

Network Tracing & Incident Response

Gestione degli incidenti e cooperazione per il
tracciamento a ritroso

Tracciamento a ritroso

- Analisi delle tracce digitali lasciate da un attacco per individuarne le reali origini
- Include:
 - Identificazione delle fonti (logs etc.)
 - Estrazione dati di interesse
 - Documentazione
 - interpretazione delle evidenze di



Tipi di Analisi

- Analisi “**post mortem**”
 - Studio a posteriori delle evidenze tempi differiti rispetto a quelli del’attacco
 - Evidenze storiche ottenute da logs o files di traccia (pacchetti catturati in precedenza)
- Analisi “**Live**”
 - Studio in tempo reale del traffico come fluisce attraverso la rete
 - Intercettazione telematica on-line

Complessità analisi

- Enorme quantità di “raw data”, cioè sequenze di pacchetti, o righe di log da analizzare
- Occorrono tool di analisi per interpretare i dati ad un livello di astrazione superiore



Analisi: Importanza Timeline

- Quasi tutte le evidenze individuabili in un log o in un packet trace hanno un timestamp
- Organizzare le evidenze collezionate in un database e poi ordinarle rispetto al tempo
- La cronologia è importante per il tracciamento e la correlazione degli eventi

Analisi: Problemi Timeline

- Teoricamente i riferimenti locali del tempo sono in relazione ad un clock di riferimento internazionalmente riconosciuto (NIST e U.S. Naval Observatory)
- Errori nella misura del tempo, ad es. clock drift
 - soprattutto se tempo non sincronizzato frequentemente
- Singola sorgente con tempo
 - tempo internamente consistente
- Sorgenti multiple con tempi
 - bisogna fare un merge delle cronologie
- Problemi anche per modifiche tempi manualmente oppure malware / intrusioni
- Analisi consistenza logica cronologia

Tracciamento a ritroso

- Validazione indirizzo sorgente
 - IP Locale, Intranet, Internet
- Esclusione indirizzi riservati, privati o improbabili

0.0.0.0/8
127.0.0.0/8
224.0.0.0/4
255.255.255.255/32

10.0.0.0/8
172.16.0.0/12
192.168.0.0/16/

1.2.3.4
5.6.7.8

24.24.24.24
23.23.23.23

- Esclusione blocchi riservati IANA

RESERVED-9	1.0.0.0 - 1.255.255.255
RESERVED-2	2.0.0.0 - 2.255.255.255
PDN	14.0.0.0 - 14.255.255.255
RESERVED-23	23.0.0.0 - 23.255.255.255
RESERVED-31	31.0.0.0 - 31.255.255.255
RESERVED-37	37.0.0.0 - 37.255.255.255
RESERVED-39A	39.0.0.0 - 39.255.255.255
RESERVED-41A	41.0.0.0 - 41.255.255.255
RESERVED-58	58.0.0.0 - 58.255.255.255
RESERVED-59	59.0.0.0 - 59.255.255.255
RESERVED-60	60.0.0.0 - 60.255.255.255
RESERVED-7	69.0.0.0 - 79.255.255.255
RESERVED-11	82.0.0.0 - 95.255.255.255
RESERVED-8	96.0.0.0 - 126.255.255.255

RESERVED-3	128.0.0.0 - 128.0.255.255
BLACKHOLE.ISI.EDU	128.9.64.26
TEST-B	128.66.0.0 - 128.66.255.255
LINKLOCAL	169.254.0.0 - 169.254.255.255
RESERVED	191.255.0.0 - 191.255.255.255
RESERVED-192	192.0.0.0 - 192.0.127.255
ROOT-NS-LAB	192.0.0.0 - 192.0.0.255
NET-ROOTS-NS-LIVE	192.0.1.0 - 192.0.1.255
NET-TEST	192.0.2.0 - 192.0.2.255
RESERVED-2A	192.0.128.0 - 192.0.255.255
RESERVED-2-A	192.0.128.0 - 192.0.255.255
IANA-192	192.88.99.0 - 192.88.99.255
RESERVED-13	197.0.0.0 - 197.255.255.255
RESERVED-14	201.0.0.0 - 201.255.255.255
RESERVED	221.0.0.0 - 223.255.255.255

Tracciamento a ritroso

- Validazione hop count
 - Step 1: Determina l'hop count "implicato" dai pacchetti ricevuti.
Original packet TTL - Final TTL (alla ricezione)
 - Step 2: effettua un Traceroute verso l'IP di interesse ottenendo un valore "attuale" dell' hop count.
 - Step 3: Se questo valore differisce sostanzialmente da quello "implicato", **l'IP potrebbe essere oggetto di "spoofing"**

OS Version	tcp_ttl	udp_ttl
AIX	60	30
FreeBSD 2.1R	64	64
HP/UX 9.0x	30	30
HP/UX10.01	64	64
Irix 5.3	60	60
Irix 6.x	60	60
Linux	64	64
MacOS/MacTCP 2.0.x	60	60
OS/2 TCP/IP 3.0	64	64
OSF/1 V3.2A	60	30
Solaris 2.x	255	255
SunOS 4.1.3/4.1.4	60	60
MS Windows 95	32	32
MS Windows NT 3.51	32	32
MS Windows NT 4.0	128	128

Problema: Traceroute filtrato!

Type escape sequence to abort.

Tracing the route to forthelife.net (216.144.196.7)

```
1 63.237.160.113 8 ms 12 ms 8 ms
2 lax-core-01.inet.qwest.net (205.171.19.149) 8 ms 8 ms 8 ms
3 sjo-core-03.inet.qwest.net (205.171.5.155) 16 ms 16 ms 16 ms
4 sjo-core-01.inet.qwest.net (205.171.22.10) 16 ms 16 ms 16 ms
5 sfo-core-02.inet.qwest.net (205.171.5.131) 20 ms 48 ms 16 ms
6 chi-core-01.inet.qwest.net (205.171.5.42) 72 ms 64 ms 68 ms
7 chi-core-03.inet.qwest.net (205.171.20.174) 64 ms 64 ms 76 ms
8 chi-edge-17.inet.qwest.net (205.171.20.154) 64 ms 64 ms 68 ms
9 63.149.1.70 80 ms 84 ms 84 ms
10 10.60.1.9 80 ms * 80 ms
11 172.16.250.1 96 ms 84 ms 88 ms
12 * * *
13 * * *
```


