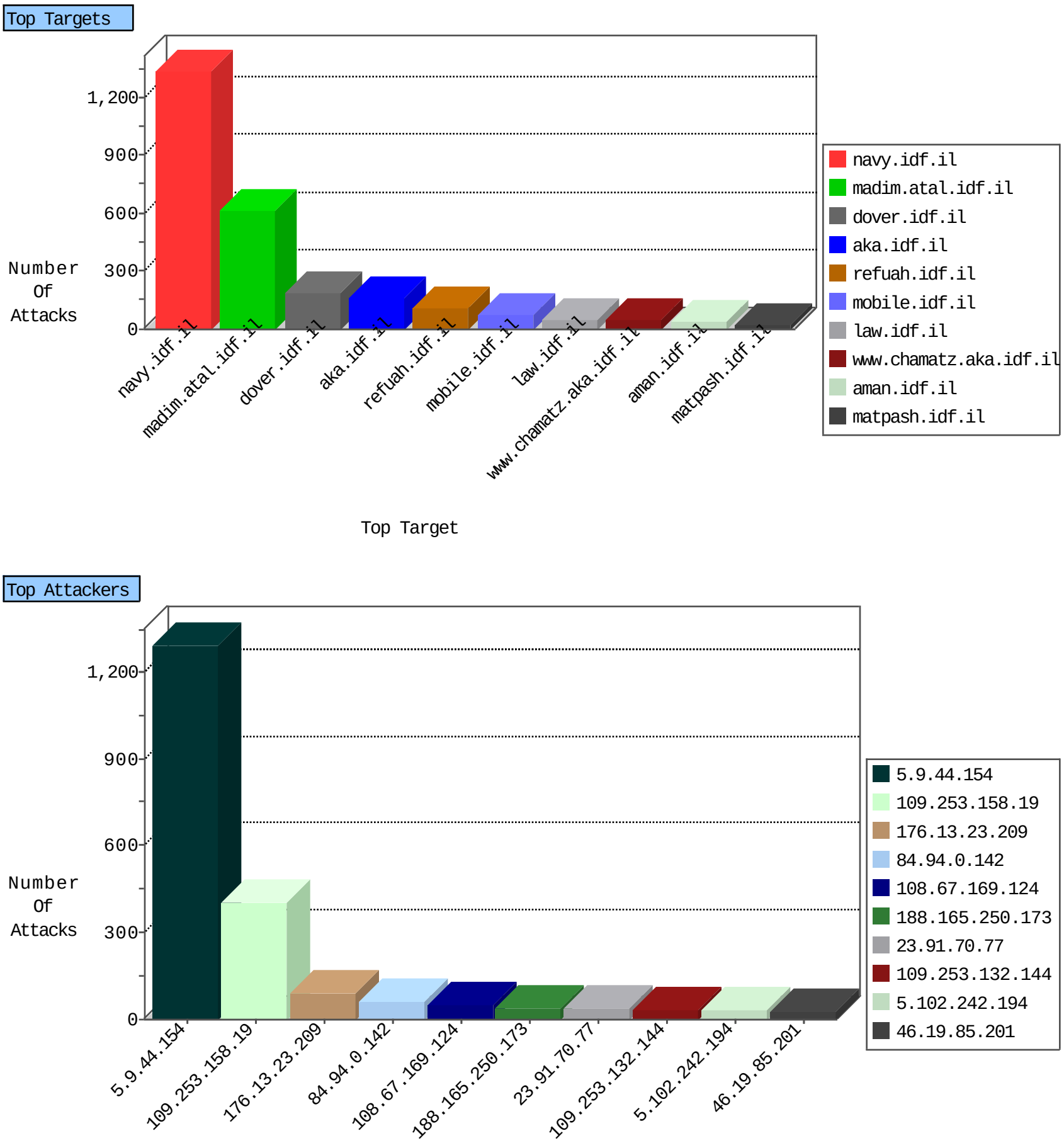
09-22-2016-21:04:06 to 09-22-2016-22:04:06

IDF Under Attack Daily Report



09-22-2016-21:04:06 to 09-22-2016-22:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.232.114	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
185.94.111.1	Russian Federation	147.237.76.198	e.yohalan.idf.il	Black List	drop	1

09-22-2016-21:04:06 to 09-22-2016-22:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
108.67.169.124	United States	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
188.165.250.173	France	147.237.77.226	www.chamatz.aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
158.85.253.245	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
23.91.70.77	United States	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
216.68.91.180	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
108.67.169.124	United States	147.237.76.42	refuah.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
168.1.80.134	Australia	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
108.67.169.124	United States	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
188.165.250.173	France	147.237.77.226	www.chamatz.aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
50.63.196.35	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
23.91.70.77	United States	147.237.76.42	refuah.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
216.26.128.28	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
74.84.136.105	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
23.91.70.77	United States	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
23.91.70.77	United States	147.237.76.42	refuah.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	1
123.126.68.132	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

