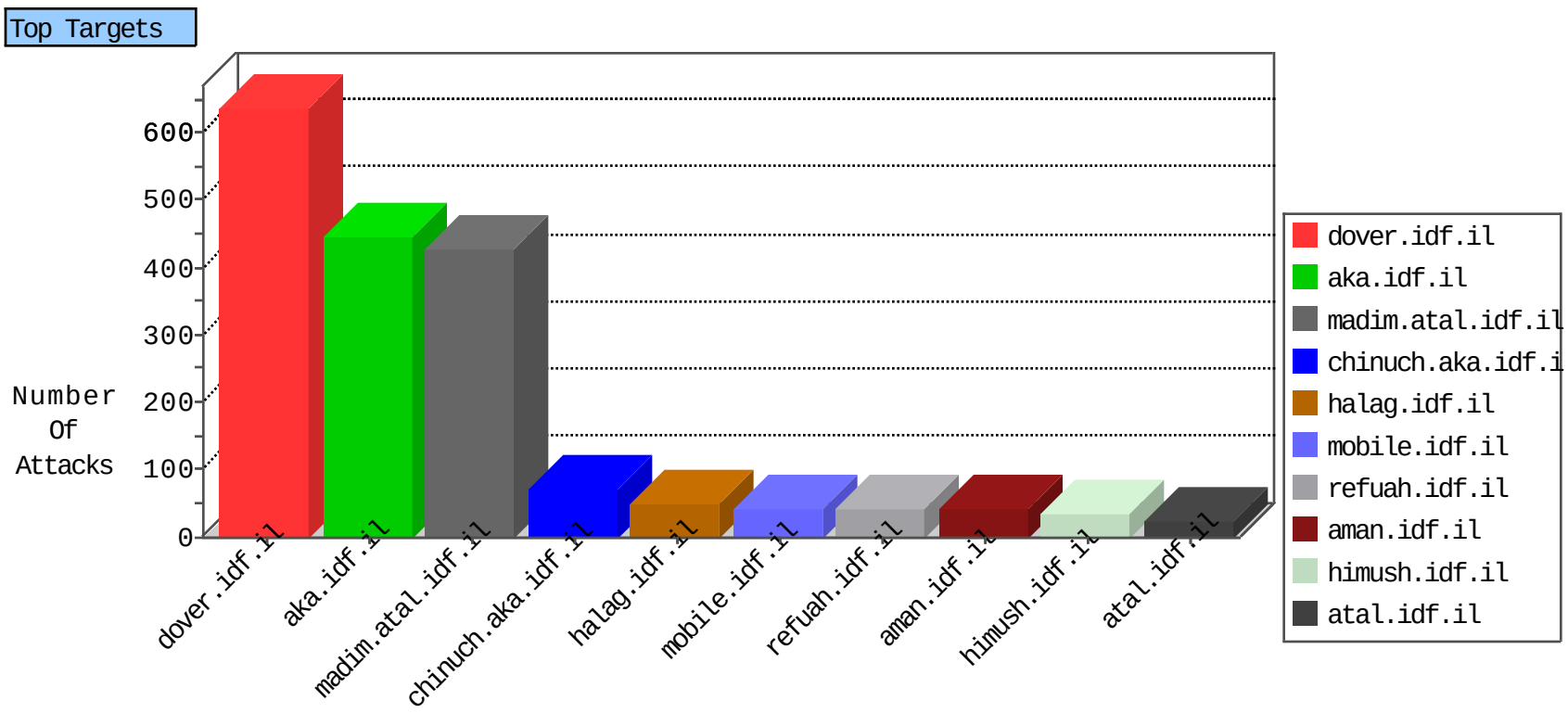
12-29-2015-17:04:00 to 12-29-2015-18:04:00

