VIROLOGIA VIRTUALE

IL PRIMO ESAME DEI PARALLELISMI TRA I VIRUS INFORMATICI E I VIRUS BIOLOGICI

Network ASSOCIATES
YOUR NETWORK. OUR BUSINESS.

Virus [n]. Un parassita intracellulare infettivo in grado di vivere e riprodursi solo all'interno di cellule viventi [dal latino: umore viscoso, veleno][1].

Virus [n]. Programma informatico, solitamente nascosto all'interno di un altro, che si auto-riproduce e auto-diffonde, danneggiando il funzionamento del computer che lo riceve.[2]

[1]Melloni [2]Encarta Reference Dictionary

COSA NASCONDE UN NOME?

Due definizioni all'apparenza completamente diverse della parola "virus". Una di origine antica, l'altra un modernismo per descrivere un fenomeno caratterizzante il tardo XX secolo e gli inizi del XXI secolo. L'unica somiglianza sembra essere nel nome.

FINO AD OGGI...

Questo documento descrive le scoperte di due dei massimi esperti in virologia, riconosciuti a livello mondiale, uno nel campo medico, l'altro in quello dei virus informatici. Hanno deciso di collaborare e, per la prima volta, di andare oltre questa apparente somiglianza per esplorare i possibili parallelismi dietro il nome in comune.

Il risultato è un approfondimento all'interno di mondi paralleli fin qui inesplorati dei virus informatici e medici – che rivelerà un incredibile numero di somiglianze fondamentali. I risultati, evidenziati in questo documento di discussione, sono stati strutturati per offrire ai professionisti del settore medico e tecnologico una maggiore comprensione del proprio settore complementare – forse scoprendo indizi che aiuteranno entrambi nella loro continua battaglia contro i rispettivi nemici.

Questa incredibile ricerca è frutto del lavoro del Dr. Rod Daniels, che dirige un laboratorio di ricerca di virologia presso il National Institute for Medical Research (NIMR) in Gran Bretagna e diffonde le informazioni sui virus alla World Health Organisation (WHO), e Jack Clark, Antivirus Technology Consultant per Network Associates, il produttore del software anti-virus McAfee, utilizzato per proteggere oltre 70 milioni di desktop in tutto il mondo.

Grazie ai loro sforzi congiunti hanno identificato un numero sorprendente di aree dove esistono parallelismi di base tra i loro rispettivi campi di competenza. Molti di questi sono cruciali per la loro comprensione dei virus e per la loro continua lotta per sconfiggerli. Tra i più sorprendenti:

* **Entrambe le tipologie di virus hanno strutture simili fatte di "building blocks"**
* **Entrambi sono maestri di travestimento e usano spesso tecniche simili per nascondersi in modo da infiltrarsi e infettare nuovi sistemi**
* **Entrambi seguono il sole nella loro diffusione in tutto il mondo; spesso nascono in Asia e si diffondono da Est verso Ovest**
* **Sia le organizzazioni mediche che quelle tecnologiche utilizzano gli stessi coefficienti per categorizzare il rischio di infezione da virus e hanno i loro centri di ricerca collocati negli stessi punti nel mondo**
* **Sia coloro che combattono i virus nel settore medico che in quello informatico hanno dovuto recentemente fronteggiare un rischio aumentato di infezione da virus, e per le stesse ragioni**

Redatto in un linguaggio non tecnico in modo che gli esperti di entrambi i settori possano comprendere le scoperte ed i concetti correlati, questo rapporto esplora varie aree in dettaglio. Network Associates, sponsor della ricerca, si augura che riunendo le idee ed i pensieri più avanzati di entrambi i settori, questo studio servirà come spunto per una ricerca continua su questi parallelismi e forse porterà a progredire nella lotta contro tutti i tipi di virus.

CONTENUTI

SEZIONE 1:
I FONDAMENTALI

La chiave per comprendere i virus e come possono essere combattuti è capire la loro struttura di base. Da questo punto, coloro che combattono i virus possono iniziare a disporre di un quadro d'insieme dei punti di forza e delle debolezze di un particolare virus, del suo comportamento, dei meccanismi secondo i quali si replica e, fondamentale, i metodi che utilizza per travestirsi e ottenere l'accesso a un nuovo sistema. Sebbene sia relativamente semplice per gli esperti informatici anti-virus decostruire questi minuscoli puzzle, è solo recentemente che scoperte nella biologia molecolare hanno consentito a coloro che combattono i virus in campo medico di fare altrettanto.

Ciò ha portato ad alcuni dei più importanti progressi nella lotta ai virus in tutto il mondo.

I BUILDING BLOCKS (COMPONENTI)

I virus, sia in campo medico che informatico, sono costituiti da ampie stringhe di elementi di base. Tali elementi possono ottenere un "valore" uno su quattro per quanto riguarda i virus biologici o un "valore" uno su due per i virus informatici.

Un Virus informatico

Esiste un parallelo pressoché diretto tra i componenti, o building blocks, che costituiscono un virus biologico e un virus informatico.

Un virus biologico, come altri organismi viventi, è costituito da componenti di base denominati nucleotidi (un tipo di composto chimico). In un virus come quello dell'influenza esistono quattro tipi diversi di nucleotide standard – guanina, adenina, citosina e uracile. Utilizzando una serie di questi quattro diversi componenti di base e ordinandoli secondo una sequenza specifica, può essere costruito il codice genetico di qualsiasi virus d'influenza. All'interno di questo codice genetico si trovano serie di tre nucleotidi chiamati codoni. Stringhe di codoni formano i geni – (dieci nel caso dell'influenza), che rappresentano la struttura delle proteine – componenti chiave che aiutano a formare il virus e a determinare la sua funzione e le modalità d'attacco (payload).

Un Virus biologico

La dimensione del virus può essere misurata dal numero di nucleotidi di cui è composto. Un tipico virus dell'influenza ha all'incirca 13.700 nucleotidi, pari a 13,7 Kb (Kilobase). (Da notare che la dimensione sia dei virus biologici che di quelli informatici viene misurata in Kbs!).

Un virus informatico è, come qualsiasi informazione o programma presente sul vostro PC, costituito da una serie di bit (l'equivalente di un nucleotide in un virus biologico) - per esempio, un virus informatico è essenzialmente una lunga stringa composta dai

numeri 1 e 0. Ogni bit può essere "on", nel qual caso corrisponde ad un 1, o "off", nel qual caso corrisponde ad uno 0. I bit sono disposti in gruppi di otto conosciuti come byte (l'equivalente di un codone di un virus biologico). Stringhe di byte formano l'equivalente di un gene nei virus biologici, ed esattamente come questi ultimi, può essere ricostruito qualsiasi virus informatico, disponendo i bit in un ordine specifico

Inoltre, la dimensione di un virus è determinata dal numero di bit che contiene sebbene venga espresso in termini di Kilobytes. Per esempio, un tipico virus informatico come Love Letter, può contenere 80.000 bit pari a 10Kb. Il parallelo è pressoché identico. L'unica differenza è che l'elemento base di un virus biologico, il nucleotide, può assumere una su quattro forme, mentre l'elemento base di un virus informatico, il bit, può assumere solo una forma su due.

CLASSIFICAZIONE DEI VIRUS

Sia i virus biologici che quelli informatici, possono essere classificati secondo la loro "patogenicità".

A livello di base i virus biologici vengono classificati come patogeni (per esempio in grado di produrre malattie) o come non-patogeni. Esistono inoltre vari livelli di patogenicità; per esempio un virus "lieve" non patogeno di Influenza può costringervi a letto per un paio di giorni ma non avrà effetti permanenti, mentre un virus patogeno virulento, come il ceppo di influenza del 1918, potrebbe addirittura essere mortale.

I virus informatici possono essere classificati allo stesso modo. Molti virus, come quello denominato Anna Kournikova, non hanno un'azione distruttiva – ovvero non tentano di corrompere o cancellare alcun file o programma. Perciò possono essere classificati come "non patogeni".

I virus informatici che sono programmati per provocare danni, come I Love You, sono molto più pericolosi (patogeni) e possono danneggiare irrimediabilmente o eliminare i file dal sistema, oppure riscrivere il software di sistema interno del computer.

In entrambi gli ambienti, i virus possono essere patogeni in alcuni ma non in tutti i casi. Per esempio, nel mondo medico l'influenza può essere fatale in soggetti anziani deboli mentre può non essere assolutamente pericolosa in individui più giovani in buona salute. Ciò è paragonabile al mondo informatico, dove i virus possono essere patogeni su un computer che utilizza un particolare sistema operativo o programma (per esempio Windows 98 o Microsoft Outlook), mentre allo stesso tempo può rivelarsi non patogeno su altri sistemi (per esempio Apple Macintosh).

