INTRODUZIONE AL CONVEGNO

(prof. Romano ONEDA)

Vorrei premettere agli interventi dei nostri eccellenti relatori, che si occuperanno di situazioni di portata e respiro nazionale e internazionale, qualche considerazione personale: una riflessione minima, più vicina al nostro ambito ristretto di utilizzo della strumentazione informatica, sul come "noi comuni mortali" viviamo la minaccia del malware.

E concedetemi di rievocare, visto che la mia età me lo consente, per un attimo gli inizi degli anni novanta (quando i miei attuali studenti nascevano…) e la situazione di allora del malware virale come l'ho vissuta, con curiosità e vivo interesse per un fenomeno che appariva, se non nuovo, quantomeno sconcertante.

Allora lo strumento principe del contagio virale era il floppy disk, ed i tempi di propagazione non erano certo quelli fulminei di oggi, con l'Internet diffuso a tutti i livelli; i virus avevano, di necessità e per fortuna, dimensioni ridotte (occorreva fare di necessità virtù, e la concisione del codice era un'abilità molto apprezzata ed i virtuosi della stringatezza erano riconosciuti ed ammirati (penso che non pochi dei presenti ricordino anche quell'ambiente culturale tra l'aristocratico e il maniaco in cui poteva nascere una competizione su chi riuscisse a stipare più comandi in una sola riga di linguaggio C…); allora gli studiosi interessati al fenomeno virale potevano ancora sperare di seguirne singolarmente l'evoluzione da vicino, studiandone i codici e approfondendone le tecniche di attacco. Conservo ancora dei quaderni dell'epoca, in cui avevo trascritto e commentato il disassemblato di vari virus che si nascondevano nel settore zero e in altri settori non utilizzati dei floppy, e, oltre ad ammirare le invenzioni stilistiche del codice virale, ricordo come fossi spesso tormentato dalla curiosità di capire quali motivazioni potevano spingere gli anonimi autori a congegnare e diffondere tali strumenti sofisticati di danneggiamento e di distruzione dei beni informatici altrui. Senza dubbio motivazioni diverse e varie, su cui a suo tempo si sono sbizzarriti psicologi e psichiatri, e che non possiamo qui approfondire, ma certamente non motivazioni commerciali, o di lucro.

Oggi al contrario, come sarà ben illustrato negli interventi successivi, ci troviamo a combattere con organizzazioni commerciali illegali che tentano di sfruttare, con altissimi profitti, ogni aspetto dell'Internet su cui si possa in qualche modo lucrare, e costituirà motivo di sorpresa apprendere quanto variegati e diversi siano gli espedienti messi in atto per conseguire questi obiettivi criminosi.

Vorrei allora accennare molto brevemente ai rischi che corriamo noi utenti singoli e comuni, utilizzatori di un computer domestico e magari fruitori di qualche altro strumento portatile di connessione alla rete.

E' di questi tempi abbastanza frequente il trovare gli utenti comuni concordi in una sottovalutazione del rischio che corrono i loro computer domestici-casalinghi, convinti come sono di non risultare prede appetibili, perché, come spesso sentiamo affermare, "non abbiamo nessun dato importante registrato e poi nemmeno facciamo transazioni commerciali, operazioni bancarie o di borsa", per cui si considerano immuni da attacchi, o, se anche saggiati da qualche scanner, non sarebbero poi considerati degni di conquista.

Si tratta di un errore di prospettiva senza dubbio pericoloso, perché ci spinge ad abbassare la guardia e ci rende ancora più facilmente vulnerabili di quanto già non lo siamo. Come mostrano le più recenti relazioni e statistiche sulla diffusione e sulla consistenza degli attacchi di malware, i computer domestici costituiscono comunque un obiettivo interessante e ricercato, sia per la possibilità di asservirli in reti (botnet) sia perchè possono essere utilizzati con profitto in tutta una serie di attività criminose cui farò qualche cenno, per maggiore chiarezza, lasciando naturalmente i maggiori dettagli ai successivi relatori.

Innanzitutto occorre non dimenticare che un computer, una volta violato, risulta nella completa disponibilità dell'invasore, che potrà operare con gli stessi privilegi del legittimo proprietario e disporre a piacimento dei servizi offerti dalla macchina: l'installazione di un keylogger, ad esempio, metterà a disposizione dell'intruso la completa registrazione dei tasti premuti, comprese quindi le varie password e credenziali di accesso, così come potrebbero venir attivate per la registrazione la webcam ed il microfono eventualmente presenti sul computer, rendendolo una stazione di ascolto e di spionaggio.

