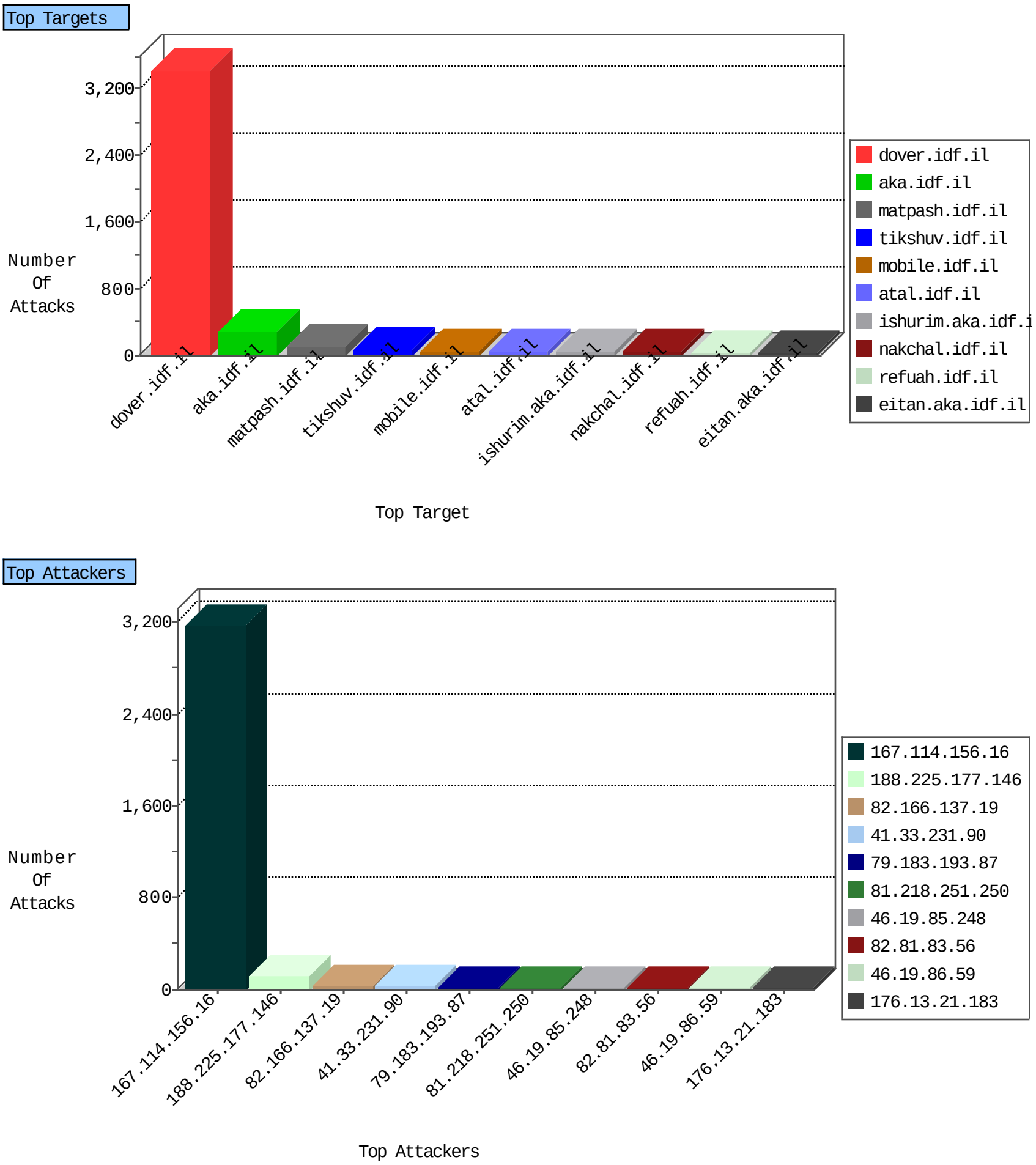
04-12-2016-10:04:09 to 04-12-2016-11:04:09

IDF Under Attack Daily Report



04-12-2016-10:04:09 to 04-12-2016-11:04:09

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	3168
80.246.137.213	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1854
82.166.137.19	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	246
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	6
195.24.234.17	Ukraine	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
82.145.218.175	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	2
45.124.196.138	India	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
46.19.86.182	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
184.105.139.94	United States	147.237.0.33	idf.il	Block_Ntp_All_Net	drop	1
124.144.153.224	Japan	147.237.77.74	law.idf.il	Block_Udp_All_Nets	drop	1
216.72.40.186	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
184.105.139.126	United States	147.237.77.74	law.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.74	United States	147.237.77.19	law-forum.idf.il	Block_Ntp_All_Net	drop	1
85.93.89.243	Germany	147.237.77.212	e.dover.idf.il	Block_Udp_All_Nets	drop	1
207.141.11.146	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.98	United States	147.237.77.178	e.matpash.idf.il	Block_Ntp_All_Net	drop	1
2.53.31.17	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
216.218.206.93	United States	147.237.77.234	halag.idf.il	Block_Udp_All_Nets	drop	1
193.43.245.250	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
184.105.139.78	United States	147.237.0.34	tikshuv.idf.il	Block_Ntp_All_Net	drop	1
85.93.89.243	Germany	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
74.82.47.41	United States	147.237.77.121	e.navy.idf.il	Block_Udp_All_Nets	drop	1
209.126.120.23	United States	147.237.0.200	m4u.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.114	United States	147.237.77.243	mobile.idf.il	Block_Ntp_All_Net	drop	1
176.31.60.249	France	147.237.72.166	aka.idf.il	Block_Ntp_All_Net	drop	1
193.43.246.250	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
184.105.139.78	United States	147.237.8.14	e.orchot.idf.il	Block_Ntp_All_Net	drop	1
114.37.56.44	Taiwan	147.237.77.74	law.idf.il	Block_Udp_All_Nets	drop	1
79.182.108.39	Israel	147.237.76.86	navy.idf.il	network flood IPv4 TCP-RST	drop	1
209.126.120.23	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.122	United States	147.237.72.156	aman.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.70	United States	147.237.0.19	madim.atal.idf.il	Block_Ntp_All_Net	drop	1

