

IRITALY TEAM



WWW.IRITALY.ORG

**“INTRODUZIONE ALLA VIRTUALIZATION:
PRO, CONTRO E SECURITY”**

AUTORI:

**FORTE DARIO
ORLANDI THOMAS**

1 THE IRITALY TEAM

Durante un recente convegno svoltosi negli Usa, uno dei relatori ha sollevato un'interessante questione relativa alla percentuale, rispetto al totale degli ambienti IT con cui si interagisce, delle macchine virtuali. Questo, in realtà, a parte le più o meno condivisibili valutazioni del mercato, non è di fatto un dato ancora certo, in quanto non è dato sapere il numero esatto delle virtual machines utilizzate, incluse quelle basate su opensource.

2 GLI AMBITI APPLICATIVI

In questo momento storico, analisti si interrogano su quali possano essere le applicazioni di sicurezza che, in generale, possano essere attivate con l'ausilio della virtualizzazione.

La gestione degli "endpoint PC", è sicuramente uno dei punti di partenza più sfruttati in questo tipo di ambiente. Con questo termine si intende la possibilità data al Dipartimento Information Technology di gestire centralmente dei PC che fisicamente sono di proprietà di terzi (per esempio dei consulenti od outsourcer in genere) ma che devono comunque accedere alle risorse aziendali. Si tratta quindi di una macchina virtuale che viene configurata secondo l'ambiente IT in cui l'"esterno" si trova ad operare e, contestualmente, consegnata allo stesso utente che dovrà poi utilizzarla per accedere alle risorse IT dell'azienda.

Messa in sicurezza dei dati sul PC. Si tratta di un altro must che deve per forza di cose essere gestito centralmente, la cui necessità è data altresì dalle esigenze di compliance legate alla legge privacy. La soluzione evidentemente più adottata è quella relativa alla crittografia del file system. Utilizzando le virtual machines, è evidentemente possibile procedere alla stessa tipologia di encryption mantenendo comunque una forte limitazione agli attaccanti in caso di violazione della macchina host. Alcuni vendor interfacciano addirittura questo metodo con l'utilizzo di token hardware.

Un'altra applicazione che di solito viene richiesta e coperta con la virtualizzazione è la gestione degli accessi remoti, mediante la quale è possibile accedere a risorse particolari della rete aziendali ancora una volta in una "cella di sicurezza" evidentemente tracciabile in ogni suo movimento. Questo tipo di applicazione torna utile anche in caso di consolidamento di più workstation in capo ad una sola o, meglio ancora, ad un server.

3 VENDORS VS. VIRTUALIZATION

L'attività dei technology vendors in generale (sia Hardware sia Software) è in continua evoluzione, così come il mercato in generale. Mentre aziende come Magirus (www.magirus.it) dichiarano una crescita a tre cifre rispetto all'annualità precedente sul segmento specifico della virtualizzazione, Intel e AMD stanno già da tempo lavorando ad un loro supporto nativo (in CPU) per la virtualization. Questo significa, in parole povere, riduzione dei tempi di latenza e maggiore produttività. Nel frattempo, anche i vari produttori di architetture di automated incident response stanno lavorando a questo argomento, presentando strumenti in grado di gestire l'imaging delle macchine compromesse direttamente dalla postazione centralizzata, anche qui diminuendo i tempi di reazione e quindi l'impatto dell'incidente, che si sa essere direttamente proporzionale alla lunghezza del processo di risposta e remediation. Va infine detto che, a proposito di VMWare, esiste una feature dell'ultima generazione denominata "encapsulation" che consente, oltre che un isolamento della completa condizione della macchina virtuale (inclusa la memoria), l'utilizzabilità del file VM per ulteriori analisi di incident response basati su tecnica LSA (Live System Analysis). Va inoltre rammentato che la Virtualizzazione non è ad esclusivo appannaggio degli amministratori di sistema e o dei cosiddetti "computer geeks". Anzi, vi sono molti utenti finali che possono trarre giovamento da questa impostazione, con particolare riferimento a quelli mobili comunque avanzati, che con i classici due giga di RAM sono in grado di gestire più ambienti all'interno dei quali far girare sia le loro applicazioni di produttività sia quelle di taglio tecnico differente.