Oltre a ciò, i virus biologici possono essere patogeni in una persona e allo stesso tempo non patogeni in un altro individuo.

OTTENERE L'ACCESSO

I virus sono "parassiti" – hanno bisogno di un "ospite" all'interno del quale riprodursi.

I virus biologici non possono esistere da soli ma hanno bisogno di un ospite,

VIRUS NON PATOGENI

Sebbene possa sembrare strano, esistono virus che, almeno in apparenza, non sembrano causare alcun danno.

Sia il mondo medico che quello informatico sono ricchi di esempi – virus che possono passare da computer a computer e da persona a persona senza effetti palesemente nocivi.

Molte varietà di virus informatici non hanno un carico distruttivo – non fanno altro che replicarsi. Questi virus semplicemente si auto-copiano da PC a PC diffondendosi attraverso le reti. La loro pericolosità risiede nel fatto che si auto replicano all'infinito sovraccaricando così le reti e danneggiando i server di posta elettronica e anche parti di Internet. Anna Kournikova è un buon esempio di questo tipo di virus.

Esiste un fenomeno simile anche nel mondo medico. Le cellule possono essere infettate da virus senza causare apparenti effetti dannosi. Il virus schiumoso è un esempio di virus non patogeno assai diffuso in molte specie. Quando un essere umano ne viene infettato, questo provoca un'infezione a lungo termine e persistente pur non manifestandosi in modo molto evidente. Studi precedenti hanno evidenziato che il virus schiumoso era diffuso in alcune popolazioni. Ricerche più recenti non hanno confermato tali risultati ma hanno dimostrato che il trasferimento dell'agente infettivo direttamente da un individuo ad un altro avviene senza alcun effetto nocivo apparente.

una cellula vivente, all'interno della quale riprodursi. In termini medici questo viene riconosciuto come parassita obbligato. Per poter entrare nell'ospite alcuni virus, come l'HIV e il virus del vaiolo, contengono alcuni componenti della cellula ospitante che possono fungere da travestimento e/o interferire con i meccanismi di difesa dell'ospite, facilitando così la trasmissione da un essere umano ad un altro. Una volta entrato in un nuovo ospite, il virus (progenie) può assumere ulteriori travestimenti per proteggersi dal sistema immunitario dell'ospite. Per esempio, i virus incorporano i carboidrati derivati dalla cellula ospite nelle loro glicoproteine di superficie per aiutarsi a evitare le difese dell'ospite che li riconoscono come un pericolo. Altri virus, come la febbre gialla, non possono trasmettersi direttamente dal loro ospite naturale (le scimmie) negli esseri umani, ma lo fanno attraverso quello che è conosciuto come vettore, in questo caso la zanzara, che punge entrambi gli ospiti potenziali.

Virtualmente anche tutti i virus informatici sono parassitari. Si nascondono all'interno di vettori, un programma o un file, che consente loro di accedere a un nuovo computer (il nuovo "ospite"). L'ampiezza della portata di diffusione di un virus informatico dipende molto dall'appeal del vettore in cui si nasconde. Per esempio il virus Love Letter si è diffuso così velocemente perché "chi non desidera ricevere una lettera d'amore?" Allo stesso modo il virus Kournikova ha scatenato interesse verso la bella tennista. In entrambi i casi il vettore in cui il virus si nascondeva ha legittimato l'accesso ad un nuovo sistema, aiutandolo così ad aggirare le difese del sistema e a infettare il nuovo computer.

Un virus informatico ottiene l'accesso a un host

Un virus biologico ottiene l'accesso a un host

POSTA AEREA

Il meccanismo di diffusione più efficace nel mondo medico è attraverso l'aria. Nel mondo online il diretto equivalente è quello di utilizzare la posta elettronica per distribuire i virus informatici.

Una volta che un ospite viene infettato e il virus inizia a auto replicarsi, sia i virus biologici che quelli informatici utilizzano vari meccanismi di trasferimento per diffondersi in nuovi ospiti, non ancora infetti.

I virus biologici possono essere trasmessi da una persona all'altra in vari modi:

Per via aerea: Alcuni virus possono essere trasmessi da una persona all'altra semplicemente trovandosi insieme nella stessa stanza. L'influenza ne è un esempio.

Fluidi corporei: Lo scambio di fluidi corporei come sangue, saliva, secrezioni vaginali e sperma possono tradursi in infezione. L'HIV si trasmette in questo modo.

Da sangue a sangue: Alcuni virus possono sopravvivere solo nel sangue: un esempio è l'epatite B.

Feci/Orale: Alcuni virus si trasmettono come risultato di scarsa igiene come per esempio la Poliomielite .

Tramite vettore: Virus trasmesso tramite puntura di insetto o morso di animale, come la Febbre Gialla o la Rabbia.

Contact: Il virus si trasmette tramite contatto diretto con lesioni infette e barriere primarie danneggiate (la pelle) nel nuovo ospite, come per esempio il vaiolo.

Nel mondo medico i virus trasmessi per via aerea sono i più contagiosi perché si trasmettono facilmente ed è più difficile proteggersi in modo efficace. Questo perché non è necessario alcun contatto fisico per contrarre il virus; si trasmette nell'aria che respiriamo per rimanere vivo. Allo stesso modo, nel mondo informatico i virus vengono più facilmente disseminati attraverso il cyberspazio – di solito tramite posta elettronica. Anche in questo caso è molto difficile proteggersi da questi virus perché non è richiesto alcun contatto fisico tra i computer (una connessione permanente o la condivisione di un floppy disk). Internet e la posta elettronica sono fondamentali per la comunicazione ma a loro è legata la minaccia costante di infezione da virus. Altri metodi per contrarre un virus informatico sono:

Tramite indirizzi Internet - Trasmissione senza alcun – o minimo - intervento umano (per esempio Code Red), attraverso la scansione di PC vulnerabili.

Scambi personali - Trasmissione attraverso screensaver condivisi o l'invio/ricezione di cartoline augurali.

Condizioni di sopravvivenza favorevoli – Alcuni virus possono sopravvivere solo su certi sistemi operativi.

Tramite vettore - Trasmissione come risultato di un'azione come il doppio click su un file, scaricamento di un programma che può avere un virus allegato.

Contatto - Le probabilità di trasmissione aumentano quando due o più computer sono collegati tra loro.

Scarsa "igiene" - l'utilizzo non corretto di programmi o protezione non adeguata.

DAVIDE CONTRO GOLIA

Molti dei virus più intelligenti e pericolosi sia nel mondo medico che in quello informatico sono quelli di dimensioni più piccole.

Un ampio numero di virus che provocano i maggiori problemi negli esseri umani, come polio, HIV, influenza, morbillo e ebola, hanno un "genoma" di dimensioni relativamente piccole, che vanno da 7,4 Kb a 19 Kb. Al lato opposto della gamma dimensionale, variola, il virus che ha causato il vaiolo (che è stato dichiarato estirpato a livello mondiale nel 1980) ha un genoma di circa 190Kb ed è stato il primo virus animale visualizzato al microscopio.

Esiste una situazione similare nel settore dei virus informatici. Dalla metà alla fine degli anni '90, prima che si diffondesse massicciamente l'utilizzo di Internet e della posta elettronica, i virus informatici dovevano adattarsi all'area di boot di un floppy disk. L'area di boot di un floppy disk è un'area piccolissima di un dischetto che contiene informazioni sulle dislocazioni, dimensioni e nomi dei file presenti sul disco. Quindi, coloro che scrivono i virus devono ingegnarsi per comprimere il loro codice in uno spazio così limitato. Alcuni dei virus meglio progettati (da un punto di vista di programmazione) sono stati creati in questo periodo e molti sono ancora diffusi oggi.

IL PRIMO VIRUS AUTOSTOPPISTA...

Probabilmente ad oggi l'unico esempio di virus informatico che non richiede un vettore per trasmettersi è Code Red.

Simile ad un "autostoppista" questo virus non si nasconde all'interno di un programma o di un file ma piuttosto si annida nelle reti, esplorando le macchine collegate per individuare i punti deboli o vulnerabili che gli consentirebbero di infettare la macchina e da cui poi ripartire con l'esplorazione.

Ancora una volta tutto ciò trova un parallelo nel mondo medico. I virus colpiscono quelle cellule con "recettori" (o punti vulnerabili) specifici sulla loro superficie. Una volta che hanno trovato un ospite adatto possono poi replicarsi e colpire altre cellule che dispongono del recettore giusto.

Un esempio è il virus FORM, progettato per il sistema operativo MS-DOS, che infetta i settori di boot di floppy disk e hard disk e continua a prosperare.

