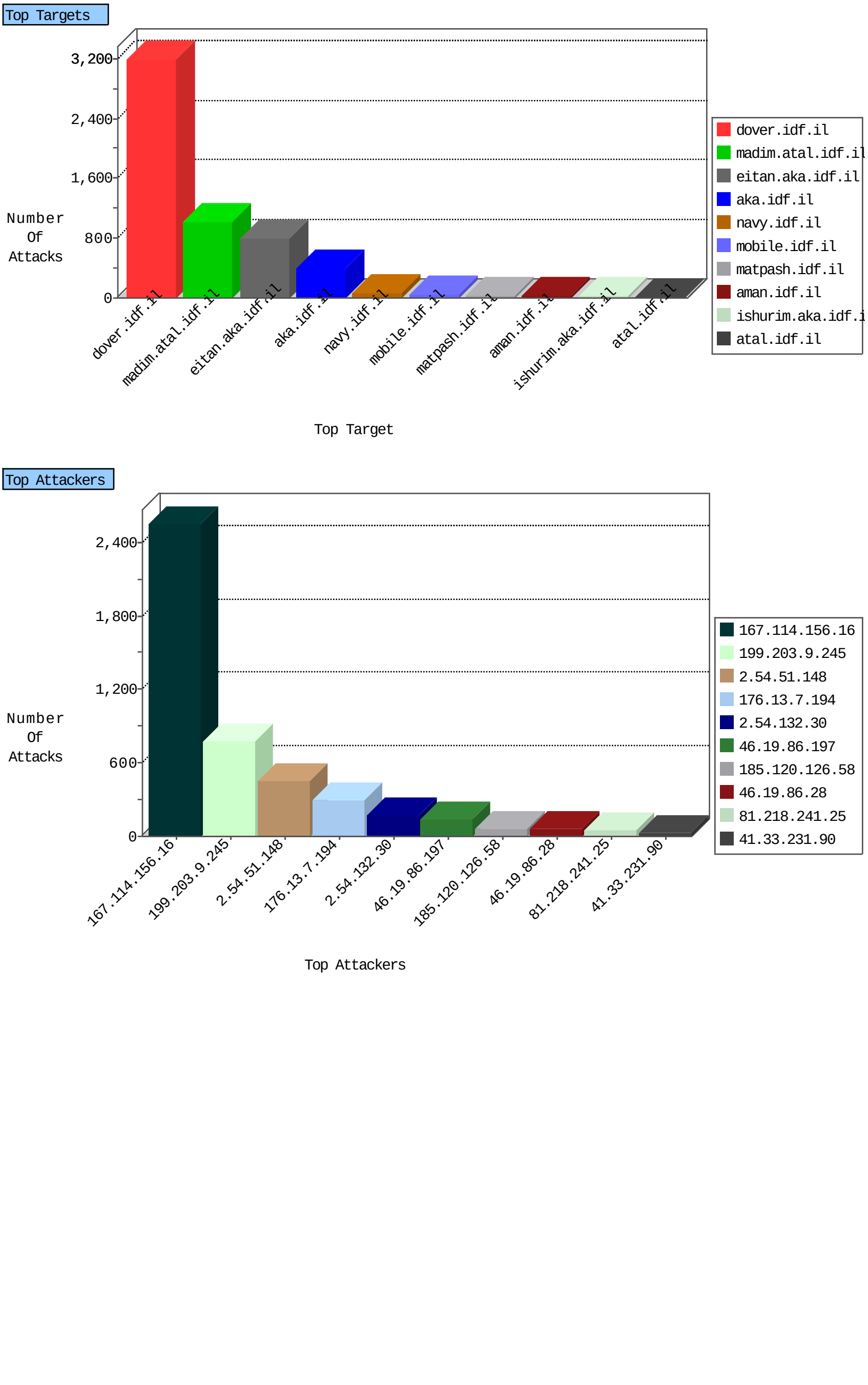
12-13-2015-17:04:09 to 12-13-2015-18:04:09

