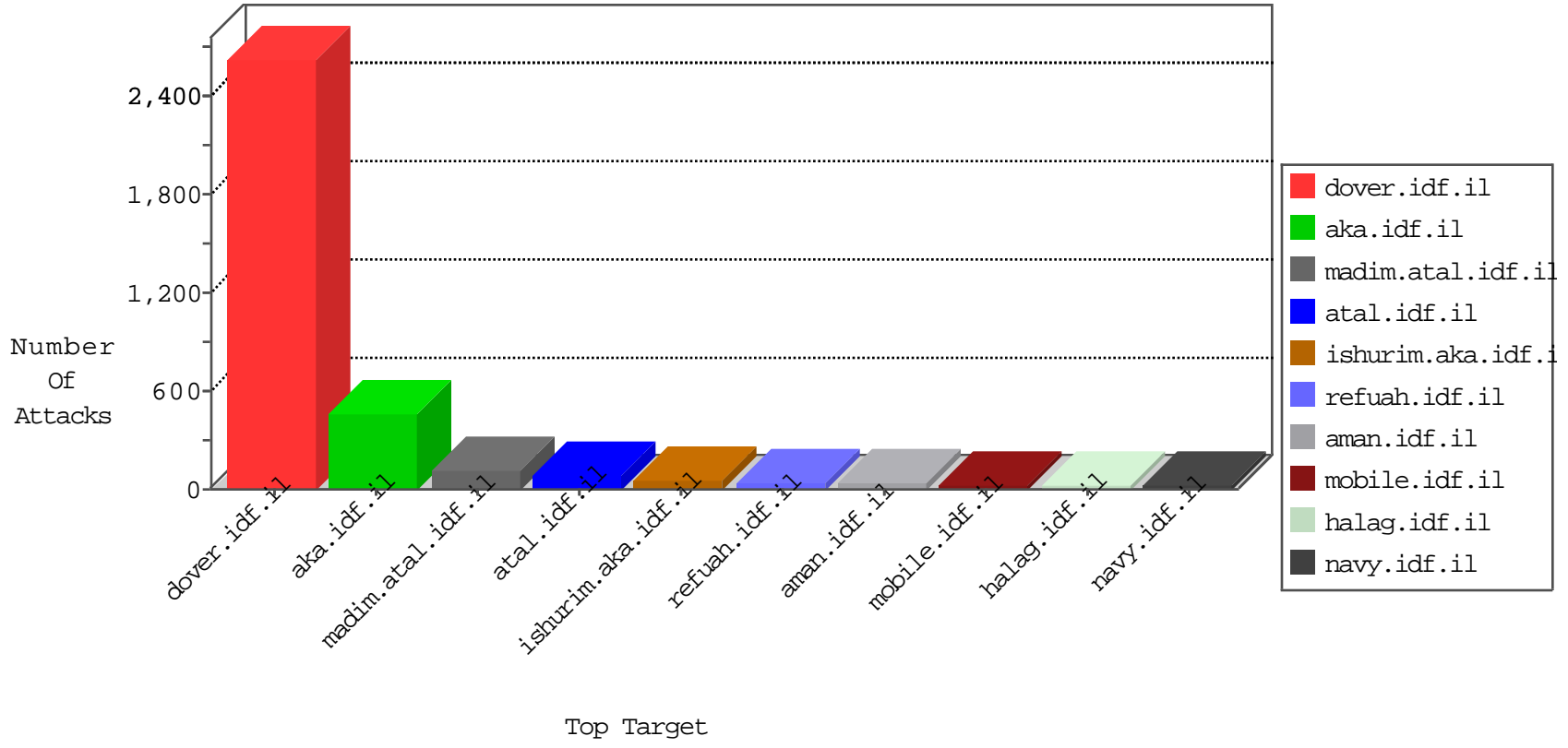


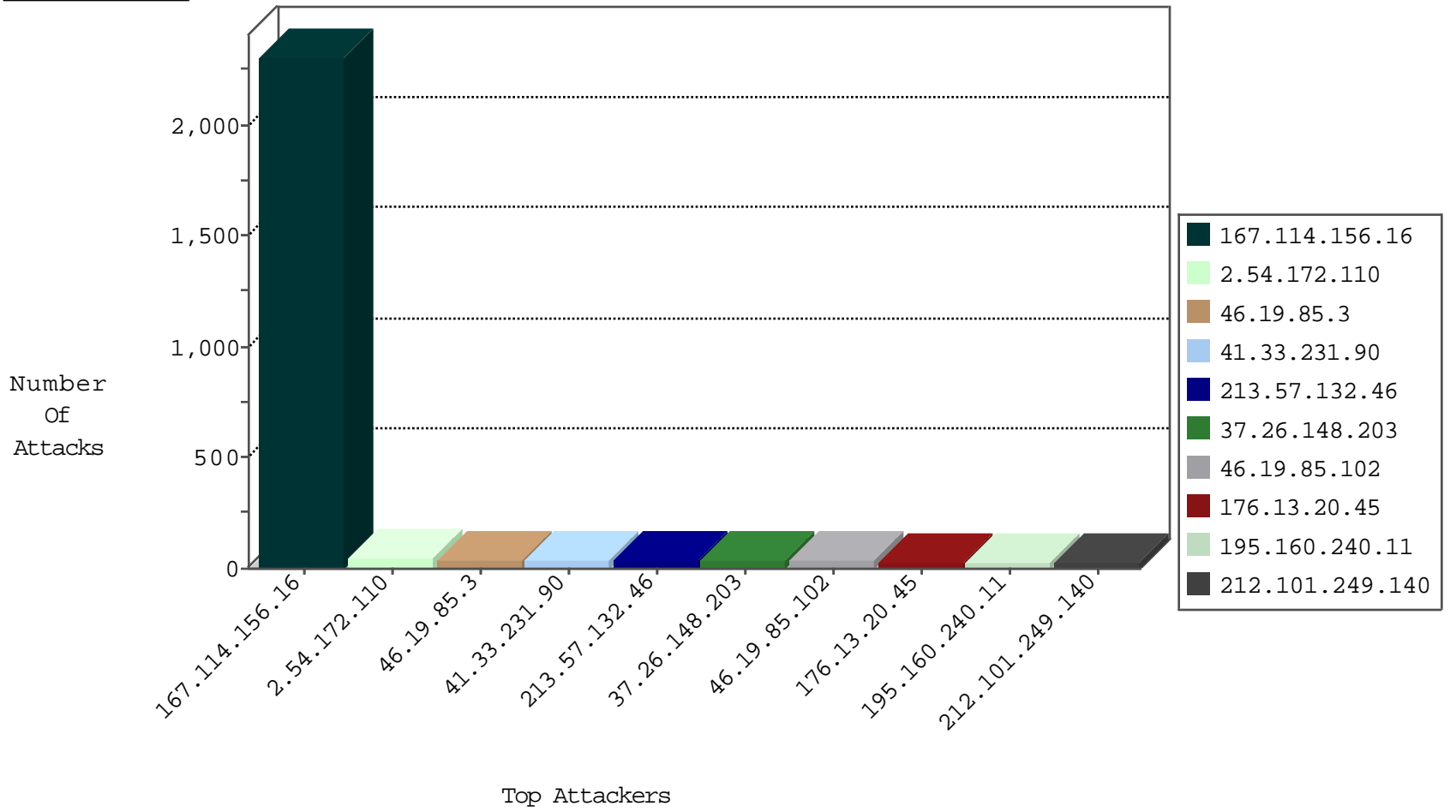
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3106
118.222.115.189	Korea, Republic of	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
81.218.56.125	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	1
85.25.217.16	Germany	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
85.25.217.16	Germany	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
27.5.180.194	India	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
79.177.201.16	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sS window 4096	2
45.79.70.23	147.237.0.200		m4u.idf.il	ET SCAN NMAP -sS window 1024	1
2.54.56.113	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
176.13.1.98	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.179.102.39	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.177.53.17	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.219.237.147	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.77.233	China	atal.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.187	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.149.137	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
178.20.72.19	147.237.0.200	Italy	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
84.109.235.122	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.125.133.180	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
61.182.170.38	147.237.0.16	China	ny-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential SSH Scan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
2.54.172.110	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	33
46.19.85.102	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	31
195.160.240.11	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	27
46.19.85.219	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	22
199.30.24.77	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
185.89.217.225		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
213.57.132.46	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	11
213.57.132.46	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
46.19.85.3	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
46.19.86.121	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
213.57.132.46	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
46.19.85.3	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
212.101.249.140	Lebanon	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
212.101.249.140	Lebanon	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
84.94.103.248	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
79.180.61.136	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.42	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
2.52.185.186	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
37.26.148.155	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
62.0.200.166	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
2.54.6.208	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.85.174	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
176.12.140.183	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
5.102.254.221	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
62.219.132.25	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
2.54.184.200	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.199	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
213.57.134.147	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.36	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.3	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
80.246.136.2	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.0.113.12	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.199	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
213.57.138.20	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
79.180.209.207	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
213.8.204.20	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.3	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
