Sicurezza e Gestione dell'Insicurezza

{,in}sicurezza delle reti

(suggerito da Alfredo)

Simona Venuti
simona.venuti@garr.it
GARR-CERT

Bei Mi' Tempi

- **Hardening:** dopo l'installazione di un sistema operativo si chiudono i servizi e le porte inutilizzate
- **Mailing List:** Sottoscrizione a mailing list di alerting o di security o dei vendor per essere informati prima possibile su eventuali vulnerabilita'
- Installazione di un **sistema di patching**, meglio se centralizzato, per mantenere le macchine aggiornate dopo il rilascio di patch
- Scrivere **politiche di contenimento** se le patch non possono essere applicate immediatamente o se devono essere testate fuori dell'ambiente di produzione
- Installare sistemi **antivirus** sulle macchine windows
- **FIREWALL?** Solitamente veniva venduto come soluzione di tutti i problemi di sicurezza ma deve essere mantenuto ed e' inutile se un servizio ha una vulnerabilita'

Bei Mi' Tempi

Se un sistemista non riusciva a compiere queste operazioni:

- Poteva utilizzare strumenti “post mortem” e analisi forense
- Poteva installare IDS per vedere cosa passasse per la rete

Le minacce da affrontare riguardavano:

- Buffer overflow locali e remoti
- Cross-site scripting
- Applicazioni “fatte in casa”

L'anello debole della catena:
i SISTEMISTI && le politiche di rete e di patching

Evoluzione delle Minacce

Aspetti legali:

- Le leggi nazionali sono molto differenti l'una dall'altra, spesso qualcosa e' illegale qua in Italia ma non per esempio in Russia o in Cina

Il "lato utente":

- Il 90% del "male" e' distribuito fra worm, virus, BOTNET su homePC

Il "lato hacker":

- L' hacking e' una prestazione professionale ben remunerata
- Attivita' illegali molto lucrose (SPAM, DdoS, BOTNET)

La h4cK3rZ-CoMMuNiTy:

- 0-day (preponderanza di minacce sconosciute)
- Close disclosure (mancata disseminazione delle informazioni)
- Nessuna necessita' di shell o di diventare root su una box

Limiti della Old SeCuRiTy

- Limitatezza nelle firme degli IDS dovuta ad una grande quantita' di vulnerabilita' sconosciute
- Banda elevata per gli utenti da casa
- Enorme quantita' di minacce e/o varianti sconosciute

I PC sono diventati "SCATOLE NERE"

nessuno (o quasi) sa cosa stanno facendo!

Gli **anelli deboli** della catena:

- **I sistemisti e le politiche** come ai bei mi' tempi
- **Gli utenti** da casa
- **l'approccio alla sicurezza**: i vecchi metodi sono inutili adesso

PAURA?

Quando il gioco si fa duro

...

I duri iniziano a giocare!

(J. Belushi)

Nuovo approccio alla SeCuRiTy

- Monitoraggio GLOBALE tramite NetFLOW
- Monitoraggio LOCALE tramite HoneyPot

*Il monitoraggio e' **"La VIA"** per sviluppare nuove politiche di difesa e si basa su:*

- Ricerca di pattern comuni nei vari tipi di attacco (Esempio: correlazioni temporali)
- Misure proattive
- Sistemi di allerta e di apertura incidenti

Monitoraggio GLOBALE: NetFLOW

NetFLOW e' un protocollo pressoche' standard (IEEE-IPFIX) usato per trasportare informazioni di sessioni ip sulla rete