Tracciamento a ritroso

- Validazione routes
 - Determinare se esiste una route valida di accesso al netblock relativo all'indirizzo IP da tracciare
 - E' possibile a tale scopo utilizzare un looking glass che permette di visualizzare la routing table di un router di core
 - <http://lg.above.net/>
 - http://nitrous.digex.net/cgi-bin/looking_glass.pl
 - <http://www.merit.edu/~ipma/tools/lookingglass.html>



MAE-West Looking Glass Results

Query: bgp
Addr: 182.1.1.2

% Network not in table

© 2002 Allegiance Internet
an [Allegiance Telecom, Inc. Company](#)
[Legal Notice](#)

Route Views Looking Glass

```
$ telnet route-views.routeviews.org
Trying 128.223.51.103...
Connected to route-views.routeviews.org.
Escape character is '^]'.
. . . . .
route-views>sh ip bgp 182.1.1.2
BGP routing table entry for 182.1.0.0/20, version 14302702
Paths: (41 available, best #41, table default)
  Not advertised to any peer
  Refresh Epoch 1
  6453 7713 23693
    66.110.0.86 from 66.110.0.86 (66.110.0.86)
      Origin IGP, localpref 100, valid, external
      rx pathid: 0, tx pathid: 0
```

Tracciamento a ritroso

- Verifica a ritroso Dominio associato all'IP
 - Una operazione di reverse resolution può fornire informazioni relative al dominio associato all'IP e a eventuali contatti

```
$ nslookup
> set type=ptr
> 26.22.209.24.in-addr.arpa
Server:  huey.cbeyond.net
Address:  64.213.152.18

Non-authoritative answer:
26.22.209.24.in-addr.arpa
name = dhcp024-209-022-026.cinci.rr.com

> set type=soa
> 26.22.209.24.in-addr.arpa
Server:  huey.cbeyond.net
Address:  64.213.152.18

*** No start of authority (SOA) records available for
26.22.209.24.in-addr.arpa
> 22.209.24.in-addr.arpa
Server:  huey.cbeyond.net
Address:  64.213.152.18

Non-authoritative answer:
22.209.24.in-addr.arpa
primary name server = ns1.columbus.rr.com
responsible mail addr = noc.columbus.rr.com
serial = 2000120401
refresh = 3600 (1 hour)
retry = 900 (15 mins)
expire = 604800 (7 days)
default TTL = 3880 (1 hour 4 mins 40 secs)
```

Tracciamento a ritroso

- Verifica mail relay associato al dominio
 - Via nslookup è possibile individuare il mail relay per un dominio, e verificare manualmente l'attendibilità dello stesso.
 - In caso di impossibilità di verifica è possibile ricorrere a <http://whois.abuse.net>

NETWORK ABUSE CLEARINGHOUSE

Look up an address in the abuse.net contact database

Database updated July 5, 2002 18:15, current size 107666 entries.

Enter the name of the domain that you would like to check, such as `example.com`.

 [Look up another domain](#)

 [Return to the abuse.net home page.](#)

This page updated: 04/03/2002

© 1999-2001 I.E.C.C.

```
$ nslookup
> set type=mx
> columbus.rr.com
Server: 192.168.1.1
Address: 192.168.1.1#53
```

Non-authoritative answer:

columbus.rr.com mail exchanger = 20 cdptpa-pub-iedge-vip.email.rr.com.

```
$ telnet cdptpa-pub-iedge-vip.email.rr.com 25
Trying 107.14.166.70...
Connected to cdptpa-pub-iedge-vip.email.rr.com.
Escape character is '^]'.
554 ERROR: Mail Refused - See
http://www.spamhaus.org/query/bl?ip=80.180.203.63
Connection closed by foreign host.
```

Tracciamento a ritroso

- Verifica su regional registries (RR)
 - Una operazione di consultazione dei DB di assegnazione sui RR ci può fornire informazioni su localizzazione e contatti
 - Il dominio associato all'e-mail del contact point ci può fornire informazioni sul possessore o responsabile del netblock
 - Il dominio associato all'e-mail del contact point ci può fornire informazioni sul possessore o responsabile del netblock

```
$ whois 182.1.1.2
. . .
NetRange:      182.0.0.0 - 182.255.255.255
CIDR:          182.0.0.0/8
NetName:       APNIC-182
NetHandle:     NET-182-0-0-0-0
Parent:        ()
NetType:       Allocated to APNIC
OriginAS:
Organization:  Asia Pacific Network Information Centre
               (APNIC)
RegDate:       2009-08-03
Updated:       2010-07-30
Ref:           https://whois.arin.net/rest/net/NET-
               182-0-0-0-0
. . .

% Information related to '182.1.0.0/16 AS23693'

route:         182.1.0.0/16
descr:         Route Object of PT Telekomunikasi
               Selular Indonesia
descr:         ISP
descr:         Jakarta
origin:        AS23693
mnt-by:        MAINT-ID-TELKOMSEL
changed:       hostmaster@idnic.net 20100924
source:        APNIC
```

Whois Query Syntax

Per cercare solo specifici **TIPI** di record si può usare la keyword:

Host
ASn
Person
ORganization
NEtwork
GRoup

Per cercare solo uno specifico **CAMPO**, si può usare la keyword o il carattere:

Handle or **!"**
Mailbox or contains **"@"**
Name or leading **."**

Alcuni esempi di keywords:

EXP and or "*"	Tutte le info associate alla richiesta
F ull or "="	Info dettagliate per ogni match
P artial or trailing ."	Match su targets che cominciano con una stringa
Q , QUIT , or R eturn	Exits Whois
SUB display or "%"	Mostra info relative a utenti di host, hosts di reti, etc.
SUM mary or "\$"	Solo summary, anche in presenza di match

Tracciamento a ritroso

- Verifica su regional registries (RR)
 - È anche possibile ottenere informazioni circa l'istadamento dei prefissi e le relative politiche

Click Network/Local Access (NETBLK-GBX-REQ000000014080)

1111 Altheimer Street South
Tacoma, WA 98402
US

Netname: GBX-REQ000000014080
Netblock: 208.51.248.0 - 208.51.251.255

Coordinator:

Global Crossing (IA12-ORG-ARIN)
ipadmin@gblix.net
+1 800 404-7714

Record last updated on 29-Nov-2001.