Oggi, i virus informatici si diffondono principalmente tramite il download di file o gli allegati di posta elettronica. Ora, è molto facile per coloro che scrivono virus allegare ampi blocchi di codice a documenti o file senza che l'utente ne sia al corrente. Ciò significa che i virus possono essere di dimensioni più grandi e di conseguenza che coloro che scrivono i virus non devono essere così abili per crearli.

SEZIONE 2:
LA SCALA DEGLI ATTACCHI

Una delle principali preoccupazioni relative ai virus sia in campo medico che informatico è la loro capacità unica di diffondersi con un tasso esponenziale allarmante, lasciando una scia di danni enormi. Coloro che combattono i virus vigilano incessantemente e dispongono di eserciti di ricercatori in costante attesa di raccogliere informazioni su questi invasori quasi invisibili per iniziare a fronteggiarli.

È di fondamentale importanza chiarire la portata di ogni attacco e monitorare la velocità con cui avanza. Il centro nevralgico di questa operazione per i virus biologici, che ha funzioni di prima allerta su scala mondiale, è l'Organizzazione Mondiale della Sanità (World Health Organisation - WHO) con sede a Ginevra, Svizzera, mentre il corrispettivo per i virus informatici è il laboratorio Anti-Virus Emergency Response Team (AVERT) di Network Associates con sede a Aylesbury, UK.

VALUTARE IL PROBLEMA

Sia gli esperti medici che quelli informatici classificano il rischio potenziale di un virus utilizzando la stessa serie di coefficienti.

Quando viene identificato un nuovo virus è fondamentale che gli esperti valutino il rischio potenziale il più velocemente possibile in modo da prevenire una crisi potenziale. Gli esperti di entrambi i settori sono reperibili 24 ore al giorno, 365 giorni all'anno, pronti a entrare in azione immediatamente per poter classificare il rischio, iniziare a sviluppare metodi per combattere/contenere il rischio e, forse più importante, mantenere gli utenti di computer e i cittadini informati.

Nel mondo medico, la minaccia derivante da un virus particolare viene definita classificandolo in gruppi (o classi) di pericolo (o rischio). Il primo sistema di classificazione è emerso dal Centre for Disease Control (CDC) negli Stati Uniti negli anni '70. Sistemi di classificazione simili sono stati adottati dalla WHO (già siglato) e dall'Unione Europea, cosicché oggi esiste un sistema di classificazione adottato globalmente. Nel Regno Unito due enti determinano la classificazione di un virus. L'Advisory Committee on Dangerous Pathogens (ACDP) decide sui pericoli potenziali presentati da un nuovo virus e la sua classificazione. L'Advisory Committee on Genetic

VIRUS BIOLOGICI

Accesso - Quanto è facile per il virus infettare un uomo; per esempio, si trasmette per via aerea o solo tramite scambio di sangue?

Manifestazione - Il virus può replicarsi nell'uomo? (Un virus non umano ha un rischio minore di uno che viene riconosciuto come infettivo per l'uomo).

Danno - Quale il probabile risultato dell'infezione?

Protezione potenziale - Sono disponibili vaccini e quanto sono efficaci?

Immunità - Qual è lo stato attuale di immunizzazione contro il virus?

Attuali livelli di rilevazione - Quante persone sono state infettate dal virus fino ad ora? Quale è la diffusione geografica di questi casi (casi isolati o diffusi?).

Rischio ambientale - È correlato al potenziale di diffusione nella popolazione umana e in altri possibili ospiti se liberato dal laboratorio (i livelli rilevati nella popolazione in condizioni normali influiscono).

VIRUS INFORMATICI

Accesso - Il virus come entra nell'ospite? Ciò ha qualche effetto sulla velocità e facilità di diffusione del virus?

Manifestazione - Quale sistema attacca il virus e potrebbe replicarsi su larga scala se per esempio attaccasse un sistema diffuso come Microsoft Windows?

Danno - Quali danni potrebbero verificarsi in un computer infettato?

Protezione potenziale - I software anti-virus esistenti proteggono anche dal nuovo virus?

Immunità - Qual è lo stato attuale di protezione anti-virus?

Attuali livelli di rilevazione - Quanti casi sono stati rilevati al momento e su quale tipo di sistema è stato trovato il virus? Per esempio, l'infezione di una grande compagnia internazionale sarebbe considerata più pericolosa di quella di un PC domestico isolato.

Rischio ambientale - È correlato al potenziale di diffusione nelle reti informatiche mondiali se il campione fosse rilevato in modo esteso.

Modification (ACGM) valuta se le manipolazioni di microrganismi a scopo medico-industriale o di ricerca possano o meno avere effetti sul loro livello di classificazione. Non esiste alcun ente industriale che ricopra un ruolo equivalente nel mondo informatico; dipende dalle singole aziende produttrici di anti-virus. In Network Associates, Vincent Gullotto, Vice Presidente degli AVERT Labs, è responsabile del rilascio di una linea ufficiale sulla natura e il rischio potenziale di un nuovo virus.

VIRUS BIOLOGICI	VIRUS INFORMATICI
Livello 1 - Non pericoloso	**Rischio Minimo**
Livello 2 - Moderatamente pericoloso	**Rischio Medio**
Livello 3 - Pericoloso	**Rischio Elevato**
Livello 4 - Molto pericoloso	**Epidemia**

Sorprendentemente, sia gli esperti di virus biologici che informatici utilizzano metodi praticamente identici per classificare un nuovo virus e lo fanno utilizzando una serie rigida di criteri di valutazione:

In ambiente medico, un fattore tra 0 e 1 è attribuito a ciascuno dei criteri di valutazione pericolo/rischio e ciò consente agli organismi ACDP/ACGM di assegnare un virus a un livello di contenimento sul posto di lavoro. Esistono quattro livelli di contenimento, da 1 a 4, con il livello 1 come più basso (non pericoloso) e 4 come più elevato (molto pericoloso). I virus con punteggi di valutazione di pericolo/rischio basso rientrano nel livello 1. I virus come quello dell'influenza e il virus vaccino (un ceppo utilizzato nel debellamento del vaiolo) sono di livello 2, HIV e Febbre Gialla sono di livello 3, mentre ebola, vaiolo (l'agente patogeno del vaiolo) e il virus dell'influenza del 1918 sono a livello 4.

In Network Associates il processo è simile - con quattro "classi di contenimento"

RACCOGLIERE INFORMAZIONI DI BASE

Sebbene non esista alcuna disposizione ufficiale né per la WHO né per un produttore di anti-virus come Network Associates, entrambi utilizzano una rete di professionisti o aziende per raccogliere informazioni fin dalle radici.

Il WHO utilizza i medici di famiglia locali che inviano spontaneamente campioni prelevati da pazienti che presentano sintomi respiratori simili a quelli dell'Influenza. Ciò consente ai gruppi di sorveglianza di misurare i livelli di Influenza nella comunità e tenere traccia di tipologie e ceppi del virus anno su anno.

Analogamente, Network Associates dispone di una rete di clienti che inviano volontariamente e regolarmente informazioni sui virus individuati e campioni di qualunque tipo di virus rilevato. Network Associates utilizza queste informazioni per estrapolare i livelli di diffusione dei virus e sviluppare soluzioni a nuove tipologie di virus circolanti.

È la buona volontà e il senso civico di pochi medici di famiglia e individui che aiutano a proteggere l'intera popolazione dai virus biologici e informatici.

equivalenti – sebbene, come spiegato in precedenza, tale valutazione è effettuata sulla base dell'esperienza e competenza di un dirigente di alto livello dell'azienda piuttosto che secondo un severo criterio di valutazione.

La classificazione deve essere effettuata velocemente poiché le aziende di anti-virus devono informare l'intera comunità informatica del rischio, senza causare allarmismi o panico. Per questo motivo, un team specifico in Network Associates è preposto a prendere decisioni in modo veloce e responsabile.

Una differenza fondamentale è, a differenza della professione medica, che non esistono criteri di classificazione standard o enti di sorveglianza per la valutazione del rischio legato ad un virus nel mondo informatico. Come risultato si crea una potenziale confusione, poiché un produttore di software anti-virus potrebbe assegnare ad un virus un "rischio basso" mentre un altro potrebbe classificarlo come "rischio elevato".

