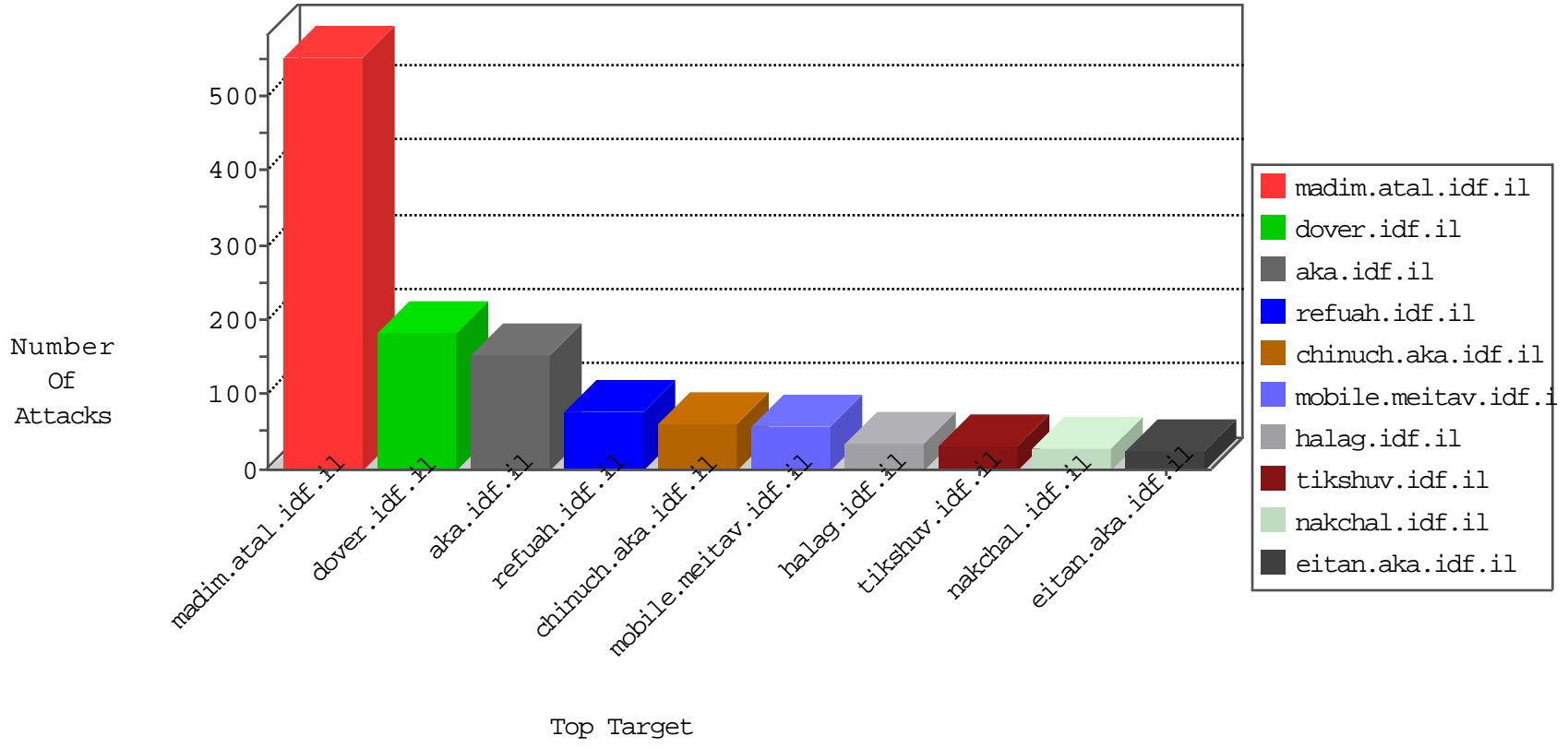


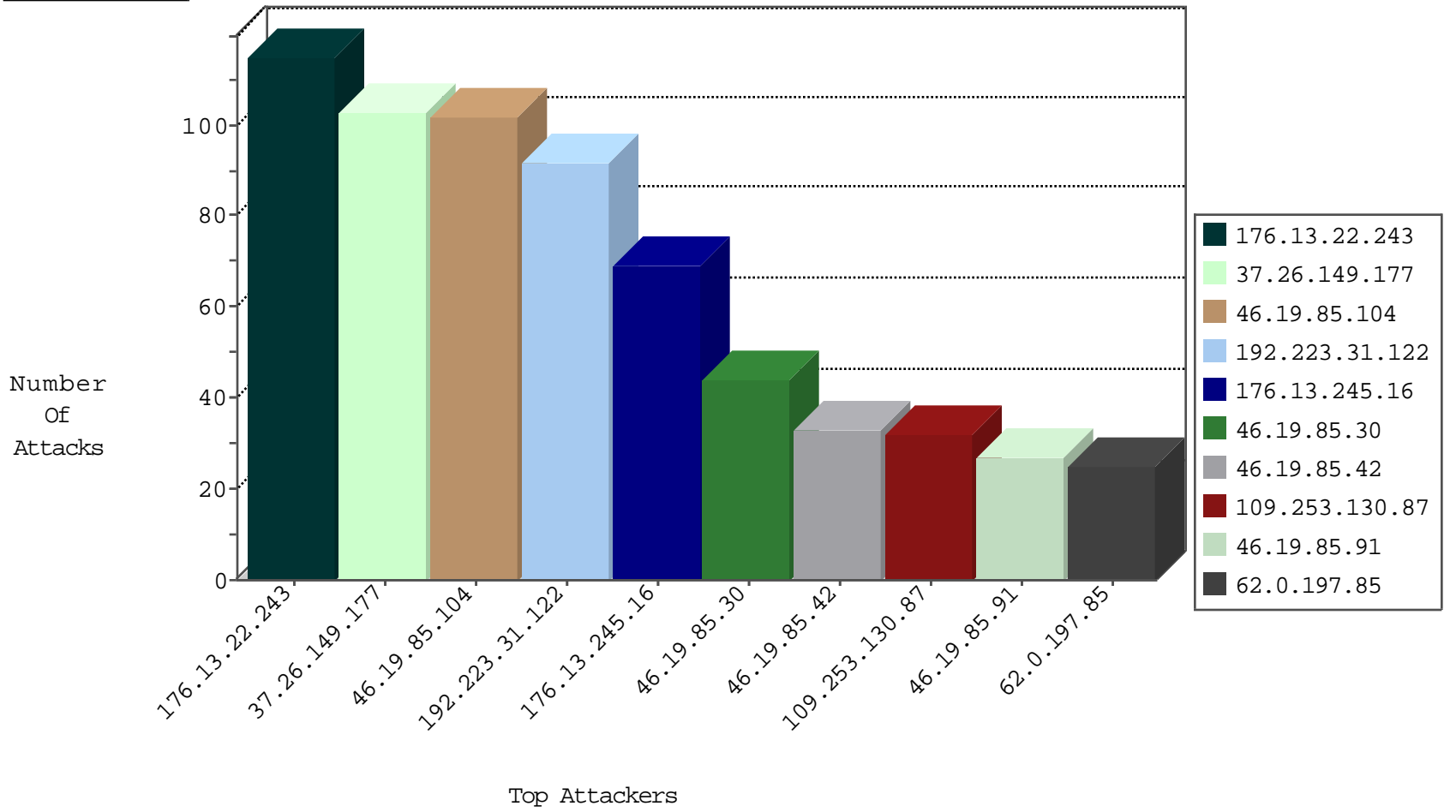
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.138.52.97	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
62.90.162.85	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
209.126.122.47	United States	147.237.76.148	ggcenter.aka.idf.il	Black List	drop	1
66.249.83.221	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
93.174.94.235	Netherlands	147.237.76.86	navy.idf.il	Black List	drop	1
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
211.149.240.243	China	147.237.76.199	e.nakchal.idf.il	Black List	drop	1
208.67.1.248	United States	147.237.76.31	nakchal.idf.il	Black List	drop	1
78.129.171.175	United Kingdom	147.237.76.177	ncore.idf.il	Black List	drop	1
209.126.122.47	United States	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1
66.249.83.219	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
78.129.171.175	United Kingdom	147.237.76.199	e.nakchal.idf.il	Black List	drop	1
46.19.86.144	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.210.225.135	France	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	2
193.111.140.106	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	1
85.14.244.113	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
62.210.225.135	147.237.77.74	France	law.idf.il	SQL Injection - Select From	4
77.126.5.4	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
76.72.249.221	147.237.76.42	Puerto Rico	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
212.179.62.20	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.0.41.2	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.115.90.150	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.245	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.23.175.84	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
45.63.28.189	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
109.64.152.17	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.154.34.238	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.138.118.189	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.139.163.107	147.237.72.166	France	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
76.72.249.221	147.237.76.44	Puerto Rico	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
62.219.136.214	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.85.210	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.90.163.155	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.143.73.210	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.221	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.91	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
45.63.28.189	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
109.65.4.134	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.154.81.40	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.172.138.181	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.80.119.226	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
62.0.197.85	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	25
212.235.98.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
89.138.173.41	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	24
46.19.85.254	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	18
192.223.31.122	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
