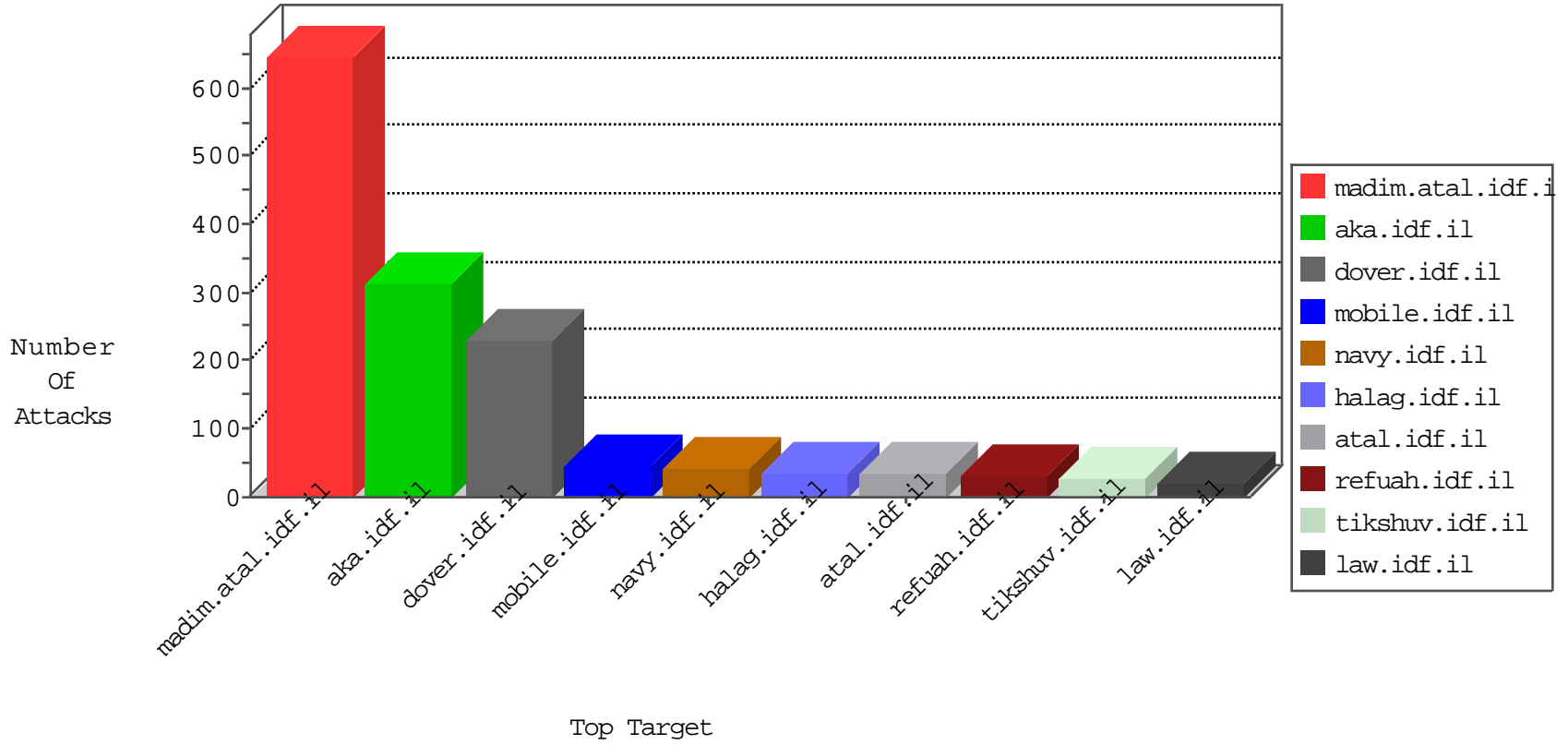


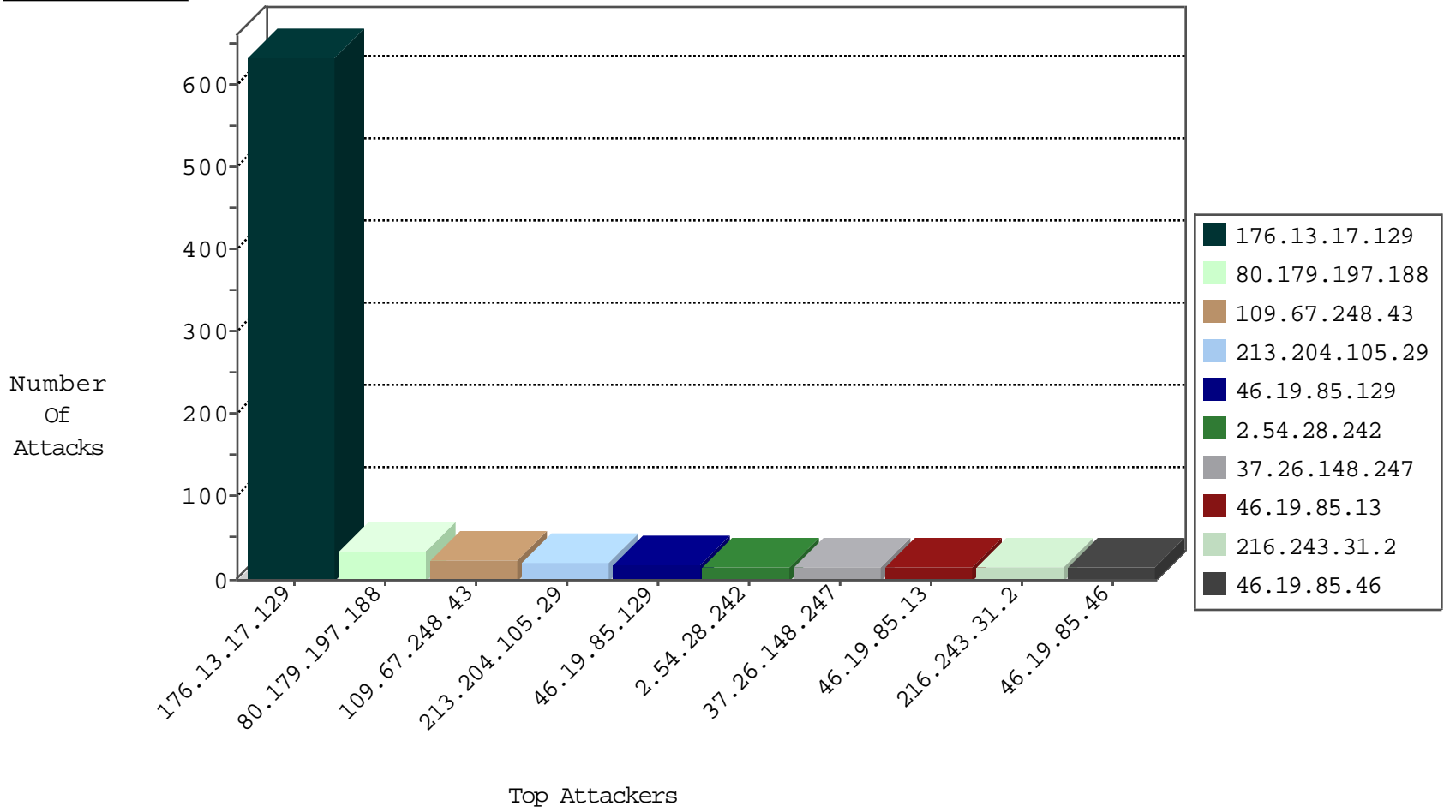
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.93.99	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	11
79.177.116.56	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	6
79.177.116.56	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
71.6.216.60	United States	147.237.0.19	madim.atal.idf.il	Block_Udp_All_Nets	drop	1
82.102.173.68	Israel	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
85.25.43.236	Germany	147.237.0.200	m4u.idf.il	Block_Udp_All_Nets	drop	1
71.6.216.39	United States	147.237.8.50	e.tikshuv.idf.il	Block_Udp_All_Nets	drop	1
89.248.174.4	Netherlands	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
71.6.216.43	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.139.34.102	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
106.120.173.109	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	7
84.245.33.104	Netherlands	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
66.135.63.82	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
109.66.21.220	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
87.70.64.124	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
149.202.54.6	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	2
84.229.208.199	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
149.202.54.6	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
149.202.54.6	Germany	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Block	2
84.228.172.91	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
10.0.0.6		147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
175.10.210.214	China	147.237.77.176	matpash.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
66.249.69.79	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
213.204.105.29	147.237.77.233	Lebanon	atal.idf.il	ET SCAN NMAP -sA (2)	10
84.245.33.104	147.237.76.42	Netherlands	refuah.idf.il	SQL Injection - Select From	6
66.135.63.82	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
137.226.113.7	147.237.72.166	Germany	aka.idf.il	ET SCAN Suspicious User-Agent Containing Web Scan/er, Likely Web Scanner	1
109.65.207.155	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.24.45.101	147.237.0.15	Spain	kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
46.120.70.63	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.28.166.109	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.88.108.112	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.67.135.125	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.102.228.208	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.76.176	China	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
208.67.1.57	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
186.112.251.35	147.237.76.31	Colombia	nakchal.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
176.13.17.129	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	272
176.13.17.129	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	136
109.67.248.43	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
2.54.28.242	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
80.179.197.188	Israel	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	13
37.26.148.247	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
80.179.197.188	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
