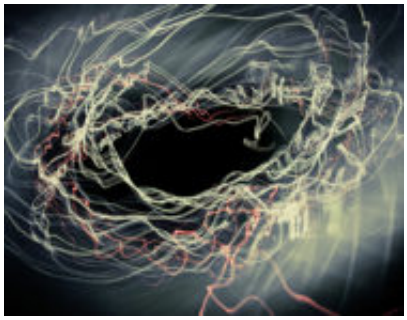
# A case history: come ho risolto un sabotaggio interno

**Author :** Vincenzo Digilio

**Date :** 8 maggio 2018



Secondo una delle ultime statistiche relative all'anno 2017[1] gli attacchi informatici con finalità di sabotaggio hanno riscontrato un incremento del 46,5% rispetto all'anno precedente. Generalmente non nutro una grande fiducia nelle statistiche, ma di questo trend ho potuto constatare personalmente la crescita, durante uno dei nostri primi Incident Case[2].

06:17 di una grigia mattina di Luglio. L'orario della chiamata ed il numero da cui proveniva non lasciavano presagire nulla di buono. dissero dall'altra parte della cornetta.
ICR-T:S è l'acronimo che utilizziamo per identificare un **I**ncident **C**ase: la prima tripletta identifica la categoria e la gravità del caso (**R**ed in questo caso, cioè la più alta nella scala) **T** sta per Type (tipologia); ed ovviamente si trattava di **S**abotaggio. Vale a dire, in altre parole, che da lì a qualche ora sarei dovuto salire su un aereo diretto a Vienna, perché il cliente con diverse sedi in tutto il mondo, era stato vittima di un attacco dall'interno.

Un Incident Case è un po' un terno al lotto. Ovviamente conoscenza del campo ed esperienza ricoprono un ruolo importantissimo, ma quando c'è una chiamata di questo tipo, fondamentalmente è già troppo tardi. Non si ha quasi mai la certezza di riuscire a mitigare o risolvere la situazione, la maggior parte delle volte è necessario pensare fuori dagli schermi e conoscere le stesse metodologie utilizzate dall'attaccante.

Fra le dieci mail che avevo ricevuto quella mattina di biglietti aerei prenotati e alberghi, cercai l'unica di cui avevo bisogno che proveniva dalla mail del mio socio con l'indirizzo https della chat criptata[3] su cui sarei entrato per ricevere il rapporto dell'intervento.

I Network System Administrator di una società di ricerche con filiali in tutto il mondo, avevano blindato gli accessi ai Domain Controller, cancellato quasi tutti i dati aziendali nelle share folders, disattivato i backup e chiuso l'accesso alla struttura vera e propria della rete attraverso i Domain Controller Virtualizzati con struttura Hyper-V. Erano già intervenuti un paio di Ingegneri cercando di sbloccare la situazione, ma senza avere successo. Nella mia mente si palesarono diversi scenari. La riuscita o meno di questo intervento era grossomodo nelle mani di chi aveva portato l'attacco: quanto erano stati accurati? Avevano messo in piedi tutte le contromisure adeguate affinché la situazione non fosse più ripristinabile?

Avrei avuto accesso fisico alla struttura e quindi ai loro domain controller all'interno del DataCenter. L'accesso diretto alle macchine è in genere un grosso vantaggio. Probabilmente la ritorsione da parte del settore IT era avvenuta di conseguenza alla notizia della chiusura di quella struttura di ricerca.

Atterrai all'Aeroporto Internazionale di Vienna alle 11:50 circa. Lì mi attendeva direttamente l'Amministratore Delegato dell'azienda, ergo potete comprendere quanto critica fosse la situazione. Mi raccontò brevemente che cosa era successo e di come da un giorno all'altro l'intera struttura fosse stata bloccata, senza riuscire più ad effettuare il log-in su di un singolo client. Tutte le password erano state ovviamente cambiate. Tuttavia, a parte chiacchiere, i dettagli tecnici di cui in realtà avevo bisogno non poteva fornirmeli.

