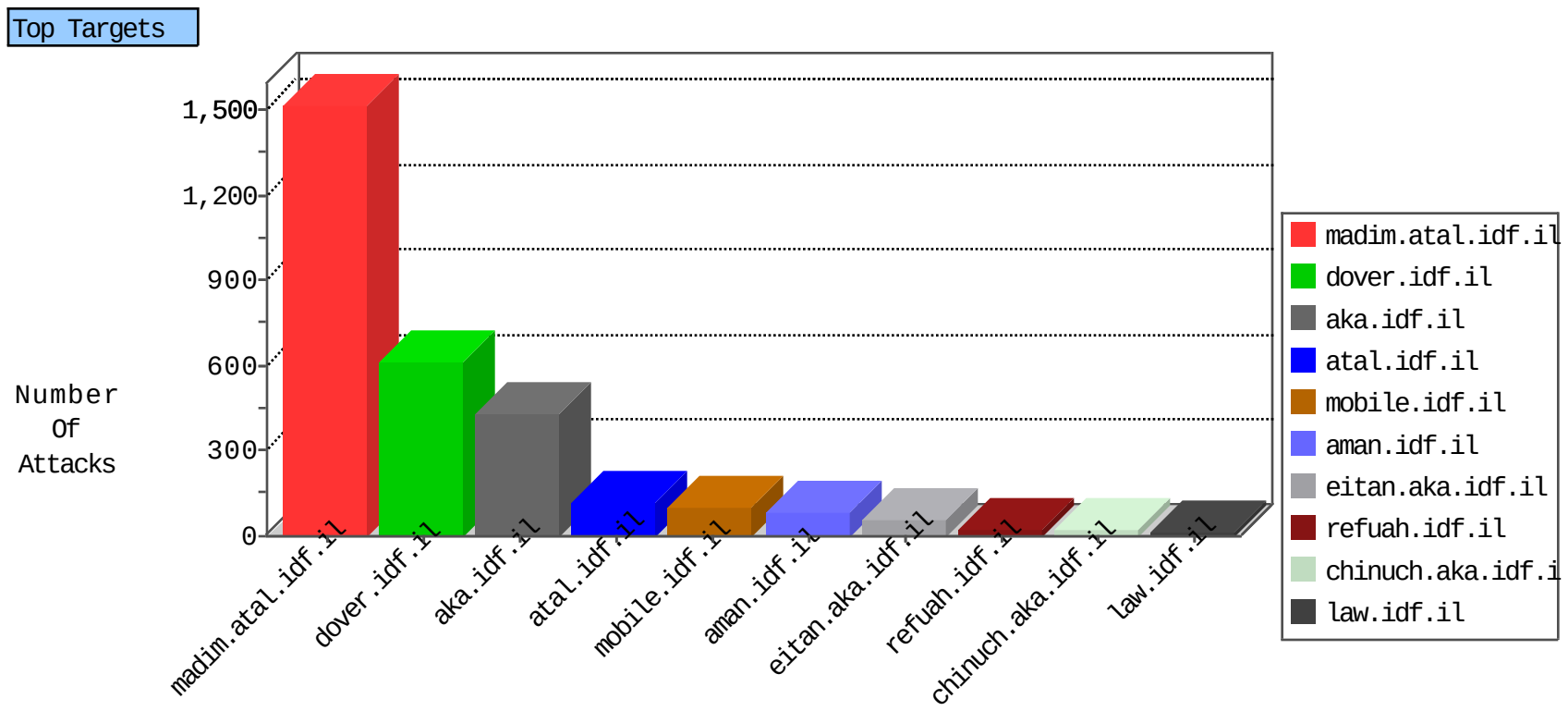
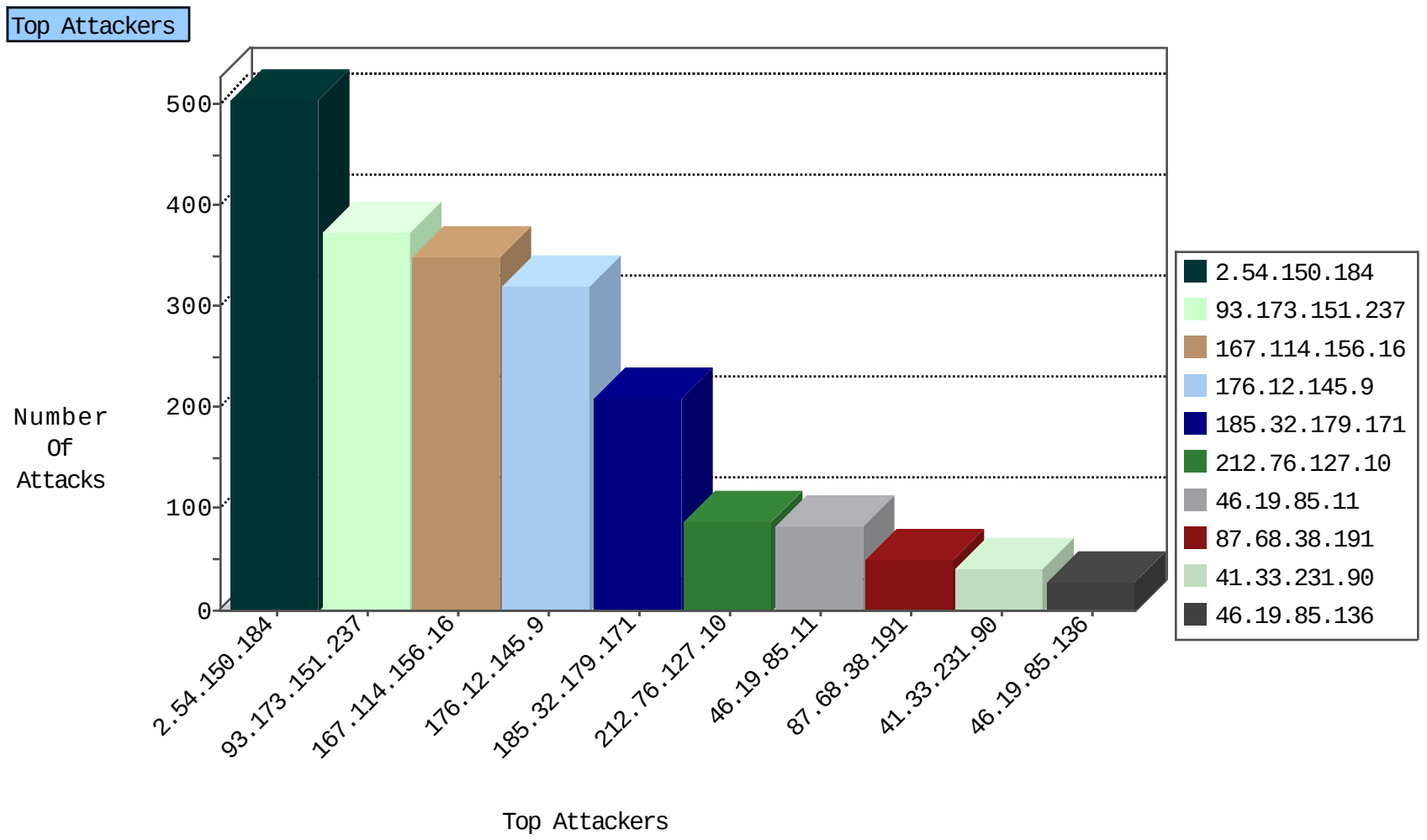
12-29-2015-18:04:03 to 12-29-2015-19:04:03

