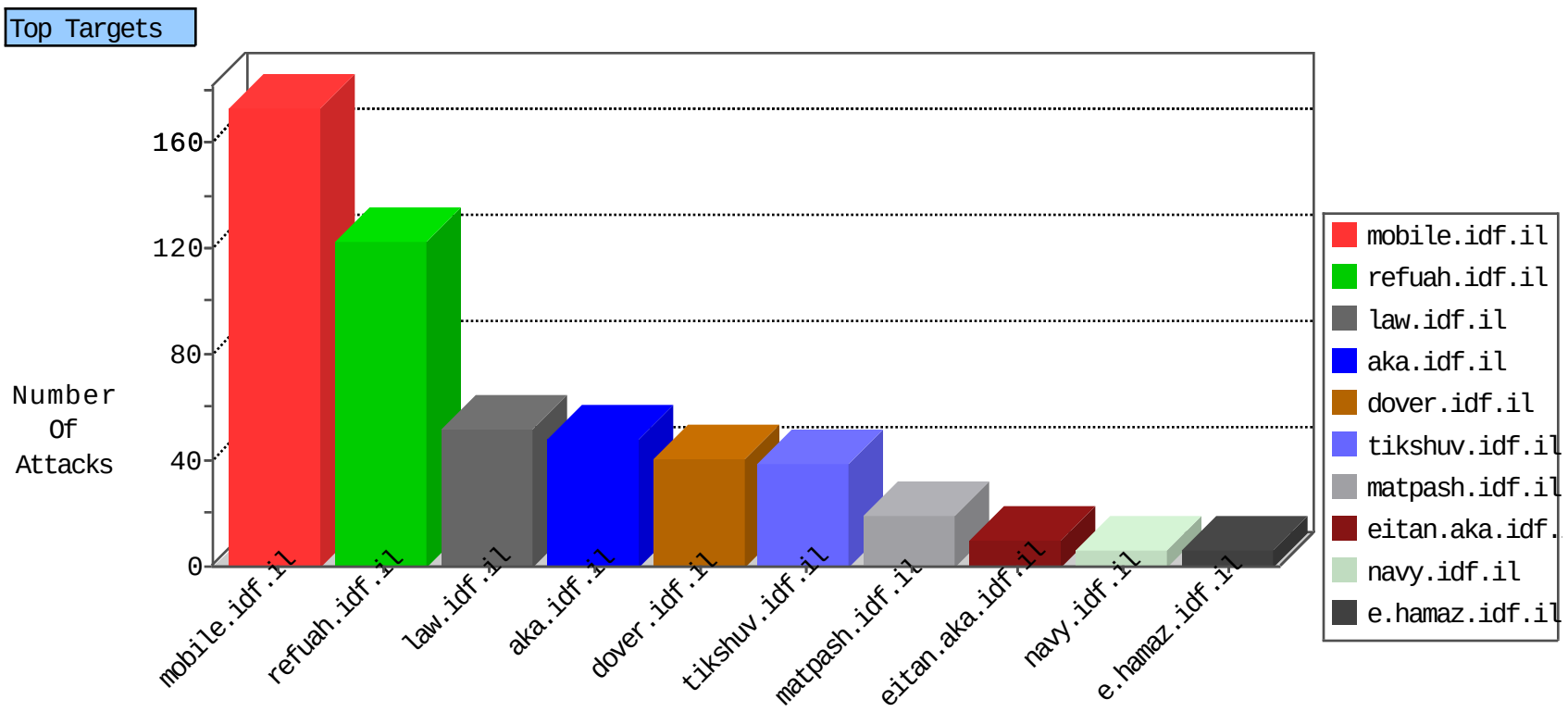
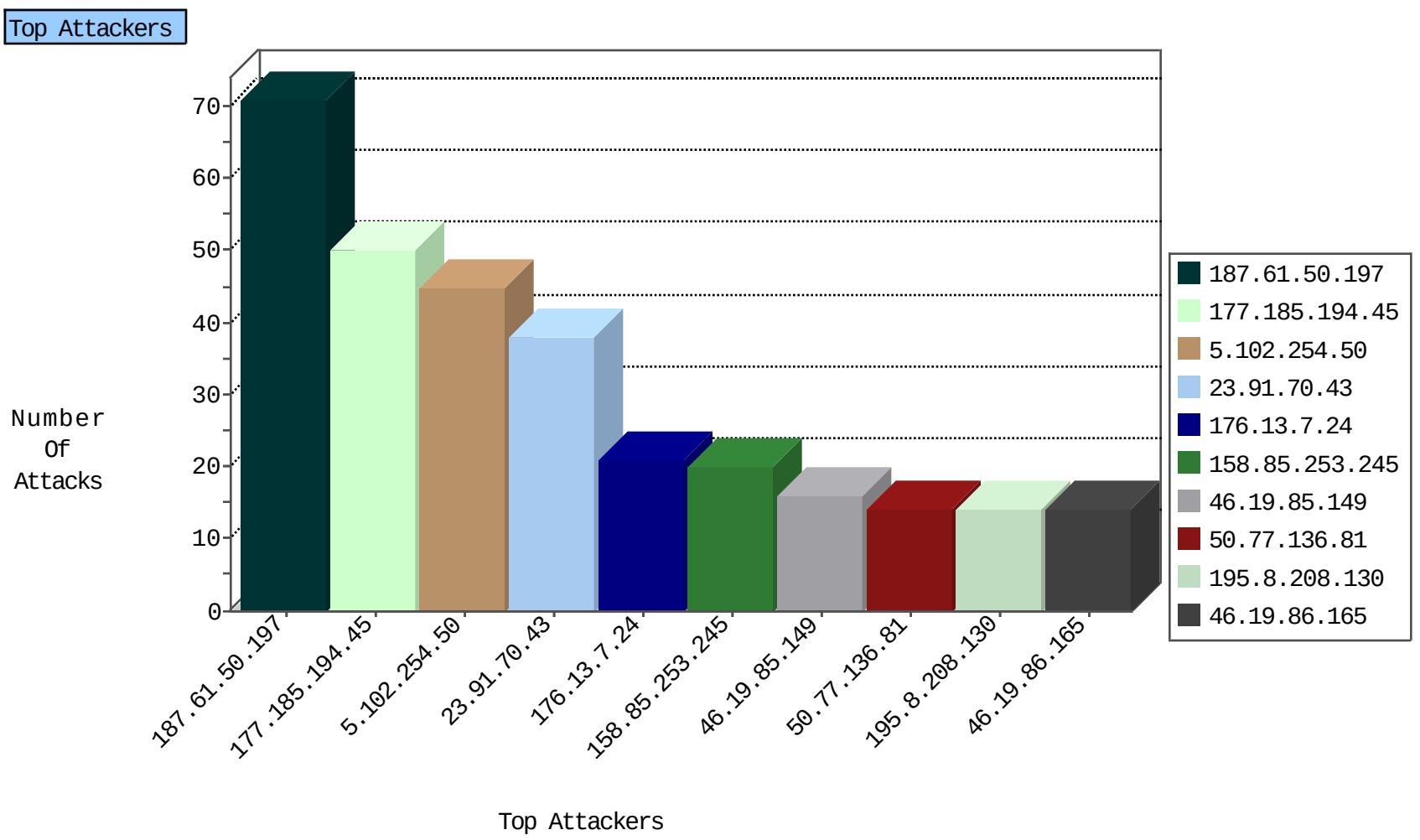
09-29-2016-02:04:07 to 09-29-2016-03:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-29-2016-02:04:07 to 09-29-2016-03:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
61.147.247.161	China	147.237.76.199	e.nakchal.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
198.44.110.15	United States	147.237.76.31	nakchal.idf.il	Black List	drop	1
37.48.106.69	Netherlands	147.237.76.31	nakchal.idf.il	Black List	drop	1
198.44.110.15	United States	147.237.76.197	e.himush.idf.il	Black List	drop	1
37.48.106.69	Netherlands	147.237.76.86	navy.idf.il	Black List	drop	1
198.44.110.25	United States	147.237.76.31	nakchal.idf.il	Black List	drop	1