Senza contare, ovviamente, il limite intrinseco alla diffusione del malicious code dato dalle macchine virtuali in genere (con le dovute riserve, ovviamente). Anche le compromissioni sono fondamentalmente gestibili verso il contenimento. Compromettere una virtual machine (quando possibile, ovviamente) ha delle ripercussioni in teoria inferiori rispetto ad una compromissione ordinaria, a causa del tipo di architettura "sandbox" in cui la macchina virtuale stessa è inserita.

In conclusione, la virtualization è il classico investimento che può contenere più finalità (per esempio di gestione IT e sicurezza) e per questo può essere "spalmato" su più centri di costo, garantendo quindi l'innalzamento del livello generale di protezione ed un ROI più tangibile.

4 Virtualizzazione per business

Ci sono diversi modi in cui un'organizzazione potrebbe trarre beneficio usando la virtualizzazione:

- ✓ Massimizzare le risorse: analizzando le varie realtà industriali si può notare come, nella maggior parte dei casi, i server vengono sottoutilizzati. Per aumentare l'utilizzo e quindi, da un punto di vista economico, per incrementare il ROI. È dunque consigliabile installare diverse macchina virtuali al fine di sfruttare a pieno le caratteristiche di un server.
- ✓ Ottimizzazione di test e sviluppo: il test e lo sviluppo dei server può essere svolto in breve tempo se si utilizzano macchine virtuali pre-configurate. La virtualizzazione stessa si presta a scenari standard che quindi possono essere riprodotti con estrema facilità ed in tempi minimi.

- ✓ Risposta immediata alle esigenze di business: il processo di sviluppo sta via via diventando sempre più complicato e soggetto a variazioni anche nel breve periodo. Spostando l'interno ambiente di sviluppo su macchine virtuali garantiamo un supporto malleabile anche a rapidi cambiamenti.
- ✓ Riduzione dei costi di continuità: il ricreare un intero sistema in un unico file e assumendo un livello di astrazione tale da poterci dimenticare dell'hardware sottostante permette di ridurre notevolmente i costi e la complessità del business continuity offrendo quindi una soluzione di alta disponibilità dei dati e soluzioni di disaster recovery in cui la macchina virtuale può essere replicata e spostata su qualunque server
- ✓ Aumento della sicurezza: allo stato attuale per isolare un sistema dobbiamo ricorrere a configurazioni di networking e di firewalls, con la virtualizzazione invece, possiamo creare le nostre macchine virtuali nello stesso server e farsi che vengano eseguite in ambienti sandbox.

5 Ambiti Operativi Per La Virtualizzazione

Vediamo di seguito alcuni degli ambiti in cui la virtualizzazione potrebbe fornire soluzioni innovative

5.1 Virtualization for sandboxing

Il primo scopo della virtualizzazione consiste nell'isolare determinate applicazioni.

Spostando l'esecuzione di singole applicazioni o di gruppi di applicazioni sulle virtual machine permette di controllare in maniera semplice e rapida due tipi di problemi: il primo legato all'instabilità delle applicazioni stesse, è ben noto come un crash di un'applicazione produce uno spreco di risorse e, nei casi peggiori, provoca il crash dell'intero sistema; il secondo problema invece riguarda la compromissione delle applicazioni che potrebbe tradursi nell'uso dell'applicazione da parte di soggetti non autorizzati oppure al rilascio involontario di privilegi.

VMware Inc. offre il miglior modo per ovviare al secondo tipo di problema. In prima battuta essi promuovono il concetto di "virtual appliances", VMware esegue nella macchina virtuale tutta una serie di applicazioni virtuali, il loro funzionamento non discosta dal funzionamento che avrebbero se venissero eseguite all'interno di un sistema operativo reale; addirittura è in grado di gestire task che coinvolgono l'area Internet come utilizzare servizi di mail e di connessioni P2P. Dal momento che queste attività vengono identificate come critiche è utile notare come un possibile attacco risulterebbe innocuo in quando l'attaccante non avrebbe accesso all'host su cui è in esecuzione la VMware virtual machine evitando dunque accessi a dati sensibili oppure all'accesso della rete aziendale.

