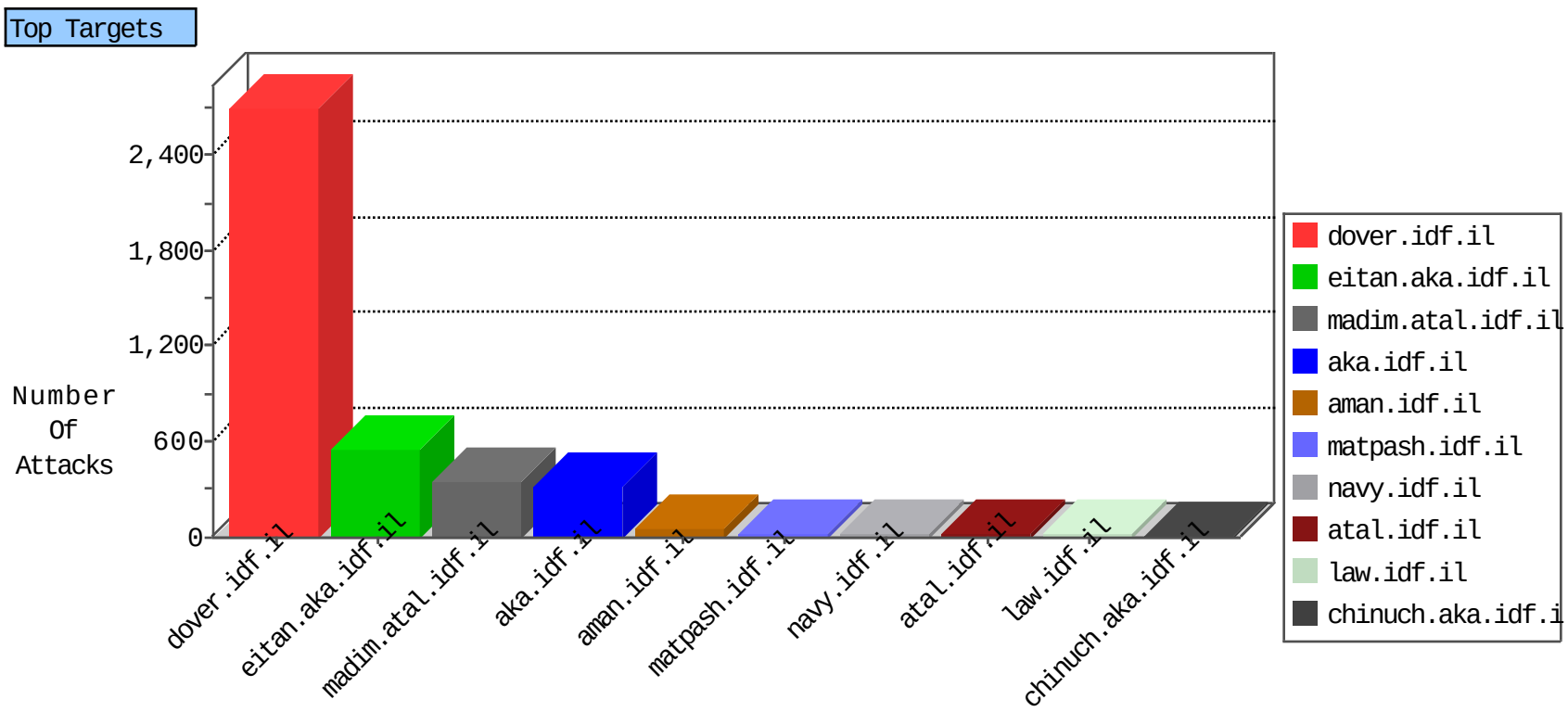
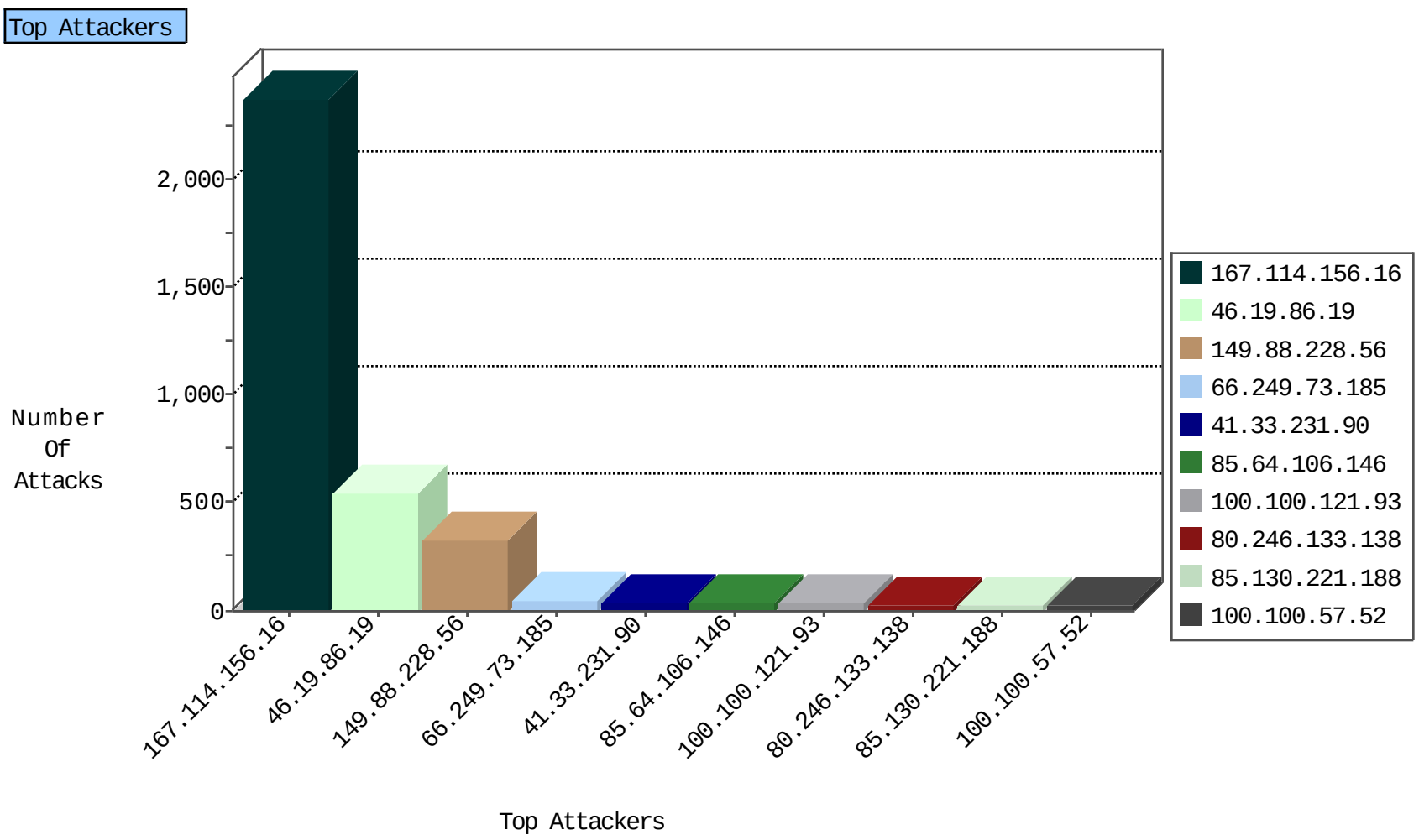
11-27-2015-20:04:00 to 11-27-2015-21:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-27-2015-20:04:00 to 11-27-2015-21:04:00