Database last updated on 28-Apr-2002 19:58:33 EDT.

The ARIN Registration Services Host contains ONLY
Internet

Network Information: Networks, ASN's, and related
POC's.

Please use the whois server at rs.internic.net for
DOMAIN related

Information and whois.nic.mil for NIPRNET Information.

% ARIN Internet Routing Registry Whois Interface

route: 208.51.251.0/24
descr: Customer Local Access
origin: AS20394
notify: hostmaster@click-network.com
mnt-by: MAINT-AS14677
changed: sroberts@click-network.com
20020110
source: RADB

route: 208.48.0.0/14
descr: GBLX-US-AGGREGATE
origin: AS3549
mnt-by: GBLX-RIPE-MNT
changed: dcooper@globalcenter.net 19991229
source: RIPE

Tracciamento a ritroso

- RWhois (Referral Whois)
 - estende e migliora Whois in una logica gerarchica e scalabile
 - mira alla distribuzione dei "network objects", o dei dati che rappresentano risorse Internet resources e persone associate
 - Si avvale della natura inerentemente gerarchica di questi network objects (domain names, IP networks, email addresses) per ricercare e fornire in maniera più accurata queste informazioni

Rwhois server data:

```
%rwhois V-1.5:001ab7:00 rwhois.exodus.net (Exodus Communications)
network:Class-Name:network
network:Auth-Area:0.0.0.0/0
network:Network-Name:216.34.168.128
network:IP-Network:216.34.168.128/26
network:Organization;I:Pixel Magic Imaging
network:Name;I:Alfred Grant Lewis
network:Email;I:glewis@pmimaging.com
network:Street;I:631 Mill Street
network:City;I:San Marcos
network:State;I:TX
network:Postal-Code;I:78666
network:Country-Code;I:USA
```

```
network:Class-Name:network
network:Auth-Area:0.0.0.0/0
network:Network-Name:216.34.160.0
network:IP-Network:216.34.160.0/20
network:Organization;I:Exodus IDC - AU/AU1
network:Name;I:Exodus IP Address Administrator
network:Email;I:ipaddressadmin@exodus.net
network:Street;I:1418 Park Center Drive
Building 1
network:City;I:Austin
network:State;I:TX
network:Postal-Code;I:78753
network:Country-Code;I:USA
```

```
network:Class-Name:network
network:Auth-Area:0.0.0.0/0
network:Network-Name:216.32.0.0
network:IP-Network:216.32.0.0/14
network:Organization;I:Exodus Communications (Exodus Legacy)
network:Name;I:Exodus Hostmaster
network:Phone;I:888-239-6387
network:Email;I:ipaddressadmin@exodus.net
network:Street;I:2831 Mission College Boulevard
network:City;I:Santa Clara
```

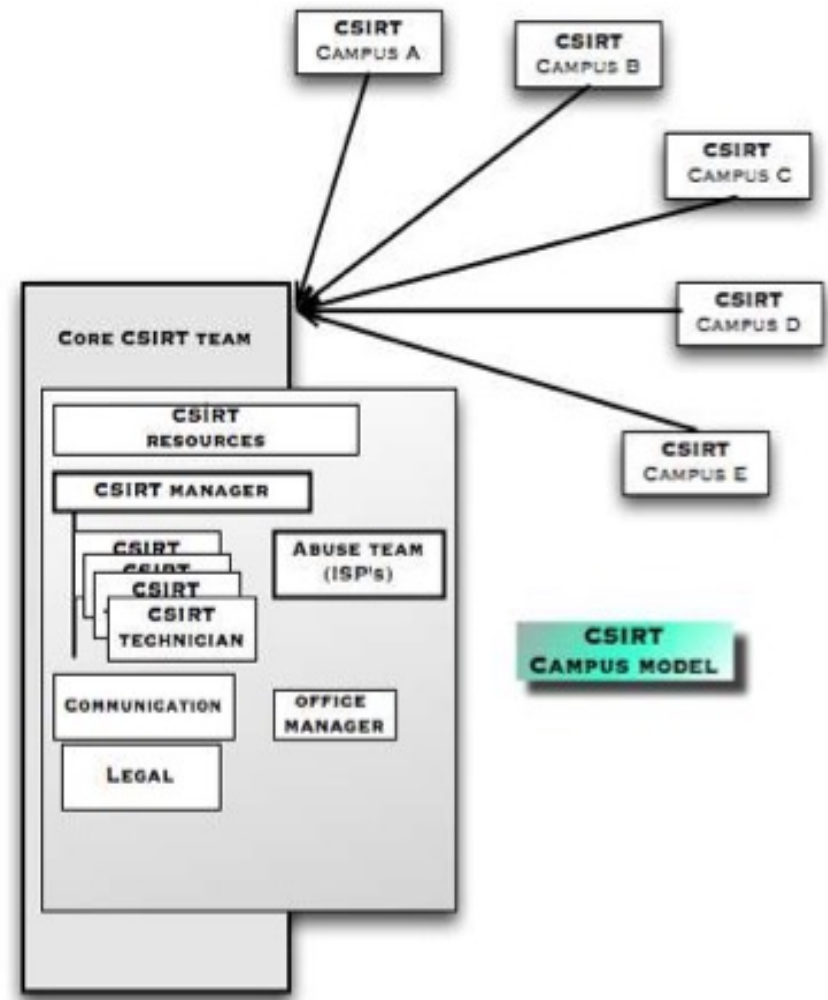
La catena di cooperazione:CSIRT

- CSIRT (Computer Security Incident Response Team) e' sinonimo di CERT (termine coniato e registrato negli USA)
- *Gruppo di esperti di sicurezza IT che ha come compito quello di reagire in caso di incidente di sicurezza, al fine di limitarne le conseguenze e assistere gli utenti nel recupero delle funzionalita' e gli amministratori nel ripristino dei sistemi*



Modello di CSIRT

- Tutte le organizzazioni di medio grandi dimensioni che si collegano in rete dovrebbero avere uno CSIRT ed un responsabile della sicurezza.
- Lo CSIRT deve:
 - Coordinare le attività di IR e fornire supporto ai vari siti/unità
 - Gestire eventuali strumenti centralizzati
 - Interagire con l'operation management degli ISP
 - Interagire con altri CSIRT e contribuire alle attività coordinate



Non solo Emergenze....

