LEGALTECH FORUM 2023
29 NOVEMBRE
Cappella Farnese | Bologna

Forenser
Digital Investigations

LEGALTECH FORUM 2023

I PROTOCOLLI DKIM, DMARC ED SPF

VANTAGGI PER LA DIGITAL FORENSICS E NEL CONTRASTO AGLI ATTACCHI DI TIPO MAN IN THE MAIL O BUSINESS EMAIL COMPROMISE

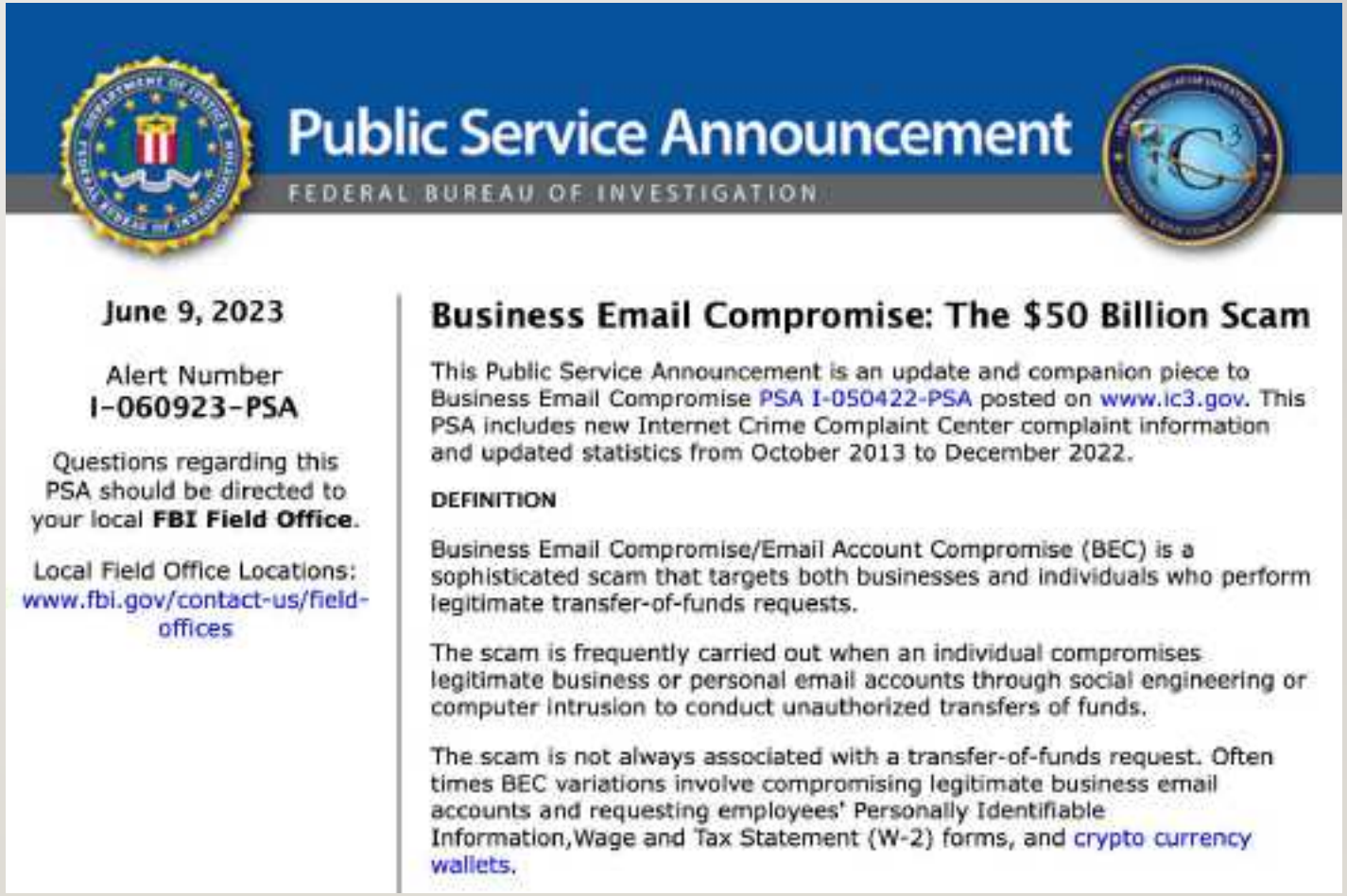
Paolo Dal Checco, Consulente Informatico Forense
Forenser Srl

