CONTROMISURE SU RECENTE CAMPAGNA MALWARE VERSO IL SISTEMA PEC

Nelle ultime settimane si è assistito ad un forte incremento dell'invio di spam, contenente malware, da parte di attaccanti molto sofisticati e organizzati, verso il sistema PEC nel suo complesso.
Sono state infatti riscontrate nuove casistiche di virus che coinvolgono l'intero sistema della PEC e che gli antivirus di mercato, presenti nelle piattaforme dei diversi gestori PEC, intercettano in ritardo in quanto non ancora note nelle proprie definizioni o varianti di codice malevole.

In particolare, InfoCert (così come i principali gestori) utilizza come antivirus la soluzione commerciale Sophos PureMessage che è basata su firme dei virus noti.

Per aumentare la reattività a nuovi attacchi ed arginare questo crescente fenomeno InfoCert, in piena collaborazione e sinergia con tutti gli altri gestori PEC, ha attivato tutta una serie di contromisure e ha intrapreso passi operativi e tecnologici che porteranno sicuri benefici nelle prossime settimane.

Prima di approfondire le misure che si stanno definendo, è opportuno ricordare che molte delle difficoltà attuali dipendono dalla natura del sistema PEC, le cui norme sono molto dettagliate dal punto di vista tecnico e oggi, proprio a causa del periodo storico in cui sono state definite, portano a rallentare il processo di identificazione e di circoscrizione del malware; ad esempio la normativa attualmente in vigore:

- non prende in considerazione MALWARE diffusi attraverso link all'interno del corpo del messaggio utente, ma soltanto VIRUS trasmessi come allegati;
- non prevede la casistica di messaggi di SPAM veicolati dall'interno del circuito PEC

Per tale ragione i gestori PEC hanno condiviso con AGID – Agenzia per l'Italia Digitale – una proposta volta a indicare **misure più aggressive e coordinate di contrasto al malware**.

Le prime misure, che verranno attuate nel brevissimo a fronte dell'avallo di AGID, sono **procedure di mutua assistenza** tra gestori PEC, una task force per il repentino scambio di informazioni ogni qual volta si verifichi un nuovo attacco:

a) condivisione URL riconosciuti come malevoli (contenuti nei messaggi PEC) per permettere ai gestori di metterli in black-list ed arginarne la diffusione;
b) condivisione di tipologie di PEC malevole;
c) condivisione indirizzi caselle compromesse tra i gestori;
d) Indication Of Compromise e payload malevoli in generale;
e) condivisione di analisi comportamentali relative a determinate tipologie di attacco.

L'EVOLUZIONE DELLA SICUREZZA PEC

Per un irrobustimento significativo del sistema PEC sarà necessario fare perno **sull'estensione del concetto di PEC virali e adeguamento tecnologico per meglio contrastare i virus/malware "zero day"**.
Prima di poter procedere all'evoluzione tecnologica, sono però propedeutiche alcune **modifiche sostanziali alle attuali Regole Tecniche sulla trasmissione PEC** (vedi il Decreto 2 novembre 2005 e relativo allegato) e quindi occorreranno tempi relativamente più lunghi per il recepimento in

normativa e relativa attuazione.

Anticipiamo alcune proposte di modifica delle Regole Tecniche avanzate dai gestori che verranno valutate da AGID:

- Ampliare il concetto di PEC contenenti virus ai vettori malevoli di nuova generazione, permettendo ai gestori di inserire, nella catena di protezione della messaggistica PEC, software antispam/anti-malware in aggiunta ai software antivirus già presenti nei sistemi PEC.
- Consentire al gestore la non accettazione o la mancata consegna per VIRUS (Malware) ammettendo l'eventualità di possibili casi di falsi positivi, attraverso gli attuali modelli comportamentali (non accettazione per virus, avviso di rilevazione virus, mancata consegna per virus) dettagliando il motivo e le cause della classificazione come malevolo.
- Consentire il superamento degli attuali SLA su messaggi PEC con contenuti ritenuti "sospetti", ammettendo, esclusivamente per essi, dei tempi di accettazione/presa in carico/consegna più ampi. In tale lasso di tempo il gestore avrebbe la possibilità di innescare appositi processi di approfondimento, gestendo nel modo opportuno i messaggi riconosciuti come malevoli.

ISTRUZIONI OPERATIVE PER IL CLIENTE/UTILIZZATORE

Quando si riceve un messaggio (PEC o da mail tradizionale) che contiene un link è opportuno verificare il contenuto del messaggio e controllare con attenzione l'anteprima dell'url.

Se, inviando un messaggio PEC, il mittente riceve un *avviso di non accettazione per virus informatici*, significa che il messaggio è stato bloccato dal gestore PEC in quanto malevole, e la stazione di lavoro o il client di posta potrebbero essere compromessi.

Per aumentare il livello di sicurezza è necessario che il cliente installi, su tutte le postazioni client, un antivirus/antispam di ultima generazione; in tal modo:

- il messaggio viene verificato all'apertura dello stesso e quindi in un momento successivo rispetto al check effettuato dall'antivirus PEC (pertanto con maggiori probabilità che il virus sia stato nel frattempo catalogato);
- possono essere applicate euristiche (se previste dall'antivirus)
- può essere verificato il contenuto di eventuali link presenti nel corpo del messaggio o negli allegati.

Quando i sistemi antivirus Legalmail verificano che, da una casella Legalmail, viene inviato virus/malware, vengono applicate automaticamente la seguente policy di sicurezza:

- viene bloccata la password della casella per impedire l'accesso e quindi l'invio di messaggi contenenti virus,
- viene inviata, al contatto del cliente, un avviso dove viene comunicato il blocco della password e vengono descritti i passi operativi per pulire la stazione di lavoro
- successivamente viene inviata, sempre al contatto del cliente, mail contenete il token per definire una nuova password della casella PEC