IDF Under Attack
Daily Report

Top Targets



Top Attackers



12-29-2015-18:04:03 to 12-29-2015-19:04:03

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	4001
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2272
167.114.156.16	Canada	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	7
37.26.146.177	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
82.80.128.235	Israel	147.237.77.235	sviva.idf.il	Block_Udp_All_Nets	drop	1
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	1
37.26.147.140	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

12-29-2015-18:04:03 to 12-29-2015-19:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
36.77.206.230	Indonesia	147.237.76.42	refuah.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
36.77.206.230	Indonesia	147.237.77.170	maarachot.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1

12-29-2015-18:04:03 to 12-29-2015-19:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
36.77.206.230	147.237.77.74	Indonesia	law.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	5
36.77.206.230	147.237.77.170	Indonesia	maarachot.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	4
36.77.206.230	147.237.76.42	Indonesia	refuah.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	3
66.249.64.218	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sA (2)	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
82.80.164.236	147.237.0.34	Israel	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
109.66.125.128	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.27.105.179	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.167.119.239	147.237.77.234	Canada	halag.idf.il	ET SCAN Potential SSH Scan	1
180.153.104.125	147.237.77.74	China	law.idf.il	ET SCAN NMAP -f -sS	1
59.45.79.117	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
104.167.119.239	147.237.77.176	Canada	matpash.idf.il	ET SCAN Potential SSH Scan	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
104.167.119.239	147.237.77.74	Canada	law.idf.il	ET SCAN Potential SSH Scan	1
151.217.178.88	147.237.77.61		e.cogat.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.210.245.151	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.167.119.239	147.237.76.177	Canada	ncore.idf.il	ET SCAN Potential SSH Scan	1
37.142.68.23	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
151.217.30.152	147.237.77.121		e.navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.167.119.239	147.237.72.14	Canada	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
37.26.147.140	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
151.217.30.48	147.237.76.86		navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
87.68.253.82	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.151.35.216	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
139.91.210.41	147.237.72.156	Greece	aman.idf.il	ET SCAN NMAP -sS window 1024	1
79.180.225.161	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.8.204.65	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
119.81.60.162	147.237.76.42	Singapore	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
77.126.15.95	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.219.238.10	147.237.0.19		madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
180.153.104.125	147.237.77.74	China	law.idf.il	ET SCAN NMAP -sS window 2048	1
59.45.79.117	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
104.167.119.239	147.237.77.179	Canada	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
168.62.238.153	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
104.167.119.239	147.237.77.121	Canada	e.navy.idf.il	ET SCAN Potential SSH Scan	1
151.217.178.88	147.237.77.74		law.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
59.45.79.117	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
104.167.119.239	147.237.77.19	Canada	law-forum.idf.il	ET SCAN Potential SSH Scan	1
151.217.178.88	147.237.76.198		e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.167.119.239	147.237.76.31	Canada	nakchal.idf.il	ET SCAN Potential SSH Scan	1
37.114.59.147	147.237.0.200	Germany	m4u.idf.il	ET SCAN Potential SSH Scan	1
151.217.30.48	147.237.77.179		e.mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.139.175.98	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
151.217.30.48	147.237.0.15		kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
213.57.62.151	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
132.3.29.79	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.29.85	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

12-29-2015-18:04:03 to 12-29-2015-19:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.76.127.10	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	81
87.68.38.191	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	51
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
176.13.23.35	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
85.65.24.138	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
79.176.164.129	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	13
79.183.12.208	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
62.0.200.160	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
46.19.86.221	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.163	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.135	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
185.32.179.200	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
37.26.146.149	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
46.19.85.163	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.181.4.53	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.126.165.101	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.149	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
74.108.110.114	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
99.238.48.146	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.66.144.45	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
74.108.110.114	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
212.76.127.10	Israel	147.237.77.234	halag.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
2.54.7.164	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.64.5.250	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
212.76.127.44	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
2.52.129.166	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.4.25	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.102.254.71	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.176.192.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.136.242	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
79.181.154.234	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.0.81.57	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
79.176.164.129	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
2.54.178.163	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.116.114.254	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
79.176.164.129	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.122	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.116.114.254	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
82.102.203.39	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
37.46.39.74	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.102.254.71	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.178.58.248	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.149	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.253.206.240	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
66.220.146.27	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
5.102.254.245	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

12-29-2015-18:04:03 to 12-29-2015-19:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.150.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	284
93.173.151.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	204
176.12.145.9	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	189
176.12.145.9	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	125
2.54.150.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	117
185.32.179.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
93.173.151.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
2.54.150.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
185.32.179.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	91
46.19.85.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	80
93.173.151.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	65
46.19.85.136	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.19.85.136	Block	25
185.32.179.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	15
93.172.15.196	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	10
207.46.13.134	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	9
46.210.245.151	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
192.114.170.10	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
176.12.145.9	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	7
2.54.38.7	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Days in mobile.idf.il/milluim	Block	6
81.218.205.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
79.176.59.130	Israel	147.237.0.34	tikshuv.idf.il	Parameter Type Violation phrase in www.tikshuv.idf.il/modules/forums/searchresults.aspx	Block	4
149.78.207.90	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
46.19.85.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
89.139.254.33	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	3
46.19.86.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.11	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	3
46.19.86.31	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.176.59.130	Israel	147.237.0.34	tikshuv.idf.il	Multiple Illegal Parameter Encoding from 79.176.59.130	None	2
81.218.241.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.26	Block	2
79.179.110.187	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
85.65.140.67	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	2
93.172.14.137	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	2
77.127.148.6	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1541	Block	2
185.27.105.118	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
84.94.38.200	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	2
79.180.251.20	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
37.26.146.220	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1133-he/atal.aspx	Block	1
85.250.180.170	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.56	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/2347.jpg	Block	1
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
109.253.209.164	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1133-he/atal.aspx	Block	1
80.246.137.191	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
212.235.112.216	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
2.52.4.25	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.178.169.157	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding my /Qg[	None	1
46.19.86.64	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
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	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9043-he/refuah.aspx	Block	1
176.13.13.175	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1

12-29-2015-18:04:03 to 12-29-2015-19:04:03