Virus e siti pericolosi: Come evitarli

Introduzione alla sicurezza informatica 1/3

Mauro Cicognini 2010

Agenda

- I virus oggi: in altre parole, le minacce esterne “attive”
  - Lo spam e la versione XXI secolo di antichi inganni
  - Antivirus/antispyware gratuiti
- I siti pericolosi: in altre parole, le minacce esterne “passive”
  - Siti malevoli
  - Siti ingannevoli
  - Phishing
  - È vero che ci sono browser più sicuri?
- Come configurare Windows con gli strumenti incorporati (usiamo almeno quelli)
  - Usare Windows Update
  - Usare Windows Defender
  - Occhio: manca l’antivirus!

Agenda della seconda sessione

- Le minacce per un adulto e per un bambino
  - Il bambino ignaro (e potenzialmente adescato)
  - Il coniuge infedele (e potenzialmente adescato)
  - Il single che semplicemente si “fa fregare”
- Il computer e la rete per i bambini e gli adolescenti
  - Il videogioco – risorsa e rischio insieme
  - Gli adulti pericolosi
  - I software di filtraggio
  - Chat, SMS, IM… come salvarsi e resistere alla tentazione dell’always on

Agenda della terza sessione

- Il problema dell'attendibilità dei contenuti su Internet
  - Il caso Wikipedia
  - I forum ed i blog
  - Le leggende metropolitane (c'erano anche prima!)
- Quali sono le minacce più pericolose?
  - La delinquenza in cerca di denaro
  - Il furto di identità
  - Spionaggio industriale (?)
- Sicurezza per l'attività professionale
  - Comunicazione ed e-mail
  - Porsi come fornitore di servizi e contenuti
  - La vetrina pubblicitaria

Sicuramente
www.clusit.it

Associazione “non profit” con sede presso
l’ Università degli Studi di Milano,
Dipartimento di Informatica e Comunicazione

Clusit
Associazione Italiana
per la Sicurezza Informatica

Gli Obiettivi

- Diffondere la cultura della sicurezza informatica presso le Aziende, la Pubblica Amministrazione e i cittadini
- Partecipare alla elaborazione di leggi, norme e regolamenti che coinvolgono la sicurezza informatica, sia a livello nazionale che europeo
- Contribuire alla definizione di percorsi di formazione per la preparazione e la certificazione delle diverse figure professionali operanti nel settore della sicurezza
- Promuovere l'uso di metodologie e tecnologie che consentano di migliorare il livello di sicurezza delle varie realtà

Il Ruolo Istituzionale

In ambito nazionale, Clusit opera in collaborazione con:

- Presidenza del Consiglio, Dipartimento per l'Innovazione e le Tecnologie
- Ministero della Difesa
- Ministero dell' Economia e delle Finanze
- Ministero della Giustizia
- Ministero dell' Interno
- Ministero dello Sviluppo Economico
- Polizia Postale e delle Comunicazioni
- Protezione Civile
- Autorità Garante per la tutela dei dati personali
- Autorità per le Garanzie nelle Comunicazioni
- Confindustria Servizi Innovativi e Tecnologici
- Università e Centri di Ricerca
- Associazioni Professionali e Associazioni dei Consumatori

I Rapporti Internazionali

In ambito internazionale Clusit partecipa a svariate iniziative in collaborazione con:

- CERT
- CLUSI (CLUSIB, CLUSI-BF, CLUSIF, CLUSIS, CLUSSIL)
- Università e Centri di Ricerca in Austria, Belgio, Danimarca, Francia, Estonia, Grecia, Inghilterra, Irlanda, Lussemburgo, Olanda, Pologna, Spagna, Svezia e Svizzera
- Commissione Europea DG Information Society
- ENISA (European Network and Information Security Agency)
- OCSE (Organisation for Economic Co-operation and Development)
- ITU (International Telecommunication Union)
- Associazioni Professionali (ISACA, ASIS, ISC², ISSA, SANS) e Associazioni dei Consumatori

I Soci del Clusit

Rappresentano oltre 500 organizzazioni, appartenenti all'intero "Sistema Paese":

- RICERCA
- INDUSTRIA
- COMMERCIO e DISTRIBUZIONE
- BANCHE, FINANZA e ASSICURAZIONI
- PUBBLICA AMMINISTRAZIONE
- SANITÀ
- CONSULENZA, AUDIT
- SERVIZI
- TELECOMUNICAZIONI
- INFORMATICA

