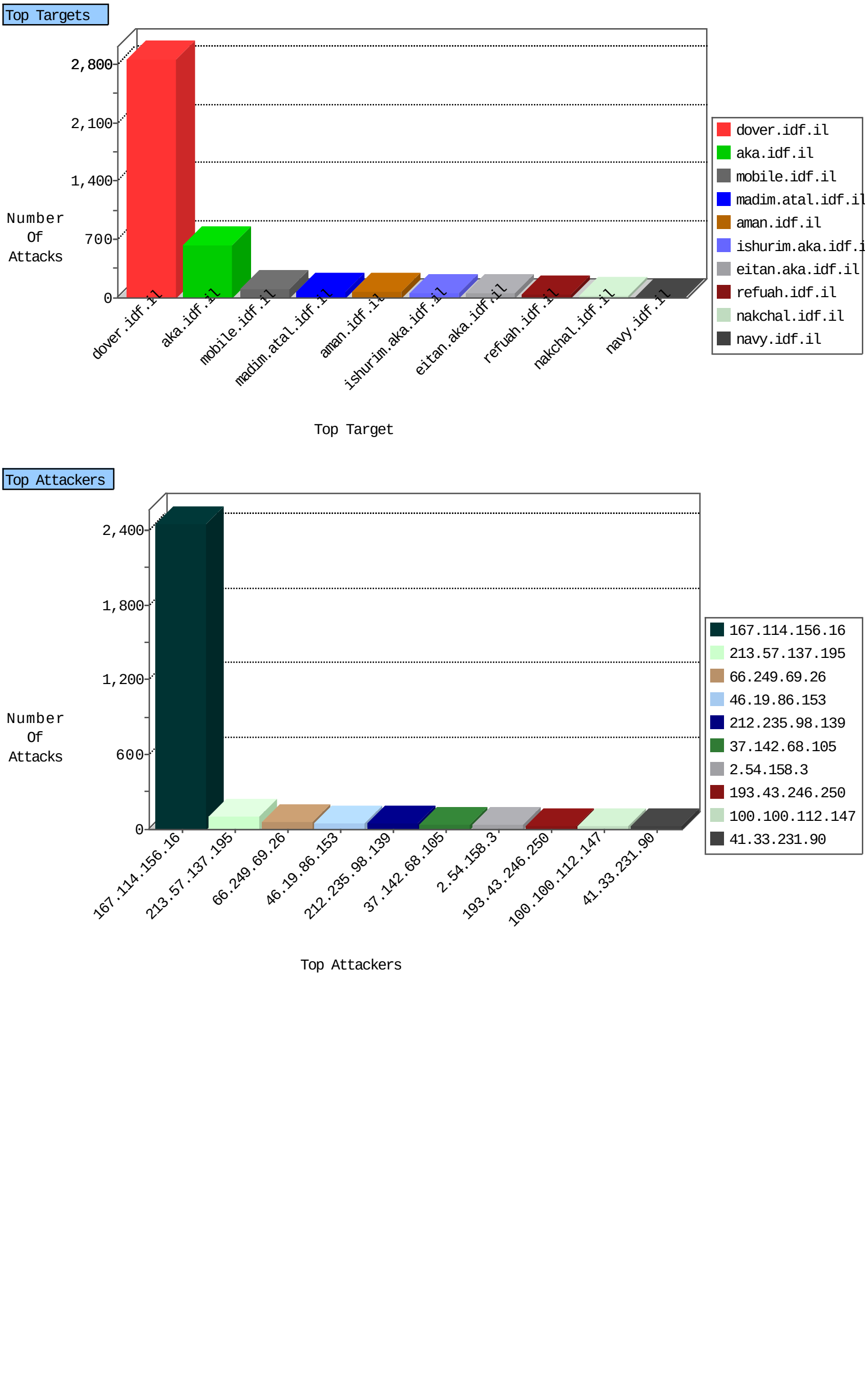
11-30-2015-10:04:06 to 11-30-2015-11:04:06

IDF Under Attack
Daily Report



11-30-2015-10:04:06 to 11-30-2015-11:04:06

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	DOS-Tool-SwitchbladG	dest-reset	3587
82.145.218.169	Europe	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	10
31.168.133.226	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
114.80.122.91	China	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
114.80.122.91	China	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
81.218.56.125	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	1
114.80.122.91	China	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
114.80.122.91	China	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
93.174.93.151	Netherlands	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
114.80.122.91	China	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
114.80.122.91	China	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
114.80.122.91	China	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
114.80.122.91	China	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
66.240.192.138	United States	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
114.80.122.91	China	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
114.80.122.91	China	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
93.174.93.151	Netherlands	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
114.80.122.91	China	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
114.80.122.91	China	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
71.6.165.200	United States	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
114.80.122.91	China	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
114.80.122.91	China	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
93.174.93.151	Netherlands	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1

