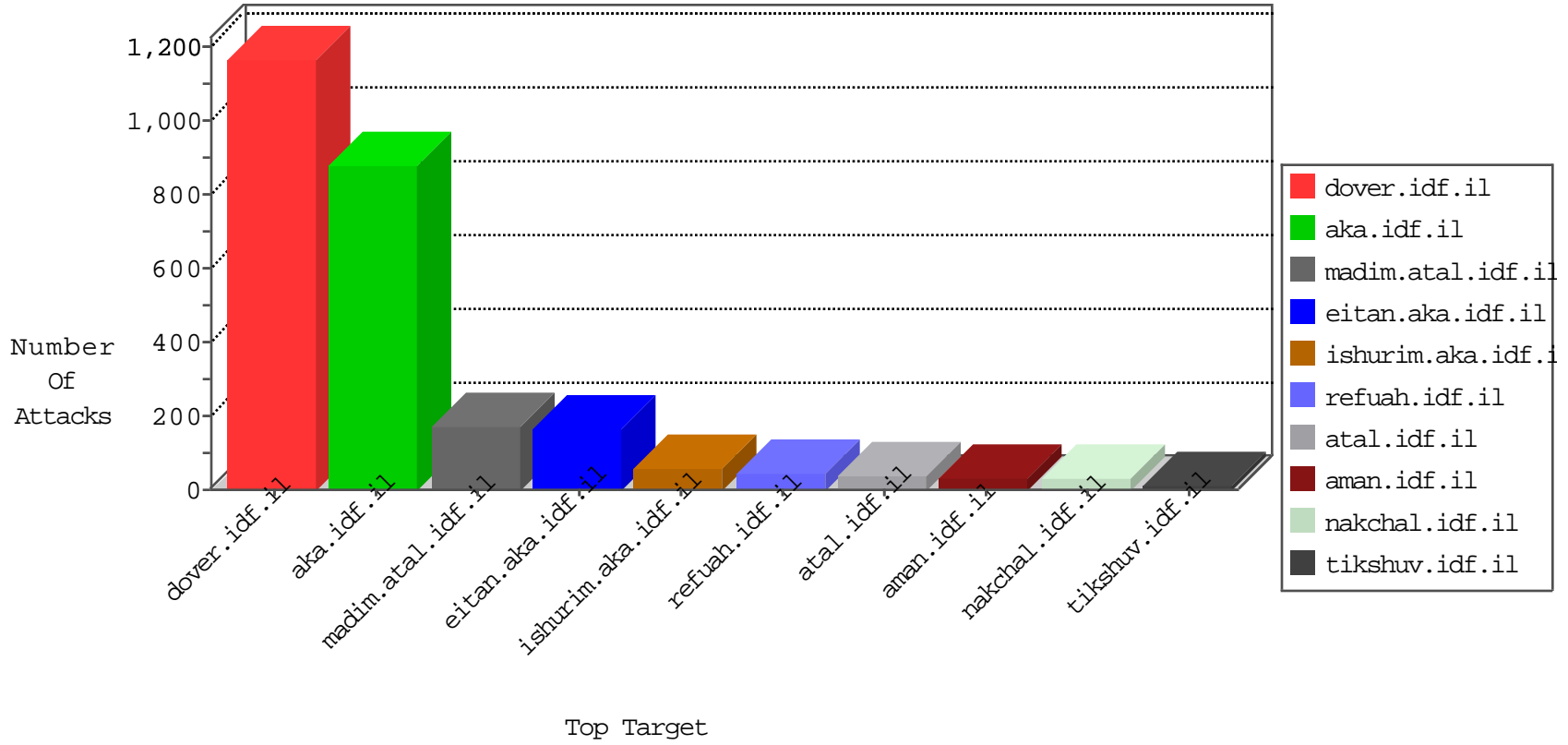


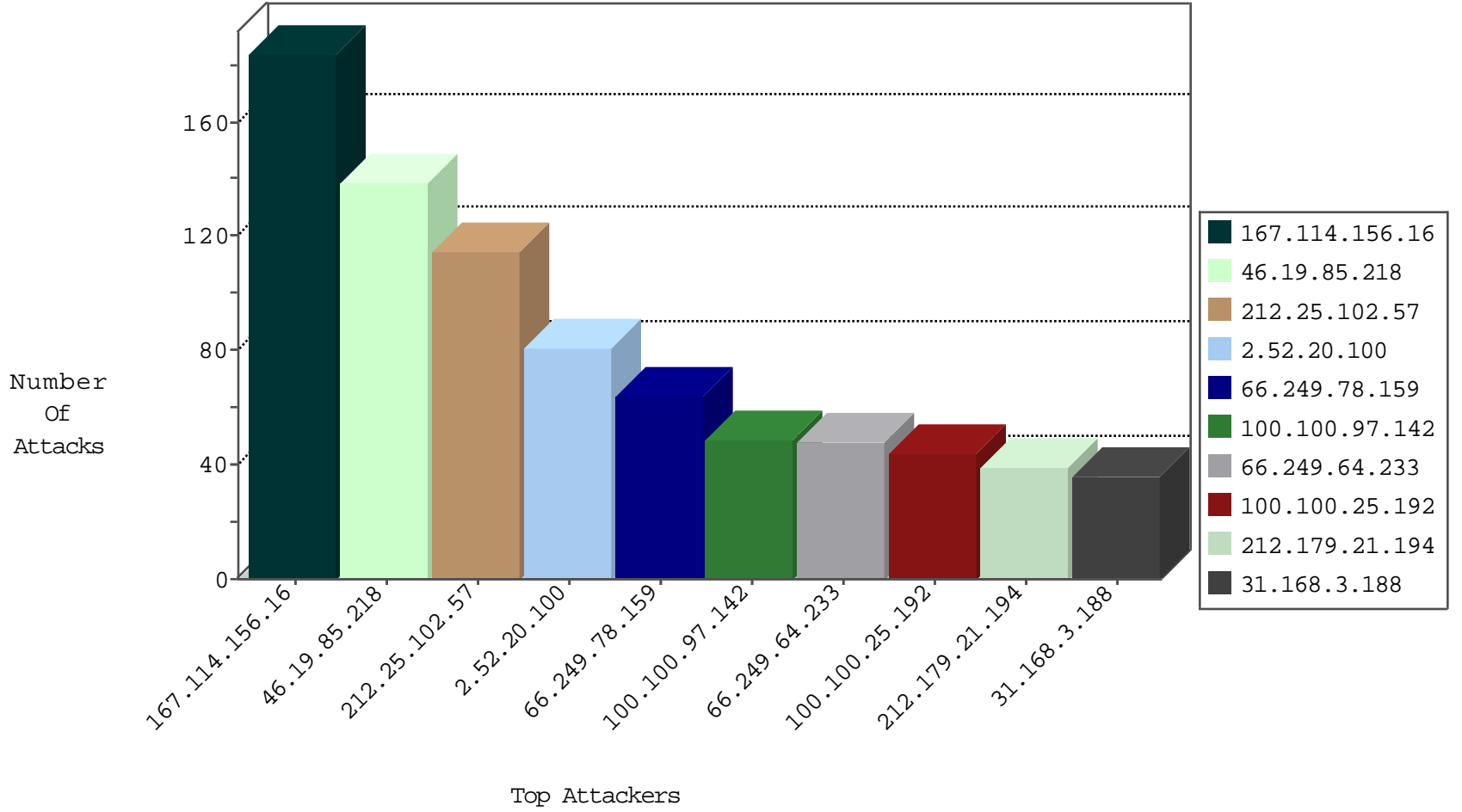
# IDF Under Attack Daily Report



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	HTTP-POST-Segmented-DoS	dest-reset	13791
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1346
167.114.229.247	Canada	147.237.0.16	my-kosher-kravi.idf.il	SYN Flood unverified cookie	drop	4
46.120.211.231	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	drop	2
134.147.203.115	Germany	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	2
176.12.143.11	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
176.13.19.126	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
93.174.93.151	Netherlands	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1
93.174.93.151	Netherlands	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.132.204	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
105.155.75.73	Morocco	147.237.77.216	dover.idf.il	12026: HTTP: LOIC DDoS Tool (ONLY enable when under DoS attack)	Block	2
167.114.229.247	Canada	147.237.0.16	ny-kosher-kravi.idf.il	13891: TLS: OpenSSL Encrypted/Unencrypted Heartbeat Packet	Permit	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	6
85.65.100.71	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.64.121.116	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
196.47.173.21	147.237.8.24	Cote D'Ivoire	e.lifestyle.idf.	ET SCAN NMAP -sS window 3072	1
79.182.3.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.3.130	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.64.195	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
132.64.171.210	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.246	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
113.248.213.100	147.237.0.19	China	madim.atal.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
37.142.117.36	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.251.56.171	147.237.77.227	Ukraine	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
24.47.224.108	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.135.26	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.163.140.142	147.237.72.14	Germany	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
85.65.99.55	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.192.16.10	147.237.77.235	Belgium	sviva.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
79.176.208.231	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.78.22.110	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.120.52.21	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
120.72.118.85	147.237.0.35	Vietnam	akaws.idf.il	ET SCAN NMAP -sS window 3072	1
109.251.56.171	147.237.77.234	Ukraine	halag.idf.il	ET SCAN NMAP -sS window 1024	1
31.6.71.154	147.237.8.24	Poland	e.lifestyle.idf.	ET SCAN NMAP -sS window 1024	1
109.66.185.178	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.138.241	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.134.149	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
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	64
100.100.97.142		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	49
66.249.64.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