La Server Room era più piccola di quanto mi aspettassi, il rec principale montava diverse blade: quella centrale era quella che mi interessava. Accesi il domain controller, e dopo qualche minuto mi apparve la schermata di log-in di Windows Server 2008 R2. La mia prima domanda aveva trovato risposta: nessuna chiave da inserire di decriptazione[4], quindi con molta probabilità gli Hard Disk non erano stati criptati, era un passo avanti. Se gli Hard Disk fossero stati criptati senza un Backup, avrei molto probabilmente chiesto di prendere il prossimo aereo per tornare in Italia. Decisi quindi di provare un approccio diretto presi dallo zaino una delle mie chiavette USB con una distro di Debian Custom per tentare di resettare la password di log-in al server. Il Bios della DELL mi presentò il mio primo ostacolo nel momento in cui premetti F9 per il Boot USB: Password…ed il puntatore lampeggiante. Inutile pensare di decodificare la password, avrei dovuto tentare di resettarla manualmente. Tolsi corrente alla blade, scollegando ogni cavo di alimentazione e lo liberai dalle slitte del rec rimuovendolo dall'unità centrale. Tenni premuto il pulsante di accensione al fine di scaricare qualsiasi carica residua presente nei condensatori della scheda madre, attesi qualche secondo e cominciai a svitare le viti del case. La polvere aveva formato uno strato ben compatto, pulii con una bomboletta ad aria compressa l'interno e prima di toccare qualsiasi componente scaricai la mia carica elettrostatica toccando la griglia metallica del pannello alla mia sinistra.

Generalmente il jumper per il reset del BIOS sulla scheda madre è composto da due pin, quasi sempre i produttori usano caratterizzarli con il colore blu e sono locati vicino il CMOS della batteria; una volta identificati è sufficiente spostare il jumper di un pin oppure rimuoverlo completamente e la password viene resettata. Ma ovviamente non era questo il caso: nessun pin-reset. Le cose si complicavano. Certo, avevo sempre l'opzione di rimuovere la batteria e procedere così al ripristino delle impostazioni di default, ma non volevo ancora percorrere questa strada. Un reset completo del BIOS avrebbe potuto comportare la perdita di alcune impostazioni fondamentali per il corretto avvio del domain controller (come le impostazioni delle memorie di massa). A giudicare dalla schermata d'inserimento password la versione del bios era vecchia e non veniva aggiornata da diverso tempo. Decisi di tentare la fortuna e procedere sfruttando una vecchia backdoor presente su alcune versioni del BIOS non aggiornate: inserì la password del bios errata numerose volte in maniera consequenziale, resettando diverse volte il sistema, alla fine ottenni il messaggio che avevo sperato: "System Disabled" ed il codice dell'errore. Il codice che ottenni era il punto chiave, accessi il mio laptop e mi collegai al sito bios-pw.org/ inserendo così le cinque cifre decimali dell'errore, ottenni quattro password, la terza si dimostrò quella corretta. Ero dentro il bios del domain controller[5].

Inserii la chiavetta USB e questa volte era solo una questione di tempo e di scelta prima che fossi riuscito a penetrare nel server. Avviai dall'USB eseguendo il boot del sistema da una distro live di debian, l'ormai "commerciale" versione di BackTrack...Kali Linux. Come pensavo i dischi erano in RAID, avrei dovuto montarli sulla distro, non era un grosso inconveniente, ma mi avrebbe fatto perdere del tempo. Decisi allora di provare con un metodo più semplice: creai una versione di boot di Windows Server su chiavetta USB (lettori ottici non erano presenti sulla macchina), avviai in repair mode la macchina ed a questo punto avevo i dischi già montati dal controller raid, da qui in poi avrei proseguito utilizzando la console di windows. Individuai il disco contenente l'installazione del Sistema Operativo e da qui mi mossi in direzione della cartella System32 effettuai un rename del file sethc.exe originale, rinominando successivamente cmd.exe in sethc.exe quello che ottenni era un shell con Elevated Pivilage nel momento del log-in, premendo semplicemente il tasto shift cinque volte. In parole più semplici, avevo sfruttato una vulnerabilità del Sistema Operativo: premendo cinque volte il tasto shift del vostro terminale vi apparirà la finestra "Sticky Keys" che non è altro che una feature di Windows che permette un sequenziamento dei tasti invece che premerli contemporaneamente (tipo il famoso ALT + CTRL + CANC). È per questo possibile richiamare la funzione nella schermata di log-in. Ciò che avevo fatto era sostituire il file che ne permetteva l'esecuzione sethc.exe con il file del Command Prompt di Windows, noto come CMD.exe[6]. A questo punto non dovevo fare altro che riavviare e premere cinque volte shift nella schermata di log-in per avere accesso alla console, con diritti di Amministratore. Così feci e con i comandi net user abilitai l'account Admin Locale settando il parametro su enable ed inserendo una nuova password[7].

