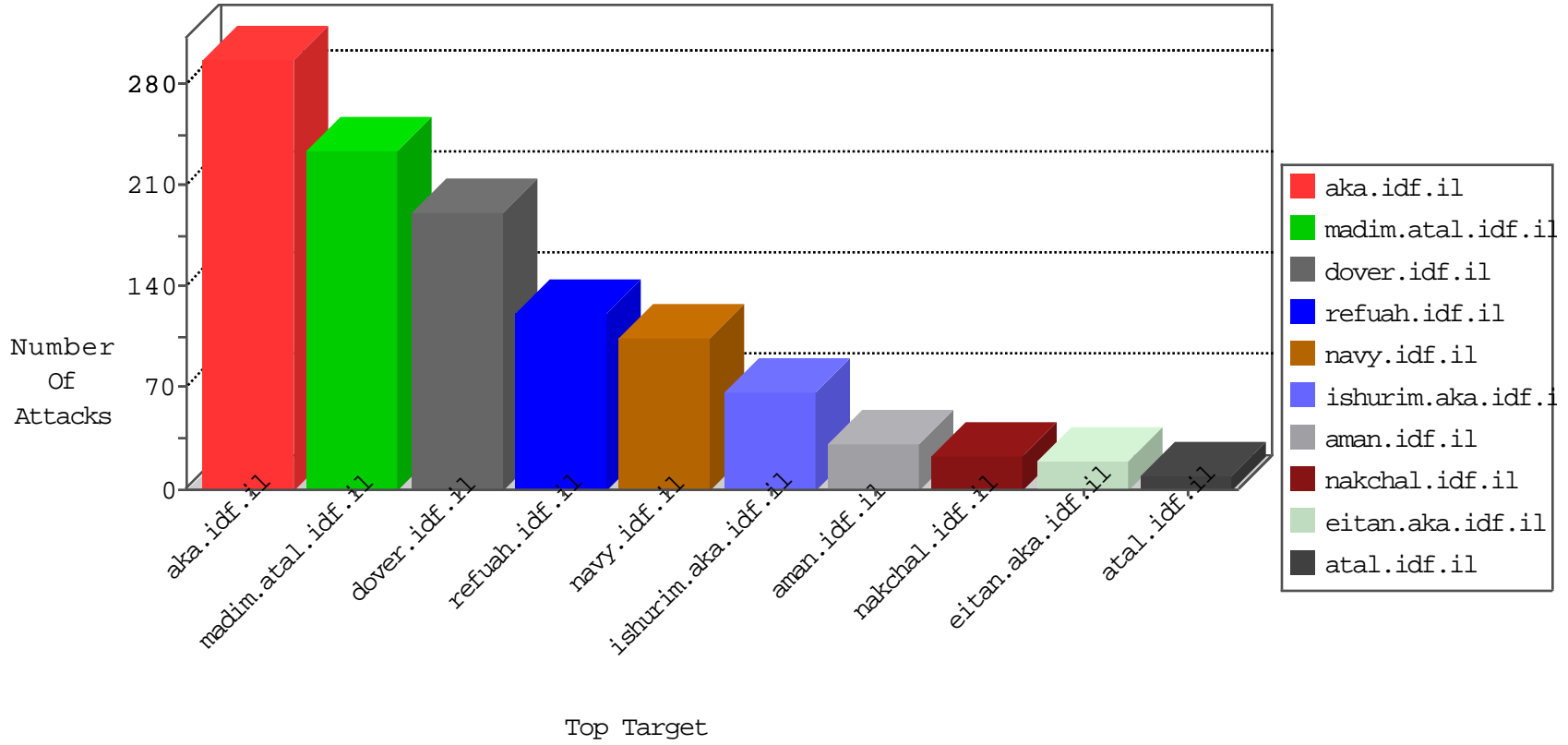


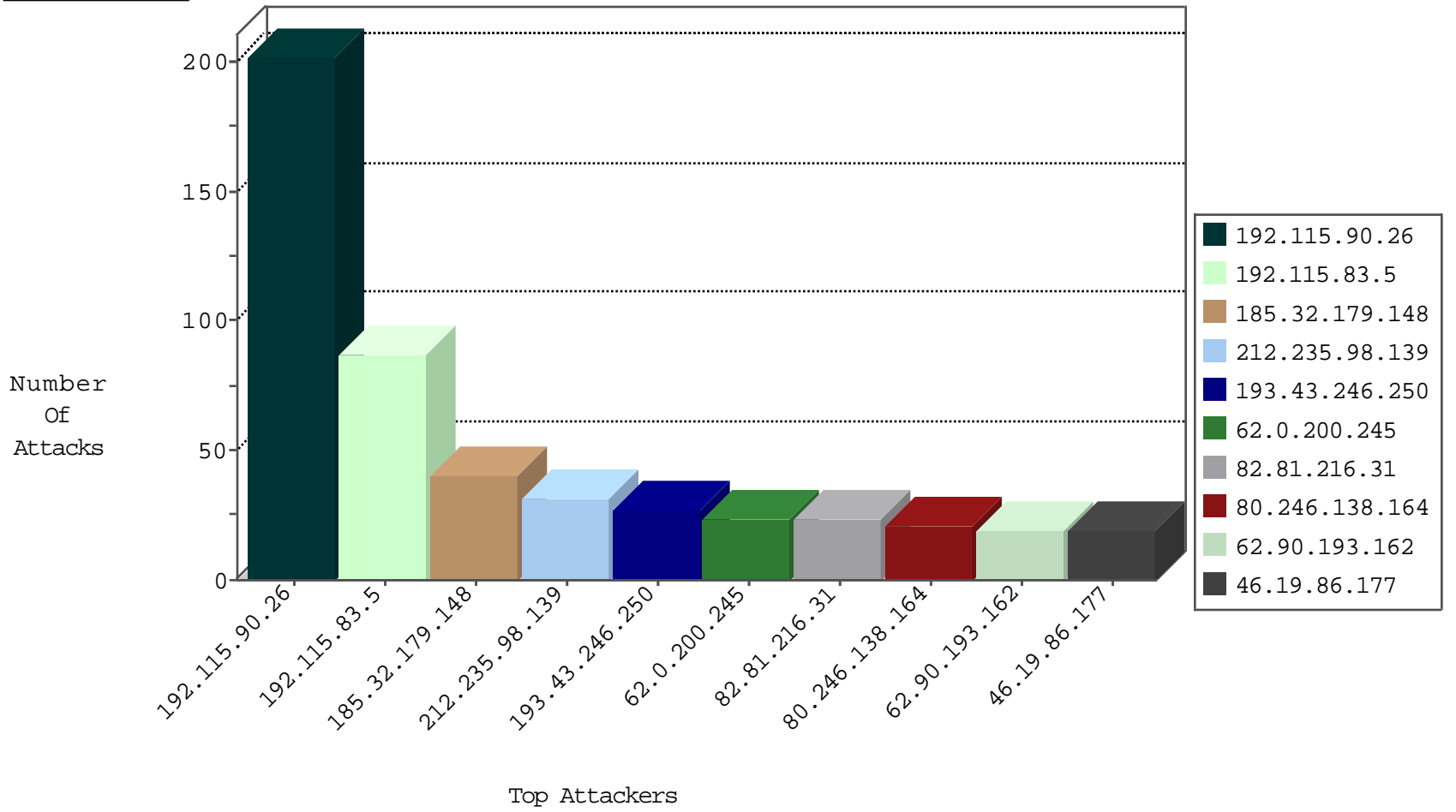
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.147.147	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2621
2.55.179.144	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	23
2.53.164.0	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
139.78.141.243	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
2.53.183.113	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
128.223.8.114	United States	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
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.194.252.8	Australia	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
192.33.90.69	Switzerland	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
208.94.63.194	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.194.252.8	Australia	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-14-2016-10:04:07 to 09-14-2016-11:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
240.0.10.13		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
37.19.115.4	147.237.77.170	Israel	maarachot.idf.il	Xenu Link Sleuth User Agent	2
108.59.253.71	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.195	147.237.77.74	Netherlands	law.idf.il	ET SCAN NMAP -sS window 1024	1
82.80.16.26	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.181.111	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.187.149	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.3.147.246	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
52.166.249.197	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.129.15	147.237.77.226	United Kingdom	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.177	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.129.15	147.237.77.176	United Kingdom	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
122.128.209.89	147.237.77.121	Korea, Republic of	e.navy.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
2.53.131.249	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.195	147.237.77.176	Netherlands	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
84.94.209.30	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.181.37.53	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.178.110.143	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.219.233.148	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.129.15	147.237.77.235	United Kingdom	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
46.121.77.31	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.129.15	147.237.77.176	United Kingdom	matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
37.26.147.197	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.129.15	147.237.76.199	United Kingdom	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
5.29.221.100	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
192.115.83.5	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	47
192.115.83.5	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	37
185.32.179.148	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	32
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
62.0.200.245	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	22
62.90.193.162	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	14
2.53.161.61	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
109.253.197.43	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	monitor	12
