Uno sguardo dalle trincee

Simona Venuti - GARR

Consortium GARR

Background

- Vedremo come si e' evoluta e si sta evolvendo la situazione delle segnalazioni e la gestione degli incidenti nel tempo
- I dati delle prossime slide sono stati collezionati dal GARR-CERT nell'arco di sette anni
- Per gli incidenti “piu' quotati”: piccolo report su chi crea maggior numero di incidenti e dettagli su cosa fa
- Le statistiche e i grafici sono stati preparati a tempo di record dai colleghi del GARR-CERT
  - Andrea Pinzani
  - Maria Sole Scollo

che ringrazio moltissimo

per il lavoro faticoso (ma bellissimo) che hanno fatto

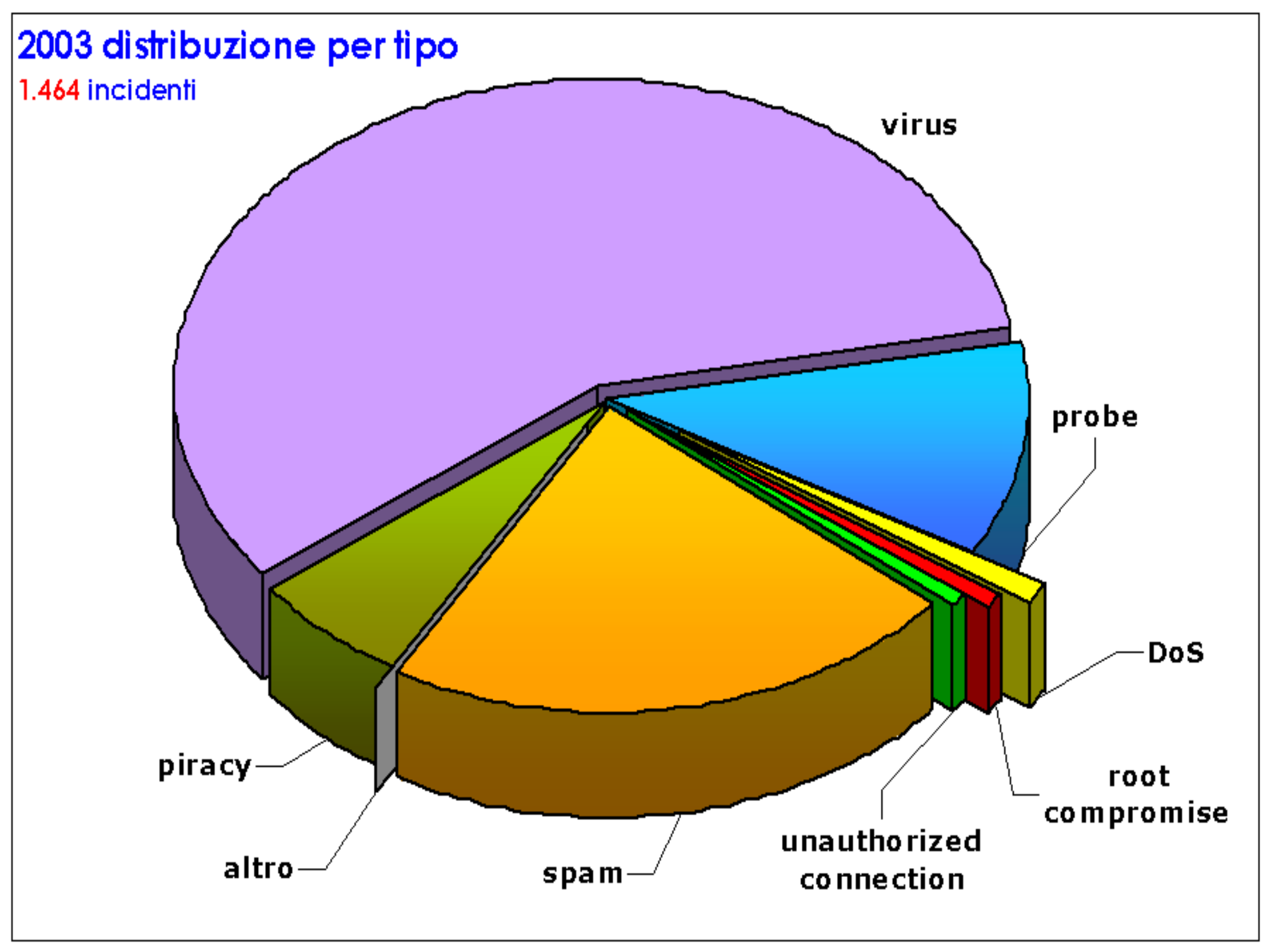
il GARR-CERT

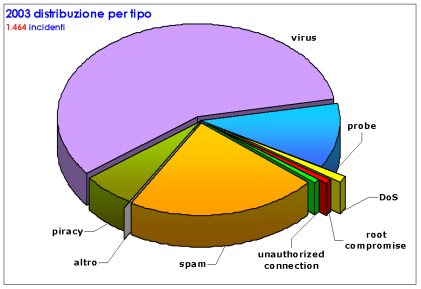
Il servizio operativo GARR-CERT ha il compito di assistere gli utenti GARR nella gestione degli incidenti di sicurezza informatica e nella realizzazione di misure preventive necessarie a ridurne il rischio.

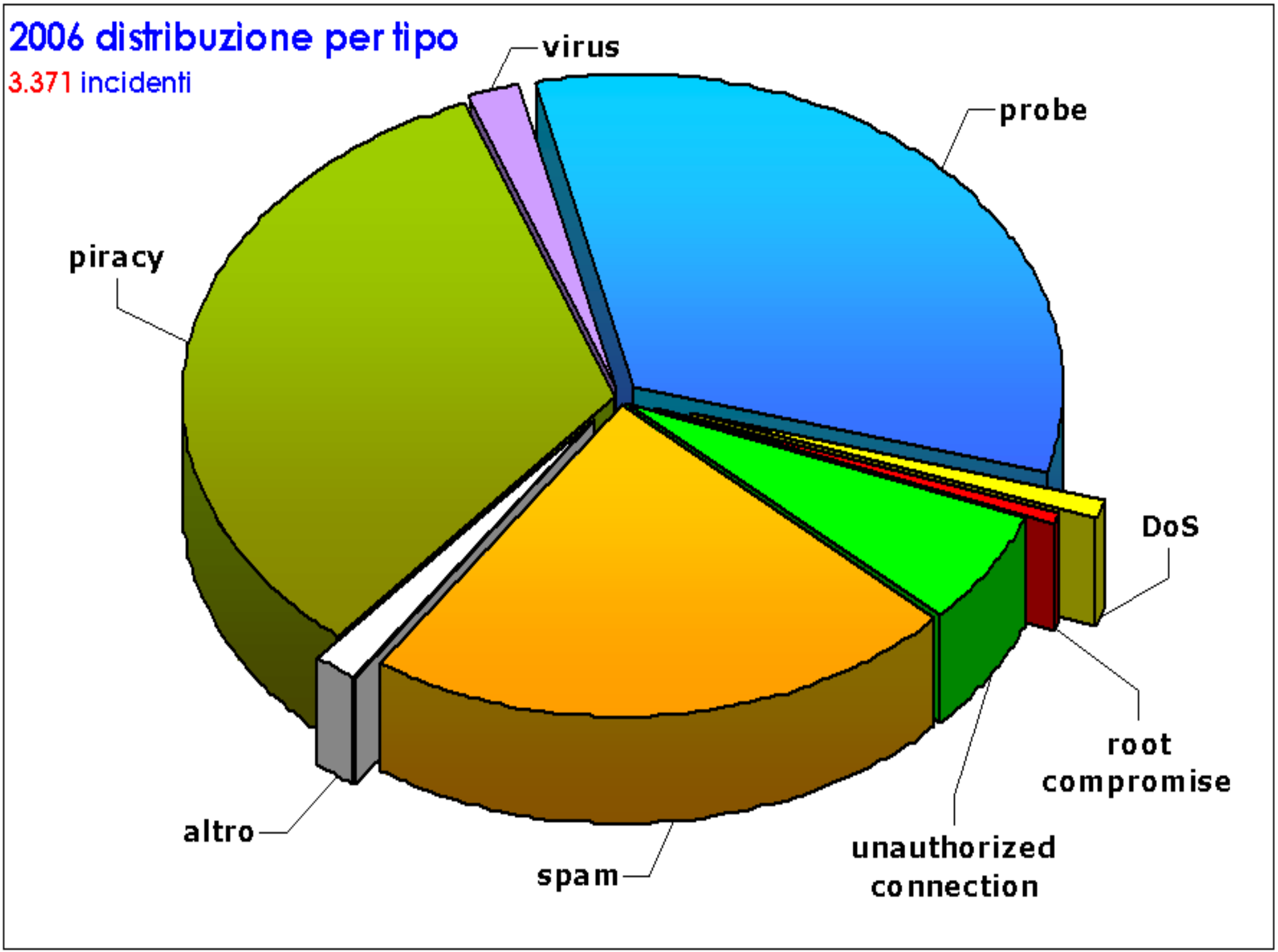
- risponde alle segnalazioni di incidenti, avvertendo gli utenti coinvolti
- diffonde informazioni sulle vulnerabilità più comuni e sugli strumenti di sicurezza da adottare
- emana direttive sui requisiti minimi di sicurezza per le macchine con accesso alla rete, verificandone il rispetto
- prova strumenti esistenti, e ne sviluppa di nuovi per specifiche esigenze di sicurezza

