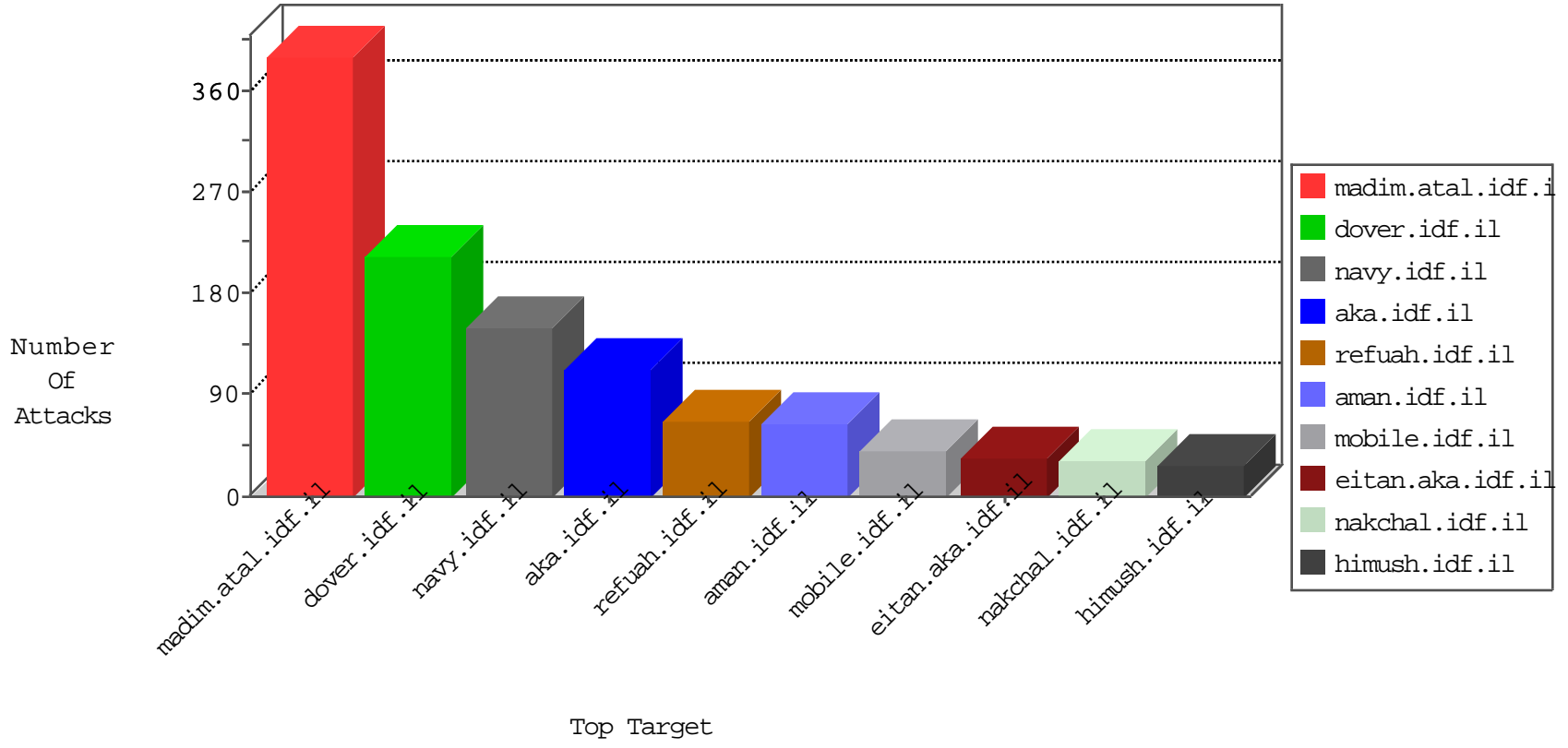


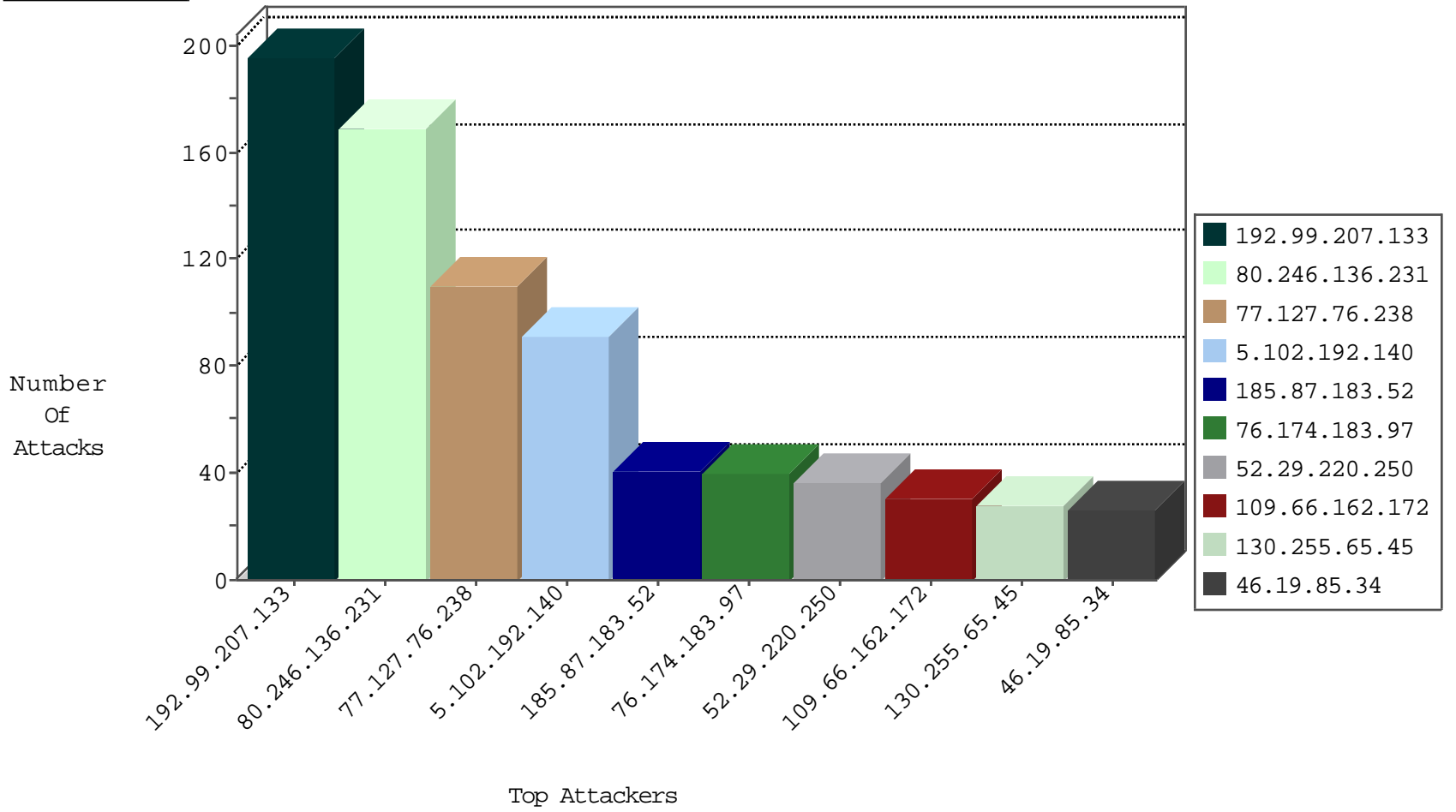
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.67.228.32	Israel	147.237.72.166	aka.idf.il	Black List	drop	5
89.163.242.39	Germany	147.237.77.227	e.hamaz.idf.il	JIM_Purple_Con_Limit_Tcp	drop	1
104.232.66.18	United States	147.237.76.176	test.ncore.idf.il	JIM_Purple_Con_Limit_Http	drop	1
89.163.242.39	Germany	147.237.77.235	sviva.idf.il	Frk_Purple_Con_Limit_Tcp	drop	1
89.45.10.243	Romania	147.237.76.30	hinush.idf.il	Black List	drop	1
104.232.66.18	United States	147.237.72.14	dover.idf.il(old)	JIM_Purple_Con_Limit_Http	drop	1
208.67.1.215	United States	147.237.76.42	refuah.idf.il	Black List	drop	1
89.163.242.39	Germany	147.237.72.166	aka.idf.il	Frk_Purple_Con_Limit_Tcp	drop	1
104.232.66.18	United States	147.237.72.14	dover.idf.il(old)	JIM_Purple_Con_Limit_Tcp	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
69.30.198.242	United States	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	6
69.30.198.242	United States	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	2
69.30.198.242	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
69.30.198.242	United States	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	2
199.58.86.206	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	1
94.102.60.21	Netherlands	147.237.77.216	dover.idf.il	10767: HTTP: Acunetix Security Scanner	Block	1
123.126.113.18	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1
151.80.31.159	France	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
91.121.143.113	147.237.77.74	France	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
91.224.160.106	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN Potential SSH Scan	1
79.181.136.76	147.237.72.156	Israel	aman.idf.il	ET SCAN NMAP -sA (2)	1
180.97.106.37	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
66.249.64.115	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
163.172.129.15	147.237.77.243	United Kingdom	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.200.137	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
163.172.129.15	147.237.76.201	United Kingdom	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.200.137	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
108.12.246.131	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
91.224.160.106	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
80.246.140.170	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
180.97.106.161	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
72.69.113.91	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 3072	1
180.97.106.37	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.76.34	China	yochalan.idf.il	ET SCAN Potential SSH Scan	1
163.172.129.15	147.237.76.201	United Kingdom	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
58.218.200.137	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
109.60.153.178	147.237.77.212	Russian Federation	e.dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.193.246.248	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 3072	1
91.224.160.106	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
76.174.183.97	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	38
192.99.207.133	Canada	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	25
192.99.207.133	Canada	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	25
192.99.207.133	Canada	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	25
