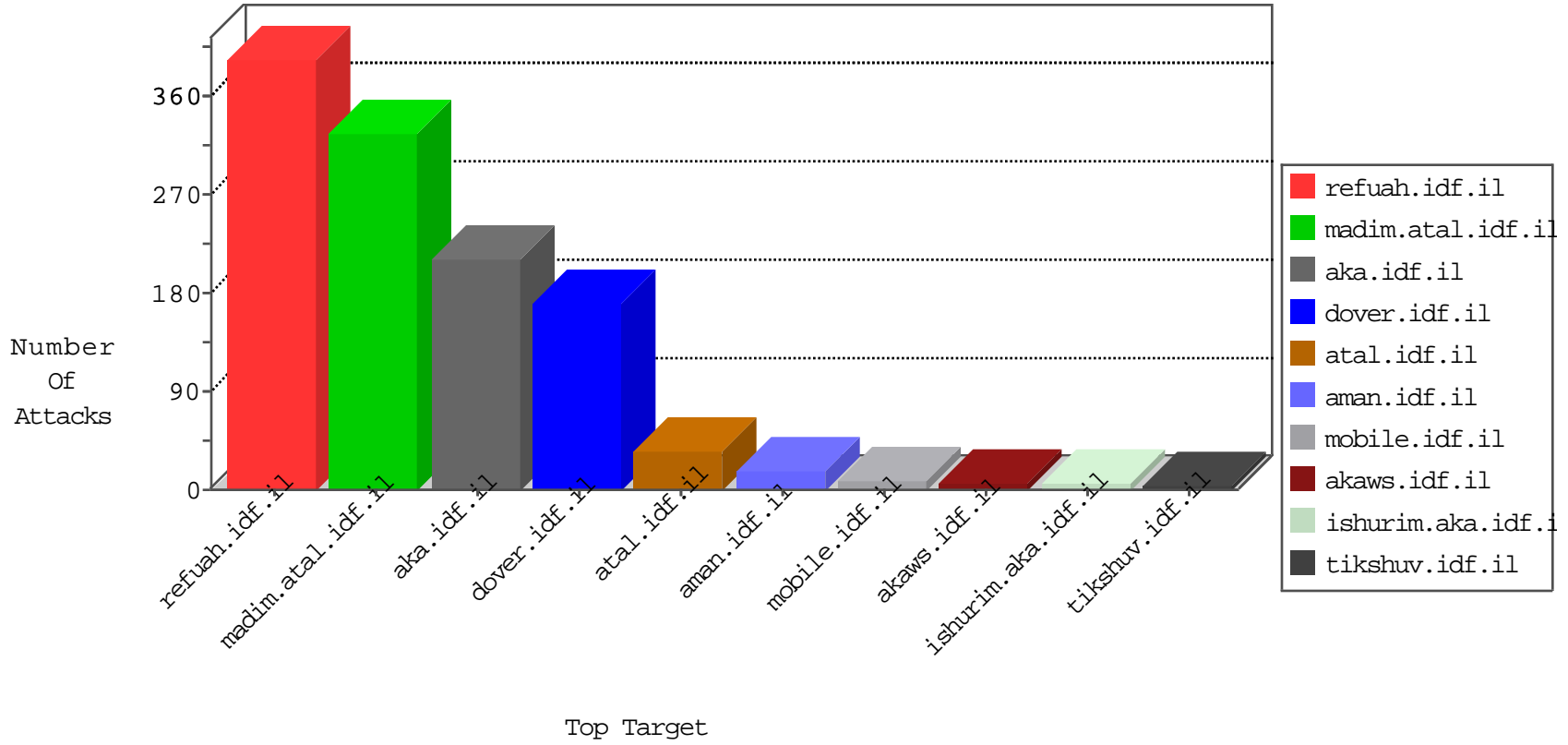


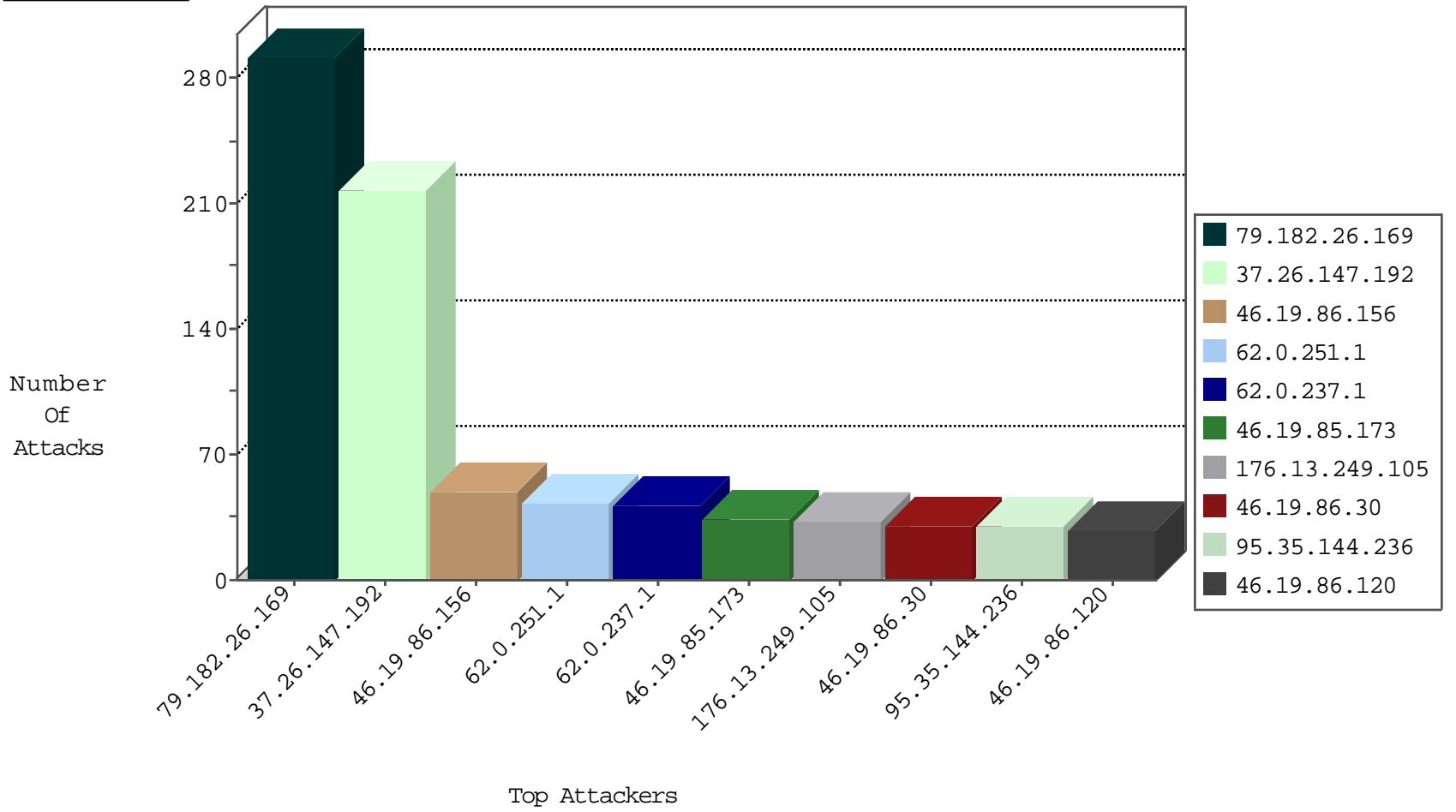
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
131.247.2.241	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
198.133.224.147	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
129.97.74.14	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
164.107.127.12	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
198.133.224.147	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.217.77.2	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.208.4.99	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
204.85.191.10	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.10.120.193	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-13-2016-08:04:09 to 09-13-2016-09:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
69.30.213.138	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3
106.38.241.105	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
79.182.32.127	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	4
46.120.122.219	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	2
81.218.245.1	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN Potential SSH Scan	1
79.182.32.127	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	1
91.224.160.106	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN Potential SSH Scan	1
79.178.4.33	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.76.30	Netherlands	himush.idf.il	ET SCAN Potential SSH Scan	1
65.60.36.203	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
190.254.135.110	147.237.77.234	Colombia	halag.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.224.160.106	147.237.72.156	Netherlands	aman.idf.il	ET SCAN Potential SSH Scan	1
5.255.90.133	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
109.226.40.40	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN Potential SSH Scan	1
94.102.52.71	147.237.77.74	Netherlands	law.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.0.33	Netherlands	idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN Potential SSH Scan	1
86.58.69.133	147.237.8.50	Slovenia	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
82.81.94.114	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN Potential SSH Scan	1
80.179.119.54	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.34	Netherlands	yochalan.idf.il	ET SCAN Potential SSH Scan	1
67.211.219.120	147.237.76.176	United States	test.ncore.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
202.65.138.2	147.237.76.198	India	e.yochalan.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.72.166	Netherlands	aka.idf.il	ET SCAN Potential SSH Scan	1
190.153.238.58	147.237.0.200	Chile	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.72.14	Netherlands	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
94.230.86.47	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN Potential SSH Scan	1
93.158.203.168	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
89.139.211.72	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.77.233	Netherlands	atal.idf.il	ET SCAN Potential SSH Scan	1