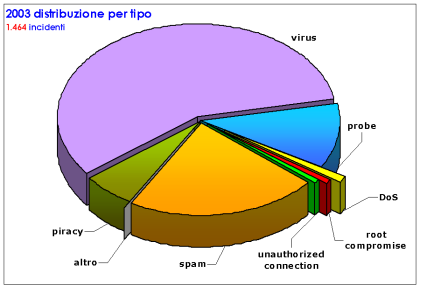
2003 distribuzione per tipo

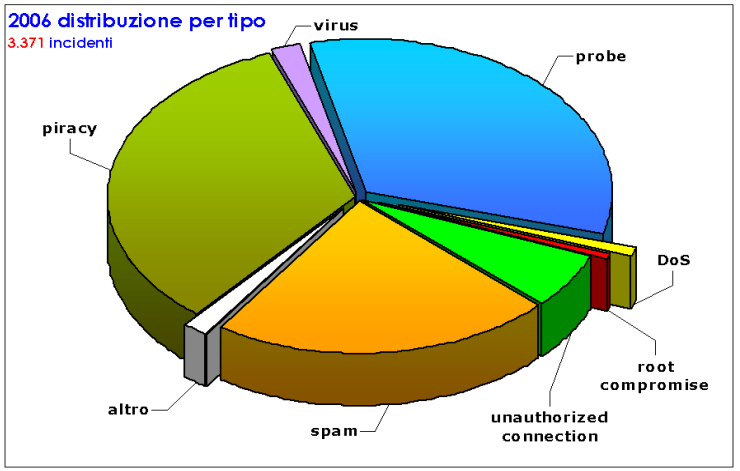
1.464 incidenti




2003 distribuzione per tipo
1.464 incidenti
virus
probe
DoS
root compromise
unauthorized connection
spam
altro
piracy

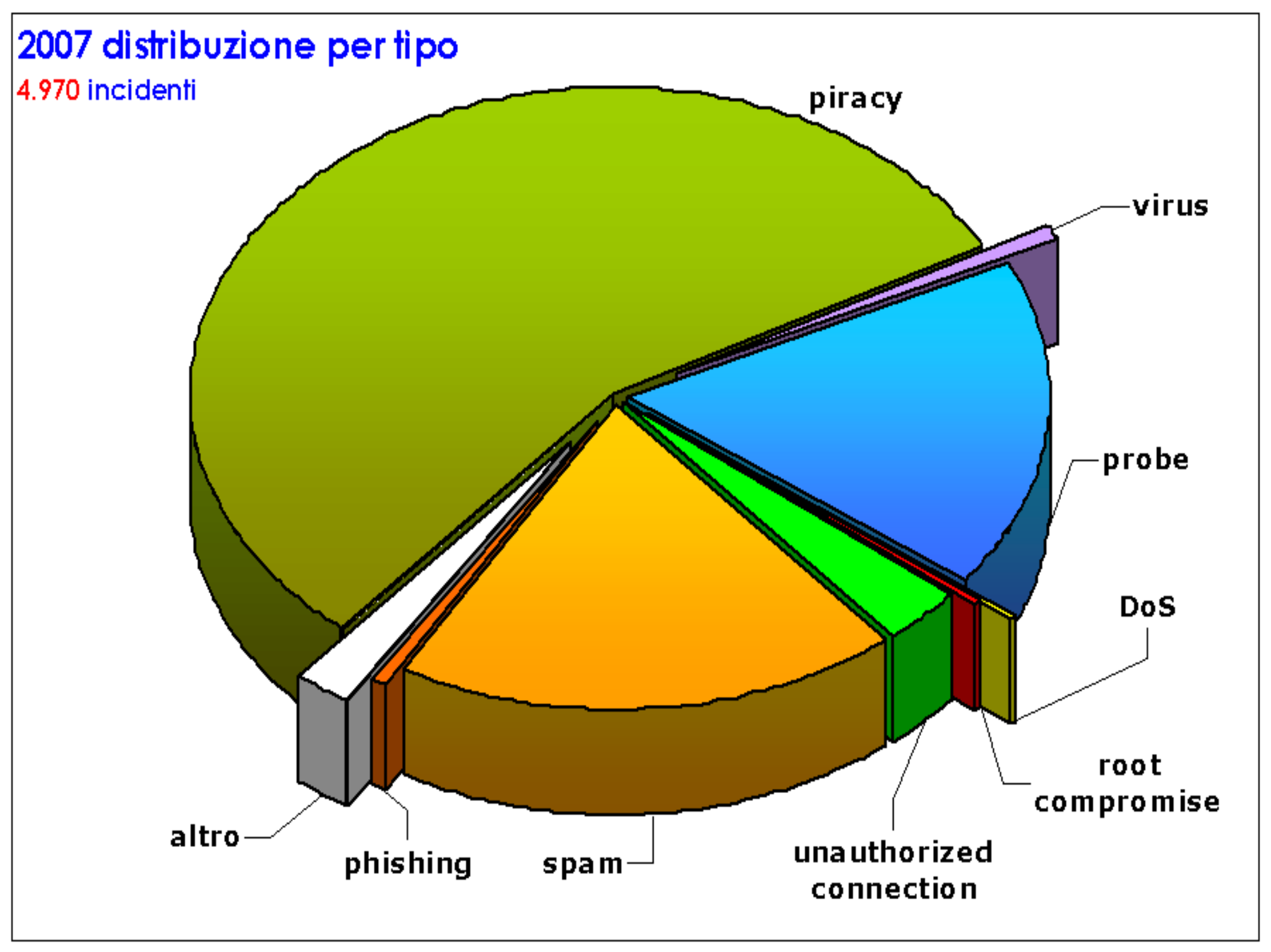

2006 distribuzione per tipo
3.371 incidenti
virus
probe
piracy
DoS
root compromise
unauthorized connection
spam
altro

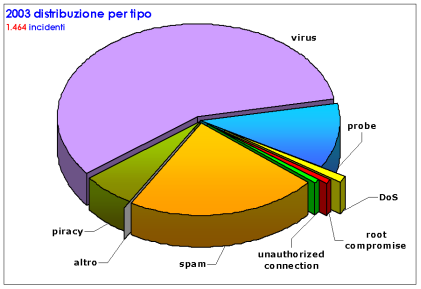

2003 distribuzione per tipo
1.464 incidenti
virus
probe
DoS
root compromise
unauthorized connection
spam
altro
piracy

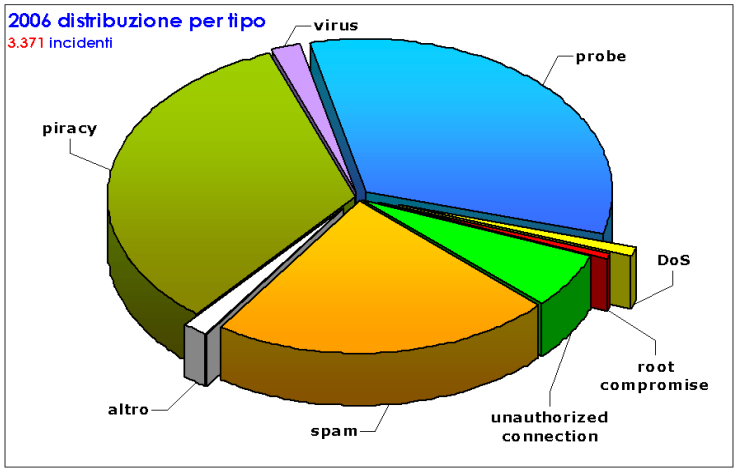

2006 distribuzione per tipo
3.371 incidenti
virus
probe
piracy
DoS
root compromise
unauthorized connection
spam
altro

