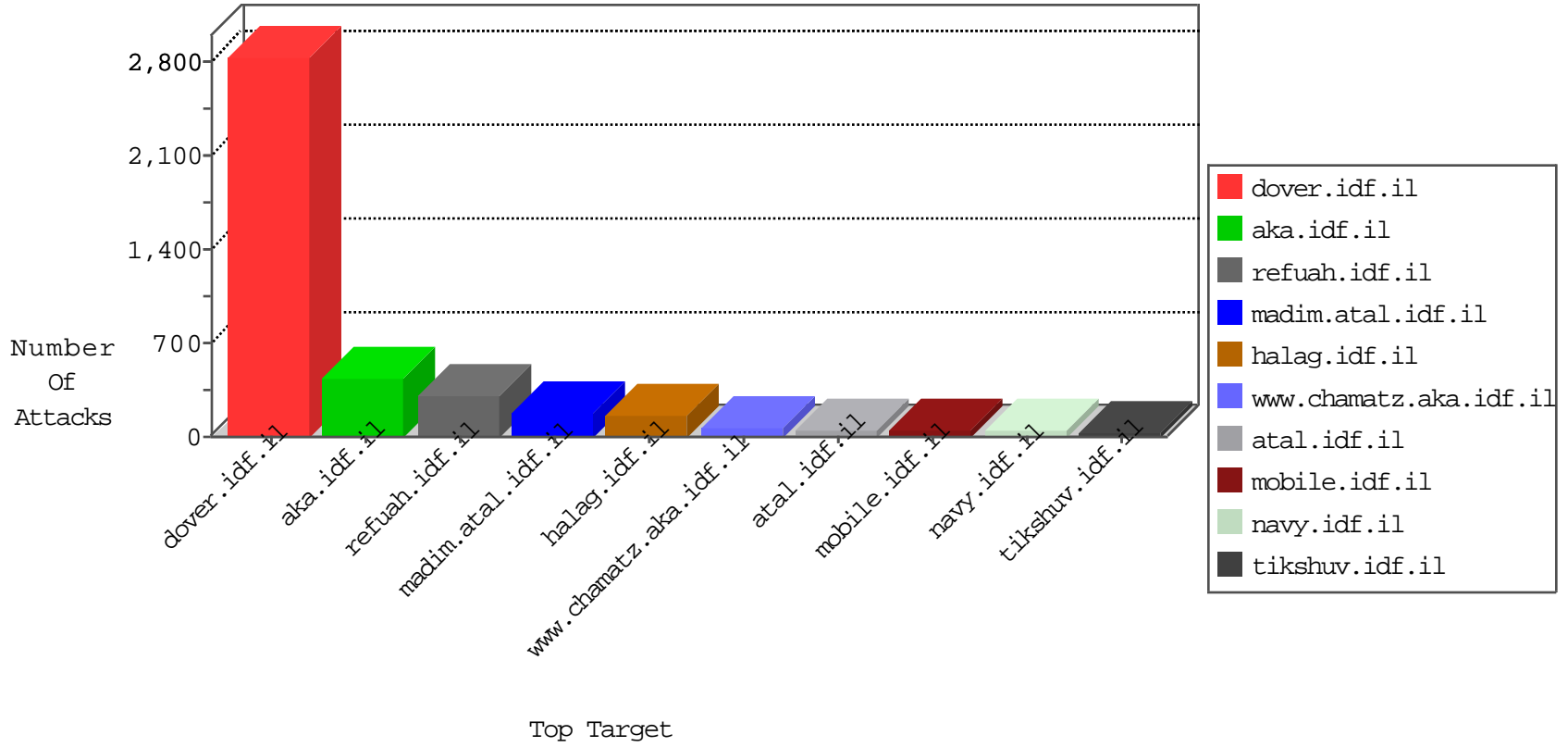




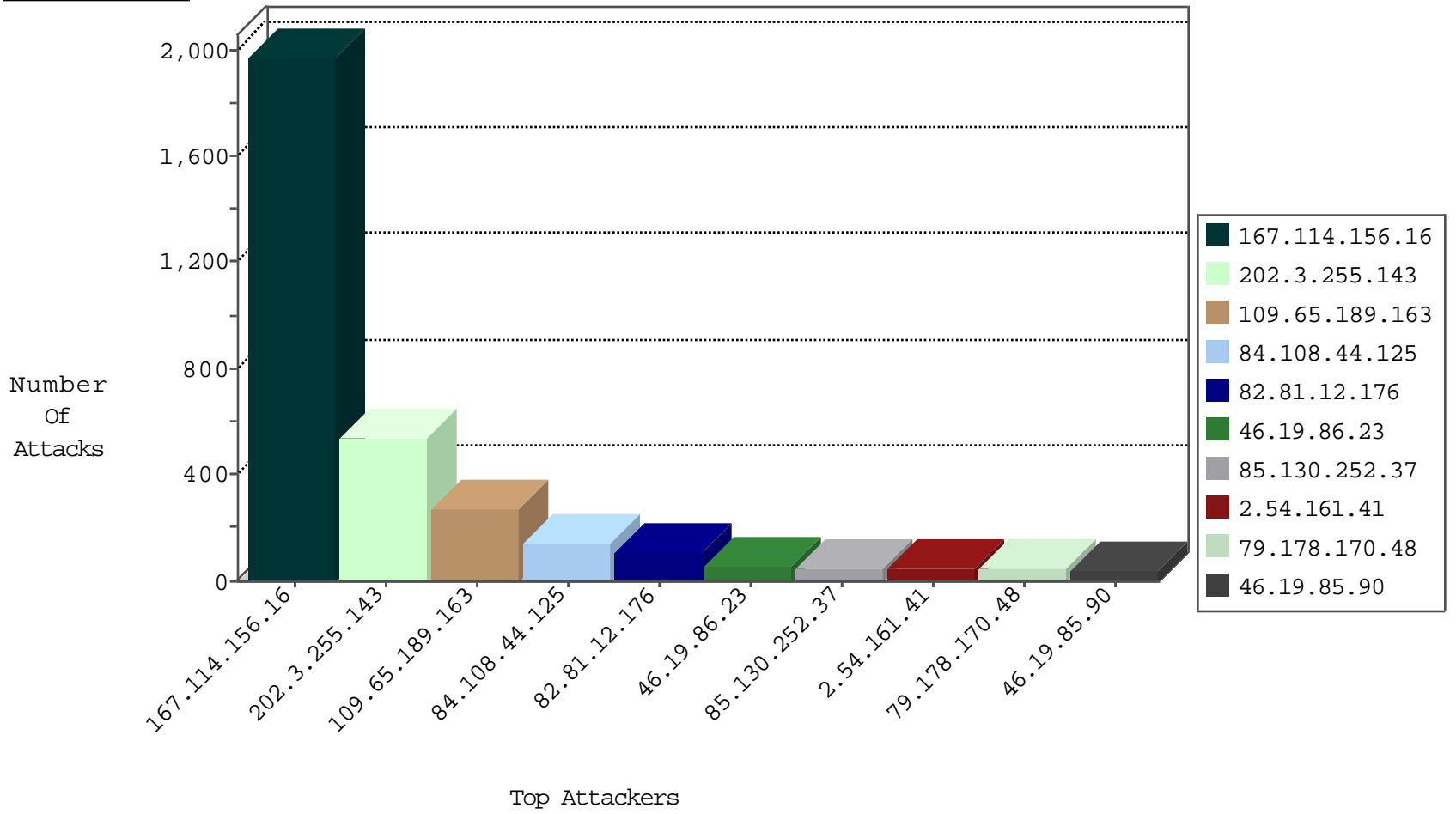
IDF Under Attack Daily Report



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	DOS-Tool-SwitchbladG	dest-reset	3099
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	108
79.181.22.18	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
157.55.39.160	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
193.242.218.6	Switzerland	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.0.153	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	12
79.181.69.129	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	4
84.109.212.72	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	2
217.132.103.140	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.76.42	refuah.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
79.179.34.77	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
202.3.255.143	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	499
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
93.174.93.181	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.181	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
131.109.15.15	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 4096	1
77.127.59.144	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
113.171.23.126	147.237.76.30	Vietnam	himush.idf.il	ET SCAN Potential SSH Scan	1
108.30.83.8	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1
93.174.93.181	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.174.93.181	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.174.93.181	147.237.76.197	Netherlands	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.174.93.181	147.237.72.156	Netherlands	aman.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.181	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
79.181.220.149	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
131.109.15.15	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 3072	1
113.171.23.126	147.237.0.17	Vietnam	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.181	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.174.93.181	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.174.93.181	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
200.139.128.16	147.237.0.35	Brazil	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
93.174.93.181	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
187.246.114.196	147.237.76.39	Mexico	mobile.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.65.189.163	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	273
84.108.44.125	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	142
79.178.170.48	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	45
202.3.255.143	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
176.77.50.12	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	25
109.173.20.71	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	22
46.19.85.90	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
46.19.85.90	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	17
46.19.86.160	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
