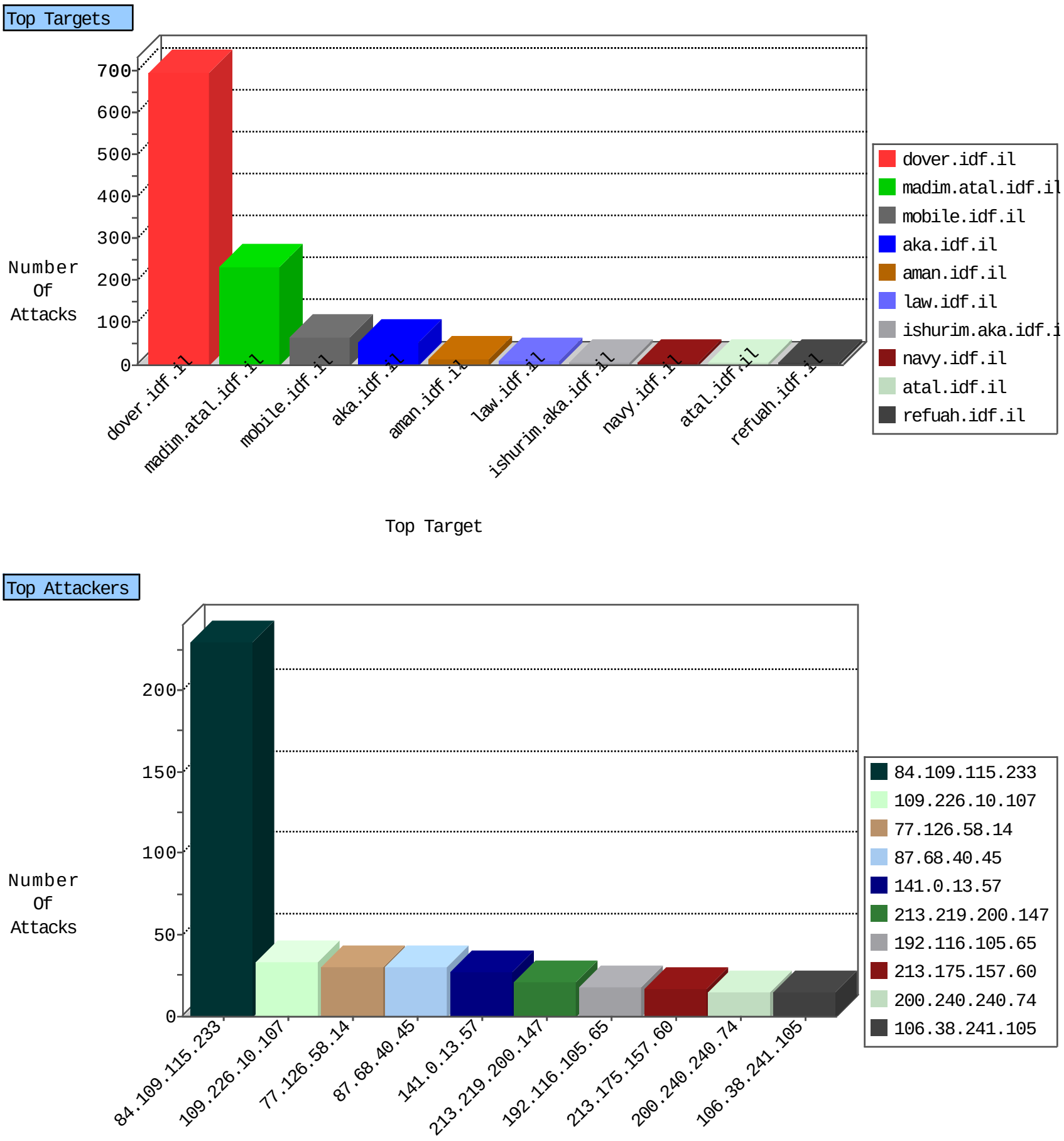
09-17-2016-00:04:01 to 09-17-2016-01:04:01

