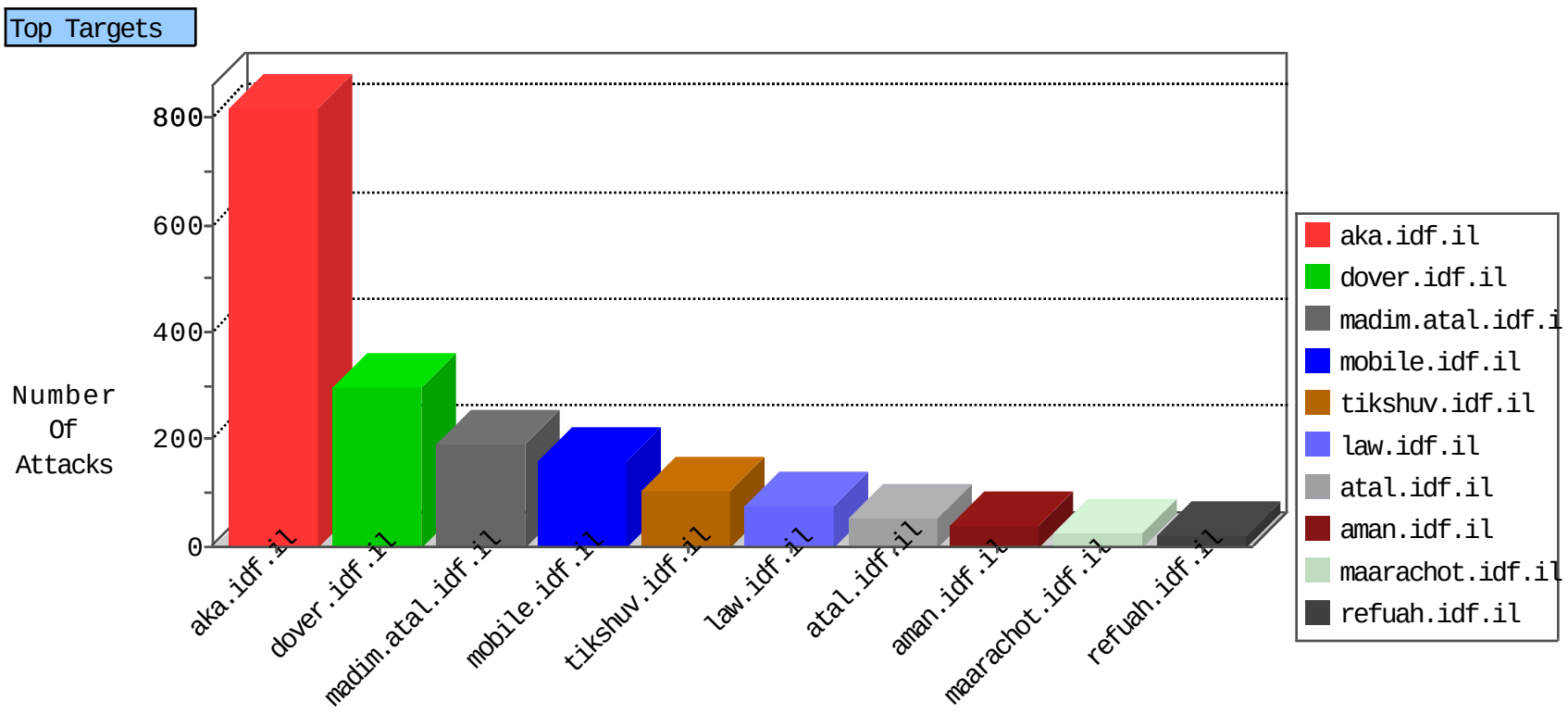
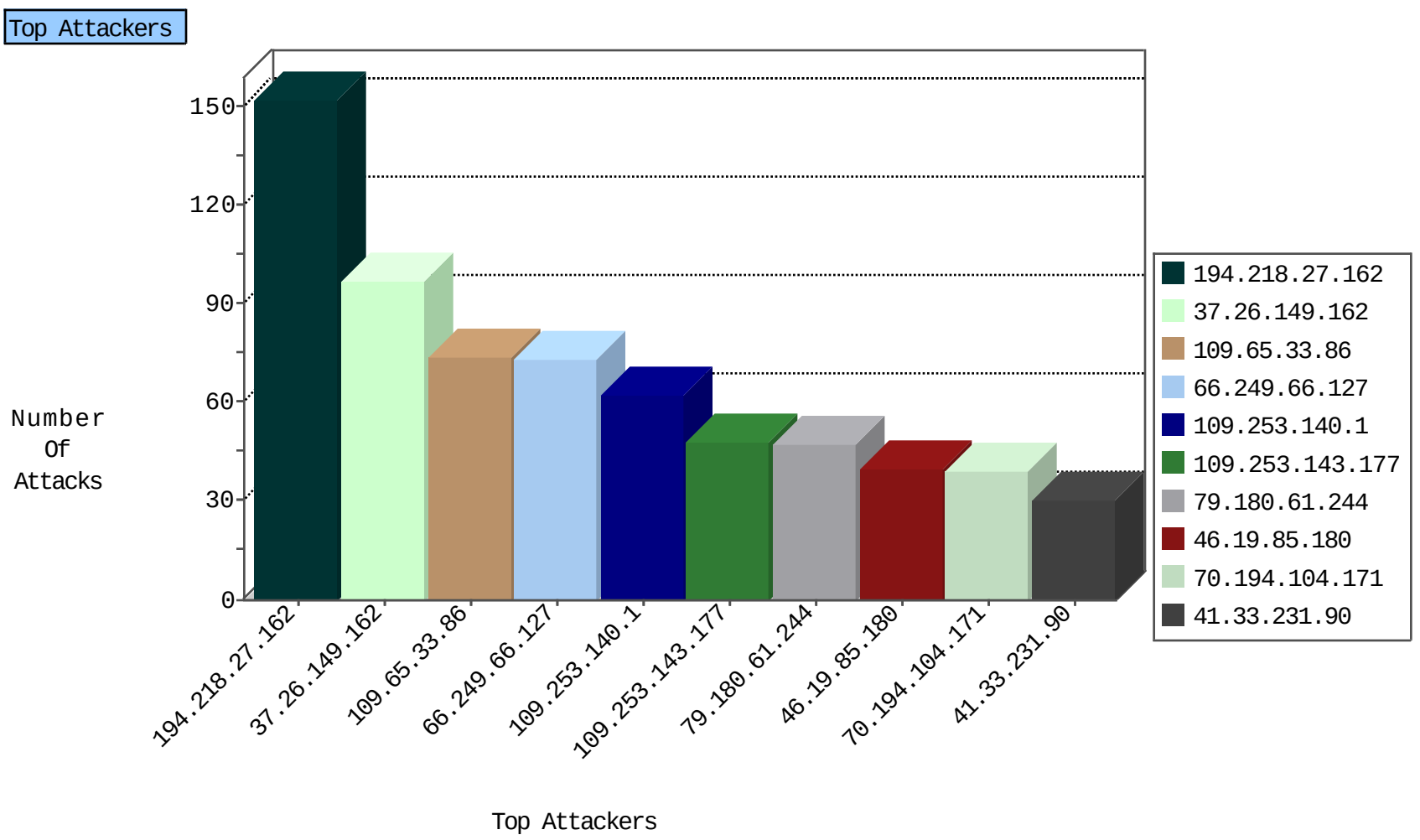
02-29-2016-09:04:06 to 02-29-2016-10:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-29-2016-09:04:06 to 02-29-2016-10:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.180.12.103	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
82.145.219.82	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	3
93.80.161.65	Russian Federation	147.237.77.233	atal.idf.il	JLM_Purple_Con_Limit_Http	drop	3
93.80.161.65	Russian Federation	147.237.77.233	atal.idf.il	JLM_Under_Attack_Con_Http	drop	2
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
198.23.141.210	United States	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.102	United States	147.237.0.35	akaws.idf.il	Block_Ntp_All_Net	drop	1
222.99.172.119	Korea, Republic of	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.114	United States	147.237.77.121	e.navy.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.86	United States	147.237.77.234	halag.idf.il	Block_Ntp_All_Net	drop	1
198.23.141.210	United States	147.237.77.243	mobile.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.102	United States	147.237.77.205	prisha.idf.il	Block_Ntp_All_Net	drop	1
180.182.220.133	Korea, Republic of	147.237.77.19	law-forum.idf.il	Block_Udp_All_Nets	drop	1
222.99.172.119	Korea, Republic of	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.118	United States	147.237.8.28	e.mobile-ks.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.98	United States	147.237.77.227	e.hamaz.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.106	United States	147.237.77.178	e.matpash.idf.il	Block_Ntp_All_Net	drop	1
180.182.220.133	Korea, Republic of	147.237.77.205	prisha.idf.il	Block_Udp_All_Nets	drop	1
222.99.172.119	Korea, Republic of	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.122	United States	147.237.77.243	mobile.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.98	United States	147.237.77.235	sviva.idf.il	Block_Ntp_All_Net	drop	1
222.99.172.119	Korea, Republic of	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.114	United States	147.237.8.24	e.lifestyle.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.74	United States	147.237.77.212	e.dover.idf.il	Block_Ntp_All_Net	drop	1
65.34.47.111	United States	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	1
222.99.172.119	Korea, Republic of	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1

