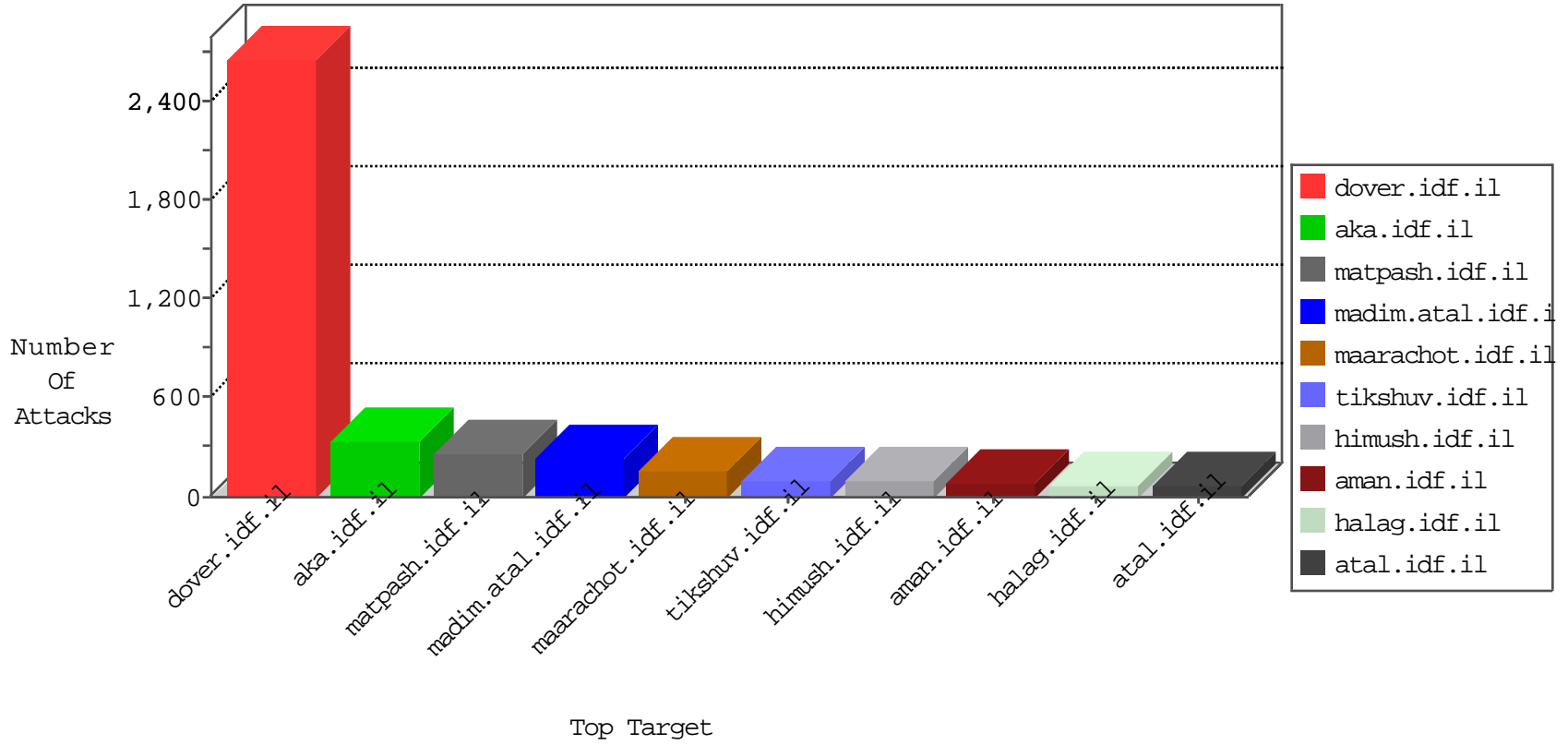


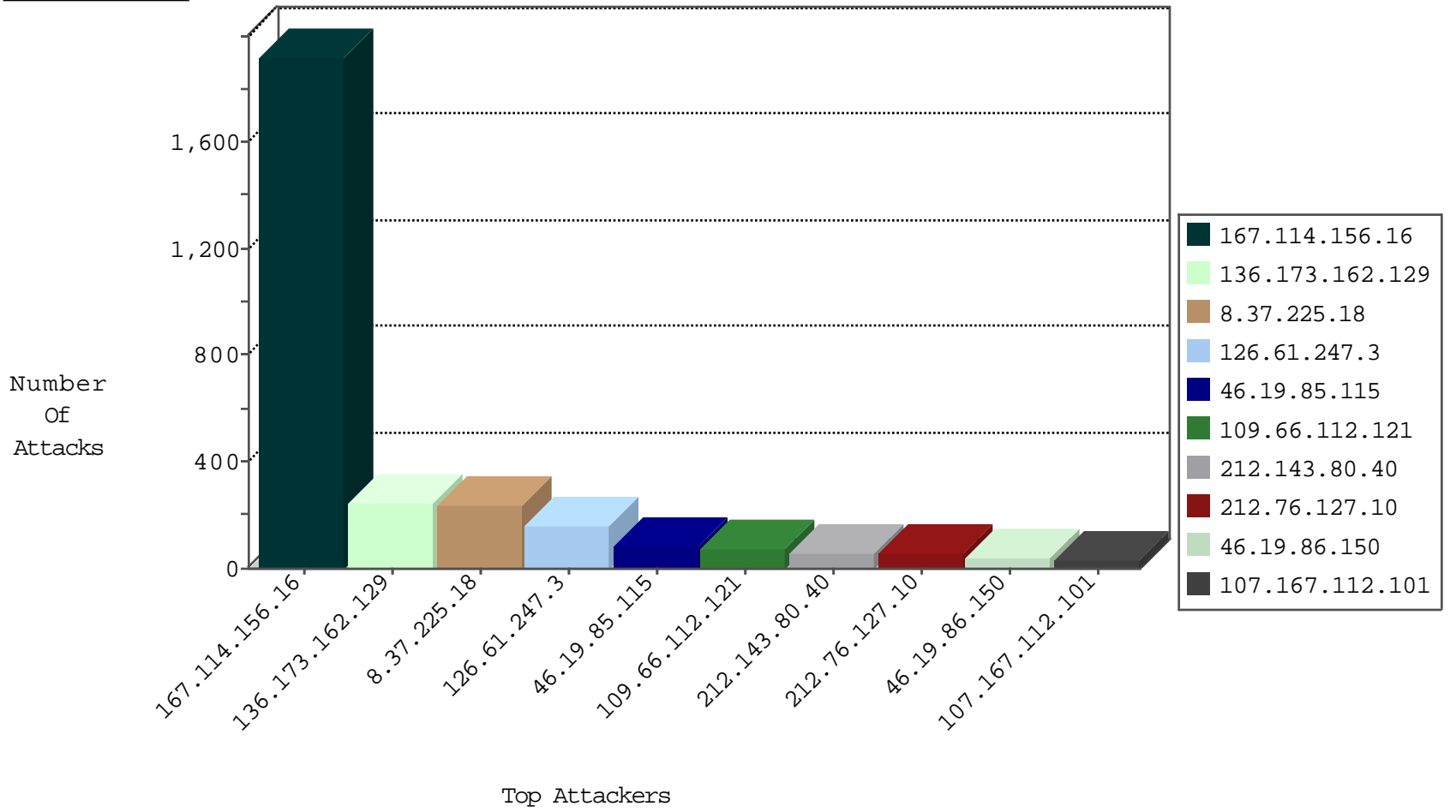
IDF Under Attack Daily Report



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	3282
79.178.11.107	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
8.37.225.18	Anonymous Proxy	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
66.249.78.102	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
107.150.98.131	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
126.61.247.3	Japan	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	70
126.61.247.3	Japan	147.237.77.216	dover.idf.il	0854: HTTP: upload* Access	Block	24
185.130.5.224		147.237.76.39	mobile.meitav.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1
185.130.5.224		147.237.77.216	dover.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1

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	2
209.126.116.147	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
107.167.112.101	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
79.182.52.174	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.93.180	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
46.117.195.164	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.172.244	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
222.186.56.42	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
213.8.204.74	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
207.232.28.187	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.120.126.73	147.237.77.216		dover.idf.il	portscan: TCP Distributed Portscan	1
82.80.196.44	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.127.206.160	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.90.167.133	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.229	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
222.186.56.42	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
136.173.162.129	Belgium	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	248
8.37.225.18	Anonymous Proxy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	119
8.37.225.18	Anonymous Proxy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	113
212.76.127.10	Israel	147.237.76.30	himush.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	54
212.143.80.40	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	39
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
107.167.112.101	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	31
126.61.247.3	Japan	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	30
193.105.199.1	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	28
2.54.191.28	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
213.8.204.67	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	23
212.76.127.44	Israel	147.237.76.30	himush.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	21
212.76.127.111	Israel	147.237.76.30	himush.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	21
80.179.37.165	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