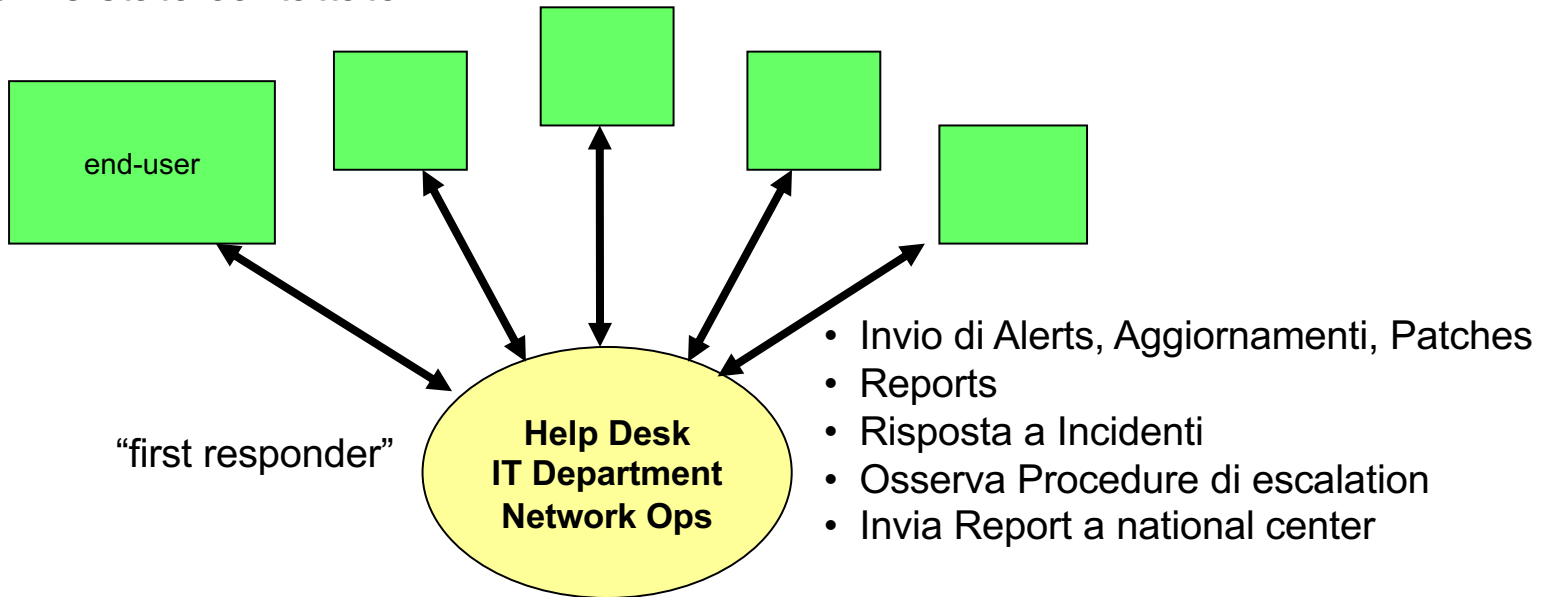
- Col tempo, gli CSIRT hanno progressivamente assunto connotati di *Security Service Providers*, includendo attività' come:
 - Security Advisory
 - Sviluppo/divulgazione di tools di sicurezza
 - Training
 - Monitoring/Auditing
 - Analisi del rischio
 -

Esigenze

- Sulla base dell'esperienza maturata negli anni:
 - Le problematiche di sicurezza sono (o possono rapidamente diventare) GLOBALI
 - In presenza di molti siti di dimensione piccola/medio piccola → gestione piu' onerosa
 - Esperienza, effort e sensibilita' alle questioni di sicurezza molto variabile tra i siti
 - Molto utile (necessaria) un'attivita' di monitoring
 - Molto utile (necessaria) un'attivita' di auditing (challenges)
 - Cruciale la comunicazione, la divulgazione delle procedure di IR e l'interazione con gli altri CSIRT

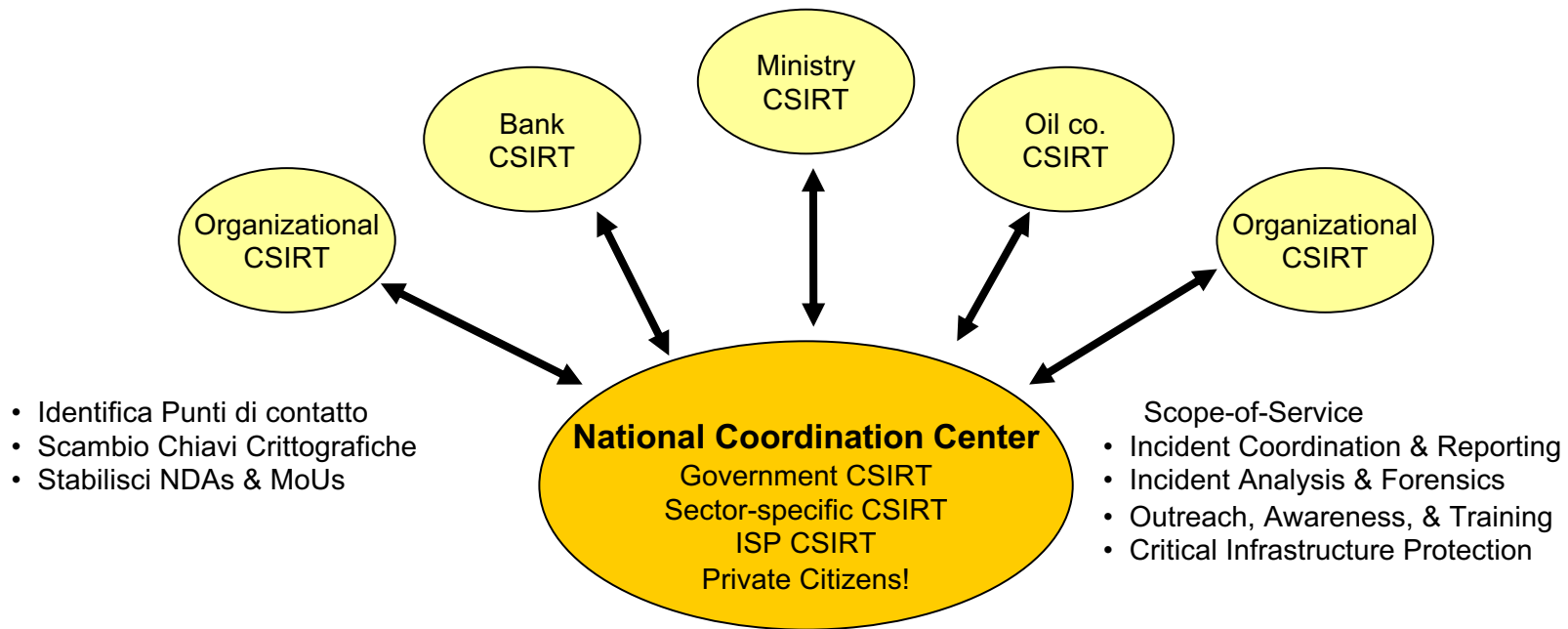
Risposta “Front-Line”