02-29-2016-09:04:06 to 02-29-2016-10:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
193.43.245.250	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
193.43.246.250	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
69.30.215.106	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
37.26.148.189	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
66.249.64.180	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
69.30.215.106	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
108.59.8.80	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
37.26.146.223	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
46.43.126.100	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	14170: HTTP: Blank User-Agent (descriptor but no string)	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

02-29-2016-09:04:06 to 02-29-2016-10:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.66.127	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	73
79.180.61.244	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
113.163.164.237	147.237.76.44	Vietnam	e.refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
37.26.146.254	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.159.144.107	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.28.169.21	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.69.204.136	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.130.223	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.111.233.218	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
217.194.198.114	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.178.200.5	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.101.55	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.143.104.105	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
164.39.11.198	147.237.77.235	United Kingdom	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.154	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
136.243.130.9	147.237.77.212	Germany	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
37.142.216.129	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.131.206	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.29.236.123	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.174.93.96	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
2.54.163.222	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.228.56.206	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.130.57	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.109.80.51	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.179.222.225	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.178.124.106	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.179.1.186	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
208.115.113.89	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
46.151.52.210	147.237.76.202	Ukraine	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
164.39.11.198	147.237.77.212	United Kingdom	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.71	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

02-29-2016-09:04:06 to 02-29-2016-10:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	101
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	51
109.65.33.86	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
70.194.104.171	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
2.52.37.98	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
109.65.33.86	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	25
69.31.51.121	Anonymous Proxy	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	24
93.80.161.65	Russian Federation	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	20
2.54.16.106	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	20
79.180.61.244	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	19
84.95.215.19	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	16
37.26.148.156	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.132.30	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.221.124	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.144	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
46.19.85.144	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
109.253.140.221	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
109.253.140.221	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
80.178.101.40	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
80.246.140.207	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
217.194.203.52	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	10
79.180.61.244	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
62.219.198.6	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
176.13.21.111	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
94.230.93.227	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
176.13.6.248	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.146.133	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
80.246.130.218	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
46.19.85.65	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
2.54.4.158	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
94.230.93.179	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
94.230.93.140	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.111	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.164.119	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
94.230.93.163	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.140.226	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.104	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
94.230.93.131	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.179.21.194	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
94.230.93.166	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.104	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.65.58.86	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
94.230.93.214	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.0	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.31.162	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
149.78.24.30	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

02-29-2016-09:04:06 to 02-29-2016-10:04:06

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
80.246.136.162	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.12.103	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.179.102.167	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.149.162	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 37.26.149.162	Block	91
109.253.140.1	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	62
109.253.143.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
46.19.85.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
176.13.2.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	20
66.249.69.26	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	16
85.64.228.236	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 85.64.228.236	Block	14
82.166.22.37	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 82.166.22.37	Block	7
109.253.202.13	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
2.54.39.226	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
109.253.221.124	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
37.26.148.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.250.245.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.198.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.149.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.81.212	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
46.19.86.90	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	3
37.26.149.162	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1597	Block	3
207.46.13.107	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.210.182.59	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/	Block	2
81.218.13.130	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 81.218.13.130	Block	2
176.13.9.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.60	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	2
157.55.2.152	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
37.26.146.184	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
79.180.61.244	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
66.249.81.218	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.85.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.149.167	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	2
66.249.79.10	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;amp;docId in www.aka.idf.il/brothers/skira/default.asp	None	1
82.102.136.65	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.66.21	United States	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.66.21	Block	1
79.183.169.121	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl17 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
46.19.86.45	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
37.26.148.195	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
123.211.14.144	Australia	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.79.222	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;pageNum in aka.idf.il/iturim/asp/displayallsoldiers.asp	None	1
66.249.69.32	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20477-he/dover.aspx	Block	1
31.154.19.5	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 31.154.19.5	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1927-he/cogat.aspx	Block	1
40.77.167.24	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
66.249.79.10	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;catID in www.aka.idf.il/giyus/forms/downloadform.asp	None	1
37.26.148.170	Israel	147.237.0.19	madim.atal.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.54.140.226	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.66.21	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1750	Block	1
212.117.136.6	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 212.117.136.6	Block	1
79.183.169.121	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl41 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.78.80	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
31.168.182.240	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy.	Block	1