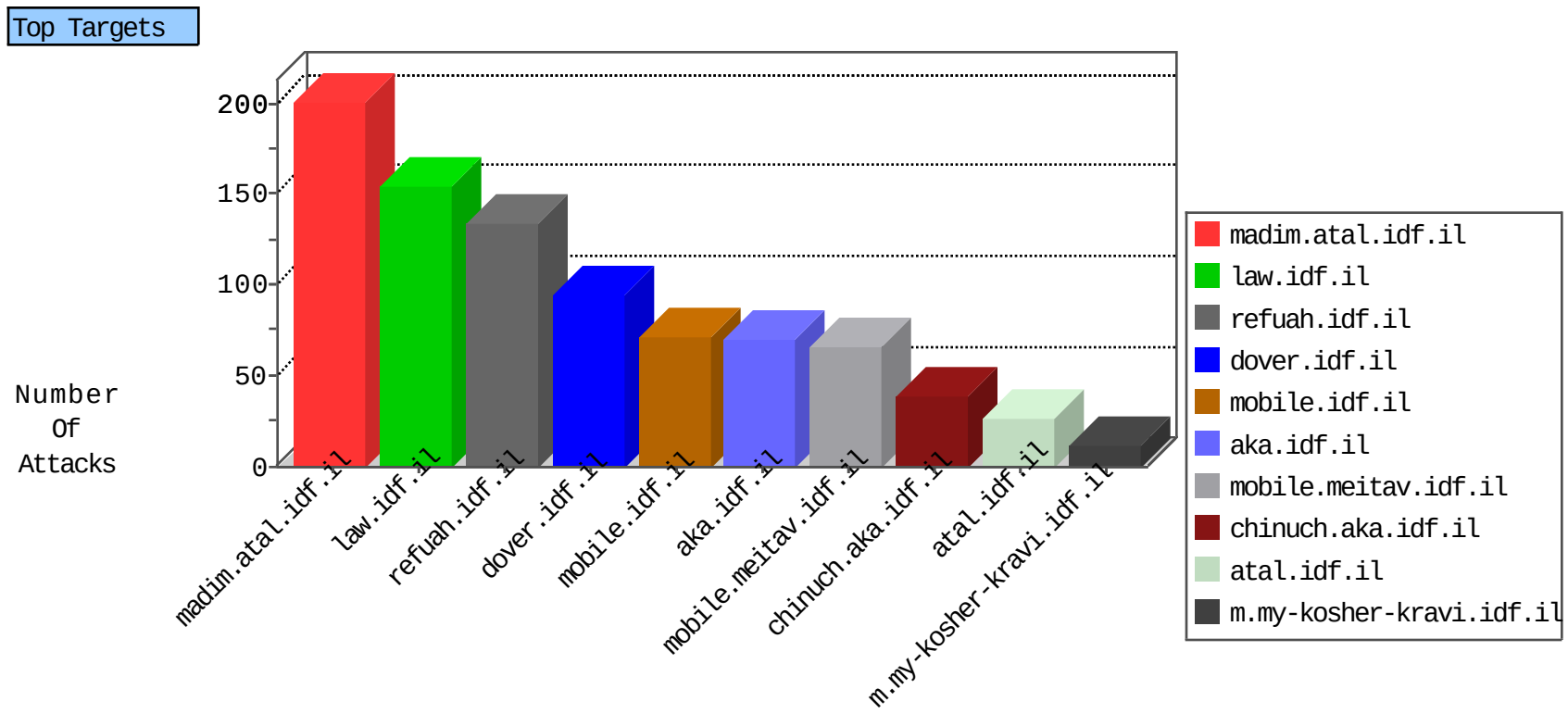
09-25-2016-00:04:09 to 09-25-2016-01:04:09

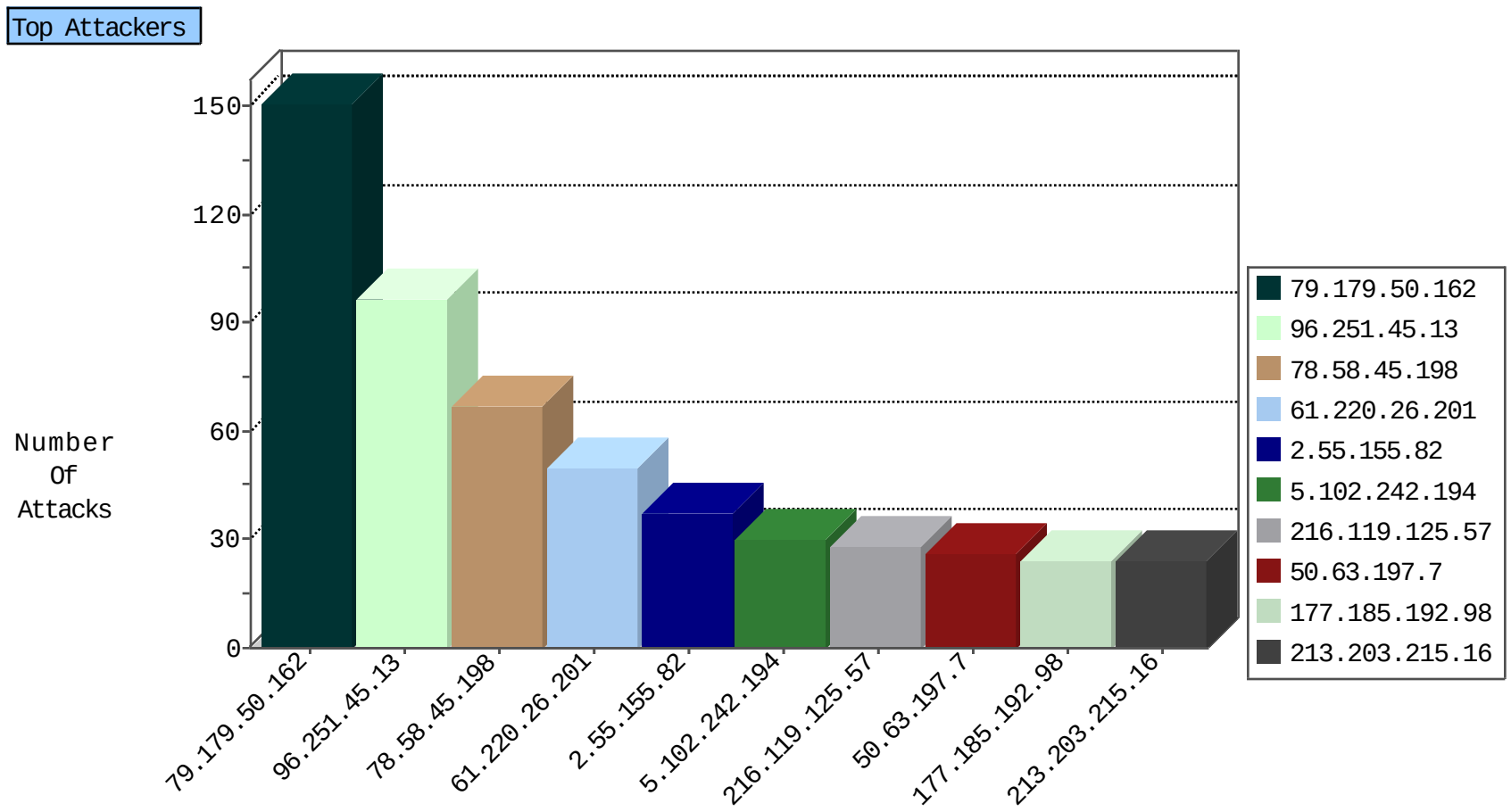
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

09-25-2016-00:04:09 to 09-25-2016-01:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.196.46	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	10
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
82.118.233.249	Bulgaria	147.237.76.199	e.nakchal.idf.il	Black List	drop	1
42.112.10.80	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1
45.32.193.80	Netherlands	147.237.76.30	himush.idf.il	Black List	drop	1
42.112.10.73	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1
42.112.10.81	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1
42.112.10.66	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1
82.118.233.249	Bulgaria	147.237.76.177	ncore.idf.il	Black List	drop	1
42.112.10.74	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1
42.112.10.85	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1
42.112.10.69	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1
82.118.233.249	Bulgaria	147.237.76.197	e.himush.idf.il	Black List	drop	1
42.112.10.75	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1
42.112.10.89	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1
42.112.10.70	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1

09-25-2016-00:04:09 to 09-25-2016-01:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
61.220.26.201	Taiwan	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
96.251.45.13	United States	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
61.220.26.201	Taiwan	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	12
23.91.70.77	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
213.203.215.16	Germany	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
73.14.6.116	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
177.185.192.98	Brazil	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
50.63.197.7	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
81.176.226.68	Russian Federation	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
184.168.27.81	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
50.63.197.7	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
96.251.45.13	United States	147.237.76.42	refuah.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
184.168.46.74	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
96.251.45.13	United States	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
216.119.125.57	United States	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
216.119.125.57	United States	147.237.76.42	refuah.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	2
216.119.125.57	United States	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	2
199.58.86.206	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	1

09-25-2016-00:04:09 to 09-25-2016-01:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
96.251.45.13	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	73
61.220.26.201	147.237.77.74	Taiwan	law.idf.il	SQL Injection - Select From	26
216.119.125.57	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	20
213.203.215.16	147.237.72.166	Germany	aka.idf.il	SQL Injection - Select From	18
177.185.192.98	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	18
