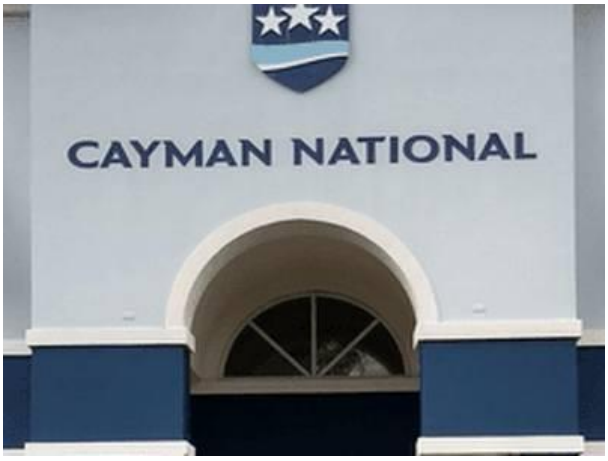
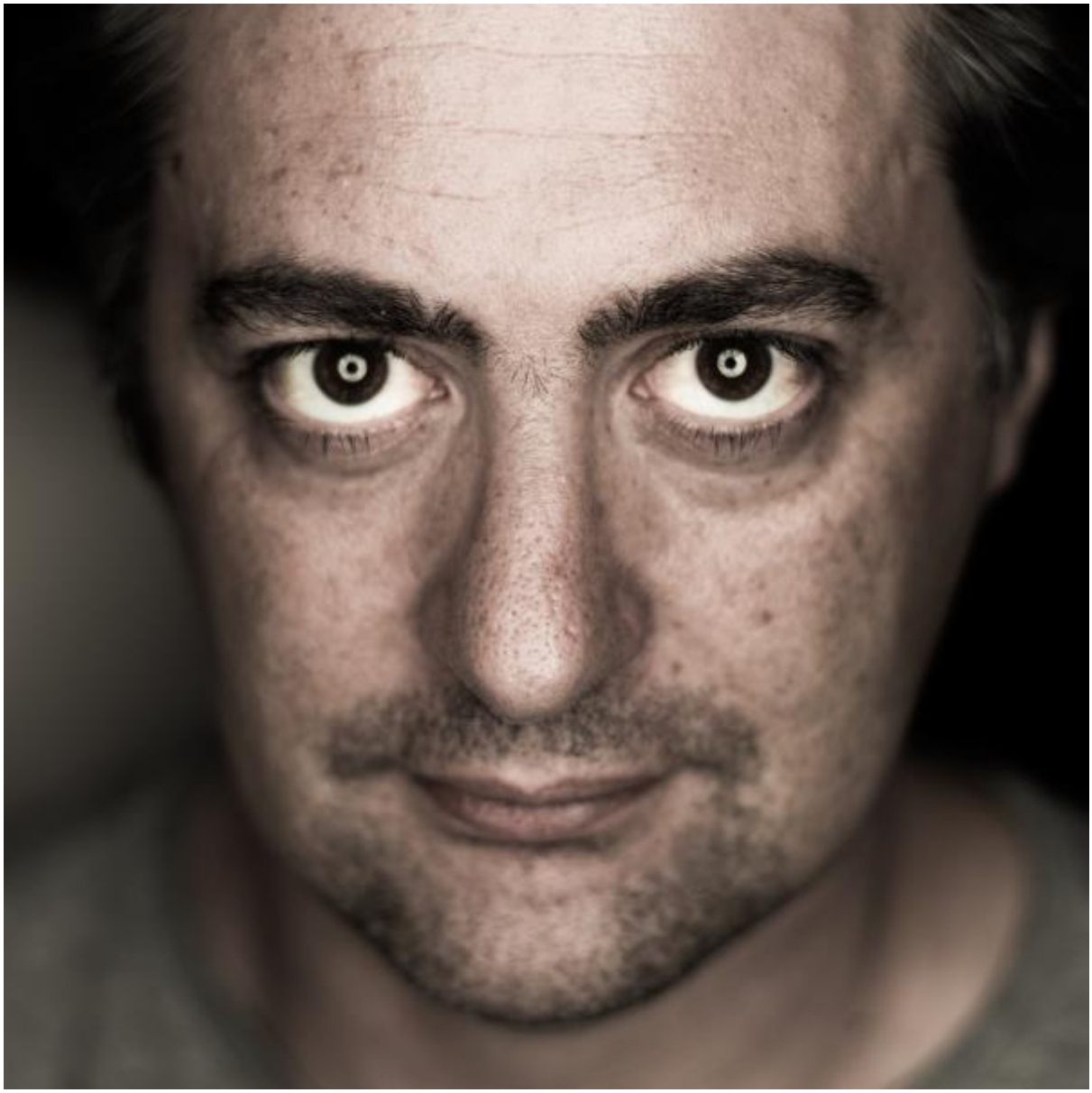


Ops, ho perso il mio sistema informativo...