82.80.29.186	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.127	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.94.103.248	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
213.8.204.20	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
89.138.71.10	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.179.210.74	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
192.117.158.209	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.134.147	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
46.19.85.36	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
212.179.210.74	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.186.4	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.148.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
176.13.20.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
176.12.143.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
141.0.9.54	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	4
37.26.148.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
109.253.193.44	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	4
176.12.136.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.136.160	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.12.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.2.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.5.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.3	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.16.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.9.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
107.167.112.127	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	2
195.60.232.57	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 195.60.232.57	Block	2
2.54.38.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
212.90.148.93	Germany	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 212.90.148.93	Block	2
46.19.85.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.148.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
185.3.146.205	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
95.211.239.230	Netherlands	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/level/15/exec/-/	Block	1
192.117.158.209	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
82.81.45.187	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
14.20.29.55	China	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/./shared/usercontrols/headerupper/	Block	1
2.54.19.235	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1779-he/dover.aspx	Block	1
204.44.127.108	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22197-ar/dover.aspx)	Block	1
109.65.110.160	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
46.19.85.174	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.24.76.140	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.108.33.179	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.74.107.118	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/geneal.aspx	Block	1
2.54.139.121	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding !:2f?84J22wj6*XgghuoH3(!!1E?bUJ6	None	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1065-he/dover.aspx	Block	1
213.8.204.20	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.52.38.232	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/sahcar	Block	1
46.19.85.3	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
83.169.10.185	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
31.168.7.218	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.12.138.139	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakchal.idf.il/1073-he/nakchal.aspx	Block	1
46.19.85.255	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.67.50.9	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.149.191	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
185.32.179.44	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
84.108.99.164	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.136.108	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.139.121	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 2.54.139.121	None	1