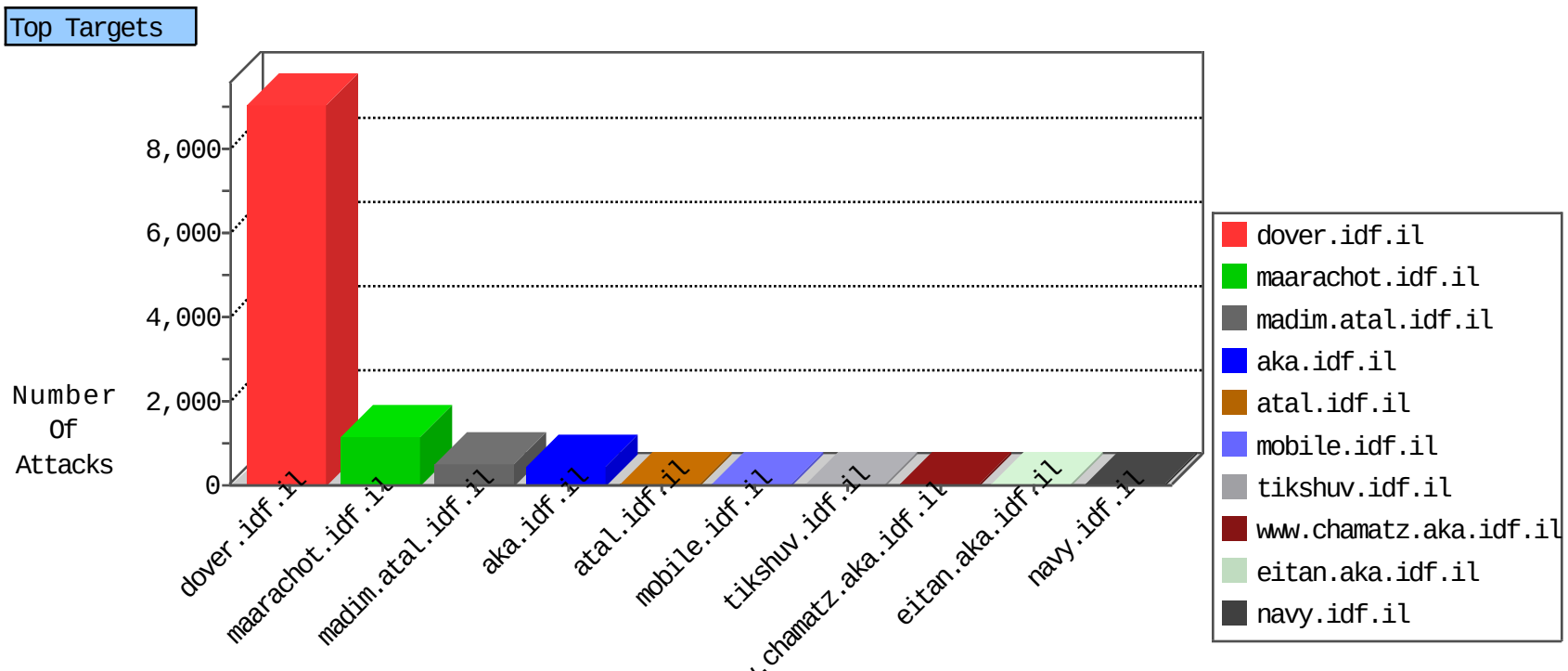
04-07-2016-16:04:01 to 04-07-2016-17:04:01

