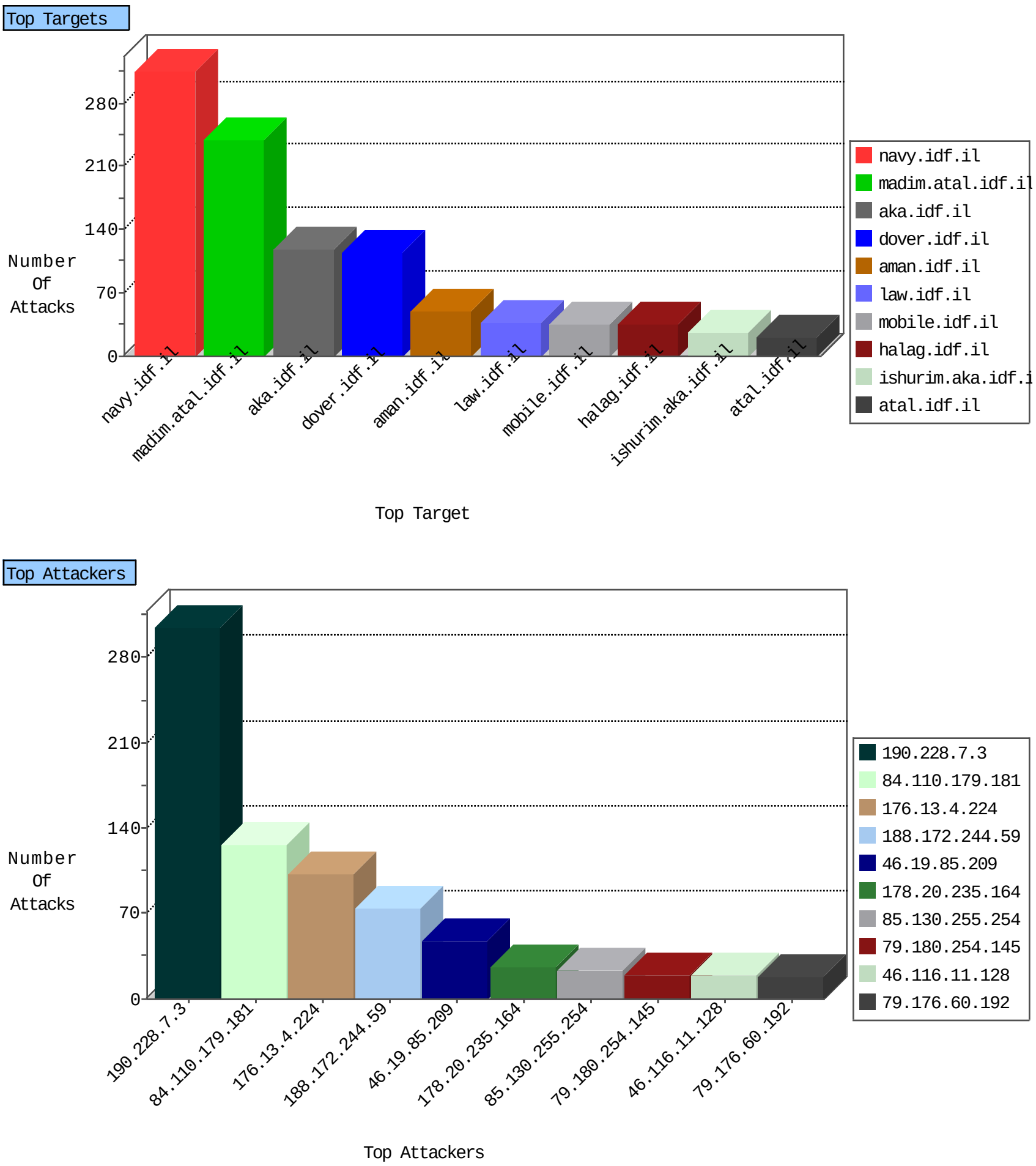
09-04-2016-22:04:03 to 09-04-2016-23:04:03

IDF Under Attack
Daily Report



09-04-2016-22:04:03 to 09-04-2016-23:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.202.233.56	Germany	147.237.76.30	himush.idf.il	Black List	drop	1
213.202.233.56	Germany	147.237.76.31	nakchal.idf.il	Black List	drop	1
66.240.192.138	United States	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1
123.59.59.52	China	147.237.77.233	atal.idf.il	block-sp-traf1	forward	1

09-04-2016-22:04:03 to 09-04-2016-23:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
178.20.235.164	Russian Federation	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
178.20.235.164	Russian Federation	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
97.74.215.165	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
45.62.248.47	Canada	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1

