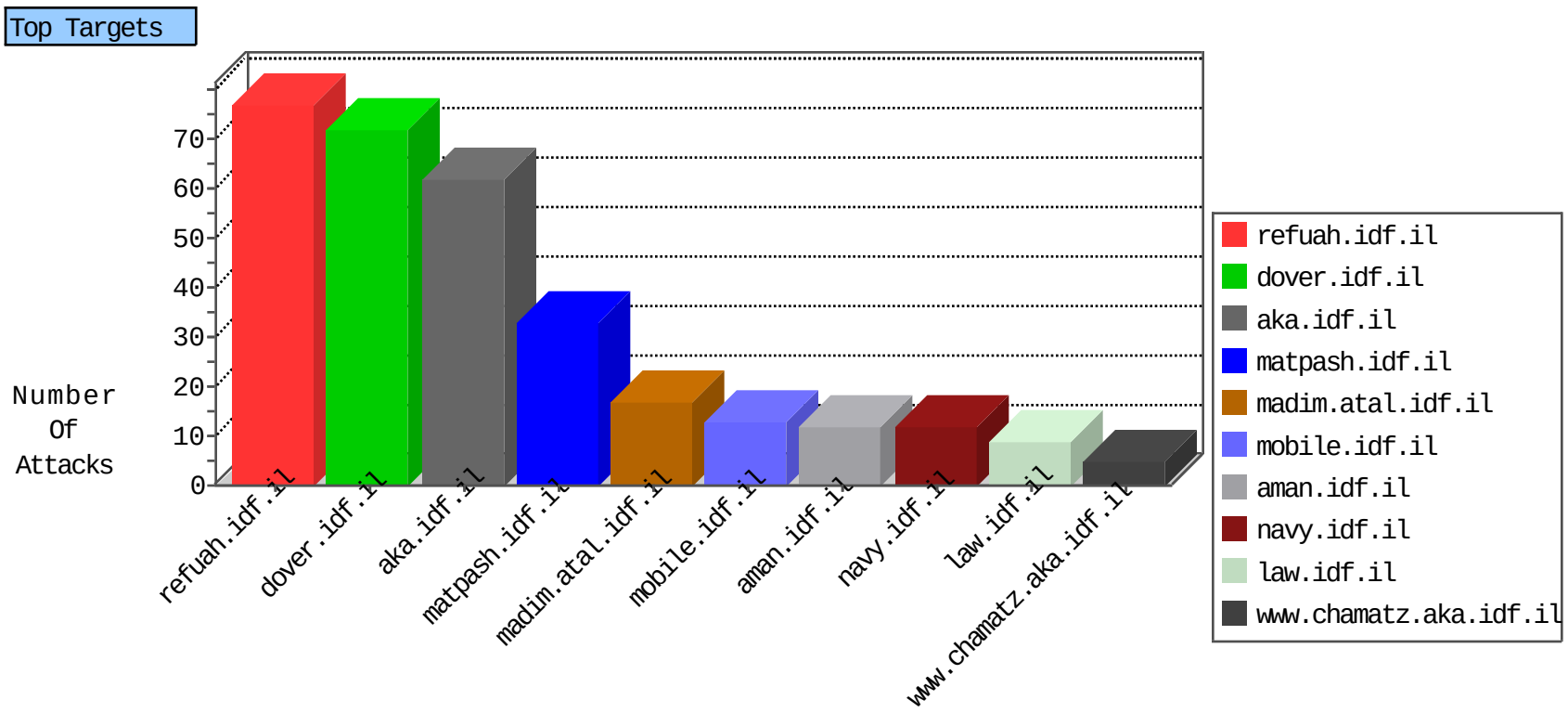
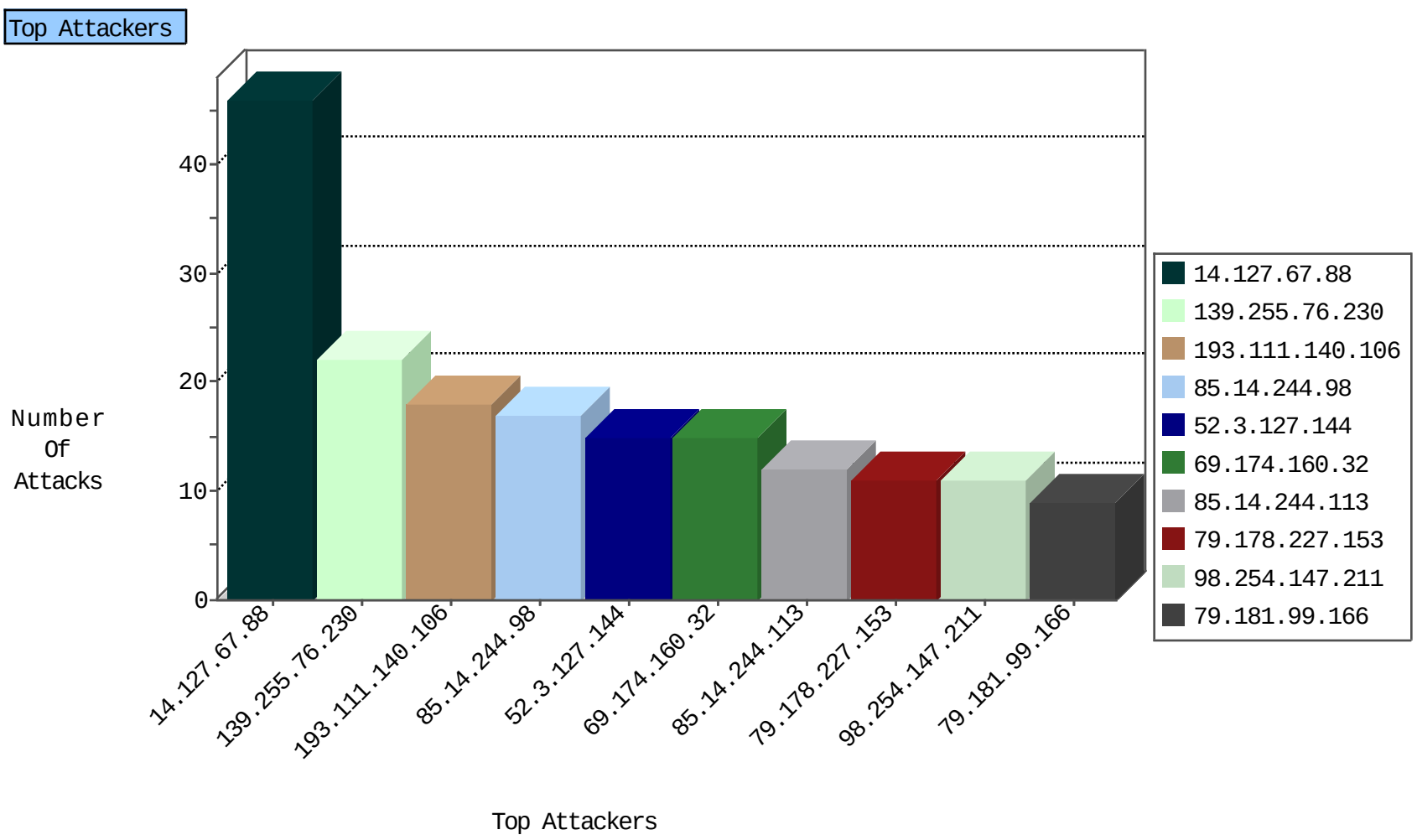
10-02-2016-07:04:04 to 10-02-2016-08:04:04