Inoltre il recupero di sistemi compromessi diventa semplice avendo applicato la tecnica di virtualizzazione. Un utente medio potrebbe riavviare la virtual machine compromessa e riportare l'interno sistema alla situazione originaria, il tutto in pochi secondi.

Con il passare degli anni, molti esperti in sicurezza hanno sollevato dubbi relativi all'introduzione del livello di virtualizzazione per isolare la virtual machine stessa e l'host sulla quale è in esecuzione. Questi dubbi trovano fondamento in quando i processi di I/O delle virtual machine vengono mediati dal Virtual Machine Monitor (VMM) il quale potrebbe essere malformato o corrotto lasciando spazio ad attacchi di tipo buffer overruns e di conseguenza

alla possibilità di compromettere l'host sul quale la macchina è in esecuzione. Al giorno d'oggi però non esistono documenti che riportano attacchi di questo genere portati a termine con successo.

5.2 Virtualization for disaster recovery and high availability

La maggior fonte di pressione da parte delle aziende è rappresentata dalla preservazione e della disponibilità costante dei servizi.

Al giorno d'oggi, la necessità primaria consiste nel fornire una soluzione efficace al problema del backup dei dati, attualmente il backup viene effettuato attraverso server appositi. Questo approccio presenta due grandi controindicazioni: la prima dovuta al periodo di tempo impiegato per effettuare il restore dei dati mentre il secondo aspetto è legato alla necessità, da parte delle aziende, di ripristinare una situazione originaria oppure di estrarre una copia di dati senza che questa operazione intralci il proprio business.

La virtualizzazione riduce drasticamente i tempi e i costi delle operazioni di “disaster recovery”. Invece di salvare i singoli file è possibile operare a livello di host, ossia copiare direttamente la macchina virtuale, in certi casi addirittura mentre questa è in esecuzione. Di conseguenza il backup verrà rappresentato da un unico file di notevoli dimensioni, nonostante questo aspetto possa creare un po' di sgomento è sufficiente pensare al tempo che impiegheremmo a dover installare un sistema operativo ex-novo e recuperare i dati persi.

Se questo modo di effettuare backup non sembra rivoluzionario, è utile ricordarsi che è possibile recuperare una virtual machine salvata su qualunque host operativo e su qualsiasi hardware consentendo quindi di ridurre in modo drastico il tempo complessivo di downtime del servizio.

Per ovviare al tempo di downtime tuttavia è possibile implementare due soluzioni alternative: la prima denominata “configurazione ad alta disponibilità” in cui dei nodi cluster condividono e bilanciano il traffico mentre una seconda soluzione meno costosa denominata “configurazione hot-standby” in cui uno o più nodi secondari entrano in funzione qualora il nodo principale cessi la sua funzione. Entrambe le soluzioni citate per essere implementate devono occupare due o più server fisici, con la virtualizzazione invece è possibile impiegare un solo server mantenendo comunque un prezzo di realizzazione di poco maggiore.

Ogni giorno, diverse realtà aziendali sviluppano sistemi di tipo mix, in cui il secondo nodo del cluster con i relativi servizi viene implementato su macchina virtuale, in pratica avremo un nodo primario presente fisicamente ma un secondo nodo all'interno di una virtual machine, pronto a fronteggiare qualsiasi caso di guasto del primo nodo. Poiché un nodo che si trova nello stato di standby non occupa risorse, all'interno di un host fisico è possibile predisporre diversi nodi virtuali nello stato di standby.

Un problema frequente è derivato dalla condivisione o dalla replicazione dei dati dall'host realmente esistente alla macchina virtuale (nodo standby). Compagnie come Vizioncore Inc. stanno cercando di ovviare a questo problema offrendo un servizio di replicazione dati per le più comuni piattaforme di virtualizzazione.