Le priorità del Clusit

- Formazione specialistica: i Seminari CLUSIT
- Certificazioni professionali: CISSP, CSSLP, SSCP, BCI
- Produzione di documenti tecnico-scientifici: i Quaderni CLUSIT
- Ricerca e studio: Premio “Innovare la Sicurezza delle Informazioni” per la migliore tesi universitaria – 4a edizione
- Attività convegnistica: oltre 50 eventi all’anno
- Security Summit: marzo 2010 a Milano, giugno 2010 a Roma (http://www.securitysummit.it/)
- Online Sicuro : il Portale italiano per la sicurezza delle informazioni e delle reti, con servizio di assistenza online a cittadini e imprese (PMI)
- Progetto Clusit per piccole e microimprese: per aiutarle a gestire il rischio IT, in collaborazione con le associazioni imprenditoriali locali

Il cosiddetto «malware»

VIRUS, WORM, BOTNET, ECC.

Malware “classici” (1)

- Virus
  - Un programma che è in grado di modificare altri programmi con il fine di inserirvi una copia, eventualmente modificata, di se stesso
- Trojan Horse
  - Un programma che maschera la proprie attività con altre attività apparentemente “innocue”
- Worm
  - Un programma in grado di auto riprodursi, ma che contrariamente ad un virus non necessita di “trasportatore”
- Codice Maligno (rogue code)
  - Un qualunque programma in grado di compromettere riservatezza, integrità e disponibilità di un sistema di calcolo
- Exploit
  - Programmi che sfruttano i difetti di altri programmi per violare la sicurezza

Malware classici (2)

- Spyware
  - Attivati con consenso carpito
  - Alcuni sembrano innocui, presentano pubblicità
    - Quasi sempre prodotti illegali
    - Spesso in realtà trasportano altro malware
  - Pericolosi: recuperano info personali dall'HD
- Dialers
  - Attivano un collegamento Internet aggiuntivo a tariffe estremamente elevate
    - Originariamente una chiamata telefonica internazionale
  - Oggi infrequenti sui PC, potrebbero minacciare gli smartphone
  - Causano un danno diretto e sensibile!

Malware atipici

- Gli hoax
  - Messaggi che allertano gli utenti circa la presenza di presunti virus che stanno per diffondersi in rete
  - Ma anche le lettere a catena: “Mandate una cartolina al povero Timmy che sta per morire”
  - Facilmente riconoscibili:
    - La fonte non è citata o non è identificabile
    - Richiedono esplicitamente di avvertire tutte le persone che si conoscono
  - Gli hoax costano:
    - Gli utenti finali sprecano tempo e risorse per avvertire i propri colleghi dell’evento, in alcuni casi diventando praticamente casi di spam
    - I fornitori di antivirus vengono sollecitati dai propri clienti a fornire una soluzione al problema

Le combinazioni…

- Le varie tipologie si possono combinare
- Ed abbiamo visto che lo fanno!
  - Worm + exploit = miscela esplosiva!
  - Diffusione rapidissima e sfruttamento automatico delle vulnerabilità
  - Un tempo miravano solo ad «uccidere» il PC, oggi in alternativa possono prenderne il controllo
    - Senza dare sintomi all'utente!
  - Si creano le cosiddette «botnet»
- Le patch, queste sconosciute
  - Nessuno applica mai le patch corrette
    - È un'esagerazione, ma non poi così lontana dalla verità
  - Tanto meno gli sviluppatori che hanno sul PC un server Web, un SQL, un Active Directory, ecc.

Struttura generale

- In generale un malware è formato da due componenti:
  - Una parte che si preoccupa delle azioni di disturbo, distruzione, spionaggio, controllo a distanza
  - Una parte (anche non un programma!) che fa sì che la prima parte si possa diffondere

La strategia di infezione

- I “vecchi” virus infettavano i file eseguibili e si riproducevano per “contatto fisico”
- I malware oggi viaggiano via Internet
  - Od anche via Bluetooth
- In vari casi sono nascosti dentro file allegati all’e-mail
  - Spesso sono essi stessi ad auto-inviarsi via e-mail
  - Il problema è spesso l’apertura automatica degli allegati
  - La vulnerabilità quindi è più spesso psicologica che tecnologica
- In altri casi si «iniettano» durante la navigazione
  - Spesso quindi sfruttano vulnerabilità tecnologiche
- Occorre comunque grande attenzione

Perché nascono i malware?