IDF Under Attack Daily Report





10-02-2016-07:04:04 to 10-02-2016-08:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.187.118.18	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	2
192.187.109.59	United States	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	2
192.187.118.68	United States	147.237.76.86	navy.idf.il	block-sp-traf1	forward	2
63.141.231.211	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	2
198.204.255.76	United States	147.237.76.30	himush.idf.il	block-sp-traf1	forward	2
63.141.231.213	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	2
173.208.198.10	United States	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	1
69.30.193.254	United States	147.237.72.156	aman.idf.il	block-sp-traf1	forward	1
173.208.213.198	United States	147.237.77.233	atal.idf.il	block-sp-traf1	forward	1
142.54.180.66	United States	147.237.77.170	maarachot.idf.il	block-sp-traf1	forward	1
63.141.242.194	United States	147.237.77.74	law.idf.il	block-sp-traf1	forward	1
192.187.118.20	United States	147.237.76.31	nakchal.idf.il	block-sp-traf1	forward	1
173.208.198.12	United States	147.237.77.216	dover.idf.il	block-sp-traf1	forward	1
69.30.226.219	United States	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	forward	1
37.186.206.220	Italy	147.237.77.205	prisha.idf.il	L4 Source or Dest Port Zero	drop	1
142.54.180.67	United States	147.237.72.166	aka.idf.il	block-sp-traf1	forward	1
63.141.250.157	United States	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	1
173.208.207.133	United States	147.237.77.176	matpash.idf.il	block-sp-traf1	forward	1
93.174.94.235	Netherlands	147.237.76.31	nakchal.idf.il	Black List	drop	1
192.187.109.59	United States	147.237.77.234	halag.idf.il	block-sp-traf1	forward	1
142.54.180.70	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	forward	1
69.30.193.250	United States	147.237.77.235	sviva.idf.il	block-sp-traf1	forward	1
173.208.207.134	United States	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	1
93.174.94.235	Netherlands	147.237.76.196	e.sviva.idf.il	Black List	drop	1