5.3 Virtualization for forensic analysis

Un altro punto di forza dell'applicazione della virtualizzazione è per scopi inerenti alla sicurezza: la forensic analysis.

I fondatori di VMware amano ricordare come agenzie che lavorano in stretto contatto con la legge come per esempio l'FBI abbiano accolto in maniera favorevole i loro prodotti, in quando soddisfavano e soddisfano tuttora l'esigenza di poter esaminare in modo offsite gli hard disk sequestrati.

Questo metodo, che in gran parte è oggi viene automatizzato, è denominato Physical To Virtual (P2V). Consente la creazione di una copia esatta e funzionante di un calcolatore, comprese le partizioni nascoste o criptate, e il tutto avviene senza alterare in alcun modo i dati.

Questo metodo inoltre consente di trasferire i dati dalla macchina virtuale al disco fisso direttamente e in poco tempo (varia in base alla dimensione del contenuto che si vuole copiare).

Allo stato attuale, le soluzioni di P2V sono fornite da Leostream, PlateSpin Ltd. E VMware. Esistono realtà emergenti di tool free che stanno prendendo sempre più piede in questo settore. Anche Symantec LiveState, azienda nota per la realizzazione di immagini "tradizionali" segue questo tipo di approccio dal momento che sono in grado di importare i loro formati proprietari in macchine virtuali.

La migrazione P2V non è solo un modo per effettuare analisi forensi ma un ottimo strumento per semplificare la fase di testing ed ottenere quelli che vengono denominati snapshot

Gli snapshot sono immagini istantanee fornite dagli strumenti di virtualizzazione e sono il risultato ottenuto dal congelamento del sistema operativo per consentire il recupero di ambienti compromessi. Il loro utilizzo è particolarmente utile quando vengono usati programmi in versione beta oppure applicativi instabili. Gli snapshot possono essere effettuati in qualsiasi momento indipendentemente che la macchina virtuale sia in esecuzione o meno. Quando una macchina virtuale è disattivata, il proprio contenuto verrà salvato nel punto di ripristino del sistema, mentre quando la macchina virtuale è attiva tutto il suo contenuto (compresi i dati volatili) è salvato all'interno del suo file immagine.

Tuttavia l'unico compromesso è legato agli strumenti definiti zero-day che consentono agli attaccanti di sfruttare determinate vulnerabilità senza lasciare tracce e senza poter essere rintracciati.

Per ovviare a questa perdita di informazioni, adottiamo strumenti quali "host intrusion detection system" (HIDS) che tracciano i file e la memoria inviando i rispettivi log ad un centro di raccolta. È da considerare che questi strumenti non solo sono ancora troppo costosi ma richiedono una notevole quantità di risorse. Inoltre non sono installati su ogni host che vogliamo proteggere e questi sistemi possono essere soggetti, a loro volta, a vulnerabilità.

La virtualizzazione applicata alla forensic risulta essere poco costosa e offre una soluzione alternativa all'analisi del caso; è possibile dunque ottenere un'istantanea del sistema includendo quindi il contenuto della RAM o del disco, includendo quindi le eventuali tracce lasciate nei file di log prima che queste vengano modificate dall'attaccante stesso. Inoltre, la natura della macchina virtuale ci permette di eseguirla su qualsiasi sistema operativo presente all'interno della nostra azienda.

Molte volte si ha la necessità di accelerare i tempi di acquisizione di un disco, con l'utilizzo della macchina virtuale è possibile implementare una soluzione che resta indipendente dalla dimensione del disco, ossia consiste nel implementare un raid 1 del disco su cui è in esecuzione la macchina virtuale. Qualora si voglia effettuare un'immagine del sistema è sufficiente staccare il disco installato a supporto, senza dunque fermare la virtual machine. Il file così ottenuto è di per se una copia forense.

5.4 Virtualization for honey potting

Allo stato attuale le community che si occupano di sicurezza hanno investito molto nel campo della ricerca in progetti e tecniche chiamate di honey potting.