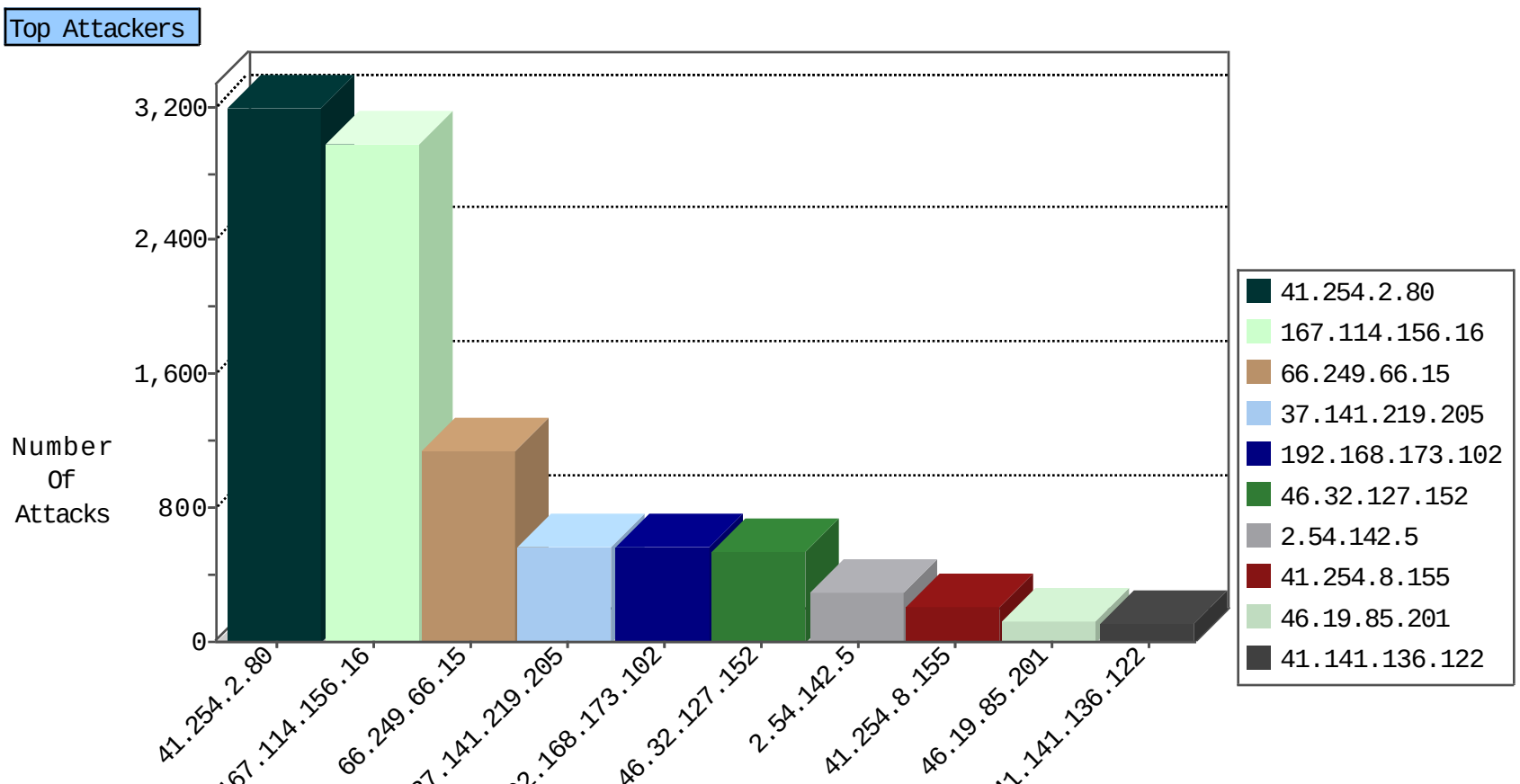
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

04-07-2016-16:04:01 to 04-07-2016-17:04:01

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	2974
41.254.2.80	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-cat	dest-reset	424
41.254.8.155	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	176
41.254.2.80	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	115
41.141.136.122	Morocco	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	102
41.248.233.173	Morocco	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	102
41.248.236.37	Morocco	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	102
105.154.177.75	Morocco	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	56
212.175.142.140	Turkey	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	31
41.254.8.155	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-cat	dest-reset	26
46.32.127.152	Jordan	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	15
79.182.163.119	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	6
37.239.68.65	Iraq	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
37.239.68.12	Iraq	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
37.141.219.205	Saudi Arabia	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
37.239.68.12	Iraq	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
37.239.68.65	Iraq	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
37.141.219.205	Saudi Arabia	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	1
105.155.151.159	Morocco	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
37.141.219.205	Saudi Arabia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
8.37.71.30	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
41.251.18.79	Morocco	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1

