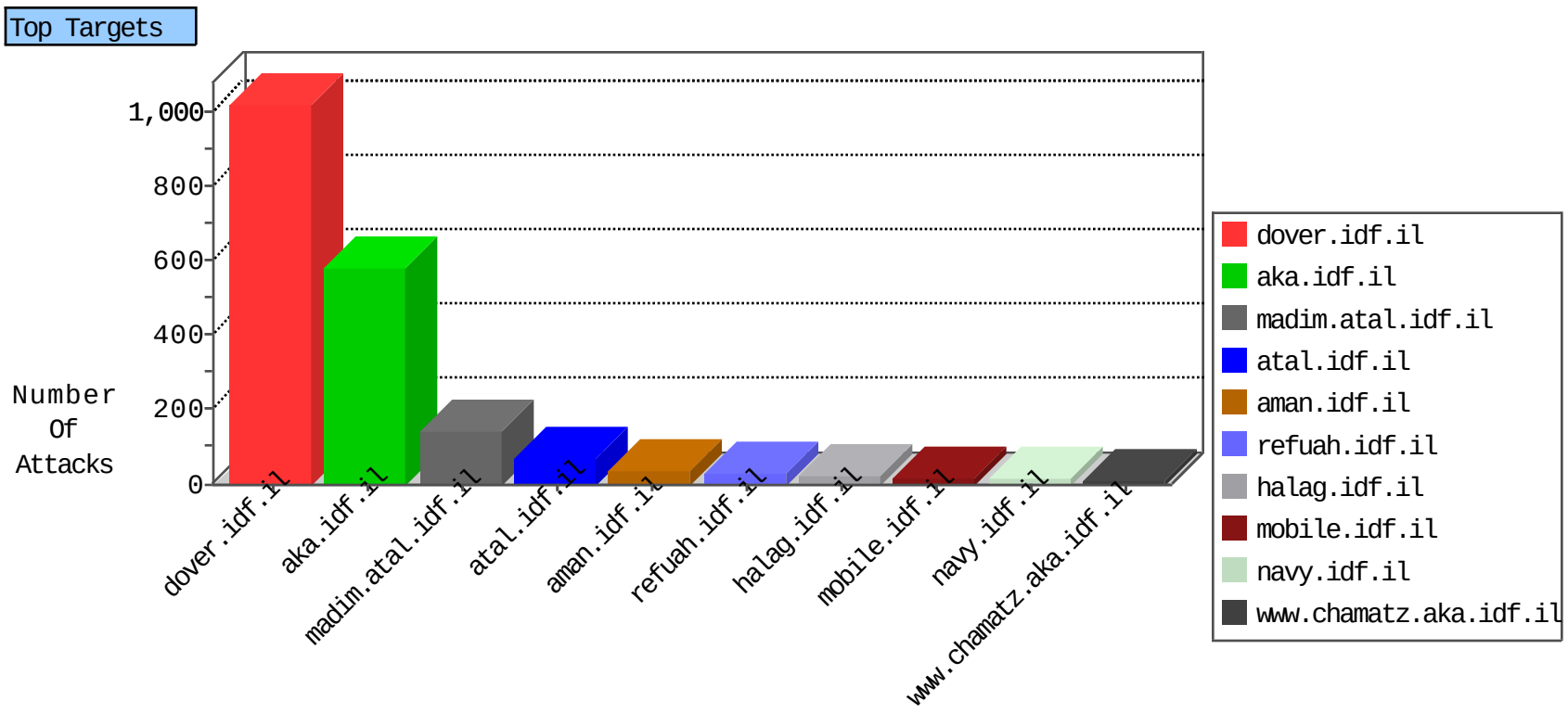
11-21-2015-18:04:00 to 11-21-2015-19:04:00

