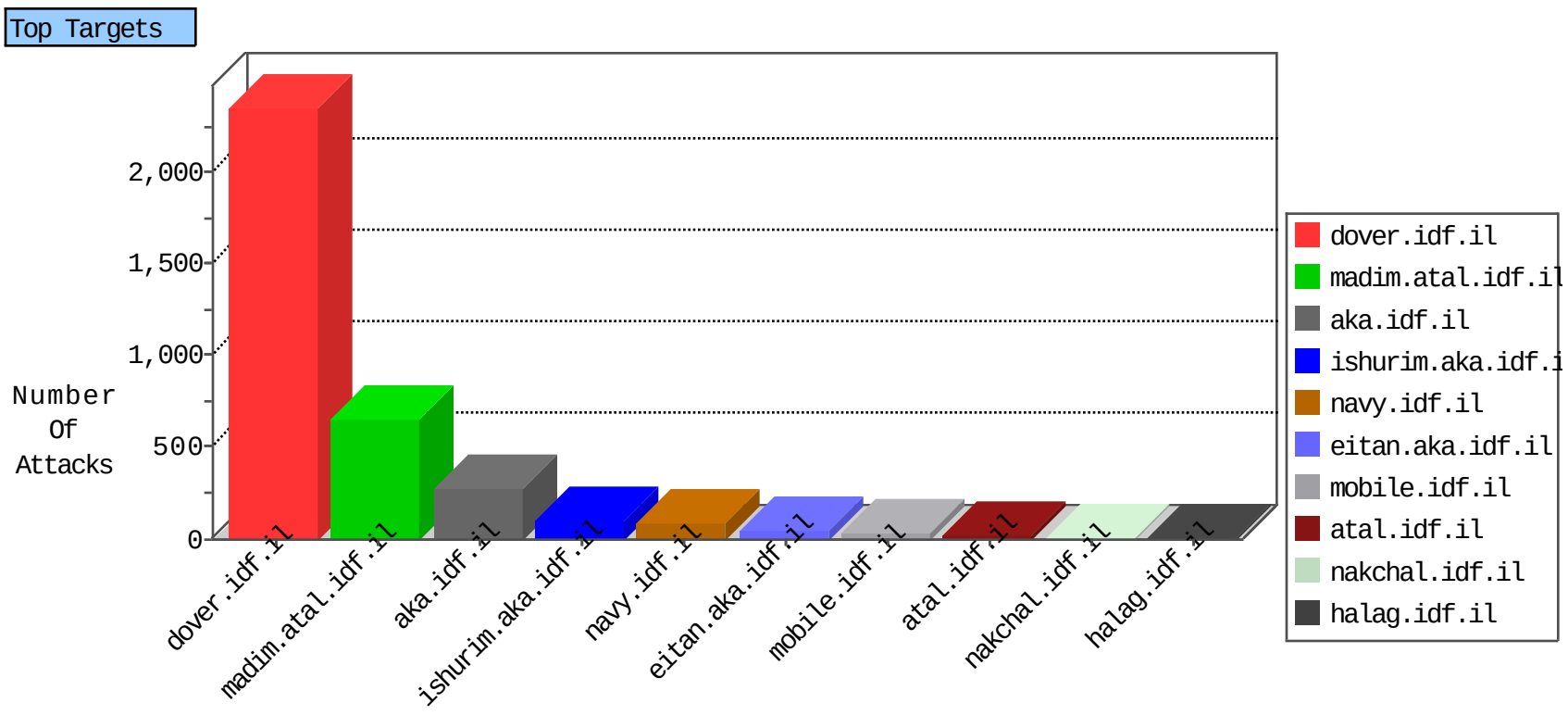
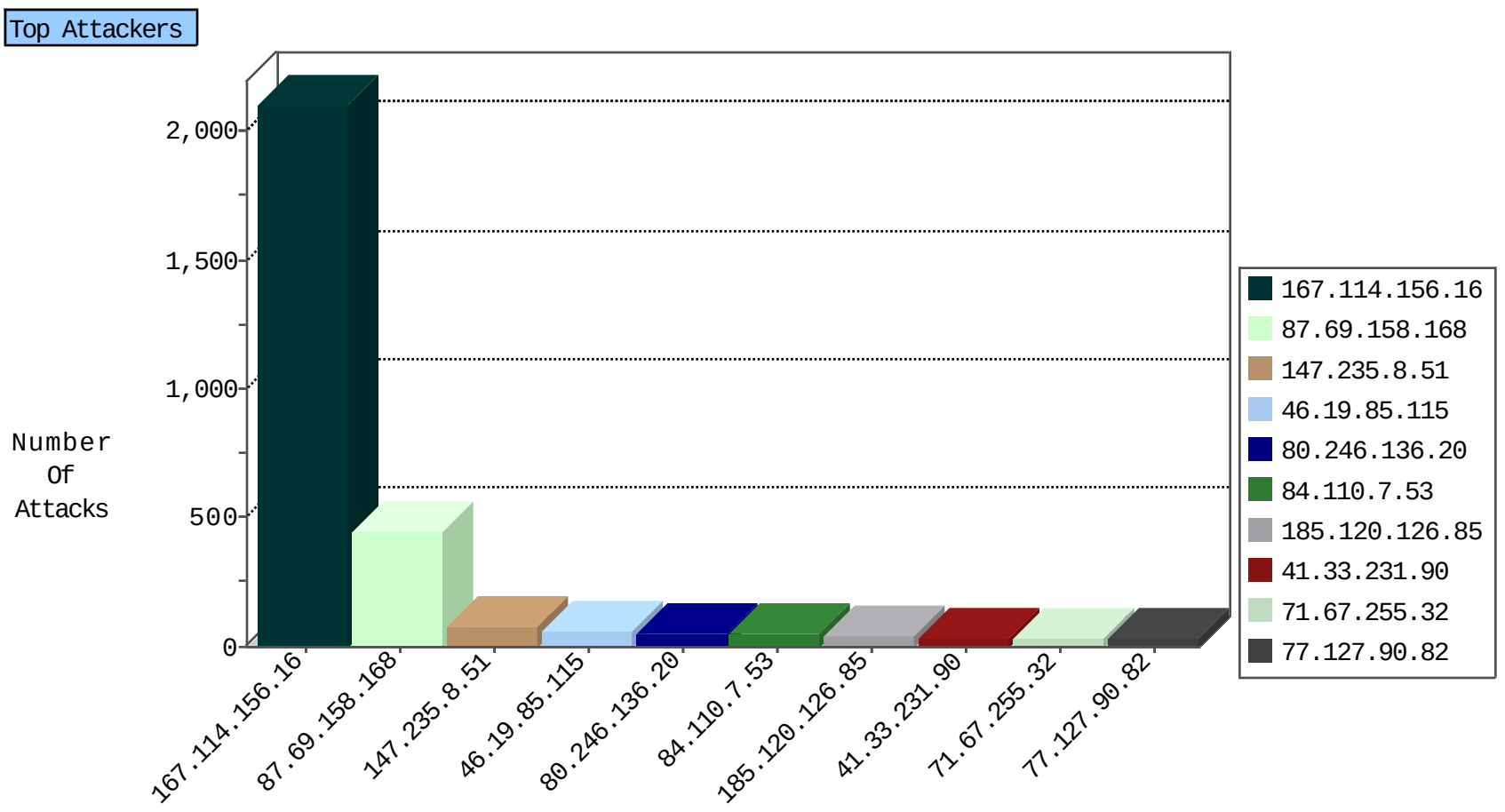
12-17-2015-19:04:02 to 12-17-2015-20:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