E quindi non dovremmo meravigliarci se il nostro computer venisse utilizzato, sempre a nostra completa insaputa, come web server per operazioni illecite come la creazione di un sito civetta, copia pressoché identica di un altro sito ufficiale, ad esempio di una banca, per operazioni di phishing; o come sito deposito da cui scaricare materiale virale da infezione e software strumentale per attacchi (una santabarbara del malware); o come archivio fonte di file piratati in violazione del copyright, non escluso il materiale video di pedopornografia; o anche, nel migliore dei casi, come base per inviare una valanga di messaggi di spam, pubblicitari ma anche di lancio dell'esca via mail mirata per potenziali vittime del phishing. Come risulta chiaro, in questi casi non è rilevante il fatto che il computer contenga dati personali importanti o meno, ma proprio il mero fatto che il computer sia funzionante ed utilizzabile.

Se poi sul disco fisso, come è fisiologico, abbiamo lasciato tracce concrete delle nostre attività, allora saranno una preda preziosa, ad esempio , oltre alle nostre varie password e credenziali di accesso (che consentiranno poi il furto di personalità) anche la rubrica dei contatti email, utile per ampliare il repertorio degli indirizzi di spam, magari da rivendere, ma anche per costruire un nostro profilo credibile, associandola ai dati che avremo ingenuamente fornito ai nostri amici sulle pagine di Facebook e degli altri social network. Attività di profilazione che costituisce poi la base dello spear phishing, per cui magari riceviamo una mail personalizzata dall'account e a firma di uno dei nostri più cari amici e con dettagli di avvenimenti cui abbiamo partecipato insieme: come pensare che non sia lui che ci manda delle foto di un suo recente viaggio? Naturalmente non abbiamo sospetti, apriamo l'allegato con le foto e così installiamo, anche qui senza saperlo, un cavallo di Troia, un trojan Horse che prende possesso del nostro computer. Ma il nostro visitatore telematico non trascurerà nemmeno di raccogliere le nostre chiavi di licenza, sia quelle del sistema operativo come quelle delle varie applicazioni installate, dati di valore facilmente spendibili sul mercato dell'illegale.

Fin qui l'attività del nostro visitatore è rimasta sotto traccia; ma potrebbe decidere anche di manifestarsi con delle offerte o delle richieste che ci appaiono improvvise sullo schermo. Per esempio un amichevole avviso che ci informa della presenza di pericolosi virus nel nostro computer e della possibilità, per un pugno di dollari, di scaricare un antivirus miracoloso che ci renderà mondi da ogni programma maligno: inutile dire che, se accediamo alla richiesta, il programma installato sarà un nuovo cavallo di Troia, tutto tranne che un antivirus. Oppure possono apparire dei messaggi ri(s)cattatori, che ci avvisano che i nostri file con i dati più preziosi sono stati resi inaccessibili con la crittografia, e se non vogliamo perderli per sempre dobbiamo pagare un riscatto: le possibilità di sorprese di questo tipo sono numerose e certo dipendenti solo dall'inventiva dei malintenzionati.

Fin dalle premesse iniziali abbiamo di proposito escluso che sui computer oggetto del nostro esame fossero state svolte attività di carattere finanziario, proprio per simulare la situazione di chi ritiene di non essere preda appetibile; certo è facilmente intuibile il rischio pesante che corre chi, al contrario, conducesse operazioni bancarie e transazioni commerciali con esposizione delle proprie credenziali e dei dati relativi ad account bancari ed a carte di credito: è ricca e abbondante la casistica degli ingenui che si sono trovati il conto corrente svuotato o ridotto ai minimi termini.

Ulteriore, frequente, possibilità è poi quella dell'asservimento del computer che, come uno schiavo, rimane in attesa di ordini insieme a migliaia di altri zombie reclutati nella stessa rete, pronti ad eseguire attività illegali che fondano la loro dirompente efficacia proprio dall' essere azioni di massa, come nel caso degli attacchi di denial of service, con cui si possono bloccare servizi web di rilevante impatto come i bancari e i commerciali, con pesanti ricadute sulle stime di affidabilità e di sicurezza delle imprese bersaglio.

Naturalmente gli zombie possono essere utilizzati per una quantità di missioni diverse, comunque in genere estemporanee, a differenza dell'utilizzo come server web , che implica una continuità di prestazioni: per questo gli zombie (o bot, che è poi un'abbreviazione di robot) non sono facilmente tracciabili, e utilizzano diverse strategie per tentare di sfuggire alle analisi di ricerca, compresa quella di adottare per i file delle denominazioni che si possano facilmente confondere con nomi legittimi del sistema operativo.

Concluderei quindi queste poche righe di introduzione con l'invito a considerare con maggiore attenzione gli aspetti della sicurezza anche dei nostri computer personali e magari a non pensare di comportarsi in maniera troppo paranoica se decidiamo di utilizzare ulteriori strumenti di analisi e di protezione oltre agli imprescindibili antivirus e firewall, e cerchiamo di controllare se il nostro amato computer finge soltanto di essere libero e tutto per noi, mentre invece è uno zombie asservito al nemico.