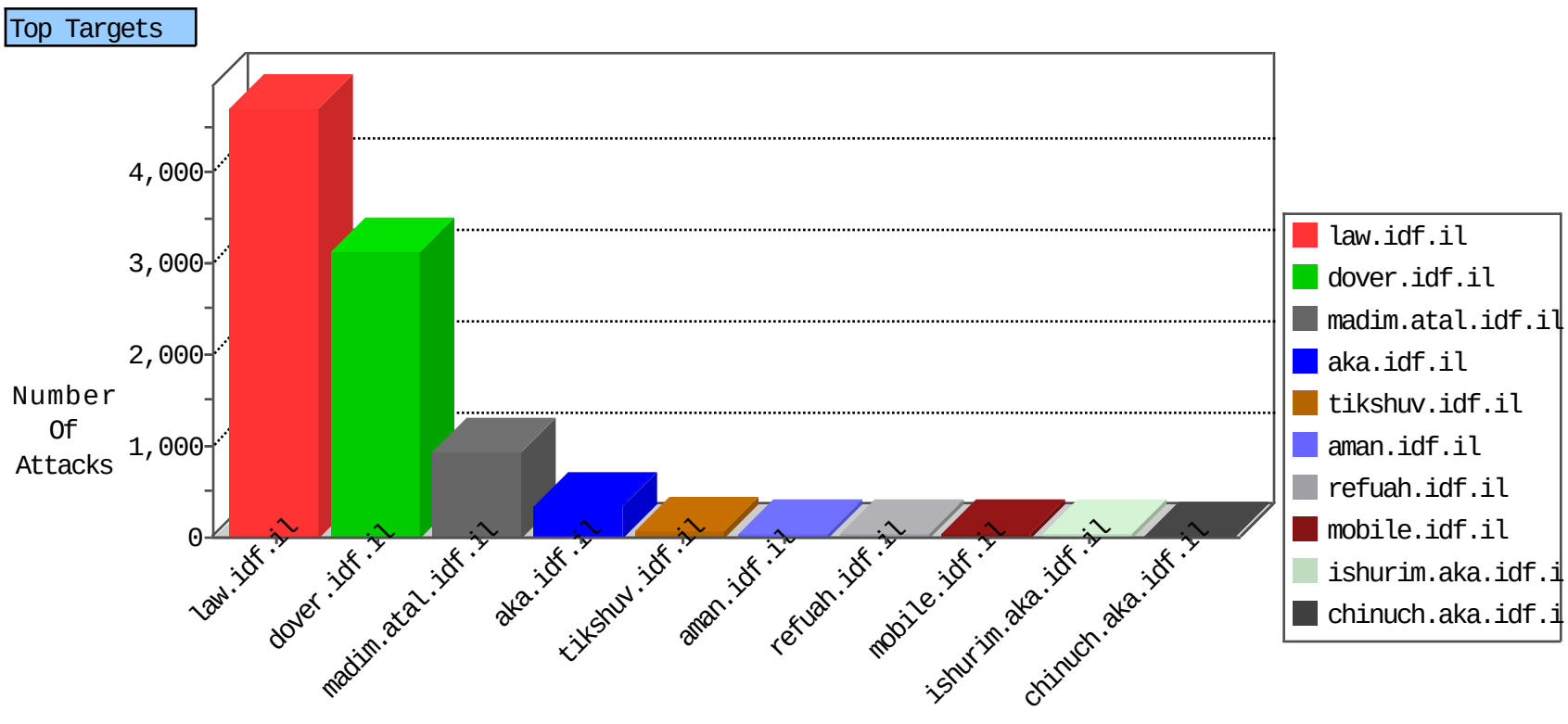
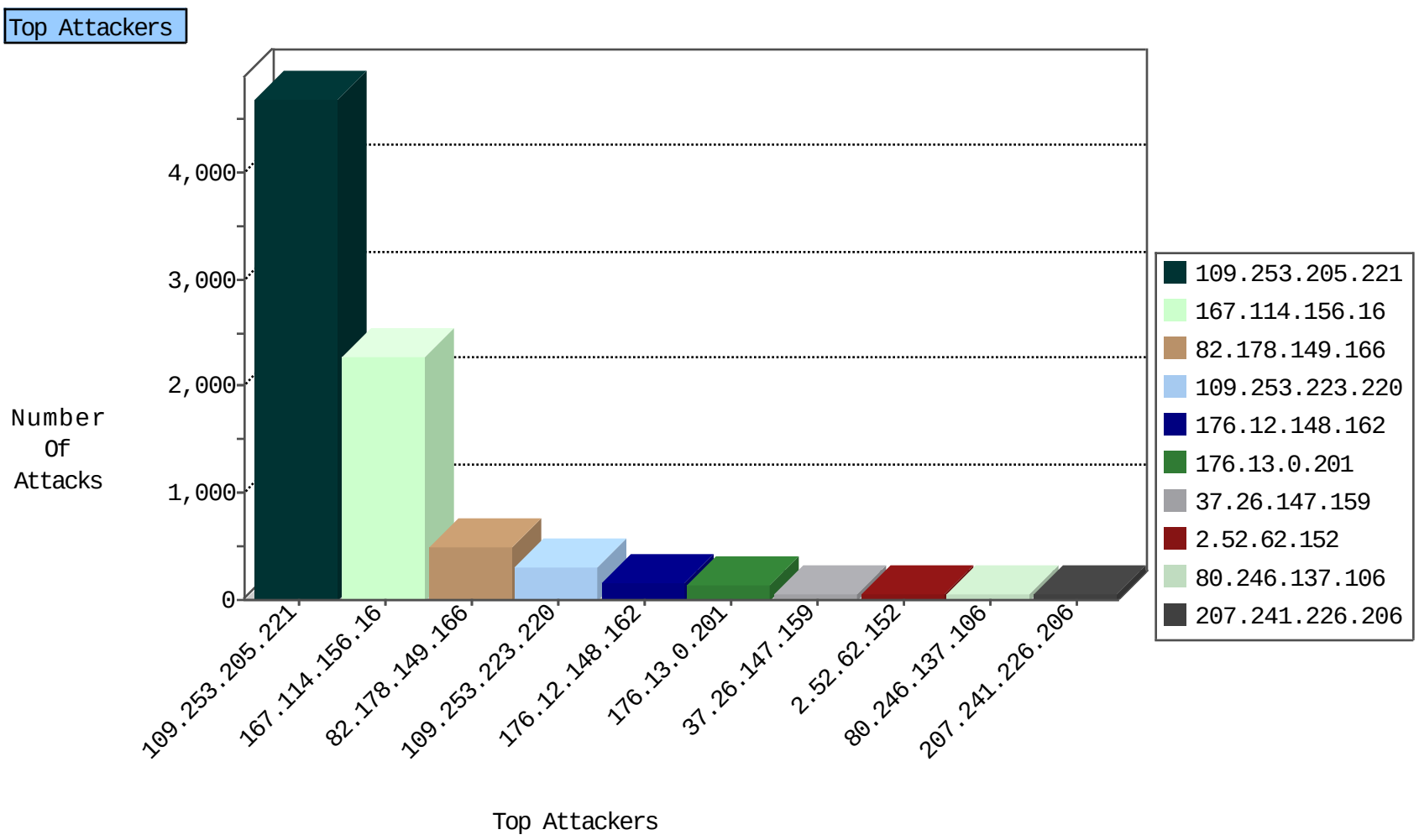
12-28-2015-08:04:05 to 12-28-2015-09:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



