A case history: Worst Case Scenario

Author : Vincenzo Digilio

Date : 13 novembre 2018

Tutta la teoria nel campo della Cyber Sicurezza offre sempre numerosi spunti, rivelandosi molto interessante da leggere: dagli alti fascicoli di *Security Planning* scritti da signori imbellettati in giacca e cravatta attorno ad un tavolo, agli infiniti protocolli d'abbecedari sugli *Incident Management*, alle intere liste di sigle come Risk Management, Problem Management e tutto l'insieme di "Best Practice" contenuto nell'ITIL (*Information Technology Infrastructure Library*[1]). Da queste lunghissime letture, è curioso vedere come la realtà riduca sempre ai minimi termini l'argomento, in binario: si riesce o non si riesce a gestire l'incident. Con questo non intendo sostenere che sia tutta carta straccia, ma che confrontarsi con il mondo reale è molte volte ben distante dalla teoria di un manuale. Ciò che veramente fa la differenza, è aver messo alla prova la sicurezza della propria infrastruttura. E non mi riferisco ad un Penetration Test[2] fatto dalla stessa società che ha condotto il Network Assessment[3] della rete. Mi riferisco ad un "vero" attacco che testi il livello di Security dell'Infrastruttura IT, gli accessi fisici alla società, il grado di preparazione e "awareness" del personale interno.

Le società italiane, dove almeno esistono ipotetici manuali del "cosa fare in caso di...", sono per lo più multinazionali. Il "Dark Web" di queste società è rappresentato dalle PMI Italiane, dove la Cyber Sicurezza è ancora un qualcosa fra l'esoterico ed il faceto. Qui, vecchi domain controller[4] con sistemi operativi obsoleti, e non più supportati, vengono esposti bellamente al pubblico con accessi RDP, dove la password del *domain admin* è utilizzata anche per accedere ai Firewall perimetrali e così via....
Ed è proprio in uno scenario del genere che si è verificato il nostro "Worst Case".

La solita chiamata dell'ormai "codice rosso" la ricevetti direttamente io, questa volta. A dir la verità, nel giro di trenta minuti, avevo già ricevuto altre sette chiamate da quel numero sconosciuto.

.

Feci la domanda da un milione di dollari:

Però! Si erano dati da fare!

Farfugliò qualcosa a metà fra il sì e il no. Il che vuol dire che non lo sapeva o che si trattava semplicemente di un “no”.

Lo scenario che mi si prospettò l’indomani si rivelò il caso peggiore che avessi mai trattato.

Il Domain Controller virtualizzato ospitava una versione obsoleta del sistema operativo Windows Server; oltretutto era esposto verso l’esterno tramite il servizio FTP (File Transfer Protocol), che prevedeva lo share dei file su un disco in locale. In queste tre righe che ho riportato, ci sono almeno una decina di macro-criticità gravi, esattamente l’antitesi della Sicurezza: cosa non bisognerebbe mai fare.

Comunque, l’attaccante scelse un classico intramontabile: *Brute Force*[5] al protocollo FTP. L’unica cosa di cui aveva bisogno era un elenco di username e password possibili. Per trovare lo username ci volevano un paio di secondi: “admin”. Per trovare la password qualche altro secondo, dato che una *wordlist* (altro non è che un file di testo con una lista di possibili password) accettabile per il *brute force*, si poteva facilmente popolare attingendo dal sito internet della società. Utilizzando ad esempio un *ruby script*[6], come *cewl* (Custom word list generator, fondamentalmente uno spider) è possibile estrapolare tutte le parole chiave da un sito internet per utilizzarle al fine di crackare una password.
Ad esempio il comando poteva somigliare a questo:

```
cewl https://sito.vittima –m 7 –d 2 – w w_list_dal_sito.txt
```

dove:

- **m** identifica la lunghezza della parola da cercare
- **d** il livello di profondità dello spider
- **w** il file .txt dove verrà salvato l'output del comando

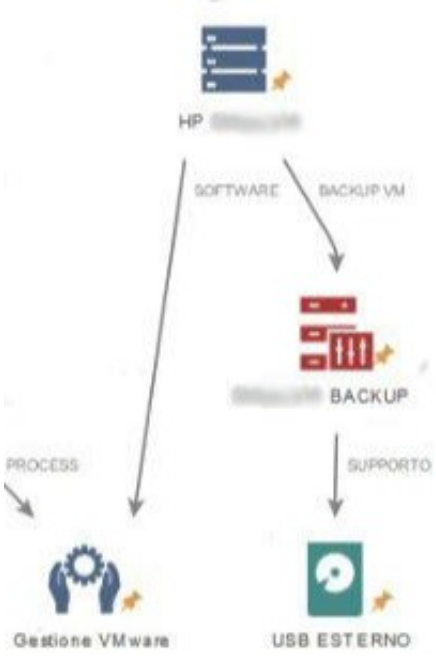
Ad altri programmi, come ad esempio *Crunch*, è possibile dare in pasto una serie di *key-words* al fine d'estrapolare una *wordlist* completa di tutte le possibili combinazioni di password, banalmente utilizzando le parole reperite dal sito internet della società vittima. Poniamo che la vostra password sia il vostro nome con una maiuscola e due cifre finali che rappresentano il vostro anno di nascita: per crackare una password del genere con la giusta world list occorre qualche secondo.
Per l'FTP non andò molto diversamente. L'attaccante digitò una command-line del genere:

```
hydra –L /lista_username_possibili.txt –P /wordlist_di_password.txt IP
 xxx.xxx.xxx.xxx –f –s 21 ftp
```

dove:

