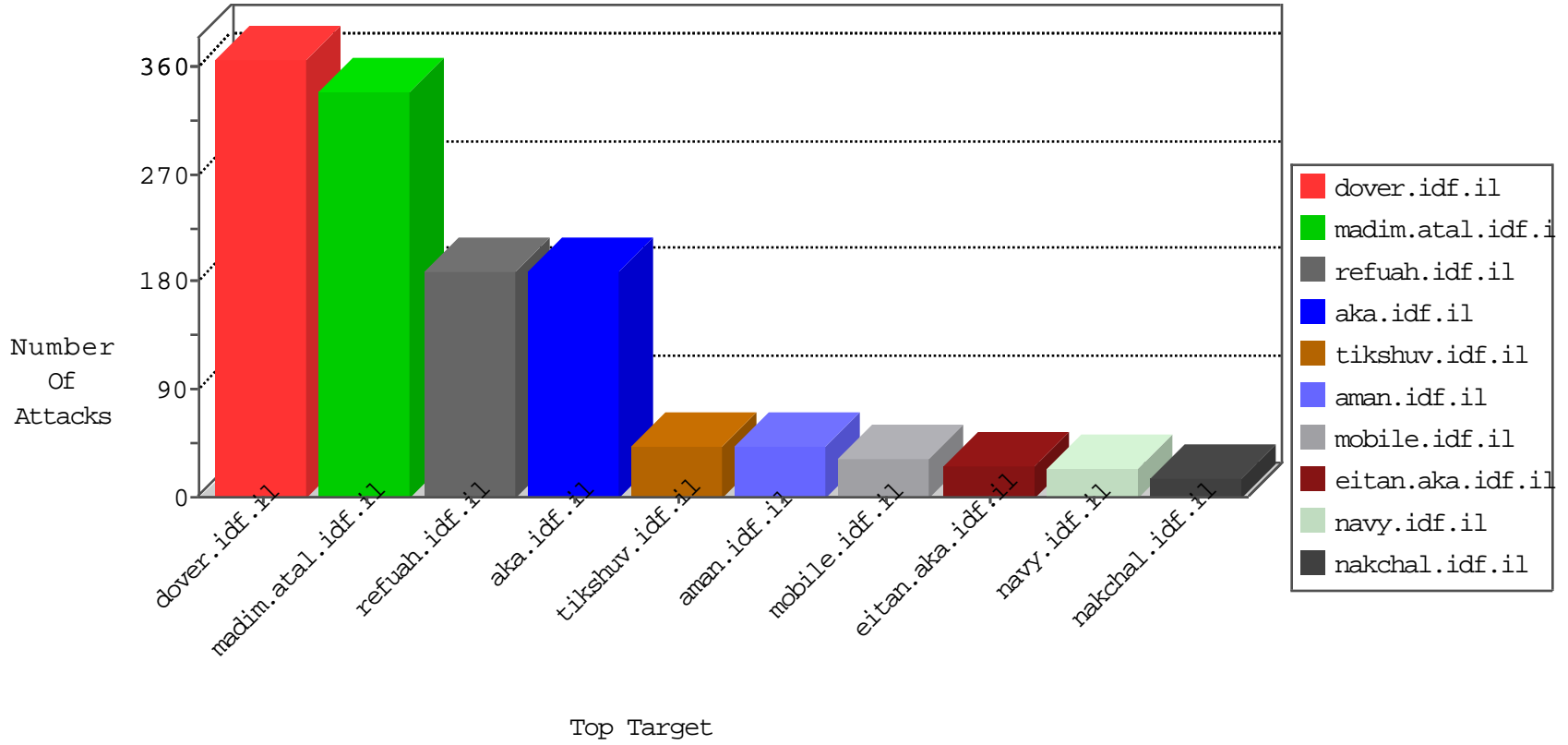


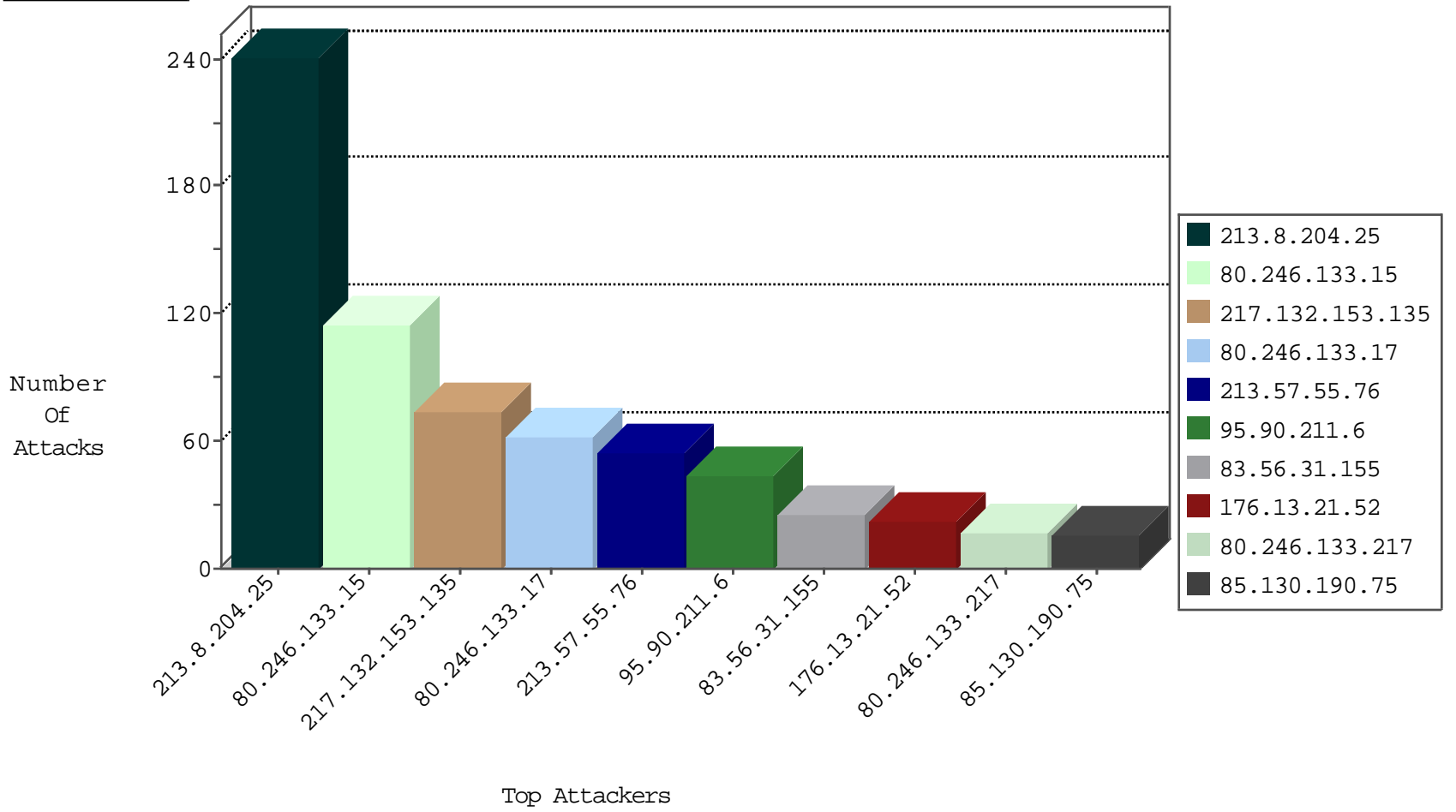
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.250.76.250	Israel	147.237.72.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
193.1.13.14	Ireland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
193.166.167.4	Finland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
153.90.1.34	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
194.254.215.12	France	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
141.22.213.34	Germany	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
195.113.161.83	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
164.107.127.12	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
143.225.229.236	Italy	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.97.74.14	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.114	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.206.158.138	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.8.126.111	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
46.19.86.178	Israel	147.237.72.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
165.242.90.128	Japan	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
131.247.2.241	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
128.208.4.99	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
194.29.178.14	Poland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
147.83.29.234	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
46.116.8.98	Israel	147.237.72.216	dover.idf.il	Black List	drop	1
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
192.91.235.230	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
139.78.141.243	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.208.4.197	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	5
5.22.134.94	147.237.72.166	Israel	aka.idf.il	GPL SCAN myscan	3
5.22.134.94	147.237.72.166	Israel	aka.idf.il	INDICATOR-SCAN myscan	3
103.207.37.81	147.237.77.176	Vietnam	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
93.158.203.147	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
202.155.58.28	147.237.76.86	Indonesia	navy.idf.il	ET SCAN NMAP -sS window 1024	1
91.209.70.158	147.237.0.15	Russian Federation	kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
202.155.58.28	147.237.72.14	Indonesia	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
66.249.66.131	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
200.195.135.82	147.237.77.212	Brazil	e.dover.idf.il	ET SCAN NMAP -sS window 3072	1
46.10.223.252	147.237.77.74	Bulgaria	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
200.195.135.82	147.237.77.212	Brazil	e.dover.idf.il	ET SCAN NMAP -f -sS	1
142.54.191.210	147.237.76.148	United States	ggcenter.aka.idf.il	ET SCAN NMAP -sS window 3072	1
141.226.242.141	147.237.77.226	Israel	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	1
109.60.153.178	147.237.77.212	Russian Federation	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
93.158.203.147	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
91.209.70.158	147.237.8.14	Russian Federation	e.orchot.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
202.155.58.28	147.237.76.38	Indonesia	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
80.246.130.231	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDoS attack	1
202.155.58.28	147.237.8.28	Indonesia	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
200.195.135.82	147.237.77.212	Brazil	e.dover.idf.il	ET SCAN NMAP -sS window 2048	1
198.20.69.98	147.237.76.199	United States	e.nakchal.idf.il	ET DROP Dshield Block Listed Source	1
142.54.191.210	147.237.76.148	United States	ggcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
