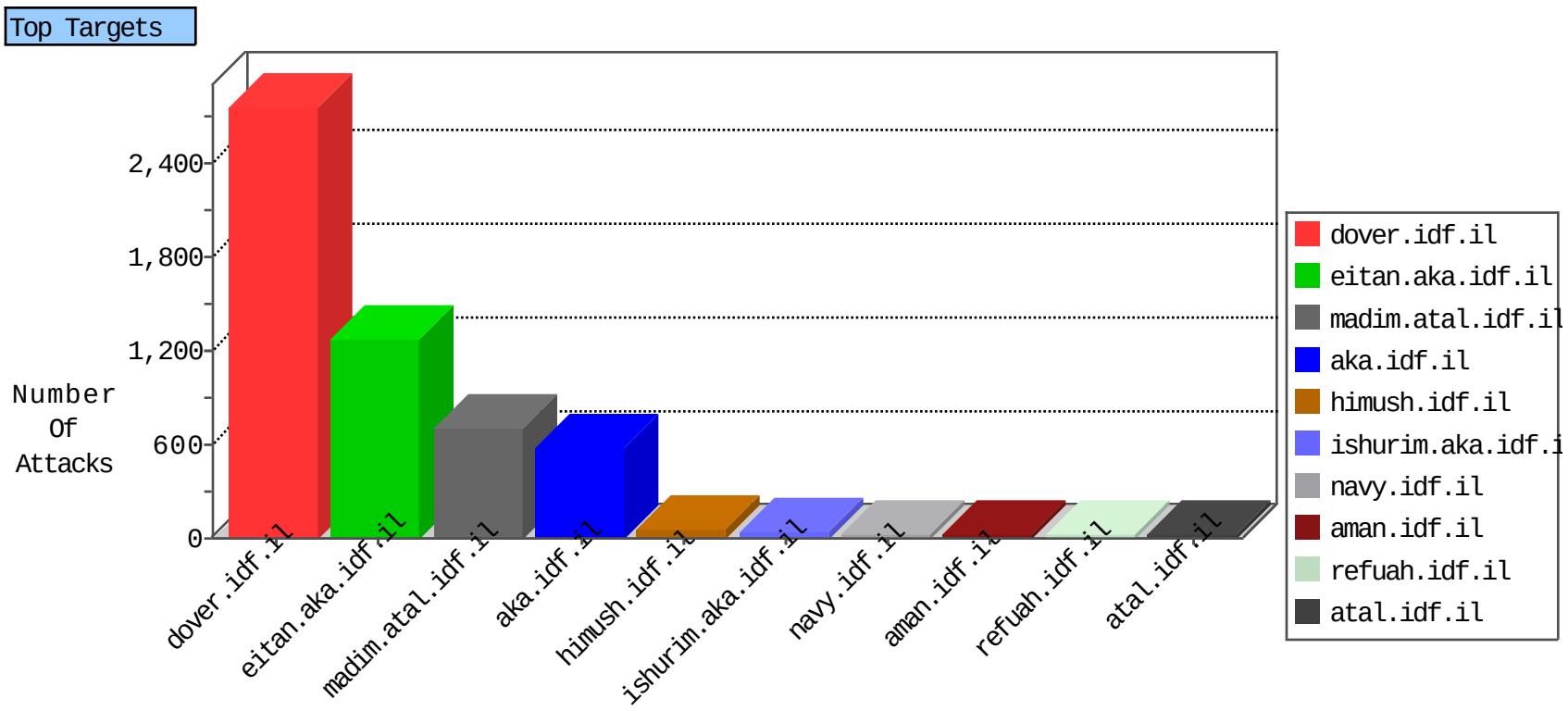
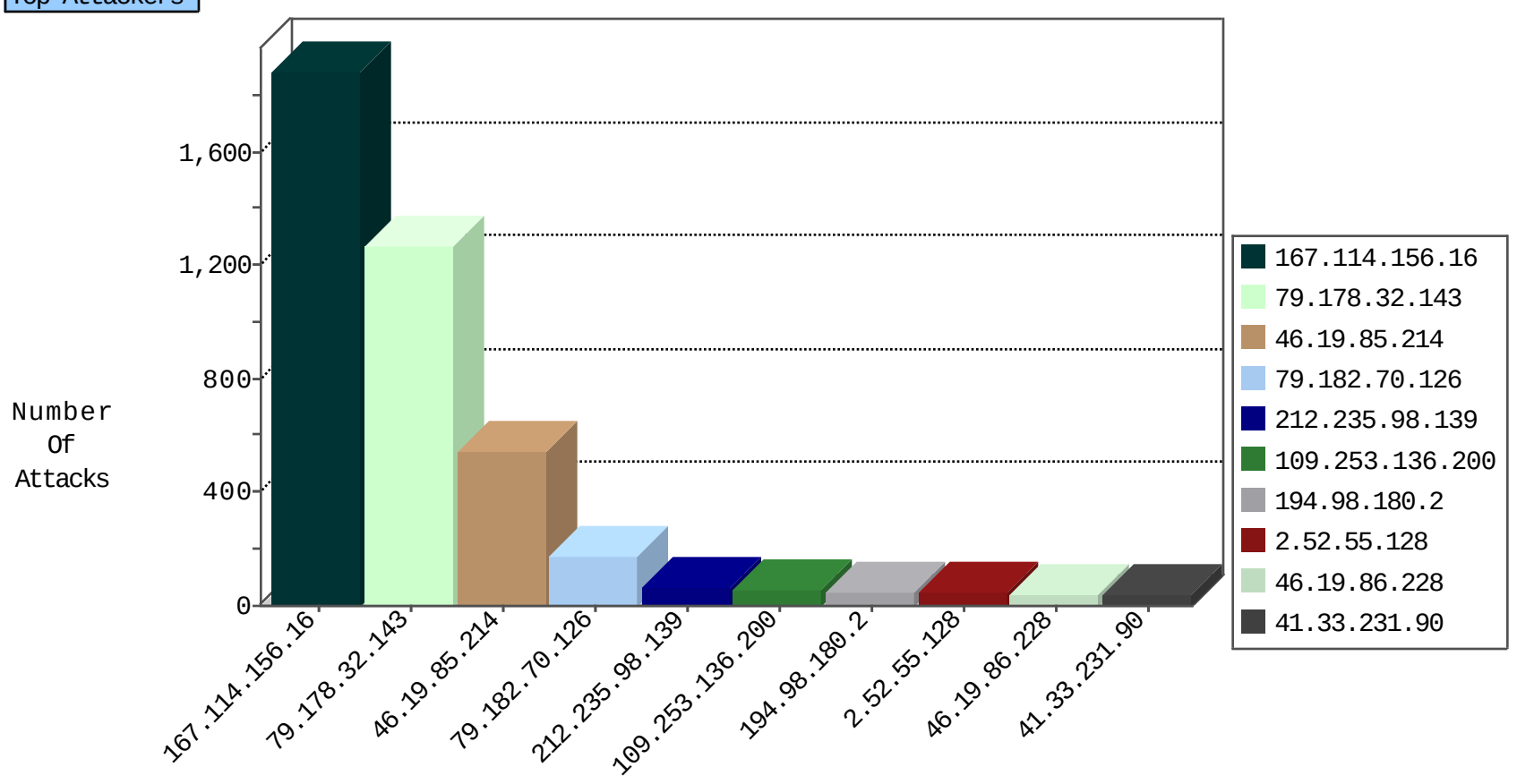
12-15-2015-18:04:01 to 12-15-2015-19:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