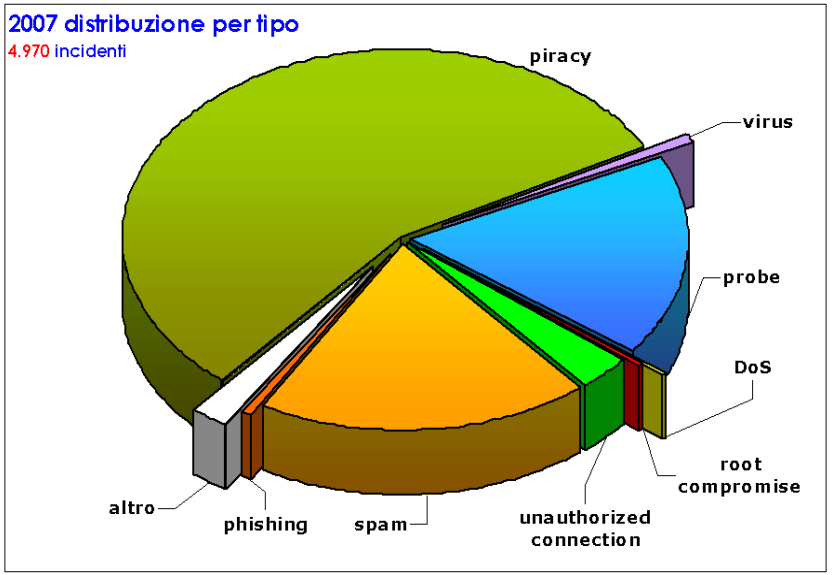
2007 distribuzione per tipo

4.970 incidenti



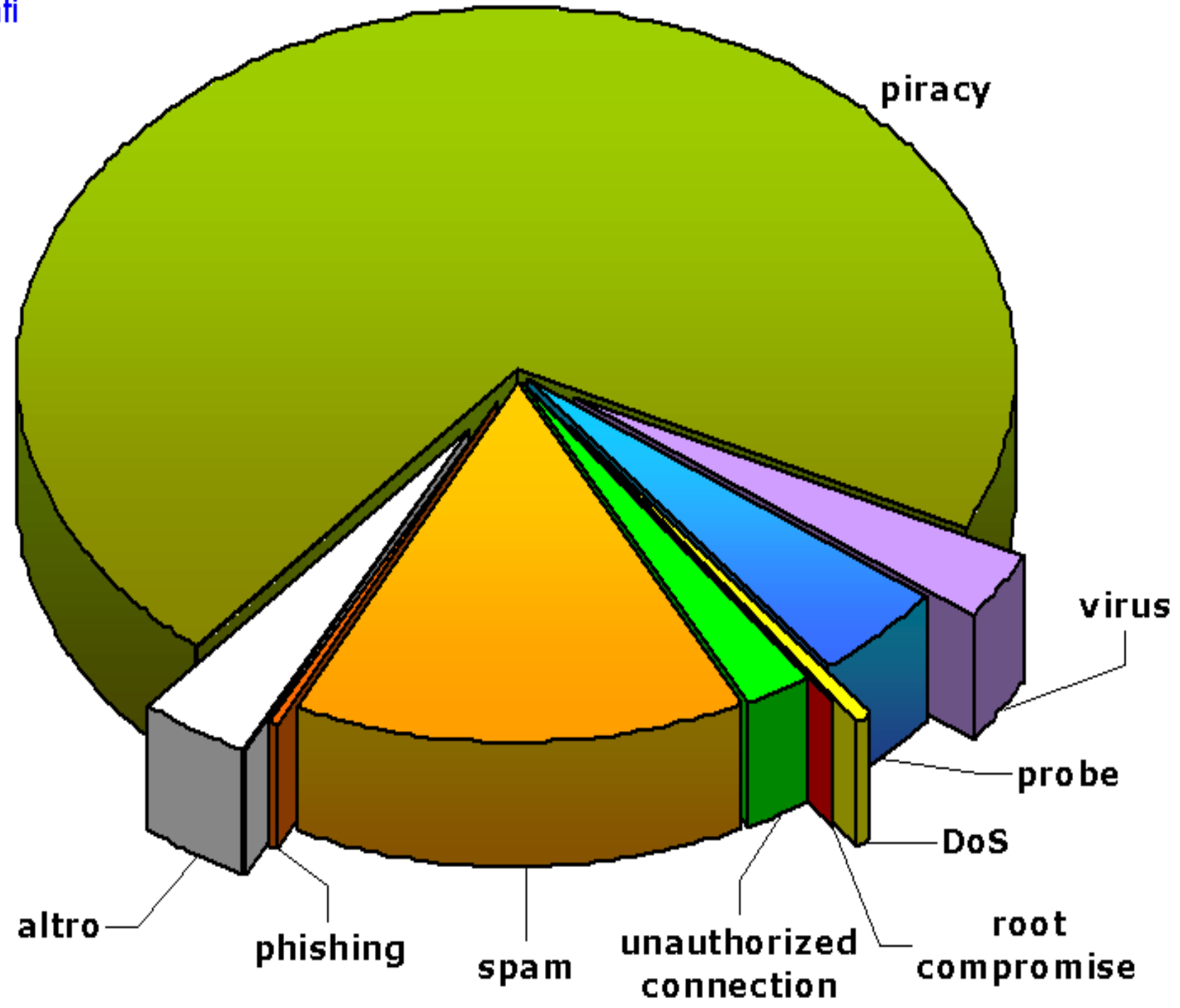

2003 distribuzione per tipo
1.464 incidenti
virus
probe
DoS
root compromise
unauthorized connection
spam
altro
piracy

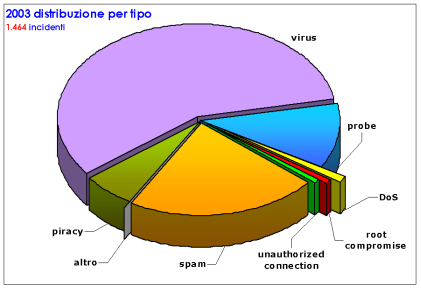

2006 distribuzione per tipo
3.371 incidenti
virus
probe
piracy
DoS
root compromise
unauthorized connection
spam
altro

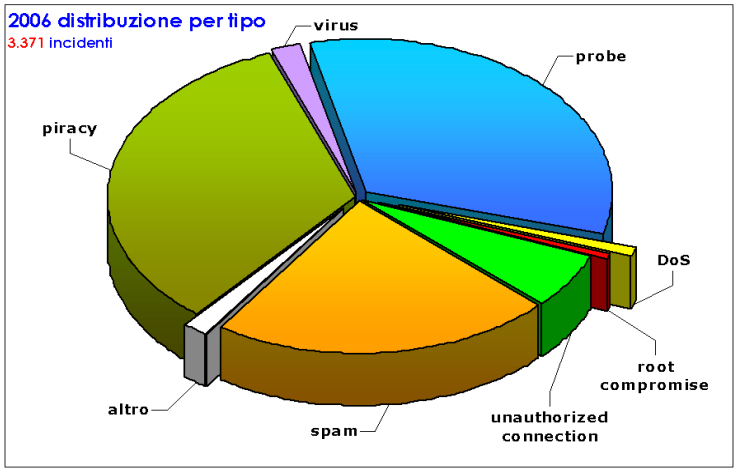

2007 distribuzione per tipo
4.970 incidenti
piracy
virus
probe
DoS
root compromise
unauthorized connection
spam
phishing
altro

