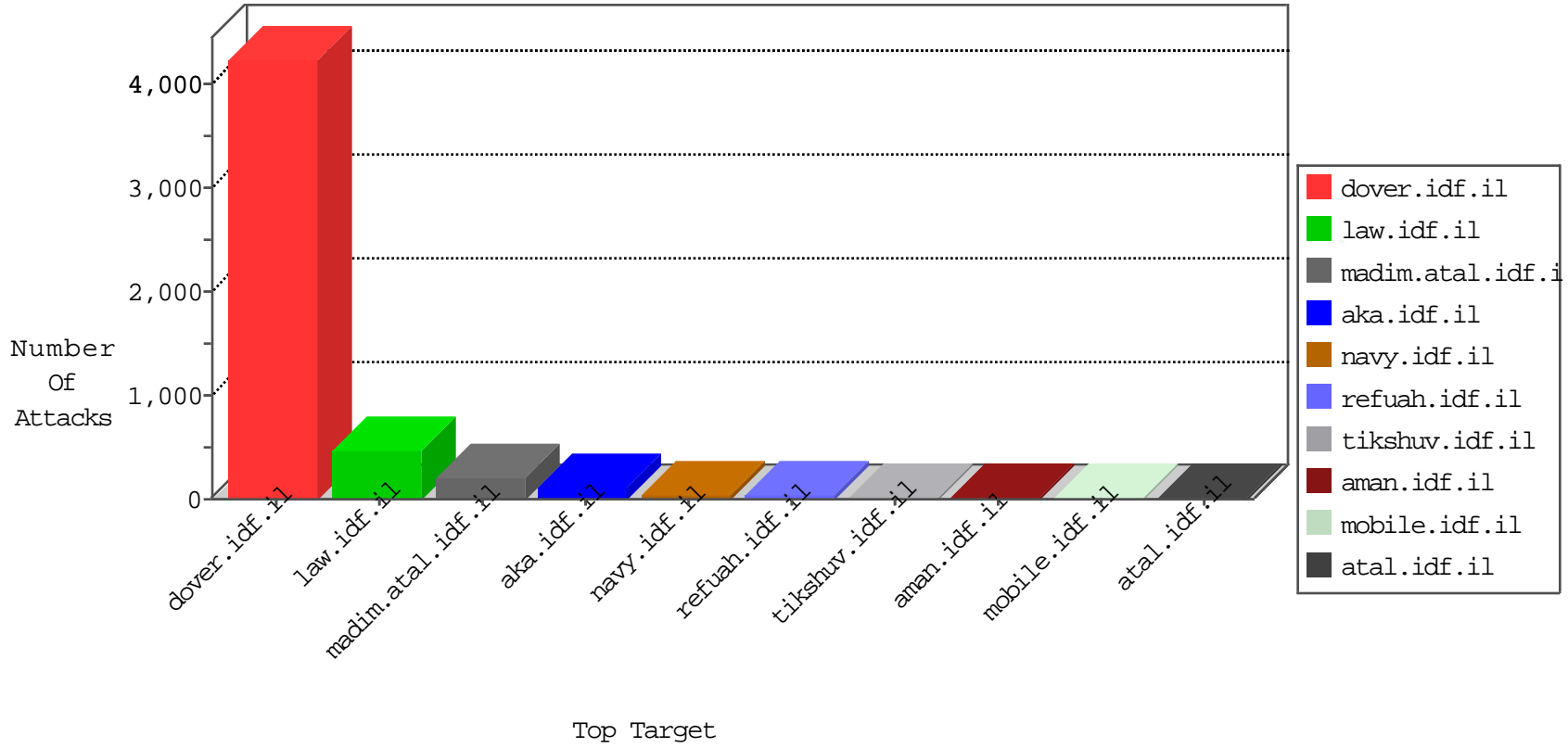


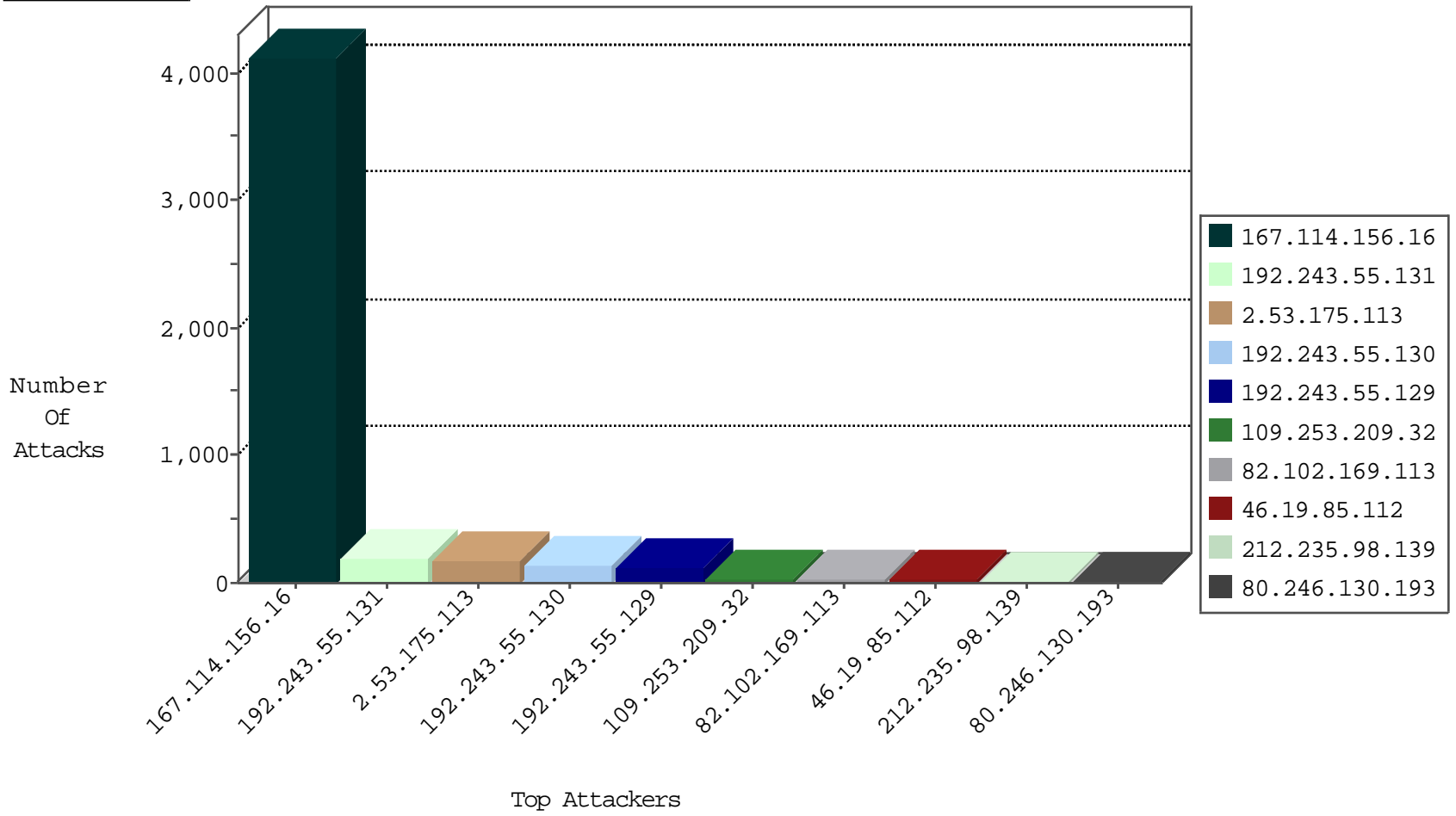
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4109
46.19.85.98	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	196
2.53.49.32	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	112
2.53.138.16	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	63
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
184.105.139.67	United States	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	1
79.181.53.76	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
2.53.46.229	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
195.11.108.162	United Kingdom	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
106.84.196.60	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
46.121.90.209	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
184.105.139.67	United States	147.237.8.24	e.lifestyle.idf.il	Block_Udp_All_Nets	drop	1
204.68.184.25	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.80	United States	147.237.8.28	e.mobile-ks.idf.il	Block_Ntp_All_Net	drop	1
82.145.211.9	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	1
212.143.142.56	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
179.43.141.194	Switzerland	147.237.0.16	my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
71.6.167.142	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.108	United States	147.237.0.16	my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
94.102.49.116	Netherlands	147.237.77.216	dover.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.199.232.162	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
213.57.42.181	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
46.4.32.75	Germany	147.237.76.31	nakchal.idf.il	C1000074: HTTP: majestic bot	Block	4
46.4.32.75	Germany	147.237.72.156	aman.idf.il	C1000074: HTTP: majestic bot	Block	2
46.4.32.75	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	2
69.30.198.242	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	7
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
201.146.98.22	147.237.0.33	Mexico	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
163.172.140.23	147.237.72.166	United Kingdom	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
80.82.78.38	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
216.218.210.34	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 3072	1
107.158.255.194	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
13.92.100.128	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	48
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	41
192.243.55.131	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	38
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	34
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	34
192.243.55.131	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	31
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	28
192.243.55.130	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	24
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	23
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	22
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	21
192.243.55.129	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	20
192.243.55.130	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	19
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	15
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	15
192.243.55.129	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	15
80.246.130.193	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
177.32.125.157	Brazil	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
2.53.175.113	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	8
82.102.169.113	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	8
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	8
