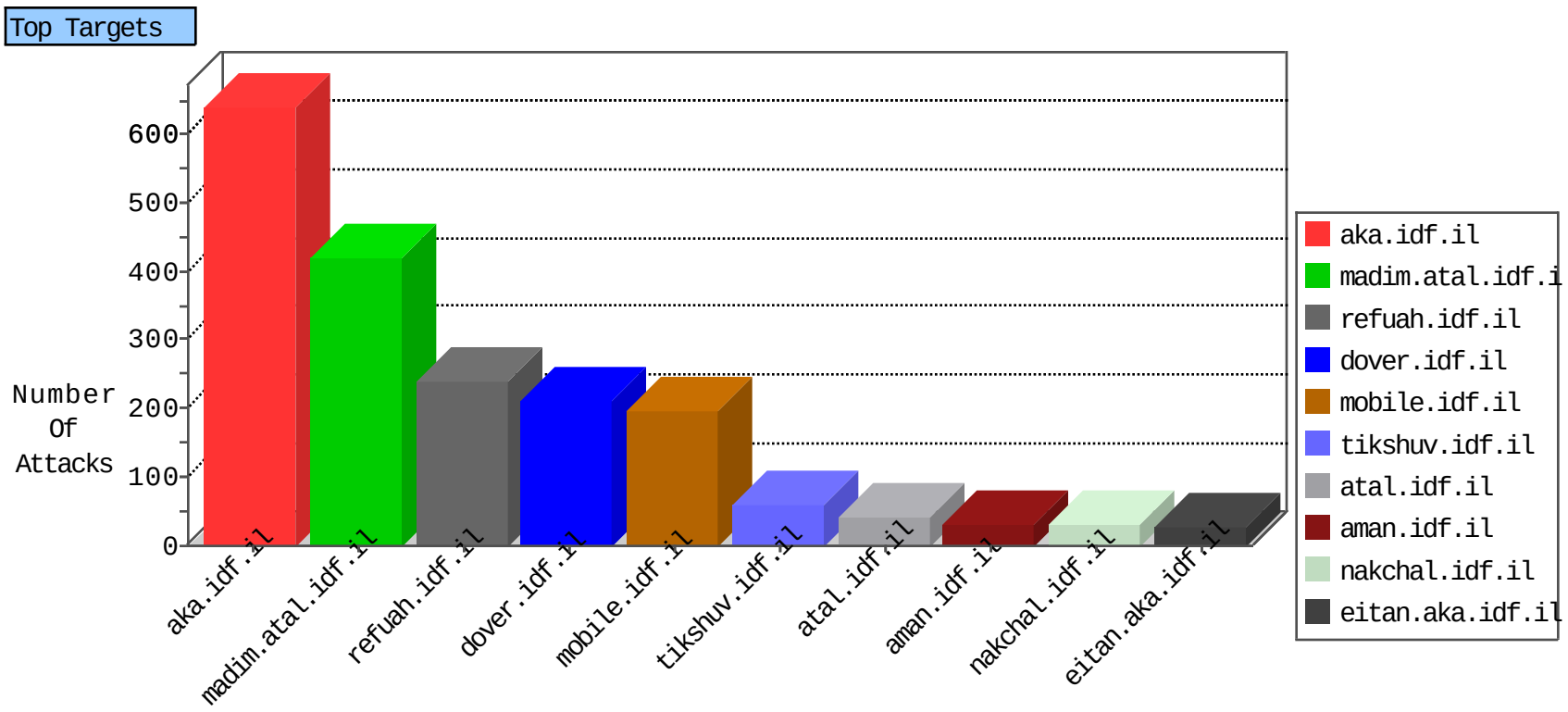
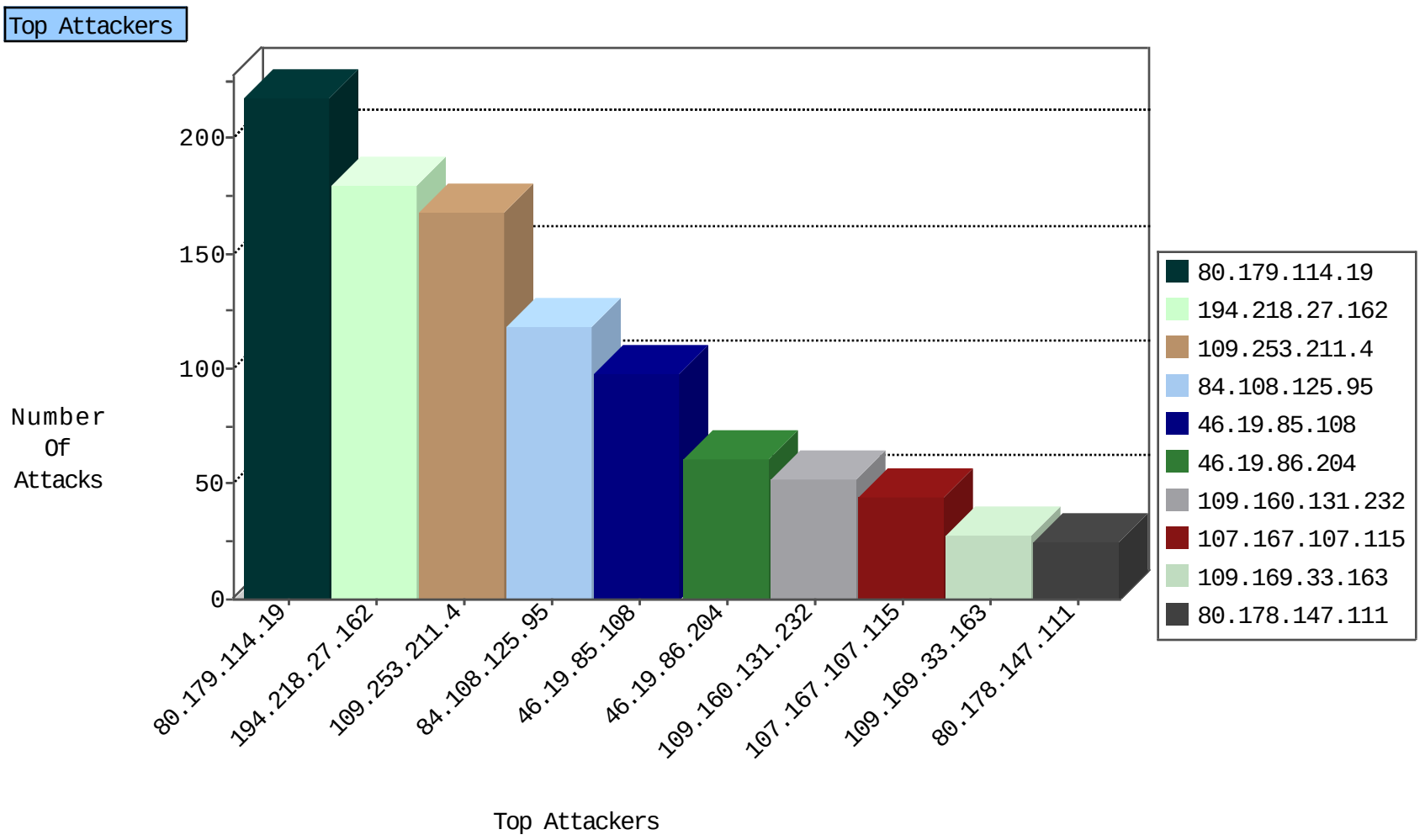
03-01-2016-18:04:06 to 03-01-2016-19:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-01-2016-18:04:06 to 03-01-2016-19:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.237.184.123	Iraq	147.237.77.216	dover.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	2
66.249.66.96	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
208.67.1.70	United States	147.237.8.24	e.lifestyle.idf.il	Block_Ntp_All_Net	drop	1
188.138.57.49	Germany	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
208.67.1.70	United States	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
31.13.102.105	Ireland	147.237.77.216	dover.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
188.138.57.49	Germany	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
220.108.165.150	Japan	147.237.77.19	law-forum.idf.il	Block_Udp_All_Nets	drop	1
208.67.1.70	United States	147.237.8.14	e.orchot.idf.il	Block_Ntp_All_Net	drop	1