85.64.171.131	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.77.216	Netherlands	dover.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.182.26.169	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	291
62.0.251.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	43
62.0.237.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	42
46.19.86.156	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	23
46.19.85.173	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
46.19.86.156	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	18
46.19.86.120	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
46.19.85.173	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	15
46.19.85.90	Israel	147.237.76.42	refuah.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
194.177.16.3	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	12
46.19.86.120	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
46.19.86.30	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
176.13.226.95	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.30	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.156	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	7
2.53.3.127	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.128	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
80.246.139.52	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.85.128	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.179.31.174	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.68	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.30	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.53.62.227	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.86.30	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
5.102.242.132	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.68	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
195.200.205.22	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
62.0.214.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.53.150.222	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
37.26.147.192	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence		alert	4
109.73.15.149	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.147.192	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence		monitor	4
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.53.33.186	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
85.130.216.204	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.7	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.130.216.204	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
185.112.232.185	Iraq	147.237.0.35	akaws.idf.il	drop	First packet isn't SYN	drop	3
84.95.232.130	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.179.101	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
192.114.184.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
2.53.179.101	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
80.246.138.121	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
31.168.49.198	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
62.0.221.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
31.210.188.109	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.147.192	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	207
176.13.249.105	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	33
95.35.144.236	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	30
46.19.86.4	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
176.13.7.47	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
109.253.201.213	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.12.93	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.210.212	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.53.159.145	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.228.134	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
95.35.172.173	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
80.246.130.13	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ct100\$ContentPlaceholder1\$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	2
91.135.102.190	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
212.76.97.12	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
176.13.228.116	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
79.182.32.127	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.182.32.127	Block	2
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
106.38.241.105	China	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
62.219.131.159	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/gyus/faq.aspx	None	1
85.64.157.128	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.64.105	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012ources/images/innerpage/goback.gif	Block	1
207.46.13.22	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19021-he/dover.aspx ½ ç - £ ½ ç - ½ ç - •	Block	1
80.246.136.250	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 80.246.136.250 (Open Mode)	None	1
62.219.142.123	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/gyus/faq.aspx	None	1
2.53.25.34	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.138.142.48	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluum/	Block	1
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.120.122.219	Block	1
80.246.136.250	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	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
2.53.54.139	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/rss	Block	1
79.182.26.169	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/gyus/forms/downloadform.asp	Block	1
147.236.238.20	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	1
80.246.139.52	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.240.236.119	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/robots.txt	Block	1
62.128.48.84	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.asp	Block	1
157.55.39.207	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atall/contact/contact.asp	Block	1
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1