212.235.98.139	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	8
46.19.85.112	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.181.10.221	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.180.53	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
84.94.74.21	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.112	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	6
5.28.184.87	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.53.175.113	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
84.94.74.21	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.112	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
84.111.126.15	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.112	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.178.18.99	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.176	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
82.102.169.113	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.179.21.194	Israel	147.237.8.27	e.madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
82.102.169.113	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
182.184.79.28	Pakistan	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.177	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
182.184.79.28	Pakistan	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
79.178.18.99	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.85.176	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
79.180.22.72	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
79.183.171.66	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.53.175.113	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.85.177	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.175.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	153
109.253.209.32	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
77.125.5.90	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 77.125.5.90	Block	6
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	6
91.200.12.114	Ukraine	147.237.77.216	dover.idf.il	PHP Attempt	Block	4
2.53.135.34	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	3
91.200.12.114	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 91.200.12.114	Block	3
2.55.1.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.135.34	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 2.53.135.34	Block	2
5.39.222.159	Netherlands	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
87.236.215.243	United Kingdom	147.237.77.216	dover.idf.il	Parameter Type Violation ID in www.idf.il/1294-en/dover.aspx	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/8/71538.pdf	Block	1
128.232.110.28	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
77.125.5.90	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/3/size338x0/1633.jpg	Block	1
37.142.68.15	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
128.232.110.28	United Kingdom	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
80.246.130.193	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
62.210.113.183	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dover/site/homepage/asp	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/sachar/resources/scripts/ticker.js	Block	1
2.53.175.113	Israel	147.237.0.19	madim.atal.idf.il	Untraceable SSL Sessions: Open Mode	None	1
207.46.13.29	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
82.81.193.82	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
62.210.252.207	France	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/	Block	1
91.200.12.114	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1540-13036-he/dover.aspx target=	Block	1
207.46.13.54	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
87.71.57.25	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
62.210.252.207	France	147.237.77.235	sviva.idf.il	Unauthorized URL Access to www.hagnas.atal.idf.il/hnap1/	Block	1