



Janusmail Manuale utente

Revisionato il 30/12/2019

Versione 2.4.0

DASHBOARD

La Dashboard di Janusmail permette agli utenti di accedere all'elenco delle email spedite e ricevute, visualizzare lo stato di consegna, rilasciarle se sono state bloccate per spam e richiedere agli amministratori il rilascio di email erroneamente bloccate in quanto reputate pericolose.

Gli amministratori possono visualizzare alcune funzioni aggiuntive che verranno descritte in seguito.

Si può accedere alla dashboard direttamente all'indirizzo inviato nella email di benvenuto, dall'opzione Antispam della barra di Zimbra:



o da menu di Microsoft Office 365/Exchange on-line, selezionando l'opzione Janusmail:



Al primo accesso è necessario autenticarsi utilizzando l'account usato per accedere alla propria casella di posta:

UserName			
type text			
Password			
type password			
Remember/Rico Forgot your passw	rda ord?/Passw	ord dimenticata	?

Spuntando la casella "Remember/Ricorda", al prossimo accesso da rete sicura, si accede direttamente alla dashboard senza che venga richiesta l'autenticazione.

Se non ricordate/conoscete la password di accesso potete cliccare su "Forgot your password/Password dimenticata?", vi verrà richiesta la vostra email e dopo aver spuntato la casella "Non sono un robot"

tyne text		
N	on sono un robot	C
	P	reCAPTCHA rivacy - Termini

vi verrà inviata una email per impostare una nuova password:



Hai ricevuto questa email in quanto hai richiesto un cambio password. Per impostare una password alternativa , premi il tasto seguente.

Imposta

	ina pas	sword	
alternativ	a		
Indica indirizzo er	nail per confe	erma	
type text			
Indica la passwore	d <mark>al</mark> ternativa		
type password			

Inserite l'indirizzo email per conferma e una password alternativa.

Successivamente potete accedere alla dashboard con questa password alternativa.

Edit		×
Customer ID:	BLS Consulting	
Domain*:	bls.it 🔻	
User		
Language*:	Italian 🔻	
	172.30	
	192.168	
Cookie Ipaddress: 🌸		

Le reti sicure si configurano nelle preferenze dei domini/Cookie IP address:

In questo esempio saranno considerati reti sicure quelle che hanno indirizzi che iniziano per 172.30 e 192.168

Prima di entrare nella dashboard verranno visualizzate eventuali novità.

Novità:

restyling della dashboard.

La nuova dashboard permette accedere in modo più semplice alle varie funzioni di Janusmail.

Spuntando l'apposita casella a fine pagina è possibile evitare che vengano visualizzate:

Non visualizzare questa pagina la prossima volta che entri

Chiudi



Nella parte alta della dashboard sono visualizzati il menù funzioni, i campi di ricerca e le icone per accedere alle varie funzioni descritte in seguito.

I Campi per Ricerca permettono di eseguire la ricerca da data a data e corrispondenza perfetta di termini in destinatario, mittente ed oggetto.

Per corrispondenza perfetta di termini si intende che se il mittente è mrossi@dominio.com e si cerca rossi non verrà trovato, mentre se si cerca mrossi, oppure dominio oppure com verrà trovato.

Quindi, inserendo un termine completo esatto, verranno visualizzate tutte le email che contengono tale termine nel destinatario/i, nel mittente o nell'oggetto.

Una volta impostati i parametri di ricerca, premere l'icona 🔍 per avviare la ricerca, cliccando invece sull'icona 🔍 verranno visualizzati i parametri avanzati di ricerca (funzione descritta in seguito)

Due ulteriori opzioni permettono di velocizzare le ricerche:

🗷 Solo email personali 🔲 Solo da rilasciare

Solo email personali: presente solo per gli amministratori, permette di visualizzare solo le email dell'amministratore stesso

Solo da rilasciare: se spuntata visualizza solo le email che possono essere rilasciate

Le icone 🧭 ? 😯 🃢 🌣

permettono accedere nell'ordine alle seguenti funzioni:

- report antispam: verrà visualizzato il report delle email bloccate da Janusmail

М

- guida utente: guida rapida alle principali funzioni della dashboard

Δ

- manuale: manuale completo di Janusmail
- news: ultime novità di Janusmail
- preferenze: permette all'utente impostare alcuni parametri di configurazione
- notifiche: visualizzazione delle notifiche di eventuali email infette o di phishing che per errore sono state consegnate
- logout: permette uscire dalla dashboard

L'icona 🗰 in alto a sinistra permette accedere al menù delle funzioni, le funzioni visualizzate dipendono dal tipo di utente che accede alla dashboard.

Esempio di menù per utente base con opzione di massmailing:

	1 1 1-1 01/10/2010	20/12/2010 m cerce
	Configurazione	Preferenze
	Massmailing	Account Esterni
-	datalora	mittente

Esempio di menù per amministratore:



Le singole funzioni verranno descritte in seguito in questo manuale.

RICERCA AVANZATA

Per attivarla, cliccare sull'icona a forma di lente di ingrandimento con un "+".

Cliccando l'icona, compariranno i campi aggiuntivi di ricerca, una volta inseriti i parametri cliccare sulla lente di ingrandimento per effettuare la ricerca.

	Janusmail	dal: 25/12/2019	🟛 al: 30/12/2019	🛍 cerca	Q Q	
mittente:			destinatario:		oggetto:	
id email:			messaggio antivirus:			
Tipo emai	іі: 🔲 ок 💻	news 🔲 spam 🔲 vir	us 📕 scam 📕 blacklisted 🛽	whitelisted 🔲 policy blo	ocked 📕 delayed	
Stato ema	all: 📃 delive	red 🛄 quarantine 💻	delivery problems 💻 release	ed		

modalità di ricerca non lavora per termini esatti, bensì per parole o porzioni di esse contenute nei campi di ricerca.

Riprendendo l'esempio di prima, se il mittente della email è <u>mrossi@dominio.it</u> e si inserisce ad es. nel campo di ricerca mittente la parola "mrossi", "rossi", "mross", "mrossi" o "ssi@dom", l'email verrà trovata. Nell'esempio seguente si può vedere come, impostando "Bounc" come termine di ricerca nel campo oggetto, compaiano tutti i risultati includenti quella serie di caratteri senza per forza combaciare precisamente, nell'esempio "Bounc".

iii Janusmai	dal: 01/10/2019	🛍 al: 30/12/2019	cerca		QQ	2 🕄	∂ † 4 ¢ 1
mittente:		destinatario:		oggetto: Bounc			
id email:		messaggio antivirus:					
Tipo email: 🛛 🔲 OK	🗖 news 🔲 spam 🔲 v	virus 🔲 scam 🔲 blacklisted	I 🔲 whitelisted 🔲 policy blo	cked 🔲 delayed			
Stato email: 🛛 🔲 del	ivered 🔲 quarantine 🛽	📕 delivery problems 🔲 relea	ased				
Email inviate:	💿 ок 💿 🧲	POLICY 0					
Email Ricevute:	ОК 0	NEW5 0 SPAM 2			BLACK 0 POLICY 0	CE DELAYED 0 SC	olo da rilasciare
	data/ora mittent	te	destinatari	C	oggetto	stato	opzioni
	17/11/2019 00:24:17 jacqalo	n41aoze@gmail.com	mbruse@bls.it	ir b	ncrease SEO&Alexa Ranks with 1% oounce rate traffic	quarantine	<u>zi k</u>

Spuntando una o più caselle "Tipo email" verranno visualizzate le email di tale tipo, Spuntando una o più caselle "Stato email" verranno visualizzate le email filtrate per stato di consegna.

Inserendo l'ID esatto della email nel campo omonimo si potrà cercare una specifica email. Tale valore è recuperabile dal header della email:

X-Mrelayin-QIDOUT: x26C1GFU030514 (email ricevuta)

X-Mrelayout-INQID: x25GpZ90065114 (email spedita)

Gli header delle email sono visualizzabili con la funzione "Mostra originale" o similare del proprio client di posta.

ELENCO EMAIL RICEVUTE/INVIATE

Nella zona centrale della dashboard vengono visualizzate le email spedite e ricevute e che soddisfano gli eventuali parametri di ricerca impostati.

	data/ora	mittente	destinatari	oggetto	stato	opzioni
SPAM	06/03/2019 13:47:36	return-3-console_hercu_e1826-3833234- 02d6fb=2@bounce3.ilconsumo.com	info@bls.it	Sino a 700⬠di sconto per festeggiare il 25mo compleanno di Materassi Fabricatore	quarantine	<u>× 4 4</u>
	06/03/2019 13:47:36	jeffreyharris@webiar.net.br	info@bls.it	What are your plans for tomorrow?	quarantine	× 4 4
SCAM	06/03/2019 13:41:27	markwright@neweramsr.com.au	mbruse@bls.it	Ho davvero bisogno di aiuto	quarantine	× 4 4
ОК	06/03/2019 13:40:59	newsletter@mailant.it	info@bls.it	Fino al 10 marzo -52% sul listino	delivered	×
NEWS	06/03/2019 13:36:15	bounce- back.mnid2m.3577.34573818.4249.0.399455	mbruse@bls.it	Manovra 2019: novità per le imprese. Scopri lâAgenda della conferenza	quarantine	× 4 4

A inizio riga è presente una casella per selezionare l'email, dopo averle selezionate sarà possibile rilasciarle tutte insieme cliccando sul pulsante "Rilascia" a fine pagina o segnalarle come spam cliccando sul pulsante "Segnala spam" a fine pagina.

Si possono evidenziare email classificate come spam, news, scam, virus, delayed e rilasciarle o email ok o delayed e segnalarle come spam, il numero tra parentesi indica quante email verranno rilasciate o segnalqte come spam.

L'ultima riga permette rilasciare o segnalare come spam le emai spuntate (casella a sinistra di ogni email). Sono anche presenti le icone per muoversi tra le pagine.

Nella dashboard vengono visualizzate solo le ultime 2000 email che rispettano i parametri di ricerca, un apposito messaggio avvisa se ci sono più di 2000 email.

Se le email ricercate non vengono visualizzate perchè oltre le 2000 email affinare i parametri di ricerca.



Rilascio Mail

In base alla classificazione delle email (spam, virus, policy blocked, ecc.) verranno visualizzate delle opzioni specifiche in fondo alla riga dell'email.

<u>Spam e nev</u>	<u>vsletter</u>					
	10/03/2019 17:52:33	douglastaylor@alsamier.ae	info@bls.it	puoi alutarmi?	quarantine	2 4 A
NEWS	10/03/2019 14:53:10	biblioteca@legislazionetecnica.it	mbruse@bls.it	Catasto fabbricati, strumenti per il tecnico e omaggio	quarantine	<u> 14 14</u>

Per le email ricevute classificate come spam o come newsletter ("bulk email") sono visualizzate le icone:

- rilascia email: entro pochi minuti l'email viene rilasciata dalla quarantena e recapitata al/ai destinatari
- **aggiunta in whitelist**: l'aggiunta in whitelist comporta che una successiva email proveniente dallo stesso mittente e destinata allo stesso destinatario verrà consegnata e non più bloccata, inoltre anche le email provenienti dal dominio del mittente verranno recapitate
- whitelist by example: gli amministratori possono impostare delle whitelist con più flessibilità prendendo ad esempio una email bloccata e definendo i parametri che permettono di identificare le email da non bloccare:

Questa funzionalità permette cr Selezionare i criteri e i valori da	eare una whitelist prendendo questa email come esempio. Laggiungere alla regola:
Mittente:	
Destinatario:	info@bls.it
Oggetto:	BONUS
server sorgente	
ip server sorgente:	
	Aggiungi regola 🙆 Chiudi

Questa regola varrà se il destinatario è info@bls.it e contemporaneamente l'oggetto contiene la parola BONUS.

Aggiunta a Whitelist

Policy blocked

	16/02/2019 20:19:39	imekeylajuku98@o2.pl	bafors@inbox.ru	Invio richiesta fattura	quarantine	X
--	------------------------	----------------------	-----------------	-------------------------	------------	---

Per le email ricevute classificate come policy blocked (ad es. allegati pericolosi) è visualizzata l'icona richiedi rilascio: l'utente non ha diritto di rilasciare in autonomia l'email, ma può richiedere agli amministratori (del cliente, di dominio o del cluster) di analizzare l'email, verificare che non costituisce pericolo e quindi rilasciarla. Viene richiesto all'utente se conosce il mittente e sta aspettando l'email, queste informazioni vengono passate all'amministratore per aiutarlo a prendere una decisione.

Scam o virus



Per le email ricevute classificate come scam (ad es. email di phishing, truffa o in generale pericolose ma senza virus) o virus (contenenti allegati pericolosi con virus, ransomware, trojan o in generale segnalati pericolosi) è visualizzata l'icona richiedi rilascio: l'utente non ha diritto di rilasciare in autonomia l'email, ma può richiedere agli amministratori del cluster di analizzare l'email, verificare che non costituisce pericolo e quindi rilasciarla. Viene richiesto all'utente se conosce il mittente e sta aspettando l'email, queste informazioni vengono passate all'amministratore per aiutarlo a prendere una decisione.



16/118

Per le email ricevute classificate come OK (quindi non bloccate) è visualizzata l'icona segnala come spam: in questo caso il sistema analizzerà l'email e utilizzer Segnala Spam le informazioni per contribuire a bloccare in futuro eventuali email simili.

Se è attivo il modulo Zimbra Advanced verrà richiesto:



Vuoi spostare l'email in posta indesiderata nelle caselle a cui è già stata consegnata?



Premendo su Si l'email già consegnata verrà spostata nella cartella posta insesiderata.



Per le email ricevute e su cui ha agito una whitelist sarà possibile rimuovere dalla whitelist cliccando sull'icona corrispondente.

BARRA CONTEGGIO EMAIL

La barra conteggio email è presente nella parte alta della schermata principale, le email sono raggruppate a seconda della tipologia.

Email inviate: OK 101	POLICY 0 Email Ricevute:	OK 147 📄	NEWS 166 SPAM 168	VIRUS 32 SCAN	1 734 WHITE 653		
-----------------------	--------------------------	----------	-------------------	---------------	------------------------	--	--

A sinistra, ci sono le EMAIL INVIATE, raggruppate in:

- "OK": le email correttamente spedite
- "Policy Blocked": email bloccate per policy

A destra, le EMAIL RICEVUTE sono raggruppate in:

- "OK": email ricevute e che hanno passato tutti i controlli
- "News": le newsletter
- "SPAM": email bloccate in quanto ritenute Spam
- "Virus": email bloccate perché risultate positive ai controlli Antivirus e Anti-malware
- "Scam": email bloccate in quanto considerate tentativi di truffa o phishing
- "Whitelisted": le email lasciate passare perché incluse in una Whitelist
- "Blacklisted": email bloccate perché presenti nelle Blacklist
- "Policy Blocked": email bloccate perché risultate positive ai filtri di Policy

Cliccando su una tipologia di email, nell'elenco compariranno le email presenti in quel gruppo.