09-29-2016-02:04:07 to 09-29-2016-03:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
177.185.194.45	Brazil	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
23.91.70.43	United States	147.237.0.34	tikshuv.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
195.8.208.130	Netherlands	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
81.177.24.40	Russian Federation	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
187.61.50.197	Brazil	147.237.76.42	refuah.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
23.91.70.43	United States	147.237.0.34	tikshuv.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
158.85.253.245	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
187.61.50.197	Brazil	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
177.185.194.45	Brazil	147.237.76.42	refuah.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
187.61.50.197	Brazil	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
50.77.136.81	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
177.185.194.45	Brazil	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
64.34.186.9	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	2
192.99.167.90	Canada	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

09-29-2016-02:04:07 to 09-29-2016-03:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
187.61.50.197	147.237.76.42	Brazil	refuah.idf.il	SQL Injection - Select From	53
177.185.194.45	147.237.76.42	Brazil	refuah.idf.il	SQL Injection - Select From	26
23.91.70.43	147.237.0.34	United States	tikshuv.idf.il	SQL Injection - Select From	20
158.85.253.245	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	14
50.77.136.81	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	8
81.177.24.40	147.237.77.74	Russian Federation	law.idf.il	SQL Injection - Select From	8
195.8.208.130	147.237.77.216	Netherlands	dover.idf.il	SQL Injection - Select From	8
212.86.219.134	147.237.77.176	Germany	matpash.idf.il	Tehila - Perl LWP with fake user agent	2
180.97.215.132	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
42.114.202.150	147.237.0.33	Vietnam	idf.il	ET SCAN Potential SSH Scan	1
45.63.28.189	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 1024	1
180.97.215.132	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
45.63.28.189	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
180.97.215.132	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
42.114.202.150	147.237.77.178	Vietnam	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
42.114.202.150	147.237.76.200	Vietnam	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
163.172.129.15	147.237.77.243	United Kingdom	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
42.114.202.150	147.237.76.197	Vietnam	e.himush.idf.il	ET SCAN Potential SSH Scan	1
212.144.3.207	147.237.76.42	Germany	refuah.idf.il	ET SCAN Potential SSH Scan	1
42.114.202.150	147.237.72.14	Vietnam	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
113.143.46.32	147.237.0.34	China	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
42.114.202.150	147.237.8.28	Vietnam	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.74	147.237.72.14	United States	dover.idf.il(old)	ET DROP Dshield Block Listed Source	1
42.114.202.150	147.237.0.35	Vietnam	akaws.idf.il	ET SCAN Potential SSH Scan	1
46.172.91.20	147.237.77.227	Ukraine	e.hamaz.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
180.97.215.132	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
40.121.139.43	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1
45.63.28.189	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
180.97.215.132	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
42.114.202.150	147.237.77.227	Vietnam	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
180.97.215.132	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
42.114.202.150	147.237.76.201	Vietnam	e.atal.idf.il	ET SCAN Potential SSH Scan	1
173.77.240.227	147.237.0.35	United States	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
42.114.202.150	147.237.76.198	Vietnam	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
163.172.129.15	147.237.76.200	United Kingdom	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
42.114.202.150	147.237.76.147	Vietnam	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
212.144.3.207	147.237.0.19	Germany	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
113.240.250.154	147.237.77.227	China	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
42.114.202.150	147.237.8.50	Vietnam	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
201.114.60.162	147.237.72.156	Mexico	aman.idf.il	ET SCAN NMAP -sS window 4096	1
42.114.202.150	147.237.8.14	Vietnam	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
46.172.91.21	147.237.76.30	Ukraine	himush.idf.il	ET SCAN NMAP -sS window 1024	1

09-29-2016-02:04:07 to 09-29-2016-03:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.102.254.50	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
176.13.7.24	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.149	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
81.218.226.208	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
2.55.54.222	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.55.159.162	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
185.32.179.152	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.221	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.26.146.162	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.165	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.86.165	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.149	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.52.66.78	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.20	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.32.179.207	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.210.93	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.21.169	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
65.55.210.164	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
68.131.64.241	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.53.8.76	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.55.40.119	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.226.218.91	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
41.82.38.118	Senegal	147.237.77.216	dover.idf.il	Header Rejection	header rejection pattern found in request	monitor	2
185.88.25.69	Iraq	147.237.77.205	prisha.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	2
2.53.169.156	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	2
185.88.25.69	Iraq	147.237.77.205	prisha.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
2.53.169.156	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
67.58.15.97	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
79.181.100.150	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
2.53.169.156	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
176.13.224.53	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
109.253.195.78	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
2.53.169.156	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
2.53.169.156	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
141.212.122.91	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
139.162.37.147	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.19.85.136	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
103.5.126.158	Cambodia	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
185.3.147.215	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
77.237.138.202	Czech Republic	147.237.77.234	halag.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
46.19.86.16	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.86	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
109.253.217.75	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
84.108.67.228	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
66.102.9.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.92	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
139.162.37.147	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.4.3.85	Iran, Islamic Republic of	147.237.76.34	yohalan.idf.il	drop		drop	1
103.5.126.158	Cambodia	147.237.76.34	yohalan.idf.il	drop		drop	1

09-29-2016-02:04:07 to 09-29-2016-03:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.102.254.50	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	9
81.218.226.208	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.177	Block	3
185.32.179.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.221	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
2.55.159.162	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
176.13.7.24	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
37.26.146.162	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.20	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
2.55.54.222	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
109.253.210.93	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
66.249.75.12	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9686-he/refuah.aspx	Block	1
46.19.85.237	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1
2.52.66.78	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
104.214.116.67	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
66.249.66.180	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	1
66.249.76.41	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on www.chamatz.aka.idf.il/404.aspx	Block	1
46.19.85.237	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method nId=uuawzk55abstljjsmsp5uzfc in URL	Block	1
2.55.40.119	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
109.253.205.237	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.66.180	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_bottom.asp	Block	1
185.32.179.152	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-he/dover.aspx	Block	1
46.19.86.144	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/buetiful assmain/giyus/general.aspx	Block	1
66.249.66.180	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
185.32.179.207	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
77.237.138.202	Czech Republic	147.237.77.234	halag.idf.il	Unauthorized URL Access to /	Block	1
66.249.66.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/.well-known/assetlinks.json	Block	1
157.55.39.234	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
66.249.66.183	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	1
46.19.85.237	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
217.69.133.225	Russian Federation	147.237.72.166	aka.idf.il	Unknown Parameter fb709480 in aka.idf.il/giyus/	None	1

09-29-2016-02:04:07 to 09-29-2016-03:04:07