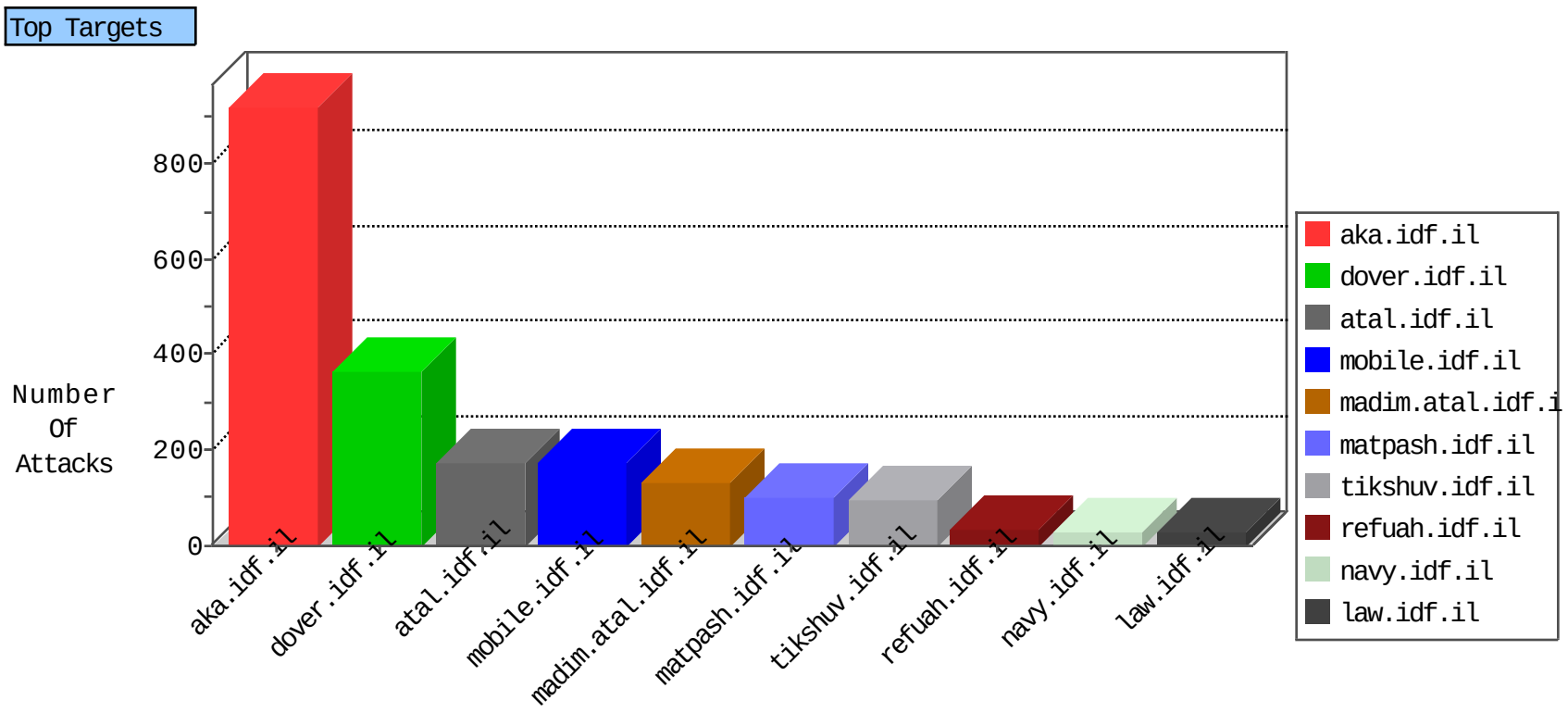
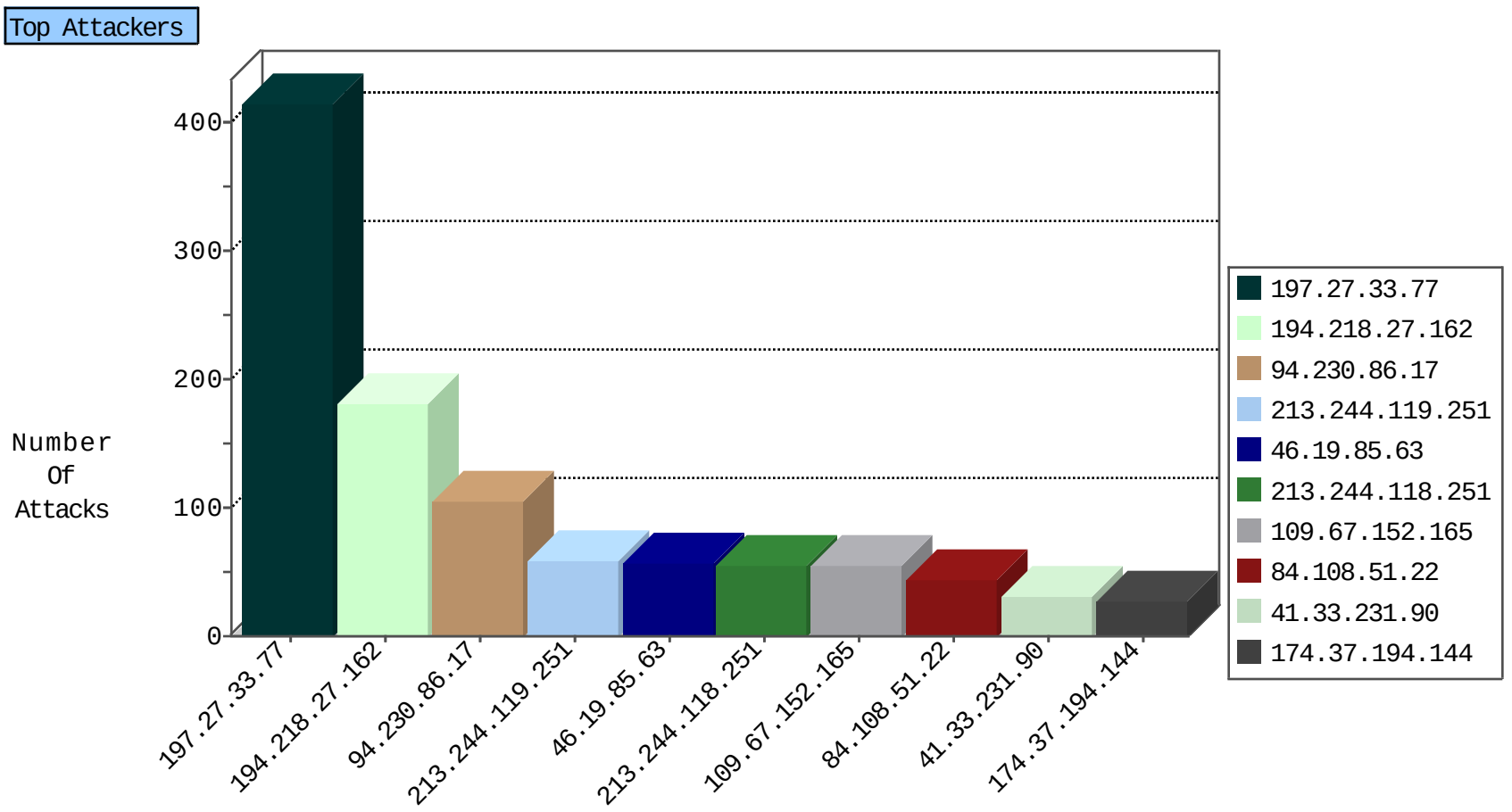
02-29-2016-20:04:00 to 02-29-2016-21:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-29-2016-20:04:00 to 02-29-2016-21:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.145.221.194	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	7
82.145.217.94	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	5
217.26.171.188	Moldova, Republic of	147.237.76.176	test.ncore.idf.il	L4 Source or Dest Port Zero	drop	4
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
185.130.5.224		147.237.77.235	sviva.idf.il	Block_Udp_All_Nets	drop	1
81.218.56.125	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.0.200	m4u.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1		147.237.72.156	aman.idf.il	Block_Ntp_All_Net	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
217.26.171.188	Moldova, Republic of	147.237.77.176	matpash.idf.il	L4 Source or Dest Port Zero	drop	1
185.130.5.201		147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
66.240.192.138	United States	147.237.77.234	halag.idf.il	Block_Udp_All_Nets	drop	1
108.59.4.196	United States	147.237.8.50	e.tikshuv.idf.il	Block_Udp_All_Nets	drop	1

