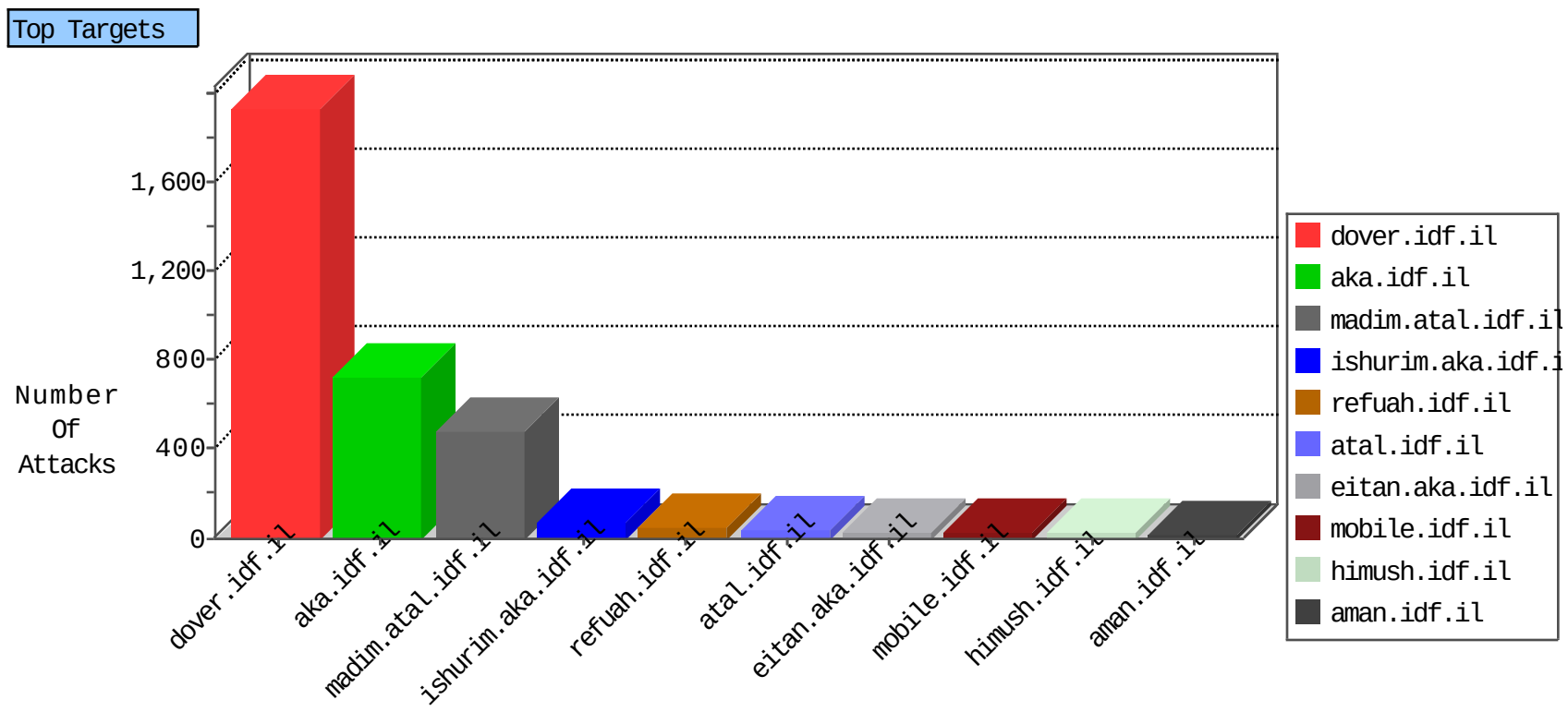
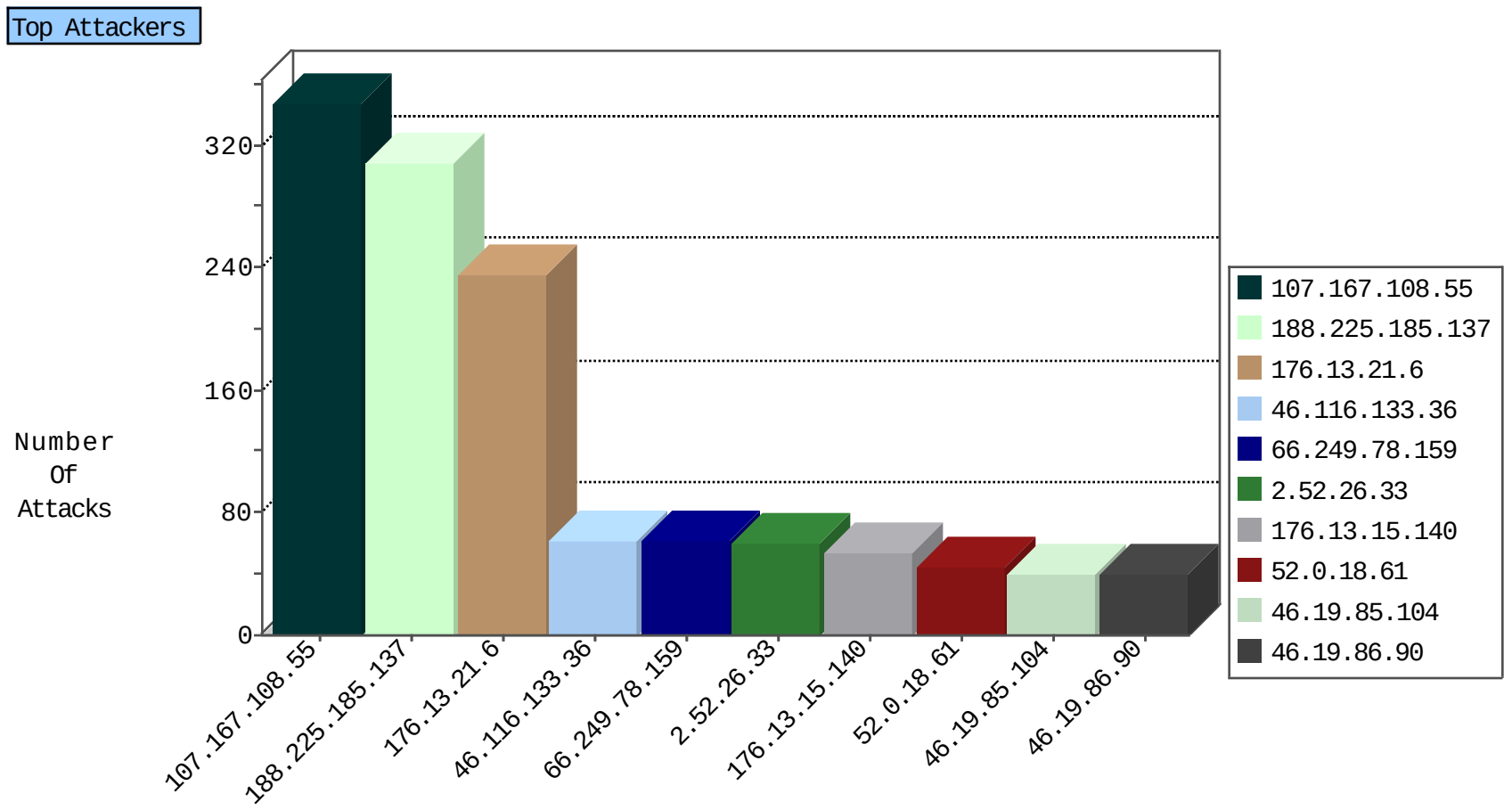
11-22-2015-13:04:06 to 11-22-2015-14:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-22-2015-13:04:06 to 11-22-2015-14:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
204.93.154.201	United States	147.237.77.216	dover.idf.il	JLM_Dover_Con_Limit_Https	drop	20
193.43.246.250	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
185.3.144.63	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
123.151.42.61	China	147.237.76.38	e.e.meitav.idf.il	JLM_Purple_Con_Limit_Udp	drop	3
80.70.128.129	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
81.218.206.82	Israel	147.237.77.170	maarachot.idf.il	Block_Udp_All_Nets	drop	3
195.160.240.11	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
123.151.42.61	China	147.237.76.38	e.e.meitav.idf.il	JLM_Under_Attack_Con_Udp	drop	2
138.134.102.16	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
46.120.52.127	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
142.4.193.203	United States	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
51.254.212.184	United Kingdom	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
46.19.85.122	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1
46.19.85.127	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
5.22.129.195	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
94.230.93.194	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
37.26.147.163	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