10-02-2016-07:04:04 to 10-02-2016-08:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.14.244.98	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	11
193.111.140.106	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	9
85.14.244.113	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	7
193.111.140.106	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	5
85.14.244.98	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	5
85.14.244.113	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	3
193.111.140.106	Germany	147.237.77.226	www.chamatz.aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
162.210.196.97	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
62.212.73.211	Netherlands	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	2
85.14.244.113	Germany	147.237.76.42	refuah.idf.il	C1000074: HTTP: majestic bot	Permit	1
193.111.140.106	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	1
85.14.244.113	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	1
85.14.244.98	Germany	147.237.76.42	refuah.idf.il	C1000074: HTTP: majestic bot	Permit	1

10-02-2016-07:04:04 to 10-02-2016-08:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.76.108	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
62.210.113.73	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
46.172.91.21	147.237.77.243	Ukraine	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
14.152.59.11	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
13.75.43.42	147.237.0.34	Hong Kong	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
208.100.26.228	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1
125.65.82.44	147.237.77.121	China	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.8.46	Ukraine	e.chinuch.idf.il	ET SCAN NMAP -sS window 3072	1
54.144.119.103	147.237.0.15	United States	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1
46.172.91.21	147.237.77.235	Ukraine	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
13.75.43.42	147.237.76.38	Hong Kong	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
208.100.26.228	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
125.65.82.44	147.237.77.235	China	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
93.114.183.170	147.237.8.45	Romania	e.eitan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.201.236.155	147.237.8.46	Ukraine	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1

10-02-2016-07:04:04 to 10-02-2016-08:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
52.3.127.144	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	15
98.254.147.211	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
176.13.233.27	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
69.174.160.32	United States	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	4
139.255.76.230	Indonesia	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
139.255.76.230	Indonesia	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	4
139.255.76.230	Indonesia	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
69.174.160.32	United States	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	3
69.174.160.32	United States	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.253.132.207	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
37.26.146.192	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
139.255.76.230	Indonesia	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	3
69.174.160.32	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
91.121.109.55	France	147.237.77.74	law.idf.il	drop	SAM rule	drop	2
77.138.64.24	France	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
141.226.218.18	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
139.255.76.230	Indonesia	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
91.121.109.55	France	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	2
24.4.50.221	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
79.181.99.166	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
139.255.76.230	Indonesia	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
84.229.12.142	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
84.229.12.142	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
5.29.225.95	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
79.178.62.55	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
46.116.44.203	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
98.109.176.53	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
24.4.50.221	United States	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	2
79.181.99.166	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
69.174.160.32	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
84.229.12.142	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
79.181.99.166	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	2
139.255.76.230	Indonesia	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	2
176.106.46.74	Palestinian Territory, Occupied	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
41.37.67.148	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
184.105.247.226	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
79.181.99.166	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
163.172.220.201	United Kingdom	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
24.4.50.221	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
74.82.47.7	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
62.210.243.100	France	147.237.72.14	dover.idf.il(old)	drop	SAM rule	drop	1
98.109.176.53	United States	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	1
185.40.66.32	Ireland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	1
24.29.81.144	United States	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	1
184.105.139.79	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
218.22.211.69	China	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
46.19.85.157	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.40.66.32	Ireland	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

10-02-2016-07:04:04 to 10-02-2016-08:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
14.127.67.88	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 14.127.67.88	Block	17
14.127.67.88	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 14.127.67.88	Block	16
79.178.227.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
14.127.67.88	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	6
14.127.67.88	China	147.237.77.176	matpash.idf.il	PHP Attempt	Block	6
80.178.191.219	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 80.178.191.219	Block	5
77.138.67.71	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	4
2.53.138.51	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.138.67.71	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar	Block	2
46.19.85.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
109.63.239.42	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/pniotanswer.aspx	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/tizmoret/gallery/	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/default.aspx	Block	1
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.51	Block	1
176.13.233.27	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
80.122.66.42	Austria	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
14.127.67.88	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.asp	Block	1
85.64.151.190	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$cb15038310 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.65.52	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.52	Block	1
176.106.46.74	Palestinian Territory, Occupied	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/homepage/homepage.aspx	Block	1
66.249.76.79	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
85.65.233.40	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/kiosk/kiosk.aspx	Block	1
77.138.233.210	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
66.249.66.103	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/departmentslobby/departmentslobby.aspx	Block	1
207.46.13.102	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
80.246.133.60	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
68.180.231.60	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1043-he/cogat.aspx	Block	1
46.121.247.107	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
106.38.241.106	China	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
77.139.66.30	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar	Block	1
66.249.75.167	Israel	147.237.77.74	law.idf.il	Parameter Type Violation SearchText in www.law.idf.il/163-6639-he/patzar.aspx	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/default.aspx	Block	1
76.91.33.211	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/general.aspx	Block	1

10-02-2016-07:04:04 to 10-02-2016-08:04:04