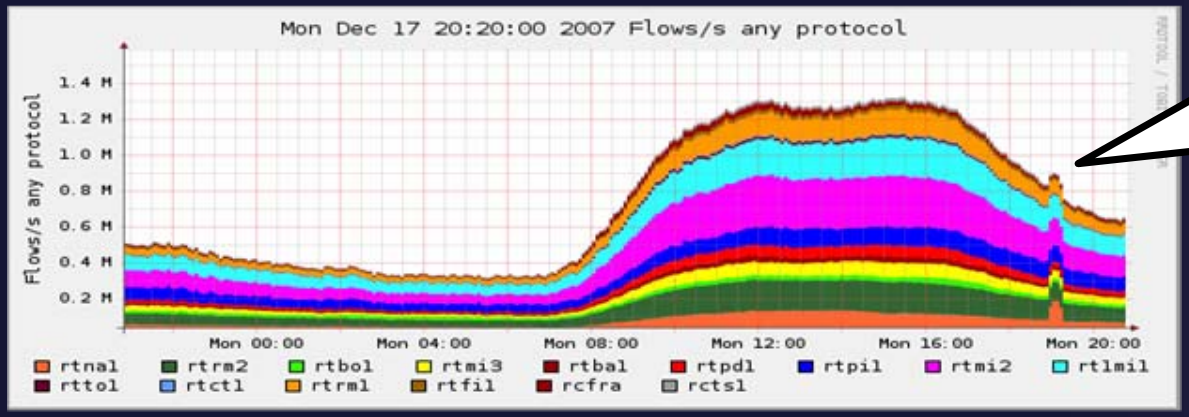
Le informazioni fondamentali sono:

ip src, porta src, ip dst, porta dst

- Utile agli NREN per vedere che succede
- Supporta informazioni sugli AS e sulle router interface
- E' supportato da quasi tutti i vendor

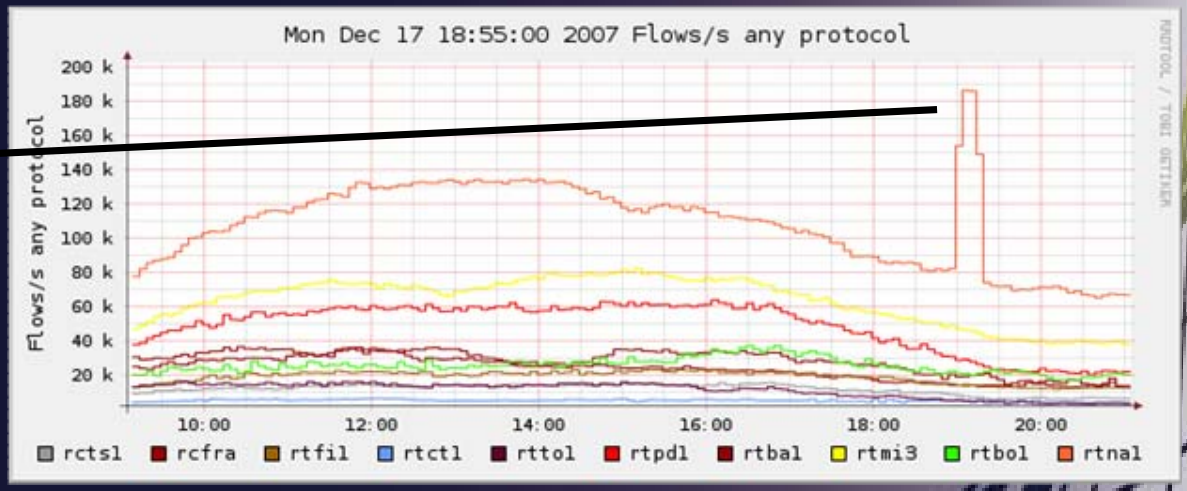
Monitoraggio GLOBALE: NetFLOW

Interfaccia grafica a NetFLOW: nfsen



Qua c'e' qualcosa di STRANO…

Effettivamente e' uno strano picco nel numero di flussi



Monitoraggio GLOBALE: nfsen

- Possiamo guardare chi e' il TOP-IP della rete GARR che fa piu' traffico:

Date first seen	Duration	Proto	IP Addr	Flows	Packets	Bytes	pps	bps	bpp
2007-12-17 19:11:24.853	1719.694	any	**x.x.186.18**	108718	114375	3.2 M	66	15446	29

- Ora si puo' indagare cosa sta facendo:

Date flow start	Duration	Proto	Src IP Addr:Port	->	Dst IP Addr:Port	Flags	Tos	Packets	Bytes	Flows
2007-12-17 19:39:09.658	0.000	TCP	GARR_IP:54642	->	**y.y.77.49:22**	....S.	0	1	60	1
2007-12-17 19:39:02.816	0.000	TCP	GARR_IP:59711	->	**y.y.74.41:22**	....S.	0	1	60	1

- L'ip GARR sta facendo ssh scan... e non solo!

