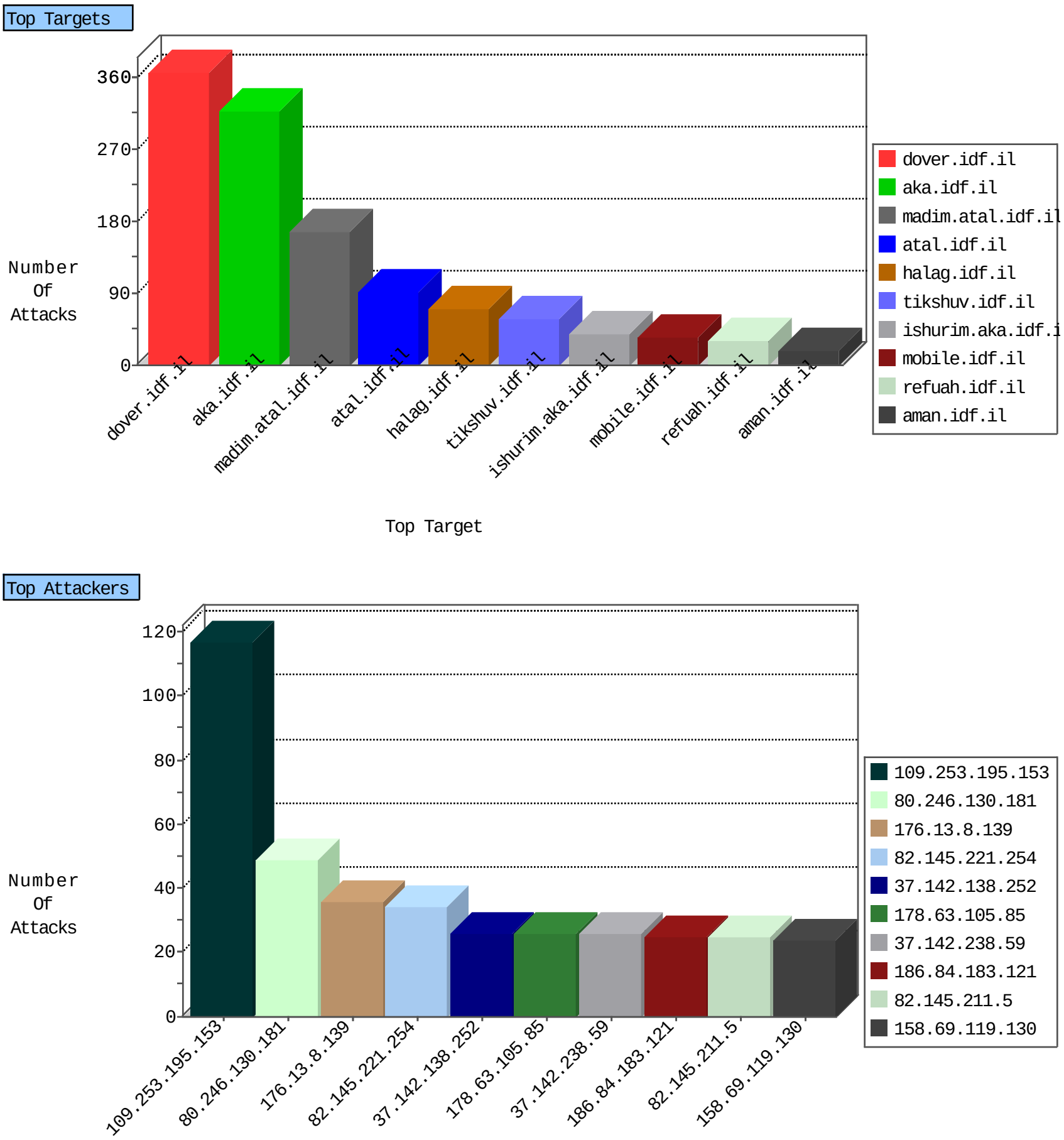
03-06-2016-19:04:00 to 03-06-2016-20:04:00

IDF Under Attack
Daily Report



03-06-2016-19:04:00 to 03-06-2016-20:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.145.221.254	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	34
82.145.211.5	Europe	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	25
134.147.203.115	Germany	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	4
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
134.147.203.115	Germany	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	2
185.94.111.1		147.237.8.24	e.lifestyle.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1		147.237.77.227	e.hamaz.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1		147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1		147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1		147.237.8.14	e.orchot.idf.il	Block_Ntp_All_Net	drop	1
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	1
185.94.111.1		147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1