192.99.207.133	Canada	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	25
130.255.65.45	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
192.99.207.133	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	24
192.99.207.133	Canada	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	24
192.99.207.133	Canada	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	24
192.99.207.133	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	24
82.145.223.103	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	21
2.53.165.144	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
87.69.79.91	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
185.87.183.52	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.34	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
185.87.183.52	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	9
109.66.162.172	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	9
87.69.79.91	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
66.87.76.153	United States	147.237.77.216	dover.idf.il	SYN Attack		monitor	9
185.87.183.52	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
185.87.183.52	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	8
46.19.85.34	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
31.13.80.36	Ireland	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
46.19.86.22	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.184	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.246.95	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.59.166	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
176.13.251.202	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.86.22	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
185.87.183.52	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
46.19.85.184	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.66.162.172	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
109.66.162.172	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.85.34	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
109.66.162.172	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
37.26.146.190	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.86.237	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
185.87.183.51	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
77.126.37.246	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
185.87.183.59	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	4
46.19.86.156	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
185.3.147.190	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.90	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
185.87.183.59	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
52.53.148.128	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
109.253.230.219	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
176.13.228.123	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
54.206.123.102	Australia	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
2.53.159.252	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
185.87.183.59	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.136.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	167
77.127.76.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	110
5.102.192.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	91
188.120.154.90	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	6
77.138.22.23	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.138.22.23	Block	4