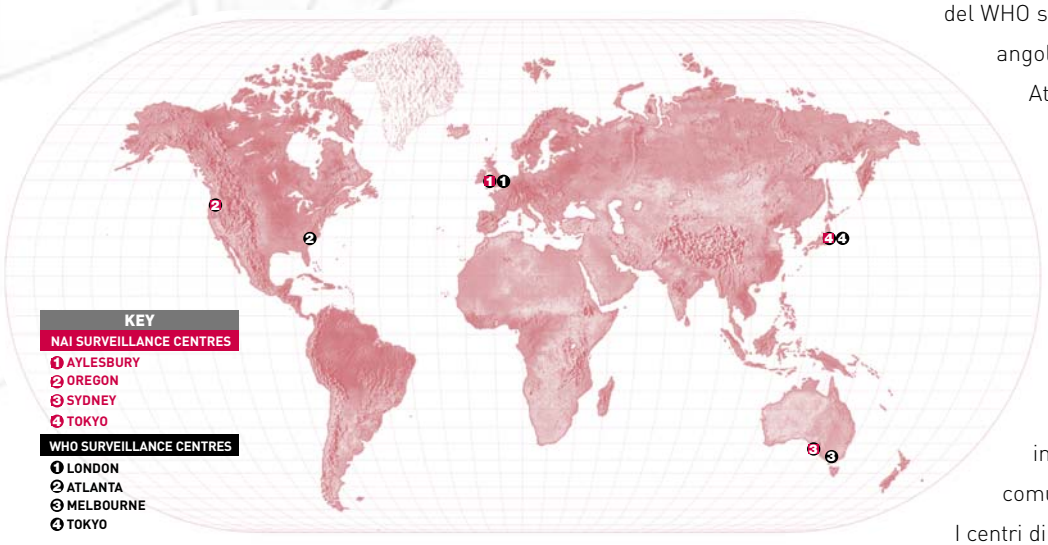
Una volta che un virus viene classificato è necessario comunicarlo il più velocemente possibile a medici di famiglia, ospedali e cittadini nel mondo medico, o utenti aziendali e privati nel settore informatico. In entrambi i settori ciò viene effettuato utilizzando varie modalità di comunicazione tra cui Internet, dichiarazioni o note di avviso a medici generici o Responsabili IT e alla stampa. L'intero processo, che va dall'identificazione di un nuovo virus alla sua classificazione, alla comunicazione del rischio al pubblico di riferimento, può durare settimane nel mondo medico, mentre in quello informatico può essere solo questione di poche ore.

METODI DI SORVEGLIANZA

Coloro che combattono i virus come Network Associates e l'Organizzazione Mondiale della Sanità (WHO) hanno strutture più o meno identiche per tracciare la diffusione dei virus.

Sia i virus biologici che quelli informatici vengono tracciati su scala globale. Entrambe le organizzazioni hanno centri situati in punti strategici in tutto il mondo che raccolgono informazioni locali e le inseriscono in un sistema di risorse centrale.

I quattro principali centri del programma di sorveglianza dell'influenza del WHO sono dislocati ai quattro angoli del mondo: Londra, Atlanta, Melbourne e Tokyo. Più o meno gli stessi posti in cui hanno sede i principali centri di controllo di Network Associates. Queste città rappresentano i centri regionali più popolati nel mondo con una buona infrastruttura di comunicazione.

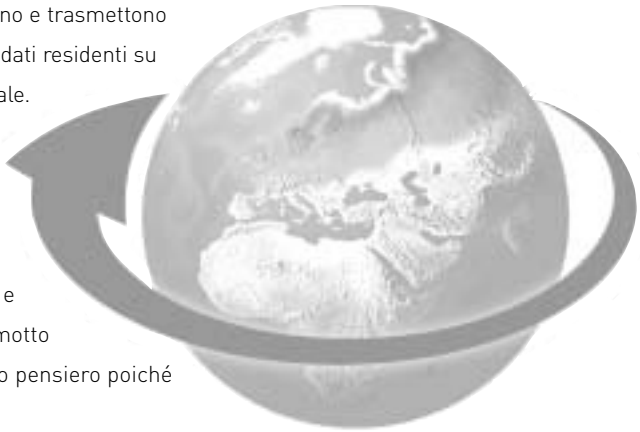


I centri di controllo sono

fondamentalmente hub di comunicazione, che raccolgono e trasmettono informazioni correlate a milioni di persone e miliardi di dati residenti su computer e in risposta a un database informativo centrale.

I loro principali obiettivi sono quelli di tracciare le tipologie e il numero di virus sia medici che informatici in circolazione, ragguagliare sulle misure precauzionali e implementare azioni appropriate per combatterli.

Sia il WHO che Network Associates devono educare e informare senza causare panico nella popolazione. Il motto degli AVERT Labs di Network Associates riflette questo pensiero poiché intende "Informare e Allertare, non Allarmare".



DA EST A OVEST

Un numero elevato di virus informatici e influenzali nascono in Asia.

Molti nuovi ceppi patogeni di influenza negli esseri umani sono arrivati a noi tramite animali come maiali, polli e uccelli acquatici. L'Asia ha un'elevata densità di popolazione e gli esseri umani tendono a vivere vicino ai loro animali. Tali fattori hanno contribuito a fare dell'Asia la fonte di ceppi pandemici di influenza sia nel 1957[3] che nel 1968[4], nonché il luogo dove il virus H5N1[5], potenzialmente letale, si è diffuso nella popolazione nel 1997.

Anche la grande maggioranza di virus informatici famosi sono stati creati o sono stati diffusi per la prima volta in Asia. Il perché di questo fenomeno è un po' più oscuro.

I virus informatici viaggiano da Est a Ovest come il sole. Questo perché di

WHO: Identificazione, il più presto possibile, dei ceppi di virus d'influenza in circolazione

WHO: Quantificazione della vastità della circolazione dell'influenza in relazione ai precedenti periodi di attività

WHO: Valutazione del contributo relativo di diversi tipi, sottocategorie o ceppi di virus influenzale al verificarsi della malattia, includendo malanni simili all'influenza nella comunità

WHO: Valutazione del contributo dell'influenza alla malattia in vari gruppi all'interno della popolazione, in particolare per regione geografica, gruppo d'età e se rilevata in ospedale o in pazienti in comunità. Ciò porterà a raccomandazioni per la formulazione di vaccini da utilizzare nella "stagione influenzale" in arrivo e per sostenere le Amministrazioni nel decidere quando/se implementare i loro "Piani Pandemici"

McAfee: Identificazione, il più presto possibile, dei tipi di virus in circolazione

McAfee: Valutazione dei probabili livelli di diffusione di nuovi tipi di virus

McAfee: Valutazione delle diverse tipologie di carico d'attacco e metodi di infezione del nuovo virus

McAfee: Sviluppo di patch o metodi preventivi per combattere ulteriori attacchi del virus

[3]A/Singapore/1/1957 (H2N2) [4]A/Hong Kong/1/1968 (H3N3) [5]A/Hong Kong/156/1997

solito si diffondono quando i computer vengono accesi al mattino, così quando ogni parte del mondo si risveglia, attivano nuovi virus e li diffondono prima che venga implementata una soluzione efficace.

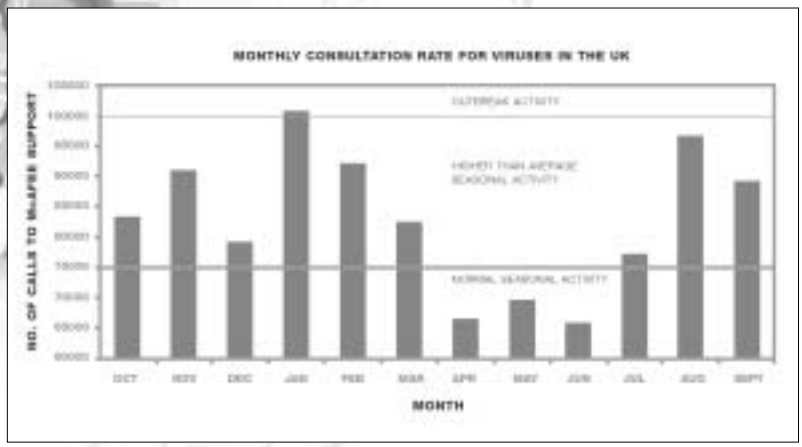
Per far sì che un virus "abbia successo" (dal punto di vista di chi scrive) deve aver costruito una "testa di ponte" nel momento in cui colpisce gli Stati Uniti, dove si trovano la maggior parte dei computer e dei principali server del mondo. Ciò significa che deve essere lanciato in Asia o Australasia in modo che nel momento in cui colpisce la Costa Ovest degli Stati Uniti possa realmente creare dei danni. Esempi recenti sono i virus Love Letter e Nimda.

