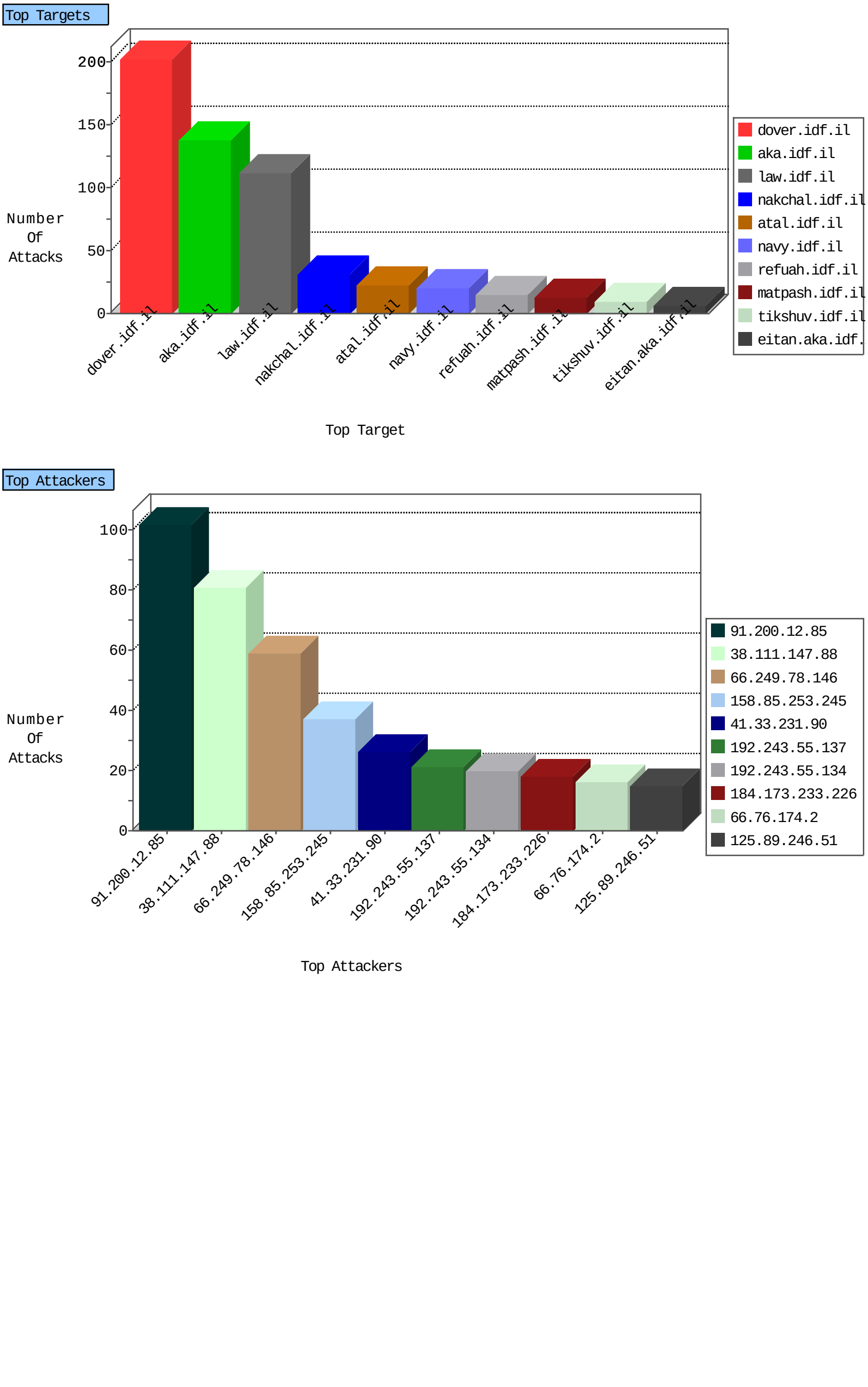
04-24-2016-05:04:06 to 04-24-2016-06:04:06

IDF Under Attack Daily Report



04-24-2016-05:04:06 to 04-24-2016-06:04:06

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	DOS-Tool-SwitchbladG	dest-reset	3
204.42.253.2	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
5.196.199.231	France	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
111.3.108.197	China	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1

04-24-2016-05:04:06 to 04-24-2016-06:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
158.85.253.245	United States	147.237.76.31	nakchal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
66.76.174.2	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
66.135.63.82	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
184.173.233.226	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
94.73.150.148	Turkey	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
184.173.233.226	United States	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
158.85.253.245	United States	147.237.76.31	nakchal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
158.85.253.245	United States	147.237.77.216	dover.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	3
23.91.70.94	United States	147.237.76.86	navy.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	3
23.91.70.94	United States	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	1
64.31.44.6	United States	147.237.77.176	matpash.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	1