Chi è stato contattato?



- I contatti vanno gestiti in logica gerarchica a partire dal proprio punto di contatto
- Unico elemento deputato a negoziare con i propri utenti per la gestione di incidenti, aggiornamenti etc.
- Segnalazioni fuori schema non vanno accettate

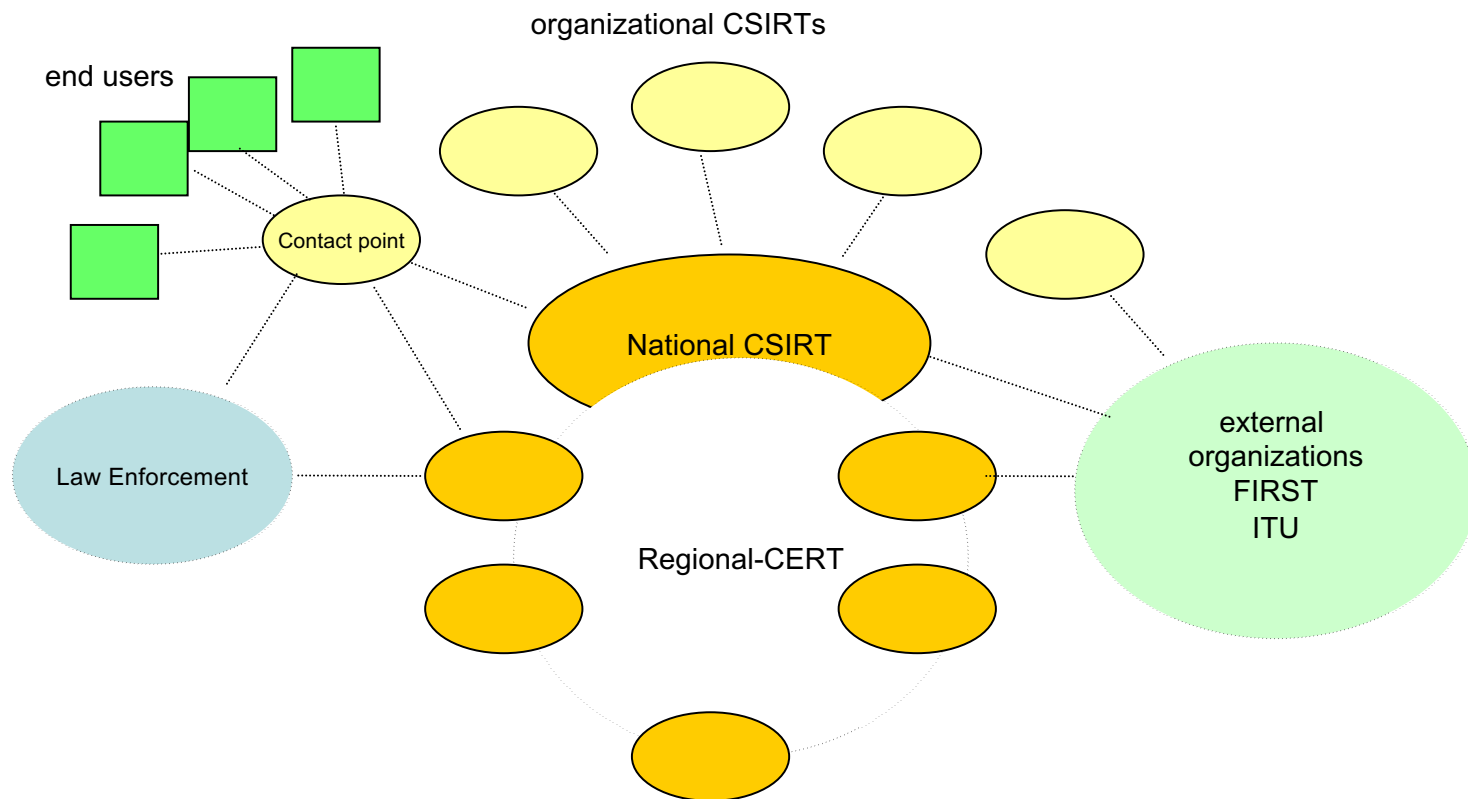
CSIRT Nazionale



The National Cyber-Security Network

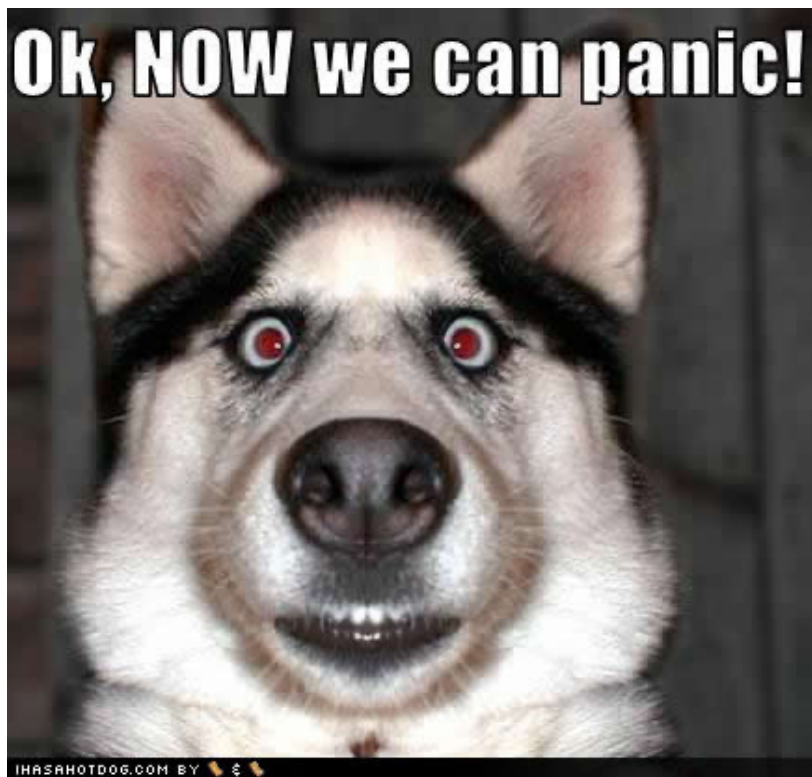
- Per garantire la fiducia reciproca le comunicazioni e-mail fra CERT andrebbero firmate con chiavi private (tipicamente PGP o X509) e verificate con chiavi pubbliche precedentemente scambiate o disponibili su repository ufficiali
- Accordi formali di cooperazione (MoU) e di non disclosure su dati di indagine (NDA)
- Scambio di informazioni su analisi e forensics
- Addestramento e aggiornamento

Cyber Security Network



- A ciascun livello gerarchico le varie organizzazioni possono avere contatti con il proprio CSIRT di riferimento e con gli organismi di Law Enforcement
- La gerarchia va seguita nella logica della cooperazione e del tracciamento

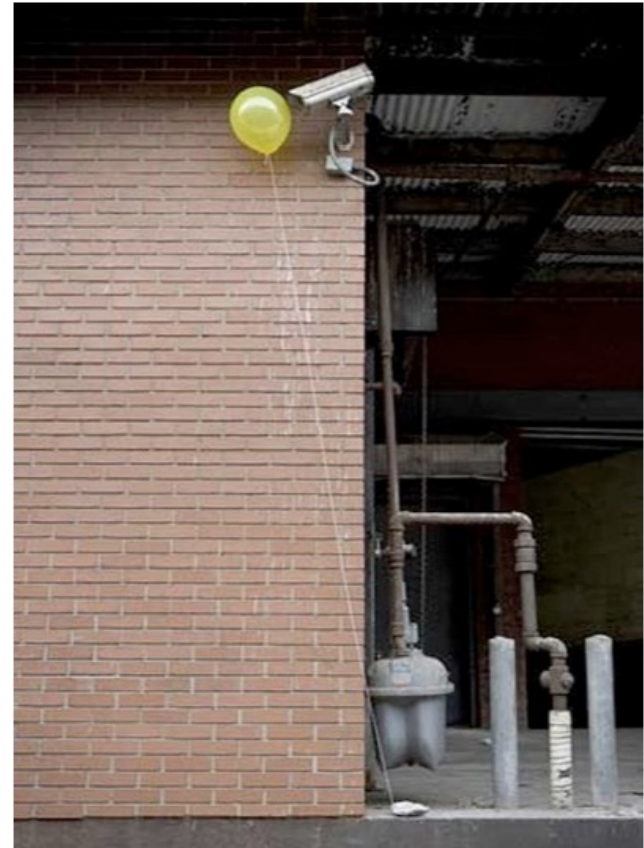
Incident Response



- Coordinamento delle azioni e verifica che le procedure di IR vengano seguite
- Punto di contatto con gli ISP e gli altri CSIRT
- Supporto per:
 - Contenere i problemi
 - Analizzare gli incidenti
 - Ripristinare i servizi

Monitoring/Auditing

- L'esperienza ha mostrato che e' fondamentale avere uno strumento che:
 - Informi sullo stato di aggiornamento dei sistemi
 - Permetta di realizzare un monitoraggio centrale dei siti
 - Il tipo e livello di monitoraggio va concordato con i siti coinvolti
- SSC (Security Service Challenges) e campagne di auditing per verificare le procedure, i canali di comunicazione e la prontezza di risposta dei siti
