Visura
TINEXTA GROUP

Linea prodotto
Digital Trust

Legalmail Security Premium

Versione 1.0 giugno 2023

www.visura.it

Sommario

Legalmail Security Premium 3
Definizioni e abbreviazioni 3
Caratteristiche 3
Sandbox sugli allegati al messaggio 4
Malware Detection sul corpo del messaggio 4
Webmail phishing protection 4
Flusso di verifica e-mail 5
Flusso standard 5
Flusso premium 6

Legalmail Security Premium

Legalmail Security Premium è un servizio di produzione InfoCert distribuito da Visura, nato per alzare il livello della sicurezza e per fronteggiare l'incremento degli attacchi informatici, sempre più veicolati tramite messaggi di posta elettronica. Questo nuovo servizio, per ottemperare anche alle nuove regole introdotte da Agid, potenzia la piattaforma PEC grazie a tre nuove soluzioni Antivirus che garantiscono i più alti standard di sicurezza che identificano con maggiore precisione eventuali minacce veicolate tramite le e-mail.

Definizioni e abbreviazioni

Acronimo	**Descrizione**
PEC	Posta Elettronica Certificata
PO	Posta Ordinaria
SMTP	Simple Mail Transport Protocol
PA	Punto di accettazione messaggi PEC (SMTP della posta in uscita)
PR	Punto di Ricezione messaggi PEC (SMTP della posta in ingresso)
PdC	Punto di Consegna (posizione delle mailbox utente)
Signature	Sequenza di caratteri alfanumerici che identificano un determinato oggetto
API	Application Programming Interface (strumenti di provisioning)

Caratteristiche

Oltre ai servizi di sicurezza standard previsti per le PEC Legalmail, Legalmail Security Premium applica tre distinte tipologie di servizio:

- Sandbox: analizza gli allegati come i file Office (docx, xlsx, ppt, ecc.), i file PDF, i file compressi (zip, gz, ecc.).
- Malware Detection: analizza i link presenti nel corpo del messaggio a livello di motore PEC.
- Webmail Phishing Protection: analizza i link presenti nel corpo del messaggio a livello di webmail.

Sandbox sugli allegati al messaggio

La Sandbox effettua due tipi di verifiche: l'analisi statica e l'analisi dinamica.
L'analisi statica prevede il lancio di svariati tool sia interni che di terze parti per l'identificazione di sample assimilabili ad attività sospette utili alla classificazione degli oggetti in "clean" o "malicious".
Questo tipo di analisi viene effettuata su macchine virtuali condivise e già istanziate a tale scopo.
L'analisi dei documenti Office/OpenOffice prevede le seguenti operazioni:

- Riconoscimento di tentativi di VBA-stomping
- Riconoscimento di progetti nascosti e altre caratteristiche sospette quali la presenza di template dinamici o utilizzo di Dynamic Data Exchange (DDE)
- Analisi delle macro attraverso MacroRaptor
- Analisi del documento attraverso olevba/oletools

Per i PDF vengono rilevati indicatori sospetti quali presenza di codice Javascript, documenti malformati, presenza di form XFA sospetti, tentativi di exploit vari come heap overflow.

Per l'analisi degli eseguibili (exe o dll) viene intrapreso il riconoscimento degli indicatori sospetti negli header, di firme digitali compromesse o invalide, riconoscimento di packer e compiler, identificazione di combinazioni sospette di import, identificazione di stringhe sospette, ecc.
Se il file è protetto da password, il sistema tenta di aprirlo ricercando la password nel corpo del messaggio.

Malware Detection sul corpo del messaggio

La componente Malware Detection viene attuata durante la fase di ricezione della mail da parte degli SMTP di front-end della PEC Legalmail, dove il contenuto viene analizzato alla ricerca di Signature note.
Se i link presenti nel messaggio sono segnalati come malevoli la mail non viene consegnata.

Webmail phishing protection

La componente ***Webmail Phishing Protection*** è scatenata dalla lettura della mail da parte dell'utente via web, ed è attuata mediante l'utilizzo di API specifiche che le consentono di essere integrata nella webmail Legalmail; essa in pratica si interpone tra l'utente e l'endpoint a cui puntano i link presenti nella mail.
Può capitare infatti che, al momento del recapito del messaggio nella *Inbox* dell'utente, un link non risulti segnalato come malevolo, ma, dato che gli elenchi dei link compromessi si aggiornano

frequentemente, è molto probabile che quando l'utente leggerà la mail il link presente risulterà segnalato.
Quindi se il cliente accede alla sua casella di posta tramite Webmail e tenta di cliccare sul link successivamente segnalato come compromesso, il modulo di protezione che si interpone tra l'utente e l'URL di destinazione blocca l'accesso alle risorse malevoli, presentando una pagina che indica che è stato effettuato l'intervento.
Di seguito alcune specifiche relative al servizio:

- Ricerca dettagliata in threat intelligence
- Matching di regole Adware su URL
- Analisi del testo del link e del contesto delle e-mail per identificare possibili attacchi BEC, Scam e phishing

Flusso di verifica e-mail

L'analisi della mail viene effettuata secondo un flusso specifico che tende a minimizzare i tempi di delivery, senza ridurre l'accuratezza della verifica.
In base ai livelli di servizio scelti dal cliente, per la parte relativa ai servizi di Antivirus, esistono due flussi principali:

- Standard
- Premium

Di seguito sono indicate le varie fasi di analisi per entrambe le tipologie.

Flusso standard

Il *flusso Standard* prevede che la fase di analisi sia eseguita secondo la seguente sequenza:

1) Un messaggio di posta elettronica viene inviato ai PA o consegnato ai PR
2) Il messaggio ed i suoi allegati vengono sottoposti alla scansione di Kaspersky
3) In caso di contenuto malevolo viene inviata ricevuta di non accettazione per virus, in caso di PA, e ricevuta di mancata consegna per virus in caso di PR. In caso di PO la mail viene semplicemente scartata.
4) Il messaggio ed i suoi allegati vengono sottoposti alla scansione di Sophos
5) In caso di contenuto malevolo viene inviata ricevuta di non accettazione per virus, in caso di PA, e ricevuta di mancata consegna per virus in caso di PR. In caso di PO la mail viene semplicemente scartata.
6) Viene verificato se il recipient ha sottoscritto l'opzione "Flusso Premium":
   - In caso affermativo, si procede con il flusso Premium

- In caso contrario la mail viene inviata al destinatario, in caso di PA, o consegnata in casella, in caso di PR.

Flusso premium

Il *flusso securizzato Premium* è il servizio che prevede, oltre alle analisi effettuate dal flusso standard, ulteriori step di verifica malware sia prima della consegna della mail in casella, che successivamente in fase di lettura della mail tramite Webmail.

Di seguito la sequenza delle operazioni relative alla fase di consegna in INBOX:

1) Il messaggio segue i passi del flusso standard fino alla verifica della sottoscrizione dell'opzione di flusso premium
2) Gli allegati della mail con estensione gestita, ed i link presenti nel corpo del messaggio, vengono sottoposti all'analisi sandbox che esegue una prima verifica di corrispondenza degli hash nei suoi database e una verifica sul codice presente nei file. Successivamente viene eseguita l'analisi statica dei file su di un pool di macchine virtuali utilizzando dei tool specifici.
3) In caso in cui il risultato dia evidenza di un comportamento malevolo, o che uno dei link presenti nella mail sia segnalato come pericoloso, la mail non viene recapitata e viene inviata ricevuta di non accettazione per virus, in caso di PA, e ricevuta di mancata consegna per virus in caso di PR. In caso di PO la mail viene semplicemente scartata.
4) Successivamente il messaggio viene analizzato dal l*ayer* di sicurezza, che confronta le *signature* del messaggio ed i link presenti, con quelle riportate nei suoi database.
5) In caso di contenuto malevolo viene inviata ricevuta di non accettazione per virus, in caso di PA, e ricevuta di mancata consegna per virus in caso di PR. In caso di PO la mail viene semplicemente scartata.
6) Se dalle verifiche precedenti non vengono rilevate anomalie, la mail viene inviata al destinatario, in caso di PA, o consegnata in casella, in caso di PR.

Di seguito la sequenza delle operazioni relative alla fase di lettura della mail tramite interfaccia webmail di InfoCert, con l'integrazione della componente di sicurezza:

1) L'utente accede alla webmail
2) L'interfaccia WEB verifica, tramite API, che l'utente abbia sottoscritto l'opzione Webmail Phishing Protection.
3) L'utente visualizza una mail e clicca su uno dei link presenti.
4) L'interfaccia WEB tramite delle chiamate API, verifica che non sia stato già segnalato come malevolo, e "segue" il link indicato.

5) Se il layer di sicurezza identifica un'attività anomala generata dall'endpoint a cui puntava il link, ne impedisce l'accesso all'utente visualizzando una pagina in cui è dettagliato il motivo del blocco.
6) Nel caso in cui non sia rilevata attività anomala, l'output della pagina Web viene restituito all'utente.