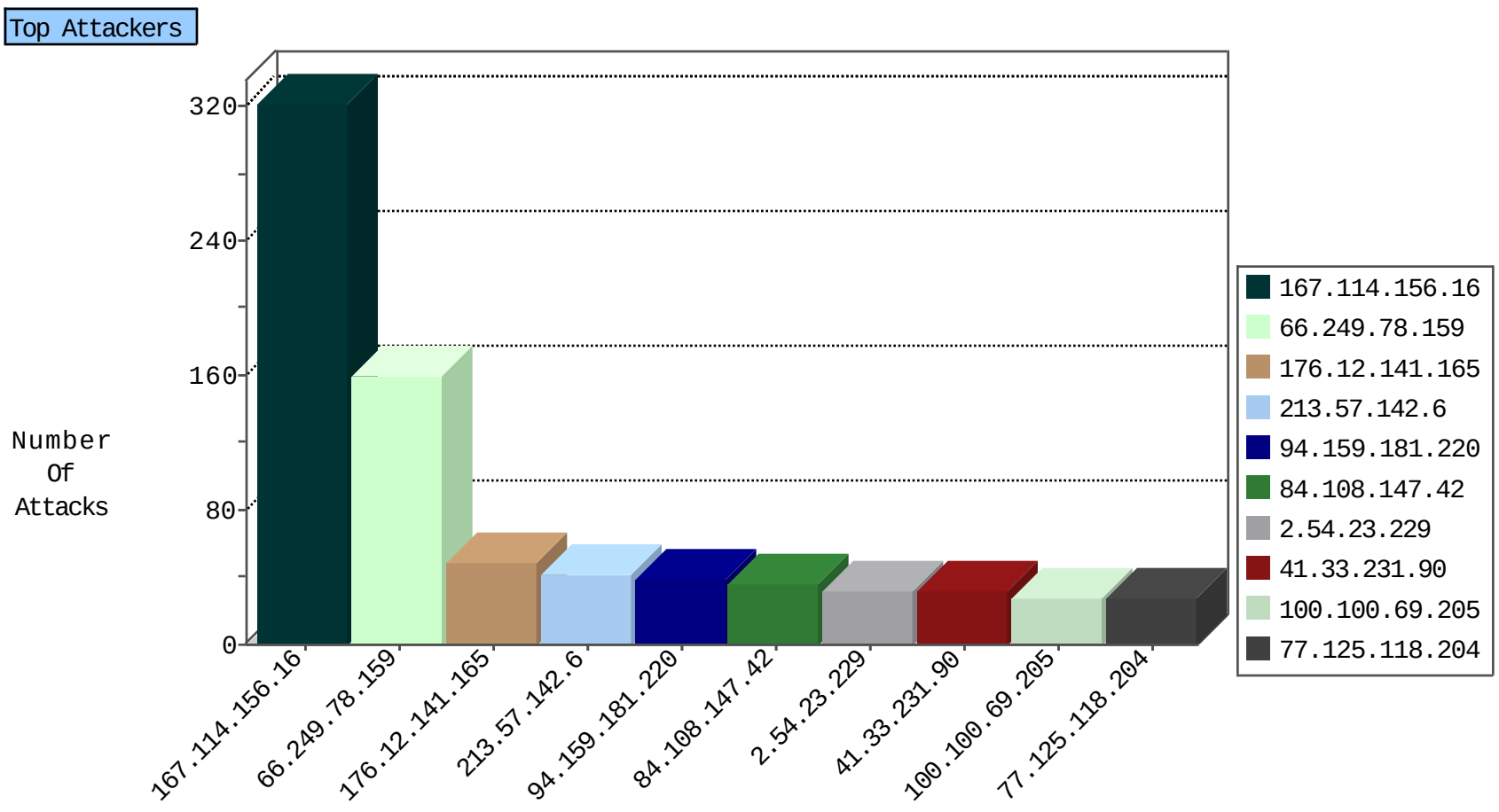
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

11-21-2015-18:04:00 to 11-21-2015-19:04:00

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	HTTP-POST-Segmented-DoS	dest-reset	20197
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	5188
79.179.109.150	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	7
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	7
79.183.101.138	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
77.125.81.195	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
87.68.253.97	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
185.120.126.74		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
82.166.22.17	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
10.0.0.8		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
146.185.239.100	Russian Federation	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	drop	1
93.174.93.151	Netherlands	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
147.236.238.33	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
134.147.203.115	Germany	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
85.25.43.94	Germany	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
146.185.239.100	Russian Federation	147.237.72.166	aka.idf.il	block-sp-traf1	drop	1