09-22-2016-21:04:06 to 09-22-2016-22:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
108.67.169.124	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	26
188.165.250.173	147.237.77.226	France	www.chamatz.aka.idf.il	SQL Injection - Select From	20
23.91.70.77	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	19
74.84.136.105	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	18
216.26.128.28	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	14
158.85.253.245	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	8
216.68.91.180	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
168.1.80.134	147.237.77.74	Australia	law.idf.il	SQL Injection - Select From	8
50.63.196.35	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	8
163.172.169.150	147.237.77.205	United Kingdom	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
45.63.28.189	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
113.240.250.154	147.237.77.227	China	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
192.151.154.43	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
100.13.130.4	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 1024	1
84.111.244.124	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
164.52.227.101	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
164.52.227.101	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1
45.63.28.189	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.129.15	147.237.77.121	United Kingdom	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
125.65.82.44	147.237.76.42	China	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
113.240.250.154	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
100.13.130.4	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
192.151.154.43	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
92.42.162.161	147.237.8.50	Russian Federation	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
185.32.179.91	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.111.37.245	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
164.52.227.101	147.237.76.44	United States	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
62.90.243.244	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	1
164.52.227.101	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
45.63.28.189	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 1024	1

09-22-2016-21:04:06 to 09-22-2016-22:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.9.44.154	Germany	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1287
5.102.242.194	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
107.167.106.89	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	23
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
2.54.205.17	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.201	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
46.19.85.201	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
213.57.221.250	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
79.178.30.57	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
88.128.80.108	Germany	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
86.130.162.162	United Kingdom	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
176.13.0.31	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
46.19.86.13	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.115.29.104	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
46.19.86.13	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.18	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.251	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
82.201.2.43	Netherlands	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
184.168.46.19	United States	147.237.72.156	aman.idf.il	drop	SAM rule	drop	6
77.139.68.80	France	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.178.170.231	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
37.26.147.184	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.86.13	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
37.26.147.200	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
2.53.28.47	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.13	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.123	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
79.180.82.64	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
188.102.158.11	Germany	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
141.226.217.109	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.253	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.180.183.249	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	4
82.102.159.65	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
77.139.14.233	France	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
80.230.227.128	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
77.138.75.89	France	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
88.128.80.108	Germany	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
176.13.13.206	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.201	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.176.113.234	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
77.125.83.148	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.146.188	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.226.241.187	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
85.64.93.175	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
37.26.146.236	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.226.241.187	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
217.132.20.50	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
213.57.221.250	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
85.64.124.34	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3

09-22-2016-21:04:06 to 09-22-2016-22:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.158.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	404
176.13.23.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	90
84.94.0.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	60
109.253.132.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
79.177.249.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
31.154.81.21	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.151.35.212	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/giyus/	Block	3
46.19.86.199	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
46.117.75.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.109.131.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
85.65.60.166	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
31.168.120.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.158.21	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
24.247.11.147	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/horaot/templates/main.asp	Block	2
141.226.217.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
185.32.179.151	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
31.39.188.171	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/	Block	2
187.160.183.19	Mexico	147.237.76.86	navy.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
201.172.180.91	Mexico	147.237.77.233	atal.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
189.218.69.253	Mexico	147.237.76.147	chinuch.aka.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
66.249.66.182	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/3382.jpg	Block	1
91.90.13.141	Ukraine	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
79.178.30.57	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
201.166.218.4	Mexico	147.237.77.226	www.chamatz.aka.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
187.161.121.100	Mexico	147.237.77.234	halag.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
63.92.225.185	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
201.172.236.225	Mexico	147.237.76.42	refuah.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
189.218.217.170	Mexico	147.237.77.74	law.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
66.249.66.188	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/2348.jpg	Block	1
177.239.233.240	Mexico	147.237.76.31	nakchal.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
94.75.72.26	Poland	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
201.166.222.155	Mexico	147.237.76.30	himush.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
187.161.121.100	Mexico	147.237.77.235	sviva.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
66.102.9.8	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
89.138.169.95	Israel	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	1
66.249.69.133	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
189.219.85.161	Mexico	147.237.77.216	dover.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
37.26.146.210	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
177.239.233.240	Mexico	147.237.76.39	mobile.meitav.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
103.210.50.29		147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	1
84.108.187.245	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
201.172.180.91	Mexico	147.237.72.166	aka.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
189.218.51.36	Mexico	147.237.76.200	eitan.aka.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
66.240.236.119	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/robots.txt	Block	1
89.138.169.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 10.100.102.4/upnpcp/notify/event	Block	1
77.138.246.186	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/	Block	1
189.219.172.149	Mexico	147.237.77.176	matpash.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
107.179.234.65	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.png	Block	1
201.172.180.91	Mexico	147.237.72.167	ishurim.aka.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
84.108.187.245	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 84.108.187.245	Block	1

09-22-2016-21:04:06 to 09-22-2016-22:04:06