Ero dentro il Domain Controller o meglio, ero dentro la macchina fisica che ospitava la struttura Hyper-V virtualizzata con il domain controller. Vale a dire che avrei dovuto bucare altre tre macchine: Il Domain Controller vero e proprio con relativa struttura Active Directory della rete, il server di storage e le macchine che ospitavano alcune WebApp interne.

Erano passate circa due ore da quando mi ero messo a lavoro. Non volevo ancora comunicare il mio successo al responsabile, perché sarebbe stato inutile se non fossi riuscito ad accedere alla struttura virtualizzata. Domandai solo un caffè, aggiungendo che avevo bisogno di tempo. La struttura Hyper-V era lock, completamente bloccata, tutte le autorizzazioni richieste per effettuare le modifiche necessitavano di una password interna con privilegi di Admin. Sì certo, potevo resettarla, reinstallarla o altro, ma non mi sarebbe servito a molto, in quanto se avessi intaccato le fondamenta dell'installazione avrei compromesso, definitivamente, tutta la rete. La prima idea fu quella di virtualizzare un'altra macchina attaccante e compromettere il domain controller attaccandolo direttamente per poi eseguire un privilege escalation una volta ottenuta una reverse shell all'interno, ma non potevo agganciare una nuova macchina alla struttura, non senza i permessi necessari. Dovevo cercare ancora, guardando il problema da una prospettiva differente. Molto probabilmente l'installazione delle macchine virtuali era avvenuta attraverso l'utilizzo di un'immagine .iso del Sistema Operativo (che anche questa volta era Windows Server 2008 R2). Cercai all'interno della configurazione ed effettivamente la mia supposizione era esatta le macchine puntavano ad un ISO del sistema operativo Boot Lock (non modificabile) su una partizione non più esistente. Se avessi potuto, in qualche modo, modificare le opzioni di boot delle macchine virtuali sarei riuscito a sfruttare lo stesso exploit utilizzato per accedere alla macchina fisica, ma non potevo. Quindi ebbi un'altra idea: se non potevo modificare il percorso di boot, potevo per lo meno simularlo. Così feci, montai una partizione virtuale[8] sulla macchina

fisica simulando lo stesso percorso target della struttura Hyper-V, utilizzai un iso di windows server rinominata come la reale, incrociai le dita ed avviai il domain controller vero e proprio… “Press Any Key for Boot from ...”...era fatta! A questo punto eseguii esattamente lo stesso processo effettuato per la macchina fisica per tutti e tre i server virtuali.
Tre ore dopo una macchina fisica e tre server virtuali erano stati violati, gli account di dominio resettati, e le password di Amministrazione restituite ai legittimi proprietari.

## Approfondimenti e Note

- [1] Cybersicurezza Il Sole 24 Ore – Pubblicazione settimanale n. 3 /2018
- [2] Cyber Division si occupa di Incident Case o Incident Response, ogni volta in cui la sicurezza di un sistema risulta compromessa. L'incident case consiste in una serie di comportamenti finalizzati a mimizzare gli effetti di una violazione, a garantire l'integrità dei dati e delle risorse del sistema, e a tentare di prevenire violazioni future.
- [3] Sono Live Chat utilizzate in maniera pseudo randomica, è sufficiente scrivere in Google live chat https per trovarne una moltitudine.
- [4] Il criptaggio viene generalmente effettuato sui sistemi Windows Microsoft utilizzando il famoso BitLocker, ma ne esistono molti altri.
- [5] La Backdoor sfruttata generalmente è denominata in diversi modi “Buffer Keyboard Overload Errors” o “ Keyboard error Overload”
- [6] E’ possibile mettere in atto questa tecnica in diversi modi, in alcuni casi è sufficiente resettare la macchina diverse volte in modo da causare un Safe-System-Boot intenzionale. Un esempio lo si può trovare qui https://www.youtube.com/watch?v=zaSv9YE_XsY&list=PLcfLJAWnrm4vCy21exBSOG5qwLHLL4zOg&index=2
- [7] net user Administrator /active:yes
  neu user Administrator nwepassword
- [8] https://en.wikipedia.org/wiki/Disk_image#Creation

A cura di: **Vincenzo Digilio**