Nell'esempio seguente è stato cliccato il pulsante SPAM:

 Janusmail	dal: 01/10/2019	前 al: 30/12/2019 前 cerca	QQ
Email inviate:	💿 ОК 101 🧧	POLICY 0 Email Ricevute: OK 147 NEWS 166	SPAM 168
	data/ora	mittente	destinatari
SPAM	30/11/2019 23:51:22	swell@fooljob.icu	mbruse@bls.it
SPAM	30/11/2019 23:50:26	bake@fooljob.icu	assistenza@bl
	30/11/2019 21:44:43	theory@blacksbrave.icu	acquisti@bls.it

Dall'elenco di email presente nella DASHBOARD si possono selezionare le singole email inviate o ricevute, ottenendo una schermata che fornisce dettagli sull'invio/ricezione, sul percorso, sul mittente e destinatario e sui test effettuati dal sistema.

Dettaglio mail								×		
Ricevuta il	18/05/2019 05:21:3	36		Ricevuta dal			bls-DC-mrelayin04			
ID	x4I3La3o023628			Id interno			x4I3LUZ0023590			
Message ID	20190517202124.523480BB6BC76E00@mail.ru Dimensione						919265 Byte			
Mittente	sampsonyuritzo2@)mail.ru		Mittente origin	nale		sampsonyuritzo2@mail.ru			
Destinatario	assistenza@bls.it			Oggetto			BANK DETAILS INCOMPLETE FOR	PAYMENT		
Stato	quarantine			Risultato anal	isi		virus_malware - Infected (Metadefend	ler.)		
Risultato dei filtri										
Processore	Тіро	Esito	Dettaglio							
clamav	antivirus	clean								
sophos	antivirus	clean								
metadefender	multi-antivirus	infected	attach=IBAN DETAILS	i.iso - result=						
reputationcheck	sender ip resolution	fail	reverse resolution of 2	3.106.123.138 failed, error: NXDOMA	IN					
reputationcheck	SPF	fail	SPF result=softfail - al	ignment=yes (from.d=mail.ru, heade	r from.d=ma	il.ru, rr from.d=)				
reputationcheck	DKIM	not signed								
reputationcheck	DMARC	fail	DMARC policy=reject -	- action=reject						
reputationcheck	sender ip reputation	normal	confidence=0.247104 p	probability=-0.0909091 produce good	messages					
reputationcheck	country	located	coordinates=[103.8000	0, 1.3667] - countrycode=SG						
reputationcheck	reputation index	dangerous	weight=-13							
spamcheck	classify	scam	scam-phishing							
Destinatari										
Username					Dominio					
assistenza@bls.it					bls.it					
Stato invio										
Data/ora	Destinatario			Server d'inoltro		Dsn	Stato	Esito		
18/05/2019 05:21:36	9 05:21:36 assistenza@bls.it						quarantined			
				Richiedi lo	ng 🙆 E	isci				

La sezione DETTAGLIO MAIL si trova nella parte alta della schermata, visualizza un riepilogo delle informazioni riguardanti l'email:

- Ora, server che ha ricevuto l'email (mailrelay) e indirizzo IP/server da cui è stata ricevuta
- ID dell'email
- Mittente, ovvero il campo "From" dell'email
- Mittente Originale, ovvero chi è effettivamente il mittente della email, che per una email inoltrata indica il reale mittente.
- Destinatario o destinatari delle email
- Oggetto
- Stato di consegna
- Risultato analisi

Dettaglio mail				×
Ricevuta il	18/05/2019 05:21:36	Ricevuta dal	bls-DC-mrelayin04	
ID	x4I3La3o023628	ld interno	x4I3LUZ0023590	
Message ID	20190517202124.523480BB6BC76E00@mail.ru	Dimensione	919265 Byte	
Mittente	sampsonyuritzo2@mail.ru	Mittente originale	sampsonyuritzo2@mail.ru	
Destinatario	assistenza@bls.it	Oggetto	BANK DETAILS INCOMPLETE FOR PAYMENT	
Stato	quarantine	Risultato analisi	virus_malware - Infected (Metadefender.)	

Successivamente viene visualizzata la sezione risultato dei filtri:

Risultato dei filtri			
Processore	Тіро	Esito	Dettaglio
clamav	antivirus	clean	
sophos	antivirus	clean	
metadefender	multi-antivirus	infected	attach=IBAN DETAILS.iso - result=
reputationcheck	sender ip resolution	fail	reverse resolution of 23.106.123.138 failed, error: NXDOMAIN
reputationcheck	SPF	fail	SPF result=softfail - alignment=yes (from.d=mail.ru, header from.d=mail.ru, rr from.d=)
reputationcheck	DKIM	not signed	
reputationcheck	DMARC	fail	DMARC policy=reject - action=reject
reputationcheck	sender ip reputation	normal	confidence=0.247104 probability=-0.0909091 produce good messages
reputationcheck	country	located	coordinates=[103.8000, 1.3667] - countrycode=SG
reputationcheck	reputation index	dangerous	weight=-13
spamcheck	classify	scam	scam-phishing

Questa sezione dettaglia le analisi effettuate sull'email e il relativo esito, Janusmail applica numerose ottimizzazioni, quindi non tutte le analisi vengono fatte su tutte le email, ma solo quelle necessarie. Ad es. se una email è già stata classificata come infetta non verranno effettuati tutti i controlli antispam.

La prima colonna indica quale **processore** (o sottosistema) ha eseguito l'analisi, sono implementati i seguenti processori:

- clamav: antivirus in grado di identificare email contenenti malware, email di spam o di scam
- sophos: antivirus secondario utilizzato se si dispone della relativa licenza e se clamav non ha identificato come infetta l'email
- metadefender: multi-antivirus che analizza i singoli allegati utilizzando gli antivirus **ESET, Total Defense, Bitdefender** e **K7**, utilizzato se attivata la funzionalità Advanced security, se presenti allegati e se clamav e sophos non hanno identificato come infetta l'email

- attach check: sistemi di analisi degli allegati, in particolare sono implementati i seguenti controlli:
 - identificazione degli allegati pericolosi (eseguibili o ad alto rischio) mediante estensione del file o tipologia di file (mime-type) in base a quanto definito nella policy allegati pericolosi (vedere per i dettagli il prossimo capitolo)
 - identificazione degli allegati pericolosi mediante un database degli hash come illustrato in seguito in questo stesso capitolo, utilizzato se attivata la funzionalità Advanced security,
 - o identificazione dei pdf pericolosi, utilizzato se attivata la funzionalità Advanced security,
 - o identificazione dei documenti office pericolosi, utilizzato se attivata la funzionalità Advanced security,
 - identificazione dei documenti pdf o office criptati
- url check: sistemi di analisi del rischio degli URL presenti nella email come illustrato di seguito in questo capitolo, utilizzato se attivata la funzionalità Advanced security,
- reputation check: sistemi di analisi della reputazione del server mittente mediante i seguenti controlli:
 - \circ $\$ analisi della risoluzione dell'indirizzo ip del server mittente
 - SPF
 - DKIM
 - DMARC
 - analisi della reputazione del server mittente mediante una valutazione statistica che determina la probabilità (valori da -1 email buone a +1 email cattive) che il server invii email pericolose o spam e la confidenzialità della valutazione (valori da 0 poco affidabile a 1 certo)
 - la nazione da cui origina l'email
 - indice di reputazione complessiva valutato utilizzando i risultati dei test precedenti (valore zero neutra, valori positivi buona reputazione, valori negativi fino a -5 reputazione sospetta, valori negativi inferiori a -5 reputazione scarsa)
- spam check: sistemi di identificazione delle email di spam, sono implementati due sistemi:
 - sistema di classificazione delle email, in grado di identificare il tipo di email di spam, scam o in alcuni casi malware mediante un database di caratteristiche aggiornato costantemente e contenente oltre 200mila entry
 - sistema di identificazione delle email di spam mediante caratteristiche delle stesse, filtro baiesano, blacklist/whitelist e sistemi collaborativi;
 questo sistema seppur affidabile è dispendioso in termini di risorse di elaborazione e quindi viene eseguito solo se i sistemi precedenti non sono stati in grado di classificare l'email i modo affidabile

La seconda colonna identifica il tipo di analisi effettuata, mentre la terza l'esito dell'analisi, in base all'esito la riga viene evidenziata con un colore diverso:

verde: esito positivo o nessun esito

giallo: esito sospetto, ma non sufficiente per prendere una decisione

rosso: esito negativo

L'ultima colonna riporta alcune informazioni di **dettaglio** sulla singola analisi, come illustrato di seguito:

Per Clamav, Sophos e Metadefender è indicato "clean" se non sono state identificate minacce, oppure è indicato l'identificativo del malware, della firma di phishing o di spam se sono state identificate minacce.

Janusmail utilizza diversi database di firme per Clamav indicate nel dettaglio, in particolare **SecuriteInfo, Sanesecurity, Porcupine o firme ufficiali di Clamav**. Ad es. **Sanesecurity.Phishing.Fake.Coin.27677.UNOFFICIAL** sta ad indicare che la firma è del database Sanesecurity, non è ufficiale di Clamav, bensì un database aggiuntivo, si tratta di un Phishing (e quindi l'email verrà classificata come Scam) e in particolare la firma è denominata Fake.Coin.27677.

Se la minaccia è stata identificata da Sophos, verrà indicato mediante la parola Sophos. che precede il nome della firma, ad es.: Sophos.Exp/20180802-B

Metadefender è in grado di identificare la minaccia mediante quattro antivirus e di conseguenza viene indicato l'antivirus o gli antivirus che hanno dato esito positivo, ad es. **ESET,a variant of Win32/GenKryptik.DILP trojan;**, in questo caso l'antivirus che ha dato esito positivo è **ESET** e il nome della minaccia è "a variant of Win32/GenKryptik.DILP" e si tratta di una minaccia di tipo "trojan"

Metadefender è in grado di identificare i file non controllabili o pericolosi è lo indica come segue: Password Protected Document

Nel dettaglio delle analisi di metadefender è anche indicato il nome dell'allegato analizzato e l'ID dell'analisi (richiamabile per successive analisi dall'appliance di Metadefender), ad es.: "attach=Purchase Order.rar - id=f5ea86962c9942de934eeb84915a31fd - result=ESET, a variant of Win32/GenKryptik.DILP trojan;"

Sotto risultato dei filtri vengono visualizzate altre due sezioni:

- Destinatari: elenco dei destinatari dell'email
- Stato invio: in cui viene riassunto il percorso effettuato dall'email.
 Viene indicata l'ora di Invio, il destinatario, il server di inoltro e lo stato dell'invio (il quale influenza anche il colore della riga, che sarà verde per le email correttamente consegnate, gialle per le email sospese e rosso per quelle rifiutate).



Le righe evidenziate in giallo indicano problemi temporanei che potrebbero risolversi, quindi il sistema ritenterà l'invio dopo un tempo che dipende da diversi fattori, mentre una riga evidenziata in rosso indica un errore definitivo, quindi non risolvibile (ad es. destinatario inesistente), in questo caso il sistema non tenterà nuovamente di consegnare l'email ed invierà una comunicazione al mittente indicandogli la tipologia del problema.

La tipologia dell'errore non è sempre chiara, viene generata dal server destinatario dell'email, un esempio molto frequente è "Service unavailable", potrebbe indicare un problema di funzionamento del server destinatario o più tipicamente una dimensione eccessiva dell'email.

Le sezioni seguenti non sempre sono visualizzate, e sono:

- Operazioni richieste
- URL
- Allegati
- Zimbra Log
- Mailbox Log

Nella sezione denominata "Operazioni richieste" sono elencate le operazioni effettuate sull'email.

Stato invio											
Data/ora	Destinatario		Server d'inoltro Dsn		Dsn	Stato					
22/05/16 23:31:42	mbruse@zimbra-s	colutions.com				quarantined					
22/05/16 23:37:31	mbruse@zimbra-s	olutions.com	[192.168.20.66] [192.168.20.66]		2.0.0	sent (ok: queued as 7060d185aa8)					
Operazioni richieste				-							
Data richiesta Richiedente				Operazione							
22/05/16 23:33:22 mbruse@bls.it			rilascia								

Nell'esempio, si può vedere come per l'email, messa in Quarantena dal sistema, sia stata poi richiesto il rilascio dall'utente.

Alcune di queste operazioni sono automatiche, in questo caso nella colonna richiedente viene visualizzato "automatic", ad es. il rilascio di delle email delayed o la rimozione delle email già consegnate e successivamente identificate come pericolose (post delivery threat remove.) Nella sezione denominata "URL" sono elencate le eventuali URL (indirizzi web) presenti nell'email. Questa sezione viene visualizzata solo se è attiva la licenza "Advanced security".

Url	Stato	
http://pt5.abellacarl.trade/rm-abai	URL :-	▲
http://www.lettermelater.com/unsubscribe.php?mid'22297&email=mbruse@bls.it		

Se l'URL è ritenuta pericolosa, o lo sono il nome host (nell'esempio pt5.abellacarl.trade) o il dominio (nell'esempio abellacarl.trade) o l'indirizzo IP corrispondente all'hostname, allora l'URL viene evidenziata in rosso.

Nella colonna stato è indicato quale sezione dell'URL è ritenuta pericolosa (URL, Nome Host, Dominio, Indirizzo IP) ed eventualmente il motivo (ad es. phishing, fraud, involved in spam, malware, ecc.). Se non è indicato il motivo (viene visualizzato un trattino "-") è perché è stato segnalato pericoloso da un amministratore e per garantire la privacy non viene visualizzato il nome.

Se l'utente è un amministratore e vuole segnalare un URL come pericoloso può cliccare sul triangolo giallo di pericolo. Sarà possibile segnalare quali sezioni del URL vanno considerate pericolose spuntandole nel riquadro che apparirà:

Selezionare alme	no uno dei valori per la segnalazione
🗹 Url:	http://pt5.abellacarl.trade/rm-abai
Dominio	abellacarl.trade
Nome host:	pt5.abellacarl.trade
🔲 Indirizzo IP	23.95.29.178
	Salva 🛛 🙆 Annulla

Successivamente viene visualizzato l'elenco delle email già ricevute che contengono lo stesso URL per permettere eventualmente di avvisare gli utenti.

Le eventuali email consegnate con lo stesso URL verranno anche segnalate all'utente nella testata del report antispam (descritto in seguito):



Inoltre se è attiva la licenza "Zimbra advanced" l'email verrà spostata dopo pochi secondi nella cartella "Posta indesiderata" (funzione post-delivery threat remove):

© Z	imbra [.]									
Mail	Contacts	С	alendar	Tasks	Briefcase	Preferenc	es Antis	pam		
🖂 New	Message	•	Reply	Reply to All	Forward	Delete	Not Spam		<i>I</i>	Actions -
▼ Mail Fo	olders	\$	Sorte	ed by Date 🔽					26	messages
🛓 Inb	ox (8) nt		🔲 🔍 mi	bruse Enjoy this S	pecial Offer a	t Our New Lo	cation - Hi, C(ONGRATI	JLATIONS	3:20 PM
Dra	afts nk (1)	•	🗆 • Lu	ixury Clubs) Early Spring	Last Sale Sale	e: extra 60% (off + Specials I	Preview!	- Luxury C	Mar 03 Collectic 🏲

28/118

L'operazione di spostamento della email viene chiaramente registrata nelle operazioni e nel log della mailbox:

Mailbox LOG							
Server	Data/ora	Casella	id	operazione	descrizione		
bls-zimbrastore02	2019-03-06 15:20:40.0	mbruse@bls.it	904369	Adding Message	Adding message to Inbox folder		
bls-zimbrastore02	2019-03-06 17:11:24.0	mbruse@bls.it	904369	moving Message	webmail moving Message to Folder Junk (id=4)		
Operazioni richieste	9						
Data richiesta		Richiedente				Operazione	
06/03/2019 17:10:20		automatic	automatic				

Nella sezione denominata "Allegati" sono elencati eventuali allegati presenti nella email. Questa sezione viene visualizzata solo se è attiva la licenza "Advanced security".