09-04-2016-22:04:03 to 09-04-2016-23:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
178.20.235.164	147.237.77.74	Russian Federation	law.idf.il	SQL Injection - Select From	14
97.74.215.165	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	8
91.121.75.9	147.237.72.166	France	aka.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	5
72.167.131.75	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	3
104.128.144.131	147.237.0.15	Canada	kosher-kravi.idf.i	ET SCAN NMAP -sS window 2048	1
61.240.144.66	147.237.77.74	China	law.idf.il	ET SCAN NMAP -sS window 1024	1
103.255.47.41	147.237.77.234	Hong Kong	halag.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
61.240.144.65	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
94.156.128.25	147.237.77.176	Bulgaria	matpash.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.224	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
211.141.78.56	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential VNC Scan 5900-5920	1
94.156.128.25	147.237.8.28	Bulgaria	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
208.100.26.228	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.158	147.237.76.198	Ukraine	e.yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
163.172.169.150	147.237.76.34	United Kingdom	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.51.213	147.237.76.44	United Kingdom	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
77.127.42.67	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.60.153.178	147.237.77.233	Russian Federation	atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
64.137.171.55	147.237.76.38	Canada	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.131	147.237.0.15	Canada	kosher-kravi.idf.i	ET SCAN NMAP -f -sS	1
61.240.144.65	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
97.105.173.114	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
94.156.128.25	147.237.77.234	Bulgaria	halag.idf.il	ET SCAN Potential SSH Scan	1
59.33.108.105	147.237.0.33	China	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
94.156.128.25	147.237.76.199	Bulgaria	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
41.253.240.226	147.237.77.61	Libyan Arab Jamahiriya	e.cogat.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
211.23.156.152	147.237.77.61	Taiwan	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
94.156.128.25	147.237.8.24	Bulgaria	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.76.198	Ukraine	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.51.213	147.237.76.44	United Kingdom	e.refuah.idf.il	ET SCAN NMAP -sS window 2048	1
89.138.118.186	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.51.213	147.237.76.44	United Kingdom	e.refuah.idf.il	ET SCAN NMAP -f -sS	1

09-04-2016-22:04:03 to 09-04-2016-23:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
190.228.7.3	Argentina	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	305
84.110.179.181	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	46
84.110.179.181	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	46
46.19.85.209	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
46.19.85.209	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	18
46.116.11.128	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
79.176.60.192	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
5.22.134.166	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.209	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.53.134.115	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
77.139.125.94	France	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
85.130.255.254	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
79.180.254.145	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
106.39.60.186	China	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	8
85.130.255.254	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
85.130.255.254	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
106.39.60.184	China	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	7
79.180.254.145	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
85.130.255.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
87.68.19.146	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.234.139	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.32.125	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
66.102.9.157	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	6
46.120.115.177	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
188.172.244.59	Austria	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
2.53.176.251	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.85.136	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
106.39.60.184	China	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	5
188.172.244.59	Austria	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
188.172.244.59	Austria	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
79.180.254.145	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
106.39.60.189	China	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	5
46.19.85.136	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
188.172.244.59	Austria	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
188.172.244.59	Austria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
188.172.244.59	Austria	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
188.172.244.59	Austria	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
84.109.9.60	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.116.11.128	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
188.172.244.59	Austria	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
188.172.244.59	Austria	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
188.172.244.59	Austria	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
188.172.244.59	Austria	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
188.172.244.59	Austria	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
188.172.244.59	Austria	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
176.13.11.142	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
85.130.234.154	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	3
109.253.214.178	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.226.218.104	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.114	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	3
188.172.244.59	Austria	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.4.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	103
84.110.179.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	34
109.64.80.87	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	6
79.176.60.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
5.29.74.190	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	3
2.53.191.15	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	3
84.109.105.52	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	3
66.249.76.35	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.35	Block	2
46.120.115.177	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
95.86.71.60	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
79.183.39.228	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
66.249.76.35	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/apple-app-site-association	Block	1
192.243.55.133	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/smalim/smalim.aspx?catid=58639	Block	1
46.19.85.98	Israel	147.237.77.226	www.chamatz.aka.idf.il	Malformed URL	Block	1
2.53.176.251	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
72.37.140.37	Italy	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 72.37.140.37	Block	1
62.217.51.69	Germany	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/klali.aspx	Block	1
8.37.231.198	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
84.108.5.170	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/about.aspx	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
192.243.55.135	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/general	Block	1
46.19.85.98	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unknown HTTP Request Method dx55pfxtoa45 in URL	Block	1
87.69.204.218	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
72.37.140.37	Italy	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main	Block	1
66.102.9.22	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
157.55.39.227	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
37.142.2.133	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1135-he/atal.aspx	Block	1
84.109.105.52	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 84.109.105.52	Block	1
2.53.21.87	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/giyus/qanda/default.asp	None	1
194.242.168.227	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/sitemap.aspx	Block	1
46.19.85.232	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
2.55.32.51	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
92.225.47.155	Germany	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.102.9.30	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
37.142.4.21	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
2.53.149.12	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
66.249.93.111	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.116.11.128	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
213.57.12.21	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/registrationwizard/undefined	Block	1
5.22.134.166	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
93.173.174.255	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
79.178.121.211	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
178.36.36.228	Poland	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
41.137.57.101	Morocco	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
2.53.149.12	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 2.53.149.12	Block	1
84.109.105.52	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/sip_storage/files/2/	Block	1
72.37.140.37	Italy	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/ishurim/main/	Block	1