 - Modi, tempi e finalita' dei challenges sono definiti separatamente per i vari siti.



Training

- Mantenimento di pagine web dedicate
- Organizzazione di tutorial e corsi
 - Best practices
 - Tools utili
 - Forensic
 - Middleware security
 - Cosa fare per aumentare la sicurezza e....

... cosa NON fare per preservarla



Security Advisory



- Segnalare le vulnerabilita' a livello di
 - Sistema operativo
 - Middleware
 - Applicativi
- Fonti:
 - Vendors
 - CERT_CC
 - Altri CSIRT
 - Siti specializzati
- Sottile distinzione tra vulnerabilita' locali e remote.
- Atteggiamento attivo: non solo segnalazioni
 - Follow up sui siti nei casi piu' importanti

... Senza esagerazioni ed inutili allarmismi

CERT/CC

www.cert.org

- CERT non è un acronimo, ma un marchio di Carnegie Mellon University
- Il CERT Coordination Center è stato il primo *computer incident response team*, fondato dal DARPA nel 1988, ora una spin-off di CMU

CERT/CC

Come gestire un incidente

- cosa fare, chi contattare, cosa comunicare
- come fare *vulnerability reports*

Come ottenere informazioni sulla sicurezza

- Attività correnti, *advisories*, incidenti, vulnerabilità, sommari, CVE
- mailing list
- fonti di informazione

CERT Security Improvement Modules

Security Practices & evaluation

→ Security Improvement Modules

- Sono piccoli trattati sulla sicurezza che indirizzano uno specifico problema. Ogni modulo contiene una serie di *practices* e di *implementations*.
- La *practice* descrive le problematiche da affrontare per risolvere uno specifico problema di sicurezza.
- La *implementation* descrive le attività da fare come descritto nella *practice*.

