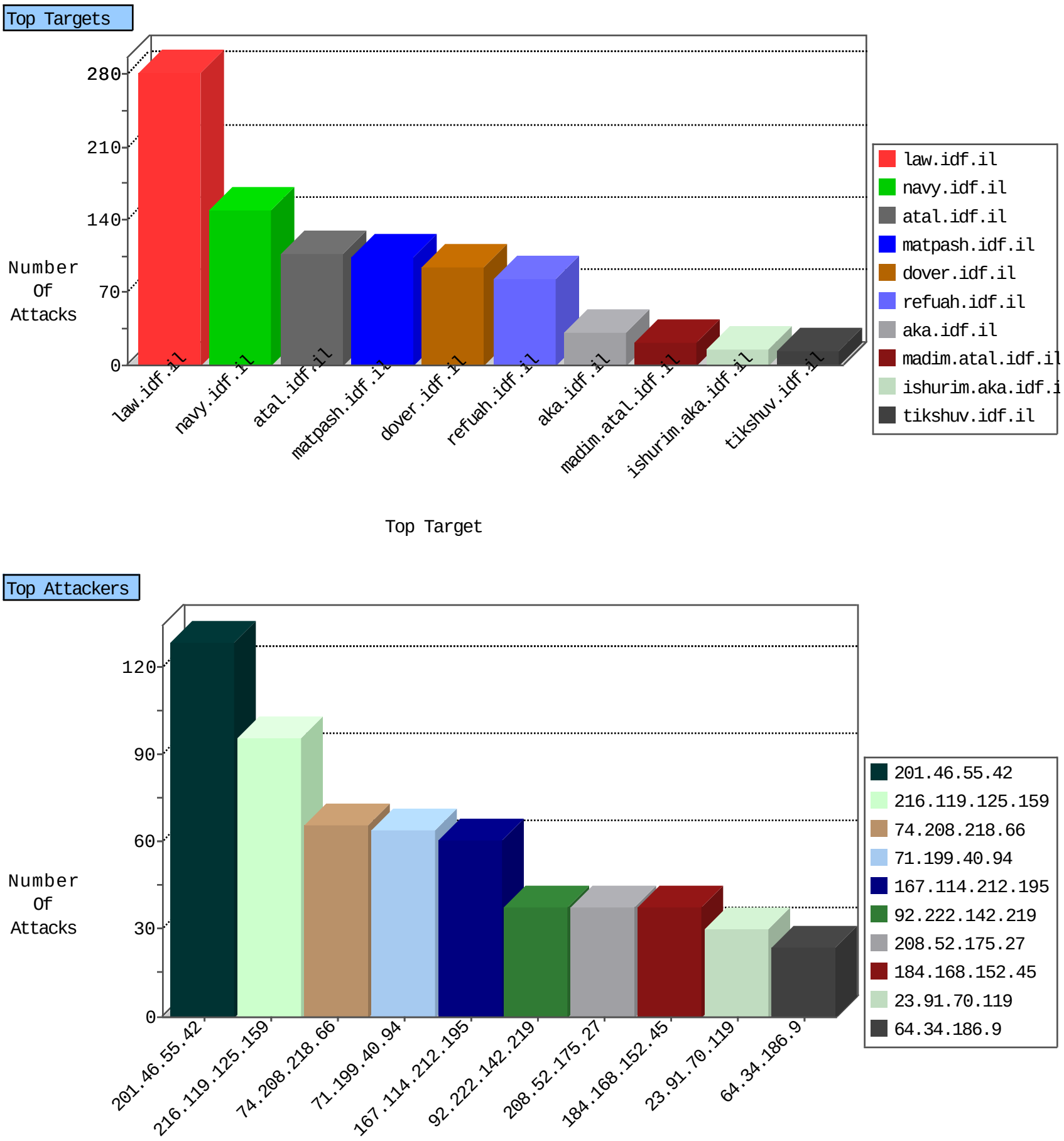
09-05-2016-06:04:05 to 09-05-2016-07:04:05

IDF Under Attack Daily Report



09-05-2016-06:04:05 to 09-05-2016-07:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.236.84.10	Netherlands	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.30	himush.idf.il	Black List	drop	1
80.82.65.168	Netherlands	147.237.76.197	e.himush.idf.il	Black List	drop	1

09-05-2016-06:04:05 to 09-05-2016-07:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
216.119.125.159	United States	147.237.77.176	matpash.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
92.222.142.219	France	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
74.208.218.66	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
208.52.175.27	United States	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	11
208.52.175.27	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	7
216.119.125.159	United States	147.237.77.176	matpash.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
177.12.161.72	Brazil	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
23.91.70.119	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
87.117.203.23	United Kingdom	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
184.168.152.45	United States	147.237.77.216	dover.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
49.236.200.182	Malaysia	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
92.222.142.219	France	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
216.119.125.173	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
184.168.152.45	United States	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
50.63.196.35	United States	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
212.147.60.96	Switzerland	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
184.168.152.45	United States	147.237.77.216	dover.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
74.208.218.66	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
216.119.125.159	United States	147.237.77.176	matpash.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
121.40.25.174	China	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
23.91.70.43	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
195.154.232.58	France	147.237.76.42	refuah.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1