12-28-2015-08:04:05 to 12-28-2015-09:04:05

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	3111
82.178.149.166	Oman	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	222
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	154
207.232.36.181	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	142
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	93
188.161.38.67	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	16
64.233.172.155	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
64.233.172.171	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
109.200.30.168	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
66.249.78.173	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
66.249.93.107	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
66.249.93.99	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
64.233.172.163	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
188.161.38.67	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
66.249.78.159	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
65.0.150.118	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
66.249.78.166	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
188.161.38.67	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	5
66.249.78.166	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
107.170.91.224	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
123.126.113.154	China	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
82.178.149.166	Oman	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	3
81.218.105.235	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
66.220.146.23	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
66.220.146.23	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
46.60.33.198	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
178.255.215.87	France	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
65.55.211.248	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
65.55.212.69	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
45.35.64.142		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
111.73.241.9	China	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
178.255.215.87	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
107.150.98.131	United States	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
66.220.146.23	United States	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
123.126.113.154	China	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

12-28-2015-08:04:05 to 12-28-2015-09:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-28-2015-08:04:05 to 12-28-2015-09:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
82.178.149.166	147.237.77.216	Oman	dover.idf.il	SERVER-APACHE Apache SSI error page cross-site scripting	406
109.64.171.89	147.237.72.166	Israel	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
151.217.178.63	147.237.8.24		e.lifestyle.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.63	147.237.0.16		my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
80.178.101.251	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
217.115.199.40	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
37.26.147.156	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.186.95.178	147.237.76.30	Canada	himush.idf.il	ET SCAN NMAP -sS window 4096	1
192.114.91.246	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
151.217.178.63	147.237.72.167		ishurim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.63	147.237.0.200		m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
119.165.52.18	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
217.115.199.40	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
41.41.196.117	147.237.76.86	Egypt	navy.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
192.186.95.178	147.237.76.30	Canada	himush.idf.il	ET SCAN NMAP -sS window 3072	1
169.55.120.153	147.237.76.30	Netherlands	himush.idf.il	ET SCAN NMAP -sS window 1024	1
151.217.178.63	147.237.77.234		halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

12-28-2015-08:04:05 to 12-28-2015-09:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.253.205.221	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2402
109.253.205.221	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	2278
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	133
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
207.241.226.206	United States	147.237.77.216	dover.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	34
153.183.212.49	Japan	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
79.180.50.250	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
2.54.139.155	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
63.143.239.12	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
5.102.227.249	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.178.50.185	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
81.218.241.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
46.210.187.244	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.85.106	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.85.106	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.52.183.152	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.14	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.54.60.43	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.142.132.236	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
132.66.85.189	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
128.127.107.123	Netherlands	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.10	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.191.227	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.10	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.182.154	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.32	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.52.183.152	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.52.183.152	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.52.183.152	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
2.54.139.155	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
176.13.0.201	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.163	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.139.155	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
2.52.183.152	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
176.13.12.55	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
188.161.38.67	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
157.55.39.211	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.54.139.155	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
207.46.13.134	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
2.54.139.155	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
212.235.50.41	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
77.127.149.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.41.150	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

12-28-2015-08:04:05 to 12-28-2015-09:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.223.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	173
109.253.223.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	133
176.12.148.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	85
82.178.149.166	Oman	147.237.77.216	dover.idf.il	Multiple Illegal Host Name from 82.178.149.166	Block	82
176.12.148.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	79
176.13.0.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	72
176.13.0.201	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.0.201	Block	68
37.26.147.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	58
2.52.62.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	56
80.246.137.106	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	55
2.54.18.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
37.26.147.180	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.147.180	Block	35
176.13.15.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	34
209.88.173.130	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/$$$&?&?$$$	Block	32
176.13.12.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
185.32.179.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
109.226.17.47	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
2.54.41.69	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
79.180.144.66	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 79.180.144.66	Block	6
192.241.201.65	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.241.201.65	Block	5
207.241.226.206	United States	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 207.241.226.206	Block	5
2.54.189.9	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
185.32.179.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
216.72.40.185	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
176.13.21.140	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
46.121.248.46	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/	Block	3
109.253.150.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.180.144.66	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	2
80.246.139.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.102.227.249	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
2.52.173.239	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
91.200.12.95	Ukraine	147.237.77.216	dover.idf.il	PHP Attempt	Block	2
2.52.179.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.12.55	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchildsubcategories/1423	Block	2
81.218.251.250	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.19.86.194	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/userdetails	Block	2
2.54.53.46	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
62.219.226.71	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	2
176.13.14.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.75.79.119	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/page/26/	Block	1
184.105.139.70	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
2.52.150.56	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
94.230.93.223	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.76.114.242	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.102.9.81	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
46.19.86.29	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.241.226.206	United States	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 207.241.226.206	Block	1
66.249.78.153	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
180.76.15.134	China	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.54.18.136	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

12-28-2015-08:04:05 to 12-28-2015-09:04:05