46.19.86.47	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
37.110.144.46	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	11
46.19.85.84	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
2.52.9.166	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
2.54.53.52	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
207.241.229.110	United States	147.237.72.166	aka.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	8
46.19.86.187	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
85.130.252.37	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.86.140	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
85.130.252.37	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
94.159.169.187	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	7
46.19.86.47	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
94.159.169.187	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
94.159.169.187	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
109.65.117.100	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
213.8.204.40	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.44	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.176.61.219	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.16	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.173	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.44	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.120.126.73		147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.228	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
157.55.39.224	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.37	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
85.130.252.37	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
85.130.252.37	Israel	147.237.0.15	kosher-kravi.idf.il	drop	First packet isn't SYN	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.142.68.115	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.228	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.43	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
156.173.207.182		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
213.8.204.40	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.180.9.14	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.43	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.176.61.219	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.147.215	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
31.210.187.76	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	58
2.54.161.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	47
185.120.126.73		147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
46.19.85.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
46.19.86.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
79.178.193.21	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
2.52.149.220	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	7
149.78.166.151	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
89.139.13.13	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
87.69.119.138	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	2
2.52.8.202	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
109.66.186.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.63.6.4	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.63.6.4	Block	2
2.54.161.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2
2.54.8.31	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
157.55.39.213	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/shared/usercontrols/headerupper/	Block	2
46.121.84.185	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https://www.idf.il/	Block	1
212.76.125.56	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https://www.idf.il/	Block	1
2.54.168.80	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
87.68.53.7	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.136.162	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.205	Israel	147.237.76.86	navy.idf.il	Multiple Abnormally Long Request from 46.19.85.205	Block	1
176.13.1.174	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.176.61.219	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.24	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version _pk_ses.20.8afc=*	Block	1
109.253.137.249	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00\$ContentPlaceHolder1\$ucNewsFlashControl\$ImageButton1.x in www.idf.il/1153-he/dover.aspx	Block	1
37.26.146.142	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
95.41.114.105	Poland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/dover.aspx/	Block	1
66.249.69.34	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training/catalog.asp	Block	1
2.54.19.100	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.109.33.69	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.180	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
141.212.122.177	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
79.180.204.217	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/3382.jpg	Block	1
37.142.68.115	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
109.66.53.57	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.48	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/1/105701.pdf	Block	1
213.8.204.40	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.28.136.4	Israel	147.237.76.86	navy.idf.il	Cookie Tampering on cookie __atrfs: Expected ab/	None	1
84.108.44.125	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
46.19.85.205	Israel	147.237.76.86	navy.idf.il	Multiple Malformed URL from 46.19.85.205	Block	1
185.32.179.148	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.176.189.102	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
46.19.85.24	Israel	147.237.77.216	dover.idf.il	Malformed URL _pk_id.20.8afc=82aedc115c2029b3.1450005523.5.1453236691.1453236691.;	Block	1
109.253.142.131	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.149.208	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
95.86.103.136	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.2	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;docid in www.aka.idf.il/main/giyus/general.aspx	None	1
185.120.126.73		147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1