CHI SONO

- Laurea e Ph.D. in Informatica, specializzazione Sicurezza Informatica, Università di Torino
- Consulente Informatico Forense (10+ anni, 2k+ casi)
- CTP, informatico, CTU informatico, Esperto d'Informatica Forense, Perito del Giudice, CT del PM, Ausiliario di PG, Iscritto all'Albo dei CTU e dei Periti del Tribunale di Torino
- Collaborazioni di docenza a contratto con UniTO (Corso Sicurezza Informatica @SUISS), UniGE (Master), UniMI e PoliMI (Master e Corsi di Perfezionamento)
- Socio ONIF, IISFA, CLUSIT, etc…
- Interessi in mobile forensics, OSINT, cryptocurrency forensics, web forensics…. in sostanza tutti gli aspetti della digital forensics

MAN IN THE MAIL

- Diversi sinonimi:
- BEC / Business Email Compromise
- MiTM / Man in The Mail
- WTF / Wire Transfer Fraud
  (l'acronimo non è dei più riusciti 😅)
- PRT / Payment Redirection Fraud
- ATF / Account Takeover Fraud
- Truffa dei bonifici, redirezione dei pagamenti, truffa dei falsi IBAN, frode delle false fatture



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

June 9, 2023

Alert Number
I-060923-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations: www.fbi.gov/contact-us/field-offices

Business Email Compromise: The $50 Billion Scam

This Public Service Announcement is an update and companion piece to Business Email Compromise PSA I-050422-PSA posted on www.ic3.gov. This PSA includes new Internet Crime Complaint Center complaint information and updated statistics from October 2013 to December 2022.

DEFINITION

Business Email Compromise/Email Account Compromise (BEC) is a sophisticated scam that targets both businesses and individuals who perform legitimate transfer-of-funds requests.

The scam is frequently carried out when an individual compromises legitimate business or personal email accounts through social engineering or computer intrusion to conduct unauthorized transfers of funds.

The scam is not always associated with a transfer-of-funds request. Often times BEC variations involve compromising legitimate business email accounts and requesting employees' Personally Identifiable Information, Wage and Tax Statement (W-2) forms, and crypto currency wallets.

https://www.ic3.gov/Media/Y2023/PSA230609

I protocolli DKIM, DMARC ed SPF: vantaggi per la digital forensics e nel contrasto agli attacchi di tipo Man in The Mail o Business Email Compromise

IN ITALIA ABBIAMO LA FATTURAZIONE ELETTRONICA…

- Si pensava che la **fatturazione elettronica** potesse fermare questo tipo di truffa (le fatture elettroniche arrivano direttamente nel **cassetto fiscale**, molto più difficili da alterare)
- Ci sono però i PDF delle **fatture di cortesia**…
- Spesso le aziende **dispongono il bonifico** avuta visione del PDF di cortesia ricevuto via email, senza verificare l'IBAN inserito nelle fatture sullo SDI

PREVENZIONE DEGLI ATTACCHI DI TIPO MAN IN THE MAIL

- Attenzione ai **cambi di IBAN** da parte dei fornitori già in essere
- Certificare IBAN (firma digitale, PEC, etc…) dei **nuovi fornitori**
- Attendere **fattura elettronica** (ma con le pro forma?)
- Fare una **telefonata** (attenzione, non è sufficiente riceverla)
- Sistemi di rilevamento Email Spoofing/SPAM (inutile se mail inviate da account fornitore)
- Utilizzo di protocolli **DKIM/DMARC/SPF** (protegge la **controparte** ma permette a entrambi **indagine forense**)

ANALISI FORENSE SU ATTACCHI DI TIPO MAN IN THE MAIL

- **Raccogliere email ricevute e inviate**, da entrambe le parti, anche da indirizzi simili a quelli corretti, partendo da prima della truffa e terminando qualche giorno dopo
- Ricostruire un **sequence diagram** degli eventi
- Verificare le firme **DKIM** delle mail ricevute
- Verificare se le mail ricevute sono coerenti con i **record SPF**
- Questione di **accountability**: anche se l'account «bucato» è quello di controparte, è importante essere comunque conformi alle best practice di sicurezza