2007-12-17 19:16:20.822	0.000	TCP	**GARR_IP:22**	->	**z.z.112.57:1227**	.AP...

- Qualcuno e' entrato in ssh dentro il GARR-ip

Monitoraggio GLOBALE: nfsen

In conclusione:

- Il GARR-CERT puo' aprire un incidente con l'APM dell'ip-GARR coinvolto per macchina compromessa, o in via precauzionale, per ssh probe.
- L'APM coinvolto puo' aprire un incidente verso l'ISP della macchina che era entrata in ssh

Ma sarebbe bello che facesse tutto da solo!

Monitoraggio GLOBALE: nfsen

Nfsen ha due sistemi per automatizzare:

- **Il sistema di alert:** utile se le condizioni non sono troppo complicate
  - Numero di flussi > numero_assoluto
  - Numero di flussi > percentuale_media_oraria
  - Top-One statistic (unico ip che trasmette)

Utile per trovare picchi,
anomalie di traffico, DDoS

Monitoraggio GLOBALE: nfsen

- **Plugin System:** capacita' di inserire codice perl all'interno dell'elaborazione dei dati per compiere azioni non contemplate
  - Anomalie di traffico basato su algoritmi BICHOS, Holtz-Winter, DdoSVAX
  - TrackStats: lista esportabile delle Top-Ports
  - PortTracker: grafico mrtg continuo delle porte piu' “gettonate”

Scarsa documentazione, basse prestazioni

fase di sperimentazione

Ricerche future

- Automazione
- Early alerting
  - Anomalie di traffico
  - DoS
  - ScanPort, ssh Probe
- Top-Ports (scritto da noi)
- Supporto a honeypot e ricerca botnet
  (vedi oltre)

Monitoraggio LOCALE

Dal momento che i metodi di analisi delle firme degli IDS non sono in grado di riconoscere tutte le vulnerabilita' e minacce dobbiamo scegliere un diverso approccio.
Mettiamo una macchina in rete e vediamo che succede: ...

... una macchina windows diventa uno ZOMBIE (cioe' parte di una botnet) appena 3 minuti dopo che si e' inserito il plug di rete!!!

Quale e' il problema? Chi la infetta? Perche'? E COME?

Si puo' rispondere a queste domande
mettendo on-line
una HONEYPOT

Monitoraggio LOCALE: HoneyPot

Ci sono due tipi di honeypot: a *bassa e alta interazione*

- **Bassa interazione:**
  - Servizi emulati
  - Macchina non bucabile
  - Scarsa manutenzione
  - Utile per rilevamento della diffusione del malware
- **Alta interazione:**
  - Servizi reali
  - Macchina completamente vulnerabile e bucabile
  - Alta manutenzione
  - Utile per catturare 0-day e minacce non documentate

Analisi HoneyPot al GARR-CERT

- Partecipazione al progetto **NoaH** mettendo a disposizione un ip della rete GARR che inoltra tutto il traffico verso la rete NoaH
- Installazione di una macchina virtuale con debian etch e tool **Honey@Home**
- Simile a seti@home sfrutta spazi di indirizzamenti inutilizzati per inoltrare tutto il traffico verso la rete NoaH, dove ci sono HoneyPot ad alta interazione
- Scopo del progetto e' collezionare traffico da piu' ip diversi possibile, per avere un'idea coerente delle minacce che incombono sulla rete, con sforzo minimo per i sistemisti

HoneyPot al GARR-CERT

Dopo questa avventura poco avventurosa abbiamo deciso di giocare un po' piu' duro, installando una **HoneyPot a bassa interazione**, sempre su una macchina virtuale xen, con debian etch

