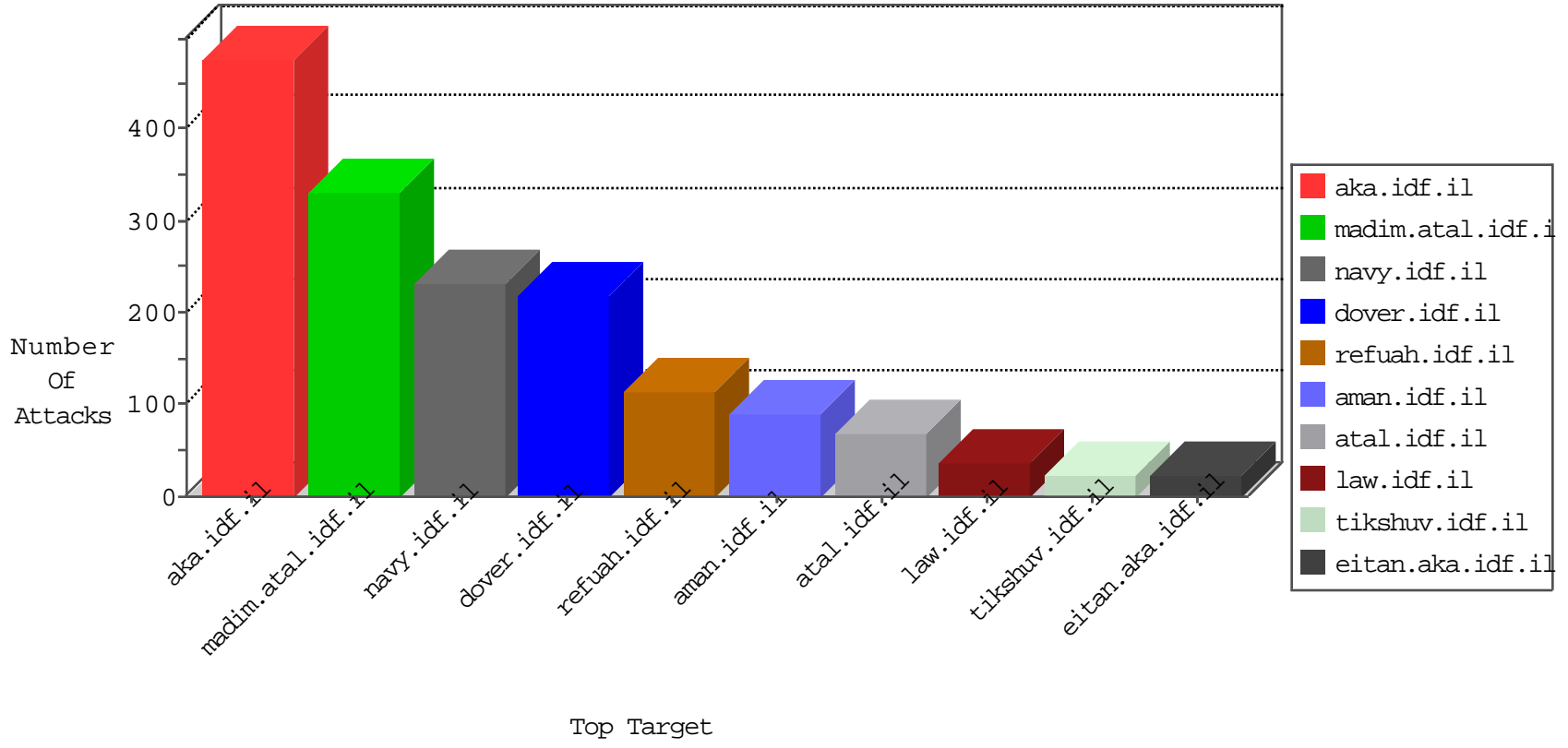


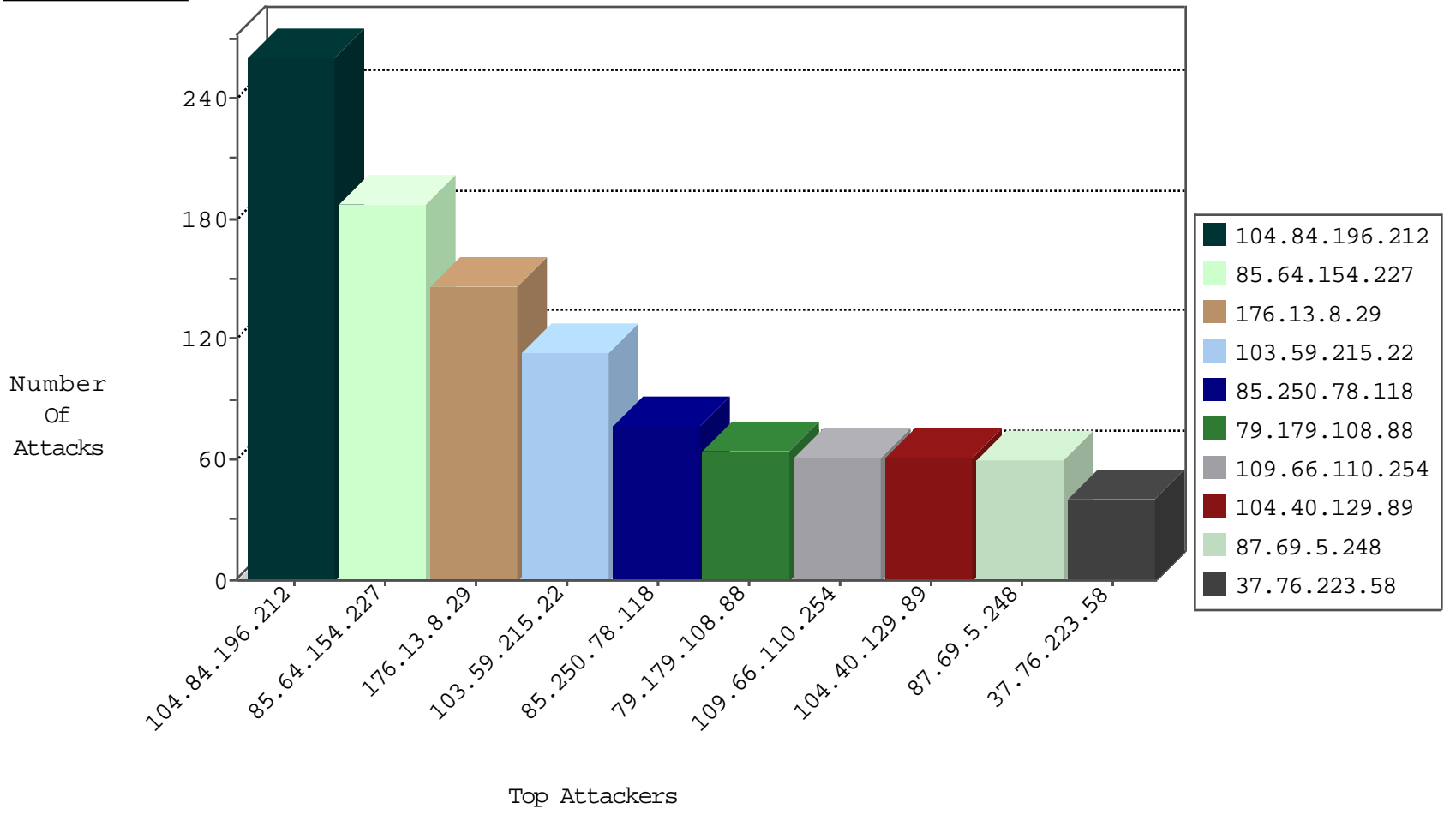
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
71.6.165.200	United States	147.237.76.201	e.atal.idf.il	Black List	drop	1
176.13.8.29	Israel	147.237.0.19	madim.atal.idf.il	DOSS-SSL-ClearText	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
177.185.192.77	Brazil	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
91.219.122.2	Poland	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
158.85.253.245	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	5
108.59.8.70	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
50.63.197.204	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
158.85.253.245	United States	147.237.77.233	atal.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
79.177.162.190	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sA (2)	35
177.185.192.77	147.237.77.233	Brazil	atal.idf.il	SQL Injection - Select From	18
91.219.122.2	147.237.77.74	Poland	law.idf.il	SQL Injection - Select From	8
158.85.253.245	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	6
109.64.55.1	147.237.72.156	Israel	aman.idf.il	ET SCAN NMAP -sA (2)	5
180.97.106.37	147.237.0.19	China	madim.atal.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
50.63.197.204	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	3
91.121.222.79	147.237.77.74	France	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
91.224.160.106	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
163.172.169.150	147.237.76.197	United Kingdom	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.129.15	147.237.77.234	United Kingdom	halag.idf.il	ET SCAN NMAP -sS window 1024	1
185.93.185.10	147.237.76.176	Ukraine	test.ncore.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.224.160.106	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.162	147.237.77.226	China	www.chamatz.aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
91.224.160.106	147.237.76.30	Netherlands	himush.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.161	147.237.77.61	China	e.cogat.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
180.97.106.37	147.237.0.34	China	tikshuv.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
91.224.160.106	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.37	147.237.0.17	China	m.my-kosher-kravi.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
163.172.169.150	147.237.77.234	United Kingdom	halag.idf.il	ET SCAN NMAP -sS window 1024	1
79.182.84.154	147.237.0.34	Israel	tikshuv.idf.il	ET SCAN NMAP -sA (2)	1
163.172.169.150	147.237.76.196	United Kingdom	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.76.117	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
161.18.218.116	147.237.77.205	Colombia	prisha.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
212.25.82.123	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.231	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.93.185.10	147.237.72.217	Ukraine	e.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.224.160.106	147.237.76.34	Netherlands	yochalan.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.162	147.237.0.16	China	my-kosher-kravi.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
91.224.160.106	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.37	147.237.76.38	China	e.e.meitav.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
91.224.160.106	147.237.0.33	Netherlands	idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
103.59.215.22	India	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	72
79.179.108.88	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	64