Ovvero come gestire male un sistema informativo bancario e distribuire al mondo tutti i dati...



Ciao,

mi chiamo Andrea Ghirardini (aka Pila).

Sono un nerd all'ultimo stadio. Mi piace la tecnologia (e più è costosa e più mi intriga), mi occupo di progettare datacenter, gioco con il network, la sicurezza informatica, mi occupo di digtal forensics e ho retaggio un po' "da birbante".

Quando mi chiedono che lavoro faccio, dico sempre ... **"Vorrei saperlo anche io..."**

Riassumo dicendo **"Vedo gente... Faccio cose..."**

Sono rimasto molto colpito dall'hack di Cayman National Bank, per vari motivi:

- **Non capita tutti i giorni**
- **Mostra come spesso le acquisizioni possano creare danni**
- **E' un sistema totalmente virtualizzato (male, ne parleremo)**
- **E' stato hackerato da Phineas Phisher (mica ****)**
- **E' tanta roba**

Perché mi sono preso male?

Perché tutto questo combina tanti campi in cui mi piace ficcare il naso:

- **I sistemi Enterprise**
- **La sicurezza informatica**
- **L'hacking**

- **L'analisi forense**
- **Sistemi Legacy**

E anche perché ho potuto osservare le cose da più punti di vista:

- **L'amministratore di sistema**
- **L'attacker**
- **Il system Architect**
- **Il computer forensics expert**

In primis...

E' tanta roba! Cioè se vi sembrava che l'hack di Hacking Team fosse una cosa di una certa rilevanza, qui siamo oltre, ma tanto oltre. Stiamo parlando di circa 2,1 TB di dati compressi (spacchettati superano i 3,5 TB).

Quando l'hack è stato pubblicato era impossibile scaricarlo via Torrent. Ho dovuto muovere molte conoscenze per riuscire ad ottenere un accountin rsync sui server di DDOS (quando ancora erano attivi) e comunque ho dovuto scaricare a pieno ritmo per 20 gg sulla fibra.

La prima domanda che mi pongo quindi è:

Ma nessuno si è accorto del fatto che sono usciti dati per un periodo MOLTO LUNGO?

L'attacker ha sicuramente effettuato l'esfiltrazione dei dati in maniera corretta (senza quindi saturare la banda) e avrà certamente notato come probabilmente non vi erano sistemi di alerting di vario tipo (IDS/IDP, verifica sull'occupazione di banda, ecc. ecc.)

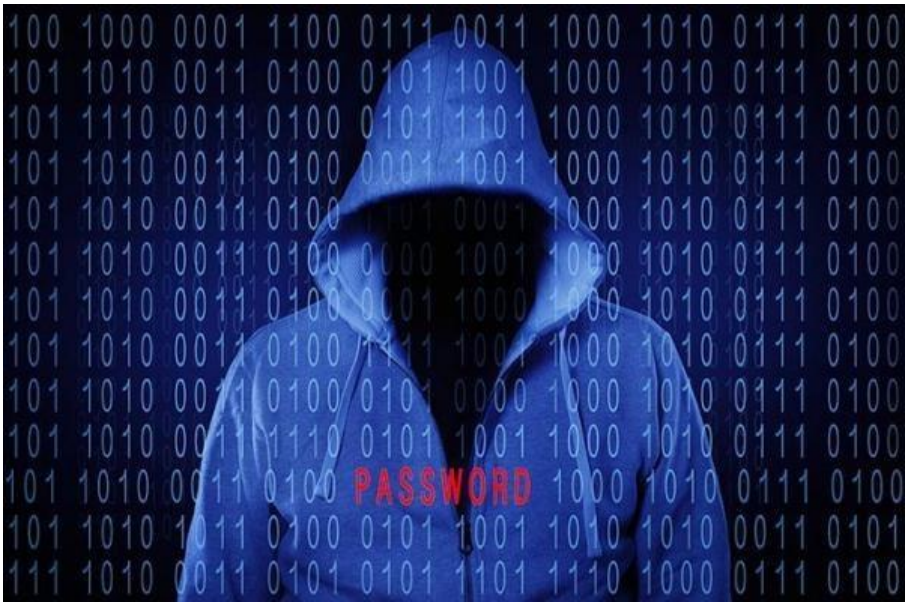
Cosa c'è dentro questo mega leak?