SPF

- **SPF / Sendr Policy Framework**
- Protocollo utilizzato per autenticare chi è autorizzato a inviare mail per un particolare dominio
- Nei record TXT del DNS del dominio vengono indicati gli IP/DNS di chi è autorizzato a inviare email
- L'ultima parte indica la «policy», cioè cosa deve fare un server che riceve una mail NON proveniente dagli indirizzi autorizzati
- Concepito come sistema antispam, può essere utile nelle attività di perizia informatica su messaggi di posta elettronica

```
$ dig -t txt forenser.it | grep spf


forenser.it.      3552    IN
      TXT    "v=spf1
include:spf.protection.outlook
.com
include:spf.sendinblue.com mx
-all"
```

DKIM

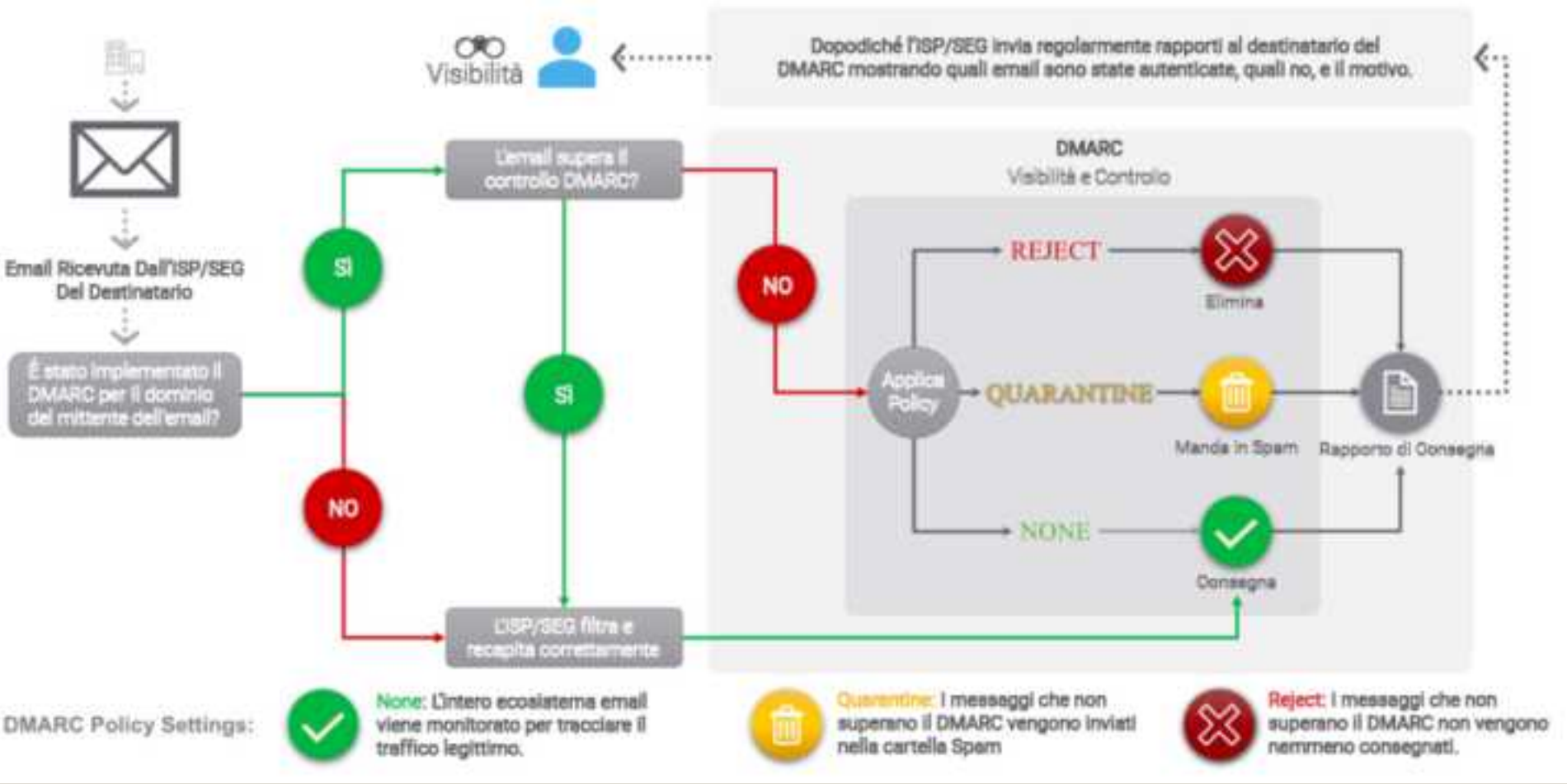
- **DKIM / DomainKeys Identified Mails**
- Protocollo utilizzato per autenticare i messaggi in base a firme digitali applicate dal server d'invio delle mail
- Può risultare utile per analisi forense delle mail
- Le firme vengono fatte con chiavi private note solo ai server
- Le chiavi pubbliche vengono memorizzate in record DNS pubblicamente accessibili e verificabili
- DKIM firma il body (testo) oltre ad altri specifici campi dell'header che possono variare

```
DKIM-Signature: v=1; a=rsa-sha256;
c=relaxed/relaxed; d=forenser.it; s=selector1;
h=From:Date:Subject:Message-ID:Content-
Type:MIME-Version:X-MS-Exchange-
SenderADCheck;
bh=wM8VFsk8X2PGjM2bsDpgcI7KZUd7YpC
WuByNBdpzI5Q=;
b=etK58y/2F9bw1q6jhZGo+zTp1FQ1Vwuhw
QWy3K01E8Dugxy3UAdqLeuBRkhLmd1gm0a
hx0g4x8ANzkJWgUt6Goc9I8bUXflBl0/JD0pCf
N4jqji0j9Hqp33gPTl+nl2AuQF0gLNj2LS[…]lE
oG+RqbiORTxwpfdw2pfuGqHeYXYogWznSO
m+OkWrg==
```