50.63.197.7	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	14
184.168.46.74	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
73.14.6.116	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
184.168.27.81	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	8
81.176.226.68	147.237.77.74	Russian Federation	law.idf.il	SQL Injection - Select From	8
23.91.70.77	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	8
175.201.131.197	147.237.72.166	Korea, Republic of	aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
91.201.236.155	147.237.77.216	Ukraine	dover.idf.il	ET SCAN NMAP -f -sS	1
180.213.5.205	147.237.0.35	China	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
60.175.134.166	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
162.213.153.44	147.237.76.177	United States	ncore.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
162.213.153.44	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
46.183.223.228	147.237.8.46	Latvia	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
125.77.28.26	147.237.77.205	China	prisha.idf.il	ET SCAN Potential SSH Scan	1
41.215.36.46	147.237.0.33	Kenya	idf.il	ET SCAN NMAP -sS window 1024	1
125.77.28.26	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
185.93.185.10	147.237.72.167	Ukraine	ishurim.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.201.236.155	147.237.77.216	Ukraine	dover.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.129.15	147.237.77.170	United Kingdom	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.200.137	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
162.213.153.44	147.237.76.176	United States	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
139.59.182.136	147.237.76.39	Singapore	mobile.meitav.idf.i	ET WEB_SERVER Poison Null Byte	1
41.215.36.46	147.237.8.46	Kenya	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
125.77.28.26	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
109.60.153.178	147.237.77.243	Russian Federation	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
209.58.129.109	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN Rapid IMAP Connections - Possible Brute Force Attack	1
91.201.236.155	147.237.77.216	Ukraine	dover.idf.il	ET SCAN NMAP -sS window 2048	1

09-25-2016-00:04:09 to 09-25-2016-01:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
78.58.45.198	Lithuania	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	41
5.102.242.194	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
79.179.50.162	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
78.58.45.198	Lithuania	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	26
89.237.113.235	France	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
46.19.86.78	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
79.179.50.162	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.181	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
157.55.39.42	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.65.60.173	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.181	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.86.159	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
195.239.16.40	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.233	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.181	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
