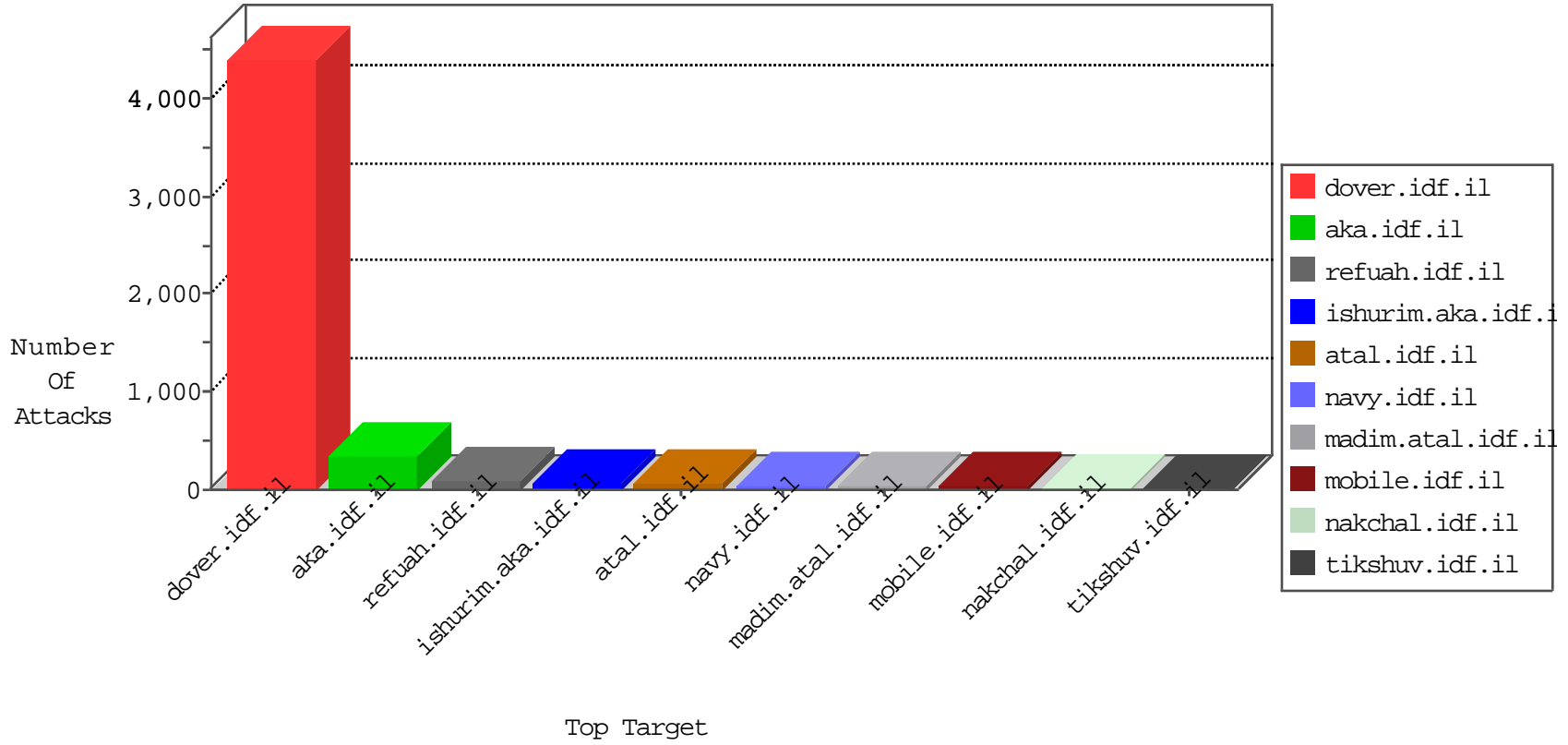


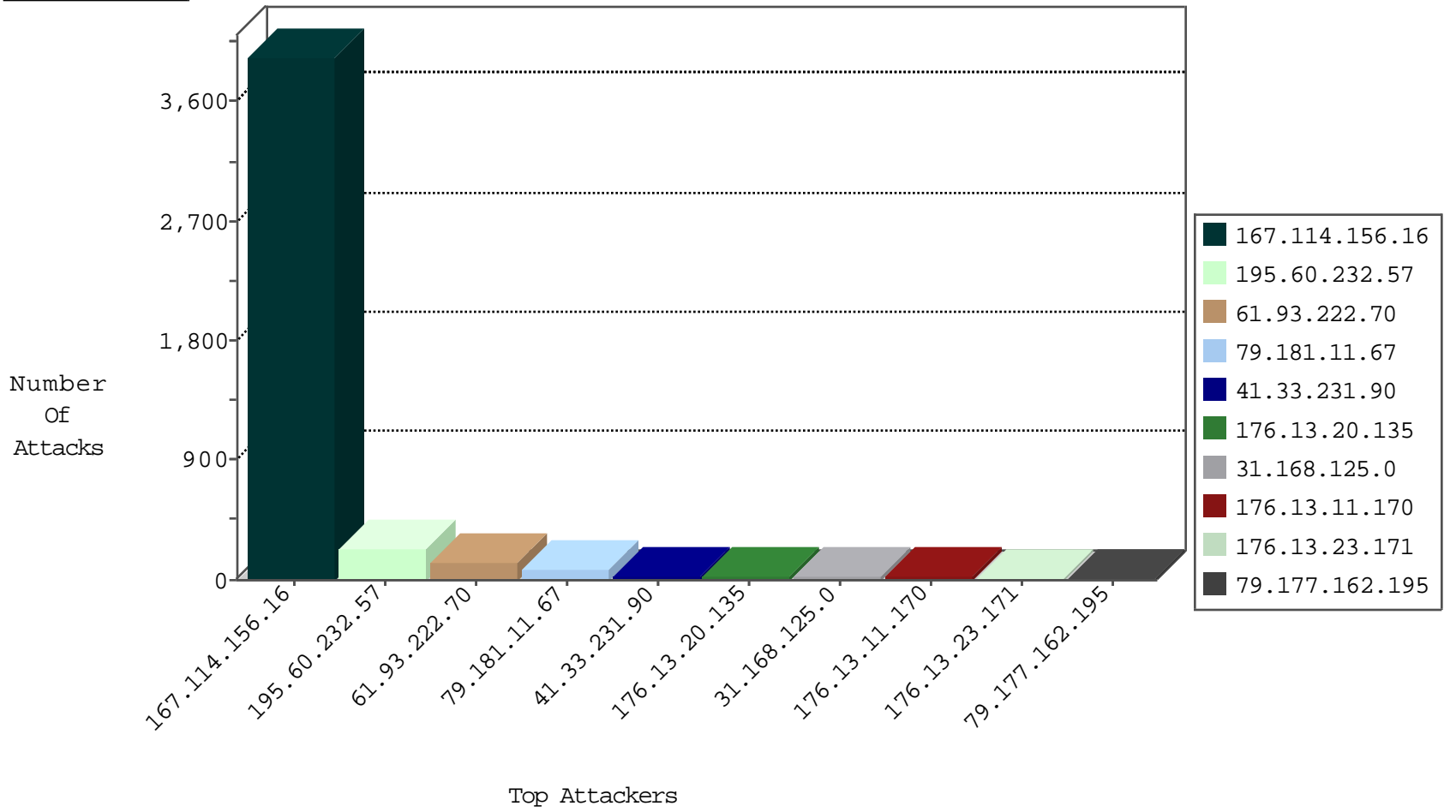
IDF Under Attack Daily Report



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	Block_Tp_Web_In	drop	3926
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	82
101.201.147.32	China	147.237.76.86	navy.idf.il	block-sp-traf1	forward	2
184.105.139.117	United States	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	1
74.82.47.17	United States	147.237.77.179	e.mazi.idf.il	Block_Udp_All_Nets	drop	1
173.49.100.3	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
176.77.32.221	Russian Federation	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Http	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
104.148.71.133	United States	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
176.77.32.221	Russian Federation	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Http	drop	1
71.6.146.185	United States	147.237.0.35	akaws.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
134.119.5.86	Germany	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
66.249.66.184	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
69.30.234.186	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
2.55.24.223	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.66.187	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
69.30.234.186	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	1
36.110.147.67	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.102.9.81	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
195.60.232.57	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.116.27.36	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.78.28.153	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
13.92.246.145	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 4096	1
109.253.226.93	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.55.165.189	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
104.219.238.10	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 1024	1
2.53.143.241	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
95.86.97.230	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.210.245	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.71.79.157	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.8.124.232	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.65.116.235	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.117.140.170	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.219.214	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.74	147.237.76.38	United States	e.e.meitav.idf.il	ET DROP Dshield Block Listed Source	1
62.219.172.178	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
46.19.86.46	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.50.47.210	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.102.242.111	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.64.226.163	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.160.75	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.219.238.10	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
219.85.47.157	147.237.8.27	Taiwan	e.madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
94.230.86.185	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.8.204.45	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.69.135.185	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.94.38.240	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.98	147.237.77.243	United States	mobile.idf.il	ET DROP Dshield Block Listed Source	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