- Curiosità
- Ricerca
- Vandalismo
- Crimine
- Guerra

Quale protezione?

- Ovviamente i virus possono anche essere presenti in programmi, documenti o immagini che scarichiamo dalla rete
- La protezione più efficace contro i virus sono gli antivirus sempre residenti

- … ma come fanno gli antivirus a trovare il virus?

Come funzionano gli AV?

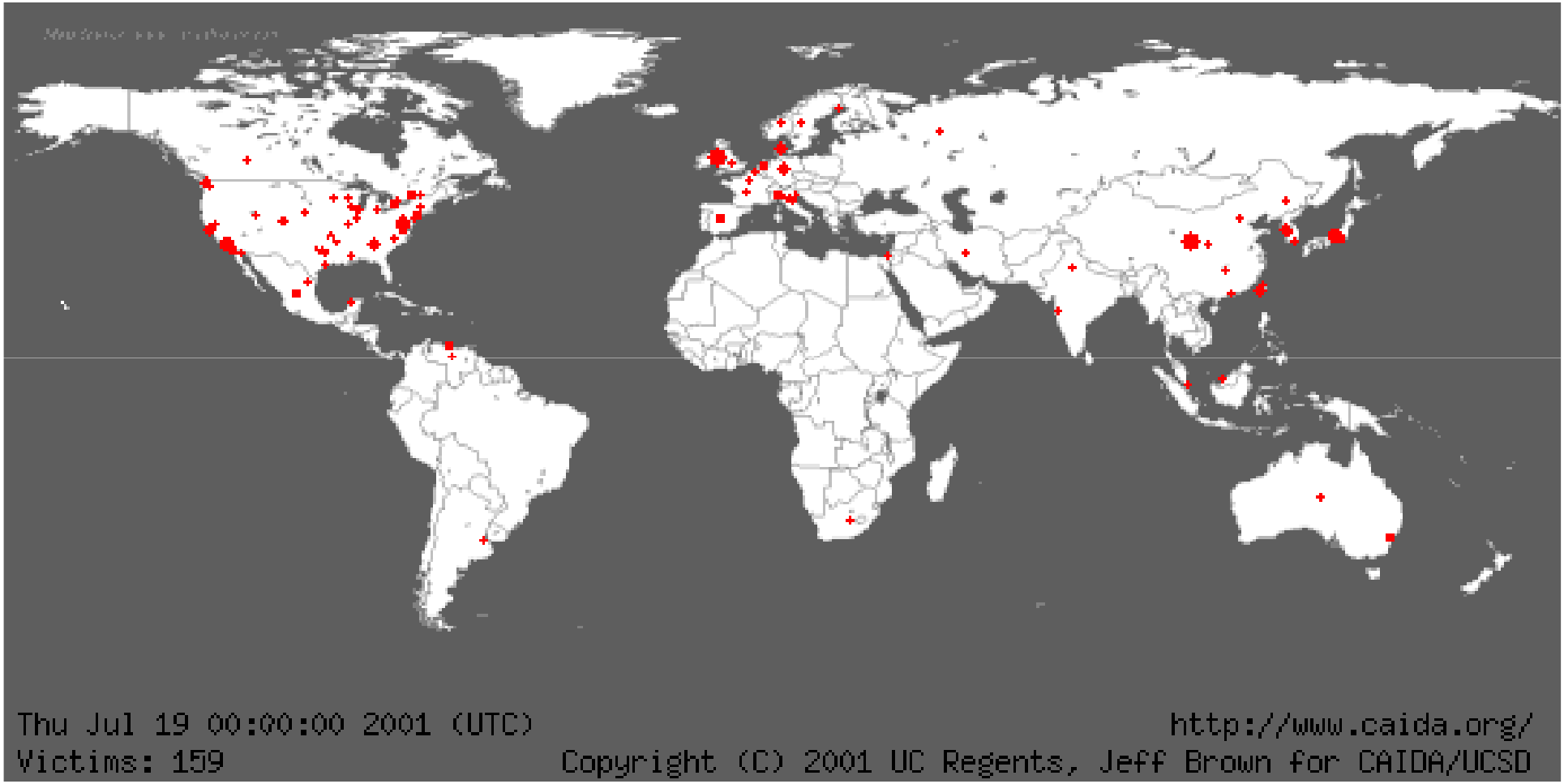
- Approccio “signature”
  - Si confronta un (piccolo) blocco di bytes nel file sospetto con quelli contenuti in un Database
  - Molto pratico ed efficiente
  - Richiede un database di impronte caratteristiche dei virus
  - Richiede un aggiornamento continuo
- Approccio “euristico”
  - Si controllano le attività “sospette”: accesso al settore di boot del disco, apertura e chiusura di moltissimi file di seguito, ecc.
  - Consente di identificare anche virus ignoti
  - Non si può garantire esattezza al 100%

