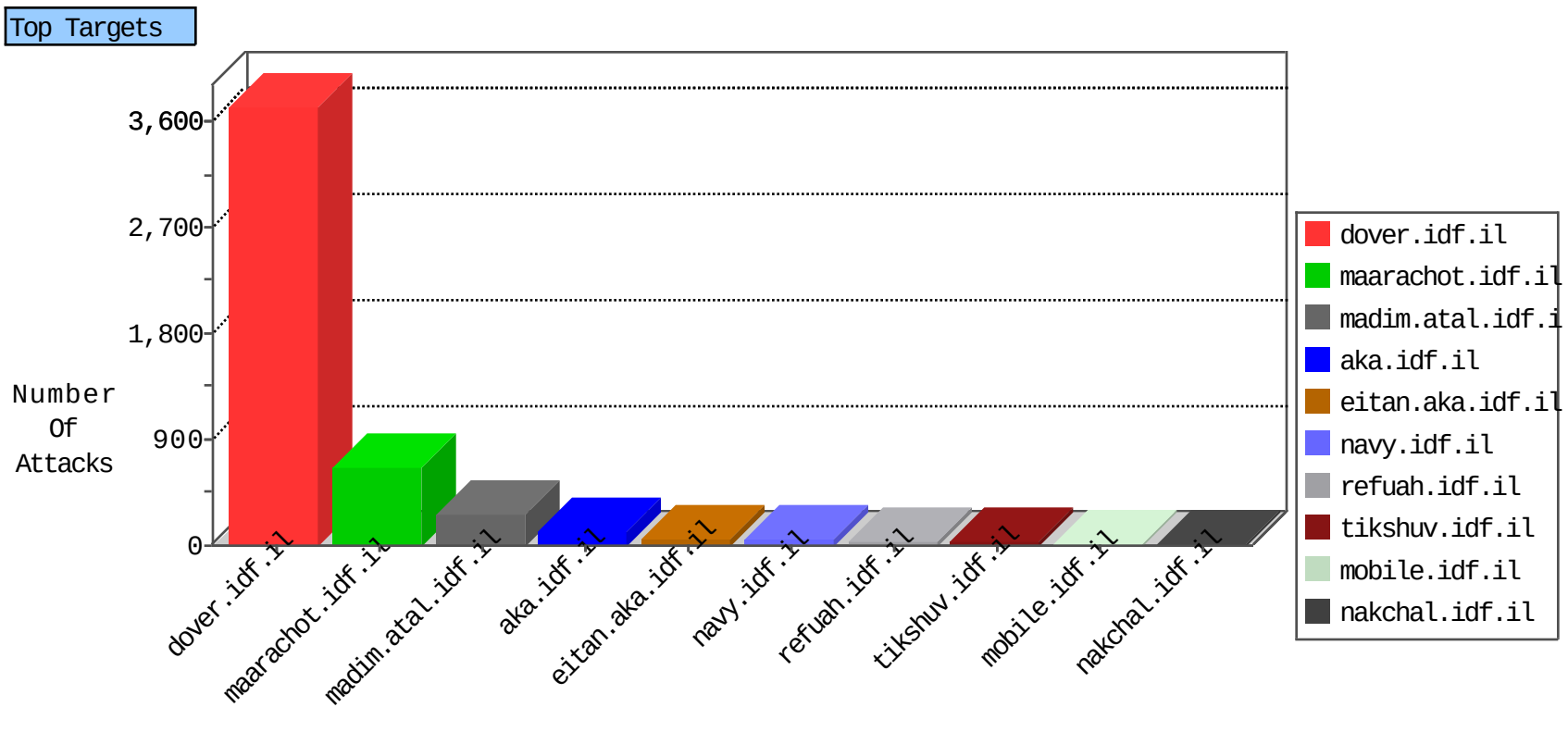
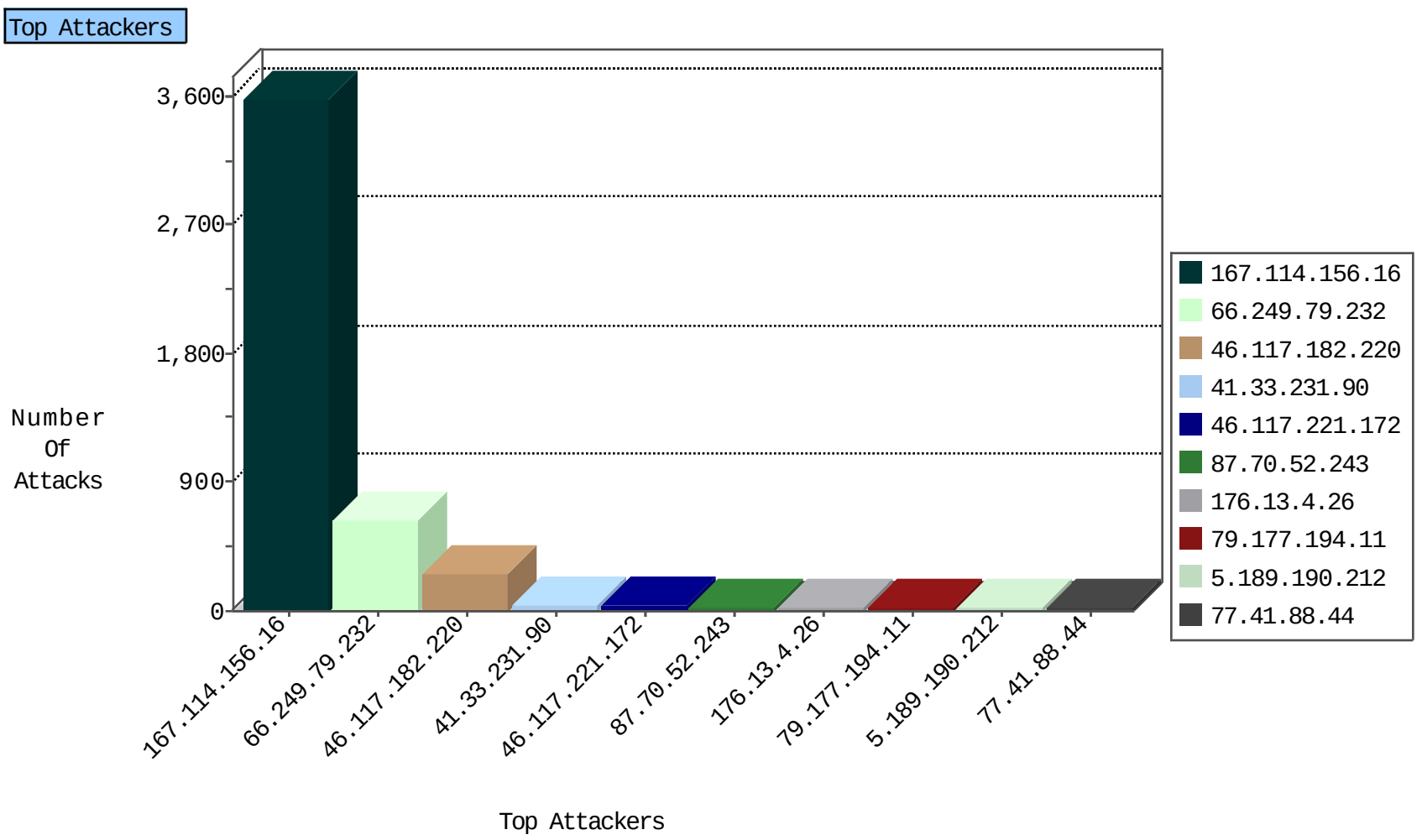
04-16-2016-11:04:08 to 04-16-2016-12:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-16-2016-11:04:08 to 04-16-2016-12:04:08

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	Block_Ip_Web_In	drop	3587
123.59.59.52	China	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	4
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
77.41.88.44	Russian Federation	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Http	drop	3
101.201.147.32	China	147.237.77.19	law-forum.idf.il	block-sp-traf1	forward	2
77.41.88.44	Russian Federation	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Http	drop	1
185.40.4.195	Russian Federation	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1	Russian Federation	147.237.0.33	idf.il	Block_Udp_All_Nets	drop	1

04-16-2016-11:04:08 to 04-16-2016-12:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.178.0.28	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
106.38.241.144	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.66.184	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-16-2016-11:04:08 to 04-16-2016-12:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.79.232	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	642
79.177.194.11	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sA (2)	22
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
193.201.227.65	147.237.0.34	Ukraine	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
40.84.149.32	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
115.29.138.97	147.237.0.33	China	idf.il	ET SCAN NMAP -sS window 1024	1
106.186.113.67	147.237.76.196	Japan	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
104.238.82.190	147.237.77.179	United States	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
104.238.82.190	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
104.232.98.38	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 4096	1
65.181.123.161	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
40.84.149.32	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 4096	1
185.70.184.186	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
13.92.245.177	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
113.240.250.154	147.237.72.166	China	aka.idf.il	ET SCAN NMAP -sS window 1024	1
104.238.82.190	147.237.77.205	United States	prisha.idf.il	ET SCAN Potential SSH Scan	1
104.238.82.190	147.237.77.74	United States	law.idf.il	ET SCAN Potential SSH Scan	1
104.238.82.190	147.237.8.45	United States	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
80.82.78.38	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
65.181.123.161	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1

04-16-2016-11:04:08 to 04-16-2016-12:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
46.117.221.172	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	32
87.70.52.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
176.13.4.26	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
46.210.154.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
77.41.88.44	Russian Federation	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
93.158.152.25	Russian Federation	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	9