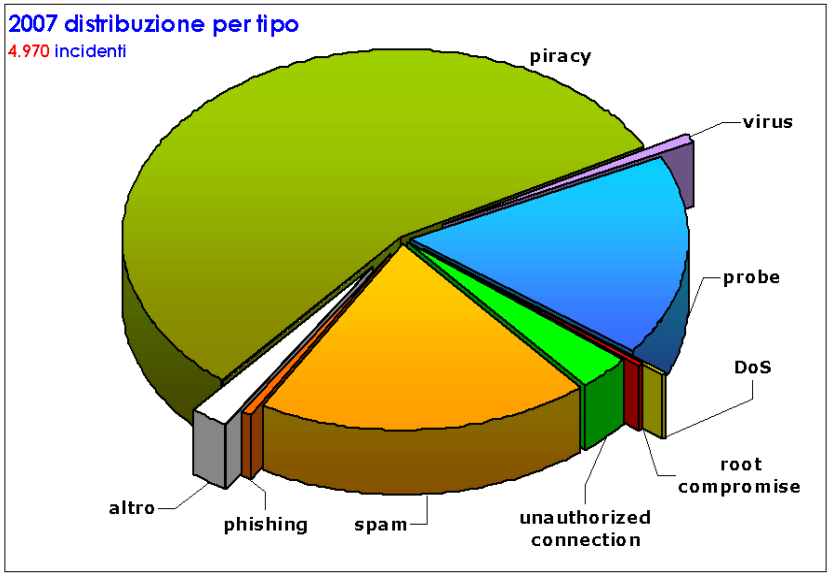
2008 distribuzione per tipo

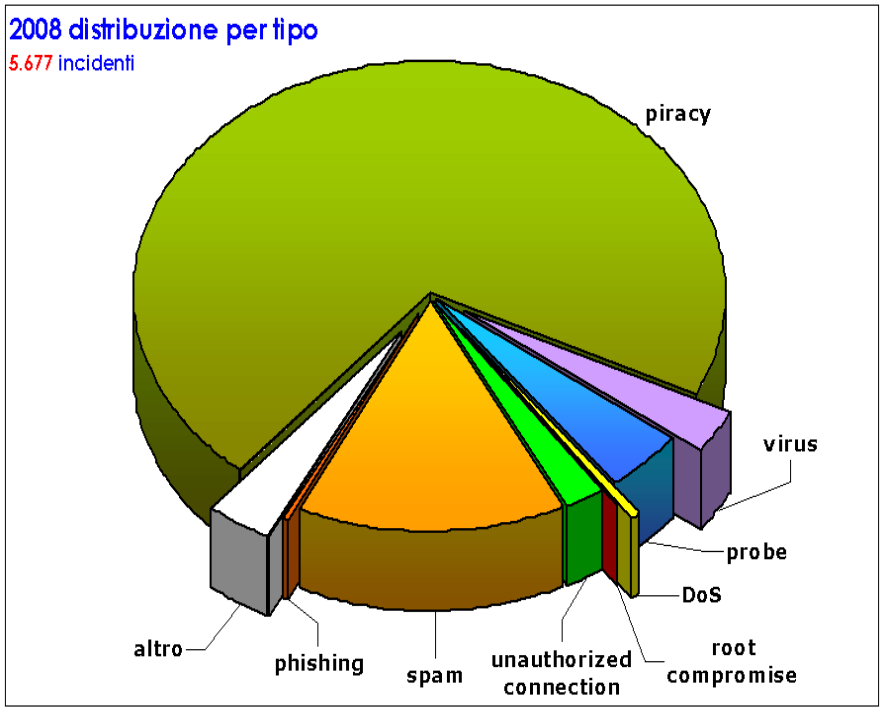
5.677 incidenti

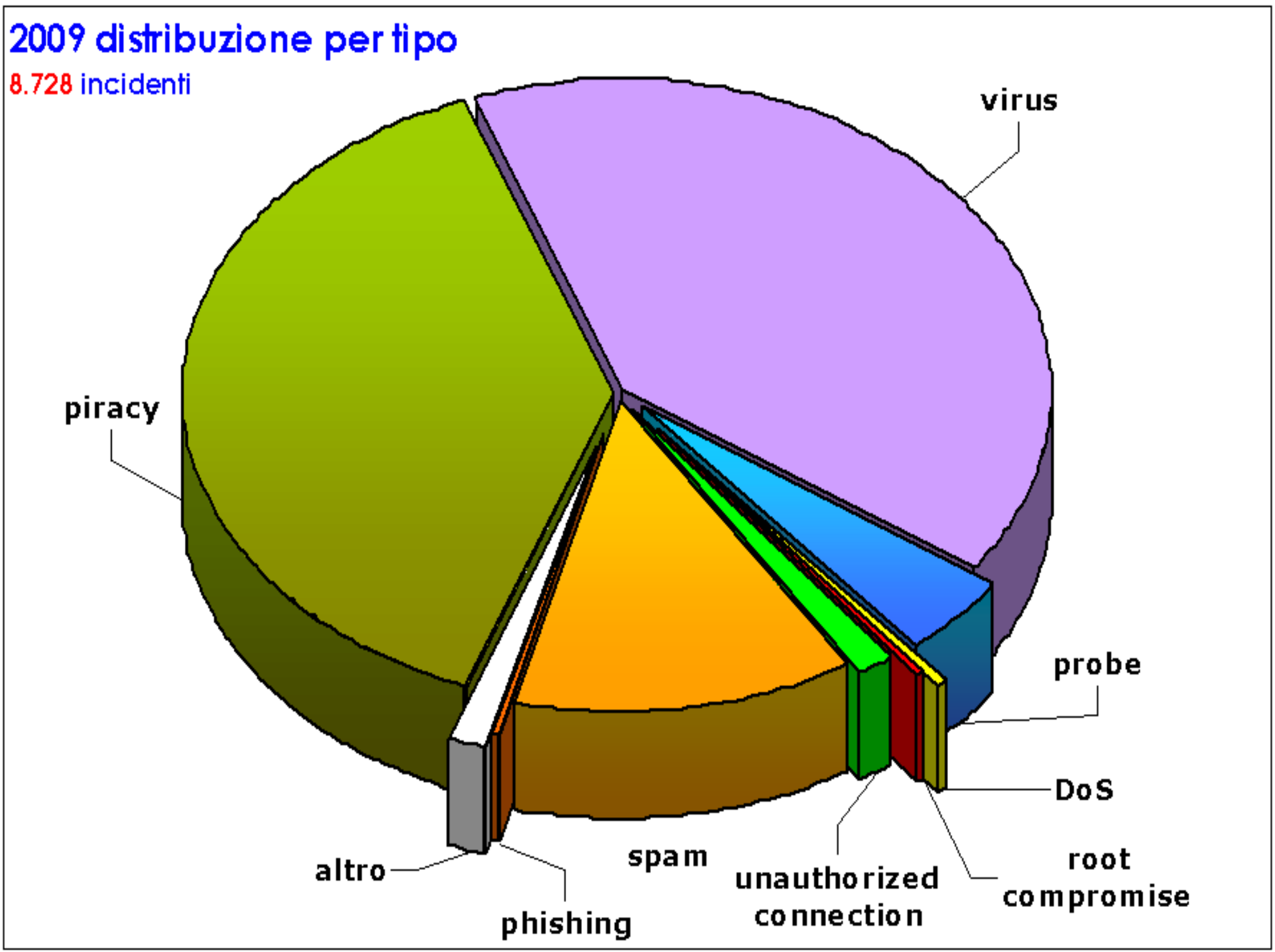


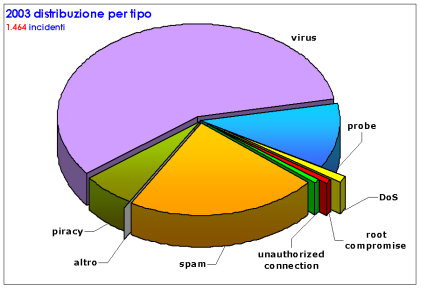

2003 distribuzione per tipo
1.464 incidenti
virus
probe
DoS
root compromise
unauthorized connection
spam
altro
piracy

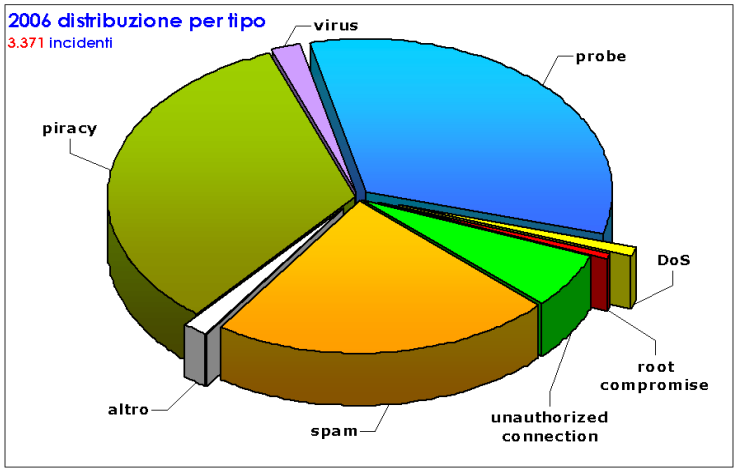

2006 distribuzione per tipo
3.371 incidenti
virus
probe
piracy
DoS
root compromise
unauthorized connection
spam
altro

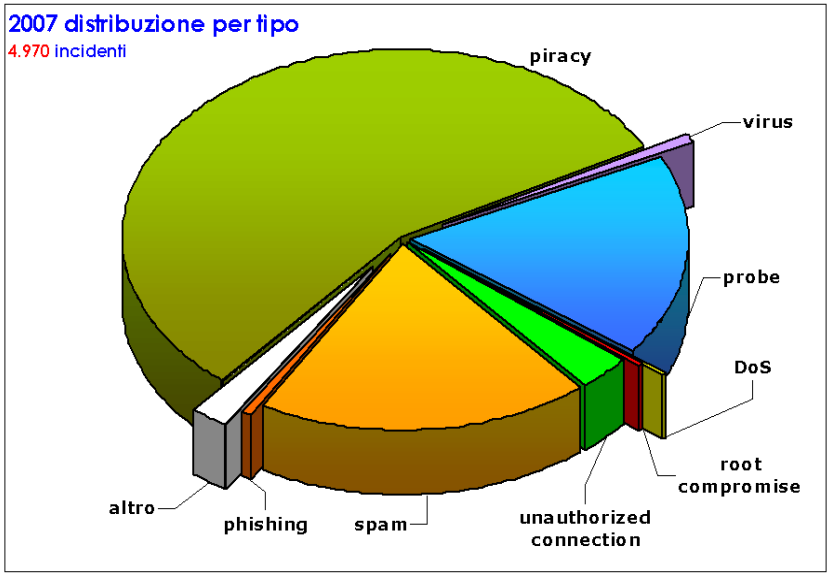

2007 distribuzione per tipo
4.970 incidenti
piracy
virus
probe
DoS
root compromise
unauthorized connection
spam
phishing
altro

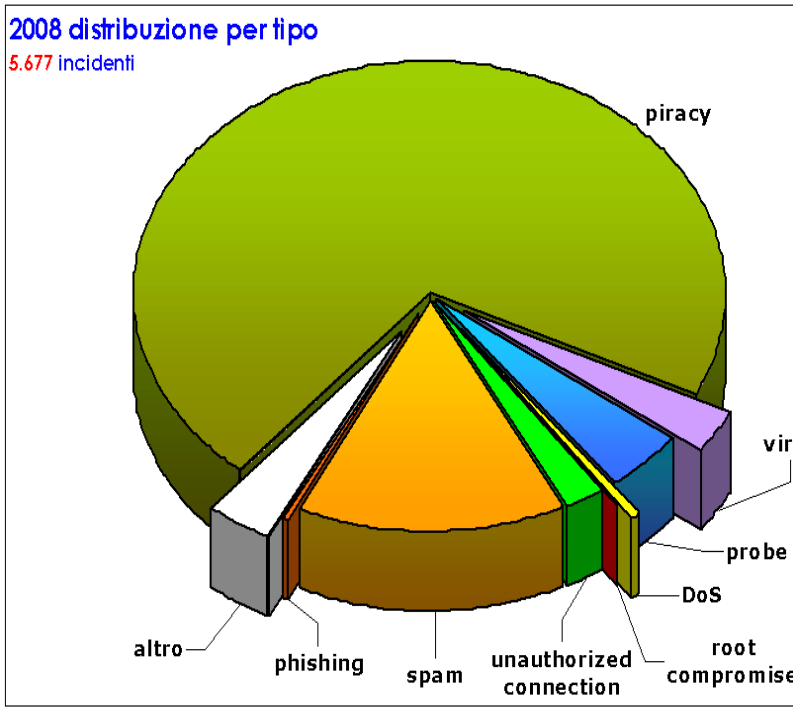

2008 distribuzione per tipo
5.677 incidenti
piracy
virus
probe
DoS
root compromise
unauthorized connection
spam
phishing
altro