03-06-2016-19:04:00 to 03-06-2016-20:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
158.69.119.130	United States	147.237.77.216	dover.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	12
158.69.119.130	United States	147.237.77.216	dover.idf.il	22095: HTTP: Joomla Image Manager folderRename Security Bypass Vulnerability	Block	12
84.111.226.92	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
84.110.53.192	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
149.78.204.185	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
62.210.225.135	France	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
89.38.209.50	Romania	147.237.0.34	tikshuv.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
66.135.63.82	United States	147.237.77.226	www.chamatz.aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
158.85.253.245	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
91.227.165.5	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
91.227.164.5	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
66.249.66.190	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
46.19.86.199	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
151.80.31.130	Italy	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-06-2016-19:04:00 to 03-06-2016-20:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
186.84.183.121	147.237.77.216	Colombia	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	17
62.210.225.135	147.237.72.166	France	aka.idf.il	SQL Injection - Select From	12
89.38.209.50	147.237.0.34	Romania	tikshuv.idf.il	SQL Injection - Select From	6
158.85.253.245	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
66.135.63.82	147.237.77.226	United States	www.chamatz.aka.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	4
202.124.109.87	147.237.72.166	New Zealand	aka.idf.il	SQL Injection - Select From	3
185.3.144.54	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.250	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.79.115	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.65.133.205	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.29.201.172	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
210.121.84.97	147.237.76.30	Korea, Republic of	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
94.102.48.193	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
196.47.173.21	147.237.76.30	Cote D'Ivoire	himush.idf.il	ET SCAN NMAP -sS window 2048	1
196.47.173.21	147.237.76.30	Cote D'Ivoire	himush.idf.il	ET SCAN NMAP -f -sS	1
80.246.139.27	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
196.47.173.21	147.237.8.14	Cote D'Ivoire	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
78.32.136.2	147.237.0.19	United Kingdom	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
192.116.190.42	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
61.163.231.229	147.237.77.205	China	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
185.32.179.175	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.121.211.91	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.142.206.111	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.76.124.254	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.187.182	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.4.51	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.139.136.159	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
196.47.173.21	147.237.76.30	Cote D'Ivoire	himush.idf.il	ET SCAN NMAP -sS window 1024	1
84.108.173.1	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
196.47.173.21	147.237.8.14	Cote D'Ivoire	e.orchot.idf.il	ET SCAN NMAP -sS window 2048	1
80.246.136.113	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
196.47.173.21	147.237.8.14	Cote D'Ivoire	e.orchot.idf.il	ET SCAN NMAP -f -sS	1
192.117.104.36	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
61.163.231.229	147.237.77.233	China	atal.idf.il	ET SCAN NMAP -sS window 1024	1
52.87.243.150	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1

03-06-2016-19:04:00 to 03-06-2016-20:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
80.246.130.181	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	48
46.116.36.45	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
46.19.86.16	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	14
37.142.238.59	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
37.142.238.59	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
80.246.133.190	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
212.179.225.154	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.237	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
80.74.102.68	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
79.177.196.232	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.142.138.252	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
37.142.138.252	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
109.253.143.187	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.67	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
109.253.143.187	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.85.251	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.158	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.26	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
178.63.105.85	Germany	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	6
46.19.85.253	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.134.81	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.33	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.41.149	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.98.224	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.134.81	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.251	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.180.104.138	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.178.113.247	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.82	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.181.9.158	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.52.195	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.147.252	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.158	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.13	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.210.149.119	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
192.114.105.254	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	6
217.132.136.149	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.40.183	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.54.4.51	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.86.148	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
91.200.12.141	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
79.183.54.166	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.237	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
5.102.195.173	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.200	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
217.132.136.149	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
2.54.4.51	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.158	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.86.203	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
217.132.136.149	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4

03-06-2016-19:04:00 to 03-06-2016-20:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.195.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	117
176.13.8.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
79.178.165.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
75.99.135.227	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	4
66.102.7.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
46.19.86.117	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
50.63.197.56	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 50.63.197.56	Block	2
79.180.206.229	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl66.y in www.aka.idf.il/main/sachar/payslips.aspx	None	2
37.26.148.140	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
17.138.56.26	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	2
66.102.7.226	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
79.177.196.232	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
66.249.64.235	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
95.175.104.77	Finland	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
87.71.6.125	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1
46.116.36.45	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
79.180.206.229	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl104.x in www.aka.idf.il/main/sachar/payslips.aspx	None	1
32.213.89.25	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
184.73.90.50	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
109.65.103.213	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 109.65.103.213	Block	1
92.253.126.93	Jordan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
46.19.85.203	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
80.246.130.206	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.178.1.34	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
8.18.120.105	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/shared/usercontrols/headerupper/	Block	1
141.212.122.129	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to /x	Block	1
66.249.64.240	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
103.15.132.132	Hong Kong	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
87.71.45.212	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/https:/www.aman.idf.il/	Block	1
189.40.65.228	Brazil	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
109.65.103.213	Israel	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	1
77.126.237.221	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
93.172.162.104	Israel	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	1
66.102.7.240	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.86.3	Israel	147.237.76.39	mobile.meitav.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtPassword in mobile.meitav.idf.il/templates/login.aspx	Block	1
80.246.133.190	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
8.18.122.156	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/shared/usercontrols/headerupper/	Block	1
157.55.39.78	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
66.249.66.182	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
109.65.103.213	Israel	147.237.0.34	tikshuv.idf.il	Distributed PHP Attempt	Block	1
89.139.243.11	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
50.63.197.56	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
79.180.206.229	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl67 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
37.142.68.100	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
109.65.103.213	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 109.65.103.213	Block	1
79.176.55.240	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
66.249.64.13	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
93.172.162.104	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/xmlrpc.php	Block	1
87.69.79.31	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/faq.aspx	Block	1
79.179.107.95	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1

03-06-2016-19:04:00 to 03-06-2016-20:04:00