L'honey pot è un sistema che assomiglia e si comporta come un ambiente/sistema produttivo. Il sistema è dislocato in punti strategici all'interno della rete aziendale, solitamente in punti d'interesse degli attaccanti. Nonostante la loro funzione possa sembrare puramente produttiva, in realtà, questi sistemi fungono da trappole. La loro missione consiste nello scoprire il più possibile circa le nuove metodologie e i nuovi strumenti per perpetrare attacchi; la raccolta di queste informazioni viene finalizzata alla ricerca di contromisure.

Prima che la virtualizzazione diventasse diffusa installare una macchina o una rete intera (un honeynet) per gli scopi di ricerca di sicurezza sarebbe stato proibitivo visti gli alti costi e gli sforzi dell'amministrazione. Oggi invece possiamo utilizzare le piattaforme libere di virtualizzazione, i generatori di traffico ed alcune soluzioni automatizzate (offerte da Akimbi Systems Inc. o Dunes Technologies). Costruire una honeynet virtuale diventa quindi possibile e facilmente realizzabile. Diverse compagnie dovrebbero valutare l'idea di realizzare un sistema virtuale che emuli il loro sistema aziendale e quindi esporlo alla possibilità di attacchi, tuttavia, nonostante la cultura legata alla sicurezza informatica è ancora agli arbori, esistono diverse realtà che stanno implementando una situazione del genere.

L'Honey potting virtuale è inoltre efficace per simulare diverse postazioni desktop e monitorare le minacce che i sistemi antivirus non sono in grado di gestire o addirittura rilevare. A tal proposito una simile applicazione è stata fatta da Microsoft con un progetto chiamato "Honeymonkey" e da IBM con un progetto chiamato "Billy Goat". Entrambi i progetti emulavano alcuni desktop e li esponevano ad internet in attesa di scoprire la diffusione di nuovi virus.

Uno svantaggio dovuto alla virtualizzazione dell'honey potting è che le macchine virtuali sono facilmente riconoscibili attraverso dei semplici controlli effettuati a livello di rete oppure a livello di sistema (dopo aver ottenuto l'accesso). Dopo aver riconosciuto la presenza di una macchina virtuale un attaccante potrebbe restare all'esterno oppure abbandonare l'attacco.

È possibile comunque trovare due argomenti che screditano il punto precedente. In primo luogo, molti attacchi sono automatizzati, come worm oppure malicious code, quindi non è così semplice, da parte di questi attacchi, valutare la presenza o meno di macchine virtuali. In secondo luogo, siccome molte compagnie stanno spostando i loro sistemi e servizi su macchine virtuali è sempre più difficile da parte dell'attaccante sapere se ha di fronte una trappola oppure un bersaglio reale.

6 Virtualizzazione e Sicurezza

L'utilizzo della virtualizzazione è stato sinora visto nei suoi aspetti innovativi, nonostante questi siano diversi e abbracciano diverse realtà è utile analizzare anche i problemi, dal punto di vista della sicurezza, che nascerebbero dall'uso di questa tecnologia. Si potrebbe iniziare da una considerazione elementare. Quando progettiamo una struttura di sicurezza per un host fisico, nella fase di analisi, consideriamo i potenziali rischi e le possibili perdite causate da un eventuale attacco o peggio ancora da un eventuale furto. Questo tipo di analisi deve essere rivista nel

caso in cui sull'host fisico siano presenti una o più macchine virtuali. Ecco quindi che l'eventuale furto dell'hard-disk comporterebbe al furto di tutte le macchine virtuali, dati annessi, presenti sul disco stesso. Nel caso in cui prevediamo delle macchine virtuali all'interno di un host è suggeribile quindi studiare in maniera più approfondita un sistema di sicurezza adeguato, visto che la compromissione dell'host, di fatto, darebbe accesso a tutte le macchine virtuali presenti su esso.