Allegati										
Nome allegato	Tipo	hash	Stato							
Screenshot 2019-02-26 at 20.41.14.png	image/png	37294de77c8e92b6cc446a423f601ff755ef8330a08ce5cb9f7406678da0dc;	•	A						

Se l'allegato è ritenuto pericoloso allora viene evidenziato in rosso.

Nella colonna stato viene indicata la fonte dell'informazione (ad es. Metadefender, Alienvault, Yara, ecc.) tranne se l'allegato è stato segnalato pericoloso da un amministratore e per garantire la privacy non viene visualizzato il nome (viene visualizzato un trattino "-").

Se l'utente è un amministratore e vuole segnalare un allegato come pericoloso può cliccare sul triangolo giallo di pericolo.

Successivamente viene visualizzato l'elenco delle email già ricevute che contengono lo stesso allegato per permettere eventualmente di avvisare gli utenti.

Le eventuali email consegnate con lo stesso allegato verranno segnalate anche all'utente nella testata del report antispam (descritto in seguito):



Inoltre, se è attiva la licenza "Zimbra advanced", l'email verrà dopo pochi secondi spostata nella cartella "Posta indesiderata" (funzione **post-delivery threat remove**):

() Zimbra	i.							
Mail Contact	s C	Calendar	Tasks	Briefcase	Preferenc	es Antis	pam	
🖂 New Message	•	Reply	Reply to All	Forward	Delete	Not Spam	₫ • Ø •	Actions -
▼ Mail Folders	0	Sorte	ed by Date 🤝					26 messages
🛓 Inbox (8)		🔲 🔹 mi	bruse Enjoy this S	pecial Offer a	t Our New Lo	ocation - Hi, CO	ONGRATULATIC	3:20 PM
Drafts		🔲 o Lu	ixury Clubs					Mar 03
🗒 Junk (1)	•		Early Spring	Last Sale Sale	e: extra 60% (off + Specials I	Preview! - Luxur	y Collectic 🏴

L'operazione di spostamento della email è chiaramente registrata nelle operazioni e nel log della mailbox:

Mailbox LOG								
Server	Data/ora	Casella	id	operazione	descrizione			
bls-zimbrastore02	2019-03-06 15:20:40.0	mbruse@bls.it	904369	Adding Message	Adding message to Inbox folder			
bls-zimbrastore02	2019-03-06 17:11:24.0	mbruse@bls.it	904369	moving Message	webmail moving Message to Folder Junk (id=4)			
Operazioni richieste	1							
Data richiesta		Richiedente			1	Operazione		
06/03/2019 17:10:20		automatic	automatic					

Cliccando invece su una delle prime quattro icone seguenti:



vengono visualizzate rispettivamente le pagine di:

- Metadefender
- Virustotal
- Joe Sandbox
- Falcon Sandbox

Se l'hash corrisponde a quello di un file già controllato verranno visualizzati i risultati delle analisi, ciò vi permetterà di analizzare un allegato sospetto e capire se è già stato classificato come malware.

Nella pagina di Metadefender vengono visualizzati quanti antivirus hanno identificato un malware, se il file è vulnerabile e se la comunità ha dato dei punteggi positivi o negativi sul file:



A You must be <u>Signed in</u> to vote

MetaDefender critical detection results

ENGINE ~	SCAN TIME	LAST UPDATED	RESULT
TACHYON	24 ms	2019-06-08	Suspicious/X97M.Obfus.Gen.6 🛕
Ahnlab	10 ms	2019-06-08	MSOffice/Downloader 🔀

Virustotal da delle informazioni simili:

36	8 36 engines detected this file									
✓ 159 ✓ Community Score	73205a0d0fdf1297ef79dedc8eed10feeada4cb34e6d061ef68949058a7e238f 1d2ecf4aca1fe204547ed0f5c455dc50.virobj attachment auto-open macros obfuscated run-file xts	99.5 KB 2019-06-09 04:52:27 UTC Size 2 days ago	XLS							
DETECTION	DETAILS RELATIONS BEHAVIOR COMMUNITY									
Ad-Aware	() W97m. Downloader. IEA	AegisLab	Trojan.MSOffice.SAgent.4lc							
AhnLab-V3	() MSOffice/Downloader	ALYac	Trojan.Downloader.XLS.gen							
Antiy-AVL	1 Trojar/MSOffice.SAgent.gen	Arcabit	HEUR.VBA. Trojan.e							
Avast	Other.Malware-gen [Trj]	AVG	Other:Malware-gen [Trj]							

Inoltre in relations si possono vedere siti, domini e indirizzi ip acceduti dal malware:

DETECTION	DETAILS RELATIONS BEHAVIO							
Graph Summary (D		Contacted URLs	Ō				
	0		Scanned	Detections	URL			
		2019-06-10	0 / 70	http://crl.microsoft.com/pki/crl/products/r	microsoftrootcert.crl			
4 contacted urls				2019-06-03	0/66	http://crl.microsoft.com/pki/crl/products/l	MicCodSigPCA_08-31-2010.	
				2019-06-04	0 / 70	http://markeetiit.club/images/HOhXww5/ WkT/HwDxNc5n8_2F8pDOh/57/7RbojF e/wJOHy2OjdBCp95kiBAV/ZD/HWGW2/ 2881A/BScLRtJ//RPJIYGpNjefaYS5cvsQ Vi	voMsXpNt3/TQxamzKsvfxw /Gj19UMC2eUEJDkv_2BO 5fv1a4cEv_2Fw9frRkqalw_ Nk6S/N7yyRjFEI4/S3XimP.a	
Contracted Deravier 0				Contacted IPs ①			0	
				IP	Aut	onomous System	Country	
Created	Domain	Registrar		8.8.4.4	151	69 - Google LLC	US	
1997-07-22	ctldl.windowsupdate.com	CSC Corporate Domains, Inc.		47.74.9.247	451	02 - Alibaba (China) Technology Co., Ltd.	JP	
1991-05-02	crl.microsoft.com	MarkMonitor Inc.		192.35.177.64	117	91 - IdenTrust	US	
2019-05-30	markeettit.club	NameCheap, Inc.		72.247.184.48	209	40 - Akamai International B.V.	NL	
2019-05-30	markeettit.email	NameCheap, Inc.						
2004-02-19	apps.identrust.com	Network Solutions, LLC						

Le sandbox sono dei sistemi che simulano l'apertura del malware su un computer e verificano se hanno dei comportamenti sospetti, quindi anche se non è ancora riconosciuto dagli antivirus può essere riconosciuto come malware.

Joe Sandbox visualizza le analisi fatte ed il risultato:

ID	Result	Score	Antivirus	Filetype	Icon	Time & Date	Name		Info		CI	ass	Graph	Actions
139319	MALICIOUS	100/100	55%	xis	×	06.06.2019 18:11:27	Cartel_del_4_5_19_297	n 🎝	↓ [↑] att	D	•	G -	-#4	۲
Window	s:		Android:			Common:								
🍂 Inje	cts		Rece	ives SMS		📌 Gener	ates Internet Traffic							
🔕 Has	s kernel mode comp	onent	send:	s SMS		HTTP Gener	ates HTTP Network Traffic							
Dro	ps PE Files		🕚 Rebo	ot		💁 Expire	d Sample							
👶 Has	more than one Pro	cess	>_ Nativ	e CMD										
😤 Has	Email attachment													
Q Disa	assembly is availabl	le												

Cliccando sull'ID si accede all'analisi dettagliata dove tra l'altro viene visualizzato il risultato dell'analisi, il livello di confidenza e la classificazione:





Falcon Sandbox è molto simile:

- Timestamp	Input	Threat level	Analysis Summary	Countries	Environment
June 7 2019, 11:40 (CEST)	Cartel_del_4_5_19_66296.xls Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, C 73205a0d0fdf1297ef79dedc8eed10feeada4cb34e6d061ef68949058a7e238f	malicious	Threat Score: 100/100 AV Detection: 64% W97m.Downloader Matched 29 Indicators #macros-on-open 2 Show Similar Samples	-	Windows 7 64 bit
June 4 2019, 11:01 (CEST)	Cartel_del_4_5_19_33723.xls Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, C 73205a0d0fdf1297ef79dedc8eed10feeada4cb34e6d061ef68949058a7e238f	malicious	Threat Score: 93/100 AV Detection: 64% W97m.Downloader Matched 25 Indicators #macros-on-open 2 Show Similar Samples	-	Windows 7 32 bit

Riassumendo le prime due icone visualizzano il risultato fornito da decine di antivirus, mentre la terza e la quarta delle simulazioni di apertura dell'allegato.

Notare che la privacy è garantita in quanto l'unica informazione passata a questi siti è l'hash indicato nella stessa riga e che identifica univocamente il malware.
Se è attiva la licenza "Zimbra advanced" nel dettaglio email vengono visualizzate le sezioni:

- Zimbra LOG: riporta i log di ricezione e smistamento della email sul/sui server Zimbra
- Mailbox LOG: riporta le operazioni effettuate sull'email sul server Zimbra

Zimbra LOG	/imbra LOG								
Server	Data/or	ı	id email		operazione		descrizione		
bls-zimbrafe	2019-03	-06 20:03:20.0	01A1B6403B		sent internally route		internally routed		
bls-zimbrafe	2019-03	-06 20:03:20.0	4924A64043	5	sent	routed to mailstore			
Mailbox LOG									
Server	Server Data/ora Casella id operazione descrizione								
bls- zimbrastore	2019-03-06 20:03:20).0 mbruse(@bls.it	904428	Adding Message	Adding message to Inbox folder			

Ciò permette di tracciare l'email fino alla casella dell'utente, visualizzando inoltre le eventuali operazioni effettuate (cancellazione email, spostamento nella cartella posta indesiderata o in altre cartelle, lettura/cancellazione email con protocollo POP3 o IMAP, ecc.) o eventuali errori di consegna (ad es. Message-ID duplicato).

Per privacy ogni utente può controllare solo le proprie email/operazioni effettuate.

DETTAGLIO EMAIL STORICHE

Il dettaglio email per le email precedenti a Maggio/Giugno 2019 aveva un formato diverso da quello descritto, dopo i dati dell' email viene visualizzato l'analisi dello **stato di invi**o, per le email spedite, o dello **stato di ricezione**, per le email ricevute, come illustrato di seguito:

		Analisi stato invio	
Quarantine	No		
Analisi Policy:	OK		
Analisi Allegati:	Nessun allegato	Mimetype list:	Extension list:

Nello stato di invio i dati visualizzati sono:

- quarantena (se l'email è stata inserita in una quarantena dal Mail Relay)
- esito dell'analisi delle policy, ovvero se l'email era in contrasto con alcune delle Policy implementate per l'invio
- esito dell'analisi degli allegati contenuti nella email e tipo di allegato

		Analisi stato ricezione	
Quarantine	No		
Analisi Spam	is not spam	Punteggio: 2.40	Test positivi: INVALID_MSGID, RDNS_NONE
Analisi Malware	clean	Dettagli: Clean	
Reputazione mittente	SPF check: pass	DKIM check: none	DMARC check: none
Origine mittente	Nazione: FR	Coordinates (approx.): [2.3500,48.8600]	
Analisi Policy:	OK		
Analisi Allegati:	Num. 1	Mimetype list: application/x-msdownload	Extension list:

Nello stato di ricezione i dati visualizzati sono:

esito delle analisi del sistema antispam, con punteggio di spam e test positivi. Se il punteggio è uguale o superiore al parametro "Livello spam" nella policy "Spam score policy", l'email viene considerata come probabile spam, se il punteggio è uguale o superiore al parametro "Livello highspam", l'email viene considerata certamente spam. Se invece l'email è compresa tra il "Livello spam" -1 e il "Livello spam" l'email viene considerata dubbia e la consegna viene ritardata (delayed email).

Dopo il tempo "Ritardo email dubbie" il test antispam viene ri-eseguito, dando tempo alle blacklist ed altri database di aggiornarsi

Janusmail by B.L.S. Consulting - Manuale utente

- l'analisi del sistema anti-malware (virus, ransomware, trojan, ecc.) con i dettagli dell'esito (nell'esempio, Clean indica l'assenza di elementi pericolosi)
- l'analisi della reputazione del mittente con gli esiti del test SPF, DKIM e DMARC
- la nazione e le coordinate geografiche approssimative dell'origine dell'email (server che ha spedito l'email)
- esito dell'analisi delle policy, ovvero se l'email era in contrasto con alcune delle Policy implementate per la ricezione (tipicamente allegati pericolosi)
- esito dell'analisi degli allegati contenuti nell'email e tipo di allegato

Janusmail effettua diversi controlli antivirus mediante più di un sistema e usando diversi database di firme.

Nel campo details viene indicato quale database ha dato esito positivo (solamente il primo, in quanto Janusmail ottimizza i controlli e se un antivirus da esito positivo non perde tempo ad eseguire ulteriori controlli con altri).

Gli antivirus utilizzati sono

- **Clamav:** con tre diversi database di firme (quelli ufficiali con tasso di efficienza non superiore al 80%, SecuriteInfo e Sanesecurity lo aumentano ad oltre il 90%). In details troverete scritto "Infected" e tra parentesi il database di firma che ha identificato il malware e la descrizione sintetica.
- **Sophos:** se avete attiva la licenza Sophos, in details troverete scritto "Infected" e tra parentesi "Sophos" e la descrizione sintetica del malware
- **Metadefender:** se avete attiva la licenza Strong security, in questo caso viene utilizzato un sistema multi-antivirus in parallelo che utilizza **ESET, Total Defense, Bitdefender** e **K7** quali motori antivirus, in details troverete scritto "Metadefender" e tra parentesi la descrizione sintetica del virus

POLICIES

Le POLICIES sono regole di accettazione ed esclusione delle email ricevute.

Una POLICY può essere generata automaticamente, quindi da meccanismi automatici del mailrelay, oppure manualmente, ovvero venire inserita dall'utente.

Per accedere alla schermata di gestione delle POLICIES, selezionare l'opzione dal menù funzioni.