109.253.147.242	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
185.3.146.242	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
94.230.86.198	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
64.233.172.171	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
84.95.208.20	Israel	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	6
31.168.91.234	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
77.125.91.169	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	4
79.181.30.242	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.129.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.117.135.34	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.10.107	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
79.176.48.125	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
87.70.10.81	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.117.182.220	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
79.182.203.182	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.48.125	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
62.219.132.15	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
157.55.39.90	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.0.60.20	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.29.4	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.205.25	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.10.107	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
79.180.178.242	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.79.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.10.107	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
46.117.182.220	Israel	147.237.0.19	madim.atal.idf.il	drop	First packet isn't SYN	drop	2
79.181.214.165	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
156.197.54.94	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
79.177.111.50	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.159.104	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
213.8.204.5	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
109.253.159.104	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
213.57.42.254	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.86.37	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.200	United States	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
188.120.154.97	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
5.102.254.9	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.107	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
66.249.93.119	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.76.39	mobile.meitav.idf.i	drop	SAM rule	drop	1
216.243.31.2	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.117.182.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	260
5.189.190.212	Germany	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	20
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	7
81.218.33.77	Israel	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	Block	4
109.64.23.56	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
81.218.33.77	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/sip_storage/files/4/	Block	3
109.65.79.2	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 109.65.79.2	Block	2