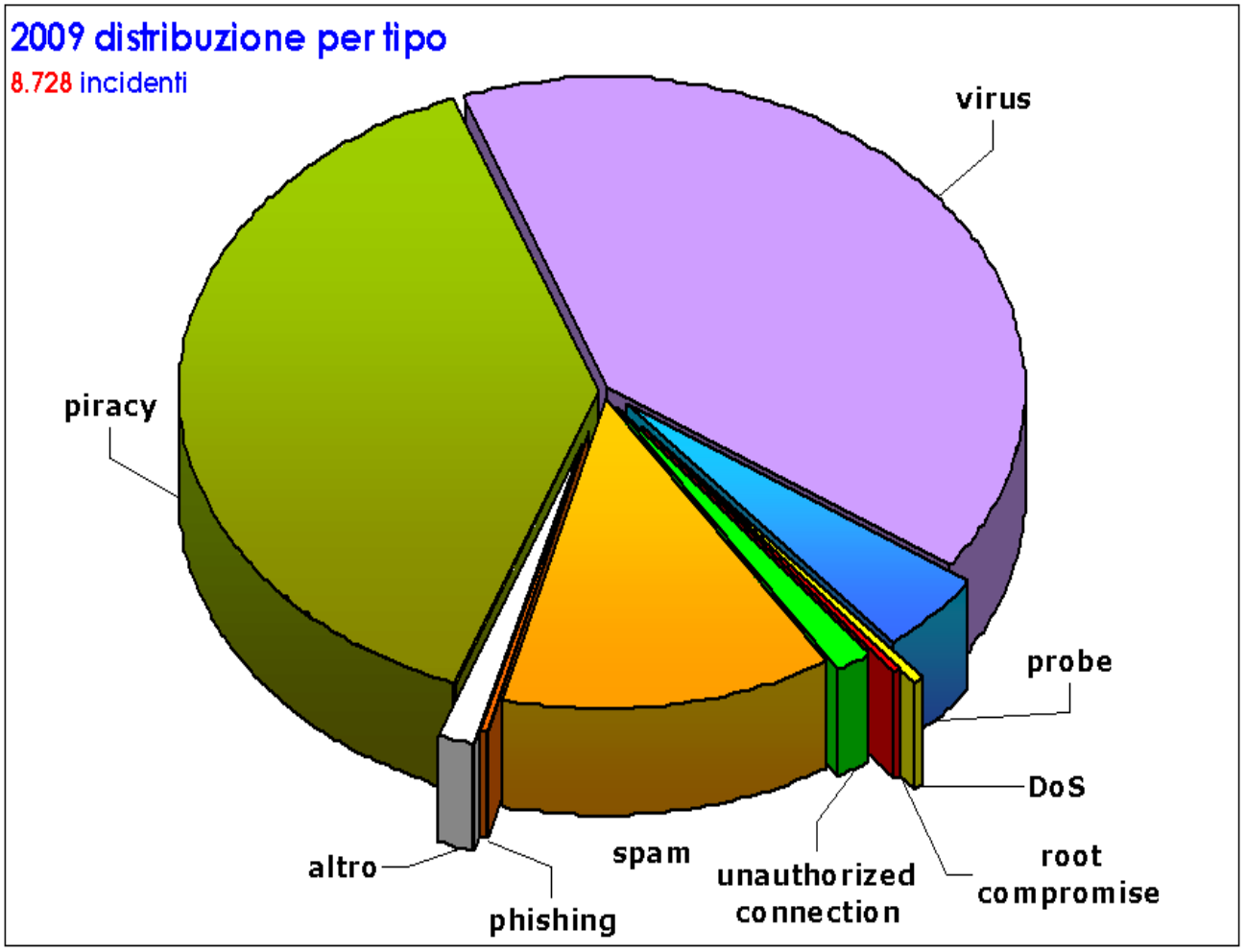

2009 distribuzione per tipo
8.728 incidenti
virus
piracy
probe
DoS
root compromise
unauthorized connection
spam
altro
phishing

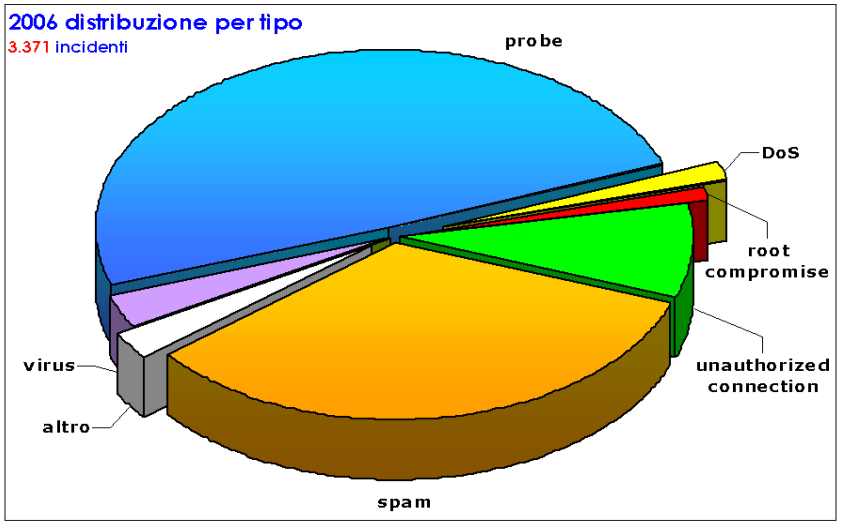

2003 distribuzione per tipo
1.444 incidenti
virus
probe
DoS
root compromise
unauthorized connection
spam
altro
piracy

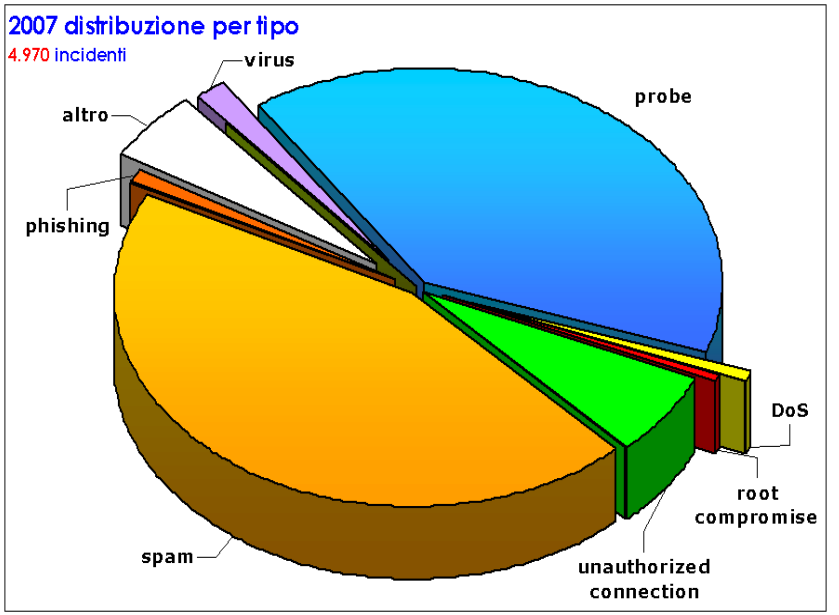

2006 distribuzione per tipo
3.371 incidenti
virus
probe
piracy
DoS
root compromise
unauthorized connection
spam
altro

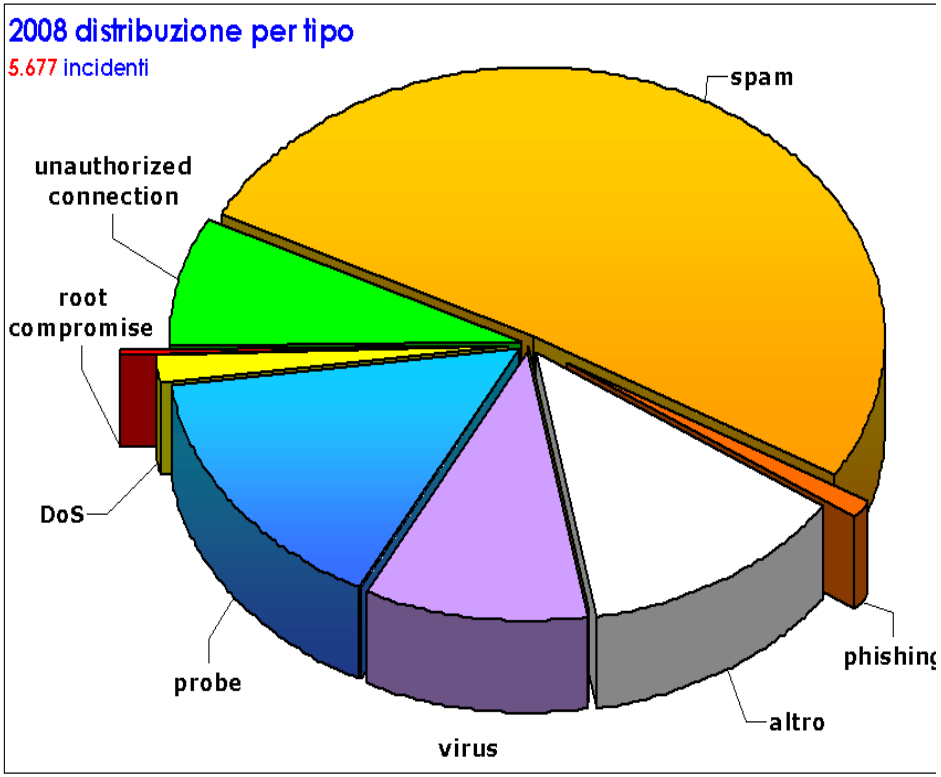

2007 distribuzione per tipo
4.970 incidenti
piracy
virus
probe
DoS
root compromise
unauthorized connection
spam
phishing
altro

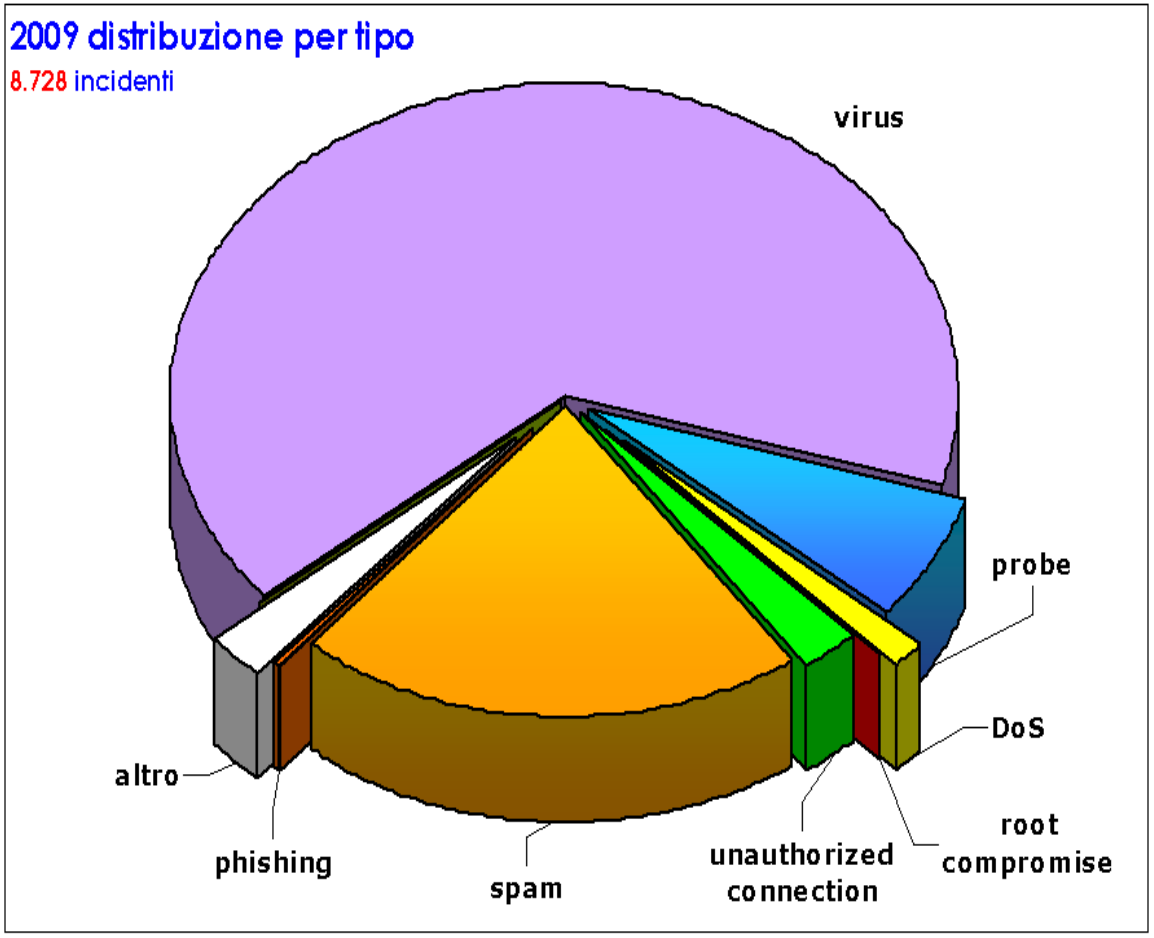

2008 distribuzione per tipo
5.677 incidenti
piracy
virus
probe
DoS
root compromise
unauthorized connection
spam
phishing
altro


