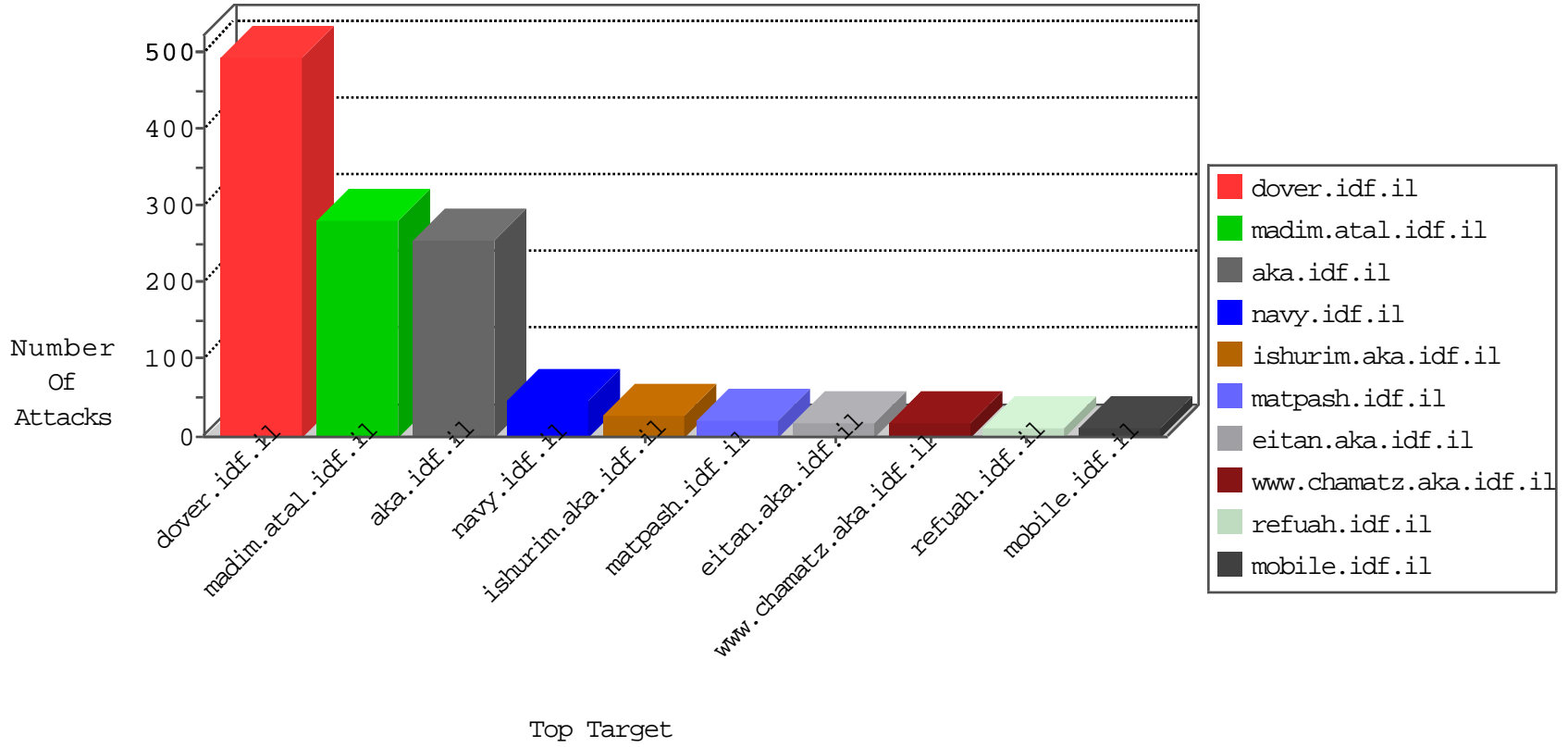


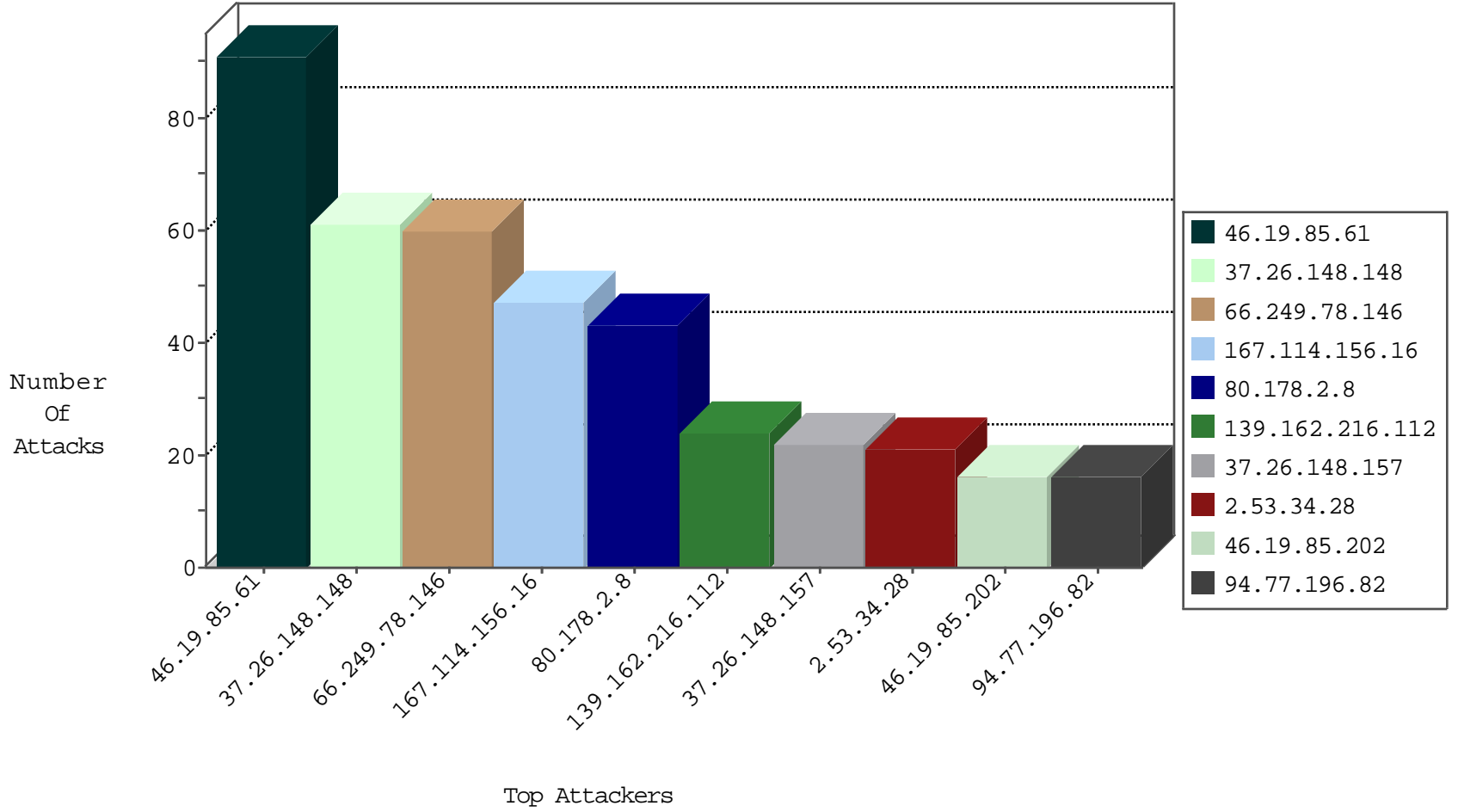
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	2996
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	865
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
177.66.108.237	Brazil	147.237.72.166	aka.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
94.102.49.116	Netherlands	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
123.59.59.52	China	147.237.77.233	atal.idf.il	block-sp-traf1	drop	1
153.196.93.127	Japan	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
185.103.252.201	Russian Federation	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
14.29.32.135	China	147.237.76.39	mobile.meitav.idf.il	JLM_Under_Attack_Con_Tcp	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
64.74.197.103	United States	147.237.72.167	ishurim.aka.idf.i	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1
93.190.69.10	Germany	147.237.76.147	chinuch.aka.idf.i	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
79.178.106.68	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sA (2)	2
193.201.227.84	147.237.0.35	Ukraine	akaws.idf.il	ET SCAN Potential SSH Scan	1
193.36.35.241	147.237.0.15	Russian Federation	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
122.3.199.144	147.237.76.38	Philippines	e.e.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
98.119.105.221	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 4096	1
66.240.213.93	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1
52.90.202.117	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 4096	1
52.90.202.117	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -f -sS	1
193.201.227.84	147.237.0.15	Ukraine	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
163.172.140.23	147.237.77.178	United Kingdom	e.matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
109.67.109.190	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
64.74.197.103	147.237.72.167	United States	ishurim.aka.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	1
52.90.202.117	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 2048	1
203.86.29.220	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN NMAP -sS window 3072	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
37.26.148.157	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
149.78.77.0	United States	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
192.0.83.67	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
188.244.36.217	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	14