04-07-2016-16:04:01 to 04-07-2016-17:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.57.45.108	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
80.246.133.232	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
212.143.66.129	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
79.179.66.52	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
188.120.148.194	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
192.187.114.11	United States	147.237.77.216	dover.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	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
66.249.78.127	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-07-2016-16:04:01 to 04-07-2016-17:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.66.15	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1138
41.254.2.80	147.237.77.216	Libyan Arab Jamahiriya	dover.idf.il	ET CURRENT_EVENTS Inbound Low Orbit Ion Cannon LOIC DDOS Tool desu string	4
197.2.105.86	147.237.76.39	Tunisia	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
197.2.105.86	147.237.76.44	Tunisia	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
197.2.105.86	147.237.76.34	Tunisia	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
197.2.105.86	147.237.76.30	Tunisia	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
197.2.105.86	147.237.76.31	Tunisia	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
197.2.105.86	147.237.77.19	Tunisia	law-forum.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
197.2.105.86	147.237.76.38	Tunisia	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
46.120.23.151	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.79	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
151.28.149.63	147.237.77.216	Italy	dover.idf.il	portscan: TCP Distributed Portscan	1
216.214.179.76	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 4096	1
149.88.92.109	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.142.253.130	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
113.190.17.20	147.237.0.16	Vietnam	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
31.168.21.104	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.213.251	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
197.2.105.86	147.237.76.42	Tunisia	refuah.idf.il	ET SCAN Potential SSH Scan	1
95.9.65.77	147.237.0.35	Turkey	akaws.idf.il	ET SCAN NMAP -sS window 3072	1
79.182.63.35	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.151.52.139	147.237.72.166	Ukraine	aka.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.188	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
174.37.194.144	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.76.42	China	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
41.254.8.155	147.237.77.216	Libyan Arab Jamahiriya	dover.idf.il	ET CURRENT_EVENTS Inbound Low Orbit Ion Cannon LOIC DDOS Tool desu string	1
149.200.179.48	147.237.77.216	Jordan	dover.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.74	147.237.76.86	United States	navy.idf.il	ET DROP Dshield Block Listed Source	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	1
149.78.154.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
197.2.105.86	147.237.76.86	Tunisia	navy.idf.il	ET SCAN Potential SSH Scan	1
31.168.80.57	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.67.172.247	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.145.1	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
197.2.105.86	147.237.76.42	Tunisia	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
105.105.167.102	147.237.77.216	Algeria	dover.idf.il	portscan: TCP Distributed Portscan	1
85.64.28.154	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
197.2.105.86	147.237.76.38	Tunisia	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5800-5820	1

04-07-2016-16:04:01 to 04-07-2016-17:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.254.2.80	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1585
41.254.2.80	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	562
46.32.127.152	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	512
37.141.219.205	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	504
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	343
41.254.2.80	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	SYN Attack		reject	228
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	226
41.254.2.80	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	196
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	77
141.0.13.80	Norway	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	72
41.254.2.80	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	61
82.173.114.35	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
41.254.2.80	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	52
2.54.152.237	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	40
37.141.219.205	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	29
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	22
130.133.152.88	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
197.16.200.153	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
41.233.212.209	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
41.254.2.80	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
197.1.106.98	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
46.19.86.27	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
37.141.219.205	Saudi Arabia	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
83.130.127.27	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
84.228.243.103	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
176.12.160.5	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
41.254.2.80	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	10
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
84.228.243.103	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
37.141.219.205	Saudi Arabia	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	10
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
84.108.26.189	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
5.22.135.139	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
41.109.49.41	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
193.43.245.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.53.27.3	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.170	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.155.145	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.181.161.122	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
37.26.148.189	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.3.144.68	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.128.45.253	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
160.178.34.118	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.67.35.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
185.27.106.124	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.57.185	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

04-07-2016-16:04:01 to 04-07-2016-17:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.142.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	291
46.19.85.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	121
2.55.30.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	38
2.53.58.121	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
176.13.17.150	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	8
2.52.134.151	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
185.27.106.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.164.115	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
197.37.178.248	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 141.8.132.78	Block	3
46.19.85.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.22	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
54.186.248.49	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	2
2.55.20.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.222	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
79.179.134.21	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.179.134.21	Block	2
85.132.77.12	Azerbaijan	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	2
41.40.210.19	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.85.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
85.132.77.12	Azerbaijan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/images/	Block	2
149.78.204.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
134.191.232.70	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.54.177.157	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
37.238.204.96	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
66.249.69.34	Israel	147.237.72.166	aka.idf.il	Unknown Parameter hc_location in www.aka.idf.il/main/giyus/general.aspx	None	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Method	Block	1
46.19.85.56	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
132.64.142.38	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1412-he/atal.aspx	Block	1
84.228.243.103	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1135-he/atal.aspx	Block	1
41.40.137.68	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	Unknown HTTP Request Method ·‹ÜÜJÉˆ³k“ in URL	Block	1
41.40.202.147	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
213.8.204.70	Israel	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
105.159.121.18	Morocco	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
38.107.78.130	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
185.120.126.121	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 185.120.126.121	Block	1
62.0.106.175	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/newsarchive.aspx	Block	1
2.53.23.239	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	Abnormally Long Header Line request header name	Block	1
134.191.232.68	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
41.40.139.199	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
212.76.124.159	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	1
173.252.122.123	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/&h=_aqfmh7g_&s=1	Block	1
66.249.66.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/size100x0/3480.jpg	Block	1
141.212.122.209	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
46.19.86.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
213.8.204.70	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/admin	Block	1
109.65.36.56	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
38.107.78.132	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1

04-07-2016-16:04:01 to 04-07-2016-17:04:01