2009 distribuzione per tipo
8.728 incidenti
virus
piracy
probe
DoS
root compromise
unauthorized connection
spam
phishing
altro


2006 distribuzione per tipo
3.371 incidenti
probe
DoS
root compromise
unauthorized connection
virus
altro
spam


2007 distribuzione per tipo
4.970 incidenti
virus
probe
altro
phishing
DoS
root compromise
spam
unauthorized connection


2008 distribuzione per tipo
5.677 incidenti
spam
unauthorized connection
root compromise
DoS
probe
virus
altro
phishing


2009 distribuzione per tipo
8.728 incidenti
virus
probe
DoS
root compromise
altro
phishing
spam
unauthorized connection

SPAM

Sistemi che consentono di veicolare lo SPAM:

- Phishing su account “reali” in cui l'utente fornisce a terzi sconosciuti le proprie credenziali
- Password deboli
- Malconfigurazioni degli MTA (open o pratially-open mail-relay)
- Virus: usano MTA istituzionale, anche con autenticazione

Si migliorerebbero molto le cose se gia' si facesse piu' attenzione ai primi tre punti

VIRUS

Veicoli di infezione:

- Browser vulnerabili
- Malware url, creati tramite cross-file scripting e file inclusion, sfruttati sia per ospitare siti di phishing che repository di binari per upgrade dei virus stessi
- Mail di SPAM
- p2p
- Virus “albanese” (viene richiesto l'aiuto dell'utente per installare il virus)

Anamnesi e sintomatologia (1)

- Mandare SPAM per carpire altri dati o procurare altre vittime
- Rubare qualsiasi tipo di credenziale (stesse
- credenziali per accessi “importanti” e no)
- Rubare informazioni (contatti, n. carte di
- credito, pagine web in cache, cookie)
- DoS e DDoS verso altri sistemi

Anamnesi e sintomatologia (2)

- Fare scan/probe per cercare sulla rete nuove macchine vulnerabili.

I tipi di scan/probe sono:

- php file include e cross-scripting
- ssh vulnerability
- ssh brute force login
- vulnerabilita' di sistemi windows

Esempio: conficker

- Sfrutta una vulnerabilita' di windows (MS08-67)
- La patch e' uscita a fine ottobre 2008
- Il virus ha iniziato a diffondersi da gennaio 2009

Probabilmente il sistema di patching
non e' corretto o troppo “permissivo”

Vettori:

- chiavette USB infettate e infettanti
- condivisioni di rete senza password o con password deboli
- botnet

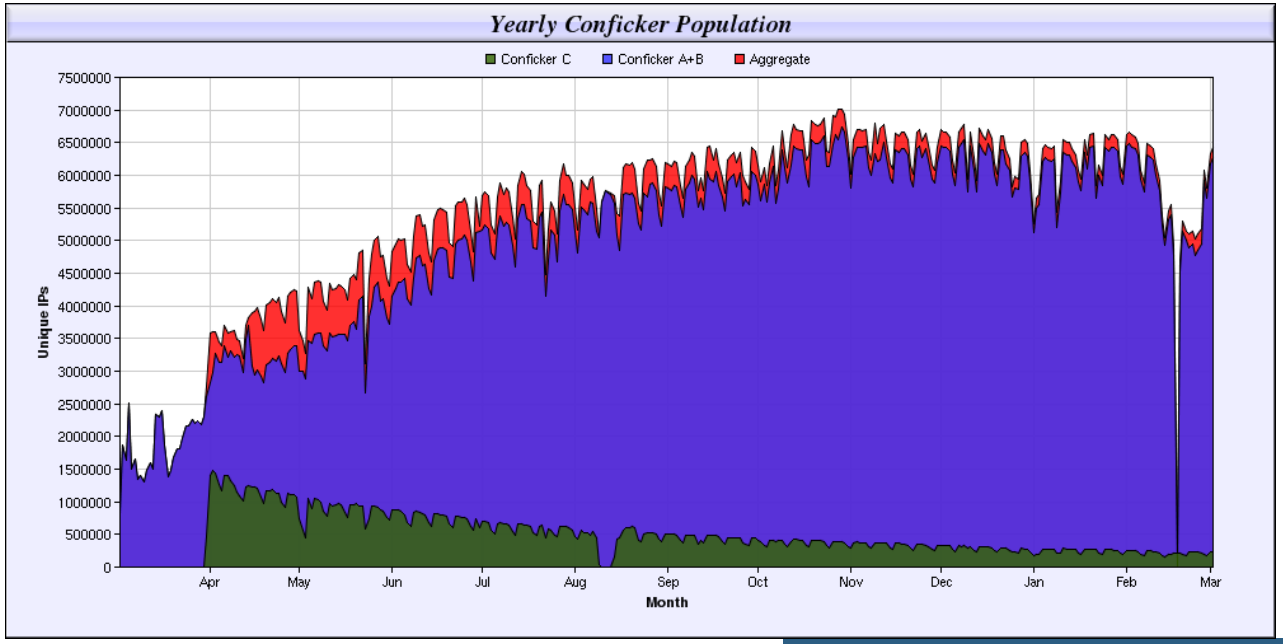
Conficker: cosa fa (1)

- Disattiva servizio backup automatico
- Elimina punti di ripristino precedenti
- Disattiva servizi di protezione
- Blocca accesso a siti web sulla sicurezza
- Apre porte affinche' il “gestore” possa accedere
- Cerca di diffondersi sulla rete locale

Conficker: cosa fa (2)

- Si aggiorna ad una nuova versione
- Scarica un worm: Waledac che ruba dati e inizia a mandare SPAM (simile a StormWorm)
- Installa un finto antivirus: Spyware Protect 2009. Con 50 euro (pagamento solo con carta di credito) ti levano il malware on-line

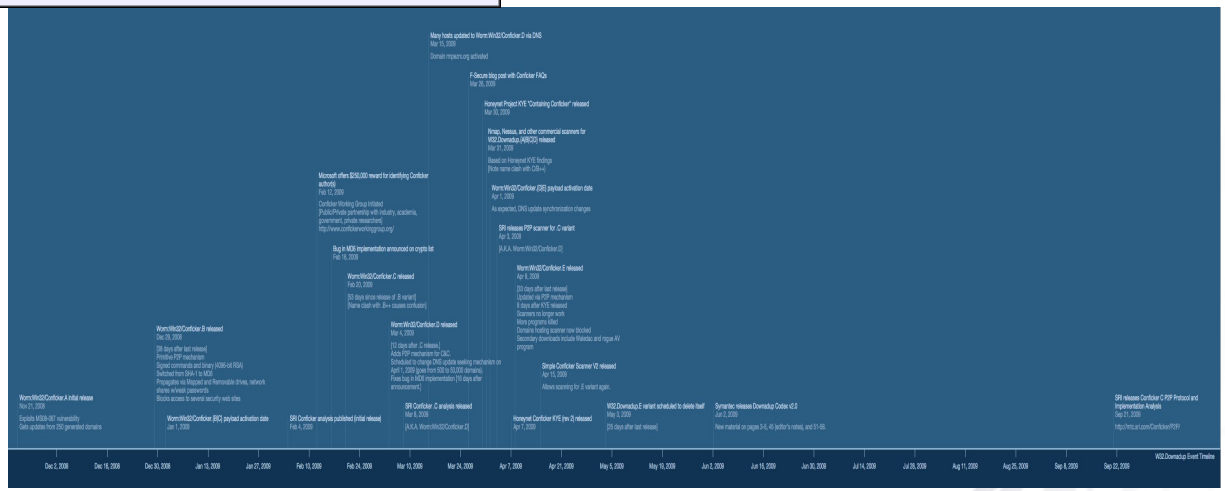
Conficker: conclusione



Controlla circa
6.5M di computer

Fonte: shadowserver.org

Non e' ancora al
massimo delle sue
capacita'



Esempio: Mebroot

- E' in circolazione dal 2006. Il virus piu' longevo per ora
- Sfrutta una o piu' vulnerabilita' dei browser
- L'utente e' indotto tramite SPAM o tramite siti approntati all'uopo a visitare pagine web malevole appositamente predisposte con l'exploit
- L'exploit sfrutta principalmente JavaScritp
- Viene scaricato all'insaputa dell'utente il programma di installazione del virus e viene eseguito

Mebroot: cosa fa

- Modifica la MBR
- Installa il rootkit su un settore non mappabile dal filesystem sull'HardDisk
- Installa una backdoor nel filesystem di windows
- Cancella i file di installazione

Mebroot: cosa fa alla MBR

- Usa una API (CreateFile) sul device \Device\Harddisk0\DR0 con permessi di scrittura
- Scrive in maniera 'raw' sul settore 0
- Le istruzioni accedono a dati e pezzi di codice su disco (il rootkit) che e' scritto in settori non riconducibili a nessun file del filesystem
- Dopo aver eseguito il codice nasconde i pezzi “sporchi” del disco taggandoli come “puliti” intercettando e modificando le relative chiamate di sistema