115.239.76.85	147.237.76.176	China	test.ncore.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
80.246.133.15	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	114
80.246.133.17	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	60
83.56.31.155	Spain	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
95.90.211.6	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	23
66.102.6.117	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
95.90.211.6	Germany	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
192.114.105.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
31.210.186.27	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
213.57.55.76	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
2.53.164.19	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
46.19.86.68	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	9
188.72.103.229	United Arab Emirates	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
212.179.104.17	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
176.13.21.52	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	9
2.53.145.75	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.147	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
95.90.211.6	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	8
176.13.21.52	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
45.74.1.195	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
2.53.45.221	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
79.176.57.245	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
84.229.8.130	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.147	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.85.47	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
85.130.190.75	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.125	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
85.130.190.75	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
5.28.158.241	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.55.76	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.85.47	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
213.57.55.76	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
213.57.55.76	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.102.195.18	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
213.57.55.76	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
213.57.55.76	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
156.196.193.153	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
212.179.104.17	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.85.82	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
176.13.21.52	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
213.57.55.76	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
213.57.55.76	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
84.108.33.171	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
98.210.201.182	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
176.13.225.190	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
100.92.222.32		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
109.253.200.133	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.221	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
37.142.201.138	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.8.204.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	239
217.132.153.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	74
80.246.133.217	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 80.246.133.217	Block	17
2.55.7.250	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation RepeatPassword in mobile.idf.il/sachar/changepassword	Block	12