11-22-2015-13:04:06 to 11-22-2015-14:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.116.133.36	Israel	147.237.72.166	aka.idf.il	C1000098: Block - dns poisoning	Block	2
81.218.57.242	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
87.68.165.134	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1

11-22-2015-13:04:06 to 11-22-2015-14:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
109.67.17.250	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.163.140.142	147.237.77.19	Germany	law-forum.idf.il	ET SCAN Potential SSH Scan	1
80.246.139.45	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.178.147.178	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.125	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.179.50	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
113.108.21.16	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
91.199.69.254	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.163.140.142	147.237.76.200	Germany	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
80.179.206.197	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.219.110.166	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.6.71.154	147.237.72.156	Poland	aman.idf.il	ET SCAN NMAP -sS window 1024	1
2.52.142.242	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.25.93.246	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
182.72.109.162	147.237.8.28	India	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1

11-22-2015-13:04:06 to 11-22-2015-14:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
188.225.185.137	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	306
107.167.108.55	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	298
107.167.108.55	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	50
52.0.18.61	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
46.19.85.104	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	39
46.19.86.90	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	39
79.183.122.205	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
95.108.158.171	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
95.108.158.152	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
5.255.253.168	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
213.57.143.226	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	28
31.168.17.161	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
5.255.253.150	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
37.26.146.241	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
148.177.129.212	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
66.249.81.212	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
178.62.80.161	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
46.19.86.156	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	23
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
5.255.253.158	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
79.183.38.209	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
207.241.226.220	United States	147.237.72.166	aka.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	20
37.140.141.2	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	17
5.255.253.170	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
109.64.120.34	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
66.249.81.212	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
109.64.192.93	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
109.65.140.149	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
192.116.98.164	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
195.212.29.183	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
46.19.86.122	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
176.12.143.75	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
100.100.114.234		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
100.100.29.79		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
84.229.145.76	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
162.243.69.172	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.81.218	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
100.100.39.120		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
141.8.142.11	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
199.203.226.21	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
192.115.29.222	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.166.190.161	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
213.57.132.245	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10

11-22-2015-13:04:06 to 11-22-2015-14:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.21.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	139
176.13.21.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	96
176.13.15.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	53
2.52.26.33	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	51
176.13.1.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
2.54.6.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
46.19.86.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 212.179.21.194	Block	11
2.54.177.106	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
176.13.4.110	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	8
46.116.133.36	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 46.116.133.36	Block	6
212.25.102.63	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 212.25.102.63	Block	6
46.116.133.36	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 46.116.133.36	Block	6
46.116.133.36	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 46.116.133.36	Block	5
46.116.133.36	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	5
80.246.136.35	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
46.116.133.36	Israel	147.237.72.166	aka.idf.il	Multiple Illegal HTTP Version from 46.116.133.36	Block	4
46.116.133.36	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 46.116.133.36	Block	4
46.116.133.36	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 46.116.133.36	Block	4
46.116.133.36	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 46.116.133.36	Block	3
81.218.174.150	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	3
2.54.48.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.47	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.116.133.36	Israel	147.237.72.166	aka.idf.il	Multiple Malformed HTTP Header Line from 46.116.133.36	Block	3
185.32.179.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.48.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.138.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.125.79.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.161.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.116.133.36	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 46.116.133.36	Block	3
46.116.133.36	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 46.116.133.36	Block	3
2.52.186.46	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.111.248.7	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
80.246.137.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.178.181.22	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
84.229.148.103	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/general.aspx	Block	2
80.246.137.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
79.179.140.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.12.139.44	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	2
89.138.229.117	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	2
212.25.102.63	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/0/size338x0/1620.jpg	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	2
176.12.146.191	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
185.32.179.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.133.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.121.64.254	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.66.112.119	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.86.154	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

11-22-2015-13:04:06 to 11-22-2015-14:04:06