192.223.31.122	United States	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
207.232.18.46	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
192.223.31.122	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	14
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
192.223.31.122	United States	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	SYN retransmit with different sequence	alert	12
192.223.31.122	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	11
109.253.209.174	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	10
192.223.31.122	United States	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	SYN retransmit with different sequence	monitor	10
176.13.245.16	Israel	147.237.0.19	madim.atal.idf.il	drop	First packet isn't SYN	drop	9
2.53.11.109	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
81.218.136.207	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
79.180.30.193	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.128	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.85.91	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.86.90	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
46.19.85.91	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.136	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.169	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.128	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.177.14.220	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.19.85.91	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.253.133.189	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.4	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.91	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.146.160	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.135	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.135	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
158.85.253.245	United States	147.237.77.233	atal.idf.il	drop	SAM rule	drop	5
46.19.85.135	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.227	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
176.13.251.143	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
84.111.21.114	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.202	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.86.170	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.254	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.148.158	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
46.19.85.202	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.128	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.86.185	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
84.94.140.112	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
2.53.176.72	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
199.30.16.160	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
192.223.31.122	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
31.168.96.254	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
62.90.162.85	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.22.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	115
37.26.149.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	103
46.19.85.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	98
176.13.245.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	56
46.19.85.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	44
46.19.85.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
109.253.130.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	28
46.19.85.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
46.19.86.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
2.53.174.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
2.53.19.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
212.235.18.146	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
109.253.133.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.143.115	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.140.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.146.101	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
79.180.30.193	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/homepage/homepage.aspx	Block	2
84.95.208.20	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
176.13.249.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
10.161.50.80		147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/exampcert/	Block	2
87.69.192.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.136.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.116.79.169	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
2.53.55.150	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
176.13.237.160	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
79.177.36.46	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	2
217.194.202.218	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gius	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
169.229.3.91	United States	147.237.76.200	eitan.aka.idf.il	Illegal Byte Code Character in Method	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/iturim/asp/wars.asp	Block	1
66.102.9.6	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
109.173.68.206	Russian Federation	147.237.76.42	refuah.idf.il	Unauthorized Method POST for 147.237.76.42/894-he/refuah.aspx	Block	1
46.19.85.104	Israel	147.237.77.216	dover.idf.il	Malformed URL (khtml,	Block	1
212.179.21.194	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	Unknown HTTP Request Method ëcû=¼" [[#8]]-Lÿ,?[[#20]]œ[[#4]]Ây`[[#31]]èiõkî•i...k°++}çö{öpæ[[#5]]]""[[#27]]&wY+úF:v">[[#6]]ôN°'í\µé[[#22]]ím in URL	Block	1
66.249.66.18	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/mobile/	Block	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Abnormally Long Request method	Block	1
46.19.86.181	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
217.194.203.125	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
46.19.85.91	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/960.css	Block	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	Illegal Byte Code Character in Method	Block	1
77.138.202.110	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/kamlar/	Block	1
66.102.9.24	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
46.19.85.104	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method 600.1.4 in URL (khtml,	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/piwik.php	Block	1
80.178.220.41	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/recruitlane.aspx	Block	1
169.229.3.91	United States	147.237.77.234	halag.idf.il	Illegal Byte Code Character in Method	Block	1