12-15-2015-18:04:01 to 12-15-2015-19:04:01

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	DOS-Tool-SwitchbladG	dest-reset	3143
46.19.85.199	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
79.178.177.137	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
82.80.139.80	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
2.54.189.154	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
115.231.222.40	China	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Http	drop	2
212.179.148.59	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
84.229.148.115	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
2.54.23.13	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
2.54.143.200	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

12-15-2015-18:04:01 to 12-15-2015-19:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-15-2015-18:04:01 to 12-15-2015-19:04:01

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
42.118.12.100	147.237.0.15	Vietnam	kosher-kravi.idf.i	ET SCAN NMAP -f -sS	1
109.67.50.180	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
94.102.48.195	147.237.77.227	Netherlands	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.147.166	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.111.155.155	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
208.52.161.177	147.237.77.216	United States	dover.idf.il	SERVER-WEBAPP Setup.php access	1
5.39.222.253	147.237.76.197	Netherlands	e.himush.idf.il	ET SCAN Potential SSH Scan	1
84.109.112.213	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.161.111	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
199.191.56.188	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -f -sS	1
79.180.13.73	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.64.93	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
191.33.36.15	147.237.76.30	Brazil	himush.idf.il	ET SCAN NMAP -f -sS	1
61.244.49.137	147.237.72.14	Hong Kong	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
113.59.33.61	147.237.76.44	China	e.refuah.idf.il	ET SCAN NMAP -sS window 2048	1
42.118.12.100	147.237.0.15	Vietnam	kosher-kravi.idf.i	ET SCAN NMAP -sS window 2048	1
109.253.198.65	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	portscan: TCP Distributed Portscan	1
94.102.48.195	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.149.188	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.173.159.73	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.151.32.163	147.237.77.216	Israel	dover.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
5.39.222.253	147.237.76.198	Netherlands	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
84.111.48.244	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
199.191.56.188	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 2048	1
5.39.222.253	147.237.76.30	Netherlands	himush.idf.il	ET SCAN NMAP -sS window 1024	1
84.94.90.239	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.62.18.105	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
70.39.184.204	147.237.77.216	Satellite Provide	dover.idf.il	portscan: TCP Distributed Portscan	1
191.33.36.15	147.237.76.30	Brazil	himush.idf.il	ET SCAN NMAP -sS window 2048	1
64.38.133.137	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 1024	1
149.78.47.127	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.117.182.179	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
113.59.33.61	147.237.76.44	China	e.refuah.idf.il	ET SCAN NMAP -f -sS	1

12-15-2015-18:04:01 to 12-15-2015-19:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.178.32.143	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1038
79.182.70.126	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	115
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	62
46.19.86.228	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	38
37.26.146.167	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	28
46.19.85.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
46.19.85.28	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	24
37.26.146.172	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
194.98.180.2	France	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	18
37.26.149.201	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
84.228.143.132	Israel	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
194.98.180.2	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
46.19.85.29	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
66.249.66.90	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
190.104.21.217	Bolivia	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
46.19.85.29	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
85.65.30.156	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
194.98.180.2	France	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.86.28	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
80.179.114.3	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
62.219.160.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.100	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.158	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
190.104.21.217	Bolivia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
31.168.149.92	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.120.20.45	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
85.65.112.204	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.59	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
80.246.0.137	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
176.0.103.49	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.19	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.143	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.97.230	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.59	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.143	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.67	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.227	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.163	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
84.108.132.90	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.109	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.55	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
85.65.195.102	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.199.251.227	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.67	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.227	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.163	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	296
79.178.32.143	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	228
46.19.85.214	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 46.19.85.214	Block	140
46.19.85.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
109.253.136.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	57
2.52.55.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	47
46.19.86.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
109.65.173.50	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	14
176.13.17.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
208.115.113.93	United States	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	8
79.182.70.126	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 79.182.70.126	Block	4
66.249.64.177	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	4
79.182.70.126	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 79.182.70.126	Block	4
84.111.108.217	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	4
2.52.19.21	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
79.182.70.126	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	4
79.182.70.126	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 79.182.70.126	Block	4
79.182.70.126	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 79.182.70.126	Block	4
79.182.70.126	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 79.182.70.126	Block	4
79.182.70.126	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 79.182.70.126	Block	4
79.182.70.126	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 79.182.70.126	Block	4
40.77.167.44	United States	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	4
79.182.70.126	Israel	147.237.72.166	aka.idf.il	Multiple Illegal HTTP Version from 79.182.70.126	Block	3
79.182.70.126	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 79.182.70.126	Block	3
157.55.39.88	United States	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	3
37.26.146.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
107.167.113.98	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	3
46.19.85.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.182.70.126	Israel	147.237.72.166	aka.idf.il	Multiple Malformed HTTP Header Line from 79.182.70.126	Block	3
79.182.70.126	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 79.182.70.126	Block	3
109.186.173.101	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.186.173.101	Block	3
66.249.64.228	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	3
212.227.29.47	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.227.29.47	Block	3
207.241.237.240	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
79.178.170.80	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	2
79.182.70.126	Israel	147.237.72.166	aka.idf.il	Multiple Illegal URL Path Encoding from 79.182.70.126	Block	2
176.13.1.119	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	2
66.249.64.218	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	2
141.0.9.34	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	2
5.29.194.240	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
176.12.143.146	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	2
84.228.54.204	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	2
109.64.101.219	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
37.26.148.139	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
192.95.29.116	Canada	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/robots.txt	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	1
87.69.109.119	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.29.110.137	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	1
176.13.22.4	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.182.70.126	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method Â¦u6^IÃªq[[#3]]Â-qab[[#15]]VJ@Ã•CÂ pgÃ¦[[#22]]T[[#21]]2Â,b[[#21]]!Â?Â?Ã‘ÂŽ:Ã‡Ã–	Block	1
149.88.86.27	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

12-15-2015-18:04:01 to 12-15-2015-19:04:01