CERT Security Improvement Modules

Security Practices & evaluation

→ Security Improvement Modules

→ Modulo 2: “Securing Desktop Workstations”

- Terminologia
- Chi deve leggere il modulo
- Che cosa viene coperto e cosa no
- Quali aspetti di sicurezza sono contemplati
- Approccio di miglioramento in 4 parti
- *Recommended practices.*

SANS

www.sans.org

- SysAdmin, Audit, Network, Security institute
- La più grande fonte per la sicurezza informatica.
- Raccoglie, sviluppa e rende disponibili documenti relativi.
- Certificazioni.
- @RISK (Weekly Vulnerability Digest)
- Internet Storm Center (Early Warning System)

SANS

Da vedere:

- Calendario dei corsi e delle conferenze
- Reading Room
- Internet Storm Center
- Newsletters (Computer Security News)
- Webcasts
- Security Policy Project
- Top 20 List

GIAC

Global Information Assurance Certification

- SANS emette certificazioni per i professionisti della sicurezza.
 - Livelli base: *Information Security Officer, Security Essential*
 - Specializzazioni: *Audit, Intrusion Detection, Incident Handling, Firewalls and Perimeter Protection, Forensics, Hacker Techniques, Windows and Unix Operating System Security*

SANS Internet Storm Center

- *"On March 22, 2001, intrusion detection sensors around the globe logged an increase in the number of probes to port 53 [...]"*
 - Il 22/3/2001 migliaia di siti che non avevano aggiornato il loro software BIND si accorsero di essere stati infettati da *Lion*.
 - Questi eventi diedero inizio al progetto che oggi è l'Internet Storm Center

SANS Internet Storm Center

Funziona come un servizio meteorologico:

- Sensori mandano periodicamente i log di IDS e FW a centri di coordinamento locali (SACCs)
- I SACCs calcolano le liste (*top 10 attacks* e *top 10 attackers*) e informano i Provider locali sui dettagli; tutti i dati vengono infine inviati a ISC
- ISC consolida tutti i dati che riceve, fornisce alla comunità allarmi tempestivi sui nuovi attacchi e genera *report* globali.

SANS

Consensus Security Vulnerability Alert

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

It has been a tough week dealing with viruses and worms, but a quiet one for new vulnerabilities. No new vulnerabilities were discovered this week in widely used software.

Alan

@RISK: The Consensus Security Vulnerability Alert

January 29, 2004

Vol. 3. Week 4

@RISK is the SANS community's consensus bulletin summarizing the most important vulnerabilities and exploits identified during the past week and providing guidance on appropriate actions to protect your systems (PART I). It also includes a comprehensive list of all new vulnerabilities discovered in the past week (PART II).

SANS Consensus Security Vulnerability Alert

Summary of the vulnerabilities reported this week

Category	- # of Updates & Vulnerabilities (Found in Part I or Part II)
----------	--

Windows	- 1 (Parts I and II)
Other Microsoft Products	- 1 (Part II)
Third Party Windows Apps	- 16 (Parts I and II)
Mac OS	- 1 (Part II)
Unix	- 1 (Part II)
Novell	- 3 (Part II)
Cross Platform	- 11 (Parts I and II)
Web Application	- 10 (Parts I and II)
Network Device	- 1 (Part II)

Part I Critical Vulnerabilities

Part I is compiled by the security team at TippingPoint (www.tippingpoint.com) as a by-product of that company's continuous effort to ensure that its intrusion prevention products effectively block exploits using known vulnerabilities. TippingPoint's analysis is complemented by input from a council of security managers from twelve large organizations who confidentially share with SANS the specific actions they have taken to protect their systems. A detailed description on the process may be found at <http://www.sans.org/newsletters/cva/#process>
Archives at <http://www.sans.org/newsletters/Table of Contents>

SANS Consensus Security Vulnerability Alert

Contents of Part I

Other Software

- (1) HIGH: Gallery Remote File Include Vulnerability
- (2) HIGH: [PHPix Remote Command Execution](#)
- (3) MODERATE: DUware Multiple Products Administrative Access
- (4) MODERATE: QuadComm Q-Shop Multiple SQL Injection Vulnerabilities
- (5) MODERATE: Gaim Client Multiple Buffer Overflow Vulnerabilities
- (6) LOW: RhinoSoft Serv-U FTP Server "SITE CHMOD" Command Overflow
- (7) LOW: McAfee ePolicy Orchestrator Agent HTTP POST Handling Flaw

Updates

- (8) [Windows XP Malicious Folder Code Execution](#)
- (9) Multiple Vendor H.323 Protocol Implementation Vulnerabilities

***** SPONSORED LINKS *****

-
-
-

SANS Consensus Security Vulnerability Alert

Esempio

(2) HIGH: PHPix Remote Command Execution
Affected: PHPix 2.0.3 and possibly prior

Description: PHPix is a web photo management software. It is reported that the user-supplied values passed to parameters such as "dispsize", "album" and "pic" used by PHPix script(s) are not sanitized. This flaw can be exploited by an attacker to execute arbitrary commands on the server running PHPix, with HTTP daemon privileges. The posted advisory shows how to craft the malicious requests to exploit the flaw.

Status: Unconfirmed by vendor, no fix available.

Council Site Actions: The affected software is not in production or widespread use at any of the council sites. They reported that no action was necessary.

References:

Project Homepage

<http://sourceforge.net/projects/phpix>

SecurityTracker Posting

<http://www.securitytracker.com/alerts/2004/Jan/1008782.html>

SecurityFocus BID

<http://www.securityfocus.com/bid/9458>

SANS Consensus Security Vulnerability Alert

Esempio

(8) Windows XP Explorer Folder Code Execution

A specially crafted folder on a Windows XP machine can lead to arbitrary code execution when the folder contents are viewed by an unsuspecting user. This is essentially a rehash of a previously reported issue "Self-Executing HTML" for a file with a ".Folder" extension.

Council Site Actions: None of the reporting council sites plan to change their original course of action based on the new information.

References:

Posting by http-equiv@excite.com

<http://archives.neohapsis.com/archives/ntbugtraq/2004-q1/0028.html>

Follow-up posting by Thor Larholm

<http://archives.neohapsis.com/archives/bugtraq/2004-01/0275.html>

Previous @RISK Newsletter Posting

http://www.sans.org/newsletters/risk/vol3_1.php (Item #2)

Secunia Advisory

<http://www.secunia.com/advisories/10708>

SANS Consensus Security Vulnerability Alert

PART II

Weekly Comprehensive List of Newly Discovered Vulnerabilities - Week 4 2004

This list is compiled by Qualys (www.qualys.com) as part of that company's ongoing effort to ensure its vulnerability management web service tests for all known vulnerabilities that can be scanned. As of this week Qualys scans for 3202 unique vulnerabilities. For this special SANS community listing, Qualys also includes vulnerabilities that can not be scanned remotely.

