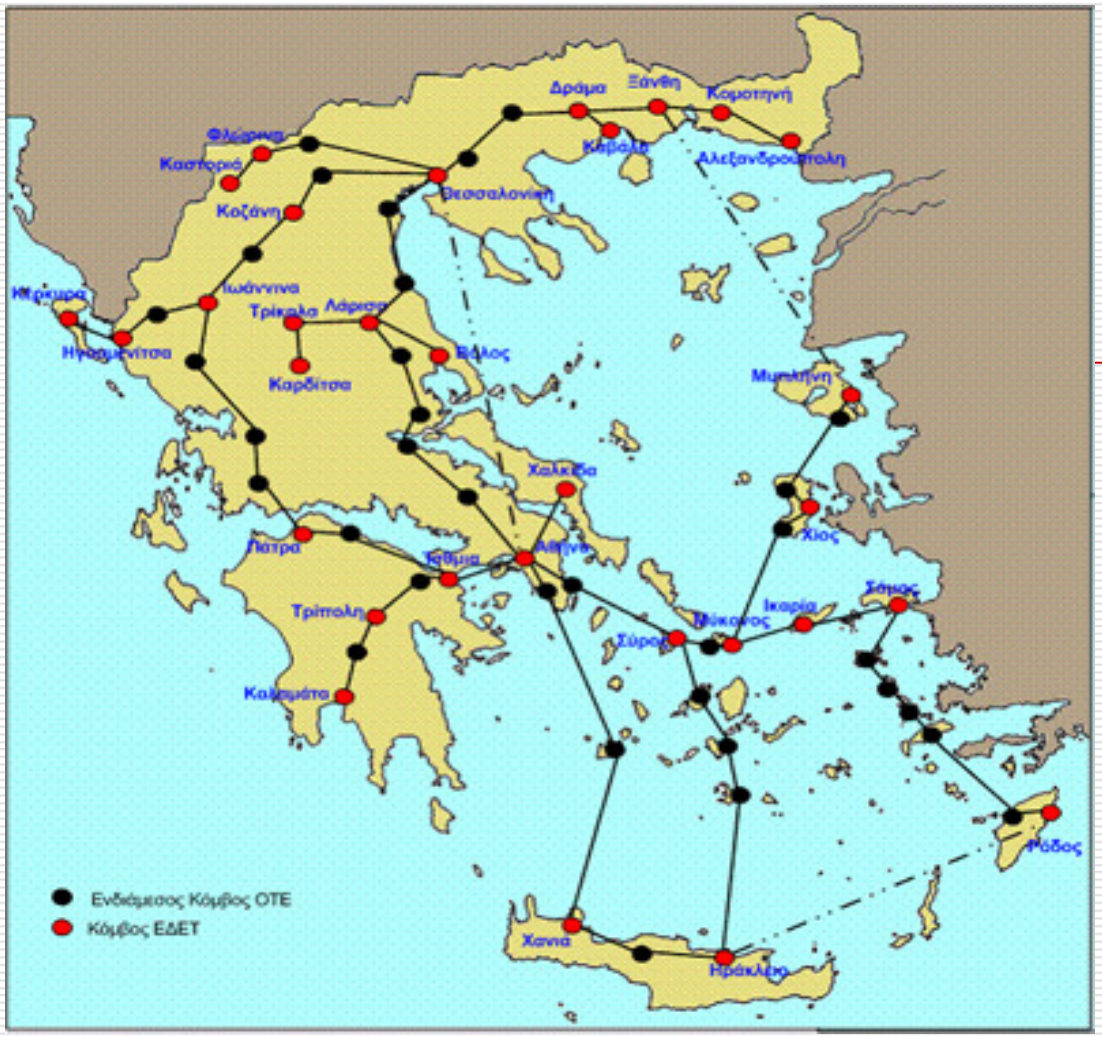
GRNET-CERT

(mini presentation)

http://cert.grnet.gr

Emai: grnet-cert@grnet.gr

The Network



GRNET 2

- WDM technology at extra high speeds (1-2,5 Gbps).

- All the nodes have Gigabit speed routers with leased wavelengths from the national telecom provider (OTE).