12-17-2015-19:04:02 to 12-17-2015-20:04:02

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	3735
101.254.199.20	China	147.237.8.27	e.madim.atal.idf.il	Frk_Under_Attack_Con_Http	drop	2
49.167.66.152	Korea, Republic of	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
188.165.42.90	France	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
101.254.199.20	China	147.237.8.27	e.madim.atal.idf.il	Frk_Purple_Con_Limit_Http	drop	1

12-17-2015-19:04:02 to 12-17-2015-20:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
52.1.90.117	United States	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
70.114.160.158	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
151.80.31.152	Italy	147.237.76.42	refuah.idf.il	C228: HTTP: AhrefBot crawler	Block	1

12-17-2015-19:04:02 to 12-17-2015-20:04:02

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
70.114.160.158	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	3
84.229.148.77	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
49.69.175.253	147.237.0.34	China	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
189.219.226.136	147.237.0.17	Mexico	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
31.14.252.194	147.237.77.176	Romania	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
114.215.145.32	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
109.186.25.185	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.159.159.122	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.65.133.218	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
83.56.3.111	147.237.77.179	Spain	e.mazi.idf.il	ET SCAN NMAP -sS window 3072	1
83.56.3.111	147.237.0.33	Spain	idf.il	ET SCAN NMAP -sS window 3072	1
66.249.69.84	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
37.142.185.175	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
114.215.145.32	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
114.215.145.32	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1
109.66.24.156	147.237.77.170	Israel	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
89.138.160.246	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
83.56.3.111	147.237.77.179	Spain	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1

12-17-2015-19:04:02 to 12-17-2015-20:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.85.115	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	63
84.110.7.53	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
77.127.90.82	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
185.120.126.85		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	28
71.67.255.32	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	28
207.241.229.104	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	18
149.20.63.13	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
109.67.187.111	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
185.120.126.85		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
79.181.110.153	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
80.246.133.226	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
190.24.146.71	Colombia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
147.235.8.51	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
109.64.154.74	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.143.8	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
79.179.56.80	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
37.26.149.150	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
147.235.8.51	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
79.180.13.215	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.53.0	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
176.13.8.5	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.163.191	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.12	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
194.177.8.252	France	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
147.235.8.51	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
109.186.171.119	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.86.12	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
84.229.148.77	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
80.246.133.226	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
46.19.85.180	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
31.154.159.79	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
66.102.9.107	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	5
5.102.254.38	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
207.241.226.40	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.183.142.23	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.184.231	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.28.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.96.80	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.211	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.229.148.77	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
79.183.143.33	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.161.43	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.85.166	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.65.91.238	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	3
79.177.106.107	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.136.20	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

12-17-2015-19:04:02 to 12-17-2015-20:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.69.158.168	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	322
87.69.158.168	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 87.69.158.168	Block	127
147.235.8.51	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	61
80.246.136.20	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	39
46.117.84.8	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
46.116.88.67	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	15
79.179.178.134	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 79.179.178.134	Block	6
221.178.182.171	China	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on navy.idf.il/templates/sendtofriend/	Block	4
107.170.39.242	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 107.170.39.242	Block	4
2.54.9.208	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 2.54.9.208	Block	3
221.178.182.204	China	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on navy.idf.il/templates/sendtofriend/	Block	3
176.228.76.193	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
221.178.182.157	China	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/1155-he/navy.aspx#par_3	Block	3
37.235.53.95	Spain	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/994-8613-he/navy.aspx.aspx	Block	3
149.88.179.179	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.12.144.93	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
95.86.125.148	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	2
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.25	Block	2
80.246.136.20	Israel	147.237.0.19	madim.atal.idf.i	Untraceable SSL Sessions: Open Mode	None	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
89.138.220.236	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
119.188.115.27	China	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on navy.idf.il/templates/sendtofriend/	Block	2
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	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
185.120.126.34		147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
93.172.43.57	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
218.205.17.208	China	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/templates/sendtofriend/	Block	2
176.228.151.132	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
80.246.137.185	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
199.223.233.224	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/templates/sendtofriend/	Block	2
37.142.241.137	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
221.178.182.182	China	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
149.78.228.220	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
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
37.142.243.183	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/controls/atuda/Â	Block	2
149.88.100.58	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.183.201.130	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
195.154.146.225	France	147.237.77.74	law.idf.il	Illegal HTTP Version HTTP/	Block	1
46.19.85.126	Israel	147.237.76.42	refuah.idf.il	Distributed Malformed URL	Block	1
109.66.184.108	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
71.67.255.32	United States	147.237.76.86	navy.idf.il	Illegal HTTP Version	Block	1
176.13.19.242	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.146.136	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.250.247.60	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
221.178.182.156	China	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/templates/sendtofriend/	Block	1
150.70.173.9	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
136.243.36.96	Germany	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
46.19.86.184	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.235.53.95	Spain	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on navy.idf.il/templates/sendtofriend/	Block	1

12-17-2015-19:04:02 to 12-17-2015-20:04:02