Summary of Updates and Vulnerabilities in this Consensus Platform	Number of Updates and Vulnerabilities
---	---------------------------------------

Windows	1
Other Microsoft Products	1
Third Party Windows Apps	16
Mac Os	1
Unix	1
Novell	3
Cross Platform	11
Web Application	10
Network Device	1

SANS Consensus Security Vulnerability Alert

- 04.4.1 - Windows - Microsoft Windows File Sharing Resource Exhaustion
- 04.4.2 - Other Microsoft Products - Microsoft Internet Explorer File Extension Misrepresentation
- 04.4.3 - Third Party Windows Apps - Need For Speed Game Client Remote Buffer Overflow
- 04.4.4 - Third Party Windows Apps - AIPTEK NETCam Webserver Directory Traversal
- 04.4.5 - Third Party Windows Apps - Anteco Visual Technologies OwnServer Directory Traversal
- 04.4.6 - Third Party Windows Apps - Darkwet WebcamXP Cross-Site Scripting
- 04.4.7 - Third Party Windows Apps - Cisco Voice Product IBM Director Agent Unauthorized Access Vu
- 04.4.8 - Third Party Windows Apps - Cisco Voice Product IBM Director Denial Of Service Vulnerabil
- 04.4.9 - Third Party Windows Apps - Netbus Directory Listings Disclosure and File Upload Vulnerab
- 04.4.10 - Third Party Windows Apps - McAfee ePolicy Orchestrator Agent Buffer Overflow Vulnerabi
- 04.4.11 - Third Party Windows Apps - Serv-U FTP Server MDTM Command Stack Overflow
- 04.4.12 - Third Party Windows Apps - TinyServer Directory Traversal
- 04.4.13 - Third Party Windows Apps - Borland Webserver for Corel Paradox Directory Traversal
- 04.4.14 - Third Party Windows Apps - Herberlin BremsServer Cross-Site Scripting
- 04.4.15 - Third Party Windows Apps - Herberlin BremsServer Directory Traversal Vulnerability
- 04.4.16 - Third Party Windows Apps - ProxyNow! Multiple Overflow Vulnerabilities
- 04.4.17 - Third Party Windows Apps - Tinyserver Denial Of Service
- 04.4.18 - Third Party Windows Apps - Tinyserver Cross Site Scripting
- 04.4.19 - Mac Os - Apple Security Update 2004-01-26
- 04.4.20 - Unix - Cherokee Error Page Cross Site Scripting Vulnerability
- 04.4.21 - Novell - Novell Netware Enterprise Web Server Multiple Cross Site Scripting
- 04.4.22 - Novell - Novell Groupwise Cross Site Scripting Vulnerability
- 04.4.23 - Novell - Novell Netware Enterprise HTTP Upload Vulnerability
- 04.4.24 - Cross Platform - JDBC Database Insecure Default Policy
- 04.4.25 - Cross Platform - Reptile Web Server Remote Denial Of Service
- 04.4.26 - Cross Platform - Mephistoles Cross-Site Scripting Vulnerability
- 04.4.27 - Cross Platform - Liquid War Multiple Buffer Overflow Vulnerabilities
- 04.4.28 - Cross Platform - thttpd CGI Test Script Cross-Site Scripting
- 04.4.29 - Cross Platform - Oracle HTTP Server 'isqlplus' Cross-Site Scripting
- 04.4.30 - Cross Platform - Gaim Multiple Buffer Overflows
- 04.4.31 - Cross Platform - AppWeb HTTP Server Request Denial Of Service
- 04.4.32 - Cross Platform - BEA WebLogic SSL Client Privilege Leakage
- 04.4.33 - Cross Platform - BEA WebLogic HTTP TRACE Method
- 04.4.34 - Cross Platform - Finjan SurfinGate FHTTP Restart Command Execution

SANS Consensus Security Vulnerability Alert

- 04.4.35 - Web Application - Q-Shop Cross Site Scripting
 - 04.4.36 - Web Application - Q-Shop SQL Injection Vulnerabilities
 - 04.4.37 - Web Application - Invision Power Board Index.php Cross-Site Scripting
 - 04.4.38 - Web Application - PHPix Arbitrary Command Execution Vulnerability
 - 04.4.39 - Web Application - TBE Banner Engine Script Execution Vulnerability
 - 04.4.40 - Web Application - IBM Net.Data Cross-Site Scripting
 - 04.4.41 - Web Application - Gallery 'GALLERY_BASEDIR' PHP Include Vulnerability
 - 04.4.42 - Web Application - Xoops Cross-Site Scripting Vulnerability
 - 04.4.43 - Web Application - Kietu Index.PHP Remote File Inclusion Vulnerability
 - 04.4.44 - Web Application - Web Blog Arbitrary File Access Vulnerability
 - 04.4.45 - Network Device - 2Wire HomePortal Arbitrary File Access
-

IHR

www.internetpulse.net

- The Internet Health Report
- Matrice di indicatori di performance (latenza di rete) fra i principali Internet Backbone statunitensi.

CIS

www.cisecurity.org

- Aiuta le organizzazioni a gestire i rischi legati alla sicurezza informatica.
- Fornisce metodologie e *tool* per misurare e migliorare lo stato dei sistemi connessi a Internet.
- Pubblica benchmarks per la verifica di configurazioni di sicurezza di molti sistemi.
 - *Prudent level of due care*
 - *Best-practice configurations*

Securityfocus

www.securityfocus.com

- E' una comunità di professionisti della sicurezza.
- Si rivolge a tutti i profili coinvolti: utenti, hobbisti, amministratori, manager.
 - BugTraq
 - Vulnerability database (bid)
 - Letteratura (Adv., Vulns., Infocus)

Altre risorse

- Zeusnews
- Sophos
- Trendmicro

... voi quali fonti di informazioni conoscete?

- Naturalmente vi sono i siti web, le knowledgebase e le mailing lists dei siti specifici dei prodotti