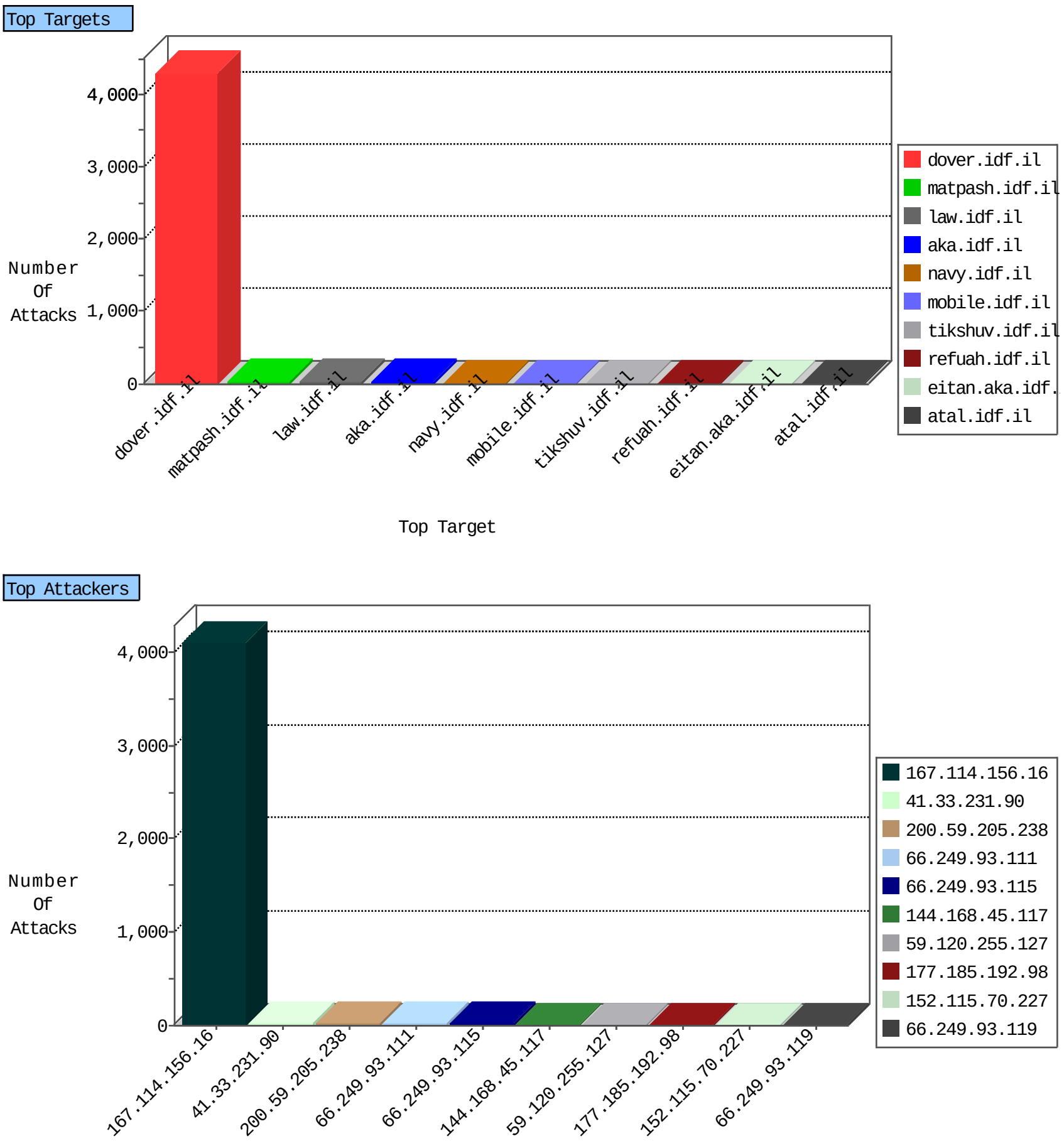
04-17-2016-05:04:09 to 04-17-2016-06:04:09

IDF Under Attack
Daily Report



04-17-2016-05:04:09 to 04-17-2016-06:04:09

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_Ip_Web_In	drop	4108
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.96	United States	147.237.0.34	tikshuv.idf.il	Block_Ntp_All_Net	drop	1
179.43.141.194	Switzerland	147.237.72.217	e.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.76	United States	147.237.77.179	e.mazi.idf.il	Block_Ntp_All_Net	drop	1
134.147.203.115	Germany	147.237.72.156	aman.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.100	United States	147.237.8.50	e.tikshuv.idf.il	Block_Ntp_All_Net	drop	1
179.43.141.194	Switzerland	147.237.77.176	matpash.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.84	United States	147.237.8.24	e.lifestyle.idf.il	Block_Ntp_All_Net	drop	1
184.105.247.224	United States	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	1
180.153.235.242	China	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.88	United States	147.237.72.156	aman.idf.il	Block_Ntp_All_Net	drop	1
179.43.141.194	Switzerland	147.237.72.156	aman.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.76	United States	147.237.77.178	e.matpash.idf.il	Block_Ntp_All_Net	drop	1

