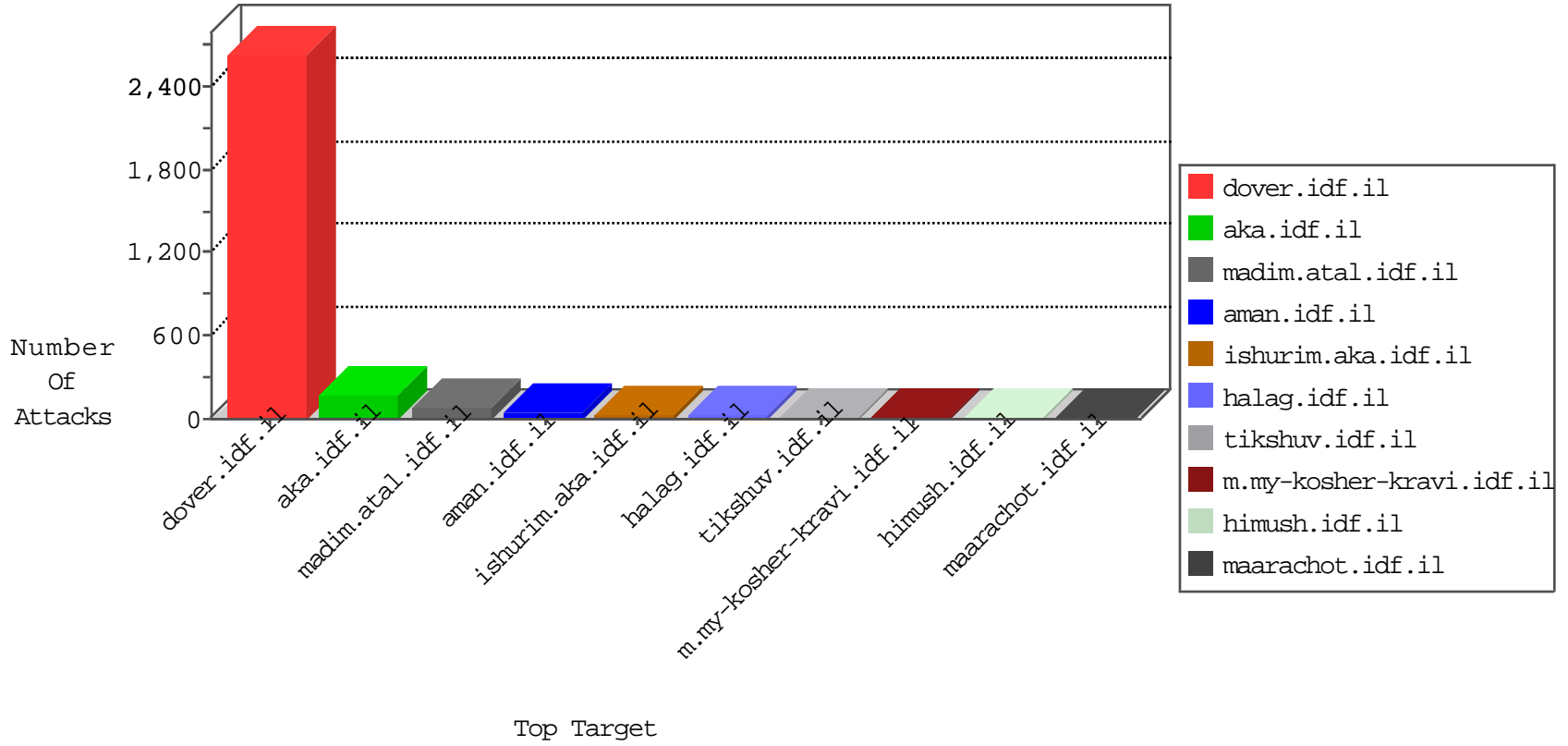


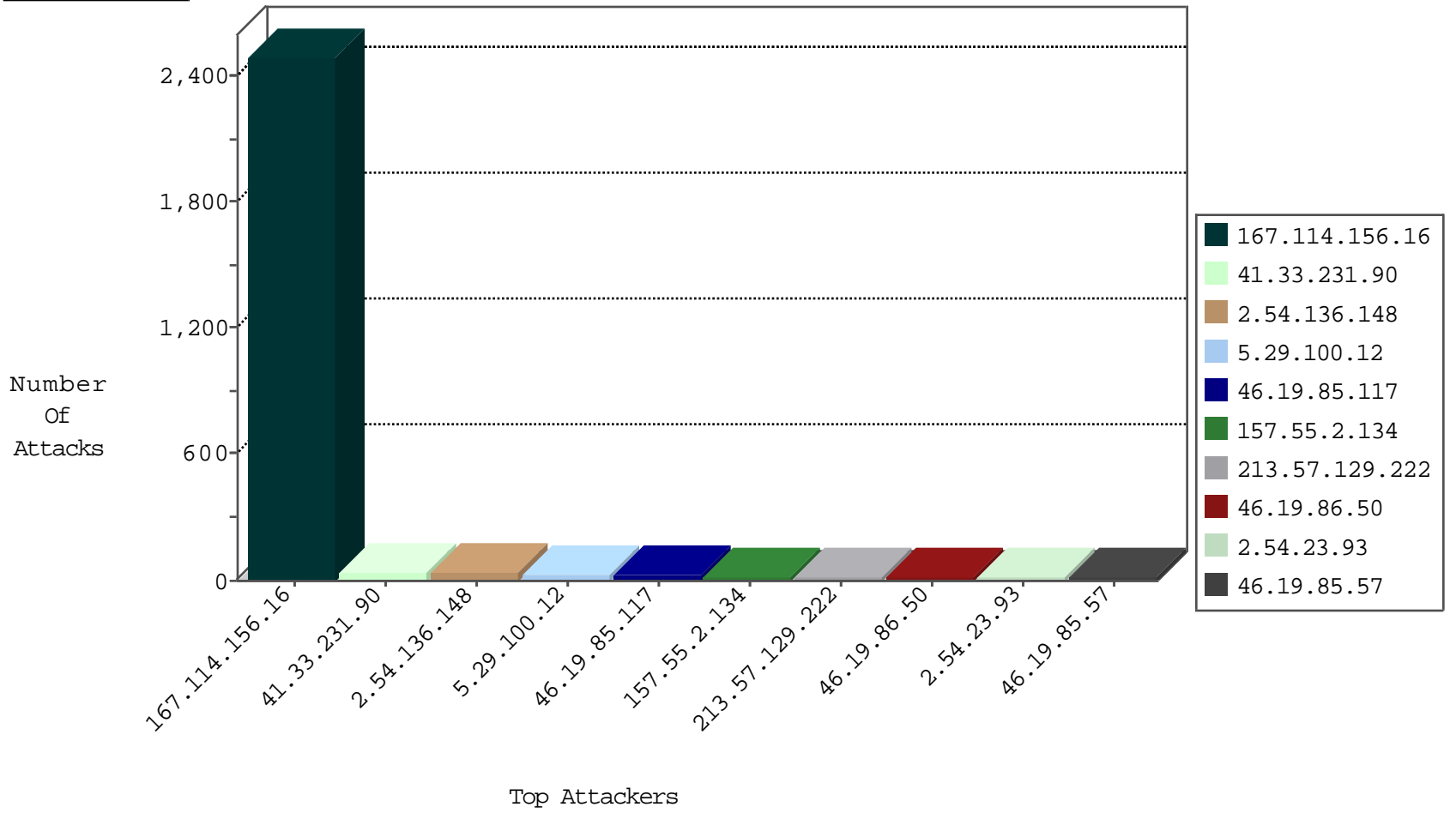
IDF Under Attack Daily Report



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	doover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3606
14.121.178.196	China	147.237.76.148	ggcenter.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
202.112.51.96	China	147.237.77.235	sviva.idf.il	block-sp-traf1	drop	1
93.174.93.151	Netherlands	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
93.174.93.151	Netherlands	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
192.3.170.124	United States	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
94.102.49.210	Netherlands	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
192.3.170.124	United States	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
93.174.93.151	Netherlands	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
94.102.49.210	Netherlands	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.165.15.152	France	147.237.77.74	law.idf.il	C228: HTTP: AhrefBot crawler	Block	1
195.154.188.74	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	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	4
171.232.56.152	147.237.0.17	Vietnam	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	3
114.134.189.13	147.237.77.216	Cambodia	dover.idf.il	portscan: TCP Distributed Portscan	1
104.192.0.226	147.237.77.176	United States	matpash.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.131	147.237.72.14	Canada	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
79.174.70.237	147.237.77.121	Russian Federation	e.navy.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.177	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
14.121.178.196	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
199.101.186.201	147.237.76.201	United States	e.atal.idf.il	ET SCAN NMAP -sS window 4096	1
178.152.30.178	147.237.8.50	Qatar	e.tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
162.248.54.64	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
104.192.0.226	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
104.192.0.226	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
104.128.144.131	147.237.8.28	Canada	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 4096	1
75.145.81.98	147.237.0.35	United States	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
157.55.2.134	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
2.54.23.93	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
100.100.77.252		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.54.136.148	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	8
2.54.136.148	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.86.181	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.141.245	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.29.100.12	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.86.181	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.160.90	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.129.222	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
