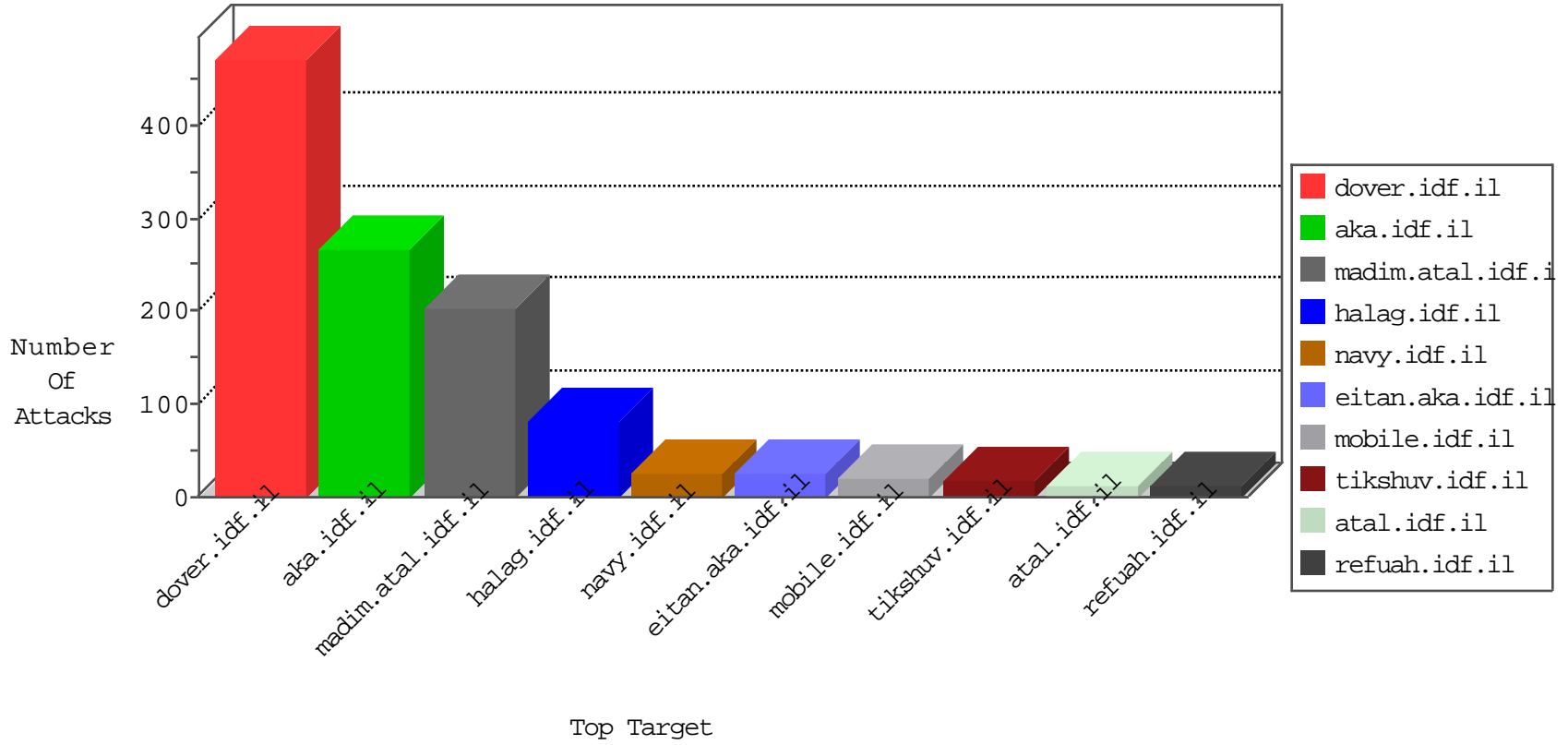


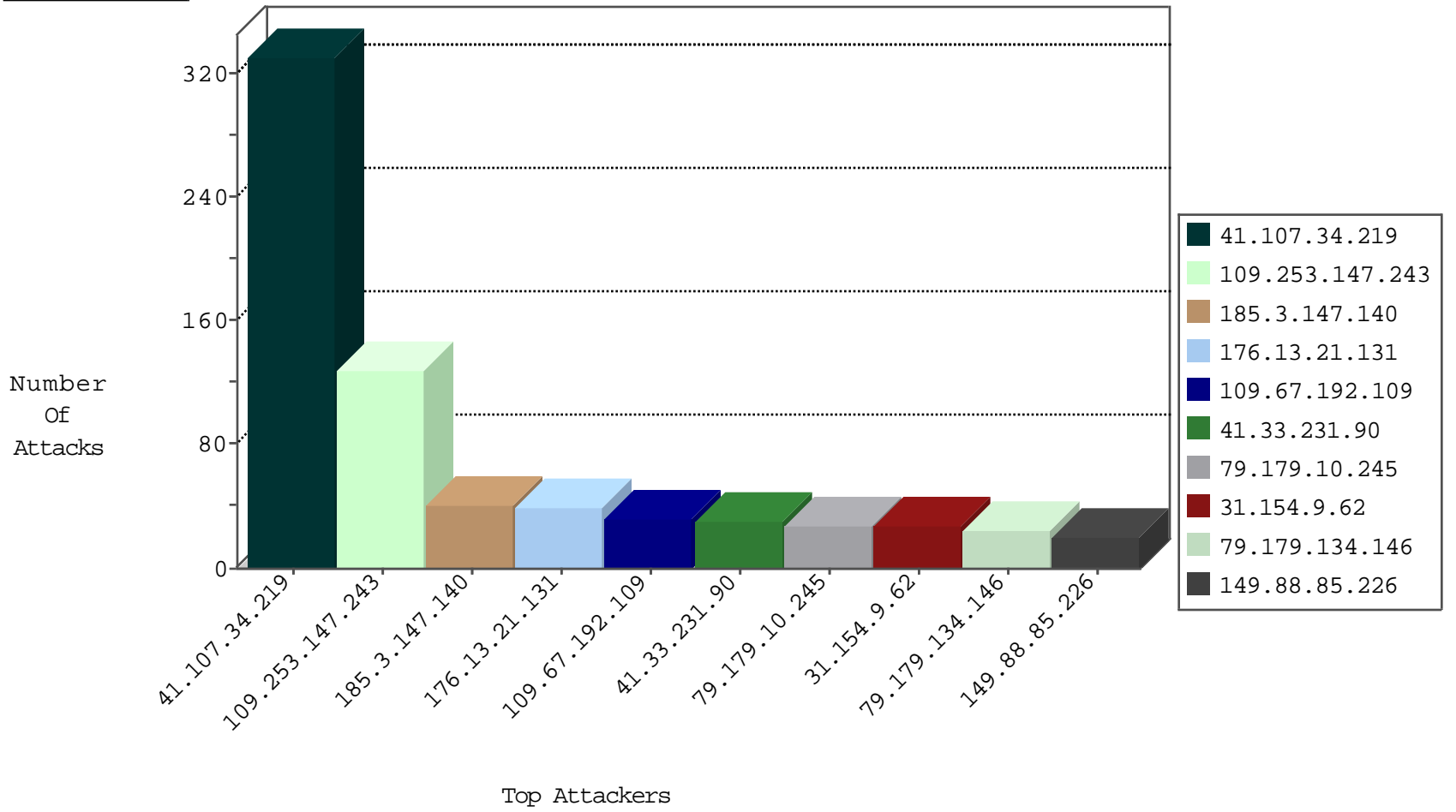
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.107.34.219	Algeria	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	256
79.180.120.16	Israel	147.237.72.156	anan.idf.il	Block_Udp_All_Nets	drop	6
31.168.240.21	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
185.94.111.1		147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
41.206.63.131	Kenya	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1
198.23.190.39	United States	147.237.8.50	e.tikshuv.idf.il	Block_Ntp_All_Net	drop	1
208.100.26.228	United States	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
196.200.16.200	Kenya	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1
41.206.63.133	Kenya	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1
208.100.26.228	United States	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
146.185.239.100	Russian Federation	147.237.77.74	law.idf.il	block-sp-traf1	drop	1
208.100.26.228	United States	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
196.200.16.201	Kenya	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
208.100.26.228	United States	147.237.76.148	ggcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1		147.237.0.15	kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
41.206.63.130	Kenya	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1
208.100.26.228	United States	147.237.77.19	law-forum.idf.il	Block_Ntp_All_Net	drop	1
196.200.16.202	Kenya	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1
74.218.110.4	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
208.100.26.228	United States	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.173.238.73	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
2.54.165.99	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
199.30.24.153	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
61.135.189.103	China	147.237.77.216	doover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	2
51.255.65.41	United Kingdom	147.237.77.170	maarachot.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.83	United Kingdom	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.49	United Kingdom	147.237.77.170	maarachot.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.88	United Kingdom	147.237.77.170	maarachot.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.6	United Kingdom	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
207.46.13.145	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
51.255.65.52	United Kingdom	147.237.77.170	maarachot.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.93	United Kingdom	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.15	United Kingdom	147.237.77.170	maarachot.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.60	United Kingdom	147.237.77.170	maarachot.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.31	United Kingdom	147.237.77.170	maarachot.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.71	United Kingdom	147.237.77.170	maarachot.idf.il	C1000146: HTTP: AhrefBot crawler	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
93.174.93.144	147.237.77.176	Netherlands	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.113	147.237.76.196	Ukraine	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.37	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
31.211.102.129	147.237.76.176	Russian Federation	test.ncore.idf.il	ET SCAN NMAP -sS window 4096	1
180.97.106.36	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