Policies									×
Descrizione		Tipo di policy		Priorità 0	:	🗹 Escludi polices	automatiche		
Cerca	1	Elimina Filtro		Hanna Nuova					
Policyid	Policy	Destination	Tipo		Azione	Priorità	Ultima modifica	Giorni di vita	
499979	Allegati pericolosi	bls.it/	Attachment	policy	Q1	1	2016-05-25 14:54:12.0	0	×
501128	Allegati firmati		Attachment	policy	AR	2	2016-05-25 14:48:28.0	0	×

La schermata che appare fornisce l'elenco delle Policies attive. Le colonne contengono, nell'ordine, le seguenti informazioni:

- **Policyid**: Numero identificativo della Policy
- **Policy**: Il nome attribuito alla Policy.

Se si tratta di una Policy automatica, il nome della Policy ne riassume le caratteristiche.

Esempio: "whitelist from <u>esempio1@esempiomail.it</u> to user <u>esempio2@esempiomail.it</u>" è la dicitura standard delle Policy di aggiunta in Whitelist automatica.

Vedremo nel paragrafo dedicato come vengono generate le Policies automatiche.

- **Destination**: Indica l'utente o il dominio per i quali è attiva la Policy
- **Tipo**: Indica la tipologia di Policy. Le tipologie e gli altri parametri sono descritti più avanti.

Janusmail by B.L.S. Consulting - Manuale utente

- Azione: Indica l'azione che il Mail Relay esegue sulla base della Policy impostata.
- **Priorità**: Definisce l'importanza della Policy nei confronti delle altre.
- **Ultima Modifica**: Indica la data e l'ora dell'ultima modifica effettuata alla Policy.
- Giorni di Vita: Indica per quanto la Policy rimarrà attiva. Questo indicatore esiste solamente nelle Policy automatiche, in quelle inserite manualmente risulterà sempre pari a 0 (cioè senza limite, quindi sempre attiva).

RICERCA POLICIES

Nella parte alta della schermata ci sono gli strumenti di ricerca delle Policies esistenti, nonché il tasto di creazione di Policies nuove. La ricerca si esegue inserendo le voci desiderate nei vari campi e cliccando il tasto "cerca".

Policies						
		Priori	tà			
Descrizione	Tipo di policy	0		Escludi polices automatich		
		\$				
S Cerca	🐺 Elimina Filtro	*	Nuova			
Policyid Policy	Destination	Тіро	Azione	Priorità	Ultima modifica	

Cliccando **Elimina Filtro** si eliminano gli effetti del filtro per Tipo di Policy.

Il campo **Priorità** permette di filtrare l'elenco in base alla priorità della Policy.

La spunta alla casella "Escludi policies automatiche" permette di vedere o escludere le Policies create automaticamente.

Tutti i filtri e la casella di ricerca sono sovrapponibili, ovvero è possibile inserire allo stesso tempo una priorità, un tipo di policy e una descrizione per ottenere i risultati che corrispondano a tutti i parametri.

INSERIMENTO MANUALE delle POLICIES

Le POLICIES possono venire inserite o eliminate solo dagli amministratori di Cliente o di Dominio.

L'amministratore di Cliente può decidere su quale dei suoi Domini impostarle.

Sia l'amministratore di Cliente che di Dominio possono impostare Policy sul singolo Utente.

Gli utenti non hanno diritto a impostare Policies, l'icona non è presente nelle loro Dashboard.

Per creare una nuova Policy si clicca il tasto "Nuova" nella schermata **POLICIES**, comparirà quindi la schermata **POLICY INSERT.** Per eliminarle, basta cliccare l'icona a forma di "X" rossa a fianco di ogni Policy dell'elenco.



Policies									×
Descrizione		Tipo di policy		Priorità		Secludi polices	s automatiche		
Cerca	1	😨 Elimina Filtro		V Nuova	•				
Policyid	Policy	Destination	Tipo		Azione	Priorità	Ultima modifica	Giorni di vita	
499979	Allegati pericolosi	bls.it/	Attachment	policy	Q1	1	2016-05-25 14:54:12.0	0	×
501128	Allegati firmati		Attachment	policy	AR	2	2016-05-25 14:48:28.0	0	×

Il campo Tipo di Policy definisce la tipologia di policy:

Attachment policy
Attachment policy
Manual blacklist
manda blackist
Manual whitelist
Manual whitelist By Example
Max email size policy
Periodic report policy
Spam score policy

Il **Tipo** può dunque essere:

- Attachment policy se la policy riguarda gli allegati
- Manual blacklist se si vuole aggiungere un indirizzo in Blacklist manualmente
- Manual whitelist se si vuole aggiungere un indirizzo in Whitelist manualmente
- Manual whitelist by example altra tipologia di whitelist, più flessibile
- Max email size policy, se si intende filtrare le mail in entrata e uscita in base alle dimensioni
- Periodic report policy, per schedulare l'invio periodico di report dettagliati sulle email filtrate da Janusmail
- Spam score policy se la policy riguarda la politica di classificazione delle email

Alcuni parametri sono comuni a tutte le Policy, e sono quelli indicati nella parte alta della schermata di inserimento.

-olicy Insen		
Tipo di Policy	Attachment policy 🔹	
Policy*:		
Priorita*:	1 ‡	
Azione Policy*:	Quarantine 2 •	
Da:		
A:		
Policy subject:		(Email address)

- **POLICY,** è la descrizione della policy
- **PRIORITÀ,** molto importante per stabilire quale policy ha priorità rispetto ad un'altra. Infatti, quando le POLICIES intervengono, la gerarchia è stabilita dal livello di PRIORITÀ di ciascuna Policy.

Si può, ad esempio, impostare una policy che permetta il passaggio di tutte le email con allegati firmati, e al contempo impostare una policy che imponga che le email con allegati pericolosi (ad es. file eseguibili) siano messe in quarantena.

La prima Policy, avendo un'importanza bassa, dovrà avere priorità bassa, ad es. 2, mentre la seconda, essendo molto importante per la sicurezza, dovrà avere priorità elevata, ad es. 8.

In questo esempio, un'email che avesse un allegato firmato ma potenzialmente pericoloso verrebbe accettata dalla prima Policy ma bloccata dalla seconda.

Essendo quest'ultima dotata di priorità superiore, l'email sospetta verrebbe bloccata.

- **AZIONE POLICY** indica quale azione la Policy debba effettuare. Può essere:
 - Allow Relay (AR) che permette all'email di passare.
 Una categoria fra Q1 e Q9, che indica in quale Quarantena conservare l'email in attesa.
 Le email in Quarantena possono essere rilasciate:
 - Tutte, dall'amministratore del cliente (quindi dalla Q1 alla Q9)
 - Dalla Q7 in giù dall'amministratore del dominio (quindi dalla Q1 alla Q7)
 - Dalla Q5 in giù dall'utente (quindi dalla Q1 alla Q5)
 - O Discard Email (DE) che indica di scartare l'email.
- DA indica l'indirizzo da cui l'email proviene.
 La policy verrà applicata alle email provenienti da quell'indirizzo.
 Se questo campo viene lasciato vuoto, vale per tutte le email che arrivano al Mail Relay.
- A indica il dominio verso cui l'email è indirizzata.
 Dall'elenco a tendina si può scegliere il dominio interessato tra tutti quelli che si hanno in gestione.
 Se si lascia vuoto questo campo, la Policy sarà valida per tutti i domini del cliente.
- Policy Subject è l'indirizzo email destinatario cui si applica la policy.
 Se questo campo viene lasciato vuoto, la policy viene applicata a tutto il dominio indicato al campo "A", o a tutte le email del cliente se il campo "A" non è stato specificato

ATTACHMENT POLICY

Le policy di questo tipo permettono di impostare regole sulla tipologia di allegati, i quali possono essere identificati per "Tipo", "Mime Type" o "Estensione".

Tipo di Policy	Attachment policy	
Policy*:		
Priorita*:	1 \$	
Azione Policy*:	Quarantine 2	
Da:		
Customer:	BLS Consulting	
A:	▼	
Policy subject:	(1	Email address)
Tipo 👂	MimeType 🔎	Estensione 🔎 🌞
		×
		×
		×
Selezionare uno o più criteri	con il rispettivo valore da aggiungere alla regola:	IL. J
	👍 Salva 🔞 Ar	nulla

Janusmail implementa oltre 400 sistemi per identificare gli allegati nelle email.

Esistono infatti numerosi standard per allegare i files alle email, e vengono inoltre usate moltissime tecniche di elusione per mascherare la presenza di allegati all'interno delle email.

Se l'allegato è un file compresso, il controllo degli allegati viene esteso anche al contenuto del file compresso (Janusmail riconosce decine di sistemi di compressione).

Il filtro per "Tipo" permette di identificare molto semplicemente le tipologie di allegato scelte tra le opzioni indicate:

їро/Туре	
Ricerca	
atttype	description
🕅 nsis	A scriptable win32 installer/uninstaller system.
🕅 high	Allegato ad alto rischio/High risk attachment
Compr	Allegato compresso/Compressed attachment
Crypt	Allegato criptato/Crypted attachment
m exe	Allegato eseguibile/Executable attachment
🕅 sign	Allegato firmato/Signed attachment
oc 📃	Documento in allegato/Document attachment

Janusmail è in grado, con diversi meccanismi "intelligenti", di identificare la tipologia di allegato, ad esempio la tipologia "high", ovvero allegati ad alto rischio.

È inoltre in grado di identificare oltre 100 tipologie di file (Mime type, vedi in seguito) o estensioni di file ritenuti pericolosi.

MimeType 🔎	Estensione 🔎 🐇		×
Mimetype		×	
Ricerca		T	X
Descrizione/Description		Mir	netype/Mimetype
3D Crossword Plugin		app	lication/vnd.hzn-3d-crossword
3GP		vid	eo/3gpp
🗖 🔲 3GP2		vid	eo/3gpp2
3GPP MSEQ File		app	lication/vnd.mseq
🕅 3M Post It Notes		app	olication/vnd.3m.post-it-notes
📃 🔄 3rd Generation Partnership Pro	ject - Pic Large	app	lication/vnd.3gpp.pic-bw-large

Il filtro per "Mime Type" permette filtrare per categoria/sottocategoria Mime (standard che identifica la tipologia di allegati):

Janusmail riconosce gli allegati non solo in base all'estensione, ma identificando il reale formato e quindi il tipo Mime.

Ad esempio, un file eseguibile DOS/Windows per definizione inizia con i caratteri "MZ" (in altre parole un qualsiasi file che inizia per MZ verrebbe eseguito sotto Microsoft Windows), ma potrebbe avere una estensione completamente diversa, ad es. ".txt" (tipico sistema di elusione dei controlli).

Janusmail riconosce il file dal contenuto e lo classifica come:

Microsoft Application

application/x-ms-dos-executable

indipendentemente dall'estensione del file.

Estensione 👂 🌞			
Estensione/file extension			
Ricerca	T		
Descrizione/Description		Estensione/file	extension
🗐 3ds Max Macroscript or Tecplot Macro		mcr	
🗐 3ds Max Script		ms	
E 4DOS Batch File		btm	
C Access Macro-Enabled Workbook		mam	
ACRobot Script		acr	
Actuate Report Object Executable		rox	
Adobe AIR Installation Package		air	
Adobe Flash ActionScript File		as	

MANUAL BLACKLIST

Questo tipo di policy serve a bloccare le email in base al mittente e al/ai destinatari.

Dopo aver assegnato un **Nome** alla Policy e averne impostato la **Priorità**, si sceglie tramite **Azione Policy** se eliminarle del tutto o inviarle a una quarantena. Gli altri campi **DA**, **A e Policy Subject** mantengono le stesse caratteristiche indicate nel capitolo **Inserimento Manuale delle Policies**.

Policy insert		
Tipo di Policy	Manual Blacklist 🔻	
Policy*:		
Priorita*:	1 ‡	
Azione Policy*:	Quarantine 1 🔹	
Da:		
A:	· · ·	
Policy subject:		(Email address)
		🚓 Salva 🙆 Annulla

MANUAL WHITELIST

Questo tipo di policy serve a evitare che un'email venga bloccata.

È sufficiente assegnare un **Nome** alla Policy e impostarne la **Priorità**.

Gli altri campi, DA, A e Policy Subject, mantengono le stesse caratteristiche indicate nel capitolo Inserimento Manuale delle Policies.

Tipo di Policy	Manual whitelist 🔹	
Policy*:		
Priorita*:	1 ‡	
Da:		
A:		
Policy subject:		(Email address)

MAX EMAIL SIZE POLICY

Questa Policy serve a impedire la ricezione o l'invio di email di dimensione troppo elevata.

Nei campi Max email size received e Max email size sent si impostano le dimensioni oltre le quali le email non verranno accettate, o nel caso di email in uscita, inviate.

Il mittente riceverà immediatamente una notifica che spiegherà l'impossibilità di spedire l'email.

Policy insert						
Tipo di Policy	Max ema	ail size policy 🔻				
Policy*:						
Priorita*:	1	÷				
A:		•				
Policy subject:			(Email addre	ss)		
Max email size recived:	0	MByte	Max email size sent:	0	MByte	
			4 Salva 🙆 Annulla			

PERIODIC REPORT POLICY

Con questa Policy si configura l'invio periodico di un Report Statistico sulle email inviate e ricevute dall'utente, dai suoi alias e dalle liste in cui il suo indirizzo è presente.

Il Report verrà inviato in orari configurabili nella policy spuntando la casella corrispondente.

Si può inoltre scegliere di ricevere il report anche nei giorni festivi, spuntando le relative caselle **Saturday**, **Sunday** o **Holidays**, sempre nelle ore impostate.

Tipo di Policy		Periodic rep	port policy	•			
Policy*:							
Priorita*:		1	\$				
Customer:		BLS Consu	lting	*			
A:			•				
Policy subject:					(Email address)		
Inviare il report a	alle ore:						
1	5	9	13	17	21		
2	6	10	14	18	22		
🔲 3	7	11	15	19	23	Sunday	
iii 4	8	12	16	20	🔲 о	- Holidays	
Testo email:							
Consultazione report tramite:	Web v		Conserva il re	eport per: 0	giorni		
Selezionare uno	o più criteri con il	rispettivo valore da	a aggiungere alla re	gola:			
				👍 Salva 🔞	Annulla		

È possibile personalizzare il testo della email inviata, lasciare vuoto il parametro "Testo email" per un testo standard predefinito.

È poi possibile selezionare se il report è consultabile direttamente nell'email oppure via web.

Nel caso di consultazione via email, nel corpo dell'email è riportato l'elenco delle email bloccate:

0	report periodico antispam/antispam periodic report	May 10, 20:
	From: no-reply@bls.it	
	To: Mauro Bruseghini	

Report email bloccate dal sistema antispam - Report email blocked by anti-spam system

Per gestirle, accedere alla dashboard al seguente link/To manage, access to the dashboard at the following link: https://dashboard.bls.it/dashboard

Motivo - Cause	Ricevuta il - Recived on	Da - From	A - To	
spam	09/05/2018 13:03	1457719936[at]qq.com	info[at]bls.it	12马a,å°æ³'åå³å¯åè′¹é18â'
spam	09/05/2018 13:05	newsletter1[at]hkyejian.com	mbruse[at]bls.it	Quote: Cisco UCS 6200 & 510
spam	09/05/2018 13:06	31824-379-353503421-6045-commerciale=bls.it[at]mai	commerciale[at]bls.it	Let Your Heart Run Wild with I
spam	09/05/2018 13:07	1289594165[at]qq.com	info[at]bls.it	19卿°è§è®¯ãAGè§è®¯è·å®
spam	09/05/2018 13:11	740302606[at]qq.com	info[at]bls.it	11æ¨å·²æä,º å¨&å°¼æ¯ âµÑæ

Nel caso di consultazione via web verrà inviata una email che permetterà di accedere al report via web:



È anche possibile accedere al report da Smartphone usando il QR Code.

