## Ambiente

Il cliente ha presentato una serie di problematiche[1] relative al proprio sistema antispam *eSafe*. Tali problematiche erano state già in parte analizzate sia dal cliente stesso, sia dal vendor (attraverso uno scambio di mail), il quale ha anche presentato una serie di patch e soluzioni che non sembrano comunque aver risolto il problema.
In seguito alle analisi di cui sopra, la causa del blocco sembra essere da attribuire al sistema eSafe (e non alle infrastrutture di contorno come apparati di rete, uplink, etc.).
Il cliente ha inoltre manifestato un certo malcontento dovuto al tempo intercorso fra la sua segnalazione e l'intervento. Inoltre il cliente attendeva uno specialista della tecnologia eSafe, avendo già notificato che la causa del blocco del sistema di posta era causata dal prodotto stesso.
Purtroppo, durante l'intervento non è stato possibile validare le ipotesi del cliente, dato che per tutta la giornata di presidio **il blocco non è avvenuto e non è replicabile**.

Come *work-around* al blocco della posta in uscita, il cliente ha creato un proprio script di monitoraggio che gira sul box eSafe (distribuzione proprietaria Linux). Questo script effettua un riavvio generale del servizio eSafe ogni qual volta la coda dei messaggi di posta in uscita supera una certa soglia. Proprio a causa del fatto che il sistema permette di aggirare il blocco totale della posta[2] tramite il riavvio del servizio, non è stato possibile determinare con esattezza quando è stata l'ultima volta che il sistema eSafe ha presentato l'anomalia identificata dal cliente come blocco.

## Vincoli e considerazioni

1. L'analisi si basa sulle informazioni rilasciate dal personale Koelliker senza una verifica sul campo;

[1] La più importante fra i malfunzionamenti rilevati consiste nel blocco del servizio e quindi nell'impossibilità di spedire mail.

[2] Il cliente riferisce che questo workaround causa un reset delle connessioni attive al momento del riavvio sul box E-Safe. Non è stato possibile indagare ulteriormente.

2. Essendo il prodotto E-Safe proprietario, non è possibile effettuare analisi approfondite della piattaforma;
3. Il cliente è infastidito in merito al servizio fornito fino ad ora ed è molto restio a lasciare eseguire analisi su aspetti che non siano quelli legati ad E-Safe;
4. Il problema non è ripetibile e quindi è assai difficile riuscire ad identificarne la causa precisa se non a seguito di log completi e mirati e di un presidio più continuativo;
5. Il cliente ha espressamente richiesto la presenza di personale certificato E-Safe.

## Attività

L'attività della giornata è cominciata con un'intervista con il cliente per determinare con esattezza la natura del problema, le condizioni di innesco, etc. Dopo la raccolta di informazioni si è passati ad un'analisi del sistema che con maggiore probabilità è la causa del blocco: il server eSafe.
Essendo però un server in produzione, e montando un sistema operativo linux-based customizzato dal vendor (privo quindi dei normali tool di analisi disponibili sulle distribuzioni più comuni) non è stato possibile effettuare un'analisi approfondita del comportamento del server che comunque, durante tutto il periodo del presidio, sembra aver funzionato correttamente.
L'attività si è conclusa con la creazione di uno script, fornito al cliente, da lanciare al momento del prossimo blocco del sistema eSafe. Tale script effettuerà la raccolta di alcune informazioni relative allo stato del sistema (sempre secondo i limiti di cui sopra) al momento del malfunzionamento. Questo può aiutare il cliente ad avere una maggiore consapevolezza della causa del problema, ed anche il vendor per la creazione di un eventuale bug-fix.

## Conclusioni

Badandosi **unicamente** sulle informazioni fornite dal cliente (per i motivi di cui sopra), il personale tecnico di Hacking Team ritiene che il blocco sia dovuto ad un consumo di risorse di sistema da parte del software eSafe (in alcune condizioni non determinabili a priori). Tale consumo di risorse sembra focalizzato non tanto sulla memoria o sullo spazio disco, quanto sul numero di connessioni effettuate. Questo elevato numero di connessioni sembra "paralizzare" lo stack TCP/IP della macchina, impedendo non solo il corretto funzionamento del sistema antispam, ma anche

l'esecuzione di altri comandi che effettuano connessioni di rete (es: telnet). È inoltre possibile ipotizzare che l'elevato numero di connessioni aperte non sia riconducibile al sistema antispam, quanto al sistema di web filtering montato sulla stessa macchina; questa è ovviamente solo una supposizione, dato che il personale tecnico di Hacking Team non ha visibilità delle *internals* del prodotto.

Il vendor (sulla base delle e-mail da lui inviate) sembra comunque non voler ricondurre un eventuale blocco dello stack TCP/IP al prodotto eSafe. Va però ricordato che il sistema operativo (configurazione, moduli kernel proprietari, etc.) viene fornito **unitamente** al prodotto e quindi, sia che la soluzione necessiti di un bug-fix del software eSafe, sia che necessiti unicamente di un intervento sistemistico, **deve essere compito del vendor mettere in atto le opportune contromisure**.

Il cliente fornirà l'output dello script consegnato a conclusione delle attività quando (e se) il blocco si verificherà nuovamente. A questo scopo Hacking Team ha consigliato di disabilitare lo script di work-around creato dal cliente per "facilitare" un nuovo blocco del sistema e poter avere quindi più dati su cui effettuare un'analisi.