5.58.76.88	147.237.0.17	Ukraine	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.144	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.144	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.144	147.237.8.27	Netherlands	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.79.104	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	1
180.97.106.36	147.237.77.205	China	prisha.idf.il	ET SCAN Potential SSH Scan	1
14.136.39.163	147.237.8.28	Hong Kong	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
115.28.218.77	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
5.58.76.88	147.237.0.15	Ukraine	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.144	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.107.34.219	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	71
185.3.147.140	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	30
79.179.10.245	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
31.154.9.62	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	26
149.88.85.226	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
109.67.192.109	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
109.67.192.109	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	15
79.179.134.146	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
109.253.209.86	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.173.23.55	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.179.134.146	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
37.26.149.163	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.143.220.82	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
79.179.60.180	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.253.140.202	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
185.3.147.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.176.116.219	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
109.253.140.202	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.65.26.210	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
31.210.187.199	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.64.57.241	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.86.19	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
185.3.147.140	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.65.61.21	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.211	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
79.176.162.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.252	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.252	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
5.29.39.29	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.65.159.177	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
79.179.131.231	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.8.86	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
185.3.147.185	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
82.81.56.54	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.125.5		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.171.122	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.106.230.106	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.76.127.111	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
212.143.238.242	Israel	147.237.77.176	natpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
79.178.96.156	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.96.239	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.126.56		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.89	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.85.136	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