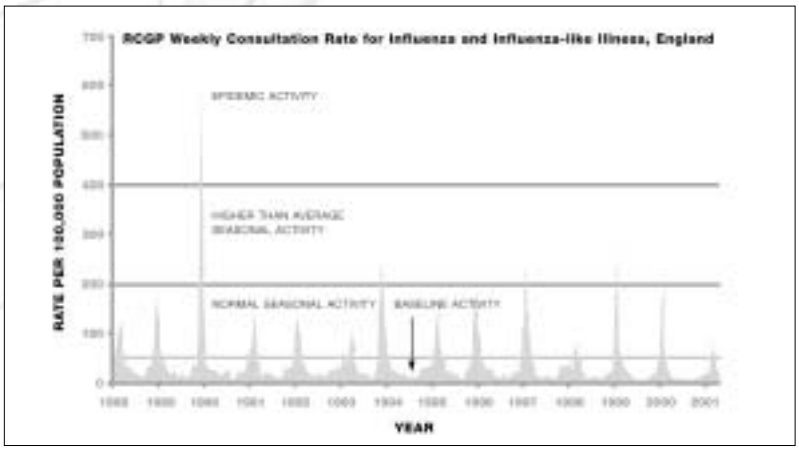
CHI È PIÙ A RISCHIO E QUANDO?

Gli indifesi, gli anziani e i deboli sono più a rischio di infezione da virus.

Qualsiasi virus rappresenta un rischio solo se non si è adeguatamente protetti. Per gli esseri umani significa che il sistema immunitario deve essere sufficientemente forte per poterlo combattere o è stato "addestrato" a combatterlo grazie a un vaccino preventivo. Le informazioni relative ai virus riconosciuti da un singolo ospite sono memorizzate nella sua "Memoria" Immunologica (che può essere considerata alla pari di un file DAT per i PC – vedi sotto).

L'esatto equivalente del sistema immunitario nel mondo dei computer è il suo software anti-virus. Per essere in grado di combattere un virus, un computer deve avere un software di protezione contro i virus in grado di riconoscerli. Le informazioni relative a tutti i vari tipi di virus e a come combatterli sono memorizzate in un particolare file all'interno del software anti-virus – denominato file DAT. Quando un utente "aggiorna" il proprio software anti-virus, aggiunge nuove informazioni al file DAT in modo che il suo sistema sia in grado di "riconoscere" nuovi tipi di virus.





VIRUS STAGIONALI

Sia i virus biologici che quelli informatici tendono a colpire in particolari periodi dell'anno.

Molti virus, in particolare quelli che interessano il sistema respiratorio, sono stagionali. Nell'emisfero Nord la stagione influenzale è solitamente intorno ai mesi di Dicembre, Gennaio e Febbraio, periodo in cui la funzione immunitaria del corpo viene compromessa dalla larga diffusione di molte malattie (in particolare respiratorie) e da fattori ambientali come periodi di luce più corti, temperature ambientali più

basse e, in alcune zone geografiche, minor disponibilità di cibo, tutti fattori che contribuiscono a ridurre il senso di benessere. In generale, ciò causa una predisposizione alle infezioni, ed esiste inoltre un maggior rischio di diffusione dei virus dovuta allo stare insieme in famiglia o in gruppo durante le festività.

Allo stesso modo avviene per i virus informatici, dal momento che molti sono creati per sfruttare le stagioni. Il periodo natalizio è il peggiore a causa dell'elevato numero di auguri, inviti, barzellette e programmi legati al Natale che si diffondono tramite posta elettronica – il perfetto "vettore" per i virus.

Alcuni tipi di virus restano dormienti su un computer fino a una particolare data e periodo prima che facciano esplodere la loro carica distruttiva. Il virus CIH ne è stato un perfetto esempio.

SEZIONE 3: **AFFRONTARE IL PROBLEMA**

Recenti passi in avanti in entrambi i settori, insieme all'enorme potenza di elaborazione dei computer oggi largamente disponibile, hanno permesso a coloro che combattono i virus di essere meglio attrezzati nel comprenderli e osteggiarli. La definizione di un virus come "agente che sfugge ai filtri, troppo piccolo da poter essere osservato al microscopio ottico, ma in grado di causare malattia moltiplicandosi in cellule viventi", ha avuto origine nel tardo diciannovesimo secolo. Quello della febbre gialla è stato il primo virus derivato dall'uomo ad essere identificato (1901) e quello dell'influenza venne isolato prima dai maiali nel 1930 e poi dagli esseri umani nel 1933. Da allora, ci è voluto circa un secolo di ricerche da parte di esperti medici virologi per sviluppare le tecniche necessarie per studiare a fondo i virus. Per contro, il primo virus informatico venne elaborato a metà degli anni '80 e gli esperti in virus hanno drammaticamente affinato la propria abilità nel corso degli ultimi 15 anni.

PREVENIRE È MEGLIO CHE CURARE

Sia in ambiente medico che informatico, lo strumento più efficace per combattare l'infezione è la vaccinazione.

Gli esperti in medicina non possono ancora "guarire" le vittime attaccate dai virus, ma hanno sviluppato una serie di metodi per aiutare il corpo a combattare l'infezione. Il metodo più efficace è sicuramente la vaccinazione.

Un vaccino è tradizionalmente una piccola quantità di una versione

I VIRUS COLPISCONO I PIÙ DEBOLI

- Negli esseri umani, i bambini sono particolarmente sensibili ai virus perché il loro sistema immunitario non è ancora completamente sviluppato
- Sono sensibili ai virus gli esseri umani che non sono stati vaccinati contro un particolare virus
- Sono a rischio le persone più anziane, il cui sistema immunitario è debole e non perfettamente funzionante
- I PC che non hanno un software anti-virus aggiornato contro un particolare virus sono sensibili ai virus
- Sono a rischio anche i nuovi computer a cui non è ancora stato installato un software anti-virus
- I vecchi computer con software anti-virus non aggiornato sono a rischio

attenuata (che può essere somministrata in forme "vive" o "uccise") o un insieme di alcuni componenti antigenici di una forma più virulenta di un particolare virus. Questo viene tradizionalmente iniettato nel corpo consentendo al sistema immunitario di "imparare" a riconoscerlo ed essere in grado di combatterlo in futuro. Sono stati inoltre sviluppati metodi moderni che utilizzano proprio il codice genetico del virus – i cosiddetti vaccini DNA/ricombinanti.

Per preparare i vaccini, i virus vengono introdotti sia in ospiti che non siano esseri umani, come per esempio l'uovo di una gallina per l'influenza, sia in cellule, talvolta di origine umana, allevate in laboratorio. Il virus prodotto viene purificato e ne viene controllata la sterilità (assenza di altri agenti infettivi e tossine potenziali) prima di renderlo disponibile alla comunità medica per la somministrazione.

Sebbene i computer possano "guarire" dopo aver contratto un virus, nel momento in cui viene adottata una cura spesso è troppo tardi per recuperare i dati perduti. È molto più efficace "vaccinare" i computer contro la possibilità di contrarre un virus prima di tutto. L'equivalente informatico di un vaccino è un'iniezione di informazioni nel file DAT del suo anti-virus. Il file DAT è fondamentalmente una lista di "firme" di un virus (una sorta di fotografia di come è fatto ciascun virus) che gli consente di riconoscere e identificare ogni singolo virus che potrebbe incontrare. Quando un nuovo file viene analizzato, il software anti-virus esegue il file DAT controllando, a livello di componenti di base di bit e byte, l'esistenza di qualsiasi firma di un virus. Se ne trova uno può allertare l'utente della presenza del virus e lo rimuove se possibile.

Aggiungere una nuova firma di un virus al file DAT (aggiornandolo) significa insegnare al software anti-virus a riconoscere un nuovo virus fornendogli i mezzi con cui potrà combatterlo in futuro.

PRECAUZIONI

VIRUS INFORMATICI

- Usare il buon senso! Per esempio non aprire allegati sospetti da mittenti sconosciuti e porre attenzione al download di file da Internet
- Aggiornare regolarmente il software anti-virus
- Effettuare il backup regolare dei file
- Salvare i documenti word in formato testo o rtf (rich text format)
- Utilizzare il PC dell'ufficio solo per lavoro
- Evitare i programmi che sembrano "divertenti"
- Consultare gli esperti di anti-virus per sviluppare una policy di sicurezza efficace
- Cancellare messaggi e-mail tipo catene di S.Antonio e messaggi "stupidi"; sono considerati spam, che servono solo ad intasare la rete

VIRUS BIOLOGICI

- Usare il buon senso! Non mettersi in una situazione a rischio di virus – per esempio, se è necessario fare un'iniezione non condividere gli aghi con persone che non si conoscono
- Mangiare in modo sano e assennato, praticare un moderato esercizio fisico e dormire adeguatamente per preservare il sistema immunitario
- Procreazione sotto controllo – esiste un contributo genetico fondamentale alla resistenza a malattie/infezioni che stiamo iniziando ora a decifrare
- Prevenzione tramite vaccinazione – Alla fine l'assunzione di buoni vaccini preventivi è la migliore soluzione

Molto interessante è il fatto che se oltre il 70% della popolazione venisse vaccinata si potrebbe raggiungere "un'immunità di massa" e limitare significativamente il diffondersi dell'influenza. La maggioranza delle persone infettate dal virus influenzale sopravvive grazie all'efficienza del proprio sistema immunitario ma alcuni sviluppano complicazioni cardiache e/o al sistema nervoso centrale. Sebbene non si conosca una terapia specifica per l'influenza, possono essere somministrati medicinali per ridurre la virulenza dell'infezione e quindi alleviare la gravità della malattia.

