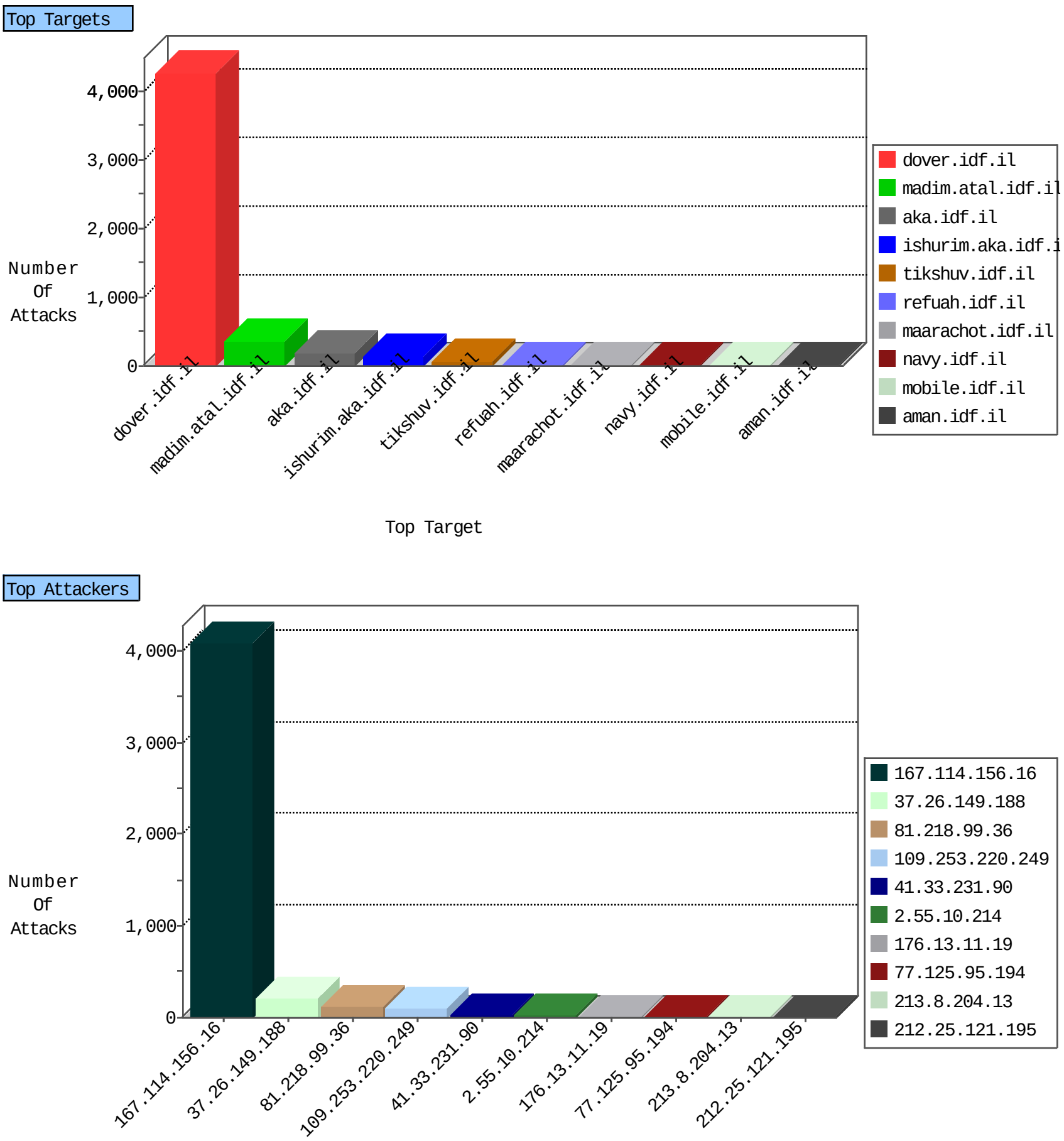
04-11-2016-11:04:07 to 04-11-2016-12:04:07

IDF Under Attack Daily Report



04-11-2016-11:04:07 to 04-11-2016-12:04:07

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	4087
77.158.88.42	France	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	320
77.158.89.41	France	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	150
149.78.50.113	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	74
212.25.121.195	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	6
212.25.121.195	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
212.179.64.162	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
134.191.232.68	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
216.218.206.81	United States	147.237.77.205	prisha.idf.il	Block_Udp_All_Nets	drop	1
179.43.144.50	Switzerland	147.237.72.14	dover.idf.il(old)	Block_Ntp_All_Net	drop	1
82.221.105.7	Iceland	147.237.77.19	law-forum.idf.il	Block_Udp_All_Nets	drop	1
179.43.141.194	Switzerland	147.237.77.61	e.cogat.idf.il	Block_Ntp_All_Net	drop	1
80.246.139.171	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1
179.43.144.50	Switzerland	147.237.77.234	halag.idf.il	Block_Ntp_All_Net	drop	1
41.21.161.151	South Africa	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
179.43.141.194	Switzerland	147.237.77.176	matpash.idf.il	Block_Ntp_All_Net	drop	1
179.43.144.50	Switzerland	147.237.77.235	sviva.idf.il	Block_Ntp_All_Net	drop	1
179.43.144.50	Switzerland	147.237.8.50	e.tikshuv.idf.il	Block_Ntp_All_Net	drop	1
82.145.211.116	Europe	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	1
184.105.139.85	United States	147.237.0.15	kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1

