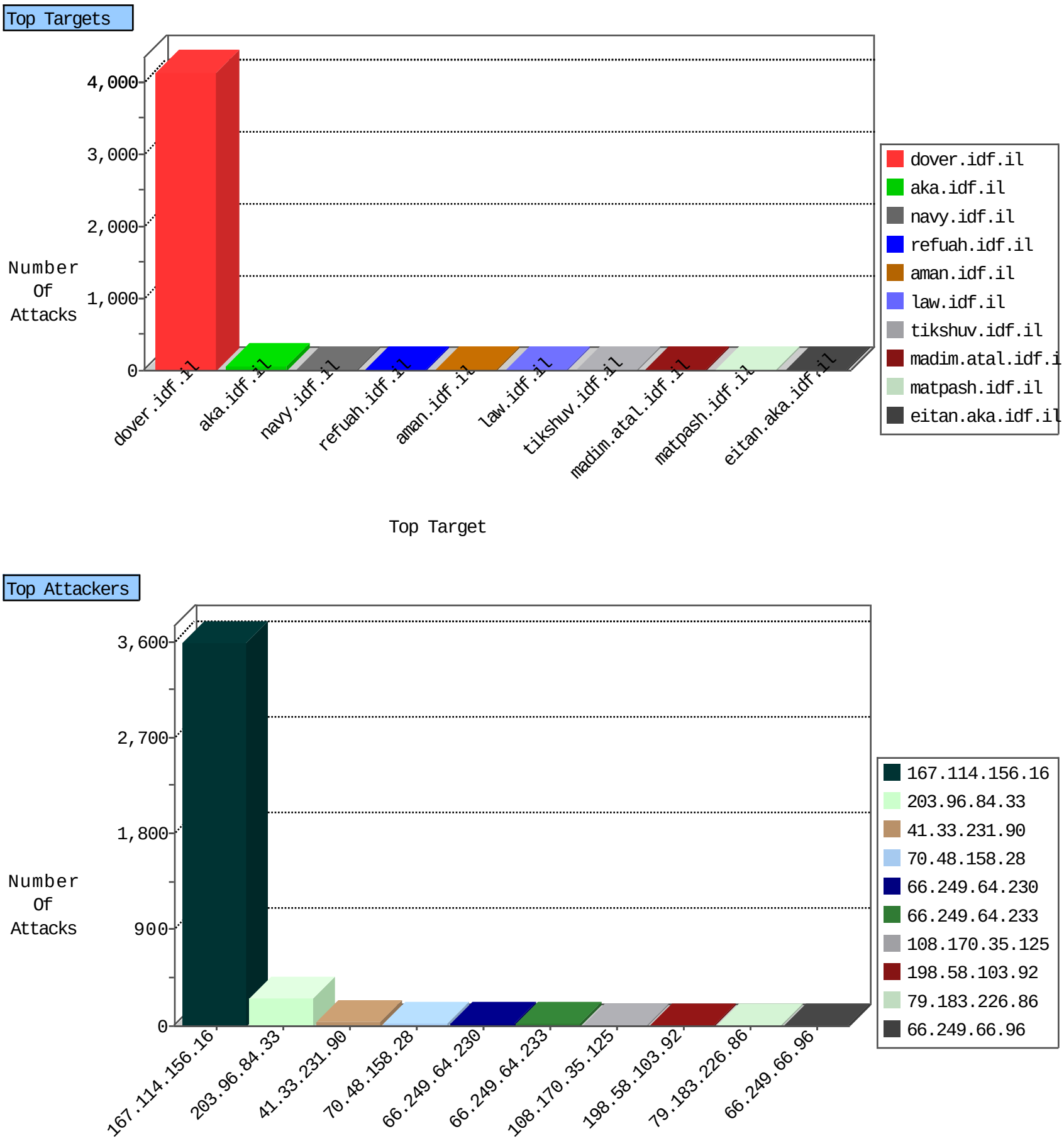
11-25-2015-01:09:00 to 11-25-2015-02:09:00

