Status report från SUNet CERT jan–mar 2004

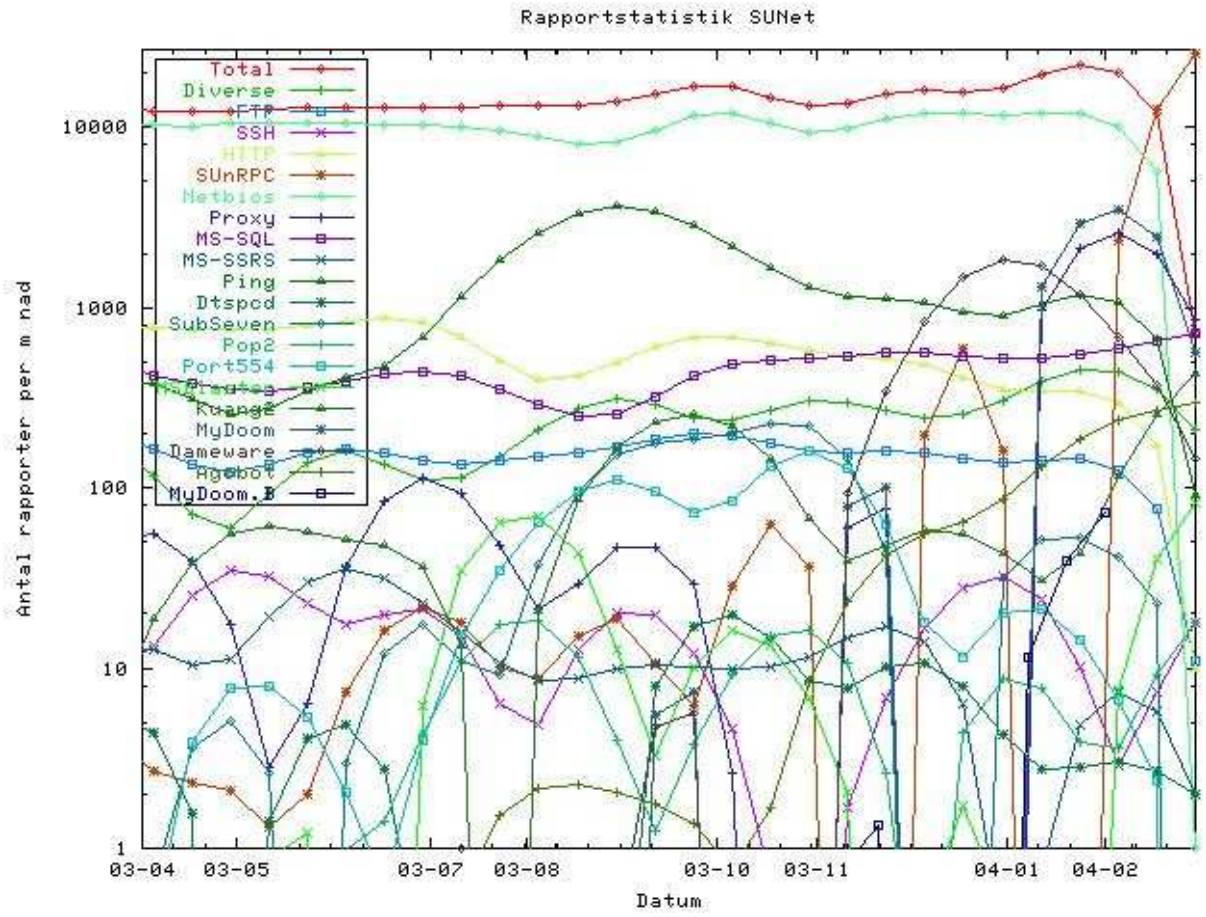
Hanterade incidents 2004 (jan–mar)

Incident type	in	out	inside	outside	undef	Sum
other					7	7
attack		2				2
backorifice–scan		1				1
copyright		2		1		3
dcom–scan		1				1
ddos		2				2
dos	1	3		2		6
ftp–attack		1				1
ftp–scan		3				3
info	5		1			6
intrusion	1			1		2
irc–bot		1				1
mssql–scan		2				2
netbios–scan		13				13
portscan		9				9
query	2					2
radmin–scan		6				6
spam		46		93		139
spam–relay		5		4		9
ssh–scan		6				6
subseven–scan		1				1
virus		11		3		14
virus–dcom		11	1			12
virus–mssql		7				7
virus–mydoom		4				4
virus–sinit		1				1
web–attack				1		1
web–scan		1		2		3

Incidenter 2004 per univ/hsk:

Univ/etc	Count
bth	2
fhsk	1
gu	9
hb	3
hgo	15
hh	5
hhs	2
hig	3
hik	2
his	1
hj	1
ks	1
kth	25
lhs	1
liu	1
lu	3
luth	3
mah	1
mdh	9
mh	8
oru	1
riksutstallningar	2
sh	3
sjohistoriska	1
slu	1
su	1
sunet	9
umu	4
uu	4
vxu	19

Rapporter (för information:)



.

Säkerhetsmeddelanden:

När	Vad	OS
040105	Linux kernel (mremap)	linux
040206	FreeBSD, NetBSD och OpenBSD	*bsd
040218	Linux kernel	linux
040219	Zone Alarm	WinXX
040317	OpenSSL	
040320	Witty −black ice defender−worm	WinXX

Via cert−kontakt−listan:

40127	MyDoom
040128	MyDoom.B
040303	beagle.J
040310	Outlook (mm)
040329	Cisco

Cert−diskussion list är flitigt använd.

Aktuellt problem: Phatbot

Nationellt samarbete:

Deltagit i Svenska Certforum−mötet nr 4

Internationellt dito:

Deltagit i TF−CSIRT mötet i Madrid, 15−16:e jan. 'Ackrediterad' status (som TeliaCERT).

RTIR programmeringskurs i anslutning till TF−CSIRT.

Eftersom ECSIRT projektet har upphört och migrerat in i TF−CSIRT så har vi fått möjlighet att prova att delta i dess datainsamlings/early−warning−verksamhet.

FIRST: nästa möte i juni, epostlistan dock rätt aktiv.

Aktiviteter

Träff för småhögskolor i Stockholm 2:a mars.

RTIR−träff i Uppsala 16:e mars.

I övrigt förberedande forensics−kursen i Uppsala efter susec (21−22 april).