Utilizzazione del tool **nepenthes:**

- Interagisce molto bene al malware, anche a quelli sconosciuti non rilevabili dagli antivirus
- Capacita' di scaricare il malware che i virus inducono a scaricare

Abbiamo ruotato su quella macchina il traffico per una DarkNet del GARR di classe C e in due giorni abbiamo collezionato circa 30Mb di malware

HoneyPot al GARR-CERT

Abbiamo sottomesso parte del malware scaricato alla Norman Sandbox, ottenendo questo risultato:

Il famosissimo SASSER worm

```
[ DetectionInfo ]
    * Sandbox name: W32/Sasser.gen
    * Signature name: Sasser.B
    * Compressed: YES
    * TLS hooks: NO
    * Executable type: Application
    * Executable file structure: OK

[ General information ]
    * File length:        15872 bytes.
    * MD5 hash: 1a2c0e6130850f8fd9b9b5309413cd00.

 [ Changes to filesystem ]
    * Creates file C:\WINDOWS\avserve2.exe.

 [ Changes to registry ]
    * Creates value "avserve2.exe"="C:\WINDOWS\avserve2.exe"
in key "HKLM\Software\Microsoft\Windows\CurrentVersion\Run".

 [ Network services ]
    * Connects to "0" on port 445.

 [ Security issues ]
    * Possible backdoor functionality [UNKNOWN] port 5554.

 [ Process/window information ]
    * Creates a mutex Jobaka3.
    * Will automatically restart after boot (I'll be
back...).
    * Creates a mutex JumpallsNlsTillt.
    * Creates process "c:\sample.exe".

 [ Signature Scanning ]
    * C:\WINDOWS\avserve2.exe (15872 bytes) : Sasser.B.
```

HoneyPot al GARR-CERT

Un BOT parte di una BOTNET

```
[ DetectionInfo ]
    * Sandbox name: W32/Spybot.gen3
    * Signature name: W32/Spybot.BEUV
    * Compressed: YES
    * TLS hooks: NO
    * Executable type: Application
    * Executable file structure: OK

[ General information ]
    * Anti debug/emulation code present.
    * Drops files in %WINSYS% folder.
    * **Locates window "NULL [class RegmonClass]" on
desktop.
    * **Locates window "NULL [class FilemonClass]" on
desktop.
    * **Locates window "NULL [class SuckMe&Class]" on
desktop.
    * **Locates window "NULL [class APIMonitor By
Rohitab]" on desktop.
    * **Locates window "NULL [class TDeDeMainForm]" on
desktop.
    * **Locates window "NULL [class TIdaWindow]" on
desktop.
    * **Locates window "NULL [class mIRC]" on desktop.
    * File length:       159744 bytes.
    * MD5 hash: 1d419d615dbe5a238bbaa569b3829a23.

 [ Changes to filesystem ]
    * Creates file C:\a.bat.
    * Creates file C:\WINDOWS\SYSTEM32\ssms.exe.
    * Deletes file %temp%\1.reg.
    * Deletes file %0.
    * Deletes file 256.
```

```
[ Changes to registry ]
    * Creates value "Windows Update"="ssms.exe" in key
"HKLM\Software\Microsoft\Windows\CurrentVersion\Run".
    * Creates value "Windows Update"="ssms.exe" in key
"HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices".
    * Creates key "HKCU\Software\Microsoft\OLE".
    * Sets value "Windows Update"="ssms.exe" in key
"HKCU\Software\Microsoft\OLE".
    * Sets value "restrictanonymous"="" in key
"HKLM\System\CurrentControlSet\Control\Lsa".

[ Network services ]
    * Looks for an Internet connection.
    * Connects to "botz.noretards.com" on port 65146.   *****
    * Connects to IRC Server.
    * IRC: Uses nickname [FUCKOFF]-555311.
    * IRC: Uses username jqxxzn.
    * IRC: Joins channel #a with password imallowed2020.
    * IRC: Sets the usermode for user [FUCKOFF]-555311 to +xt.
    * Attempts to delete share named "IPC$" on local system.
    * Attempts to delete share named "ADMIN$" on local system.
    * Attempts to delete share named "C$" on local system.
    * Attempts to delete share named "D$" on local system.

 [ Process/window information ]
    * Creates process "C:\CMD.EXE".
    * Creates a mutex ssms.exe.
    * Creates process "C:\WINDOWS\SYSTEM32\ssms.exe".
    * Will automatically restart after boot (I'll be back...).
    * Checks if privilege "SeDebugPrivilege" is available.
    * Enumerates running processes.

 [ Signature Scanning ]
    * C:\a.bat (5894 bytes) : WinREG.A.
    * C:\WINDOWS\SYSTEM32\ssms.exe (159744 bytes) :
W32/Spybot.BEUV.
```

