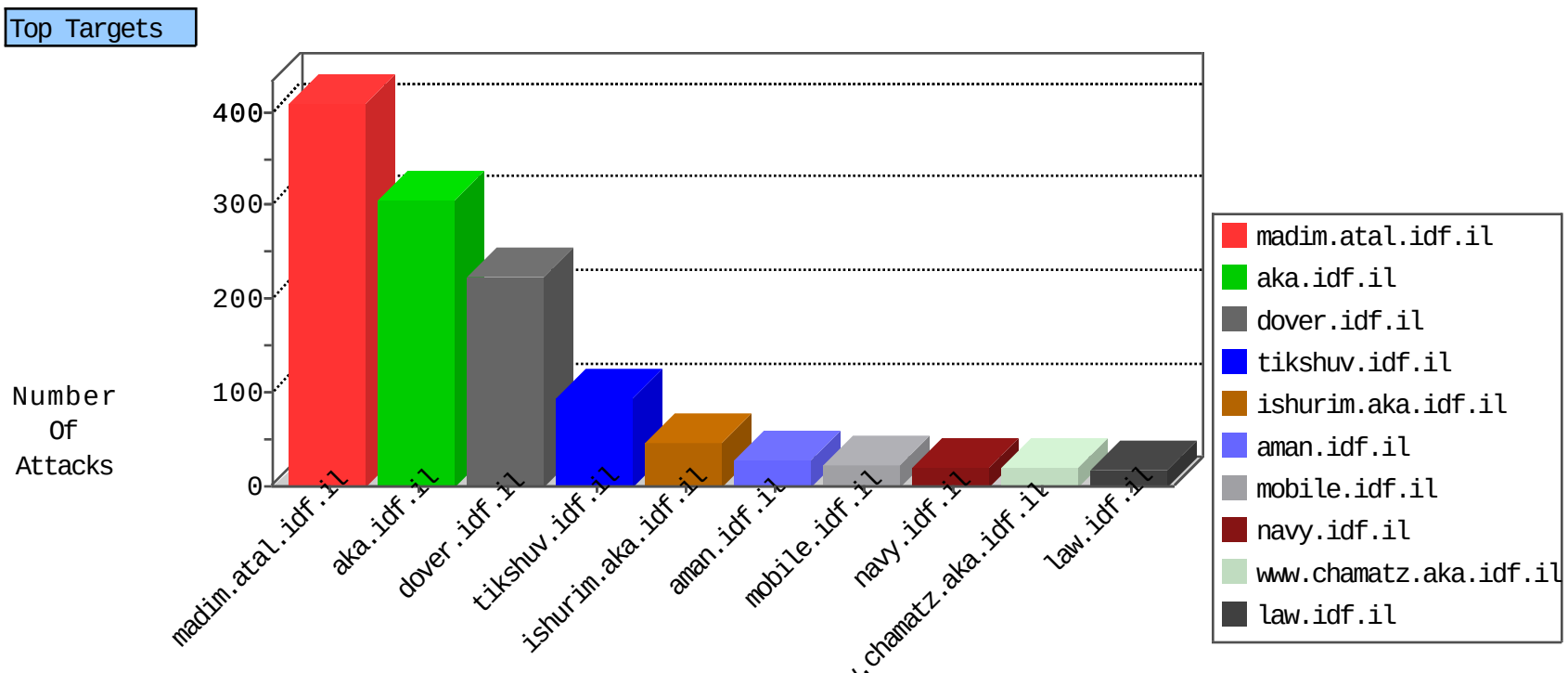
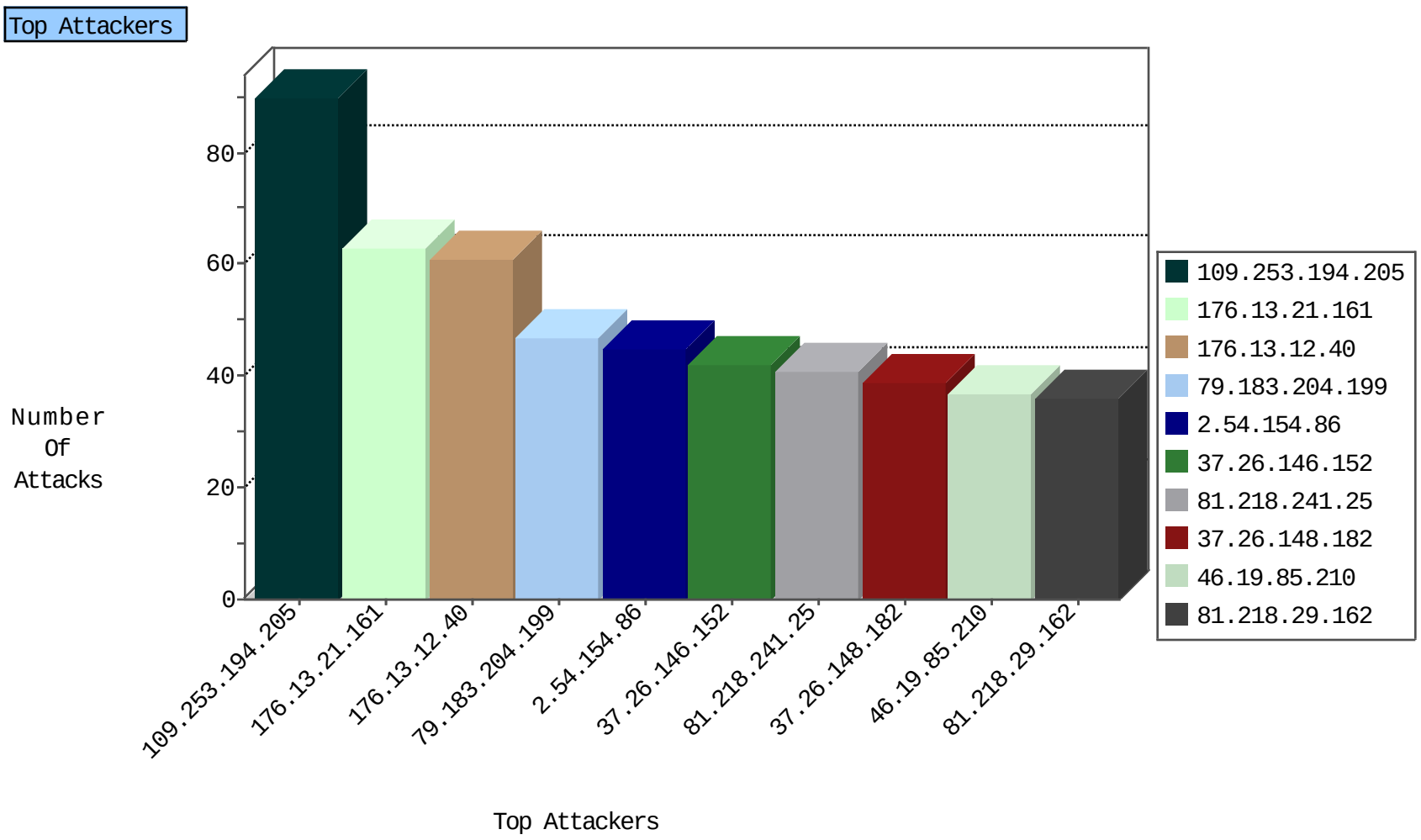
03-06-2016-10:04:03 to 03-06-2016-11:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-06-2016-10:04:03 to 03-06-2016-11:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.241.25	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	91
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	76
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
134.147.203.115	Germany	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	2
24.90.51.170	United States	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.122	United States	147.237.77.243	mobile.idf.il	Block_Ntp_All_Net	drop	1
89.248.160.132	Netherlands	147.237.77.205	prisha.idf.il	block-sp-traf1	drop	1
24.90.51.170	United States	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.86	United States	147.237.77.227	e.hamaz.idf.il	Block_Ntp_All_Net	drop	1
24.90.51.170	United States	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
212.71.235.23	United Kingdom	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
89.248.160.132	Netherlands	147.237.77.235	sviva.idf.il	block-sp-traf1	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.102	United States	147.237.77.205	prisha.idf.il	Block_Ntp_All_Net	drop	1
89.248.160.132	Netherlands	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	drop	1
24.90.51.170	United States	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
216.218.206.77	United States	147.237.8.46	e.chinuch.idf.il	Block_Udp_All_Nets	drop	1
23.94.69.234	United States	147.237.77.179	e.mazi.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.106	United States	147.237.8.46	e.chinuch.idf.il	Block_Ntp_All_Net	drop	1
89.248.160.132	Netherlands	147.237.77.19	law-forum.idf.il	block-sp-traf1	drop	1
24.90.51.170	United States	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
139.162.152.84	Netherlands	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1

03-06-2016-10:04:03 to 03-06-2016-11:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.130.171	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	12
79.183.204.199	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	11
192.118.12.102	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	8
82.166.141.45	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	8
2.54.164.200	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	4
82.80.193.236	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	3
79.179.210.119	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
177.17.188.131	Brazil	147.237.77.216	dover.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	1

03-06-2016-10:04:03 to 03-06-2016-11:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
185.72.179.221	147.237.77.170		maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
138.134.102.15	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.71.100.187	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.166.137.197	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.2.245	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.219.112.52	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.235.98.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.116.114.154	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.164.133.149	147.237.0.34	Russian Federation	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
31.168.220.230	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
194.90.178.37	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.131.89	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.228.214.151	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.193	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
87.71.31.140	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.80.193.236	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.23.177	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