149.88.123.49	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.147.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	127
176.13.21.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
176.13.14.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
37.26.149.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
176.13.9.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	5
2.54.161.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
87.69.250.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.120.126.5		147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	2
2.54.3.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.120.231.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
212.76.102.106	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.76.102.106	Block	2
213.8.204.40	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-en/dover.aspx	Block	2
162.243.72.220	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 162.243.72.220	Block	2
66.249.81.212	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
162.243.72.220	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
109.65.26.210	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
77.126.100.74	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
185.82.200.91		147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
27.3.26.25	Vietnam	147.237.77.216	dover.idf.il	Parameter Type Violation lang in www.idf.il/templates/navmenu/navmenu.css.aspx	Block	1
149.78.18.15	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
91.69.66.105	France	147.237.77.216	dover.idf.il	Parameter Type Violation id in www.idf.il/1294-en/dover.aspx	Block	1
213.57.235.106	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
194.90.128.185	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 194.90.128.185	Block	1
66.249.81.218	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
37.26.149.163	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
2.54.63.176	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
109.67.192.109	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
79.179.10.245	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
46.121.107.15	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/controls/atuda/	Block	1
185.82.200.91		147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
31.13.113.64	Ireland	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
157.55.39.39	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
94.159.168.128	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
199.30.24.218	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.112	Block	1
41.107.34.219	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
109.253.132.51	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/size220x0/sip_storage	Block	1
212.76.102.106	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/hinuch	Block	1
83.220.238.197	Russian Federation	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
65.55.210.119	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
185.120.125.5		147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012ources/images/innerpage/goback.gif	Block	1
157.55.39.106	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
37.26.146.192	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
105.155.28.85	Morocco	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
207.46.13.180	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1393-en/dover.aspx	Block	1
46.19.85.136	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
2.54.161.158	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1432	Block	1