Utilizzo HoneyPot al GARR-CERT

- Cattura e apertura automatica di incidenti relativi agli IP-GARR che si connettono alla HoneyPot, invio automatico dei log a APM
- Segnalazione automatica a ISP esterni di macchine infette
- Monitoraggio tramite nfsen delle connessioni alla darknet
- Tramite Sandbox estrapolazione di ip dei server di BOTNET da mettere in nfsen per monitorare il traffico di BOT

Tracciamento BotNet

Stiamo facendo tentativi per tracciare e rilevare computer all'interno della rete GARR che fanno parte di BotNet
Non essendoci nessun punto di riferimento o strumento gia' pronto stiamo indirizzando la ricerca in varie direzioni:

- Sfruttare le SandBox per carpire l'indirizzo del server bot
- Sfruttare le connessioni alle DarkNet, che per definizione sono dovute a traffico “cattivo”
- Sfruttare correlazioni temporali fra tentativi di connessione alla DarkNet, segnalazioni al CERT e analisi del traffico di un IP affetto da virus tramite nfsen
- Cercare cooperazione internazionale tramite policy comuni (v. ITU – Botnet Mitigation document)

Ricerche future

- Ulteriori evoluzioni delle minacce:
  - Tecniche di DNS Fast FluXing per nascondere l'ip di un server di BotNet
  - Tecniche antidebugging e offuscamento per eludere il funzionamento delle SandBox
  - Tecniche di riconoscimento e rilevamento HoneyPot (con relativo DoS punitivo)
  - Tecniche di riconoscimento e rilevamento di ambienti emulati, macchine virtuali
  - Tecniche di riconoscimento kernel hook (Sebek)

Per essere PRATICI

- Le minacce sono molto gravi e dannose
- Per mitigare questa situazione ci sentiamo di consigliarvi caldamente degli strumenti che per noi sono stati utili

nfsen e HoneyPot

APM & nfsen

- Monitoraggio picchi
- Monitoraggio anomalie di traffico
- Controllo del traffico
- Non ispeziona il payload del pacchetto (quindi non sniffa il traffico)

APM & HoneyPot

- Utilissime su rete locale:

  sia sulla LAN che dietro NAT

- Con opportuni script permette di **individuare macchine infettate** negative all'antivirus, senza intervento dell'utente
- Puo' permettere il **riconoscimento dell'IP** di una macchina infettata quando viene segnalato come "cattivo" l'ip del NAT
- Facilita' d'uso e scarsa manutenzione

APM & GARR-CERT

Il GARR-CERT e' disponibile e aperto
a fornire documentazione integrativa
materiale e supporto
a chi fosse interessato
a sviluppare soluzioni di questo tipo

cert@garr.it

...

domande?

Riferimenti

- Minacce
  - http://www.cert.org/archive/pdf/Botnets.pdf
  - http://www.clusif.asso.fr/fr/production/ouvrages/pdf/CyberCrime2006.pdf
- NetFlow - IPFIX
  - http://en.wikipedia.org/wiki/Netflow
  - http://www.rfc-archive.org/getrfc.php?rfc=3917
- nfsen & nfdump
  - http://nfdump.sourceforge.net
  - http://nfsen.sourceforge.net
- HoneyPot
  - http://www.fp6-noah.org/ - http://www.honeyathome.org/
  - http://nepenthes.mwcollect.org/
  - http://sandbox.norman.com/
- ITU Botnet Mitigation Document
  - http://www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html