email Security

**N** **N-ABLE**<sup>TM</sup>  
SpamExperts<sup>TM</sup>

# 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.

 **BONUS TRACK** 

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

bertoidicybersecurity.com  [Vai al carrello](#)

**Dominio disponibile** Chiama il numero 800-790178 per acquistare l'assistenza

bertoidicybersecurity.com è disponibile

€ 0,99/anno ~~€ 24,57~~<sup>?</sup>

per il primo anno

Ecco perché è fantastico.

- ✓ "Cyber" è una parola chiave ad alto valore aggiunto con un prezzo medio di vendita pari a € 1.986,00.
- ✓ "Security" e "Cyber" sono due parole chiave molto utilizzate.
- ✓ Utilizza l'estensione .com.

[Aggiungi al carrello](#)

# 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](mailto:nome.cognome@bertoidicibersecurity.com) per spedire al dominio vero [nome.cognome@bertoidicibersecurity.com](mailto:nome.cognome@bertoidicibersecurity.com)
- Utilizzare la **I maiuscola = I 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/>



# 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»

Grazie per l'attenzione!