IDF Under Attack
Daily Report



12-13-2015-17:04:09 to 12-13-2015-18:04:09

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	3429
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	87
82.132.244.222	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
134.147.203.115	Germany	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	2
59.34.142.100	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
146.185.239.100	Russian Federation	147.237.76.86	navy.idf.il	block-sp-traf1	drop	1
172.98.67.108		147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1

12-13-2015-17:04:09 to 12-13-2015-18:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-13-2015-17:04:09 to 12-13-2015-18:04:09

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
117.21.248.87	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
117.21.248.87	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
92.222.242.103	147.237.76.42	France	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
84.94.209.128	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.187.227	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.181.228.132	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
78.169.6.84	147.237.76.31	Turkey	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
192.186.95.178	147.237.77.121	Canada	e.navy.idf.il	ET SCAN NMAP -sS window 2048	1
2.54.20.24	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.11.44	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
117.21.248.87	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
117.21.248.87	147.237.76.39	China	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
92.222.242.103	147.237.76.44	France	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
84.108.174.126	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.77.79.38	147.237.76.202	China	e.halag.idf.il	ET SCAN Rapid POP3 Connections - Possible Brute Force Attack	1
79.183.176.19	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.178.59	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
78.193.2.8	147.237.77.212	France	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
192.186.95.178	147.237.77.121	Canada	e.navy.idf.il	ET SCAN NMAP -sS window 3072	1
46.19.85.4	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.186.95.178	147.237.77.121	Canada	e.navy.idf.il	ET SCAN NMAP -f -sS	1
2.54.4.43	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

12-13-2015-17:04:09 to 12-13-2015-18:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
199.203.9.245	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	666
185.120.126.58		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	42
46.19.86.197	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	40
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
46.19.86.197	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	29
46.19.86.197	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
100.100.16.12		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
46.19.86.197	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	22
37.26.146.174	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
46.19.86.197	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	20
185.120.126.58		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	20
81.218.241.25	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
46.19.86.178	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
109.150.86.73	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	17
66.102.9.81	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	15
188.120.148.212	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.85.250	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
46.19.86.13	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
149.88.151.160	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.206	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	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
46.19.86.178	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
176.13.5.233	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
2.52.33.246	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.133	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
213.57.131.178	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
46.19.85.5	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
85.64.75.153	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
85.64.75.153	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
81.218.241.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
109.67.63.44	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.140.189.227	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.206	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.181.102.60	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.59.255	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
84.229.249.38	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.100	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.117.252.177	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
199.203.9.245	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.250.255.71	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
37.19.122.110	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
84.229.249.38	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.211	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
40.77.167.54	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.125.246.202	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.158	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.211	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.125.78.20	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.126.144.122	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

12-13-2015-17:04:09 to 12-13-2015-18:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.51.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	300
2.54.51.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	151
176.13.7.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	138
176.13.7.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
2.54.132.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
199.203.9.245	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 199.203.9.245	Block	100
176.13.7.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	52
46.19.86.28	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	50
2.54.132.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	44
2.54.132.30	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 2.54.132.30	Block	23
37.26.148.166	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 37.26.148.166	Block	10
185.32.179.47	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
46.121.211.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
176.13.12.44	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 176.13.12.44	Block	5
199.203.9.245	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 199.203.9.245	Block	5
84.109.132.138	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 84.109.132.138	Block	4
176.13.12.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.12.44	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	3
149.88.78.244	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 149.88.78.244	Block	3
2.54.51.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	3
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/$$$&?&?$$$	Block	3
46.117.163.76	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.8.173.107	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
46.116.58.216	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
109.67.63.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
185.120.126.56		147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
37.142.136.246	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 37.142.136.246 (Unknown SSL Session)	None	2
66.249.66.16	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	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
109.186.8.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.28	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	2
176.12.140.217	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
2.54.142.155	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
176.12.151.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
176.13.5.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.66.43	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx	Block	1
37.26.147.154	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
95.86.68.70	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.220.158.101	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1
176.12.136.80	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.36.156	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
79.180.24.197	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.125.78.20	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
95.222.28.134	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
2.54.186.189	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
85.64.244.252	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.120.146.218	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/tfasim.aspx.	Block	1
149.88.78.244	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
82.166.152.130	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

12-13-2015-17:04:09 to 12-13-2015-18:04:09