PREVENIRE L'ATTACCO

Pochi e semplici passi per non essere attaccati dai virus.

Esistono varie precauzioni molto simili da mettere in atto per proteggersi sia dai virus biologici che da quelli informatici.

COMBATTERE L'INFEZIONE

Comprendere come opera un virus è la chiave per scoprire un vaccino.

Sebbene i virus biologici esistano da migliaia di anni è solo negli ultimi 30-40 anni che gli scienziati hanno iniziato realmente a comprenderli. Fin dagli anni '70 i ricercatori sono riusciti a scoprire i segreti di come sono costruiti e come funzionano i virus e come interagiscano con i loro ospiti. Ciò è avvenuto grazie allo sviluppo delle tecniche di biologia molecolare che consentono agli scienziati di:

- mutare i virus in modi che non si vedono spesso in natura e studiare gli effetti di tali mutazioni sulla replicazione del virus e la loro patogenesi,
- sezionare i geni individuali dei virus e definire quali funzioni delle proteine codificate sono in isolamento, esprimendole in potenziali cellule ospiti.

Di base, essendo in grado di isolare un virus e ricostruirlo, i ricercatori forniscono informazioni cruciali per lo sviluppo dei vaccini.

I virus informatici sono molto più semplici (al confronto!) da scoprire e ricostruire in modo da poter creare dei "vaccini". Questo perché non appena gli esperti dei laboratori AVERT di Network Associates dispongono di un campione di un nuovo virus possono esaminarne il codice in dettaglio e osservare il suo comportamento più e più volte in laboratorio. In questo modo possono comprendere i meccanismi che questo utilizza per replicarsi e diffondersi.

Comunque, in entrambi i settori, il numero di virus in circolazione sta crescendo e sono stati sviluppati nuovi metodi per identificarli. Uno di questi, l'adozione di un approccio euristico, è stato utilizzato dagli esperti in virus sia medici che informatici.

EURISTICA

Recenti progressi in termini di potenza elaborativa dei computer hanno consentito a coloro che combattono i virus sia in campo medico che informatico di identificare nuovi virus ancora sconosciuti in modo più efficiente utilizzando un approccio euristico.

L'euristica è un metodo per identificare genericamente i virus rispondendo in modo effettivo a un gioco di 20 domande. Per i virus nuovi e sconosciuti esiste un approccio più veloce rispetto al controllare esattamente se un nuovo campione corrisponde o meno ad una lista di tutti i virus conosciuti.

Sia nel mondo medico che in quello informatico, ciò è diventato possibile solo grazie ai progressi effettuati nella tecnologia e nella potenza di elaborazione, che consente al software di analizzare in modo efficace domande e risposte alla velocità della luce. In passato ciò era impossibile perché, per quanto riguarda il mondo medico, esistevano troppe domande da porre per essere in grado di utilizzare questo metodo in un periodo di tempo utile. Nel mondo informatico, gli utenti non vogliono assolutamente avere alcun tipo di ritardo causato dal loro software anti-virus. L'euristica non si è perciò rivelata un metodo utile fino a un paio di anni fa, quando i processori sono diventati abbastanza potenti da poter gestire un numero enorme di calcoli nel tempo necessario, portando avanti allo stesso tempo altre operazioni.

Questo sistema funziona ponendo una serie di domande e, a seconda dei risultati, identifica il codice valido o i virus definiti/potenziali. Ciò può essere fatto utilizzando l'euristica positiva o negativa:

- L'euristica positiva cerca di ottenere un'identificazione positiva di un virus ricavando risposte positive. Per esempio, "Si trasmette tramite e-mail a chiunque nell'indirizzario?" Se la risposta è sì, allora si passa alla domanda successiva.
- L'euristica negativa funziona in senso opposto cercando di identificare i virus potenziali ottenendo risposte negative. Per esempio, "È un programma registrato?" Se la risposta è no, si passa alla domanda successiva.

Identificando i virus in questo modo, gli esperti possono essere preavvertiti di potenziali problemi e sviluppare strategie per combattere i virus, alcuni dei quali mai incontrati prima.

IL SANTO GRAL

Né il mondo informatico né quello medico saranno mai in grado di eliminare o sconfiggere completamente i virus.

In generale i vaccini ed i programmi anti-virus non sono efficaci al 100%, sebbene il vaiolo sia stato "estirpato" nel 1980 a seguito di una lunga ed intensiva campagna di vaccinazione mondiale. Attualmente, il vaccino per l'influenza più efficiente ha un'efficacia del 70%. Allo stesso modo, gli esperti informatici anti-virus non potranno mai rendere un computer totalmente sicuro. La ragione principale in entrambi i casi è il tasso di mutazione dei virus che costringono gli esperti di entrambi i settori ad una continua rincorsa.

Negli esseri umani, i virus mutano naturalmente finché il più recente

vaccino non è più efficace. I vari virus mutano in modi differenti così che mentre alcuni vaccini possono dare una protezione per tutta la vita, per mantenere attiva la protezione contro il virus dell'influenza i singoli devono ricevere vaccini nuovi e aggiornati. Per esempio, un tipico vaccino per l'influenza potrebbe essere efficace per circa cinque anni prima che il virus muti in maniera tale che la risposta immunitaria ricavata dal vaccino non sia più in grado di riconoscerlo. I ricercatori quindi devono formulare un vaccino completamente nuovo.

Allo stesso modo, per quanto sia efficace il più recente software anti-virus, coloro che scrivono i virus analizzano costantemente il suo codice per identificare dei "buchi" attraverso i quali poter inserire il loro ultimo virus. Oltre a tutto ciò, i virus più recenti e i loro metodi di infezione trovano un limite solo nell'immaginazione umana e non è realistico immaginare un pacchetto software anti-virus impenetrabile a meno che non lasci assolutamente nulla sul PC!

Infatti, l'unico modo reale in cui i computer e gli esseri umani possono rimanere immuni dalle infezioni al 100% è essere tenuti in quarantena, senza modo di condividere informazioni o entrare in contatto con un portatore di virus o un virus che si trasmette tramite l'aria. È una soluzione, sebbene piuttosto radicale!

SEZIONE 4:
UN RISCHIO MAGGIORE

Sebbene esistano descrizioni di una malattia simile all'influenza a partire dal V secolo A.C., la prima pandemia ben documentata è quella dell'influenza del 1918. In modo simile, il primo virus informatico ufficialmente riconosciuto - "Brain"- è stato identificato nel 1986 nonostante solo nel 1999, con il manifestarsi del virus Melissa, il mondo si è trovato di fronte alla prima epidemia registrata causata da un virus informatico.

Non è una coincidenza il fatto che le prime pandemie abbiano impiegato così tanto tempo a manifestarsi e in entrambi i casi le probabilità di epidemia più frequenti e anche peggiori sono più forti che mai. La crescente minaccia rappresentata da parte dei virus sia medici che informatici non è dovuta solo all'evoluzione dei virus stessi, ma anche a una serie di cambiamenti fondamentali nel nostro modo di vivere.

AEROPLANI, TRENI E POSTA ELETTRONICA...

I rischi di pandemie mediche e di epidemie informatiche sono cresciuti notevolmente negli ultimi anni per ragioni fondamentalmente molto simili.

Ci sono due ragioni fondamentali per l'aumento delle minacce da parte dei virus: la crescita della popolazione e l'infrastruttura dei trasporti.

La crescita della popolazione mondiale (sia in termini di computer che umana) durante gli ultimi anni è la ragione più ovvia.

Con sempre più portatori potenziali di virus che entrano in contatto con un

numero sempre maggiore di ospiti potenziali il rischio di un'infezione molto estesa aumenta ogni giorno. Inoltre, in ognuno dei due settori, si è verificato uno sviluppo cruciale che ha aumentato il problema potenziale.

In passato, sia i virus biologici che quelli potenziali sembravano essere confinati in un'area geografica specifica. Ciò perché si verificavano pochi contatti tra le persone o i computer attraverso le frontiere internazionali. Con l'avvento dei trasporti aerei e di Internet, i virus odierni possono diffondersi in modo molto semplice e veloce in tutto il mondo. L'epidemia di influenza del 1918 ci mise quattro mesi per diffondersi nel globo a causa del vasto numero di soldati e lavoratori che attraversavano le frontiere portando l'infezione con loro. Oggi, con l'ordinarietà dei viaggi aerei, è questione di giorni.