195.60.232.57	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	211
79.181.11.67	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	75
61.93.222.70	Hong Kong	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	57
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	29
61.93.222.70	Hong Kong	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	27
5.22.130.75	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.85.16	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	15
61.93.222.70	Hong Kong	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	13
176.13.23.171	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
109.66.51.73	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.176.117.169	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
195.60.232.57	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
109.253.142.208	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.177.162.195	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
79.177.162.195	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
79.178.16.200	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
200.68.136.136	Mexico	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
31.168.125.0	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
31.168.125.0	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
200.68.136.136	Mexico	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
61.93.222.70	Hong Kong	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	7
109.64.238.204	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.168.172.179	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.102.242.80	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.186.0.115	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.101.129	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.56.249	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
54.217.220.236	Ireland	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.156.122	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.117.136.6	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
165.171.240.45	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
93.172.23.123	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
105.44.30.249	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
185.3.147.109	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.26.148.251	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		alert	4
5.28.172.80	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.3.157	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.135.162	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
185.32.179.219	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
178.255.215.87	France	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.127.144.68	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.59.52	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
176.13.7.139	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.197	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.146.22	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.71.23.149	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.130.87	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.20.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
176.13.11.170	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 176.13.11.170	Block	17
87.68.18.167	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	11
176.13.7.208	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	5
176.13.19.226	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