85.64.154.227	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
37.76.223.58	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
103.59.215.22	India	147.237.76.86	navy.idf.il	SYN Attack		monitor	35
37.26.149.159	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
87.69.5.248	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
88.7.114.90	Spain	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
185.93.35.174	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
104.84.196.212	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
104.84.196.212	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
87.68.32.234	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
104.84.196.212	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
87.68.32.234	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
104.84.196.212	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
104.84.196.212	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
87.69.36.120	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
104.84.196.212	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
104.84.196.212	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
87.69.36.120	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
104.84.196.212	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
104.84.196.212	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
104.84.196.212	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
104.84.196.212	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
104.84.196.212	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
104.84.196.212	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
104.84.196.212	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
89.139.233.52	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
104.84.196.212	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
104.84.196.212	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
104.84.196.212	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
104.84.196.212	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
104.84.196.212	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
104.84.196.212	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
104.84.196.212	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
87.69.5.248	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
104.84.196.212	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
100.92.233.191		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
87.69.5.248	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	9
185.3.147.67	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
77.125.11.163	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
46.19.86.84	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
103.59.215.22	India	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
100.92.189.105		147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	7
2.53.38.220	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
87.69.5.248	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
71.236.80.197	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.179.98.29	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
71.236.80.197	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	6
109.253.218.48	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.8.29	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	146
85.64.154.227	Israel	147.237.72.166	aka.idf.il	Automated Vulnerability Scanning V1	Block	128
85.250.78.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	77
109.66.110.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	61
85.65.61.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