Prima di proseguire con l'analisi degli impatti sulla sicurezza delle virtual machine dobbiamo chiarire la funzione degli hypervisors. Gli Hypervisors sono programmi che consentono a diversi sistemi operativi di usare lo stesso hardware. Questi programmi, nonostante alcune figure presenti nel settore dichiarano essere semplici, studiati per interagire con i nuovi sistemi operativi e dunque facili da proteggere, risultano essere complessi ed è noto che, con l'aumentare della complessità, aumentano anche i problemi di sicurezza. L'utilizzo delle virtual machine, e con essi l'uso di programmi Hypervisors, ha creato un tornado che potrebbe sconvolgere le conoscenze di sicurezza apprese sinora. L'introduzione del layer di hypervisors crea un nuovo layer di attacchi. In questo livello, in cui le macchine virtuali diventano “ingestibili” e “non protette”, emergono i problemi relativi alla sicurezza e, viste le dinamiche di movimento e i cambi di modello delle virtual machine, il ciclo di test e di patching diventa frammentato, inadatto e complesso.

Un altro aspetto potrebbe essere legato agli applicativi, diventa sempre più difficile proteggere i dati in uso in quanto, essendo virtuali, non è noto dove questi vengono immagazzinati.

Nella fase di studio della virtualizzazione emerge il problema legato all'attacco “guest-to-guest attacks” dove un attaccante potrebbe acquisire in maniera impropria ai privilegi amministrativi ed accedere quindi al controllo completo della macchina ottenendo il controllo completo delle macchine virtuali. Quest'attacco presuppone che l'utente maligno abbia già ottenuto l'accesso all'host. Tuttavia questo tipo di attacco non è semplice da perpetrare se viene abilitata la crittografia (eludibile con alcune nozioni matematiche). Non solo è possibile compromettere l'host su cui sono in esecuzione le macchine virtuali ma è possibile compromettere le macchine virtuali stesse ed accedere quindi all'host sulle quali sono in esecuzione. Questo attacco prende il nome di “guest-hopping attacks” dove una vulnerabilità all'interno del layer hypervisors permette di violare la protezione della virtual machine e accedere all'host.

Un ulteriore problema è dato dalla gestione degli indirizzi IP. In un ambiente virtualizzato gli indirizzi IP delle macchine virtuali cambiano ogni qualvolta queste vengono create, dismesse oppure spostate da un server (fisico) all'altro. Siccome i modelli di sicurezza tendono ad associare gli indirizzi IP con una locazione, diventa estremamente difficile configurare in maniera corretta un firewall ed è estremamente difficile indicare all'intrusion detection system quali siano i sistemi da tenere sotto controllo.

Altri esperti sottolineano che dal momento in cui su un server è possibile eseguire diverse macchine virtuali eterogenee anche di diverso sistema operativo, per un attaccante è sempre più facile trovare un modo in cui perpetrare un attacco, visto che sullo stesso server (target) coesistono sia sistemi Windows che sistemi Linux.

Osservando i vari scenari presenti si nota come stanno nascendo rootkit basati su virtual machine. Un esempio di proof-of-concept è SubVirt che sfrutta alcuni bug di sicurezza e posiziona un VMM (virtual machine monitor) sotto

l'installazione di sistemi Windows o Linux. Dal momento che un sistema operativo è ospitato in una virtual machine, i rootkit installati su di esso diventano impossibili da rilevare in quanto i software di sicurezza non hanno accesso al sistema oggetto dell'attacco.