195.239.16.53	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
160.176.172.6	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.87	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.182.129.163	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
128.139.10.231	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
185.120.124.9	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
128.139.10.231	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
79.183.96.191	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.75	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.76.109	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
172.56.39.88	United States	147.237.76.39	mobile.meitav.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
172.56.39.88	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
2.55.155.82	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
172.56.39.88	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
79.178.255.5	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
172.56.39.88	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
128.232.110.28	United Kingdom	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
80.246.133.10	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
172.56.39.88	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	2
37.26.148.149	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
172.56.39.88	United States	147.237.76.39	mobile.meitav.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	2
172.56.39.88	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	2
37.110.39.136	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
172.56.39.88	United States	147.237.76.39	mobile.meitav.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	2
23.248.234.8	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
85.96.210.141	Turkey	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
172.247.83.194	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
78.181.87.40	Turkey	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	1
46.19.86.159	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.48	United States	147.237.0.35	akaws.idf.il	drop		drop	1
2.53.149.180	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
76.90.211.5	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.63	United States	147.237.0.35	akaws.idf.il	drop		drop	1
46.19.86.52	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.179.50.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
2.55.155.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
37.26.146.249	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.224	Block	4
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	3
76.119.39.89	United States	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/error.htm parameter aspxerrorpath	Block	3
213.57.143.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.146.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
104.174.96.236	United States	147.237.77.170	maarachot.idf.il	Distributed Unauthorized HTTP Method	Block	2
79.179.50.162	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
37.26.146.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
139.59.182.136	Singapore	147.237.76.39	mobile.meitav.idf.il	Illegal Byte Code Character in URL ¸[[#20]]¸	Block	1
84.109.235.191	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 84.109.235.191	Block	1