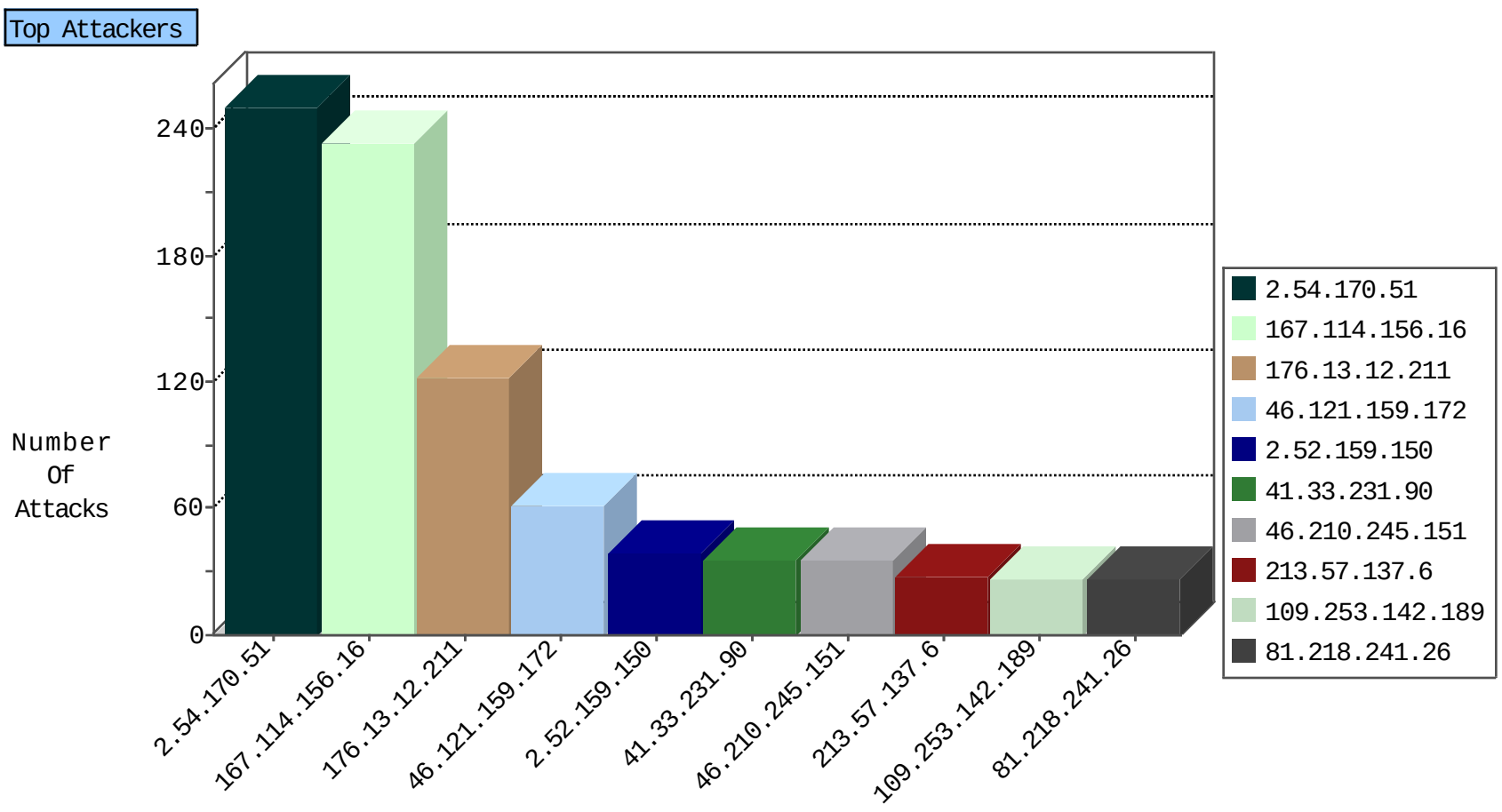
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

12-29-2015-17:04:00 to 12-29-2015-18:04:00

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	4561
81.218.241.26	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	95
167.114.156.16	Canada	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	8
66.249.78.159	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
84.85.202.109	Netherlands	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
37.26.148.200	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
82.81.12.22	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	forward	2
203.166.137.11	Singapore	147.237.77.74	law.idf.il	Invalid TCP Flags	drop	1
203.166.137.12	Singapore	147.237.77.74	law.idf.il	Invalid TCP Flags	drop	1
84.85.202.109	Netherlands	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
85.65.61.140	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
184.105.139.78	United States	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1

12-29-2015-17:04:00 to 12-29-2015-18:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.59.40.198	France	147.237.77.216	dover.idf.il	12651: HTTP: Open Flash Chart PHP File Upload Vulnerability	Block	6
62.90.95.139	Israel	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1