220.231.195.122	147.237.76.86	China	navy.idf.il	ET SCAN NMAP -sS window 3072	1
62.219.24.52	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.199.146.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.182	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
5.29.68.115	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

03-06-2016-10:04:03 to 03-06-2016-11:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.183.204.199	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
81.218.241.25	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	18
84.94.199.194	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.86.227	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.13	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
96.47.68.190	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
81.218.29.162	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	10
31.168.89.106	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	10
31.168.89.106	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	10
46.19.86.110	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
81.218.29.162	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
138.134.102.16	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.85.199	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.211	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
109.65.29.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
37.26.146.152	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.182.135.26	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.152	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.85.199	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
62.0.236.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
176.13.15.10	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.215	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.152	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
46.19.85.199	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
149.50.89.15	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.26.146.152	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
84.95.207.195	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.107	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.152	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
31.168.89.106	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
81.218.29.162	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.128.127	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
37.26.146.152	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.199	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
81.218.134.75	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.152	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.211	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
81.218.29.162	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
109.65.29.44	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
66.249.93.142	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	5
2.54.40.241	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
109.236.93.203	Netherlands	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
81.218.29.162	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.15	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.236.93.203	Netherlands	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
188.120.148.207	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.22.135.205	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.107	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.102	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.194.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	90
176.13.21.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	63
176.13.12.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	59
2.54.154.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