GRNET 3

-Part of the “Information Society” program of the Finance and Economy Ministry
- Covers about 7.000 kilometers of fiber optics
- Connects 90 research and education organizations
- Allows the data transfer at extra high speeds (multiple wavelengths of 10 Gbps

- All Universities, Technical Institutes, some government (>400k users)
- The School Network (potential 200k users)
- Student DSL network

GRNET-CERT

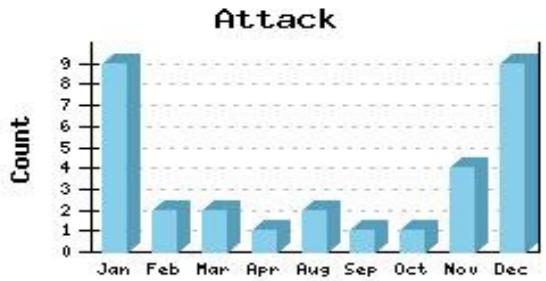
- 3 people (1 admin, 2 tech)
- Hours 08:00 am – 08:00 pm, voicemail after hours (see web page)

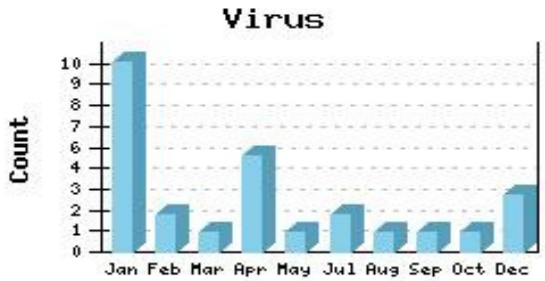
- Information Dissemination (vulns, advisories etc)
- Maintain/try tools
- Contact point for incidents
- Participate in national forums

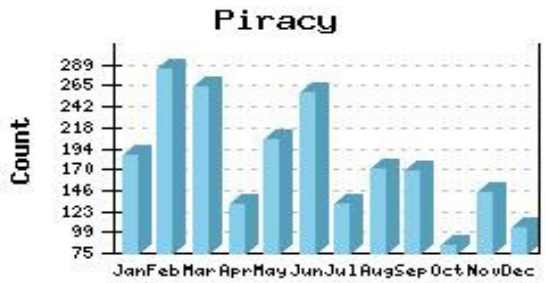
INCIDENTS RECORDED

Category	2001	2002	2003	2004	2005	2006	2007
Attack	88	132	35	60	15	26	27
DDOS	24	3	5	2		0	
DOS	9	2	5	2		0	4
Fraud / Phishing	2	15	4	1	11	**46**	**47**
Intrusion	23	20	8	7	13	4	3
Offensive Mail	4	6	2		1	1	
Piracy (P2P)		2	23	110	15	**405**	**2129**
Port Scanning	54	36	32	77	75	**94**	**204**
Privacy						1	
Proxy	1	3	1			0	
Site Defaced	27	1	16	3	43	30	18
Spam	34	23	40	52	41	88	**261**
Virus	27	15	5	180	24	18	28
Vulnerabilities							11
Total	**293**	**258**	**176**	**494**	**238**	**713**	**2732**

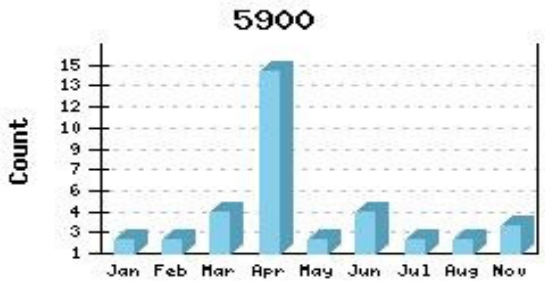
Top Categories

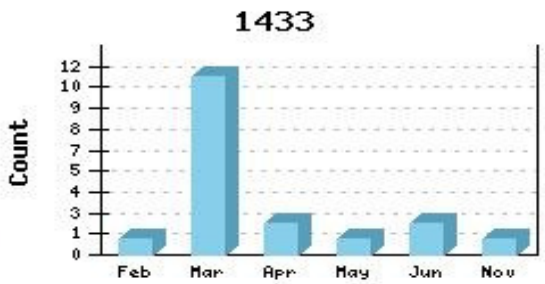






Top Ports





Current projects

- Deployment malware sensors on CD
- Baby steps in malware analysis

Current Activity

Top 10 IPs

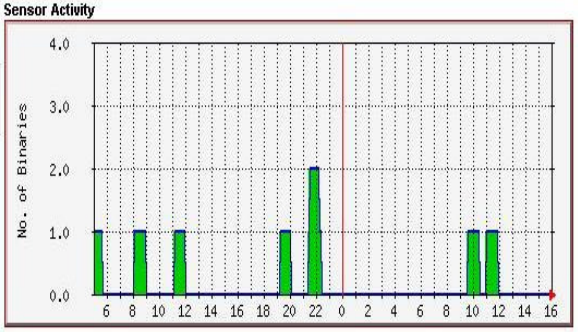
IP	Host	Geo	Count
195.246.[redacted]	195.246.[redacted]	RO	2