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	3562
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
66.240.192.138	United States	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
153.31.119.142	United States	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
87.69.191.71	Israel	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
93.174.93.151	Netherlands	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
153.31.119.142	United States	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1

11-27-2015-20:04:00 to 11-27-2015-21:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.165.15.60	France	147.237.77.233	atal.idf.il	C228: HTTP: AhrefBot crawler	Block	1
46.19.86.111	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

11-27-2015-20:04:00 to 11-27-2015-21:04:00

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
66.249.78.147	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
59.45.79.117	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
43.229.53.89	147.237.0.34	Japan	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
222.213.255.87	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.45.79.117	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
190.252.22.109	147.237.8.28	Colombia	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.45.79.117	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.72.156	Netherlands	aman.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
46.172.71.252	147.237.77.170	Ukraine	maarachot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
59.45.79.117	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	1
43.229.53.89	147.237.0.17	Japan	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
186.210.119.24	147.237.76.30	Brazil	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.45.79.117	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
79.180.62.124	147.237.77.74	Israel	law.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
46.172.71.252	147.237.77.234	Ukraine	halag.idf.il	ET SCAN NMAP -sS window 1024	1

11-27-2015-20:04:00 to 11-27-2015-21:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.86.19	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	483
66.249.73.185	United States	147.237.77.216	dover.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	36
149.88.228.56	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
100.100.121.93		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
80.246.133.138	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
100.100.57.52		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	24
100.100.120.6		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	17
37.142.64.109	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	12
85.64.106.146	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	12
100.100.25.97		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
188.120.148.200	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
109.64.39.245	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
220.255.98.33	Singapore	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.169.174.11	Portugal	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
188.120.148.200	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
75.32.230.150	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.26	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
85.130.171.48	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
85.64.106.146	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
93.172.8.156	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
85.64.106.146	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.148.134	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
89.138.240.248	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
31.154.160.207	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.64.106.146	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
212.179.173.137	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.148.163	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.73.193	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.108.1.57	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
89.138.240.248	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
119.73.253.6	Singapore	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.64.106.146	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
93.172.8.156	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
85.130.221.188	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.65.184.99	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
2.52.172.5	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
85.130.221.188	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
85.130.221.188	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
85.130.171.48	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
185.120.126.48		147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	4
2.52.172.5	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
100.100.43.211		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
197.119.77.225	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.160.227.156	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
94.159.140.40	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
2.52.172.5	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
212.235.83.63	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.88.228.56	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 149.88.228.56	Block	157
149.88.228.56	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	131
46.19.86.19	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.19	Block	56
178.137.167.94	Ukraine	147.237.72.166	aka.idf.il	PHP Attempt	Block	6
178.137.167.94	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 178.137.167.94	Block	5
157.55.39.122	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	4
109.65.42.187	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	4
46.116.98.44	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-he	Block	4
92.53.96.105	Russian Federation	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
192.116.48.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
89.221.250.23	Sweden	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
37.26.148.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.12.148.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.142.68.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.12.151.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
195.56.240.100	Hungary	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
104.152.108.121	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	3
37.142.177.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
103.241.148.4	Australia	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
80.178.251.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
103.241.148.4	Australia	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 103.241.148.4	Block	2
176.13.23.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.94.35.75	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
89.221.250.23	Sweden	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 89.221.250.23	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
2.54.38.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
62.0.102.146	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
109.66.62.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ufi/reaction/	Block	2
66.249.65.80	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	2
157.55.39.107	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	2
84.228.165.247	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
109.64.218.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.8.32	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	2
5.29.160.26	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
104.152.108.121	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 104.152.108.121	Block	1
74.208.105.30	United States	147.237.72.156	aman.idf.il	eMail Hoarding	Block	1
185.32.179.31	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
85.65.57.31	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
212.235.83.63	Israel	147.237.72.166	aka.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 212.235.83.63	Block	1
54.167.178.253	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
141.212.121.208	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/	Block	1
40.77.167.35	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
2.54.42.44	Israel	147.237.77.216	dover.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 2.54.42.44	Block	1
66.249.73.151	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1065-he/dover.aspx	Block	1
66.249.64.160	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/1117-7664-he/nakhal.aspx	Block	1
149.88.206.254	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
109.160.227.156	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1