37.26.148.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	37
46.19.85.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	37
109.253.205.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	28
2.54.187.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	19
66.249.64.233	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	8
176.13.14.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
95.86.66.66	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 95.86.66.66	Block	4
37.26.148.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
109.253.215.198	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.23.47	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.32.198	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.209.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.151.40.42	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/homepage/www.youtube.com/v/3g51ei5nuhg	Block	3
50.93.198.132	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
46.19.85.13	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	2
80.246.137.2	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
50.93.198.132	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 50.93.198.132	Block	2
5.22.135.205	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	2
81.218.251.251	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
199.16.156.124	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/6/size220x0/7826.jpg	Block	2
80.74.103.204	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/	Block	2
95.86.102.161	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush	Block	2
109.66.13.110	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1
41.230.14.223	Tunisia	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/contactus/contactus.aspx	Block	1
212.150.255.134	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/8/	Block	1
84.109.3.71	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized URL Access on maarachot.idf.il/xmlrpc.php	Block	1
184.105.247.196	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
80.178.101.44	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
109.64.33.196	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
37.26.148.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Parameter Type Violation on madim.atal.idf.il/mobile/1088-he/meretz.aspx parameter ctl00$ContentPlaceHolder1$txtMobile	Block	1
213.151.41.61	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/&sa=u&ved=0ahukewj80bw-16vlahupg5okhtf6aeaqfggnmaa&usg=afqjcnhcdsh5ryhkeugapxldsq7fowjwnw	Block	1
81.218.134.75	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 81.218.134.75	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1399-en/dover.aspx	Block	1
66.249.64.243	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
109.253.142.255	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	1
212.179.46.16	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.tech.atal.idf.il/style/shared/reset.css	Block	1
84.109.119.241	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
185.89.217.225		147.237.77.74	law.idf.il	URL is Above Root Directory www.law.idf.il/../images/1.he/navigation/navigation_arrow.gif	Block	1
113.76.90.223	China	147.237.76.31	nakchal.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
109.64.33.196	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/xmlrpc.php	Block	1
213.151.63.4	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/68496.pdf&sa=u&ved=0ahukewjkwcvk06vlahvh-g4khxrndzyqfggxmau&usg=afqjcnf1lqenko5rrixrsew9o4u81jiwzq	Block	1
81.218.134.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/5/	Block	1
212.25.102.57	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to tech.atal.idf.il/style/shared/reset.css	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/history/history/stm	Block	1
46.19.85.103	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1