09-05-2016-06:04:05 to 09-05-2016-07:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
216.119.125.159	147.237.77.176	United States	matpash.idf.il	SQL Injection - Select From	72
74.208.218.66	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	48
23.91.70.119	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	24
92.222.142.219	147.237.76.42	France	refuah.idf.il	SQL Injection - Select From	20
208.52.175.27	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	20
184.168.152.45	147.237.77.216	United States	dover.idf.il	SQL Injection - Select From	20
177.12.161.72	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	18
23.91.70.43	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	18
204.93.196.218	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	9
49.236.200.182	147.237.77.74	Malaysia	law.idf.il	SQL Injection - Select From	8
87.117.203.23	147.237.77.74	United Kingdom	law.idf.il	SQL Injection - Select From	8
50.63.196.35	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	8
121.40.25.174	147.237.77.74	China	law.idf.il	SQL Injection - Select From	8
212.147.60.96	147.237.77.74	Switzerland	law.idf.il	SQL Injection - Select From	8
216.119.125.173	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	6
121.40.25.174	147.237.77.216	China	dover.idf.il	SQL Injection - Select From	5
213.203.204.143	147.237.77.74	Germany	law.idf.il	SQL Injection - Select From	5
50.77.136.81	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	5
91.121.71.132	147.237.77.74	France	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	4
172.98.198.49	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 4096	1
115.45.132.120	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.201.236.155	147.237.72.167	Ukraine	ishurim.aka.idf.il	ET SCAN NMAP -sS window 4096	1
91.201.236.155	147.237.72.167	Ukraine	ishurim.aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
208.100.26.228	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sS window 1024	1
71.86.124.86	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -f -sS	1
172.98.198.49	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 3072	1
23.91.75.231	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.72.167	Ukraine	ishurim.aka.idf.il	ET SCAN NMAP -sS window 3072	1
83.18.88.163	147.237.8.28	Poland	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
71.86.124.86	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 2048	1

09-05-2016-06:04:05 to 09-05-2016-07:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.185.12.173	South Africa	147.237.77.216	dover.idf.il	drop	SAM rule	drop	18
213.60.255.71	Spain	147.237.77.233	atal.idf.il	drop	SAM rule	drop	18
64.34.186.9	United States	147.237.76.86	navy.idf.il	drop	SAM rule	drop	18
173.198.251.2	United States	147.237.76.86	navy.idf.il	drop	SAM rule	drop	18
79.170.196.68	United Kingdom	147.237.77.74	law.idf.il	drop	SAM rule	drop	16
71.199.40.94	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
71.199.40.94	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	14
71.199.40.94	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	13
217.132.123.77	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
83.168.250.50	Sweden	147.237.77.74	law.idf.il	drop	SAM rule	drop	12
71.199.40.94	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
71.199.40.94	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	10
46.19.86.138	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
201.46.55.42	Brazil	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
69.158.58.23	Canada	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
201.46.55.42	Brazil	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
79.170.196.68	United Kingdom	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
50.63.197.11	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
201.46.55.42	Brazil	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
158.69.119.162	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	6
81.176.226.68	Russian Federation	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	6
201.46.55.42	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
201.46.55.42	Brazil	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
97.74.215.197	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
74.84.136.105	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	6
158.85.253.245	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	6
201.46.55.42	Brazil	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
64.34.186.9	United States	147.237.77.233	atal.idf.il	drop	SAM rule	drop	6
98.19.222.133	United States	147.237.77.233	atal.idf.il	drop	SAM rule	drop	6
201.46.55.42	Brazil	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
201.46.55.42	Brazil	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
98.194.194.25	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
201.46.55.42	Brazil	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
201.46.55.42	Brazil	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
201.46.55.42	Brazil	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
201.46.55.42	Brazil	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
98.194.194.25	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
201.46.55.42	Brazil	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
201.46.55.42	Brazil	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
73.148.127.249	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
201.46.55.42	Brazil	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
201.46.55.42	Brazil	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
201.46.55.42	Brazil	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
73.148.127.249	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	4
167.114.212.195	Canada	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
201.46.55.42	Brazil	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
167.114.212.195	Canada	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
98.194.194.25	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	4
167.114.212.195	Canada	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
73.148.127.249	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4

09-05-2016-06:04:05 to 09-05-2016-07:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.151.32.163	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 213.151.32.163	Block	4
84.95.208.20	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	3
84.95.208.20	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
138.134.192.10	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	1
66.249.69.119	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
213.151.32.163	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	1
131.253.26.250	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
46.116.92.29	Israel	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	1
139.162.13.205	Singapore	147.237.77.233	atal.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.69.123	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/tizmoret/gallery/showpicture.asp	Block	1
217.132.123.77	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	1
131.253.27.46	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
67.82.251.214	United States	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
65.55.211.243	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
157.55.39.89	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
84.95.208.20	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/general/piwik.php	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
131.253.36.203	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
75.82.117.252	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
66.249.69.93	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/935-4489-he/patzar.aspx	Block	1
157.55.39.201	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
131.253.24.146	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
2.53.174.3	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/960.css	Block	1
131.253.36.206	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
80.250.159.14	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
66.249.69.97	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/942-he/patzar.aspx	Block	1
131.253.26.237	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.76.79	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	Block	1
40.77.167.76	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19149-he/dover...	Block	1

09-05-2016-06:04:05 to 09-05-2016-07:04:05