82.166.69.222	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 82.166.69.222	Block	4
66.249.76.52	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	3
82.166.69.222	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	3
46.19.85.151	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.45.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.199.13	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
64.116.185.6	Panama	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	2
2.53.165.144	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
80.178.19.104	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 80.178.19.104	Block	2
109.253.221.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.29.221.220	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
77.138.22.23	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/ishurim/main/	Block	2
87.204.157.42	Poland	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.19.86.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
217.132.153.238	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
77.138.56.243	France	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/favicon.ico	Block	1
194.153.113.13	Germany	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/robots.txt	Block	1
95.110.194.252	Italy	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
185.120.125.26	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation asperrorpath in www.idf.il/error.htm	Block	1
66.249.64.224	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/365-he/patzar.aspx	Block	1
95.110.194.252	Italy	147.237.77.243	mobile.idf.il	PHP Attempt	Block	1
87.71.47.106	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https://www.aman.idf.il/	Block	1
207.46.13.57	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.76.53	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding /BPv^_V*oD^ in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
95.110.194.252	Italy	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
82.235.9.18	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
66.249.64.227	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1495-he/atal.aspx	Block	1
109.65.77.202	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	1
80.178.19.104	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/home/default.aspx=1	Block	1
2.53.38.118	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
212.143.47.164	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/https://www.aman.idf.il/	Block	1
157.55.39.74	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/edim/requests/	Block	1
66.249.79.130	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/sip_storage/files/8/1558.jpg	Block	1
66.249.64.12	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
95.110.194.252	Italy	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 95.110.194.252	Block	1
82.238.223.99	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
194.153.113.13	Germany	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	1
66.249.76.42	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/sip_storage/files/5/1555.jpg	Block	1
109.67.234.150	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
93.173.16.7	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
46.19.86.122	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
212.199.144.158	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.13.246.95	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1