La prima volta che si accede al report antispam da un PC o uno smartphone viene visualizzato quanto segue:

Report antispam

E' stata inviata una email, per accedere al report seguire le istruzioni presenti nella email

ed inviata una email per confermare l'accesso:



Attivazione report antispam Questa è una email automatica a seguito della richiesta di accesso al report web.

Se il PC da cui state accedendo NON è a vostro uso esclusivo



per visualizzare il report

Se invece il PC da cui state accedendo è a vostro uso

esclusivo

Premere qui

le prossime volte potrete accedere immediatamente senza autenticazione da questo PC Premendo questo pulsante sarà possibile accedere solo a questo report dal PC che si sta usando, per visualizzare un altro report sarà necessario ripetere questa procedura.

Premendo questo pulsante sarà possibile accedere a questo report ed ai successivi report da questo po senza dovere ripetere questa procedura. Utilizzare questa opzione dal proprio PC o smartphone. Questa opzione comporta l'uso di un cookie memorizzato sul browser del PC/smartphone utilizzato per riconoscere l'utente.

Janusmail® - © Copyright 2018 B.L.S. Consulting S.r.I.

Questo è un esempio del report antispam via web:

JANUSMAIL	
Report Antispam	
	Italiano 🔻 💮
L'email ricevuta il 19/02/2019 11:48 con mittente billiards5@notariato.it e oggetto fatture scadute potrebbe contenere un virus. Ti consigliamo di non aprirla e cancellarla.	Rimuovi notifica
L'email ricevuta il 06/03/2019 15:20 con mittente mbruse@gmail.com e oggetto Enjoy this Special Offer at Our New Location potrebbe contenere link pericolosi. Ti consigliamo di non aprirla e cancellarla.	Rimuovi notifica
🗷 email dubbie 🗆 spam 🗷 newsletter 🕜 malware	
Rimuovi le email dal report una volta verificate Cliccando su nascondi le email verranno rimosse dal report, saranno comunque visibili nella <u>dashboard o</u> cliccando su visualizza le email saranno nuovamente visibili. Nascondi Visualizza	ppure

Email spam/dubbie

- 17/03/2019 09:52 1401-829-23503-429-acquisti=bls.it@mail.batteryrestoree.bid Turmeric Diet is the new Trend
- № 07/03/2019 15:29 finance@telvoxglobal.com Invoice(s) monthly fees March 2019.
- 🛋 🗄 07/03/2019 11:51 info@accademiaformazione.com Gare MePA: Milano 9 Aprile
- 1:31 information@contact.regus.com La professionalità dietro l'angolo
- 14:14 mailreturn@smtp17.ymlpsvr.com Marchi popolari su richiesta

È possibile scegliere la lingua in cui è visualizzato il report direttamente dall'email o successivamente:



Cliccando sulla rotellina è possibile personalizzare il formato del report, questa scelta verrà memorizzata per il singolo utente:



Le scelte possibili sono:

Preferenze				
	visualizzazione grafici			
	email suddivise per mittente			



Spuntando "visualizzazione grafici" verranno visualizzati i grafici statistici delle email bloccate negli ultimi 30 giorni:



Spuntando "email suddivise per mittente" le email verranno raggruppate per mittente e se il numero è elevato (superiore a 10) il blocco di email non viene visualizzato, se non premendo sul mittente. Se invece non viene spuntata, le email vengono visualizzate in sequenza.

La prima parte del report visualizza, se necessario, delle notifiche:



L'email ricevuta il **19/02/2019 11:48** con mittente **billiards5@notariato.it** e oggetto **fatture scadute** potrebbe contenere un virus. Ti consigliamo di non aprirla e cancellarla.



L'email ricevuta il 06/03/2019 15:20 con mittente mbruse@gmail.com e oggetto Enjoy this Special Offer at Our New Location potrebbe contenere link pericolosi. Ti consigliamo di non aprirla e cancellarla.

Le notifiche possono essere di diverso tipo e sono precedute da un'icona specifica:



è una notifica di una email già consegnata e contenente un possibile virus



è una notifica di una email già consegnata contenente dei link a siti pericolosi (URL)

Dopo aver verificato quanto notificato è possibile cliccare sul pulsante "Rimuovi notifica", quindi la notifica non verrà più visualizzata.

La sezione seguente permette scegliere quali email visualizzare nel report:

🕑 email dubbie	🗆 spam	newsletter	malware	

Spuntare la tipologia per email da visualizzare, eventualmente inserire nel campo di ricerca il mittente, l'oggetto (anche parzialmente) e premere l'icona di ricerca.

×

Rimuovi notifica

×

Rimuovi

notifica

Successivamente vengono visualizzate le email bloccate divise per tipologia:



Email spam/dubbie

- 🛋 🔤 07/03/2019 09:52 1401-829-23503-429-acquisti=bls.it@mail.batteryrestoree.bid Turmeric Diet is the new Trend
- 1 08/03/2019 09:04 1tacflashlight@final-bubble.bid Military Grade Tactical Flashlight Now 75% Of-f
- 08/03/2019 07:37 amazonsurvey@pink-shave.us \$100 Amazon Survey Opportunity!

Cliccando su una email vengono ne visualizzati i dettagli:

Email	
Data/ora	07/03/2019 09:52
Mittente	1401-829-23503-429-acquisti=bls.it@mail.batteryrestoree.bid
Destinatari	acquisti@bls.it
Oggetto	Turmeric Diet is the new Trend
Id Messaggio	x278qJOY032504
Motivo del blocco	spam
Punteggio	



Cliccando sulle icone a inizio riga o sui pulsanti in coda alla pagina di dettaglio è possibile rilasciare l'email o aggiungerla in whitelist e quindi rilasciarla.



Il pulsante Preview permette di visualizzare l'email (se non è ritenuta pericolosa) per decidere se rilasciarla:

Attenzione: l'email visualizzata potrebbe essere una email di phishing (truffa) o puntare ad un sito che contiene codice pericoloso (virus, ecc.), prestare quindi molta attenzione. Se ci sono dubbi non rilasciate l'email e contattate il vostro amministratore di rete

From : Fastest fat burner -Fastest.fat.burner@batteryrestoree.bid Subject : Turmeric Diet is the new Trend



Dopo aver verificato le email nel report ed averle eventualmente rilasciate o aggiunte in whitelist consigliamo di "nasconderle" dai successivi report. Così facendo nel prossimo report verranno visualizzate solo le email arrivate nel frattempo e non di nuovo tutte.

Per fare questo cliccare sul pulsante "Nascondi":



Cliccando su "Visualizza" si annulla l'effetto di "Nascondi" e verranno visualizzate di nuovo tutte le email bloccate nell'ultimo mese.

SPAM SCORE POLICY

Tipo di Policy	Spam score policy 🔻	
Policy*:	Punteggio spam	
Priorita*:	1 ‡	
Customer:	BLS Consulting	•
A:	•	
Policy subject:		(Email address)
Livello Spam:	5 Livello Highspam: 10	
Blocco newsletter:	Si 🔻	
Ritardo email dubbie:	60	
Qurantena attiva:	Si 🔻	
Selezionare uno o più criteri co	n il rispettivo valore da aggiungere alla regola:	

Questo tipo di policy permette di impostare i parametri del sistema antispam.

I parametri principali sono il "Livello spam" e il "Livello Highspam".

Se il punteggio spam calcolato su una email è inferiore al Livello Spam, l'email non sarà considerata spam.

Se il punteggio è compreso tra il livello SPAM e il livello HIGHSPAM, sarà considerata probabile spam.

Se è superiore al livello HIGHSPAM sarà considerata sicuramente spam.

Negli ultimi due casi l'email sarà di default inserita nella **Quarantena Spam** (**QS**) da cui potrà essere rilasciata dall'amministratore o dai destinatari. Il sistema utilizza le email con punteggio superiore al livello **HIGHSPAM** per apprendere come sono fatte le email di spam ricevute.

Se il punteggio spam è compreso tra "Livello spam" -1 e "Livello spam" allora la classificazione è dubbia, in questo caso la consegna della email viene ritardata (delayed emails). Dopo i minuti indicati nel parametro "Ritardo email dubbie" viene ripetuto il test antispam. Ciò permette alle blacklist e altri sistemi collaborativi di aggiornarsi. Se il punteggio sarà ancora dubbio l'email verrà comunque consegnata.

È possibile poi specificare se le Newsletter (bulk-emails) devono essere bloccate (per tutto il dominio), ogni utente potrà dalle proprie preferenze scegliere se riceverle.

L'ultimo parametro indica se la quarantena è attiva oppure no

Se la si disattiva, tutte le email non pericolose (quindi non quelle contenenti virus, allegati pericolose o classificate come scam) verranno consegnate agli utenti.

In questo caso però le email di spam avranno scritto nell'oggetto [SPAM] e le newsletter avranno scritto [NEWSLETTER], gli utenti potranno definire quindi dei filtri che spostano queste email in apposite cartelle.

Di seguito due esempi di filtri per Zimbra:

Edit Filter	Edit Filter
Filter Name: Spam	Filter Name: Bulk emails
If any - of the following conditions are met:	If any - of the following conditions are met:
Subject V contains V [SPAM]	Subject • contains • [NEWSLETTER]
Perform the following actions:	Perform the following actions:
Move into folder - Junk	Move into folder - Bulk emails
✓ Do not process additional filters	✓ Do not process additional filters
OK Cancel	OK Cancel

POLICIES AUTOMATICHE

Le Policies automatiche sono di due tipi: Automatic Whitelist Sender to Receiver e Automatic Whitelist Domain Sender to Domain Receiver with not fail SPF. Queste due Policies sono native del sistema di Mail Security di BLS, e costituiscono un efficacissimo sistema per ridurre il problema dei Falsi Positivi.

Automatic Whitelist Sender to Receiver

Questa Policy si crea automaticamente ogni volta che viene inviata un'email da parte del cliente a un suo contatto.

L'indirizzo del contatto viene registrato dal sistema che, in futuro, permetterà alle email provenienti da quell'indirizzo di passare.

La Priorità di queste Policies è impostata di default a 5, in modo che eventuali altre Policies di sicurezza importanti possano comunque avere precedenza, mentre quelle di Spam non fermino le email con Policy di Whitelist automatica.

Nell'elenco delle Policies viene indicato, come nome della Policy, tra quali indirizzi questa è attiva.

Policies					
Descrizione	whitelist from marksavino0104@gmail	Tipo di policy		Priorità	
			•	0	÷
S Cere	ca	😨 Elimina Filtro		Huova	
Policyid	Policy	Destination	Tipo		Azione
538105	whitelist from marksavino0104@gmail.com to user msavino@bls.it	msavino@bls.it	Automatic to receiver	whitelist sender	AR
H A					

Automatic Whitelist Domain Sender to Domain Receiver with not fail SPF

Anche questa Policy si crea automaticamente ogni volta che viene inviata un'email da parte del cliente a un suo contatto.

Il suo funzionamento è simile alla Automatic Whitelist Sender to Receiver, con la differenza che non sarà soltanto l'indirizzo del contatto a cui viene inviata l'email ad essere automaticamente inserito in una whitelist con priorità 5, ma l'intero suo dominio a patto che il TEST SPF effettuato su quel dominio non fallisca.

DURATA E SCADENZA DELLE POLICIES AUTOMATICHE

Come già accennato in precedenza, le Policies automatiche hanno una scadenza.

Scadono dopo 365 giorni, indicati nella colonna **Giorni di Vita**, dalla data di ULTIMA MODIFICA. Per sapere se la Policy è ancora attiva, è sufficiente verificare se siano passati più o meno di 365 giorno da tale data.

Policyid	Policy	Destination	Tipo	Azione	Priorità	Ultima modifica	Giorni di vita
146331	whitelist from esempio1@esmail.it to user mbruse@bls.it	mbruse@bls.it	automatic whitelist sender to receiver	AR	5	2016-02-08 15:20:15.0	365
471168	whitelist from esempio2@esmail.it to user mbruse@bls.it	mbruse@bls.it	automatic whitelist sender to receiver	AR	5	2016-04-14 11:22:44.0	365
42117	whitelist from esempio3@esmail.it to user mbruse@bls.it	mbruse@bls.it	automatic whitelist sender to receiver	AR	5	2016-05-04 17:23:01.0	365

La scadenza delle Policies è effettiva solo per quelle create automaticamente, NON per quelle create manualmente, per le quali i giorni di vita saranno sempre indicati come "0".

Il senso di questa funzione è evitare che delle Policies create per scambi di email saltuari vadano a intasare per lungo tempo le policies aziendali.

DOMAIN PREFERENCES

Da questa schermata è possibile configurare le proprie preferenze di dominio. Per accedere cliccare sulla corrispondente opzione del menu funzioni.

Domain preference						×
Utente	msavino			Dominio		
Ricerca	🐺 Elimina Filtro	0		Huden Nuc	va	
ID Cliente		Dominio	login name	Lingua	Cookie IpAddress	
000000		bls.it	msavino@bls.it	it	172.30	×
1/1) H					

Cliccando il tasto "NUOVA" si aggiunge una preferenza, ovvero si impostano alcuni parametri per tutti gli utenti di un dominio o per il singolo utente.

Cliente:	BLS Consulting	
Dominio*:	bls.it 🔻	
Login name:		
Lingua*:	Italian 🔻	
	172.30	
	192.168	
Cookie Ipaddress: 🐣		
Preferenze ricerche dashboard:		
Ckeck su 'Solo da rilasciare'	No T	
Estrai gli utlimi n°	0 giorni	

Impostare le preferenze per un dominio/utente specificando:

Cliente: cliente cui il Dominio appartiene

Dominio: il Dominio per cui si imposta la preferenza

Login Name: l'indirizzo email dell'utente. Se si lascia vuoto, varrà per tutti gli utenti del dominio

Lingua: con questo parametro si può impostare la lingua di default degli utenti del dominio

Cookie Ipaddress: gli indirizzi ritenuti sicuri, ovvero per i quali il Mail Relay riconoscerà il cookie e non chiederà le credenziali ad ogni accesso alla dashboard

Sotto "**Preferenze ricerche dashboard**" è possibile scegliere se la casella "**Solo da rilasciare**" è di default spuntata e nelle ricerche avanzate il numero dei giorni su cui verranno fatte le estrazioni.

GESTIONE ALIAS

Per accedere cliccare sulla corrispondente opzione del menu funzioni.