Ci ho studiato per parecchio tempo prima di capire cosa vi fosse. Ed è interessante quello che ho trovato.

Allora gli archivi sono organizzati un po' così, alla brutto demonio.

Ho impiegato un po' di tempo a capire cosa ci fosse all'interno (diciamo una buona settimana), per scoprire che:

- **Vi sono due sistemi informativi completi**: Uno è quello della Fiduciaria e uno quello della banca
- **I dati sono mescolati e organizzati in due distinti package**, uno denominato June e uno denominato October
- **I file sono zip e all'interno vi sono molti file 7z.** Sono convinto che siano stati ripacchettizzati da Phineas Phisher
- **I package non sono identici ma vi sono delle differenze, anche importanti**
- **I file 7z contengono una alberatura specifica, corrispondente con l'esportazione delle VM, così come viene effettuata da Hyper-V. Solo un archivio non rispetta questa struttura e sembra quindi preso direttamente dallo storage**



Hacker

E' evidente che l'hacker sia arrivato ai dati degli hypervisor.

Come può avere fatto?

Le strade sono pressoché due:

1. E' riuscito ad arrivare sul Directory Service ed ottenere un account con privilegi amministrativi (per lo meno su Hyper-V).
2. E' passato dallo storage. Stiamo parlando di Phineas Phisher e quindi la cosa non è assolutamente strana. Vi ricordo che usò un attacco banale sul protocollo iSCSI (gestito a **** in molte reti), per rubare gran parte dei dati di Hacking Team

Sysadmin

Ha fatto un lavoro pessimo.

Il fatto che due sistemi informativi di due compagnie differenti stessero mescolati non ha alcun senso (se non quello prettamente economico). Dubito che Phineas Phisher si sia preso la briga di sfondare due diversi sistemi, tanto più dopo aver letto il suo paper a commento dell'hack).

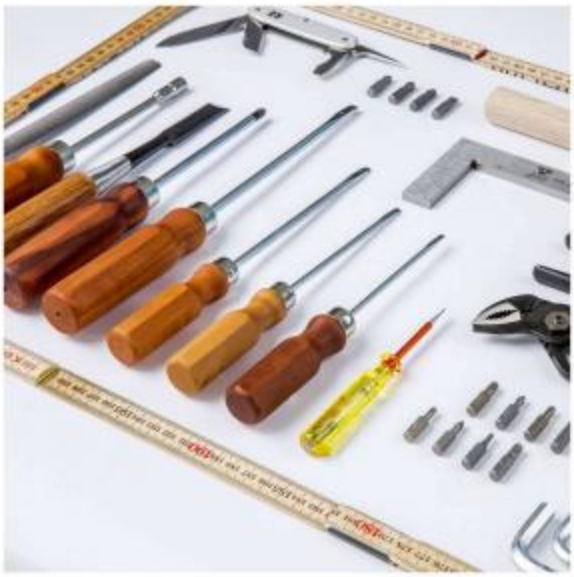
Certamente non ha messo in piedi dei sistemi di monitoraggio della banda (non pretendo un SIEM, ma uno schifo di mrtg che proiettasse i dati su un monitor con l'uso della banda avrebbe già aiutato).

Se l'attacker è riuscito ad arrivare sul Domain Controller il lavoro di hardening e gestione dei sistemi è stato osceno.

Se è passato dallo storage vuol dire che si tratta di un errore di progettazione della network grande come la piramide di Cheope

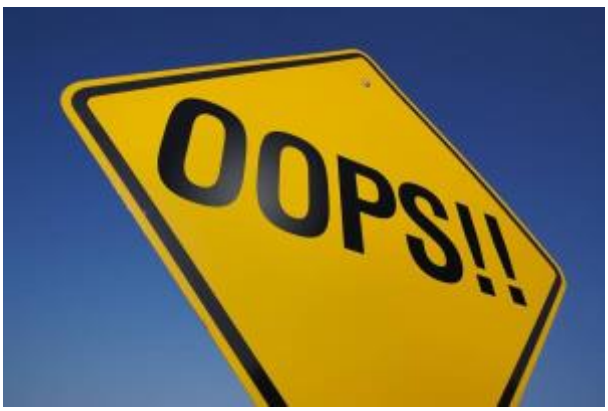
Il security expert, probabilmente, era mioccuggino, con dei problemi mentali, e doveva aver battuto la testa da qualche parte, perché non ne ha presa una giusta manco a pedate.