84.111.37.230	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
66.102.9.83	United States	147.237.0.15	kosher-kravi.idf.il	drop	First packet isn't SYN	drop	15
213.8.241.210	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
207.241.229.71	United States	147.237.72.166	aka.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	14
109.64.177.15	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
5.29.64.35	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.19.85.6	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
31.177.36.114	Netherlands	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
5.29.64.35	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
87.71.4.25	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
79.176.58.141	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	9
109.253.215.141	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
109.253.143.218	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
31.168.169.234	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
5.102.254.183	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.121.75.50	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
192.114.91.244	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
62.90.182.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.109	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.108.99.164	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.143.80.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.206	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.246.130.53	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
212.150.66.161	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.110.131	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
192.114.105.254	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	6
185.27.107.82	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
212.143.80.40	Israel	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	6
31.168.157.83	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.178.13.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
94.159.155.26	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.114.105.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
77.127.240.177	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.26	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.13.9.167	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.115	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	78
109.66.112.121	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 109.66.112.121	Block	75
46.19.86.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
126.61.247.3	Japan	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 126.61.247.3	Block	29
2.52.9.65	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
185.32.179.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
80.246.138.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
46.19.86.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
185.32.179.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
80.246.136.52	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
2.52.10.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.33	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
31.168.93.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
81.218.251.250	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
2.54.177.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.137.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
84.111.165.10	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
109.253.192.82	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
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	2
2.54.145.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
2.52.33.6	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakchal.idf.il/894-he/nakchal.aspx)	Block	2
176.13.13.249	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.95.199.42	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 84.95.199.42	Block	2
89.87.35.168	France	147.237.76.42	refuah.idf.il	Distributed Parameter Type Violation on www.refua.atal.idf.il/1518-he/refuah.aspx parameter ct100\$ContentPlaceHolder1\$txtLastName	Block	2
46.117.58.146	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
126.61.247.3	Japan	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
185.3.147.174	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationervice.aspx/getauthuser	Block	2
199.16.156.125	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/size220x0/17882.jpg	Block	2
2.54.1.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
185.32.179.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.18.56	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.7.128	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	2
31.168.221.35	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
89.163.146.245	Germany	147.237.72.156	aman.idf.il	PHP Attempt	Block	1
79.182.174.26	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 79.182.174.26	Block	1
141.212.122.112	United States	147.237.76.42	refuah.idf.il	Multiple Malformed URL from 141.212.122.112	Block	1
66.249.79.234	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/modules/forums.frm/frmuserdetails.aspx	Block	1
120.61.9.244	India	147.237.77.74	law.idf.il	PHP Attempt	Block	1
2.54.10.134	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.89.217.225		147.237.76.42	refuah.idf.il	URL is Above Root Directory www.refua.atal.idf.il/./images/shared/home.png	Block	1
46.163.68.111	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
109.186.164.109	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
84.94.119.65	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.13.22.124	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.136.58	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
173.252.73.106	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.29	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1