04-17-2016-05:04:09 to 04-17-2016-06:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
59.120.255.127	Taiwan	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
177.185.192.50	Brazil	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
177.185.192.98	Brazil	147.237.77.216	dover.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
200.59.205.238	Argentina	147.237.77.176	matpash.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
200.59.205.238	Argentina	147.237.77.176	matpash.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
152.115.70.227	Denmark	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
70.89.127.78	United States	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	3
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
144.168.45.117	United States	147.237.76.42	refuah.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1
144.168.45.117	United States	147.237.0.15	kosher-kravi.idf.i	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1
144.168.45.117	United States	147.237.76.147	chinuch.aka.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
144.168.45.117	United States	147.237.0.19	madim.atal.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1
144.168.45.117	United States	147.237.76.200	eitan.aka.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1
106.38.241.106	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
144.168.45.117	United States	147.237.0.34	tikshuv.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
144.168.45.117	United States	147.237.76.31	nakchal.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1

04-17-2016-05:04:09 to 04-17-2016-06:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
200.59.205.238	147.237.77.176	Argentina	matpash.idf.il	SQL Injection - Select From	23
177.185.192.98	147.237.77.216	Brazil	dover.idf.il	SQL Injection - Select From	12
152.115.70.227	147.237.76.86	Denmark	navy.idf.il	SQL Injection - Select From	12
59.120.255.127	147.237.77.74	Taiwan	law.idf.il	SQL Injection - Select From	12
177.185.192.50	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
113.240.250.154	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.98	147.237.77.212	United States	e.dover.idf.il	ET DROP Dshield Block Listed Source	1
104.171.122.176	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
88.204.187.90	147.237.76.200	Kazakstan	eitan.aka.idf.il	ET SCAN NMAP -sS window 2048	1
171.249.111.159	147.237.0.35	Vietnam	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
82.117.208.243	147.237.0.34		tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
144.168.45.117	147.237.76.200	United States	eitan.aka.idf.il	ET WEB_SERVER Possible bash shell piped to dev tcp Inbound to WebServer	1
144.168.45.117	147.237.76.42	United States	refuah.idf.il	ET WEB_SERVER Possible bash shell piped to dev tcp Inbound to WebServer	1
144.168.45.117	147.237.0.34	United States	tikshuv.idf.il	ET WEB_SERVER Possible bash shell piped to dev tcp Inbound to WebServer	1
144.168.45.117	147.237.0.15	United States	kosher-kravi.idf.il	ET WEB_SERVER Possible bash shell piped to dev tcp Inbound to WebServer	1
115.118.57.159	147.237.0.35	India	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.171.122.176	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
88.204.187.90	147.237.76.200	Kazakstan	eitan.aka.idf.il	ET SCAN NMAP -sS window 3072	1
88.204.187.90	147.237.76.200	Kazakstan	eitan.aka.idf.il	ET SCAN NMAP -f -sS	1
144.168.45.117	147.237.76.147	United States	chinuch.aka.idf.il	ET WEB_SERVER Possible bash shell piped to dev tcp Inbound to WebServer	1
144.168.45.117	147.237.76.31	United States	nakchal.idf.il	ET WEB_SERVER Possible bash shell piped to dev tcp Inbound to WebServer	1
144.168.45.117	147.237.0.19	United States	madim.atal.idf.il	ET WEB_SERVER Possible bash shell piped to dev tcp Inbound to WebServer	1
128.199.242.96	147.237.72.166	Singapore	aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1

04-17-2016-05:04:09 to 04-17-2016-06:04:09

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	36
66.249.93.111	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
66.249.93.115	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
66.249.93.119	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
31.168.184.245	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
109.253.135.93	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
207.46.13.30	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
66.96.128.60	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	4
212.150.252.34	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
118.173.128.200	Thailand	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
93.158.152.49	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.66.47	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
182.118.22.216	China	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	3
83.130.108.189	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
50.101.171.19	Canada	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	2
157.55.39.163	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
208.115.113.89	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
157.55.39.32	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
207.46.13.136	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
5.39.222.159	Netherlands	147.237.0.33	idf.il	drop		drop	1
182.118.22.216	China	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.232	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
84.111.159.184	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.247.203	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.122	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
5.39.222.159	Netherlands	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.79	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
144.168.45.117	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
87.71.99.253	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
216.218.206.71	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.238	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
169.57.0.199	Mexico	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.123	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.8	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.108	United States	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
144.168.45.117	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
216.218.206.80	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.3.144.26	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
182.118.21.203	China	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.203	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
218.22.211.69	China	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
74.82.47.24	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
37.187.114.171	France	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.115	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
144.168.45.117	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
94.230.86.252	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
216.218.206.88	United States	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

04-17-2016-05:04:09 to 04-17-2016-06:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
199.30.24.127	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
65.55.210.234	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
199.30.25.177	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
66.102.8.243	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
216.218.206.68	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
157.55.39.163	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/navy/navy	Block	1
68.180.230.45	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9182-he/refuah.aspx	Block	1
66.102.8.238	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
207.46.13.19	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
84.109.68.245	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	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/6/2826.jpg	Block	1
199.30.24.10	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.182.39.174	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1
207.46.13.30	United States	147.237.77.243	mobile.idf.il	Suspicious Response Code	Block	1
109.253.135.93	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	Block	1
79.182.39.174	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/xmlrpc.php	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
207.46.13.67	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
157.55.2.169	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.79.119	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
199.30.24.158	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.182.195.92	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/m/main/rabanut/general.aspx	Block	1
207.46.13.136	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 207.46.13.136	Block	1
157.55.39.1	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/|½¿|λ¿½	Block	1
67.230.138.196	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	Block	1
84.108.72.124	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/mobile	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1

04-17-2016-05:04:09 to 04-17-2016-06:04:09