- **Ha sbagliato nella separazione delle informazioni.** Phineas Phisher lascia intuire che sia passato da un server web (e si trova). Se da questo è arrivato sull'hypervisor (sia dalla parte del server sia dallo storage). Vuol dire aver inanellato una sequenza di ***** che non stanno ne' in cielo ne' in terra.
- **Non ha gestito la sicurezza perimetrale.** Nessun sistema perimetrale ha rilevato l'intrusione iniziale, i covert channel usati per entrare nella rete (sempre covert siano stati), l'aumento di banda esponenziale nella fase di information leaking
- **Non ha gestito correttamente l'hypervisor.** Non parliamo di un errore banale, non parliamo di una configurazione sbagliata. **No stiamo dicendo che ha pestato la madre di tutti i merd****, il tutto perché non conosceva minimamente le potenzialità del sistema di hypervisor che è stato scelto (Hyper-V)**



Analizzando i pacchetti si scopre che:

- **Hyper-V è una figata**! Tutto quello che vi serve per analizzare i sistemi è dentro i sistemi Microsoft. Se non volete strafare basta un PC ben carrozzato con Windows 10 Pro. Se volete fare gli "sboroni", prendete un server e installateci Windows server core, se avete due soldi un Windows Server Standard non si nega a nessuno.
- **Windows 10 ha delle potenzialità assurde per quanto riguardo riguarda la gestione dei sistemi virtuali di casa Microsoft**. Potete obbiettare che si può fare la stessa cosa montando Vmware Workstation Player su un PC, ma qui il livello di integrazione è massimo. Inoltre tutta la parte di virtualizzazione è totalmente gratuita, cosa che certo non è poco.
- **Come computer forensics expert** posso dire che con un sistema Widnows ben carrozzato (e X-Ways Forensics) si possono fare cose assurde.

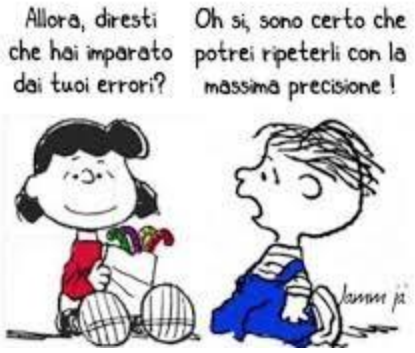


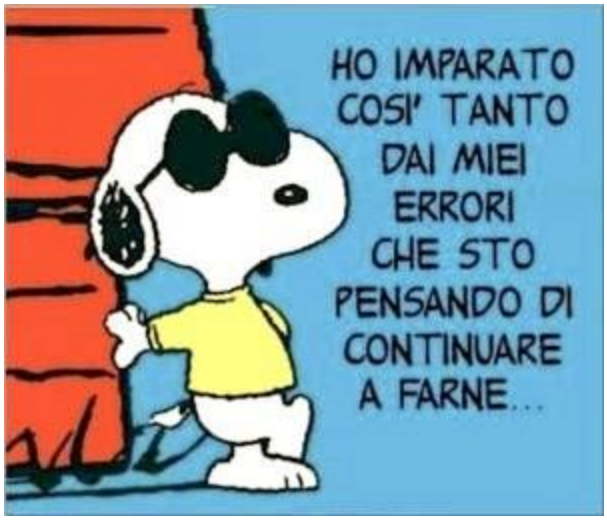
Venghino siori e siore! Venghino a vedere le cose più assurde mai viste da occhio umano!

La prima e unica fiera degli scherzi e delle burle in campo IT, abbiamo incompetenze a tutti i livelli, dal network, alla security, passando per la progettazione dei sistemi informativi.

Venghino siori e siore! Venghino a vedere gli scherzi della natura e i mostri che pensavate esistessero solo nelle favole! Il manager incompetente, il sistemista incapace, il security manager "solo sulla carta", il network expert che non capisce nulla di reti!

Venghino siori e siore!





Errori, errori ovunque!

Partiamo dalle basi. Una cattiva progettazione è sempre una pessima base su cui costruire un sistema e poi renderlo sicuro (anche qui errore di fondo dato che la sicurezza deve accompagnare il sistema fin dal progetto).