Update

Top Submitted Files

Binary	Count	First	Last
a3781d5747a5bd632d0966e061416088	2	2008-01-28 04:38:47	2008-01-29 10:50:14

Sensor Activity



Submitted Files

Sensor	Date	Time	Source IP	Binary	Detection	Detail
[redacted]	2008-01-29	10:50:14	195.246.[redacted]	a3781d5747a5bd632d0966e061416088		link://195.246.246.141:25492/fTrlPQ==
[redacted]	2008-01-29	09:27:04	195.246.[redacted]	a3781d5747a5bd632d0966e061416088		link://195.246.246.141:47981/fTolAw==

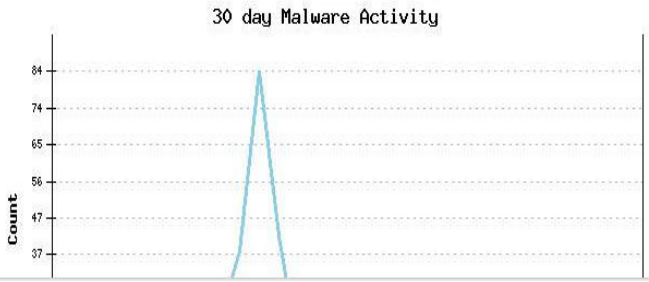
Search

enter IP Address

enter Binary

History

2008-01-29	2	2007-12-31	3	2007-11-30	4	2007-10-31	21	2007-09-29	11	2007-08-31	9	2007-07-31	24
2008-01-28	7	2007-12-28	4	2007-11-29	5	2007-10-30	14	2007-09-28	9	2007-08-30	6	2007-07-30	64
2008-01-27	3	2007-12-27	6	2007-11-28	11	2007-10-29	20	2007-09-27	8	2007-08-29	3	2007-07-29	6
2008-01-26	2	2007-12-26	1	2007-11-27	44	2007-10-28	7	2007-09-26	2	2007-08-28	4	2007-07-28	21
2008-01-25	4	2007-12-25	6	2007-11-26	6	2007-10-27	10	2007-09-25	27	2007-08-27	6	2007-07-27	19
2008-01-24	3	2007-12-24	3	2007-11-25	12	2007-10-26	13	2007-09-24	47	2007-08-26	4	2007-07-26	18
2008-01-23	3	2007-12-23	7	2007-11-24	5	2007-10-25	14	2007-09-23	16	2007-08-25	7	2007-07-25	16
2008-01-22	8	2007-12-22	8	2007-11-23	6	2007-10-24	18	2007-09-22	16	2007-08-24	8	2007-07-24	48
2008-01-21	6	2007-12-21	5	2007-11-22	8	2007-10-22	3	2007-09-21	11	2007-08-23	6	2007-07-23	21



Search

enter IP Address enter Binary

History

2008-01-29	2
2008-01-28	7
2008-01-27	3
2008-01-26	2
2008-01-25	4
2008-01-24	3
2008-01-23	3
2008-01-22	8
2008-01-21	6
2008-01-20	7
2008-01-19	10
2008-01-18	1
2008-01-17	4
2008-01-16	5
2008-01-15	11
2008-01-14	8
2008-01-13	6
2008-01-12	13
2008-01-11	42
2008-01-10	84
2008-01-09	38
2008-01-08	21
2008-01-07	20
2008-01-06	19
2008-01-05	13
2008-01-04	5
2008-01-03	4
2008-01-02	4
2008-01-01	5

2007-12-31	3
2007-12-28	4
2007-12-27	6
2007-12-26	1
2007-12-25	6
2007-12-24	3
2007-12-23	7
2007-12-22	8
2007-12-21	5
2007-12-20	148
2007-12-19	103
2007-12-18	22
2007-12-17	11
2007-12-16	7
2007-12-15	7
2007-12-14	23
2007-12-13	9
2007-12-12	18
2007-12-11	4
2007-12-10	24
2007-12-09	5
2007-12-08	10
2007-12-06	18
2007-12-05	10
2007-12-04	13
2007-12-03	6
2007-12-02	9
2007-12-01	2