04-11-2016-11:04:07 to 04-11-2016-12:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.125.95.194	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
91.197.103.1	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
213.8.204.40	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
82.81.76.144	Israel	147.237.77.170	maarachot.idf.il	C1000008: HTTP: Xenu UserAgent	Block	6
87.69.134.147	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
217.132.118.149	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
77.126.142.236	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
37.26.147.204	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
51.254.215.130	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
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

04-11-2016-11:04:07 to 04-11-2016-12:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
80.246.139.171	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
80.82.78.38	147.237.0.33	Netherlands	idf.il	ET SCAN NMAP -sS window 1024	1
208.100.26.228	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.217	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	1
176.13.0.205	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.168.67.206	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.78.48.204	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
115.28.218.77	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
82.80.193.240	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.136.226	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.244.82.139	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	portscan: TCP Distributed Portscan	1
80.82.78.38	147.237.76.197	Netherlands	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
212.199.57.193	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.103	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1
208.100.26.228	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.178	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
191.55.74.165	147.237.0.35	Brazil	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
37.26.146.231	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.88.156.194	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.78.36.125	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
109.186.154.228	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.178.205.141	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.8.204.40	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

04-11-2016-11:04:07 to 04-11-2016-12:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
81.218.99.36	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	111
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	29
2.55.10.214	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
46.19.85.140	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	8
5.29.154.233	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
84.95.252.189	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
2.54.132.15	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.219.229.32	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.168.13.78	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
62.0.197.69	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
2.54.143.211	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.253.137.241	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.158.88.42	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
213.8.204.13	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
213.8.204.13	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
37.26.149.188	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence		monitor	4
85.64.215.202	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
82.80.23.114	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.86.124	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
176.13.11.19	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.179.25.225	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
37.26.149.188	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence		alert	4
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.182.11.51	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.6.240	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.64.156.155	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
192.114.91.248	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.242.15	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.120.206.229	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
185.3.146.195	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
178.154.189.8	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.110	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.211.182	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.43.179	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.178.205.141	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.67.145.239	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.5.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
118.173.130.68	Thailand	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
199.203.84.86	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.53	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.42	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.71.18.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.147.192	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
132.64.165.70	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.197.77	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.148	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.166.134.138	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.11.137	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-11-2016-11:04:07 to 04-11-2016-12:04:07

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
46.19.85.105	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3

04-11-2016-11:04:07 to 04-11-2016-12:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.149.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	205
109.253.220.249	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
176.13.11.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
109.253.146.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
176.13.21.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.10.51	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.55.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.149	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
46.19.85.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.179.25.225	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
37.26.149.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.52.167.164	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
213.254.241.4	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
176.13.20.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
175.43.95.77	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 175.43.95.77	Block	2
216.218.206.68	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
79.178.192.192	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
46.19.86.154	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.i	Malformed URL	Block	1
81.218.53.114	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/_vti_bin/owssvr.dll	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
194.114.146.227	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
175.43.95.77	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-9703-en/dover.aspxjavascript:	Block	1
2.55.10.214	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
217.132.122.96	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/general.aspx	Block	1
178.141.253.188	Russian Federation	147.237.77.74	law.idf.il	Parameter Type Violation FileName in www.law.idf.il/templates/getfile/getfile.aspx	Block	1
46.116.35.169	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/forms	Block	1
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.i	Multiple Unknown HTTP Request Method from 169.229.3.91	Block	1
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	1
68.180.230.187	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/894-en	Block	1
213.8.204.40	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giuse	Block	1
46.19.86.99	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
125.206.36.218	Japan	147.237.77.216	dover.idf.il	Parameter Type Violation ID in www.idf.il/1294-en/dover.aspx	Block	1
31.168.208.149	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl13 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
80.178.126.169	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.117.6.93	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/promotioncube/	Block	1
178.141.253.188	Russian Federation	147.237.77.74	law.idf.il	Parameter Type Violation InfoCenterItem in www.law.idf.il/templates/getfile/getfile.aspx	Block	1
41.45.126.121	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Illegal Byte Code Character in Method	Block	1
82.81.70.160	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
2.53.50.102	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.75.76.161	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/page/33/	Block	1
213.151.32.163	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/tizmoret/faq/default.asp	None	1
31.184.238.200	Russian Federation	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/656-en/	Block	1
157.55.39.194	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/giyus/qanda/default.asp	None	1
81.218.53.114	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 81.218.53.114	Block	1
52.30.171.229	Ireland	147.237.72.166	aka.idf.il	Unauthorized URL Access to /	Block	1
192.115.248.2	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	1

04-11-2016-11:04:07 to 04-11-2016-12:04:07