DMARC

- **DMARC / Domain-based Message Authentication, Reporting and Conformance**
- Protocollo utilizzato per autenticare i messaggi e verificare se si tratti invece di spoofing
- Fa uso dei protocolli SPF e DKIM per valutare la bontà di un messaggio
- Permettere al ricevente di scartare i messaggio
- Con l'opzione 'RUA' (Reporting URI for Aggregate) i destinatari informano il mittente dello scarto
- Con opzione 'RUF' (Reporting URI for Forensic data) il destinatario inviare al mittente «**report forensi**» dell'evento (per capire se si tratta di semplice spam, spear phishing, spam massivo, etc…)

DMARC: COME FUNZIONA

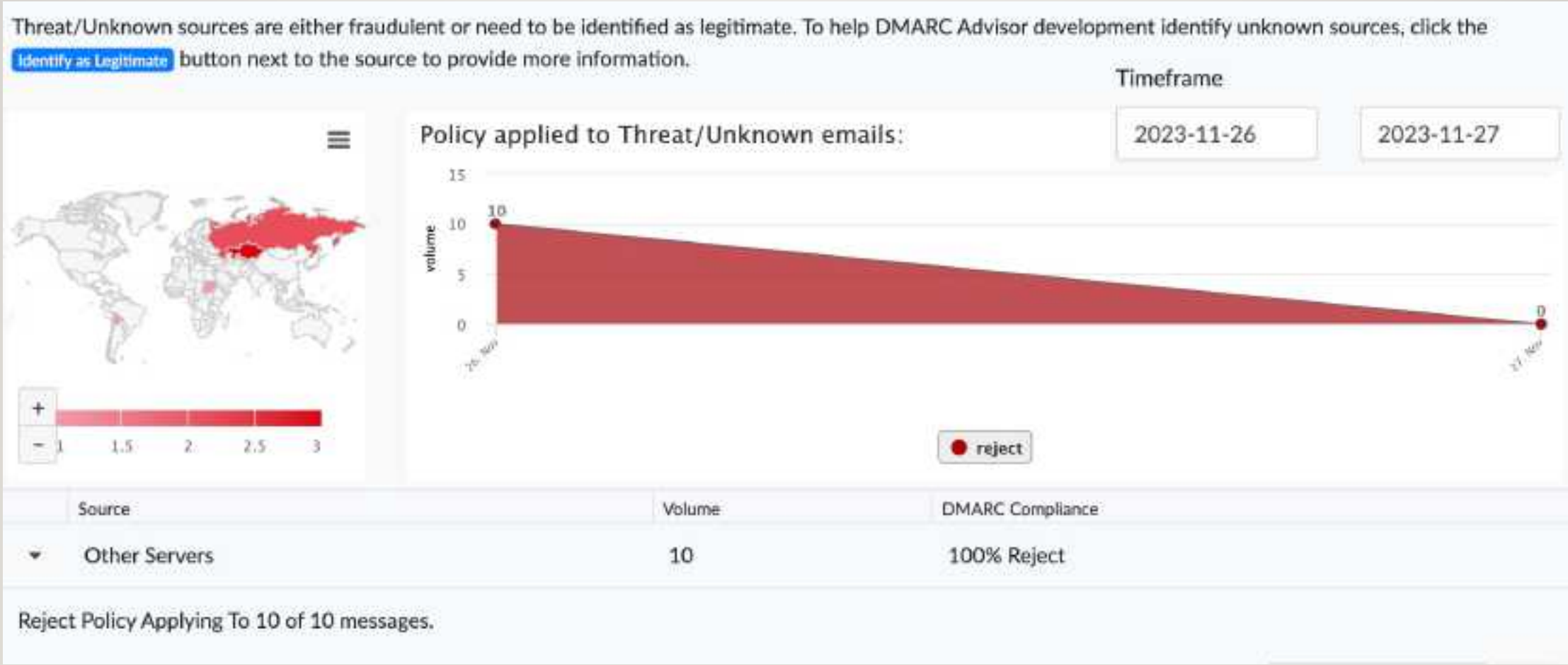


https://www.proofpoint.com

DMARC: ESEMPIO PRATICO

https://dmarcadvisor.com

DMARC: ESEMPIO PRATICO



https://dmarcadvisor.com

DMARC: ESEMPIO PRATICO

	Server Name	From: domain count	Message count	IP count	Compliance
▾	nxdomain	1	9	8	0% (SPF: 0%, DKIM: 0%)

Column meanings | 15 of 18 Columns Visi

From: Domain	IP	PTR	Country	Messages	Policy Applied	Override Reason	DKIM DMARC	DKIM Raw	DKIM d=	DKIM Selectors	SPF DMARC	SPF Raw	SPF Domain	Reporter
dalchecco.it	[illegible]	nxdomain		2	Reject	none	fail	none	none		fail	fail	dalchecco.it	google.com
dalchecco.it	[illegible]	nxdomain		1	Reject	none	fail	none	none		fail	fail	dalchecco.it	google.com