Mebroot: cosa fa al sistema

- Copia i file che gli serviranno nel silesystem
- Si inserisce fra i servizi e si fa partire a ogni boot
- Inizia a rubare I dati sul sistema:
  - IMAP/POP3/SMTP username, passwords, informazioni sui server per client: AK-Mail, Thunderbird, TheBat
  - Bookmark
  - Indirizzi e-mail da Windows Address Book
  - Password e dati dei vari FTP client: Trellian FTP, WS_FTP, Total Commander, Crystal FTP, Pro e GlobalSCAPE
  - Monitorizza browser (Internet Explorer, Firefox, Opera) per controllare gli accessi a conti correnti bancari delle banche piu' famose (lista che contiene circa 2.500 siti ufficiali di banche)
- Ogni 20 minuti trasferisce i dati rubati a domini autogenerati di volta in volta

Mebroot: conclusioni

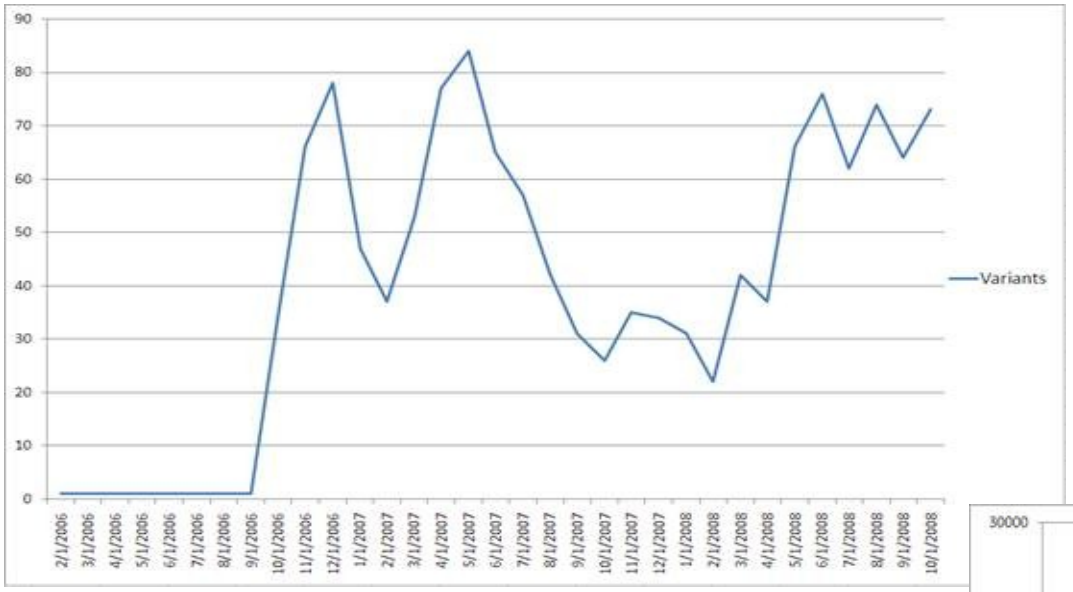
- Difficile da individuare. Gli antivirus trovano il programma di backdoor ma non riescono a trovare ed eliminare il rootkit

- Se si protegge la MBR da BIOS si installa nel partition boot record

- Puo' servire piu' virus differenti, come il Torpig, che utilizzano il sistema di tenere il rootkit mappato nella MBR e non sul SO

- Multipiattaforma: si installa sia su linux che windows

Mebroot: conclusioni (2)

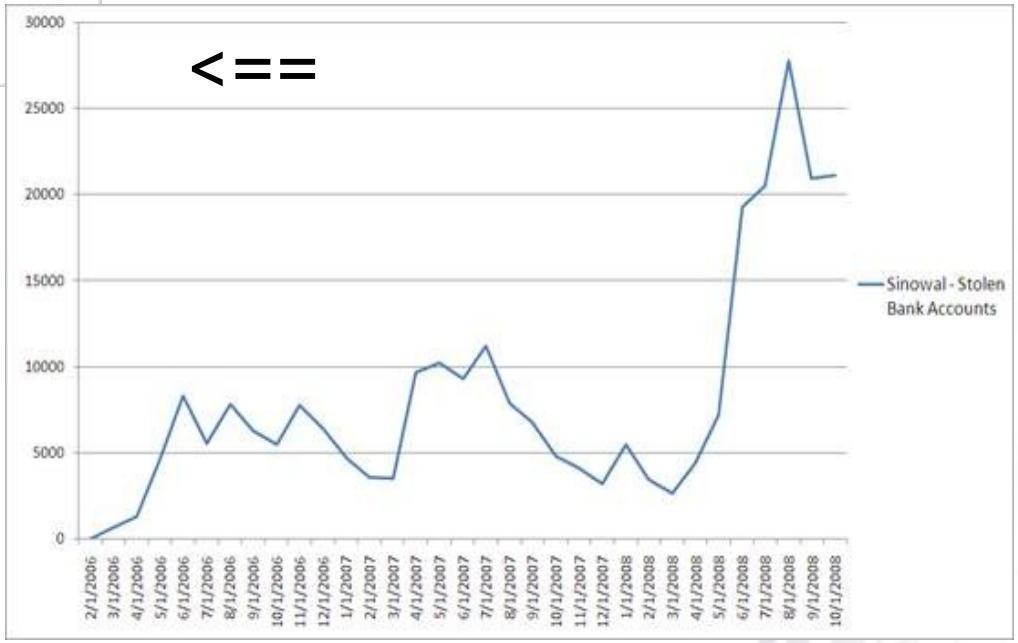


Varianti del virus:
picco di quasi 90
varianti
Il 09.01.2007

<==

Picco di 27.000
bank account
rubati il 09.01.2008

==>



Esempio: Zeus botnet

- E' in circolazione dal 2005 dalla Russia (con amore)
- Il binario (con backdoor) si compra per 700/800$, il sorgente per 4.000/5.000$, c'e' anche la versione 'public'
- Chiunque lo compri puo' crearsi la propria botnet personalizzata, anche se probabilmente dietro il "rivenditore" si nasconde un solo individuo
- Ottimo strumento di partenza per il "businnes" delle botnet, facilissimo da usare e configurare

Vettori:

- QUALSIASI vunerabilita', sia nei browser, nei PDF file, via SPAM, phishing, sistema operativo etc etc
- Solite tecniche di uso delle chiavi di registro, rootkit per nascondersi, aggancio a programmi residenti di sistema per mascherare il traffico

Zeus Botnet: cosa fa

Prima dell'installazione viene configurato e creato il binario personalizzato, fra le altre cose, con:

- il nome della botnet
- il sito dove scaricarsi il DinamicConfig (configurazione successiva)
- la chiave per crittare le comunicazioni
- l'intervallo di tempo in cui passare I dati raccolti al server
- Un server di controllo per capire se la box infettata e' nattata

Zeus Botnet: cosa fa (2)

Dopo essersi installato la prima cosa che fa e' prendersi la DinamicConfiguration dal sito codificato nel binario:

- Url di aggiornamento del binario
- Url del 'drop server' per I log e le informazioni rubate
- Url del 'backup config file' per emergenze
- Lista di url che se inseriti fanno scatenare il log
- Lista di url che se inseriti scattano uno screenshot del video, che viene scattato al primo click del tasto sinistro del mouse
- Lista di coppie di url che, se inserita la prima, si viene rediretti alla seconda
- Lista di url che se inseriti fanno scattare il log delle transaction authentication (TAN)
- Lista di coppie domini/ip da inserire nel file di hosts

Zeus Botnet: cosa ruba

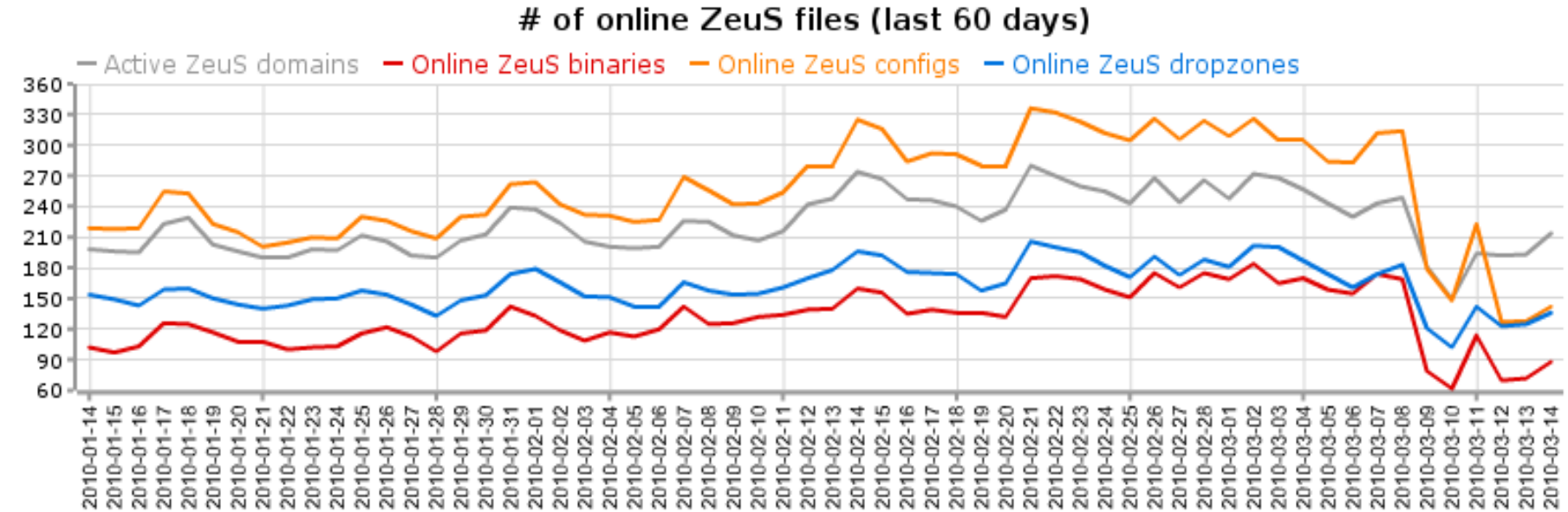
- Cattura dati inseriti nelle form web prima che vengano crittati
- Inietta dati addizionali in form di webpage elencate, in modo che l'utente inserisca dati aggiuntivi non richiesti dalle form originali
- Compila una lista di url che potrebbero contenere credenziali di login o session ID
- Cattura cookie che spesso contengono credenziali di accesso a siti web
- Copia credenziali contenute nel "protected store" dei browser
- Puo' copiarsi qualsiasi file sul pc infetto
- Puo' controllare completamente il pc da remoto tramite VNC
- Puo' scaricare ed eseguire qualsiasi file o binario
- Puo' danneggiare irrimediabilmente il pc infetto cancellando file di sistema