100.100.25.192		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	44
212.117.136.8	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
100.100.82.73		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	34
2.52.20.100	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	32
193.43.245.250	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
85.130.251.207	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
100.100.14.151		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
100.100.28.123		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	21
37.26.148.165	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
109.186.100.27	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
37.19.116.220	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
46.19.86.94	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
66.249.93.192	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
100.100.28.123		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	13
109.186.100.27	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	13
2.52.20.100	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	12
46.19.86.6	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
80.246.133.49	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.254	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.52.20.100	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
100.100.33.240		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
2.52.20.100	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
64.19.78.243	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	11
46.19.86.140	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
2.52.185.82	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
1.47.164.35	Thailand	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.15	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.19.85.15	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.166	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
195.212.29.187	Europe	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
62.0.197.69	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
40.77.167.104	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	9
77.127.61.93	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
37.26.148.145	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
80.246.133.235	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.179.144	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
132.66.85.114	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
31.168.17.161	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
85.65.39.26	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
5.29.62.214	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
66.249.81.212	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
5.102.254.91	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.25.102.57	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	109
46.19.85.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	84
46.19.85.218	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.218	Block	41
31.168.3.188	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/resources/styles/	Block	36
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	28
194.114.146.227	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 194.114.146.227	Block	7
80.246.136.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
176.228.157.64	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
176.12.148.98	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	5
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
87.69.87.164	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	3
79.179.38.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.17.168	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 2.54.17.168	Block	3
85.65.0.83	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
212.179.132.204	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	3
46.117.161.91	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Å	Block	2
37.26.148.160	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
89.139.24.193	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.178.190.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
93.40.121.51	Italy	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/	Block	2
79.178.219.208	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
85.65.39.26	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
212.179.132.204	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 212.179.132.204	Block	2
82.80.198.164	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
185.32.179.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.142.171.104	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	2
85.65.174.40	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
82.81.5.2	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
62.90.178.209	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ https://twitter.com/	Block	2
46.19.86.121	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.75	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.65.17.196	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/https://www.aman.idf.il/	Block	1
2.52.22.188	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.93.140	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/layoutdev.css	Block	1
176.13.6.9	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.143	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/resources/images/general/pdficon.gif	Block	1
109.186.100.27	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
40.77.167.50	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/kanlar/klali/default.asp	None	1
80.230.37.13	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.179.132.204	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakchal.idf.il/sip_storage/files/8/	Block	1
95.35.254.91	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.29.205.166	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
79.179.131.26	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
2.54.18.246	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.125.95.128	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/movies/yassin7.	Block	1
46.19.85.177	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Parameter Type Violation __EVENTVALIDATION in m.my-kosher-kravi.idf.il/templates/training/training.aspx	Block	1