03-01-2016-18:04:06 to 03-01-2016-19:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.150.189.2	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
84.109.181.137	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
87.71.72.103	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
84.228.28.56	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
80.246.133.216	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	2
84.109.18.197	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
192.116.55.245	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
5.28.183.129	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
199.30.24.240	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
31.154.158.133	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
51.255.162.163	United Kingdom	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2

03-01-2016-18:04:06 to 03-01-2016-19:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	8
80.246.130.172	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
219.146.12.120	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.183	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.71.59.57	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.8.46	China	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
85.65.145.23	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
188.120.152.77	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.142.230.166	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.138.11	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
27.209.85.196	147.237.8.14	China	e.orchot.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.130.5.165	147.237.77.227		e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
79.183.133.243	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.165	147.237.76.199		e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
79.181.229.250	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.165	147.237.76.42		refuah.idf.il	ET SCAN Potential SSH Scan	1
79.176.111.102	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.220	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.93.29	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
220.178.252.141	147.237.0.34	China	tikshuv.idf.il	SERVER-APACHE Apache Tomcat Web Application Manager access	1
137.226.113.7	147.237.77.176	Germany	matpash.idf.il	ET SCAN Suspicious User-Agent Containing Web Scan/er, Likely Web Scanner	1
219.146.12.120	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
46.116.46.173	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.87.16.148	147.237.77.176		matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
219.146.12.120	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.3	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.70.25.231	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
208.52.144.78	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
40.117.149.78	147.237.76.39	United States	mobile.meitav.idf.i	ET SCAN NMAP -sS window 4096	1
85.64.102.16	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.154.94.14	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.165	147.237.77.234		halag.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.165	147.237.76.200		eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
79.182.56.130	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.165	147.237.76.177		ncore.idf.il	ET SCAN Potential SSH Scan	1
79.179.231.200	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.165	147.237.72.156		aman.idf.il	ET SCAN Potential SSH Scan	1
77.126.191.14	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
159.253.248.28	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.120.130.3	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
219.146.12.120	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.193	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN NMAP -sS window 1024	1

03-01-2016-18:04:06 to 03-01-2016-19:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
80.179.114.19	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	212
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	120
84.108.125.95	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	118
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	60
107.167.107.115	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	44
80.178.147.111	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
109.169.33.163	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	24
109.67.38.18	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
212.179.21.194	Israel	147.237.76.177	ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	22
46.19.85.3	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
38.93.232.120	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
79.177.217.184	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
109.67.214.130	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
178.140.27.226	Russian Federation	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
185.32.179.159	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.26.148.150	Israel	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	8
51.39.33.28	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.116.39.62	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
5.22.134.209	Israel	147.237.72.166	aka.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
216.86.59.131	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.240	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.176	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.181.191.239	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.176	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
85.130.202.239	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.95.134.220	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.154.11	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.146.77	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
149.78.47.171	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.173.21	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.13	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
31.210.186.130	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
87.69.93.154	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
195.34.139.6	Austria	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
31.210.187.136	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
176.13.20.128	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
185.32.179.213	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
37.26.148.150	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
109.169.33.163	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
178.140.27.226	Russian Federation	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.54	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
176.13.20.128	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
212.101.249.140	Lebanon	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.148.150	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.85.170	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
109.67.160.166	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.170	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
31.210.187.199	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

03-01-2016-18:04:06 to 03-01-2016-19:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.211.4	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	168
46.19.85.108	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	98
46.19.86.204	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	61
109.160.131.232	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	52
80.178.189.27	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 80.178.189.27	Block	11
46.19.86.144	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	7
5.29.71.33	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 5.29.71.33	Block	7
66.249.78.146	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/sachar/forms/downloadform.asp	Block	7
217.132.2.53	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 217.132.2.53	Block	7
46.19.85.219	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
109.253.212.46	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
80.178.189.27	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	6
2.52.154.11	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
37.26.148.241	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
132.76.50.6	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 132.76.50.6	Block	5
31.154.190.155	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
217.132.2.53	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	4
5.29.71.33	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	4
66.249.66.96	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/forms/downloadform.asp	Block	4
46.19.85.127	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.134.144	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
84.108.63.207	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.77	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
132.76.50.6	Israel	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	3
109.65.200.98	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.117.47.161	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/	Block	3
168.63.200.167	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
31.154.94.69	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 31.154.94.69	Block	3
2.54.186.104	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
66.249.69.26	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	2
83.54.196.215	Spain	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
5.22.131.11	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/default.aspx	Block	2
14.120.162.115	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1511-en/dover.aspx/rk=0/rs=ojr2inyjfy4a2zrauyfjypq0coq-	Block	2
2.52.154.11	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	2
31.154.94.69	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
2.54.171.205	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	2
199.203.247.130	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
87.69.73.128	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl51 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
82.166.76.90	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/trigger.png	Block	1
37.26.148.209	Israel	147.237.77.243	mobile.idf.il	Multiple Untraceable SSL Sessions from 37.26.148.209 (Open Mode)	None	1
132.76.50.6	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/ajax/updatestatus.php	Block	1
77.125.6.20	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/idkunpratimishiyim.aspx	Block	1
94.159.153.156	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$82 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
46.121.232.50	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 101 cookies	Block	1
220.178.252.141	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/manager/html	Block	1
168.235.197.27	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
85.64.5.3	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
31.154.94.69	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/updatestatus.php	Block	1
109.253.213.219	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
2.54.191.32	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1

03-01-2016-18:04:06 to 03-01-2016-19:04:06