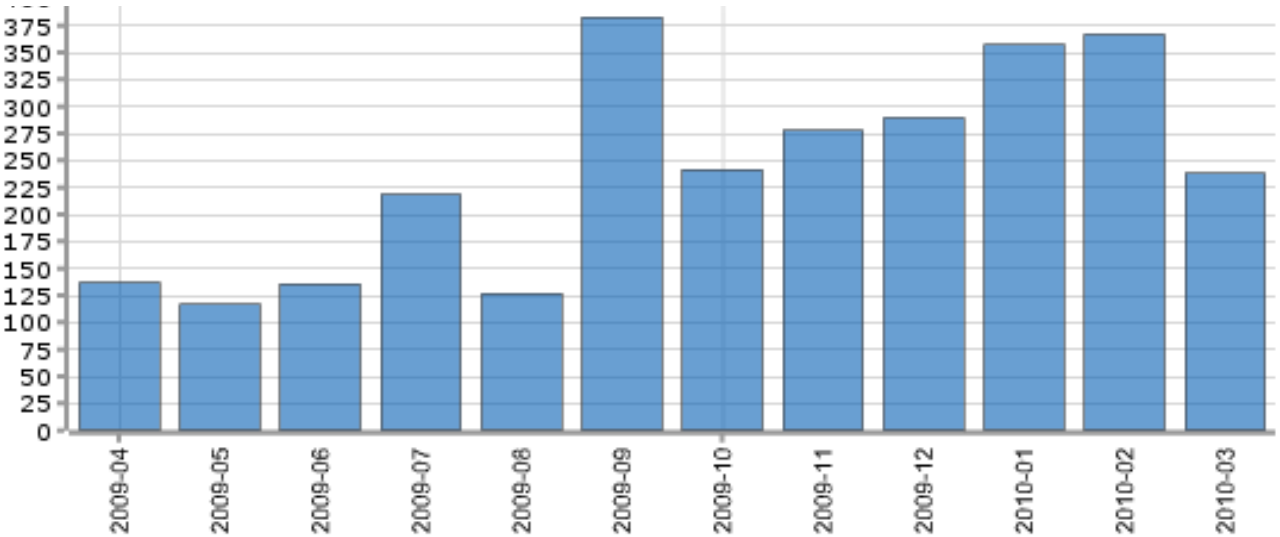
Zeus Botnet: conclusioni

In una settimana di monitoraggio si e' osservato:

- 75.000 nuove macchine fanno parte della botnet Zeus "principale" (600.000 per le "derivate")
- Oltre 75Gb di dati rubati
- 68.000 credenziali rubate durante 4 settimane
- 2.000 certificati SSL rubati
- Connessione con altre botnet (Waledac)
- Viene rilevato da solo il 10% degli antivirus

Zeus Botnet: conclusioni (2)





Fonte
zeustracker.abuse.ch

Aggiornamenti Microsoft aprile 2010

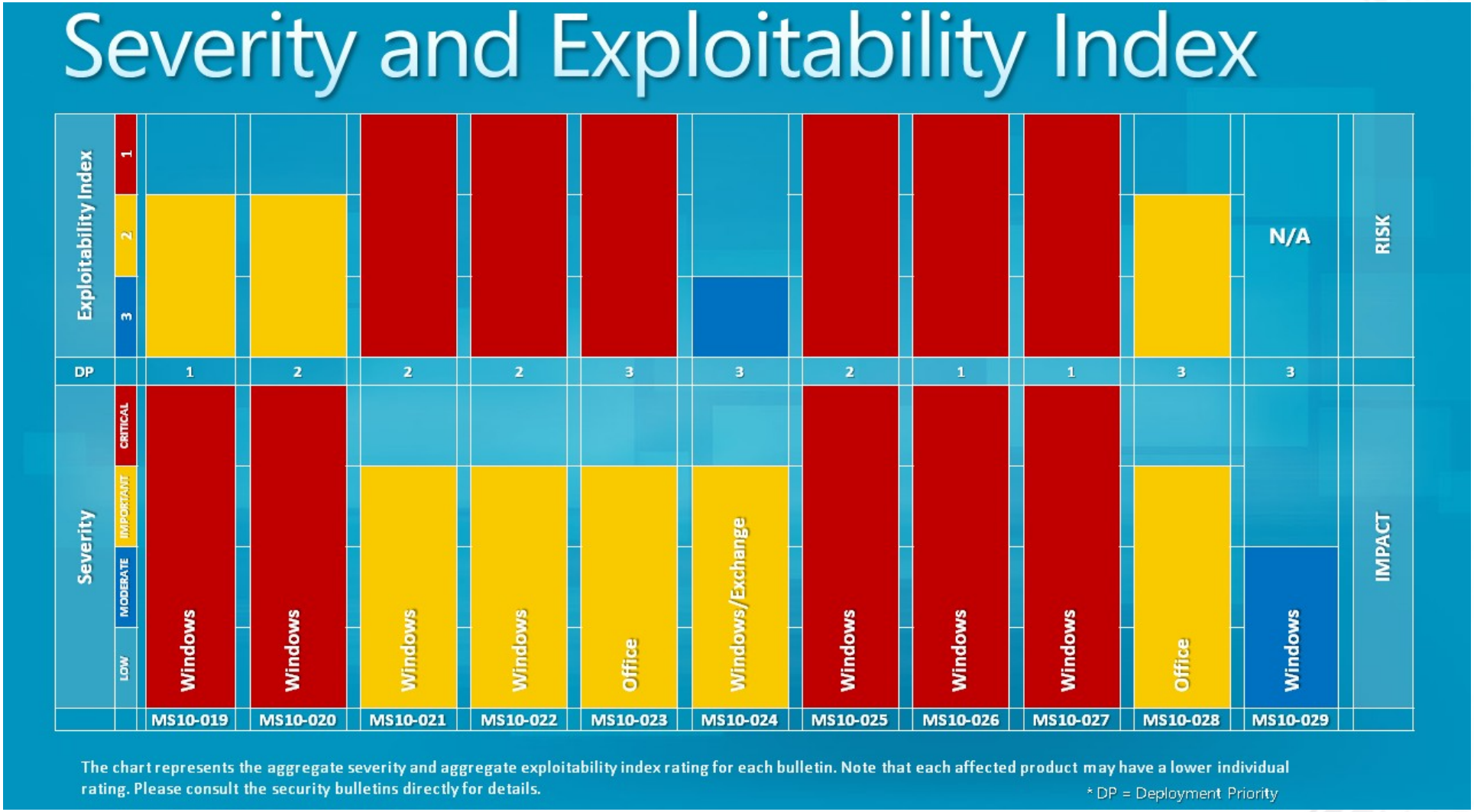
April 2010 Windows Security Bulletins

Bulletins	Windows 2000	Windows XP	Windows Server 2003	Windows Server 2008	Windows Vista	Windows Server 2008 R2	Windows 7
MS10-019	Critical	Critical	Critical	Critical	Critical	Critical	Critical
MS10-020	Critical	Critical	Critical	Critical	Critical	Critical	Critical
MS10-021	Important	Important	Important	Moderate	Moderate SP1/SP2 / Important RTM	Moderate	Moderate
MS10-022	Important	Important	Important	NA*	NA*	NA*	NA*
MS10-024	Important	Important	Important	Important	NA	Important	NA
MS10-025	Critical	NA	NA	NA	NA	NA	NA
MS10-026	Critical	Critical	Critical	Critical	Important	NA	NA
MS10-027	Critical	Critical	NA	NA	NA	NA	NA
MS10-029	NA	Moderate	Moderate	Moderate	Moderate	NA	NA

* Customers will be offered these as Defense-in-Depth updates.

Fonte: www.ghacks.net

Aggiornamenti Microsoft aprile 2010



Fonte: www.ghacks.net

Difese nelle trincee

Lato GARR: monitoraggio e sistemi di early alerting

Lato sistemista: patching, password

Lato utente: password, attenzione

Futuro nelle trincee

- **Lato MINACCE - non c'e' mai fine al peggio:**
  - Aumento del “bad traffic”
  - Nuovi sistemi di comunicazione (p2p, crypt)
  - Sistemi sempre piu' furbi e meno invasivi
- **Lato GARR - monitoraggio automatico:**
  - Studio di anomalie di traffico
  - Monitoraggio botnet/HoneyPot
  - Studio DNS e 'fast flux' domain
  - Studio sistema automatico per apertura incidenti
- **Lato Europa/internazionale - coordinamento e comunicazione:**
  - Coordinamento per soluzione di problemi urgenti
  - Standardizzazione sistemi di trasmissione delle informazioni
  - Cooperazione e ricerca per migliorare il monitoraggio

Trincee di riferimento

Generale:

- www.garr.it, www.cert.garr.it

Conficker:

- mtc.sri.com/Conficker
- shadowserver.org

Mebroot:

- www2.gmer.net/mbr
- mkwingzero.com/virus/52-threat-info/86—sinowal-analysis-of-rsa-lab.html

Zeus:

- zeustracker.abuse.ch
- www.fortiguard.com
- netwitness.com