IDF Under Attack Daily Report



09-17-2016-00:04:01 to 09-17-2016-01:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	network flood IPv4 ICMP	drop	186381
213.219.200.147	Russian Federation	147.237.77.216	dover.idf.il	network flood IPv4 ICMP	drop	46
109.226.10.107	Israel	147.237.77.216	dover.idf.il	Black List	drop	33
192.116.105.65	Israel	147.237.77.216	dover.idf.il	Black List	drop	18
213.175.157.60	United Kingdom	147.237.77.216	dover.idf.il	network flood IPv4 ICMP	drop	17
200.240.240.74	Brazil	147.237.77.216	dover.idf.il	network flood IPv4 ICMP	drop	15
212.199.221.116	Israel	147.237.77.216	dover.idf.il	Black List	drop	14
193.0.240.58	Ukraine	147.237.77.216	dover.idf.il	network flood IPv4 ICMP	drop	13
80.179.155.25	Israel	147.237.77.216	dover.idf.il	Black List	drop	12
112.211.251.105	Philippines	147.237.77.216	dover.idf.il	network flood IPv4 ICMP	drop	12
5.35.91.58	Russian Federation	147.237.77.216	dover.idf.il	network flood IPv4 ICMP	drop	12
85.114.105.118	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Black List	drop	12
85.114.105.161	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Black List	drop	12
103.42.206.73	India	147.237.77.216	dover.idf.il	network flood IPv4 ICMP	drop	11
80.90.83.17	Albania	147.237.77.216	dover.idf.il	network flood IPv4 ICMP	drop	11
80.179.119.22	Israel	147.237.77.216	dover.idf.il	Black List	drop	11
185.23.175.81	Israel	147.237.77.216	dover.idf.il	Black List	drop	11
85.120.251.154	Romania	147.237.77.216	dover.idf.il	network flood IPv4 ICMP	drop	10
62.128.42.1	Israel	147.237.77.216	dover.idf.il	Black List	drop	9
177.67.200.30	Brazil	147.237.77.216	dover.idf.il	network flood IPv4 ICMP	drop	9
50.122.81.106	United States	147.237.77.216	dover.idf.il	network flood IPv4 ICMP	drop	9
85.114.106.3	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Black List	drop	9
195.66.156.6	Ukraine	147.237.77.216	dover.idf.il	network flood IPv4 ICMP	drop	8
82.202.92.167	Czech Republic	147.237.77.216	dover.idf.il	network flood IPv4 ICMP	drop	8
194.44.212.28	Ukraine	147.237.77.216	dover.idf.il	network flood IPv4 ICMP	drop	7
90.188.239.231	Russian Federation	147.237.77.216	dover.idf.il	network flood IPv4 ICMP	drop	7
71.8.36.26	United States	147.237.77.216	dover.idf.il	network flood IPv4 ICMP	drop	6
213.226.206.226	Czech Republic	147.237.77.216	dover.idf.il	network flood IPv4 ICMP	drop	6
4.53.161.218	United States	147.237.77.216	dover.idf.il	network flood IPv4 ICMP	drop	6
213.8.196.17	Israel	147.237.77.216	dover.idf.il	Black List	drop	6
124.248.169.126	Cambodia	147.237.77.216	dover.idf.il	network flood IPv4 ICMP	drop	6
193.85.74.128	Czech Republic	147.237.77.216	dover.idf.il	network flood IPv4 ICMP	drop	6
178.209.107.186	Russian Federation	147.237.77.216	dover.idf.il	network flood IPv4 ICMP	drop	6
186.237.147.62	Brazil	147.237.77.216	dover.idf.il	network flood IPv4 ICMP	drop	5
195.175.110.58	Turkey	147.237.77.216	dover.idf.il	network flood IPv4 ICMP	drop	5
88.83.203.109	Russian Federation	147.237.77.216	dover.idf.il	network flood IPv4 ICMP	drop	5
82.112.185.213	Russian Federation	147.237.77.216	dover.idf.il	network flood IPv4 ICMP	drop	5
178.167.77.17	Russian Federation	147.237.77.216	dover.idf.il	network flood IPv4 ICMP	drop	5
62.128.45.65	Israel	147.237.77.216	dover.idf.il	Black List	drop	5
185.85.210.214	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	network flood IPv4 ICMP	drop	4
80.82.238.130	France	147.237.77.216	dover.idf.il	network flood IPv4 ICMP	drop	4
62.122.244.139	Russian Federation	147.237.77.216	dover.idf.il	network flood IPv4 ICMP	drop	4
122.15.142.89	India	147.237.77.216	dover.idf.il	network flood IPv4 ICMP	drop	4
36.66.89.10	Indonesia	147.237.77.216	dover.idf.il	network flood IPv4 ICMP	drop	4
85.117.58.126	Georgia	147.237.77.216	dover.idf.il	network flood IPv4 ICMP	drop	4
177.54.237.42	Brazil	147.237.77.216	dover.idf.il	network flood IPv4 ICMP	drop	4
94.230.166.92	Russian Federation	147.237.77.216	dover.idf.il	network flood IPv4 ICMP	drop	4
187.60.34.102	Brazil	147.237.77.216	dover.idf.il	network flood IPv4 ICMP	drop	3
177.139.180.24	Brazil	147.237.77.216	dover.idf.il	network flood IPv4 ICMP	drop	3
85.114.107.226	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Black List	drop	3