109.253.147.242	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
157.55.39.43	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
46.19.85.40	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unknown HTTP Request Method a6.1458986135.1.1458986135.1458986135.; in URL asp.net_sessionid=m2xely55mbxlsiycb5izru45	Block	1
91.210.146.159	Ukraine	147.237.0.34	tikshuv.idf.il	PHP Attempt	Block	1
79.179.182.1	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/templates/homepage/mobile	Block	1
66.249.66.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/2828.jpg	Block	1
207.46.13.144	United States	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
40.77.167.25	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-14886-en/dover.aspx	Block	1
86.90.251.188	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/templates/shared/usercontrols/headerupper/	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1779-he/dover.aspx	Block	1
157.55.39.81	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
46.19.86.37	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
104.236.55.186	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 104.236.55.186	Block	1
81.218.33.77	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 81.218.33.77	Block	1
66.249.66.123	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/2351.jpg	Block	1
207.46.13.157	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/templates/departmentslobby/	Block	1
46.19.85.40	Israel	147.237.77.226	www.chamatz.aka.idf.il	Abnormally Long Request method	Block	1
89.138.204.235	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/mobile	Block	1
74.82.47.3	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-18538-en/kkkkkkk=620c1ab7kkkkkkk_620c1ab7	Block	1
108.227.98.31	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
207.46.13.172	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/templates/shared/usercontrols/navmenu/	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1511-	Block	1
46.19.85.40	Israel	147.237.77.226	www.chamatz.aka.idf.il	Illegal HTTP Version	Block	1
91.210.146.159	Ukraine	147.237.0.34	tikshuv.idf.il	Admin Blocking	Block	1
79.178.131.172	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/home/default.aspx	Block	1
193.143.77.10	Poland	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/test/wp-admin/	Block	1
46.117.182.220	Israel	147.237.0.19	madim.atal.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 208.115.113.82	Block	1
151.236.48.39	United Kingdom	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/wp-admin/	Block	1
46.19.85.40	Israel	147.237.77.226	www.chamatz.aka.idf.il	Malformed URL asp.net_sessionid=m2xely55mbxlsiycb5izru45	Block	1
91.210.146.159	Ukraine	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 91.210.146.159	Block	1
79.179.182.1	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 79.179.182.1	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	1
207.46.13.136	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/matash	Block	1
37.97.167.6	Netherlands	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/wordpress/wp-admin/	Block	1
109.65.79.2	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
85.64.155.24	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1379-he/dover.aspx	Block	1