04-24-2016-05:04:06 to 04-24-2016-06:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
158.85.253.245	147.237.76.31	United States	nakchal.idf.il	SQL Injection - Select From	16
66.76.174.2	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	12
184.173.233.226	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	10
23.91.70.94	147.237.76.86	United States	navy.idf.il	SQL Injection - Select From	10
158.85.253.245	147.237.77.216	United States	dover.idf.il	SQL Injection - Select From	6
66.135.63.82	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
64.31.44.6	147.237.77.176	United States	matpash.idf.il	SQL Injection - Select From	6
94.73.150.148	147.237.77.74	Turkey	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	3
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
125.89.246.51	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	2
58.218.204.211	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
125.89.246.51	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
37.187.61.4	147.237.0.15	France	kosher-kravi.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
183.60.48.25	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
125.89.246.51	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
13.92.178.142	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
109.72.215.18	147.237.0.16	United Kingdom	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
13.92.178.142	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -f -sS	1
125.89.246.51	147.237.77.243	China	mobile.idf.il	ET SCAN Potential SSH Scan	1
91.99.30.39	147.237.76.31	Iran, Islamic Republic of	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
125.89.246.51	147.237.77.205	China	prisha.idf.il	ET SCAN Potential SSH Scan	1
81.169.215.81	147.237.72.14	Germany	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
125.89.246.51	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
125.89.246.51	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	1
125.89.246.51	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.211	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
125.89.246.51	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.30	China	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
125.89.246.51	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
158.255.5.147	147.237.77.170	Russian Federation	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
117.20.41.62	147.237.0.35	Singapore	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
13.92.178.142	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
81.169.215.81	147.237.72.14	Germany	dover.idf.il(old)	ET SCAN NMAP -sS window 4096	1
125.89.246.51	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
80.82.78.38	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
125.89.246.51	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
125.89.246.51	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
58.218.204.211	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
125.89.246.51	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1

04-24-2016-05:04:06 to 04-24-2016-06:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
38.111.147.88	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	80
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	57
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
198.58.103.115	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
109.253.215.252	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.160.176.43	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.243.55.137	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.134	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	4
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
37.187.165.74	France	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
192.243.55.134	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
8.37.227.70	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	4
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
66.249.66.190	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.135	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
8.37.227.69	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	3
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
50.245.63.203	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
85.93.91.84	Germany	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
197.114.9.169	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
8.37.227.68	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	2
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
91.200.12.106	Ukraine	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	2
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
91.200.12.106	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	2
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
208.115.111.73	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
95.87.233.210	Bulgaria	147.237.0.35	akaws.idf.il	drop		drop	1
70.39.186.218	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
184.105.247.246	United States	147.237.8.27	e.madim.atal.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1
8.37.227.81	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
109.72.215.18	United Kingdom	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
91.200.12.85	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 91.200.12.85	Block	42
91.200.12.85	Ukraine	147.237.72.166	aka.idf.il	PHP Attempt	Block	21
91.200.12.85	Ukraine	147.237.77.74	law.idf.il	PHP Attempt	Block	4
91.200.12.85	Ukraine	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 91.200.12.85	Block	3
91.200.12.85	Ukraine	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 91.200.12.85	Block	3
91.200.12.85	Ukraine	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 91.200.12.85	Block	3
91.200.12.85	Ukraine	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 91.200.12.85	Block	3
91.200.12.85	Ukraine	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 91.200.12.85	Block	3
91.200.12.85	Ukraine	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 91.200.12.85	Block	3
66.102.6.191	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
91.200.12.85	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	2
91.200.12.85	Ukraine	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 91.200.12.85	Block	2
91.200.12.85	Ukraine	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 91.200.12.85	Block	2
91.200.12.85	Ukraine	147.237.77.176	matpash.idf.il	PHP Attempt	Block	2
91.200.12.85	Ukraine	147.237.76.200	eitan.aka.idf.il	PHP Attempt	Block	1
91.200.12.85	Ukraine	147.237.0.34	tikshuv.idf.il	PHP Attempt	Block	1
187.44.148.42	Brazil	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;popId in www.aka.idf.il/lomdim/tochen/	None	1
91.200.12.85	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	1
78.46.23.198	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
66.249.64.34	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
109.253.215.252	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
187.44.148.42	Brazil	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp-login.php	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/home/pniot.aspx	Block	1
37.187.61.4	France	147.237.0.15	kosher-kravi.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.64.61	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/size100x0/3120.jpg	Block	1
157.55.39.215	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
91.200.12.85	Ukraine	147.237.72.156	aman.idf.il	PHP Attempt	Block	1
207.46.13.164	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/yoman.asp	Block	1
38.111.147.88	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
91.200.12.85	Ukraine	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	1
91.200.12.85	Ukraine	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
91.200.12.85	Ukraine	147.237.0.15	kosher-kravi.idf.il	PHP Attempt	Block	1
187.44.148.42	Brazil	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
66.249.65.223	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
91.200.12.85	Ukraine	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
68.180.230.45	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
66.102.6.131	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
187.44.148.42	Brazil	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/wp-login.php	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;amp;popId in www.aka.idf.il/lomdim/news/	None	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1393-en/dover.aspx	Block	1
91.200.12.85	Ukraine	147.237.77.233	atal.idf.il	PHP Attempt	Block	1

04-24-2016-05:04:06 to 04-24-2016-06:04:06