11-30-2015-10:04:06 to 11-30-2015-11:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
195.154.191.162	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
212.235.62.200	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
188.165.15.32	France	147.237.76.30	himush.idf.il	C228: HTTP: AhrefBot crawler	Block	1

11-30-2015-10:04:06 to 11-30-2015-11:04:06

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	3
77.126.240.126	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
50.204.188.142	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -f -sS	1
220.231.195.122	147.237.77.179	China	e.mazi.idf.il	ET SCAN NMAP -sS window 2048	1
2.54.41.231	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
208.67.1.27	147.237.72.14	United States	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
185.32.179.217	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.173.142.128	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.80.196.44	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.182.171.91	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
50.204.188.142	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 2048	1
2.54.189.254	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
220.231.195.122	147.237.77.179	China	e.mazi.idf.il	ET SCAN NMAP -f -sS	1
2.54.5.115	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
208.67.1.27	147.237.0.200	United States	m4u.idf.il	ET SCAN Potential SSH Scan	1
188.214.128.12	147.237.0.17	Romania	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
85.250.110.45	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.218.153.16	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

11-30-2015-10:04:06 to 11-30-2015-11:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.69.26	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	56
213.57.137.195	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	51
213.57.137.195	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	51
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	46
2.54.158.3	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
46.19.86.31	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
100.100.111.80		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	24
193.43.246.250	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
192.114.3.241	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	18
100.100.112.147		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
212.199.244.112	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	17
2.52.165.50	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
100.100.112.147		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
134.191.232.69	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.154.121	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.249.69.34	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.146	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
207.46.228.208	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	9
46.19.86.153	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.178	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.86.242	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
79.181.150.55	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
95.86.78.46	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
193.43.245.250	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
134.191.232.72	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
193.43.246.250	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	8
79.181.150.55	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
138.134.192.10	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
37.142.68.105	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.91	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.43	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
134.191.232.68	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
169.253.194.1	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.106.226.202	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
213.57.131.247	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
40.77.167.91	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.173	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.164.63	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.238	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.116.252.121	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.60.12	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.127.83.152	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
134.191.232.70	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.174.24	Israel	147.237.77.216	dover.idf.il	SYN Attack		reject	6
2.54.44.134	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
77.125.77.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
157.55.39.38	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.201	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

11-30-2015-10:04:06 to 11-30-2015-11:04:06

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
207.46.13.119	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

11-30-2015-10:04:06 to 11-30-2015-11:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	38
37.142.68.105	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	33
176.12.147.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/$$$&?&?$$$	Block	18
2.54.158.3	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	8
46.19.85.187	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	5
89.138.161.102	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	4
5.150.253.80	Sweden	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
169.253.194.1	United States	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
176.12.151.76	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/login parameter Password	Block	3
146.185.149.117	Netherlands	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
2.54.154.121	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
186.192.129.73	Brazil	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
87.230.85.14	Germany	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
54.252.198.64	Australia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
146.185.149.117	Netherlands	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
2.52.165.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
188.161.245.23	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/894-ar	Block	2
186.192.129.73	Brazil	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
87.230.85.14	Germany	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
2.54.183.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
192.118.11.121	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
46.19.85.47	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/login parameter Password	Block	2
5.150.253.80	Sweden	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.150.253.80	Block	2
212.179.21.194	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ufi/reaction/	Block	2
54.252.198.64	Australia	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
173.252.90.100	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.1.141	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtAreaRemarks in m.my-kosher-kravi.idf.il/templates/training/training.aspx	Block	2
109.67.148.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.42.247	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.181.150.55	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
5.150.253.80	Sweden	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
54.252.198.64	Australia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	2
46.19.86.164	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.179.230	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.136.198	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.46.13.144	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
77.127.109.222	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.16	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
223.240.123.26	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-he/matpash.aspx/trackback/	Block	1
66.249.64.229	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1240-he/atal.aspx	Block	1
176.13.12.203	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.149.177	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
84.111.65.20	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/pniotchangerecruitmentdate.aspx	Block	1
212.179.21.194	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.121.123.170	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.39	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

11-30-2015-10:04:06 to 11-30-2015-11:04:06