04-12-2016-10:04:09 to 04-12-2016-11:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.251.250	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	24
5.29.16.50	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	19
213.246.49.97	France	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
194.90.153.50	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
94.159.209.141	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
185.106.92.47	Russian Federation	147.237.76.147	chinuch.aka.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	3
157.55.39.162	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
147.236.31.113	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
149.50.93.5	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
192.114.5.10	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
157.55.39.215	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
185.106.92.47	Russian Federation	147.237.76.42	refuah.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
185.106.92.47	Russian Federation	147.237.76.147	chinuch.aka.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
61.135.189.122	China	147.237.76.31	nakchal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-12-2016-10:04:09 to 04-12-2016-11:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
213.246.49.97	147.237.77.74	France	law.idf.il	SQL Injection - Select From	5
66.249.93.109	147.237.76.86	Europe	navy.idf.il	ET SCAN NMAP -sA (2)	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
46.60.43.166	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.154.54	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
208.100.26.228	147.237.77.233	United States	atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
2.53.51.234	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.106.92.47	147.237.76.147	Russian Federation	chinuch.aka.idf.il	ET WEB_SERVER Muieblackcat scanner	1
149.78.177.135	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
88.204.187.90	147.237.77.233	Kazakstan	atal.idf.il	ET SCAN NMAP -f -sS	1
82.166.242.41	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.176.86.172	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.151.52.139	147.237.72.156	Ukraine	aman.idf.il	ET SCAN NMAP -sS window 1024	1
8.30.124.66	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 4096	1
212.150.177.182	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.53.52.72	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.88.20.232	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
88.204.187.90	147.237.77.233	Kazakstan	atal.idf.il	ET SCAN NMAP -sS window 2048	1
85.64.241.66	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.103.183	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

04-12-2016-10:04:09 to 04-12-2016-11:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
188.225.177.146	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	75
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
79.183.193.87	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	22
188.225.177.146	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	21
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	14
46.116.20.99	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	13
46.19.85.248	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
77.124.9.188	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
31.154.174.107	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
185.27.106.59	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.248	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
2.53.129.80	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
82.166.198.101	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
176.13.21.183	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
82.81.83.56	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
46.19.85.37	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
176.13.21.183	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
2.55.51.154	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
207.46.13.74	United States	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	8
46.19.86.59	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.59	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
79.180.150.131	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.130.247.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.229.27.225	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.19.9	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.10.16	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.199.148	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.178.169.81	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.121.96.254	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
147.236.31.63	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
5.22.131.118	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
82.81.83.56	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
80.179.9.115	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
82.81.83.56	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
147.236.31.63	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	5
79.183.193.87	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
5.102.195.71	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
176.228.5.113	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
213.151.46.163	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.53.143.69	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.86.59	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
37.142.64.58	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
46.19.86.59	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
31.168.77.225	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.22.253	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.132.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.150.231	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.1.100	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.179.244.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-12-2016-10:04:09 to 04-12-2016-11:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.120.131.128	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	17
46.19.85.194	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	12
46.60.43.166	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 46.60.43.166	Block	6
109.253.150.231	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/login parameter Password	Block	5
94.188.161.145	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	5
94.188.161.145	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew	Block	5
132.68.150.6	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	4
109.65.21.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
2.55.180.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
132.68.150.6	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 132.68.150.6	Block	2
37.26.149.191	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	2
109.65.130.234	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	2
2.55.190.100	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	2
199.30.25.7	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
199.30.25.34	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
157.55.12.81	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
199.30.24.43	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
207.46.13.72	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
199.30.24.113	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.86.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
199.30.24.210	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.66.12	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/m/	Block	1
93.190.152.161	Europe	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 93.190.152.161	Block	1
81.218.118.126	Israel	147.237.72.166	aka.idf.il	Malformed HTTP Header Line 2	Block	1
212.25.119.193	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
180.76.15.32	China	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list2005b.htm	Block	1
67.222.60.182	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/wordpress/wp-admin/	Block	1
66.249.64.137	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	1
81.218.118.126	Israel	147.237.72.166	aka.idf.il	Abnormally Long Header Line request header name	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
132.68.150.6	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/2/	Block	1
93.190.152.161	Europe	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/8/	Block	1
50.62.161.33	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/test/wp-admin/	Block	1
81.218.118.126	Israel	147.237.72.166	aka.idf.il	Malformed URL	Block	1
37.187.114.171	France	147.237.77.234	halag.idf.il	Unauthorized URL Access to /irj/portal	Block	1
213.57.213.209	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
2.53.174.50	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/main/sachar/faq.aspx	None	1
184.168.193.154	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/wp-admin/	Block	1
68.180.231.61	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
66.249.64.149	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
46.60.43.166	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
82.81.83.56	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
81.218.118.126	Israel	147.237.72.166	aka.idf.il	Abnormally Long Request method	Block	1
5.29.240.253	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.234	Block	1
66.102.7.233	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
46.19.85.154	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.19.85.154	Block	1
81.218.118.126	Israel	147.237.72.166	aka.idf.il	NULL Character in Header Name at	Block	1
2.55.46.52	Israel	147.237.76.42	refuah.idf.il	Suspicious Response Code	Block	1

04-12-2016-10:04:09 to 04-12-2016-11:04:09