Aliases					×
Ricerca	mbruse@bls.it				
S Ricerca	Elimina Filtro				
Cliente		Username	Alias	Attivo	
000000 - BLS Consulting		mbruse@bls.it	abuse@bls.it	No	×
000000 - BLS Consulting		mbruse@bls.it	aggiornamento@bls.it	Yes	×
000000 - BLS Consulting		mbruse@bls.it	alert@bls.it	No	×
000000 - BLS Consulting		mbruse@bls.it	all@bls.it	No	×
000000 - BLS Consulting		mbruse@bls.it	backup@bls.it	Yes	×

Da questa schermata è possibile visualizzare gli Alias e le liste di distribuzione cui ogni indirizzo email gestito dal Mail Relay è associato. Le alias sono normalmente sincronizzate con quelle del proprio server di posta, è comunque possibile aggiungerlo manualmente.

Le alias vengono usate per:

- raggruppare i report antispam in modo da inviarne uno solo e non uno per ogni alias
- permettere ad un utente la gestione delle email inviate anche agli alias e alle liste di distribuzione
- permettere l'accesso alla dashboard con un'alias (solo se l'alias è attiva)

Cliccando "NUOVO" si aprirà la seguente schermata.

Nuovo		×
ID Cliente:	BLS Consulting •	
Username :		
Alias :		
Attivo:	Si 🔻	
	👙 Salva 🙆 Annulla	

Da qui si configurano i vari campi:

Id cliente: il Cliente per cui si impostano gli Alias

Username: l'indirizzo email cui associare Alias o Lista

Alias: l'Alias o la Lista che si intende associare all'indirizzo email

Attivo: selezionando "SI", si rende valido l'Alias o l'indirizzo della lista per accedere all'account Mail Relay dell'utente
SENT EMAIL MONITOR

Questa sezione offre una visualizzazione aggregata in tempo reale delle email inviate da ciascun Dominio appartenente al cliente.

Per accedere cliccare sulla corrispondente opzione del menu funzioni.

Monitor email inviate						×
Domini bloccati Domini con utenti bloccati Cliente: BLS		BLS Consulting		Dominio		C > 🔊
Dominio	Data/ora ultimo invio	Email Inviate	Invio bloccato	Invio temporanemente bloccato	Data/ora blocco	
antonioreale.it		0	No	No		🗳 📼
assipavia.it	2019-03-08 12:34:00.0	20689	No	No		🗳 📰
bls.it	2019-03-08 12:41:00.0	844857	No	No		💰 🖷

Le varie colonne indicano il **Dominio, Data e Ora** dell'ultimo invio da quel Dominio, **Email Inviate**: il conteggio delle email inviate da quel dominio, **Invio Bloccato**: se l'invio per l'intero dominio è stato bloccato da un amministratore, **Invio temporaneamente bloccato**: se l'invio è stato bloccato dal sistema automatico di monitoraggio del volume delle email inviate, **Data/Ora del blocco**: quando è iniziato il blocco.

Le due icone alla fine di ciascuna riga permettono di accedere ad altre schermate che forniscono ulteriori dettagli sulle email inviate, la prima icona apre una finestra che mostra le stesse colonne del monitoraggio del traffico, ma organizzato per utente. La seconda icona apre una finestra che indica le ultime 50 email inviate dagli utenti del dominio.

Domini bloccati o contenenti utenti bloccati sono evidenziati in rosso, mentre domini temporaneamente bloccati o contenenti utenti temporaneamente bloccati sono evidenziati in giallo.

Cliccando su una riga viene aperta una finestra che permette di bloccare/sbloccare l'invio e definire i parametri che regolano il sistema automatico di monitoraggio del volume di email inviate.

ominio*	cloud-solutions.it			
de blannte	No			
rio bloccato	Yes			
vio temporaneamente bloccato	No			
	© Yes			
assimo numero di email/minuto per domain	200			
assimo numero di email/minuto per utente	40			
lassimo numero di email/ora per utente	200			

Prestare molta attenzione all'uso di "Invio bloccato": infatti impostando questo parametro a "Yes" tutte le email inviate dall'utente dei dominio vengono bloccate e viene immediatamente segnalato al mittente l'impossibilità di recapitare l'email, attenzione: **l'email non verrà rispedita.**

Impostando invece il blocco temporaneo le email verranno tenute in coda e solo dopo un'ora verrà notificato all'utente che l'email non è stata ancora consegnata. Appena si sbloccherà l'account le email in coda verranno immediatamente consegnate.

Il sistema automatico di monitoraggio del volume di email inviate verifica che il numero di email/minuto o all'ora indicate non vengano superato. Appena questi limiti vengono superati (per un uso improprio da parte dell'utente o più comunemente perché la casella ad insaputa dell'utente viene usata per inviare spam) viene impostato un blocco temporaneo. Gli amministratori ricevono quindi una email con la notifica del problema con le istruzioni per sbloccare nuovamente l'account dopo aver risolto i problemi di sicurezza.



Nel caso di server **Zimbra**, e se la funzione è stata attivata, vengono bloccati contestualmente anche gli account. In guesto modo l'uso improprio della casella viene impedito e si evita l'accumulo di email nelle code del server **Zimbra**.

Cliccando sull'icona "Senders" verranno visualizzati i singoli utenti e se l'account Zimbra è stato bloccato:

Utenti bloccati Utente					🔕 Esci 🧲 🔎		
Utente		Data/ora ultimo invio	Email inviate	Invio bloccato	Invio temporaneamente b	l Utente bloccato su Zimbra Data/ora blocco	
assistenza@bls.it		2016-05-17 16:41:00.0	23	No	No	No	📼 🔒 🔏

Quindi oltre alle colonne già descritte per i domini, viene evidenziato se l'account Zimbra è stato bloccato.

Le tre icone a fine riga permettono di:

0

visualizzare le ultime 50 email, utile per verificare se si tratta di un uso improprio o di un falso positivo

bloccare o sbloccare l'account Zimbra

Cambiare la password dell'account Zimbra

Utilizzando le ultime due icone sarà quindi possibile rimettere in sicurezza l'account Zimbra cambiando la password eventualmente compromessa e sbloccare l'account senza dover accedere alla console di gestione di Zimbra.

Anche nel caso degli utenti sarà possibile, cliccando su una riga, accedere alla schermata che permette il blocco/sblocco dell'invio e impostare parametri personalizzati per il sistema automatico di monitoraggio del volume di email inviate:

assistenza@bls.it
No
O Yes
No
Ø Yes
50
200

Prestare molta attenzione all'uso di "Invio bloccato".

Impostando questo parametro a "Yes" infatti tutte le email inviate dall'utente vengono bloccate e viene immediatamente segnalato al mittente l'impossibilità di recapitare l'email, attenzione: l'email non verrà rispedita.

Impostando invece il blocco temporaneo, le email verranno tenute in coda e solo dopo un'ora verrà notificato all'utente che l'email non è stata ancora consegnata. Appena si sbloccherà l'account, le email in coda verranno immediatamente consegnate.

Il sistema automatico di monitoraggio del volume di email inviate verifica che il numero di email/minuto o all'ora indicate non vengano superate. Appena questi limiti vengono superati (per un uso improprio da parte dell'utente o più comunemente perché la casella viene usata per inviare spam ad insaputa dell'utente) viene impostato un blocco temporaneo.

REGOLE ANTISPAM

Con questa opzione è possibile personalizzare il punteggio del sistema antispam. Questa opzione è disponibile solo per gli amministratori del cluster, in quanto le regole agiscono su tutti i clienti, domini e utenti del cluster.

Per accedere cliccare sulla corrispondente opzione del menu funzioni.

Antispam Rules					×
Descrizione	Rule id	۶ 🕺	÷		
Ruleid	Descrizione	Regola	Punteggio	Attiva	
NOT_ANNUL_SCON	ANNULLAMENTO SCONTRINO Bricoio	Subjectraw =~ /NOTIFICA ANNULLAMENTO SCONTRINO/i	-2.0	Si	×
UNDER_IN_FROM	From name contains underscore character	From:raw =~ /_/i	0.5	Si	×
RCVD_IN_PSKY	Received via a relay in PSKY	eval:check_rbl('psky-lastexternal', 'bad.psky.me.', ^127\.0\.0\2\$')	1.5	Si	×
RCVD_IN_TRUNC	Received via a relay in TRUNCATE	eval:check_rbl('trunc-lastexternal', 'truncate.gbudb.net.', ^127\.0\.0\2\$)	1.5	Si	×
RELATA1	relata di notifica in subject	Subject:raw =~ /relata di notifica/i	10.0	Si	×
RETURN_RECEIPT	Ricevuta di ritorno	Subject:raw =~ /return receipt/i	-3	Si	×
RCVD_IN_EMAILREG_0	Sender listed at http://www.emailreg.org/	eval:check_rbl_sub('emailreg-trusted', '127.0.\d+.0')	-20	Si	×
RCVD_IN_EMAILREG_1	Sender listed at http://www.emailreg.org/	eval:check_rbl_sub('emailreg-trusted', '127.0.\d+.1')	-20	Si	×

Cliccando sull'icona "+" è possibile aggiungere una nuova regola, cliccando sulla croce rossa a fine riga si disattiverà la regola, cliccando direttamente su una regola è possibile modificarla.

Una regola deve essere identificata da un **Rule Id univoco**, e includere una descrizione della regola.

Nuovo		×
Rule ID* :	RELATA1	
Descrizione* :	relata di notifica in subject	
Regola*	Subject:raw =~ /relata di notifica/i	
Punteggio*:	10.0	
Attivo*:	Si 🔻	
	👍 Salva 🙆 Annulla	

La regola segue in linea di massima questa sintassi:

parametro dell'email da valutare = ~ (uguale e tilde) regular expression

Il parametro normalmente è: Subjectraw (oggetto della email) o Fromraw (mittente della email)

La regular expression più comune è quella usata per indicare una parola o frase contenuta nel parametro, la sintassi è:

/parola o frase/, se si aggiunge una "i" sta ad indicare che la ricerca è case insensitive, quindi non tiene conto delle maiuscole/minuscole.

Ad es. una regola che identifica le email che hanno nell'oggetto la frase "relata di notifica" si scriverà Subjectraw = ~ /relata di notifica/i

Il punteggio si somma al punteggio valutato dal sistema antispam, può essere positivo o negativo.

Il livello normale per considerare una email come spam è 5 (impostabile con la policy Spam score policy descritta prima), quindi se si aggiunge 10 come in questo esempio è molto probabile che l'email verrà considerata spam, se si aggiunge 100 si avrà la certezza.

Analogamente, se il punteggio si imposta a -10 è molto probabile che l'email verrà fatta passare, con -100 sicuramente verrà fatta passare.

BILLING

Questa opzione visualizza il numero di caselle attive per singolo dominio e per un determinato mese. Vengono valutate le caselle che hanno spedito email "Sender", e quelle che le hanno ricevute "Receiver".

Per accedere cliccare sulla corrispondente opzione del menu funzioni.

Mail Billing						×
Cliente: BLS Consulting Anno-Mese: 2019 V 03 V						🔎 🖲 📑
Customer	Dominio	Anno/mese	Sender	Receiver	Total	Aggiornato il
000000 BLS Consulting	bls.it	2019/03	44	35	60	2019-03-08 00:04:45.0
000000 BLS Consulting	blscloud.com	2019/03	6	10	11	2019-03-08 00:04:45.0
000000 BLS Consulting	cloud-solutions.it	2019/03	1	2	2	2019-03-08 00:04:45.0

Cliccando sull'icona a fine riga viene visualizzato l'elenco delle caselle corrispondenti.

È possibile esportare l'elenco dei domini e dei domini suddivisi per cliente, con l'indicazione in questo caso delle opzioni commerciali attive (Strong security, Zimbra advanced, ecc.) e del numero di caselle licenziate:

	A	В	С	D	E	F
1	ELENCO ACCOUNT 201903					
2						
2	Customer:	Expiry Date:	Mailbox			
з			licensed:		Opti	ons:
4	BLS Consulting(000000)		50	Zimbra advanc	ed- Strong secur	ity- Mass Mailing- Email archive
5	Domain	Year/month	Sent	received	Total	Last Update
6	bls.it	201903	44	35	60	2019-03-08 00:04:45.0
7	blscloud.com	201903	6	10	11	2019-03-08 00:04:45.0
8	cloud-solutions.it	201903	1	2	2	2019-03-08 00:04:45.0
9	mail-solutions.it	201903	0	4	4	2019-03-08 00:04:42.0
10	zimbra-solutions.com	201903	0	5	5	2019-03-08 00:04:43.0
11	zimbra-solutions.it	201903	1	1	1	2019-03-08 00:04:45.0
12	Total:		66	57	97	
13						

Queste estrazioni sono utili per ri-addebitare il costo del servizio a clienti o altre aziende del gruppo.

ALLEGATI PERICOLOSI

Questa opzione permette accedere al database delle firme (hash SHA1) dei file pericolosi.

Per accedere cliccare sulla corrispondente opzione del menu funzioni.

Allegati pericolosi					×	
hash		Inserito da		\mathbf{S}		
date from: 08/03/2019 🗒		date to:				
Hash	Inserito da	Data	Attivo			
fe3d4bd68d9e048570bec85f807eef195a785ed1cbf351e8e35bda92acc14822	Metadefender	2019-03-08 14:09:41.0	Si	0		
fe7f81b757558fb7c3ff7f81b527efea10dc8bf7cb7ca03ddf39c8bf4d75ee3e	Metadefender	2019-03-08 14:06:13.0	Si	0	10.°	
fe808f4baf85524d2e12ba0b5283db8bbab4e07f3bf9772086f4e6770138a982	Metadefender	2019-03-08 14:03:24.0	Si	0		

La colonna "Inserito da" indica la fonte della firma. Le firme possono venire segnalate dagli amministratori (da **dettaglio email** come illustrato nei paragrafi precedenti), e vengono inoltre aggiunte da Janusmail, che le ottiene costantemente da più fonti (mediamente **13000 firme a settimana**).

Le firme vengono usate in fase di ricezione di una nuova email: se un allegato ha una firma uguale ad una presente nel database, l'email viene bloccata come malware (virus) e nella descrizione viene indicato "hash" e fonte della firma.

Inoltre, se è attivo il modulo **Advanced security**, alla ricezione di una nuova firma vengono ricontrollate tutte le email ricevute fino a quel momento e, se la firma corrisponde, viene notificato all'utente mediante il report antispam (vedi paragrafo dedicato).Inoltre, se è attivo il modulo **Zimbra advanced**, l'email viene automaticamente spostata nella cartella "posta indesiderata" dopo pochi secondi.

Nel caso di falsi positivi (rari ma sempre possibili) si può disattivare la firma cliccando sull'apposita icona.

L'icona a forma di busta a fine riga permette visualizzare l'elenco delle email ricevute che contengono un allegato con la stessa firma. Mentre le quattro icone riportate sotto permettono visualizzare le analisi sulle pagine di metadefender, virustotal, joe sandbox e falcon sandbox.

L'uso di queste icone è già stato illustrato nel dettaglio email.

THREATS INDICATORS

Questa opzione permette di accedere al database degli indicatori di minaccia, cioè domini, nomi host, url e indirizzi ip coinvolti in attacchi di phishing o frodi, campagne di spam, diffusione di malware ecc...

Per accedere cliccare sulla corrispondente opzione del menu funzioni.