11-21-2015-18:04:00 to 11-21-2015-19:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

11-21-2015-18:04:00 to 11-21-2015-19:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
176.12.141.165	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	12
77.125.118.204	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	12
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
77.125.15.99	147.237.0.34	Israel	tikshuv.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
62.38.250.31	147.237.76.196	Greece	e.sviva.idf.il	ET SCAN NMAP -f -sS	1
200.121.165.81	147.237.77.227	Peru	e.hamaz.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
93.172.191.171	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.183.28.189	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.38.250.31	147.237.76.196	Greece	e.sviva.idf.il	ET SCAN NMAP -sS window 2048	1
58.253.96.122	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
199.101.186.178	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
178.62.126.13	147.237.72.14	United States	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
80.246.133.15	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.198.211	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

11-21-2015-18:04:00 to 11-21-2015-19:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	56
84.108.147.42	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	27
213.57.142.6	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	23
167.114.234.35	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
100.100.87.120		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	23
2.54.23.229	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	21
79.177.227.85	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
176.12.141.165	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
213.57.142.6	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	18
176.12.141.165	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	17
176.13.12.218	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
100.100.69.205		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
100.100.7.70		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	16
77.125.74.198	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
100.100.0.25		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
132.66.236.210	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
100.100.69.205		147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	11
2.54.23.229	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
100.100.102.76		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
82.166.22.17	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
79.180.4.3	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
199.16.156.125	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	9
79.177.43.244	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
79.183.101.138	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.181	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
209.6.145.20	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
84.108.111.66	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
209.6.145.20	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
213.57.142.233	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
79.183.225.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
5.28.150.19	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.67.102.148	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
2.52.51.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
82.81.163.138	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
213.57.130.121	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
79.182.223.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.26.148.203	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.54.176.137	Israel	147.237.77.243	mobile.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.132.25	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
109.66.162.203	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
77.125.118.204	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Urgent Data Enforcement	TCP segment with urgent pointer. Urgent data indication was stripped. Please refer to sk36869.	alert	6
213.57.132.25	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
5.29.131.218	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
89.138.76.247	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.66.162.203	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.119.180	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
77.125.118.204	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Urgent Data Enforcement	TCP segment with urgent pointer. Urgent data indication was stripped. Please refer to sk36869.	drop	6
213.57.132.25	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6

11-21-2015-18:04:00 to 11-21-2015-19:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	80
94.159.181.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
84.108.70.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	24
149.78.250.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	20
2.54.24.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
192.116.149.145	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 192.116.149.145	Block	6
85.64.22.233	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	6
85.64.22.233	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/pages/fan_status.php	Block	6
79.182.165.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
79.182.56.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.117.23.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.120.126.72		147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.121.108.146	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.176.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.247.30.234	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/iturim/resources/images/body/images/main.jpg	Block	3
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
89.138.77.31	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.85.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.139.60	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.180.115.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
62.90.219.220	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
46.19.85.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
62.219.137.97	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/contactus.aspx	Block	2
80.246.139.29	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
77.127.174.7	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	2
40.77.167.43	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	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
79.181.180.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.6.37	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	2
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
46.19.85.220	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
89.138.76.247	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.72	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
84.108.94.196	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
66.249.75.38	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/news/news.in.aspx	Block	1
66.249.64.56	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
157.55.39.229	United States	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
2.54.176.137	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22638-he/dover.aspx.	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9696-he/refuah.aspx	Block	1
213.57.241.199	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.72	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method ppppppp_fda4ab59 in URL	Block	1
87.69.92.136	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Unknown Parameter gt; in www.aka.idf.il/main/rabanut/general.aspx	None	1
5.144.59.11	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	1
82.81.163.138	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.177.224.201	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	1
109.160.135.236	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1

11-21-2015-18:04:00 to 11-21-2015-19:04:00