- **hydra** è il nostro login cracker
- **L la lista dei possibili username**
- **P la lista delle possibili password**
- **s è la porta del servizio ftp ed il protocollo**
- **f stop al success (Hydra s'interrompe appena trova username e password)**

Solo pochi minuti di attesa ed il gioco è fatto: l'attaccante ha accesso al servizio FTP con credenziali di amministratore! Ora, immaginate il livello di compromissione a cui era potuto giungere l'attacco alla società, una volta che gli hacker arrivarono a scoprire che quella password era valida non solo per il servizio FTP, ma che veniva utilizzata anche per l'accesso come Domain Admin. A quel punto...partita chiusa!



Ciò che fecero dopo, fu un puro esercizio di stile. Arrivarono sino al server dei Backup presenti sulla stessa rete, non essendo le VLAN segmentate, e sganciarono il ransomware. Attesero ore ed ore che tutti i backup fossero interamente criptati, compresi i dischi USB collegati alla macchina (ovviamente sarebbe stato controproducente per loro rivelare la propria presenza, almeno non prima di essersi sbarazzati di ogni possibilità di ripristino della rete).
Fatto ciò, non gli rimaneva che eseguire il dropper in tre punti differenti di snodo del traffico ed attendere...magari un venerdì notte, così nel weekend ci sarebbe stato tutto il tempo per criptare l'intera rete indisturbati.

Quando intervenni erano rimaste le ceneri ed una richiesta di riscatto di diversi *bitcoin*. Backup, Log, Domani Controller, sistemi di produzione, firewall, erano tutti stati manomessi/cancellati o criptati. L'intera rete era compromessa.
Negli scacchi si definisce zugzwang quando l'unica mossa possibile da fare sarebbe quella di non muovere. Con l'intera struttura compromessa in mano ai Cyber Criminali per giorni, l'unica opzione era ordinare un giorno di fermo e rimettere su l'infrastruttura da zero (o quasi) in tempi record. Ciò che feci, fu recuperare la struttura Active Directory da righe di comando su un Domain Controller precedente l'avvento di *powershell*.

Effettuai prima delle interrogazioni alla struttura dell'Active Directory:

```
dsquery user OU
=insieme,DC=dipendente,DC=soci
età,DC=com
dsquery com
puter OU=insieme,DC=di
pendente,DC=società,DC=com
dsquery ou OU=insieme,DC=dipendente,DC=società,DC=com
```

Poi importai l’elenco degli utenti:

```
CSVDE -f C:\users.csv -r  objectClass=user
```

Infine tutta l’infrastruttura completa:

```
CSVDE -f nome_del_dominio.csv
```

Quasi l’intero Team di *Cyber Division* fu coinvolto, lavorando l’intera notte. L’intervento all’unisono di diversi specialisti fu di vitale importanza. L’Analista Microsoft Security, convocato d’urgenza, operò chirurgicamente sul *.csv* che avevo estrapolato dal server infetto, al fine di ricostruire il nuovo Domain Controller, esportando sull’ultima architettura Microsoft Server tutta la foresta del dominio. Il Security Engineer, dopo aver analizzato il firewall con la collaborazione di uno degli IT esterni, circoscrisse l’intero perimetro dell’infrastruttura convogliando il traffico in uscita ed in ingresso su un *Server SySLog* in modo da monitorare qualsiasi movimento sulla rete (insomma, se qualcuno fosse entrato o uscito da quella rete, l’avremmo visto). Una moltitudine di servizi erano in running, uno su tutti il buon vecchio telnet. L’analista coinvolto, da laboratorio lavorò celermente sulla struttura del ransomware, in modo da poterlo segregare ed isolare il più velocemente possibile.
All’alba, l’azienda aveva ripreso le main activity ed il pericolo di bancarotta della società era stato scongiurato.

Referenze:

1. https://en.wikipedia.org/wiki/ITIL_security_management
2. https://en.wikipedia.org/wiki/Penetration_test
3. https://en.wikipedia.org/wiki/Information_Technology_Security_Assessment
4. https://en.wikipedia.org/wiki/Domain_controller
5. https://en.wikipedia.org/wiki/Brute-force_attack
6. https://en.wikipedia.org/wiki/Ruby_(programming_language)

Articolo a cura di **Vincenzo Digilio**