79.180.99.76	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authentication/service.asmx/getauthuser	Block	6
2.53.49.15	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	6
2.53.22.216	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.108.175.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.139.96.159	France	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
109.65.29.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.53.50.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.147.253	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.116.45.101	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
2.53.159.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.137.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.53.38.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.139.59.145	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/pniot.aspx	Block	2
108.55.218.71	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	2
46.19.86.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.124.23.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.28.140.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.69.119	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
46.19.86.28	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
93.158.152.52	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17082-en/dover.aspx,	Block	1
77.126.1.237	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/5/70995.pdf	Block	1
159.220.74.2	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/patzar/news/default.asp	Block	1
66.249.64.137	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/.well-known/assetlinks.json	Block	1
94.15.27.49	United Kingdom	147.237.76.86	navy.idf.il	Distributed NULL Character in Method	Block	1
85.130.141.102	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
5.28.158.241	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.75.172	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
94.15.27.49	United Kingdom	147.237.76.86	navy.idf.il	Distributed Illegal Byte Code Character in Header Name	Block	1
77.138.11.46	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	1
176.13.232.204	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
94.15.27.49	United Kingdom	147.237.76.86	navy.idf.il	Distributed Unknown HTTP Request Method	Block	1
66.249.65.52	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.52	Block	1
85.130.141.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
31.210.186.27	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized Method POST for www.eitan.aka.idf.il/1093-he/eitan.aspx	None	1
79.183.92.53	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	1
157.55.39.36	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1
66.249.75.176	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/894-he/atal.aspx	Block	1
66.102.9.5	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
94.15.27.49	United Kingdom	147.237.76.86	navy.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
80.246.138.6	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.138.68.87	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/giyus/kadatz/	Block	1
207.232.21.105	Israel	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to e.lc4.gov.il/	Block	1
94.15.27.49	United Kingdom	147.237.76.86	navy.idf.il	Illegal Byte Code Character in Header Value	Block	1
66.249.65.52	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/.well-known/apple-app-site-association	Block	1
89.139.136.67	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/requestpayslipexplanation.aspx	None	1
31.210.186.27	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter SearchText in www.eitan.aka.idf.il/938-he/eitan.aspx	None	1