46.19.85.57	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
199.203.215.1	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.182	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
213.57.129.222	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.57	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.147.198	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.182	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
213.57.129.222	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.136.148	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.29.100.12	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
2.54.136.148	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
2.54.55.212	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.52.151.234	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
80.246.137.98	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.54.136.148	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.52.178.140	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
5.29.100.12	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
5.29.100.12	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence		monitor	4
109.186.12.40	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
149.78.51.107	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
100.100.35.21		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
37.26.149.239	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.29.100.12	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
109.64.32.54	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.80.196.44	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.207	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.136.183	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
213.57.131.120	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
2.52.184.56	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
109.66.21.245	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.50.235	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.58	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.129.101	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.54.136.148	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
5.29.100.12	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.117	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
46.19.86.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
176.13.15.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
46.19.85.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.85.84	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
176.13.7.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.12.138.214	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
46.19.85.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.148.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.18.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.86	Israel	147.237.0.19	madim.atal.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/1133-22638-he/dover.aspx.	Block	2
80.246.136.238	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.86.204	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
66.249.66.28	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
212.76.106.136	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
114.134.189.13	Cambodia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
84.109.32.5	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
197.37.10.159	Egypt	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/xmlrpc.php	Block	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
2.54.8.140	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.17	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
46.19.86.233	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.46.13.119	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2003/september/09.stm).	Block	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
5.29.146.75	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
194.90.15.61	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation pageNum in www.idf.il/1414-he/dover.aspx	Block	1
66.249.66.31	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
176.12.149.238	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
212.143.40.198	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
114.134.189.13	Cambodia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
85.158.181.29	Austria	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refuah.atal.idf.il/blog/wp-admin/	Block	1
37.26.148.254	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
197.37.10.159	Egypt	147.237.77.233	atal.idf.il	PHP Attempt	Block	1
176.13.19.137	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/main/rabanut/general.aspx	None	1
2.54.56.212	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.155	United States	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 157.55.39.155	Block	1
54.162.124.221	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
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	1
108.30.189.83	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
31.154.92.63	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
197.37.10.159	Egypt	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
79.177.132.141	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.66.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-16893-he/dover.aspx	Block	1
2.52.56.65	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.12.149.238	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
124.73.7.208	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1043-11784-ar/cogat.aspx/trackback/	Block	1
46.19.86.54	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1