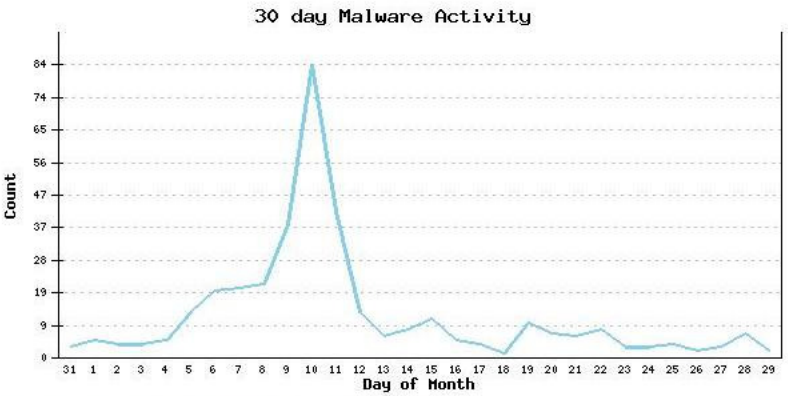
2007-11-30	4
2007-11-29	5
2007-11-28	11
2007-11-27	44
2007-11-26	6
2007-11-25	12
2007-11-24	5
2007-11-23	6
2007-11-22	8
2007-11-21	10
2007-11-20	21
2007-11-19	25
2007-11-18	4
2007-11-17	4
2007-11-16	37
2007-11-15	30
2007-11-14	10
2007-11-13	6
2007-11-12	15
2007-11-11	10
2007-11-10	4
2007-11-09	6
2007-11-08	7
2007-11-07	6
2007-11-05	44
2007-11-04	8
2007-11-03	10
2007-11-02	10
2007-11-01	10

2007-10-31	21
2007-10-30	14
2007-10-29	20
2007-10-28	7
2007-10-27	10
2007-10-26	13
2007-10-25	14
2007-10-24	18
2007-10-22	3
2007-10-21	3
2007-10-20	4
2007-10-19	5
2007-10-18	8
2007-10-17	3
2007-10-13	1
2007-10-12	17
2007-10-11	14
2007-10-10	10
2007-10-09	15
2007-10-08	17
2007-10-07	8
2007-10-06	5
2007-10-05	9
2007-10-04	22
2007-10-03	17

2007-09-29	11
2007-09-28	9
2007-09-27	8
2007-09-26	2
2007-09-25	27
2007-09-24	47
2007-09-23	16
2007-09-22	16
2007-09-21	11
2007-09-20	13
2007-09-19	7
2007-09-18	3
2007-09-14	7
2007-09-13	15
2007-09-12	28
2007-09-11	34
2007-09-10	2
2007-09-09	24
2007-09-08	17
2007-09-07	15
2007-09-06	17
2007-09-05	7
2007-09-04	1
2007-09-03	25
2007-09-02	14
2007-09-01	7

2007-08-31	9
2007-08-30	6
2007-08-29	3
2007-08-28	4
2007-08-27	6
2007-08-26	4
2007-08-25	7
2007-08-24	8
2007-08-23	6
2007-08-22	3
2007-08-21	2
2007-08-20	3
2007-08-19	6
2007-08-18	5
2007-08-17	3
2007-08-16	5
2007-08-15	4
2007-08-14	2
2007-08-13	5
2007-08-12	6
2007-08-11	14
2007-08-10	5
2007-08-09	9
2007-08-08	19
2007-08-07	8
2007-08-06	17
2007-08-05	9
2007-08-04	10
2007-08-03	16
2007-08-02	17
2007-08-01	15

2007-07-31	24
2007-07-30	64
2007-07-29	6
2007-07-28	21
2007-07-27	19
2007-07-26	18
2007-07-25	16
2007-07-24	48
2007-07-23	21
2007-07-21	1
2007-07-20	72
2007-07-19	55
2007-07-18	67
2007-07-17	53
2007-07-16	55
2007-07-15	1
2007-07-14	12
2007-07-13	208
2007-07-12	264
2007-07-11	127
2007-07-10	150
2007-07-09	32
2007-07-08	10
2007-07-07	14
2007-07-06	82
2007-07-05	85
2007-07-04	54
2007-07-03	90
2007-07-02	26
2007-07-01	13



Top Virus Types	Count
W32/Sdbot.worm virus	60
W32/Sdbot.worm.gen.h virus	55
Win32:SdBot-4142 [Trj]	47
Backdoor.Agent.YRG	43
Win32:Trojan-gen {Other}	34
a "backdoor" program	29
Worm.Allaple-2	27
Win32:Allaple [Wrm]	24
MemScan:Backdoor.Agent.YRG	21
Generic.dx trojan	19

Top Countries Count	
GR	238
PL	30
RO	27
DE	16
HU	15
SK	5
NL	5
NO	3
RU	3
UA	3