dalchecco.it	[illegible]	nxdomain		1	Reject	none	fail	none	none		fail	fail	dalchecco.it	google.com
dalchecco.it	[illegible]	nxdomain		1	Reject	none	fail	none	none		fail	fail	dalchecco.it	google.com
dalchecco.it	[illegible]	nxdomain		1	Reject	none	fail	none	none		fail	fail	dalchecco.it	google.com
dalchecco.it	[illegible]	nxdomain		1	Reject	none	fail	none	none		fail	fail	dalchecco.it	google.com
dalchecco.it	[illegible]	nxdomain		1	Reject	none	fail	none	none		fail	fail	dalchecco.it	google.com
dalchecco.it	[illegible]	nxdomain		1	Reject	none	fail	none	none		fail	fail	dalchecco.it	google.com

https://dmarcadvisor.com

CONCLUSIONI

- In **fase d'indagine**, DMARC, DKIM + SPF forniscono al ricevente uno strumento per autenticare, le mail inviate da controparte e verificare se sono originali o 'spoofed', così da poter redigere una **perizia informatica forense** che descriva le modalità di attacco e, possibilmente, i dettagli di quale casella di posta elettronica è stata compromessa
- Allo stesso modo, possono aiutare a **prevenire gli attacchi** nel senso che chi li implementa evita che terzi impersonino il proprio account e possano quindi truffare eventuali controparti (utile anche per questioni di **accountability**, si pensi al GDPR o D.Lgs. 231/2001 che prevede analisi e valutazione del rischio e opportune contromisure)