12-29-2015-17:04:00 to 12-29-2015-18:04:00

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
66.249.66.50	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
50.204.188.142	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 3072	1
192.116.83.2	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.242	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
151.217.178.88	147.237.77.178		e.matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
2.52.48.219	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
139.91.210.41	147.237.77.235	Greece	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
109.64.201.168	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
108.61.164.250	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 1024	1
89.139.190.142	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.81.83.90	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.132.27.9	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
50.204.188.142	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
185.32.179.228	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.168.207.232	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
151.217.30.48	147.237.76.44		e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
109.253.202.248	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.48.223	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
95.86.99.252	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.108.237.36	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.127.56.81	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.235.55.32	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

12-29-2015-17:04:00 to 12-29-2015-18:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
213.57.137.6	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	28
2.54.45.241	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	20
109.253.142.189	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
46.19.85.146	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
109.253.142.189	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
79.182.184.120	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
79.176.155.101	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
2.52.128.83	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
2.52.159.150	Israel	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
66.249.78.37	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
81.218.241.26	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	10
31.210.188.105	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
91.226.112.200	Slovakia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
2.52.128.83	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
141.0.14.12	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.121.159.172	Israel	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
79.176.155.101	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
79.178.215.230	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
207.46.13.178	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.106	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.21	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
85.250.195.90	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.52.159.150	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.178.175.50	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.21	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.150.184	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.145.207	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
85.250.195.90	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.177.101.165	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
185.32.179.166	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
2.52.159.150	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.6.31	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.45.19	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.81	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.138	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.13.6.31	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.159.150	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.85.20	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.5	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.106	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
62.219.149.68	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.212.55	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.138	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.20	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.176.109.203	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
80.246.139.32	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.159.150	Israel	147.237.77.234	halag.idf.il	SYN Attack		reject	5
46.19.85.170	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5

12-29-2015-17:04:00 to 12-29-2015-18:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.170.51	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	120
176.13.12.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	86
2.54.170.51	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	81
46.121.159.172	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	49
2.54.170.51	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 2.54.170.51	Block	49
176.13.12.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	36
46.210.245.151	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
185.32.179.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.179.105	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
91.200.12.73	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/6/3916.pdf/trackback/	Block	3
109.253.132.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.94.38.200	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	3
79.181.188.82	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	3
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
81.218.205.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.64.97.57	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	2
176.12.160.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
194.90.25.122	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
80.246.130.219	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
82.80.152.34	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	2
94.230.86.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.125.104.193	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
212.76.108.198	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/&sa=u&ved=0ahukewjk682atohkahvetbqkhftndzwqfggimaa&usg=afqjcnhcvyyg7w1cq-yhd5_ammzoyodtwa	Block	2
185.32.179.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.179.124.17	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	2
195.95.183.254	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/319,	Block	2
212.117.154.242	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	2
77.127.201.70	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.127.201.70	Block	2
109.64.35.245	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/mas.aspx	Block	2
46.19.85.241	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
79.176.112.153	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
149.50.77.124	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.170	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
89.138.201.42	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
217.132.118.213	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/mas.aspx	Block	1
31.154.145.214	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.65.236.59	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
70.112.198.97	United States	147.237.76.30	himush.idf.il	Illegal Byte Code Character in Method Â¯[[#0]][[#0]][[#0]]CÂ£[[#11]]Â”ÃœÃ€a[RÃ–P[[#27]][[#30]]Â¡Ã¦Â¿[[#3]]Â?/Ã·ÃŸÃ?d[[#7]]Ã´&Ã‘[[#19]]Â?Â‘Zy[[#16]][[#27]]:Â 2[[#8]]•Ã?Â?Â‰Ã˜Ã¡ÃšÂ?mÂƒÂ–AÂ”Ã˜Ã”Ã˜ÃŸÃ¦Ã‹lÃ”Â£Ã‰Ã”ÃªÃª+[[#20]]RÃ˜W_ÂœÃ‚Ã„[[#7]]Ã¥(Ã‰=1Â€Â„	Block	1
109.253.139.34	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.142.197	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.16	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
93.173.48.151	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/miluim/miluimnikpail/general.aspx	Block	1
79.178.191.121	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
128.232.110.29	United Kingdom	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to 147.237.76.200/	Block	1
37.142.184.152	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
88.81.181.174	Italy	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.179.231.229	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
77.92.72.214	United Kingdom	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

12-29-2015-17:04:00 to 12-29-2015-18:04:00