02-29-2016-20:04:00 to 02-29-2016-21:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.65.164.149	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
61.135.189.110	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	8
79.177.51.42	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
2.54.159.136	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
213.57.232.123	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
5.9.111.70	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
69.30.201.98	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
46.116.28.23	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
69.30.201.98	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
51.255.65.27	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	2
51.255.65.95	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
162.250.190.142	Canada	147.237.77.216	dover.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1

02-29-2016-20:04:00 to 02-29-2016-21:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
174.37.194.144	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sA (2)	2
122.141.236.69	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
79.182.124.65	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
122.141.236.69	147.237.76.39	China	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
77.125.104.241	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.67.125.214	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.49	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.173.56.69	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
38.105.146.70	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 4096	1
87.69.251.170	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.102.241.236	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.29.203.226	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.250.234.228	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
186.114.110.196	147.237.76.42	Colombia	refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
84.94.187.254	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
183.56.166.188	147.237.0.200	China	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
80.246.139.196	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
122.141.236.69	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
79.182.148.115	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
122.141.236.69	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
79.177.210.164	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
122.141.236.69	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
46.120.196.145	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.65.116.71	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.71	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
88.249.106.23	147.237.77.235	Turkey	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
38.105.146.70	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 3072	1
217.194.196.7	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.69.98.235	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.52.5.54	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.228.172.46	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.99.32.3	147.237.77.216		dover.idf.il	portscan: TCP Distributed Portscan	1
81.47.142.161	147.237.72.166	Spain	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.130.72	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

02-29-2016-20:04:00 to 02-29-2016-21:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
197.27.33.77	Tunisia	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	153
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	120
94.230.86.17	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	104
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	60
109.67.152.165	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	53
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
84.109.144.248	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
5.22.131.18	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
46.19.86.47	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
66.249.78.216	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
197.27.33.77	Tunisia	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
213.244.119.251	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	16
213.244.118.251	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	15
109.253.133.198	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
213.244.118.251	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	15
46.19.85.183	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
213.244.119.251	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
84.111.155.155	Israel	147.237.8.50	e.tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
100.127.230.44		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
176.13.4.173	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
197.27.33.77	Tunisia	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.65.100.26	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.26.244	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.26.149.220	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.169	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.147	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
37.26.147.224	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
213.244.118.251	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
85.250.176.84	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
46.19.85.169	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	7
77.127.14.48	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.64.198	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.181.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.222.130	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.168.28.44	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.106	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.178.209.151	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.28.174.38	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.8.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
100.127.230.44		147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	6
149.78.45.13	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.102.254.21	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.134.209	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.175	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

02-29-2016-20:04:00 to 02-29-2016-21:04:00

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
79.181.116.173	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.210.186.156	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
128.210.106.73	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.8.134	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
217.132.73.127	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.10.137	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

02-29-2016-20:04:00 to 02-29-2016-21:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
197.27.33.77	Tunisia	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 197.27.33.77	Block	79
46.19.85.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	53
84.108.51.22	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	43
197.27.33.77	Tunisia	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 197.27.33.77	Block	29
197.27.33.77	Tunisia	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 197.27.33.77	Block	25
197.27.33.77	Tunisia	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 197.27.33.77	Block	23
79.181.27.198	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.181.27.198	Block	20
197.27.33.77	Tunisia	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 197.27.33.77	Block	19
197.27.33.77	Tunisia	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 197.27.33.77	Block	18
197.27.33.77	Tunisia	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 197.27.33.77	Block	10
89.138.109.239	Israel	147.237.76.39	mobile.meitav.idf.il	Cookie Tampering on cookie .ASPNETAUTH: Expected 0102C2D23CA73341D308FEC24A7E723641D30800093200300038003000360038003300340036000012F00FF, Observed 0102B186452B3041D308FEB1FE86F63241D3080009320030003800300036003800330034003600000012F00FF	None	10
79.180.14.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
197.27.33.77	Tunisia	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 197.27.33.77	Block	8
91.228.197.248	Poland	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	7
197.27.33.77	Tunisia	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 197.27.33.77	Block	7
197.27.33.77	Tunisia	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 197.27.33.77	Block	6
91.228.197.248	Poland	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 91.228.197.248	Block	6
109.253.133.198	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
46.19.85.106	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	5
66.249.66.184	United States	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il/main/giyus/general.aspx	Block	4
216.35.195.247	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	4
2.54.2.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
95.86.108.88	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 95.86.108.88	Block	3
197.27.33.77	Tunisia	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 197.27.33.77	Block	3
5.29.110.169	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
197.27.33.77	Tunisia	147.237.76.147	chinuch.aka.idf.il	Multiple Unauthorized URL Access from 197.27.33.77	Block	2
109.65.80.48	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
197.27.33.77	Tunisia	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 197.27.33.77	Block	2
149.78.45.13	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
109.65.100.26	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
185.89.217.234		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
170.170.59.133	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
109.253.138.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.10.137	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
170.170.59.133	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
66.102.7.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.66.69	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.66.69	Block	2
149.88.252.13	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
94.159.167.253	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.183	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
84.191.10.118	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	1
207.46.13.22	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
62.109.175.229	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1398-en/dover.aspx	Block	1
149.255.204.93	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
37.26.148.182	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.186.167.8	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
79.177.104.247	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
94.230.86.17	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
193.41.209.2	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1

02-29-2016-20:04:00 to 02-29-2016-21:04:00