37.142.250.133	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 37.142.250.133	Block	4
176.13.0.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.146.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.149.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.229.56.106	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 84.229.56.106	Block	2
46.19.85.224	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
175.45.57.190	Hong Kong	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/giyus/	Block	2
37.26.146.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.66.172.185	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/guyus	Block	2
180.97.106.37	China	147.237.0.34	tikshuv.idf.il	Multiple Untraceable SSL Sessions from 180.97.106.37 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
79.177.30.116	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to ww.idf.il/kamlar	Block	1
66.249.93.87	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
109.67.174.110	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
46.4.74.42	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/miluum/templates/inner.asp	Block	1
80.178.251.210	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	1
2.55.155.202	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
77.138.132.84	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/lomdim/tochen/	Block	1
108.46.232.143	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/general.aspx	Block	1
66.249.69.214	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/portalmiluum/templates/inner.asp	Block	1
37.26.148.189	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.109.209.142	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
180.97.106.162	China	147.237.0.16	my-kosher-kravi.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
79.178.187.202	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
67.205.134.104	United States	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.160.226.216	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
80.246.139.51	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.55.155.202	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/layout2.css	Block	1
176.13.228.18	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.138.245.158	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/about.aspx	Block	1
109.66.4.57	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/https://www.aman.idf.il/	Block	1
66.249.76.117	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
79.179.108.88	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
180.97.106.162	China	147.237.77.226	www.chamatz.aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
67.205.134.104	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on aka.idf.il/giyus/	Block	1
109.253.245.138	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
89.237.64.180	France	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/favicon.ico	Block	1
80.246.140.111	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
5.29.162.82	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
180.97.106.37	China	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
77.138.245.158	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
66.249.93.83	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/1.he/langstyle.css	Block	1
37.142.250.133	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012ources/images/innerpage/goback.gif	Block	1
84.229.56.106	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/giyus	Block	1
79.179.173.134	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https://www.aman.idf.il/	Block	1