Allo stesso modo, prima dell'avvento di Internet, un virus informatico poteva metterci anni per diffondersi nei continenti poiché poteva essere trasmesso da macchina a macchina solo tramite floppy disk. Questo ovviamente restringeva il potenziale di diffusione del virus. Oggi, con l'uso pressoché universale della posta elettronica e di Internet questo processo può avvenire in pochi secondi.

Molto interessante è il fatto che sia stata la prima epidemia registrata causata da un virus informatico nel 1999, Melissa, a dare il via alla creazione di un programma formale di valutazione del rischio per preallertare gli utenti di computer dei potenziali danni causati da nuovi virus.

I viaggi internazionali e Internet sono perciò i principali fattori determinanti della massiccia crescita nella minaccia dei virus sia per gli esseri umani che per i computer.

IL POTERE DELLA RETE

La crescente disponibilità dei "blueprints (struttura)" dei virus su Internet ha aumentato il pericolo rappresentato dai virus biologici e informatici.

Ovviamente, tutti i virus informatici sono scritti dagli uomini, tuttavia esiste un crescente rischio di virus biologici creati in laboratorio dall'uomo e rilasciati all'esterno sia in modo involontario o volontario. Per esempio, un numero ristretto di persone ha ipotizzato che l'HIV potrebbe essere un virus creato dall'uomo.La ragione di ciò è che le istruzioni per creare virus sia medici che informatici sono disponibili gratuitamente su Internet e con il crescente numero di programmatori tecnici esperti e i progressi nella scienza medica molti virus oggi potrebbero essere creati in un laboratorio o sul Pc di casa.

È improbabile, nel prossimo futuro, che i virus biologici possano essere "assemblati" a casa da adolescenti curiosi così come avviene per molti virus informatici – ma è possibile che ciò possa cambiare nel lungo termine.

La legge può essere d'aiuto fino a un certo punto. Per esempio, attualmente in molti paesi non è illegale per un Internet Service Provider (ISP) ospitare istruzioni su come creare qualsiasi tipo di virus. Alcune misure sono già state prese – per esempio fino a poco tempo fa, programmare un virus informatico faceva parte del (programma) di alcuni corsi per computer – ma molte altre ancora dovranno essere adottate.

MUTAZIONE

Il maggior problema con entrambi i tipi di virus è che mutano ad una tale velocità che le misure anti-virus non riescono a tenere il passo.

Sia i virus biologici che quelli informatici mutano con un ritmo elevato, il che li rende obiettivi in continuo cambiamento per le misure anti-virus. Gli esperti in entrambi i settori non possono far altro che lavorare alacremente per combattere il presente. Per esempio, i ricercatori medici possono sviluppare un vaccino per un ceppo di virus, ma entro breve il virus sarà mutato a un tale livello che il vaccino non sarà più efficace. Allo stesso modo, coloro che compilano i virus informatici possono prendere il ceppo originale di un virus e adattarlo per colpire vari punti di vulnerabilità di un computer aggirando così le misure anti-virus esistenti.

È praticamente impossibile per gli esperti di entrambi i settori prevedere quale sarà il prossimo virus a colpire e sviluppare in modo proattivo metodi per combatterli. Purtroppo, si reagisce sempre "a posteriori".

Nuovi virus biologici appaiono come risultato di una mutazione, che avviene casualmente durante il processo di replicazione del virus. Sebbene molte di queste nuove mutazioni siano nocive, solo un piccolo numero diventerà trasmissibile e genererà, quindi, ceppi epidemici. Ogni nuovo ceppo di un virus individuato viene classificato secondo le sue caratteristiche – per esempio tre tipi di influenza (A, B e C) infettano l'uomo, ma le pandemie mondiali sono state associate solo al tipo A e, mentre il tipo B può causare epidemie, i virus di tipo C provocano malattie di lieve entità. I virus di tipo A possono essere classificati ulteriormente sulla base del loro subtipo di Emoagglutinina (H) - di cui ne esistono quindici H1-15 conservate negli uccelli. Solo tre subtipi H1-3 hanno causato pandemie nell'uomo.

Le emoagglutinine dei virus influenzali sono responsabili dell'inizio dell'infezione. Modifiche o mutazioni al loro interno contribuiscono alla loro capacità di sfuggire dalle risposte del sistema immunitario e continuare a diffondersi nella popolazione umana. Determinando le sequenze dei geni di emoagglutinina dell'influenza, i ricercatori medici possono costruire "alberi" filogenetici (o evolutivi) per i virus in circolazione nell'uomo per aiutarli a mappare lo sviluppo di un particolare tipo di virus. Comprendendo come mutano questi virus, i ricercatori possono cercare di prevedere come possono evolversi in futuro per avere più tempo a disposizione per lo sviluppo di misure preventive contro una possibile pandemia.

La capacità di costruire "alberi" di virus è relativamente nuova, grazie all'avvento di tecniche di ordinamento rapido dei geni e la disponibilità di elevata potenza elaborativa dei computer. Comunque, a differenza di quanto avviene nel mondo informatico, sarà impossibile ottenere una fotografia evolutiva completa per l'Influenza poiché i metodi per isolare i virus sono stati disponibili solo a partire dagli anni '30.

Mentre un virus informatico in grado di mutare seguendo percorsi simili a quelli di un virus biologico deve ancora essere creato, essi mutano effettivamente tramite un processo di continuo aggiornamento, "sniffing" e riscrittura. Questo processo è il risultato della continua battaglia tra coloro

LA STORIA DELLE PANDEMIE

Fin da quando se ne ha memoria ci sono state solo 4 pandemie di influenza negli esseri umani – 1889/90, 1918, 1957 e 1968. Il numero di epidemie mondiali per i virus informatici è simile – solo 2-4 all'anno a partire dal 1999.

Il problema principale è che nessuno sa in entrambi i casi quando scoppierà la prossima "bomba"...

che scrivono i virus cercando di aggirare nuove misure di sicurezza e le società di anti-virus che cercano di fermarli! Per esempio, quando si è manifestato il virus Love Letter, i produttori di anti-virus hanno sviluppato velocemente un aggiornamento per il loro software per proteggersi. Non appena questo è apparso, i virus writer sono riusciti a capire come funzionava l'aggiornamento e a produrre un nuovo "ceppo similare" di Love Letter. Questo processo è continuo, tanto che esistono oltre 30 derivati del virus Love Letter!

IL VIRUS EVOLVE

I sistemi "immunitari" sia medici che informatici dell'anno scorso potrebbero essere in gran parte inefficaci oggi.

Il grado di evoluzione a cui i virus sia medici che informatici sono sottoposti nel tempo porta i "sistemi immunitari" sia dell'uomo che dei computer ad adattarsi in modo che un sistema immunitario di soli pochi decenni fa potrebbe essere praticamente inefficace oggi.

Il sistema immunitario umano richiede "un'istruzione" nel tempo per essere in grado di distinguere tra agenti immunizzanti che dovrebbero essere presenti nel corpo e quelli che non dovrebbero esserci. Acquisisce memoria immunitaria con l'esposizione ad antigeni estranei, tra cui agenti infettivi e vaccinazioni, come il vaccino anti influenzale, per stroncarli. Quindi, se si potesse prendere un essere umano di 100 anni fa e collocarlo nell'ambiente odierno, probabilmente soccomberebbe molto velocemente all'esposizione ad un virus perché non riconoscerebbe (non essendo mai stato esposto) molti degli agenti infettivi attualmente in circolazione.

Allo stesso modo un sistema immunitario informatico – il file DAT – è "allenato" a riconoscere nuovi virus grazie all'incessante attività di aziende come Network Associates. Risulta quindi vitale che gli utenti aggiornino il file DAT regolarmente poiché un file DAT vecchio è totalmente inefficace contro i virus più recenti. A causa della velocità con cui i virus informatici vengono generati, se aggiornate il vostro software antivirus saltuariamente ha la stessa efficacia che se provaste a proteggere il vostro PC con un software anti-virus di dieci anni fa – non passerebbe molto tempo prima di rimanere infetti![6]

LE CONSEGUENZE FINALI

Gli effetti di un virus diffuso su vasta scala sono potenzialmente enormi, in termini di perdite di uomini e/o ore PC.

Naturalmente le conseguenze finali provocate da un virus informatico non sono comparabili con gli effetti di un virus umano.

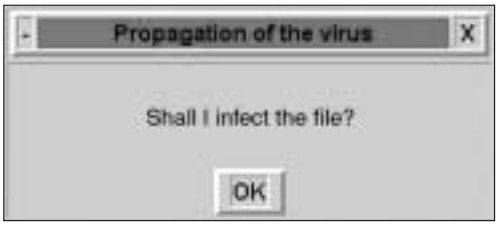
L'influenza uccide normalmente circa 3.000 persone all'anno in Inghilterra. Il 1999 è stato un anno particolarmente "orribile" con 20.000 morti a causa del virus.