IDF Under Attack Daily Report



11-25-2015-01:09:00 to 11-25-2015-02:09:00

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	DOS-Tool-SwitchbladG	dest-reset	2791
79.182.181.40	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	4
79.182.181.40	Israel	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	2
183.60.48.25	China	147.237.76.201	e.atal.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
187.11.202.51	Brazil	147.237.76.147	chinuch.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
123.151.42.61	China	147.237.76.30	himush.idf.il	JLM_Under_Attack_Con_Udp	drop	1
14.192.208.156	Malaysia	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1

11-25-2015-01:09:00 to 11-25-2015-02:09:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

11-25-2015-01:09:00 to 11-25-2015-02:09:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
222.186.56.115	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
66.249.64.238	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
222.186.56.115	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.130.145.216	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.56.115	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
119.73.228.130	147.237.77.226	Singapore	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 4096	1
119.73.228.130	147.237.77.226	Singapore	www.chamatz.aka.idf.il	ET SCAN NMAP -f -sS	1
113.59.33.61	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.67.232	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
222.186.56.115	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.130.145.216	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.56.115	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
27.221.10.43	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
171.42.196.217	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
119.73.228.130	147.237.77.226	Singapore	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 2048	1
113.59.33.61	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
82.117.208.243	147.237.72.217		e.idf.il	ET SCAN NMAP -sS window 1024	1

11-25-2015-01:09:00 to 11-25-2015-02:09:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1506
203.96.84.33	New Zealand	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	254
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
70.48.158.28	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
66.249.64.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
108.170.35.125	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
198.58.103.92	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
40.77.167.76	United States	147.237.76.86	navy.idf.il	drop	SAM rule	drop	8
66.249.66.96	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
207.46.13.34	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.249.64.230	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.86.153	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.60.42.195	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
109.66.17.208	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
50.155.109.40	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.118.24.10		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
157.55.39.217	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.54.42.55	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.64.230	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
66.249.64.235	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
142.167.247.240	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	4
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
199.30.16.169	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
166.137.136.55	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
82.114.168.157	Yemen	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
5.255.253.188	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.0.218	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.222.241	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
128.232.110.28	United Kingdom	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
185.120.126.82		147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
209.82.30.253	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
93.172.155.99	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
128.232.110.28	United Kingdom	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
208.115.113.89	United States	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	2
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
128.232.110.28	United Kingdom	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
5.255.253.188	Russian Federation	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
61.135.190.72	China	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
98.169.81.6	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
79.183.218.91	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
131.253.25.143	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
85.240.122.101	Portugal	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
128.232.110.28	United Kingdom	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
185.120.126.82		147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	2
79.207.140.138	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2

11-25-2015-01:09:00 to 11-25-2015-02:09:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.181.184.137	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
98.71.195.80	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	2
5.102.207.23	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	2
80.246.137.11	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.85.225	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
85.65.182.184	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	2
66.249.66.103	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
89.138.69.239	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.183.226.86	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
46.19.86.19	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
141.212.122.160	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
5.102.207.23	Israel	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.mag.idf.il/xmlrpc.php	Block	1
105.229.14.148	South Africa	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.64.243	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
88.156.130.182	Poland	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
37.142.188.69	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
188.138.9.49	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
79.183.226.86	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 79.183.226.86	Block	1
79.176.222.201	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
5.102.207.23	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.67.232	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
94.159.181.187	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
79.183.226.86	Israel	147.237.77.233	atal.idf.il	Distributed PHP Attempt	Block	1
46.121.249.208	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.102.207.23	Israel	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
149.88.94.173	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.183.226.86	Israel	147.237.0.34	tikshuv.idf.il	Distributed PHP Attempt	Block	1
105.229.14.148	South Africa	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1779-he/dover.aspx	Block	1
66.249.66.72	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/civiladministration/minhalnews/pages/knesiyothaghamolad.aspx	Block	1
88.156.130.182	Poland	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
37.142.188.69	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/xmlrpc.php	Block	1
190.16.187.167	Argentina	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
79.183.226.86	Israel	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	1
79.176.222.201	Israel	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
5.102.207.23	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	1
109.64.7.124	Israel	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1
66.249.73.142	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il/	Block	1
79.183.226.86	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/xmlrpc.php	Block	1
61.135.190.71	China	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to 147.237.0.19/	Block	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
5.102.207.23	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
157.55.2.131	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.183.226.86	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 79.183.226.86	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
77.12.5.7	Germany	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1

11-25-2015-01:09:00 to 11-25-2015-02:09:00