79.183.119.244	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.181.26.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.99.82	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.115	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
73.44.179.61	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
37.26.146.138	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
87.203.102.200	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
40.77.167.31	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.15	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
40.77.167.57	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
66.249.93.180	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
128.242.249.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
207.46.13.49	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
88.254.109.108	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.41	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.253.218.56	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.102.213.180	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
212.150.128.10	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.41	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
207.46.13.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.22	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
66.249.78.12	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.150.128.10	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
217.132.78.189	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.15	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
66.87.142.238	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
2.53.34.28	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
37.26.146.227	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
192.99.232.7	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
69.115.172.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.199.108.62	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.202	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
185.3.147.159	Israel	147.237.72.166	aka.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
46.19.85.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	91
37.26.148.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	57
80.178.2.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
37.26.148.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
37.26.148.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
185.32.179.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
37.26.148.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
84.108.129.210	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.108.129.210	Block	12
37.26.148.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
193.43.246.250	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
84.108.52.34	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
193.43.245.250	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
79.177.242.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.33.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.28.167.155	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/gyus/general.aspx	Block	1
157.55.2.181	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/	Block	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	Multiple Abnormally Long Request from 169.229.3.91	Block	1
94.199.151.22	United Kingdom	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
74.82.47.2	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
185.32.179.223	Israel	147.237.0.19	madim.atal.idf.il	Untraceable SSL Sessions: Open Mode	None	1
62.0.114.185	Israel	147.237.76.86	navy.idf.il	Cookie Tampering on cookie __atrfis: Expected ab/	None	1
169.229.3.91	United States	147.237.72.167	ishurim.aka.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
84.108.129.210	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakchal.idf.il/templates/news/mobile	Block	1
66.249.64.235	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
105.109.78.254	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
188.120.148.50	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqquantity.aspx	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/gyus/general.aspx	Block	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	Abnormally Long Request method	Block	1
66.249.66.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/3481.jpg	Block	1
199.30.24.179	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unknown HTTP Request Method from 169.229.3.91	Block	1
109.253.218.56	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.178.93.153	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/589-he/patzar.aspx=	Block	1
188.120.148.155	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in Method	Block	1
89.138.215.245	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
66.249.66.125	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/6/3426.jpg	Block	1
203.133.169.231	Korea, Republic of	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
182.57.251.16	India	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1038-en/dover.aspx/	Block	1
157.55.2.129	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
192.116.165.226	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
93.172.136.76	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1