81.218.251.250	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	5
80.246.130.222	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/contactus.aspx	Block	5
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	4
31.168.125.0	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
65.55.210.112	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
46.19.86.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.7.71	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
61.93.222.70	Hong Kong	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/shared/usercontrols/headerupper/	Block	2
80.246.133.154	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
61.93.222.70	Hong Kong	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/shared/usercontrols/headerupper/	Block	2
176.13.10.230	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on www.refua.atal.idf.il/templates/general/mobile	Block	2
61.93.222.70	Hong Kong	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 61.93.222.70	Block	2
82.81.31.204	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
2.53.139.3	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
61.93.222.70	Hong Kong	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	2
79.178.16.200	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
149.78.23.55	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 149.78.23.55	Block	2
87.69.225.228	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
109.253.142.208	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
85.65.116.235	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 103 cookies	Block	1
46.19.86.18	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
199.30.25.73	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
176.13.15.203	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/	Block	1
79.178.16.200	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
157.55.12.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.116.29.253	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/nakhal	Block	1
87.69.225.228	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 87.69.225.228	Block	1
46.19.85.194	Israel	147.237.76.42	refuah.idf.il	Illegal HTTP Version	Block	1
185.5.223.250	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 185.5.223.250	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/1/3141.jpg	Block	1
138.134.102.16	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	1
46.19.86.58	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/news/mobile	Block	1
199.30.25.125	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
37.26.146.197	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.180.150.131	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00\$ctl00\$cphMain\$cphSachar\$cb14641110 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
157.55.39.81	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
61.93.222.70	Hong Kong	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/main/sachar/faq.aspx	None	1
95.86.83.172	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/resource/userfollowresource/create/	Block	1
46.19.85.194	Israel	147.237.76.42	refuah.idf.il	Malformed URL he-il,he;q=0.8,en-us;q=0.6,en;q=0.4	Block	1
192.116.172.24	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/7/70517.pdf	Block	1
2.53.29.241	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/general/mobile	Block	1
141.212.122.81	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to /x	Block	1
87.68.18.167	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 87.68.18.167	Block	1