66.249.76.90	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
139.59.182.136	Singapore	147.237.76.39	mobile.meitav.idf.il	Multiple Malformed URL from 139.59.182.136	Block	1
109.64.33.160	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/he/navy.aspx	Block	1
77.125.46.173	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
157.55.39.42	United States	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
139.59.182.136	Singapore	147.237.76.39	mobile.meitav.idf.il	Illegal HTTP Version	Block	1
5.29.171.247	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
89.237.113.235	France	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
213.57.147.49	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	1
66.249.76.100	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list1.htm	Block	1
46.19.86.75	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
139.59.182.136	Singapore	147.237.76.39	mobile.meitav.idf.il	Multiple NULL Character in Method from 139.59.182.136	Block	1
128.68.1.58	Russian Federation	147.237.76.42	refuah.idf.il	Unauthorized Method POST for 147.237.76.42/894-he/refuah.aspx	Block	1
204.79.180.152	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/templates/home.asp	Block	1
66.249.75.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/894-he/dover.aspx	Block	1
139.59.182.136	Singapore	147.237.76.39	mobile.meitav.idf.il	Malformed HTTP Header Line 2	Block	1
68.180.229.184	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1
66.102.9.2	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
139.59.182.136	Singapore	147.237.76.39	mobile.meitav.idf.il	NULL Character in Header Name at [[#1]][[#0]][[#0]]6[[#0]][[#5]][[#0]][[#5]][[#1]][[#0]][[#0]][[#0]][[#0]][[#0]][[0]]	Block	1
139.59.182.136	Singapore	147.237.76.39	mobile.meitav.idf.il	Abnormally Long Request method	Block	1
207.46.13.172	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/family	Block	1
66.249.76.66	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/894-he/nakhal.aspx	Block	1
139.59.182.136	Singapore	147.237.76.39	mobile.meitav.idf.il	Malformed URL ¸[[#20]]¸	Block	1
37.26.146.165	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
104.174.96.236	United States	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 104.174.96.236	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-ar/cogat.aspx	Block	1
66.102.9.24	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
139.59.182.136	Singapore	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/changelog.txt	Block	1
139.59.182.136	Singapore	147.237.76.39	mobile.meitav.idf.il	Illegal Byte Code Character in Header Name [[#0]]œ[[#0]]•[[#0]]/[[#0]]5À[[#18]][[#0]]	Block	1
84.94.73.5	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
213.8.204.14	Israel	147.237.77.233	atal.idf.il	Suspicious Response Code	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
139.59.182.136	Singapore	147.237.76.39	mobile.meitav.idf.il	Multiple Illegal Byte Code Character in Method from 139.59.182.136	Block	1
104.174.96.236	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/sip_storage/files/4/	Block	1
139.59.182.136	Singapore	147.237.76.39	mobile.meitav.idf.il	Unknown HTTP Request Method [[#22]][[#3]][[#1]][[#0]]•[[#1]][[#0]][[#0]]{[[#3]][[#3]][[#21]]¿RŸB-SÈj{Íñ-Ø•‡dÑtURÈdÐu²RT'[[#19]][[#15]]}[[#0]][[#0]][[#28]]À/À+À0À,À[[#19]]À in URL ¸[[#20]]¸	Block	1