Perché due sistemi di due diverse compagnie condividono lo stesso hardware? Non ha senso se non per un discorso di economia, ma ha ancora meno senso dato che le richieste di un sistema bancario hanno esigenze ben diverse da quelle di un sistema di una fiduciaria. **Prima leggerezza.**

Se presupponiamo che Phineas Phisher abbia ripetuto l'attacco che ha fatto in HAcking Team (e sembra dal documento che lo abbia fatto) e sia passato su iSCSI, scopriamo due errori macroscopici:

- **La rete per il trasporto dei blocchi (SAN) e la rete dei dati (LAN) non erano fisicamente separate**
- **Non è stato usato un protocollo di autenticazione per la parte di iSCSI**

Tutte le VM (**non so se mi sono spiegato, TUTTE LE VM**) non erano crittografate. Attenzione, probabilmente questo non sarebbe servito ugualmente (maledetto virtual hardware) ma certamente avrebbe complicato la vita. Ricordiamoci inoltre che la crittografia ha efficacia diversa a seconda del layer su cui è stata utilizzata.

Spiegone tecnico da far sanguinare le orecchie...

Quindi, riepilogando, **le basi su cui si fondava il sistema non erano, molto probabilmente, corrette.**

La sicurezza perimetrale non lo era sicuramente (per tutti i motivi fin qui spiegati), **i sistemi di alerting inesistenti o inefficaci.**

E quindi che si fa? Si inizia a giocare!

Partiamo.

Per prima cosa si identificano le macchine. Nel pacchetto di Ottobre si scopre il DC. Si può iniziare da quello per fare una cosa semplice, ovvero attaccare il Domain Controller e da lì cambiare la password di Administrator di Dominio.

A questo punto, una volta preso il controllo del DC è sufficiente creare un "Internal Virtual Switch" per sistema informativo e aggiungere progressivamente le varie VM.

Ho identificato due sistemi informativi. Tutti i server che iniziano con "CN" fanno parte della Cayman National Bank, mentre i server con nomi vari sono quelli della fiduciaria delle isole Cayman.

Ho inziato dai database server, per passare poi ai gestionali, e ai sistemi AntiMoney Laudering.

Inutile dire che tutti questi contengono milioni di dati personali di cui la banca si è ben guardata dal comunicare la perdita.

Tutto questo solo perché avevo voglia di esplorare il sistema e di complicarmi la vita.

Se ben ricordate i Panama Paper, essi scaturivano tutti dal mail server dello studio Mossak Fonseca.

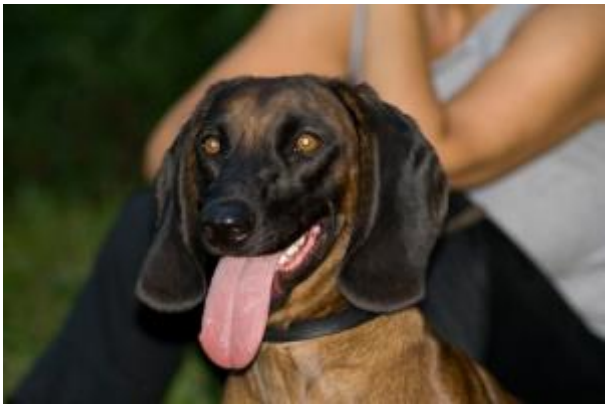
Anche in questo caso abbiamo sia mail server della Cayman National Bank (Sistema Exchange), sia due enormi File Server, sia della Banca sia della Fiduciaria.

Per estrarre i dati è sufficiente montare con un doppio click le immagini VHDX su Windows 10 e usare X-Ways Forensics.

SI PUO' FARE !!!!

Si sarebbe potuto evitare? Certamente!

Bastava fare le cose in maniera corretta e non "cinofallica" (cit. Matteo Flora)



Iniziamo dalla progettazione:

- **La network va opportunamente ridondata e suddivisa. Il backend va separato dal front end (SAN e LAN)**
- **Ogni segmento di rete con destinazione diversa va confinato in una sua specifica VLAN**
- **La parte iSCSI va gestita opportunamente (CHAP Maledizione!)**
- **Servono due Cluster separati (vale per Hyper-V)**

Passiamo alla parte di sicurezza:

- **Crittografia pervasiva a tutti i livelli** (Storage, Virtual Disk, traffico di rete, Database)
- **Separazione in tenant diversi**
- **Shielded VM** (per questo Hyper-V è meglio di Vmware e per questo servono due Cluster)
- **Hardening dei sistemi operativi delle VM e degli Hypervisor**
- **Almeno due diversi Domini (in questo caso almeno tre)**
- **Firewall perimetrali**
- **Sonde IDS/IDP**
- **Separazione netta dei dati interni ed esterni**
- **Mappatura dei vettori di attacco, VA/PT periodici**
- **Centralizzazione dei log e analisi in realtime con un sistema SIEM**

Andrea Ghirardini

ghirardini@beitsa.ch

+39 377 110 110 1