Qualche numero

- I primi virus nel 1986 (Brain)
  - Boot sector virus
  - In 5 anni provoca danni per 50M di $
- 2/11/88: l'Internet Worm di Robert Morris
  - Studente di PhD della Cornell University, mette fuori causa, nel giro di poche ore, 6000 computer connessi a Internet sfruttando la rete ed alcune vulnerabilità del SUN OS
- Nel '90 nascono i "macro"
- Nel '97 oltre 14.000 virus, 200 nuovi ogni mese
- Nel 2000 oltre 50.000 virus (500 attivi), più di 800 al mese
- Nel 2001 il primo «ibrido», CodeRed
- Nel 2003 il più veloce sinora, Slammer
- Nel 2006 iniziano a diffondersi le botnet

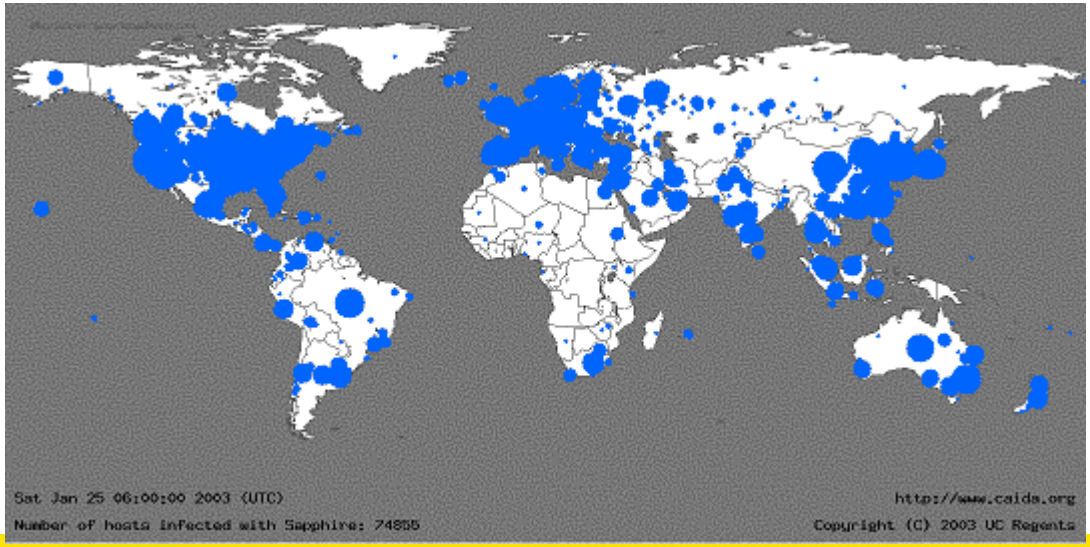
- Il malware costa!

CodeRed


Thu Jul 19 00:00:00 2001 (UTC)
Victims: 159
http://www.caida.org/
Copyright (C) 2001 UC Regents, Jeff Brown for CAIDA/UCSD

Il «virus delle poste»

- SLAMMER
  - Iniziò a diffondersi appena prima delle 05:30 UTC sabato 25 gennaio 2003
  - Raddoppiava il numero di host infettati ogni 8.5 secondi
  - Ha infettato più del 90% dei computer vulnerabili entro 10 minuti
- Sfruttava un buffer overflow di Microsoft SQL Server or MSDE 2000 (Microsoft SQL Server Desktop Engine)
- Vulerabilità già scoperta e segnalata nel luglio 2002
- Microsoft aveva rilsciato una patch per la vulnerabilità ancora prima di rendere nota quest'ultima (cfr. http://www.microsoft.com/security/slammer.asp)
- Ha infettato almeno 75000 computer, ma probabilmente molti di più
- Ha causato fermi delle reti più disparate, cancellazione di voli aerei, interferenze ad elezioni, e guasti ad apparati Bancomat



È solo un problema di PC?