79.181.223.216	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.182.102.137	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.46	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.13	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
190.24.146.71	Colombia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.10	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
213.204.105.29	Lebanon	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.129	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
62.219.135.44	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
94.159.153.41	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.122	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.221	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.46	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
195.110.40.242	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.58	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.39.64	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.13	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.229	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
41.77.152.171	South Africa	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.85.221	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
5.28.166.109	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
5.102.254.203	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.129	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
79.176.183.9	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
212.179.21.194	Israel	147.237.76.177	ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
85.64.71.234	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
37.46.39.177	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.129	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
66.96.128.60	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	4
147.235.8.74	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.85.10	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
80.179.197.188	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
147.235.8.74	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
91.65.252.211	Germany	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.208	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
5.102.195.3	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.104	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
80.246.140.248	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
176.13.1.128	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.102.195.90	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.133	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.22.129.226	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.17.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	223
94.159.153.41	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	4
66.249.64.233	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	3
37.26.148.247	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
109.65.153.116	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
46.19.85.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
132.74.95.21	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/2/109482.pdf	Block	2
176.13.1.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
82.102.136.65	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.54.191.51	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
79.182.102.137	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
37.203.114.113	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
84.229.133.22	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/	Block	1
5.22.129.226	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1133-ar/dover.aspx	Block	1
173.247.228.10	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/wp-login.php	Block	1
46.19.86.122	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.65.77.19	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/general.aspx?docid=70911	Block	1
80.179.197.188	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
66.102.8.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
185.120.125.11		147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https://www.aman.idf.il/	Block	1
41.77.152.171	South Africa	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
134.191.232.69	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
87.69.192.25	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/default.aspx'	Block	1
5.28.166.109	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
213.151.48.113	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/901-7991-he/tikshuv.aspx&sa=u&ved=0ahukewicu pfsmk_lahwko5okhad4db0qqoubccqwb&sig2=sba5-ntee6jrw6umerl-g w&usg=afqjncu31pkddhumc1b2sg02j70qsha	Block	1
66.249.64.240	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
46.116.5.162	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
37.26.149.165	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name H*8[[#27]]û`ð[[#19]][[#24]]ÁkαÆÿ@\$.il	Block	1
2.52.148.27	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.102.8.238	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
188.120.148.46	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catld in www.aka.idf.il/main/giyus/general.aspx	None	1
137.226.113.7	Germany	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
41.236.242.115	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
93.223.139.140	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
17.142.156.109	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1
78.108.161.226	Lebanon	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.116.162.32	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
37.26.149.165	Israel	147.237.72.166	aka.idf.il	Malformed HTTP Header Line 1	Block	1
109.160.130.248	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
82.102.136.66	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
2.54.25.167	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.50	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;docid in www.aka.idf.il/main/giyus/general.aspx	None	1
199.59.148.211	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/9/size220x0/16069.jpg	Block	1
149.50.85.120	United States	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
41.236.242.115	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
37.8.45.254	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
79.178.25.222	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
183.206.160.57	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/editorold/editor/	Block	1
46.116.218.124	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https://www.idf.il/	Block	1