Tuttavia, alcuni parallelismi possono essere ricavati, dal momento che gli effetti di ceppi di influenza meno pericolosi hanno delle similitudini nel mondo informatico.

Sia il virus dell'influenza che i virus informatici hanno un maggior effetto

[6]Data from Computer Economics, 2001

sulle aziende – Il Consumer Health Information Centre stima che in Inghilterra oltre 150 milioni di giorni lavorativi vengono persi ogni anno a causa di "malanni legati all'influenza" per un costo di 6.75 miliardi di sterline. Allo stesso modo i virus informatici hanno un enorme effetto in campo finanziario. File persi o danneggiati portano a ingenti perdite di informazioni, costringono a dover rifare il lavoro e riducono la produttività: tutti effetti reali causati da un virus informatico. Il costo totale globale associato ai virus nel 2001 è stato di 10,7 miliardi di dollari. Code Red si è rivelato il virus più costoso del 2001 con 2,6 miliardi di dollari. Circa 1,5 miliardi di dollari sono derivati da perdità di produttività, mentre 1,1 miliardi di dollari sono stati spesi per ripulire i sistemi infettati dal virus. Il virus più costoso di tutti i tempi è stato Love Letter nel 2002 con un costo di 8,7 miliardi di dollari in perdita di produttività e pulizia (fonte: Computer Economics, 2001).



Il Virus Educato

I VIRUS DEL FUTURO

In entrambi i mondi alcuni dei virus più pericolosi sono quelli che attaccano il sistema immunitario o il software anti-virus.

Nel mondo medico, un virus che attacca il sistema immunitario esiste già nella forma dell'HIV; ciò porta il sistema immunitario a non essere in grado di combattere le malattie infettive perché viene attaccato e distrutto. Allo stesso modo, nel mondo informatico alcuni dei virus più difficili da combattare sono quelli che attaccano il software anti-virus, in particolare quelli che ingannano il software anti-virus, e quindi l'utente, riportando false informazioni su se stesso. (per esempio, sebbene il software anti-virus possa aver trovato un virus riportandolo all'utente, il virus intercetta il messaggio e dice all'utente che tutto va bene!). Questi tipi di virus informatici sono conosciuti come "virus disonesti".

All'estremo opposto ci sono i "virus educati". Si tratta di un virus apparso nel Gennaio 1996 che chiedeva all'utente se volesse essere infettato o meno dal virus stesso. Poiché molte persone davano l'ok alla casella di dialogo senza realmente leggere o prestare attenzione a quanto scritto (perché solitamente quando si seleziona "no" vengono poste altre domande), il virus è diffuso ancora oggi!

CONCLUSIONI

Questa indagine preliminare nei mondi paralleli dei virus ha portato alla luce notevoli somiglianze in termini di composizione e funzionalità. Naturalmente esistono delle differenze fondamentali tra il lavoro dei virologi medici e quello dei ricercatori anti-virus – non ultime le conseguenze in caso di errore! Comunque sembrano esistere sufficienti parallelismi per gli esperti in entrambi i settori per imparare almeno qualcosa l'uno dall'altro in alcune aree specifiche.

Come evidenziato in una delle aree analizzate da questa indagine, le aziende produttrici di anti-virus informatici possono per esempio imparare dalla loro controparte medica come valutare il rischio dei virus. Mentre i ricercatori medici e le industrie farmaceutiche hanno un certo numero di

Gruppi Consultivi che utilizzano criteri riconosciuti per categorizzare i virus in gruppi di pericolo che sono accettati a livello mondiale, non esiste qualcosa di analogo nel mondo informatico. La valutazione del rischio di nuovi virus non viene determinata solo dalle singole aziende ma si basa anche sull'istinto individuale piuttosto che su una formula comprovata. Questa anomalia, cioè che diverse società produttrici di anti-virus possano rilasciare allarmi differenti in relazione alla minaccia costituita da un nuovo virus, può solo dare adito a confusioni e incomprensioni nelle persone. I processi di definizione di questo rischio sono così simili in entrambi i settori che esistono evidenti casi nel mondo informatico in cui si attui un'ampia collaborazione industriale in materia.

Un'area dove le aziende anti-virus sono molto più progredite rispetto alle loro controparti mediche è la velocità e la capacità non solo di raccogliere informazioni sui virus in circolazione ma anche di elaborare queste informazioni consentendo loro di adottare contromisure immediate per combatterli. Naturalmente per le aziende anti-virus essere in grado di raccogliere ed elaborare tutte queste informazioni in modo automatico tramite una rete di computer è molto più facile data la reale natura della "bestia". Il codice di un virus informatico viene fornito in un formato leggibile mentre quello di un virus biologico deve essere ricavato dall'applicazione di tecniche piuttosto complesse e lunghe prima che sia disponibile in un formato utilizzabile da un pc per l'analisi. Inoltre, esiste una documentazione registrata completa dei virus informatici di come sono nella loro infanzia rispetto ai virus biologici che sono in circolazione da migliaia di anni.

Le infomazioni genetiche relative ai virus biologici stanno diventando sempre più accessibili attraverso dei database, ma registrazioni complete non esistono ancora dal momento che le tecniche per l'isolazione e la caratterizzazione dei virus sono piuttosto recenti. Disporre dell'accesso immediato a tali informazioni è di valore incommensurabile. La capacità di monitorare la situazione a livello mondiale in tempo reale non solo funge da sistema di avviso precoce per qualsiasi attacco, ma fornisce inoltre un sistema di informazioni di reazione immediate su chi sta vincendo nella continua battaglia tra la razza umana e i virus. Ovviamente l'informatizzazione dell'intero sistema di sorveglianza dei virus della comunità medica è un processo in continua evoluzione, ma esempi provenienti dall'industria informatica mostrano che i benefici che ciò offre superano di gran lunga gli sforzi e le spese affrontate.

È auspicabile che questa indagine fornisca spunti di meditazione agli esperti di entrambi i settori stimolando ulteriori lavori in questi affascinanti parallelismi. Sviluppi in tutti campi della scienza possono arrivare dalle fonti più diverse e forse un giorno un importante passo avanti nella Medicina o nella tecnologia arriverà dalla scoperta che i rispettivi virus condividono molto più che il semplice nome.

TERMINI RELATIVI AI VIRUS UTILIZZATI SIA NEL SETTORE MEDICO CHE IN QUELLO INFORMATICO:

In the wild - Virus che è ampiamente diffuso tra la popolazione

Quarantena - Isolamento di un computer o di un essere umano da qualsiasi interazione con i potenziali portatori di virus

Vettore - Un programma (parte di codice) di cui i virus informatici hanno bisogno per inserirvisi e ottenere l'accesso a un PC. Similmente, alcuni virus biologici richiedono un ospite/vettore intermedio per trasferirsi da un ospite "naturale" agli umani

Parassitario - Entrambi i virus sono parassitari in natura – hanno bisogno di una cellula o di un programma informatico per replicarsi

Immunità - La difesa di una persona o di un Pc contro l'infezione causata da virus

Laboratorio - Il posto dove sia i virus reali che virtuali vengono studiati e dove vengono sviluppate le cure necessarie

Dormiente - Un tipo di virus che può trasmettersi da un ospite ad un altro ma non ha effetto immediato

Rete di sorveglianza - Un sistema mediante il quale i virus reali e virtuali vengono individuati attraverso coloro che li hanno sperimentati per primi

Mutazione - La natura in continuo cambiamento e evoluzione dei virus reali e virtuali

Euristica - Un metodo per l'identificazione di un virus ponendo domande per eliminare le possibili alternative

Stagionale - Un periodo durante il quale sia i virus reali che quelli virtuali diventano predominanti o più diffusi - solitamente durante la stagione invernale

Vaccinazione - I passi che una persona deve fare per proteggere se stesso o un Pc dall'infezione

Decodifica - Analisi e valutazione di un virus, per facilitarne la comprensione

Patogeno - Sia i virus biologici che quelli informatici hanno vari livelli di patogenicità – più patogeno è il virus, più danni può causare

Ceppo - Quando i virus di sviluppano e mutano, essi danno vita a nuovi "ceppi" o variazioni del virus

Isolamento - Questo è l'unico stato in cui una persona o un computer può esistere senza essere a rischio di infezione.

E UNA PAROLA DA NON CONFONDERE...!

Bug (baco) - Nel mondo medico questo è un termine dialettale spesso usato per indicare un batterio, meno frequentemente un virus. Nel mondo informatico non indica assolutamente un virus bensì un errore umano nel codice di un programma che lo porta a non funzionare correttamente...

e-mail: Info_Italia@NAI.com