Riprendendo il concetto di macchina virtuale, ossia un'istanza del sistema operativo che è in esecuzione tra l'hardware ed il sistema ospite, quindi ad un livello inferiore, più vicino alla macchina, rispetto al sistema operativo stesso. È utile ribadire come il sistema operativo in esecuzione sulla macchina virtuale non è neppure consapevole di essere in esecuzione all'interno di un VM ma pensa di lavorare come un normale OS, e soprattutto non è in grado di individuare rootkit e malware vari celati all'interno della stessa virtual machine. Se si riesce quindi a creare un software che installa un monitor di macchina virtuale, il quale al suo interno esegue il sistema operativo originale, si possono nascondere dei rootkit e sovvertire il sistema target. Per di più tramite dei servizi si può propagare il controllo anche ad eventuali sistemi guest che si trovano al di sopra. I moderni sistemi di anti-rootkit clean-up confrontano il contenuto dei registri, analizzano le discrepanze all'interno delle chiamate di sistema API per controllare la presenza di rootkit user-mode o kernel-mode; questa tattica diventa inappropriata se il rootkit viene salvato all'interno di una virtual machine. Precisamente lo scopo di questo esperimento è quello d'impadronirsi di Windows XP modificando il kernel ed avviandolo con una versione ad hoc di Virtual PC; nel caso di Linux, viene considerata la distribuzione Gentoo combinata a VMWare. Ciò si può realizzare se il cosiddetto VMBR (Virtual Machine Based Rootkit) modifica la sequenza di boot, caricandosi prima del sistema operativo, e in seguito lo avvia tramite un VMM. Con questo SubVirt sono stati in grado di installare un Phishing Web Server, un Keylogger, un servizio che esegue una scansione per trovare dati sensibili, ed un altro che adotta delle contromisure affinché non s'individui questa macchina virtuale. E' stato poi implementato un meccanismo che controlla il modo in cui il sistema si riavvia, anche emulando spegnimenti e stand by. Possibili soluzioni a questa minaccia sono: implementazione a livello hardware di un sistema di controllo rootkit, di una macchina virtuale sicura che parta prima dei sistemi operativi, e boot anche dalla rete, tramite fidati dispositivi come un CD-ROM o una chiavetta USB. I ricercatori concludono che i rootkit VM-Base siano una reale minaccia dal momento che sono implementabili e visti i diversi virtual machine monitors distribuiti in maniera open-source dalla community o commercialmente dai rispettivi vendors. Su sistemi attuali come x86, questi rootkit sono capaci di eseguire un sistema target mostrando minime differenze sia dal punto di vista prestazionale sia dal punto di vista del tracciamento. Inoltre il pericolo è così reale, afferma il team di ricercatori, che durante la creazione di SubVirt, uno degli autori ha usato accidentalmente una macchina infettata dal rootkit proof-of-concept senza accorgersi che stava usando un sistema compromesso. Nonostante molti sostengono l'invisibilità di questo rootkit si nota comunque la possibilità di rilevarlo in modalità offline in virtù di alcune modifiche apportate al hard disk del computer necessarie per il suo funzionamento.

Un altro esempio in materia di malware è Blue Pill. La creatrice del malware sostiene, attraverso la sua creazione, di poter inserire del codice arbitrario nel kernel di Vista senza sfruttare nessun bug del codice del sistema. La nuova tecnica effettivamente è in grado di bypassare una policy cruciale anti-rootkit integrata in Vista, che prevede che i software kernel-mode siano dotati di firma digitale per essere caricati nei sistemi x64-based. L'unico modo di rilevare Blue Pill sarebbe quello di sfruttare una falla nella tecnologia Advanced Micro Devices (AMD) Secure Virtual Machine Pacifica, se si potesse creare un metodo di rilevamento generico per la tecnologia di virtualizzazione, allora Blue Pill potrebbe essere isolato, ma questo significherebbe anche aver trovato un bug nella tecnologia Pacifica. L'idea alla base di Blue Pill è semplice: il vostro sistema operativo inghiottisce la 'Pillola Blu' e si sveglia all'interno

della Matrice controllata dall'hypervisor ultra leggero del rootkit. Tutto questo avviene “on-the-fly” (senza riavvio del sistema al contrario di SubVirt) e non si noteranno neanche rallentamenti di performance o problemi con nessun dispositivo installato. Originariamente Blue Pill è stato implementato per funzionare con sistemi Vista x64, ma come suggerisce l'ideatrice del rootkit, nulla vieta di effettuare il porting del codice per sistemi operativi come Linux, BSD che possono girare su piattaforme x64.

In conclusione, con l'introduzione delle macchine virtuali si sono aggiunti tutta una serie di dinamismi all'interno della infrastruttura IT che i normali sistemi di sicurezza non prevedono. Un esempio su tutti è la copia di un dato da una risorsa virtuale ad una risorsa fisica, la quale aggiunge un livello di complessità in più e dunque possibili problemi di sicurezza.