09-17-2016-00:04:01 to 09-17-2016-01:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
86.132.208.154	United Kingdom	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	1
111.255.177.208	Taiwan	147.237.77.216	dover.idf.i	13118: ICMP: Windows DirectAccess Server IPv6 Invalid Header Denial-of-Service Vulnerability	Block	1

09-17-2016-00:04:01 to 09-17-2016-01:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
79.179.151.172	147.237.72.156	Israel	aman.idf.il	ET SCAN NMAP -sA (2)	7
5.255.90.133	147.237.77.216	Netherlands	dover.idf.il	ET SCAN NMAP -sS window 1024	1
178.20.188.164	147.237.77.121	Jordan	e.navy.idf.il	ET SCAN NMAP -sS window 2048	1
162.243.218.193	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1
133.208.21.66	147.237.77.234	Japan	halag.idf.il	ET SCAN NMAP -sS window 1024	1
123.206.85.139	147.237.0.200	China	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
212.92.127.197	147.237.76.198	Russian Federation	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
66.249.64.113	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
212.92.127.197	147.237.72.167	Russian Federation	ishurim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
58.218.200.137	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
212.92.127.197	147.237.8.24	Russian Federation	e.lifestyle.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.227.67.158	147.237.77.243	Sweden	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
178.20.188.164	147.237.77.121	Jordan	e.navy.idf.il	ET SCAN NMAP -sS window 4096	1
178.20.188.164	147.237.77.121	Jordan	e.navy.idf.il	ET SCAN NMAP -f -sS	1
133.242.4.52	147.237.0.15	Japan	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
133.208.21.66	147.237.77.212	Japan	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
120.76.102.141	147.237.77.235	China	sviva.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
223.215.141.116	147.237.77.178	China	e.matpash.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
66.249.66.238	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
212.92.127.197	147.237.76.176	Russian Federation	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
58.218.200.137	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
212.92.127.197	147.237.72.156	Russian Federation	aman.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
58.45.139.84	147.237.76.42	China	refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
202.155.58.28	147.237.76.177	Indonesia	ncore.idf.il	ET SCAN NMAP -sS window 1024	1

09-17-2016-00:04:01 to 09-17-2016-01:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
87.68.40.45	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
77.126.58.14	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
141.0.13.57	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	27
213.57.157.210	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
176.13.244.49	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
79.177.55.53	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
92.241.58.118	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
185.20.5.157	United Kingdom	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
94.99.84.187	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
185.20.5.157	United Kingdom	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
159.220.74.2	United Kingdom	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
106.38.241.105	China	147.237.76.86	navy.idf.il	drop	SAM rule	drop	2
212.179.241.1	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
81.84.23.4	Portugal	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
106.38.241.105	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
185.20.5.157	United Kingdom	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
79.177.52.193	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
46.19.85.56	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
106.38.241.105	China	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
95.90.245.200	Germany	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
176.13.232.98	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
84.111.233.36	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
141.226.218.54	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.91.20.62	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
106.38.241.105	China	147.237.77.234	halag.idf.il	drop	SAM rule	drop	1
221.181.73.62	China	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	1
31.168.114.2	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	1
106.38.241.105	China	147.237.72.167	ishurim.aka.idf.il	drop	SAM rule	drop	1
92.241.58.118	Jordan	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
172.56.35.176	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
79.177.52.193	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
133.208.21.66	Japan	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.19.85.182	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
106.38.241.105	China	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	1
216.243.31.2	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
2.53.53.18	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
95.164.68.118	Ukraine	147.237.0.33	idf.il	drop		drop	1
141.226.218.85	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
108.184.209.16	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
221.181.73.62	China	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
31.168.114.2	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
106.38.241.105	China	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	1
188.120.154.177	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
92.241.58.118	Jordan	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
173.208.187.98	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
139.162.37.147	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.86.113	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
106.38.241.105	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
216.243.31.2	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

09-17-2016-00:04:01 to 09-17-2016-01:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.109.115.233	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	230
46.19.86.94	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.120.229.81	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	2
66.102.9.5	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
68.180.228.159	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2027-he/cogat.aspx	Block	1
46.19.85.56	Israel	147.237.76.86	navy.idf.il	Malformed URL	Block	1
181.215.117.118	United States	147.237.77.233	atal.idf.il	PHP Attempt	Block	1
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
77.138.104.132	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
46.19.85.56	Israel	147.237.76.86	navy.idf.il	Unknown HTTP Request Method 5u1qehabs in URL	Block	1
181.215.117.118	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/wp-login.php	Block	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.41	Block	1
185.3.147.83	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.64.113	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
92.241.58.118	Jordan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arabic/	Block	1
66.249.76.71	Israel	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/apple-app-site-association	Block	1
157.55.39.54	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1

09-17-2016-00:04:01 to 09-17-2016-01:04:01