- CELLULARI
  - Sono computer con un’antenna
  - Hanno S.O. e programmi
  - Sono collegati
- PALMARI
  - Sono computer
  - Hanno S.O. e programmi
  - Sono collegati
- CONSOLLE GIOCO
  - Sono computer
  - Hanno S.O. e programmi
  - Sono collegate

Tre fattori preoccupanti

- La scomparsa delle “diversità biologiche” che è sempre stato l’elemento che ha consentito la sopravvivenza alle grosse epidemie
- Il costante incremento della complessità dei prodotti ICT
- La diffusione delle tecnologie ICT negli apparati di largo consumo
  - Con la diffusione dei “giochi” sui cellulari, giochi che potranno essere scaricati da Internet, ci si attende un grosso aumento di virus per questo tipo di dispositivi
- È indubbio che l’attenzione di chi realizza malware vada di volta in volta verso i bersagli meno protetti

Sono un fenomeno passeggero?

- NO!
  - Sono un fenomeno endemico
  - Sono in crescita numerico
  - Vedono una costante e forte evoluzione tecnologica
- Risposte tecniche (antimalware)
- Risposte organizzative
  - + attenzione
  - + informazione
  - + collaborazione
- Parte della sicurezza totale

PRECAUZIONI?

Qualcosa che blocchi queste minacce

- I guardiani del PC sulla rete si chiamano «personal firewall»
- Windows lo incorpora a partire da XP SP2
- Oggi di fatto la condizione di partenza è «tutto chiuso»
  - Bisogna esplicitamente dire «sono in una rete fidata, consenti l'accesso»
- Gli altri S.O. (Mac, Linux, ecc.) da tempo hanno funzioni molto simili o superiori

Un ANTIVIRUS aggiornato

- Gli Antivirus/Antispyware ci proteggono da ciò che scarichiamo esplicitamente
  - Posta, Chat, IM, Browser, ecc.
  - Anche le chiavette USB!
- È vero che costano, ma molti PC sono venduti con AV/AS in versione «a tempo» per qualche mese
- Ne esistono svariati completamente gratuiti – in ordine alfabetico:
  - Antivir PE
  - Avast! Home
  - AVG
  - Avira
  - ClamAV (ClamWin) – è anche «Open Source»
  - Comodo
  - Microsoft Security Essentials
  - Panda Cloud
  - Ecc.

Aver cura del software

- Se usate Windows, usate Windows Update
- Usate se potete un po' di "diversità genetica" per il software
  - Spesso conviene usare il «generico» anche in informatica

- Non guasta avere qualche copia di sicurezza di programmi, documenti e dati
  - Esistono ad esempio anche dei servizi di backup online
  - A volte si trovano addirittura incorporati nel canone dell'antivirus, o come opzione

Navigare con cautela

- Attenzione ai «pescatori»… non diventiamo pesci!
  - Ovvero: il phishing
  - Facciamo qualche esempio
  - …
- Fortunatamente oggi i maggiori browser e client di posta incorporano funzioni di protezione
- Utilizzare comunque con un po' di sana diffidenza i siti «dinamici» e le estensioni
  - Con *estrema* cautela le estensioni in formato ActiveX

Ci sono browser più sicuri di altri?

- Non ne siamo certi
- Sicuramente ci sono *comportamenti* più pericolosi di altri
- Risulta probabilmente meno intuitivo capire di essere in una «zona malfamata»
- Alcuni indicatori però sono costanti:
  - Siti molto pieni di immagini pubblicitarie
  - Siti con offerte incredibilmente convenienti
  - Siti con errori di ortografia o addirittura di lingua
  - Ecc.

Gli strumenti di Windows

- Windows Update
  - Vediamo dov'è e come funziona…
- Windows Defender
  - Vediamo dov'è e come funziona…
- Occhio: all'inizio non c'è l'antivirus!
  - Va scaricato (o acquistato) ed installato
  - Abbiamo già detto che ne esistono parecchi anche gratuiti

DOMANDE?

Per contatti: Mauro Cicognini <mcicognini@clusit.it>

GRAZIE! ☺