Threats indicator										×
hash				Classificazione	Dalla data : 04/03/2019	Ξ.	Alla data : 08/03/2019		¥	
Cerca Domain T il										
Hash	Classification	Data	lp	Hostname	Domain	Url		Active		
00025d5ffbe644b5a8bc16c7ce15e48038	OTX white	2019-03-06	105.225.14.211					Si	8	
000760d0865c2bcc3ddd444e83b427207	OTX white	2019-03-06			pirates-mist.ru			Si	0	E°
000f56ab5f3e5b5b0287f7d7e523c5b26b;	OTX white	2019-03-07			pcmindustries.com			Si	8	
001139912d9ce5731fb1409801a30235b;	OTX Green	2019-03-07	119.194.48.196					Si	0	5.0
0020fb71a4ad98c2ab756d4eb842996b8	OTX white	2019-03-06				http://maracuja.	u/IsnB-iD7n_Y-HHd/En/Past-Due-Invoices/	Si	0	

La colonna "Classification" indica la tipologia di minaccia, nel caso la minaccia non sia nota (ad esempio se per qualche motivo è riservata), viene indicato un livello di sensibilità dell'informazione secondo quanto indicato in questa pagina:

https://www.us-cert.gov/tlp

È possibile, per gli amministratori, segnalare una minaccia (da "dettaglio email" come già illustrato nel rispettivo paragrafo). Inoltre, Janusmail recupera costantemente da diverse fonti nuovi indicatori (mediamente 9000 indicatori di minaccia a settimana).

Gli indicatori di minaccia vengono usati in fase di ricezione di una nuova email: se l'email contiene, nel corpo o negli allegati, uno o più di questi indicatori, viene calcolato un punteggio che determina il blocco dell'email se supera una determinata soglia (come **SCAM** se le minacce sono di tipo phishing, frode, coinvolte nella diffusione di malware, come **SPAM** se coinvolte in campagne di spam o come **NEWSLETTER** se sono presenti numerosi link di tipo ad/tracking, cioè usati per monitorare gli utenti per campagne marketing.)

Inoltre, se è attivo il modulo **Advanced security**, quando viene segnalato un nuovo URL pericoloso vengono controllate tutte le email ricevute fino a quel momento e se contengono l'URL viene notificata all'utente mediante report antispam (come già illustrato nel paragrafo dedicato).

Janusmail by B.L.S. Consulting - Manuale utente

Se inoltre è attivo il modulo Zimbra advanced l'email viene spostata nella posta indesiderata dopo pochi secondi.

Nel caso di falsi positivi (rari, ma sempre possibili) si può disattivare l'indicatore di minaccia cliccando sulla apposita icona.

L'icona a forma di busta a fine riga permette di visualizzare l'elenco delle email ricevute che contengono un allegato con lo stesso indicatore di minaccia.

DMARC REPORT

Il report DMARC raccoglie le informazioni inviate da server che hanno ricevuto email dai vostri domini, sia che siano state spedite da vostri utenti, sia che siano email di spam o phishing che usano impropriamente i vostri indirizzi email.

Quindi ad es. se voi inviate delle email ad un destinatario che usa Google Gmail, i server di Google vi invieranno periodicamente dei report statistici via email indicando il numero di email ricevute, da che server e se queste email sono ricevute da server compliant con SPF e firmate correttamente con DKIM.

Si può usare questo strumento per analizzare i dati ricevuti e sistemare la configurazione per attivare le policy DMARC.

Per poter ricevere i report DMARC è necessario impostare un record DNS appropriato:

_dmarc.bls.it IN TXT v=DMARC1; p=none; pct=100; rua=mailto:dmarc873245@bls.it; sp=none; aspf=r;

i principali parametri sono:

p=none che indica che la policy di fatto non è attivata, ma permette ricevere le informazioni per poi attivare la policy

rua=mailto:dmarc873245@bls.it indica l'email a cui inviare le informazioni

L'email da indicare è sempre quella indicata, ma va autorizzata la ricezione, chiedere al nostro servizio assistenza di essere autorizzati.

Le informazioni arriveranno periodicamente e saranno accessibili mediante questa funzione.

Per accedere cliccare sulla corrispondente opzione del menu funzioni.

Report DMARC							×
Dalla data : 01/03/2019 💼 Alla data : 03/04/2019 BLS Consulting	Dominio Cliente: Dominio Cloud-soluti	ons.it 🔻		🗹 Filtro Domini	o 💈	D X	
Server domain	Description	Message count	Server count	SFP compliance	DKIM compliance	DMARC compliance	
not found		4	1	0%	0%	0%	*
bls.it	Janusmail by BLS	2	1	100%	50%	100%	

Selezionare il periodo e il dominio da analizzare:

the second second second second		and the second						2
Dalla data : 22	/03/2019	Alla data : 29/03/2	019	Cliente:	BLS Consulting	Dominio	bls.it 🔻	

Si possono filtrare solo i record che hanno come dominio quello selezionato:

Filtro Dominio		¥
----------------	--	---

ciò riduce i dati da analizzare ma consigliamo successivamente di ripetere l'analisi senza filtro.

Server domain Description Message count Server count SFP compliance **DKIM compliance** DMARC compliance Janusmail by BLS 462 2 bls.it 98% 75% 100% 2 not found 320 0% 0% 0% sparkpostmail.com massmailing Sparkpost 221 1 0% 100% 100% aruba.it forwardes Aruba 36 14 0% 30% 30% 4 4 100% musvc.com massmailing MailUp 0% 100% 4 1 imanpack.it 0% 0% 0% tin.it 2 1 0% 0% 0% 2 1 0% 100% 100% seeweb.it hosting web & mail forwarders Microsoft Office 365 1 1 0% 100% 100% outlook.com

Questo è un esempio di report:

I server mittenti vengono raggruppati per dominio (l'indirizzo ip del server mittente viene risolto e viene estratto il dominio), per ogni dominio vengono riportati il numero totale di email inviate, il numero di server, la percentuale di server compliant con SPF, DKIM e DMARC.

Nel campo description è indicato la tipologia di server:

- Janusmail by BLS: indica i server utilizzati dal nostro sistema di mail security
- massmailing _____: indica i server utilizzati per spedire bulk email (newsletter)
- forwarders _____: indica i server che hanno rigirato (forward) le email ai vostri server

Le righe sono evidenziate in colori diversi utili per evidenziare a colpo d'occhio tipi diversi di server.

Gli amministratori possono cliccare sul tasto "+" per aggiungere una descrizione e scegliere il colore con cui evidenziare la riga.

Cliccando su una riga verrà visualizzato il dettaglio dei server:

Server ip add	PTR	Message cou	SPF result	SPF domain	SPF policy evaluated	DKIM result	DKIM domain	DKIM policy evaluated	Reporters
91.196.64.11	smtpout005.bls.it.	338	pass	cegos.it	pass	pass	cegos.it	pass	beiersdorf.com, linkedin.com, google.com, mmc.com, esa2.lyondellbasell.iphmx.com, mail1.magna.com, sercoglobal.com, bmwgroup.com, bp.local, dhl.com, airfrance.fr
91.196.64.11	smtpout005.bls.it.	112	pass	cegos.it	pass	fail	cegos.it	fail	google.com

Le righe evidenziate in verde sono compliant con SPF o DKIM e considerate valide per DMARC (si dice che i domini sono allineati)

Le righe non evidenziate in verde sono anomale e vanno analizzate. E' possibile che:

- non sia impostato correttamente l'SPF (se l'SPF domain corrisponde e l'SPF result è uguale a fail o softfail)

SPF result	SPF domain
softfail	bls.it

- il server non firma correttamente con il protocollo DKIM (se il DKIM domain corrisponde e DKIM result è uguale a fail) o più probabile la firma non è valida in quanto firmata da un server non autorizzato che non dispone della chiave privata corretta

DKIM result	DKIM domain
fail	bls.it

il server non firma con il protocollo DKIM (se il DKIM domain e DKIM result sono vuoti)

DKIM result	DKIM domain

L'SPF o il DKIM possono superare il test ma il dominio può non corrispondere (si dice che non è allineato):

SPF result	SPF domain	SPF policy evaluated
pass	preferredone.com	fail
DKIM result	DKIM domain	DKIM policy evaluated
pass	aseaps2019.com	fail

In questo caso si può trattare di una email ruotata (forwarded) da un altro server o può essere una truffa.

Se l'SPF non è impostato correttamente o le email non sono firmate con DKIM vanno sistemati per rendere compliant la policy, ad es.:

Server ip add	PTR	Message cou	SPF result	SPF domain	SPF policy evaluated	DKIM result	DKIM domain	DKIM policy evaluated
5.144.171.59	vm2737.cloud.seeweb.it.	2	pass	q360.it	fail	pass	cegos.it	pass

In questo caso le email provengono da un server in hosting, il DKIM è compliant e allineato è sufficiente per attivare la policy DMARC.

In quest'altro caso l'SPF non è compliant e neanche il DKIM quindi almeno uno dei due va sistemato:

Server ip address	PTR	Message cou	SPF result	SPF domain	SPF policy evaluated	DKIM result	DKIM domain	DKIM policy evaluated
62.149.158.245	smtpcmd01-d.aruba.it.	6	softfail	cegos.it	fail	fail	cegos.it/aruba.it	fail

Se analizziamo il record SPF notiamo che il server indicato non è elencato:

v=spf1 ip4:91.196.64.115 ip4:5.144.169.194 ip4:37.9.236.186 include:sparkpostmail.com ~all

Basta quindi aggiungere al record SPF l'indirizzo del server per renderlo compliant:

v=spf1 ip4:91.196.64.115 ip4:5.144.169.194 ip4:37.9.236.186 ip4:62.149.158.245 include:sparkpostmail.com ~all

Notare che vanno sistemati i server che per qualche motivo devono spedire le email (chiamiamoli server autorizzati) del vostro dominio, i server che invece sono utilizzate per spedire spam o email di phishing non vanno ovviamente resi compliant.

Una volta sistemati tutti i server autorizzati è possibile attivare una policy DMARC, es.:

_dmarc.bls.it IN TXT v=DMARC1; p=reject; pct=100; rua=mailto:dmarc873245@bls.it; sp=none; aspf=r;

Come si vede la policy è impostata per rifiutare le email da server non autorizzati (p=reject).

Quindi se si attiva questa policy, le email con il dominio bls.it verranno scartate se provenienti da server non autorizzati.

Una volta impostata la policy DMARC lo strumento è molto utile per identificare eventuali truffe che utilizzano i vostri indirizzi email.

Questo è un esempio:

Server ip add	PTR	Message cou	SPF result	SPF domain	SPF policy evaluated	DKIM result	DKIM domain	DKIM policy evaluated
79.7.70.130	s1.imanpack.it.	4	softfail	cegos.it	fail	fail	cegos.it	fail

Come si vede sono state spedite 4 email da un server non compliant con il record SPF e firmate in modo non valido con DKIM, quindi si tratta probabilmente di email di phishing che usano il dominio indicato.

AUTORESPONDERS

Questa opzione permette di specificare le caselle email su cui è attivo un sistema di risposta automatica.

Per accedere cliccare sulla corrispondente opzione del menu funzioni.

Autoresponnders				×
Email:	Cliente:	- 🔊 🕺 😤		
Email	Customer		Attivo	
assistenza@bls.it	000000 - BLS	Consulting	✓ Ⅲ	×
H 4 1 /1 P H				

Una delle funzioni già descritte in precedenza di Janusmail sono le whitelist automatiche, ovvero l'aggiunta automatica in whitelist del destinatario di un'email, che determina che le risposte di tale destinatario non verranno bloccate dal sistema antispam indipendentemente dal contenuto e dal server di provenienza.

Questo vale anche per le risposte automatiche, quindi se è attivo un sistema di risposta automatica su una casella, il mittente di ogni email spedita alla casella verrà aggiunto alla whitelist.

Per ovviare a questo inconveniente, è possibile specificare in questa tabella gli indirizzi email su cui è attiva una funzione di risposta automatica. Le email provenienti da questi indirizzi verranno in questo modo escluse dal sistema delle whitelist automatiche.

Non è necessario specificare le caselle su cui si attiva la funzionalità di fuori ufficio, queste email verranno riconosciute automaticamente e escluse dal sistema di whitelist automatiche.

MASS MAILING

Le funzioni descritte di seguito fanno parte del modulo Mass mailing, questo modulo permette inviare email transazionali o di marketing (bulk email, newsletter) garantendo la massima consegnabilità possibile.

A differenza delle email tradizionali hanno un sistema di spedizione completamente diverso basato sui seguenti principi:

- 1) ogni email ha un singolo destinatario, in pratica ogni email è unica, ovviamente è possibile inviare ad una lista di destinatari (lista di distribuzione) ma per ogni destinatario verrà generata una email unica
- 2) le email vengono inviate un numero limitato di volte, quindi in caso di problemi il sistema non continuerà a tentare di consegnare l'email per giorni, ma proverà solo un numero predefinito di volte
- 3) ogni destinatario viene controllato prima di inviargli una email, quindi se ha richiesto di non ricevere più email la spedizione verrà bloccata
- 4) in caso di problemi non verranno generate email di risposta multiple (bounce email) bensì alla conclusione della spedizione il mittente riceverà un report sullo stato di consegna delle email alla lista di distribuzione
- 5) nelle email è possibile aggiungere un link per richiedere la cancellazione dalla lista di distribuzione (unsubscribe link)

Questa modalità di spedizione favorisce la consegnabilità delle email, senza pregiudicare la reputazione del mittente.

CONTATTI

Questa opzione permette gestire il database dei contatti comune a tutte le liste di distribuzione.

Per accedere cliccare sulla corrispondente opzione del menu funzioni.

Contacts						×
Customer:	T	Email]	🕺 🄄	
Categoria: -	▼ Attivo ▼ Verificata	a consent request	consent response	▼ unsubscribe request ▼		
CustomerCliente	Email	Nome	Azienda	Stato	Attivo	
000000 - BLS Consulting	mbruse@blscloud.com	Mauro Bruseghini	B.L.S. Consulting S.r.I.		<	×
	м					

Le ultime tre icone in alto a destra permettono rispettivamente:

- inserire un nuovo contatto
- importare i contatti da un file in formato CSV
- esportare i contatti in formato CSV

Se un contatto viene disattivato non verranno inviate email anche se presente in una lista di distribuzione.

E' possibile associare un contatto ad una categoria, ciò permetterà creare velocemente liste di distribuzione estraendo tutti i contatti di una determinata categoria:

Contact insert		
Cliente:	BLS Consulting	T
Email address*:		
Nome:		
Cognome:		
Categoria 1º liv.:	cliente - Cliente effettivo	Category Management
Categoria 2º Liv.:	-	
Categoria 3º Liv.:	cliente - Cliente effettivo	
Azienda:	contatto - Contatto commerciale	
Indirizzo:		
Localita:	prospect - Possibile cliente	
Codice Postale:		
Provincia:		
Nazione:		
Telefono		
etichetta1		
etichetta2		
etichetta3		
Attiva:		
		Salva 🙆 Anr

Le categorie sono gerarchiche su tre livelli, è comunque possibile specificare dei valori solo per il primo livello od i primi due.