82.81.216.31	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
212.143.118.26	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
80.246.130.137	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
46.19.85.7	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
46.19.86.160	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
31.168.23.59	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	9
109.253.229.127	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	9
195.160.242.40	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	7
82.81.216.31	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
195.160.242.40	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
82.80.198.164	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
79.182.32.167	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
109.253.131.197	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.125	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
62.0.232.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.125	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
37.26.148.204	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
2.54.192.95	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
80.246.138.164	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.86.177	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	6
79.178.63.197	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.80.196.44	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
2.54.192.95	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.86.177	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.73	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
80.246.138.164	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.160	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
62.90.193.162	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
176.13.243.240	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.86.177	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.73	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
80.246.138.164	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
176.13.243.240	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
185.32.179.148	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
82.80.198.164	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
109.253.199.144	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
141.226.162.209	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.69	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.86.91	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
82.81.216.31	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
84.111.139.163	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.115.90.26	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	202
46.19.86.126	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
46.19.86.198	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
5.29.204.108	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	5
2.53.151.142	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
5.29.204.108	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakchal.idf.il/sip_storage/files/2/	Block	3
89.138.169.40	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
2.53.161.227	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
77.139.33.88	France	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
213.8.71.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 213.8.71.26	Block	2
37.26.148.201	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
77.138.178.241	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluum/	Block	2
212.25.126.82	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
80.179.223.31	Israel	147.237.77.176	matpash.idf.il	Distributed Unauthorized HTTP Method	Block	2
2.53.21.117	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
80.179.223.31	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 80.179.223.31	Block	2
176.13.232.71	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gius	Block	2
77.139.168.208	France	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
139.162.13.205	Singapore	147.237.77.235	sviva.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.102.9.26	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
106.186.113.132	Japan	147.237.76.86	navy.idf.il	Multiple NULL Character in Method from 106.186.113.132	Block	1
46.19.85.80	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
213.8.10.14	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	1
80.246.130.137	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
176.13.249.161	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
68.180.228.251	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1073-he/nakhal.aspx	Block	1
132.68.204.108	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
84.95.251.240	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.180.55.205	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
204.79.180.166	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/miluum/templates/inner.asp	Block	1
157.55.39.196	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/rabanut/www.rabanut-downloads.webs.com	Block	1
66.249.64.124	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catId\u003d59116\u0026pageNum\u003d3 in www.aka.idf.il/edim/yoman/yoman.asp	None	1
106.186.113.132	Japan	147.237.76.86	navy.idf.il	NULL Character in Method	Block	1
46.19.86.1	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
2.53.155.45	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
80.246.133.213	Israel	147.237.76.42	refuah.idf.il	Suspicious Response Code	Block	1
77.125.92.236	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-17802-he/dover.aspx	Block	1
46.121.253.55	Israel	147.237.72.166	aka.idf.il	Unknown Parameter x in www.aka.idf.il/main/sachar/payslips.aspx	None	1
132.70.66.9	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized HTTP Method	Block	1
79.182.32.167	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
210.174.30.231	Japan	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/giyus/	Block	1
176.13.20.15	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
66.249.65.142	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/.well-known/apple-app-site-association	Block	1
46.19.86.64	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.66.48.102	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 127.0.0.1/callback.json	Block	1
80.246.137.70	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
194.90.66.9	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
54.81.158.232	United States	147.237.72.156	aman.idf.il	Unauthorized Method HEAD for 147.237.72.156/	Block	1
132.70.66.9	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/2/	Block	1