LISTE DI DISTRIBUZIONE

Questa opzione permette gestire le liste di distribuzione.

Per accedere cliccare sulla corrispondente opzione del menu funzioni.

0	DistributionList					×
	Nome lista:	Cliente:	Solo attive	۰ 🕺 🍳	2	
	Nome	Customer			Attivo	
	clienti 1	000000 - BI	LS Consulting		~ III	×

Cliccando sull'icona + è possibile aggiungere una lista di distribuzione, viene quindi visualizzata la pagina che permette aggiungere l'elenco dei destinatari della lista di distribuzione con diverse modalità, come illustrato nella prossima pagina.

Janusmail by B.L.S. Consulting - Manuale utente

BLS Consulting	v		
clienti 1			
inatari			
oio una colonna con relenco delle e rubrica contatti	emaii da importare. La prima riga deve conte	enere il utolo "email"	na il file e Importa
remi il bottone 'aggiungi' per aggiun	ngere tutti i contatti della categoria seleziona	ata -	🔻 👍 Aggiungi
Attivo	Numero di errori	Disabiliato	*
1	BLS Consulting clienti 1 clienti 1 matari plo una colonna con l'elenco delle e rubrica contatti remi il bottone 'aggiungi' per aggiur Attivo	BLS Consulting Image: Clienti 1 Imatari Imatari olo una colonna con l'elenco delle email da importare. La prima riga deve conta rubrica contatti remi il bottone 'aggiungi' per aggiungere tutti i contatti della categoria seleziona Attivo Numero di errori	BLS Consulting clienti 1 Imatari olo una colonna con l'elenco delle email da importare. La prima riga deve contenere il titolo "email" (freche selezion rubrica contatti rubrica contatti remi il bottone 'aggiungi' per aggiungere tutti i contatti della categoria selezionata [- Attivo Numero di errori Disabiliato

Cliccando su "Seleziona il file e importa" è possibile importare la lista dei destinatari da un file in formato CSV.

E' anche possibile importare i destinatari dal database dei contatti selezionando la categoria e cliccando su "Aggiungi".

Cliccando sull'icona "+" è possibile aggiungere un singolo destinatario nella lista.

Cliccando sull'icona Rubrica è possibile selezionare i destinatari dal database dei contatti.

E' anche possibile specificare delle regole dinamiche per il popolamento della lista di distribuzione:

regole dinamiche							
Categorie	Località	Provincia	Nazione	etichetta1	etichetta2	etichetta3	*
cliente -> italia							🗟 🗶
cliente -> spagna							B ×

Queste regole verranno usate per estrarre i dati dal database dei contatti quando inizia la spedizione di una newsletter.

Nell'esempio sopra sono selezionati i clienti di Italia e Spagna.

EMAIL TEMPLATE

Questa opzione permette gestire i modelli di email da spedire con la funzionalità di mass mailing.

Per accedere cliccare sulla corrispondente opzione del menu funzioni.

Customer:	Nome	Attivo 💽 🗴	BeePro new project	
Cliente	Nome	Descrizione	Attivo	
000000 - BLS Consulting	consenso1	email richiesta consenso GDPR	~ III	* *
000000 - BLS Consulting	News letter Zucchett	News letter Zucchetti. KOS	~ m	×
H 4 1 /1 P H				

Cliccando sull'icona + è possibile aggiungere un nuovo modello (template) di email. L'email va scritta in HTML o più semplicemente utilizzare il servizio BeePro per costruire il modello.

Cliccando sull'icona BeePro new project si accede direttamente alla creazione di un nuovo progetto, mentre cliccando su BeePro projects si accede alla gestione dei progetti, l'uso di questo sistema è illustrato di seguito.

Per accedere a BeePro utilizzare un browser e aprire la seguente pagina:

https://pro.beefree.io



Inserire quindi l'email e la password per accedere.

Janusmail by B.L.S. Consulting - Manuale utente

Verranno quindi visualizzati i progetti inseriti:



Cliccando su "Create a new project" verrà creato un nuovo progetto contenente uno o più messaggi (modelli di email)

Arial ▼ ≟ ▼	14px B I U S × ² X E<
II destinata	ario di questa email è [firstname] [lastname] di [company].
Annulla	Insert merge tags
	Email (Janusmail)
	First name (Janusmail)
	Last name (Janusmail)
	Company (Janusmail)

In questo modo è possibile personalizzare l'email inserendo nel testo l'indirizzo email del destinatario, il nome, il cognome o la ragione sociale dell'azienda.

Autorizzo Non autorizzo Arial 14px Ξ ¶¶ ¶ & 않 Special links ▼ Merge tags Autorizza (consenso privacy) Janusmail Annulla l'iscrizione | Dimentica i miei dati | Vermen I Non autorizza (consenso privacy) Annulla l'iscrizione A 💟 in 🖸 面 Dimentica i miei dati Verifica i miei dati

Inoltre si possono aggiungere dei link (con la funzione special links) che attivano diverse funzionalità:

Le funzioni sono:

- autorizza: da usare per link o pulsanti per autorizzare il trattamento dei dati (consenso privacy/GDPR), se il destinatario clicca su questo link/pulsante verrà memorizzata la data, l'ora e l'indirizzo IP di chi autorizza il consenso
- non autorizza: da usare per link o pulsanti per non autorizzare il trattamento dei dati (consenso privacy/GDPR), se il destinatario clicca su questo link/pulsante verrà memorizzata l'opposizione al trattamento nel database dei contatti
- annulla iscrizione: permette inserire un link per richiedere la cancellazione dalla newsletter
- dimentica i miei dati: permette inserire un link per richiedere la cancellazione dei propri dati (diritto all'oblio)
- verifica i miei dati: permette inserire un link per richiedere la verifica dei propri dati (verrà inviata una email con la richiesta al responsabile privacy dell'azienda)

E' inoltre possibile aggiungere un' immagine (che nelle email inviate risulterà invisibile) chiamata "dynamic image":

	Richiesta consenso	
B.L.S. Consulting s.r	Cliccare sul pulsante "autorizzo" per dare il consenso al trattamento dei dati. ••• Potete vedere l'informativa cliccando <u>qui</u> .	
	Autorizzo	Auto width
	Non autorizzo	20%
II destinatario di q	uesta email è [firstname] [lastname] di [company].	Align
<u>Annulla l'iscrizio</u>	<u>Dimentica i miei dati</u> <u>Verifica i miei dati</u>	Dynamic image Dynamic Url https://[dynamicimage]
		Dynamic Url https://[dynamic

Nell'esempio è evidenziata con la bandiera italiana, specificare nel campo Dynamic Url: https://[dynamicimage]

Inserire questa immagine è utilissimo, in quanto verrà visualizzata appena l'utente visualizza l'email, Janusmail memorizza quindi quando un utente legge effettivamente l'email e non solo se l'ha ricevuta.

ROWS

 My Projects 	 Projects Templates Settings 	
consenso1 1		
Order by: Created	Last updated Name	
	consenso1	Edit message 🔍
	Last edit 21 hours ago by Mauro Brusegnini	View details
0000		Send test
	✓ Collaborate	Create a copy
	A comporter	Move
		Export

Le opzioni permettono:

- editare il messaggio. creare una copia, muoverlo in un altro progetto, cancellarlo
- inviare una email di test con questo messaggio
- esportarlo, usare l'opzione di esportazione "Kepp my images online"



Questa opzione permette mantenere online le immagini inserite nella email, contribuendo a mantenere contenuta la dimensione dell'email favorendone la consegnabilità. Cliccare quindi su "Copy the HTML code":



Incollare quin	di il codice HTML	nel template i	nel campo Modello:
----------------	-------------------	----------------	--------------------

S11				
Cliente:	BLS Consulting			
nome*:	consenso1			
Descrizione	email richiesta consenso GDPR			
Link template:	https://pro.beefree.io/224096/201271/389391/message	Open template	BeePro new project	🛃 BeePro projects
Oggetto*:	Richiesta consenso			
<pre>Modello <!DOCTYPE html PUBLIC</pre> </pre>	"-//W3C//DTD XHTML 1.0 Transitional //EN" "http://www.w3.org/TR/x	html1/DTD/xhtml1-trans	sitional.dtd">	

Incollare anche il link al template nel campo Link template, cliccando poi su Open template si potrà andare direttamente in gestione del modello su BeePro.

-

Il link da copiare è l'url visualizzato nel browser per la pagina seguente:



Questa opzione permette schedulare l'invio delle email di tipo mass mailing.

Per accedere cliccare sulla corrispondente opzione del menu funzioni.

Pianificazione invio newsletter						×
Customer:	Name:			Active	🞗 🍳	÷
Cliente	Autore	Modello A	Modello B	Lista di distribuzione	Attiva	
000000 - BLS Consulting	mbruse@bls.it	consenso1		clienti 1	Inviata	e 🔤 🔤
000000 - BLS Consulting	dscappini@bls.it	consenso1		clienti 1	Inviata	2000
000000 - BLS Consulting	dscappini@bls.it	consenso1		clienti 1	Invio bloccatto	e 🔤 🔿
000000 - BLS Consulting	mbruse@bls.it	consenso1		clienti 1	×	¥ [∞] ⊕ ¢

Cliccando sull'icona + è possibile aggiungere una nuova schedulazione.

A fine di ogni riga sono presenti le icone per:

- vedere lo stato di di spedizione di una newsletter
- bloccare immediatamente l'invio di una spedizione in corso
- inviare una email di test a dei destinatari selezionati

Cliente:	BLS Consulting		•	
Modello A		🔎 🗶		
Modello B		🔎 🗶		
Lista di Distribuzione				<i>»</i> ×
Pianificazione (date e ora)	16/04/2019 15:00		31	
Richiesto Consenso	yes •			
Unsuscrive Link	yes •			

Selezionare quindi un modello (email template), è possibile specificarne due (modello A e B), se se ne specificano due metà delle email verranno spedite con un modello e metà con l'altro. Sarà quindi possibile valutare l'efficacia dei due modelli di email verificando quanti destinatari si "convertiranno" con un modello e quanti con l'altro.

Selezionare quindi la lista di distribuzione a cui inviare l'email e la data/ora di inizio spedizione.

Se poi il flag "Richiesto consenso" viene posto uguale a yes, le email verranno inviate solo ai contatti che avranno espresso il consenso.

Se viene messo a yes il flag Unsuscribe Link, nell'intestazione della email (headers) verrà aggiunti il link per permettere l'annullamento dell'iscrizione alla newsletter.

Ovviamente questi due flag vanno impostati in base al tipo di email da inviare, ad es.:

- per una email di richiesta consenso privacy/GDPR andranno posti entrambi a no
- per una email di marketing andrà posto a yes il flag "Richiesto consenso" e a no il flag "Unsubscribe Link"
- per una newsletter andranno posti entrambi a yes

A conclusione della spedizione delle email alla lista di distribuzione verrà inviato al mittente una email che permette accedere al report delle spedizioni.
Shipments Details					3
Stato 🗹 Da spedire 🛛 Spedite	🕑 Invio fa	llito Des	tinatario		🔎 💢
Destinatari	Inviata il	Stato	Stato Dett.	Tentativi	Prossimo inv
dscappini@asm.pv.it	2019-05- 30 18:00:49.0	NOUSER	Bad destination mailbox address	10	2019-05-30 18:30:10.0
dscappini@gmail.com	2019-05- 30 14:49:10.0	SENT	Mail succesfully sent to dscappini@gmail.com	1	2019-05-30 14:48:30.0

Sarà possibile selezionare spuntando le apposite caselle:

- le email ancora da spedire
- le email già spedite
- le email che hanno avuto problemi di spedizione

Janusmail dispone di diversi sistemi di statistiche per monitorare il funzionamento del sistema. Queste funzioni sono disponibili per gli amministratori dei server e quindi esulano da questo manuale.

È però possibile, per un amministratore dei server, attivare l'invio giornaliero delle statistiche agli amministratori dei clienti.

L'email viene spedita poco dopo le 4:00 e riporta sia le statistiche delle ultime 24 ore sia le statistiche dell'ultima settimana. Segue un esempio di email:



Le statistiche comprendono i seguenti grafici:

Volume di email gestite ogni 10 minuti (report giornaliero) od ogni ora (report settimanale) per mailrelay



Tempo medio di routing (in secondi) del messaggio di email



Indica il tempo complessivo, comprensivo del tempo di ricezione, analisi e consegna al server di destinazione.

Janusmail by B.L.S. Consulting - Manuale utente

Tempo suddiviso per macro fasi in secondi



Janusmail inizia a processare l'email mentre viene consegnata (azzurro), poi esegue una prima serie di controlli (giallo), salva l'email in coda e quindi esegue i controlli che richiedono più tempo di elaborazione (verde).





Se il server si sovraccarica, normalmente aumentano le fasi di controllo antivirus e antispam.

Un aumento molto limitato nel tempo della sola fase di controllo antivirus clamav o dell'antispam possono significare un aggiornamento delle firme in corso e conseguente interruzione momentanea del servizio (normalmente di qualche decina di secondi.)

Tempo di consegna in secondi



In azzurro è indicato il tempo medio di consegna per tutti i clienti.

Se ci sono problemi di consegna (tempi superiori ai 15 minuti di una email) viene riportato anche il grafico del cliente (in questo caso il nostro) per indicare una anomalia di consegna.

Normalmente le anomalie di consegna sono dovute a problemi di raggiungibilità del server di posta di destinazione causati da backup in corso, interruzione di servizio o per mancanza di connettività.

SOMMARIO

DAS	HBOARD	2
RICERCA AVANZATA		11
ELE	NCO EMAIL RICEVUTE/INVIATE	12
	Spam e newsletter	14
	Policy blocked	15
	Scam o virus	15
	ОК	16
	Whitelisted	16
BAR	RA CONTEGGIO EMAIL	17
DET	TAGLI EMAIL	19
DET	TAGLIO EMAIL STORICHE	38
POL	ICIES	40
	RICERCA POLICIES	42
	INSERIMENTO MANUALE delle POLICIES	43
	ATTACHMENT POLICY	47
	MANUAL BLACKLIST	51
	MANUAL WHITELIST	52

Janusmail by B.L.S. Consulting - Manuale utente	117/118
MAX EMAIL SIZE POLICY	53
PERIODIC REPORT POLICY	54
SPAM SCORE POLICY	65
POLICIES AUTOMATICHE	67
Automatic Whitelist Sender to Receiver	67
Automatic Whitelist Domain Sender to Domain Receiver with not fail SPF	67
DURATA E SCADENZA DELLE POLICIES AUTOMATICHE	68
DOMAIN PREFERENCES	69
GESTIONE ALIAS	71
SENT EMAIL MONITOR	73
REGOLE ANTISPAM	78
BILLING	80
ALLEGATI PERICOLOSI	82
THREATS INDICATORS	83
DMARC REPORT	85
AUTORESPONDERS	90
MASS MAILING	92
CONTATTI	93
LISTE DI DISTRIBUZIONE	95
EMAIL TEMPLATE	98

Janusmail by B.L.S. Consulting - Manuale utente	118/118
SCHEDULAZIONE EMAIL	106
STATISTICHE	110
SOMMARIO	116