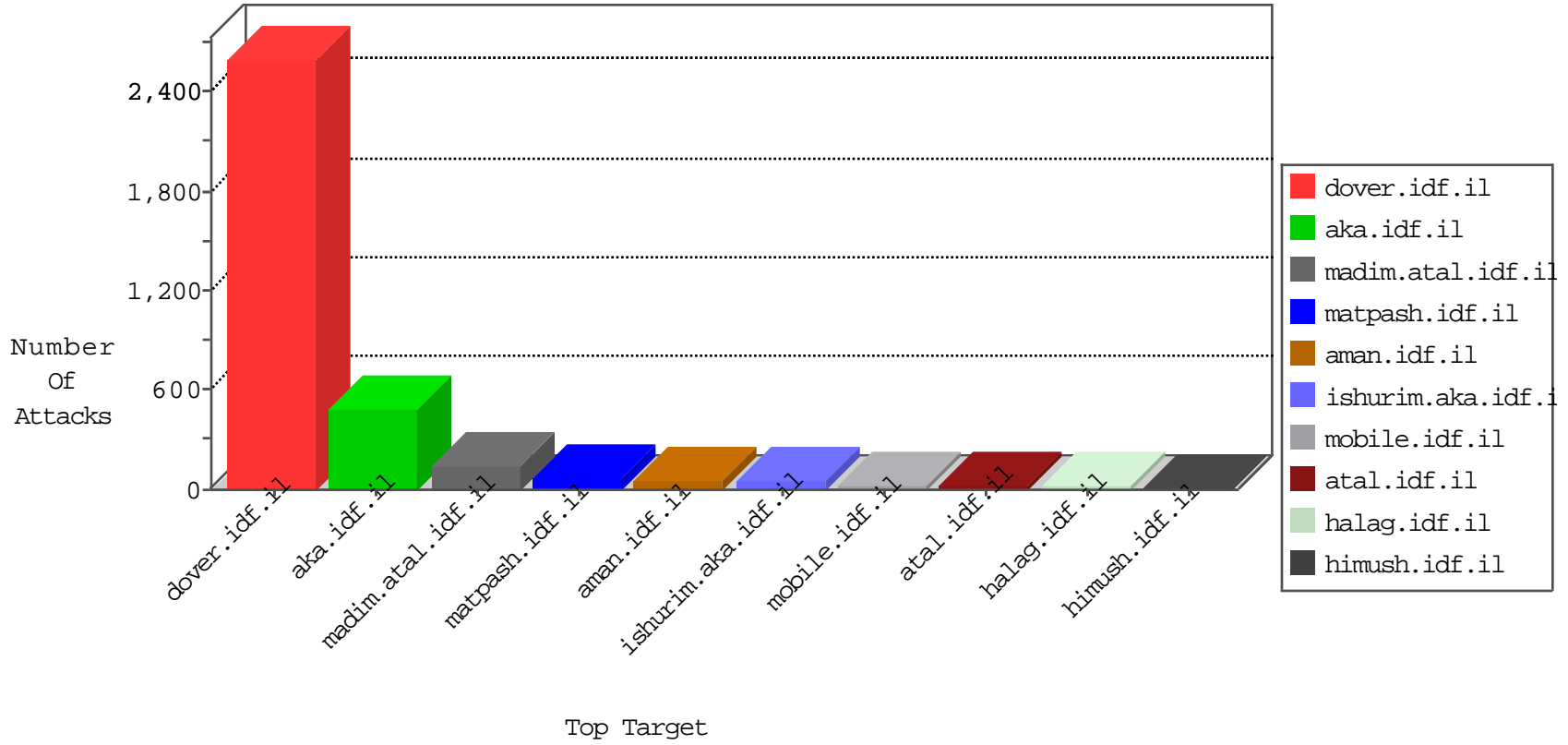


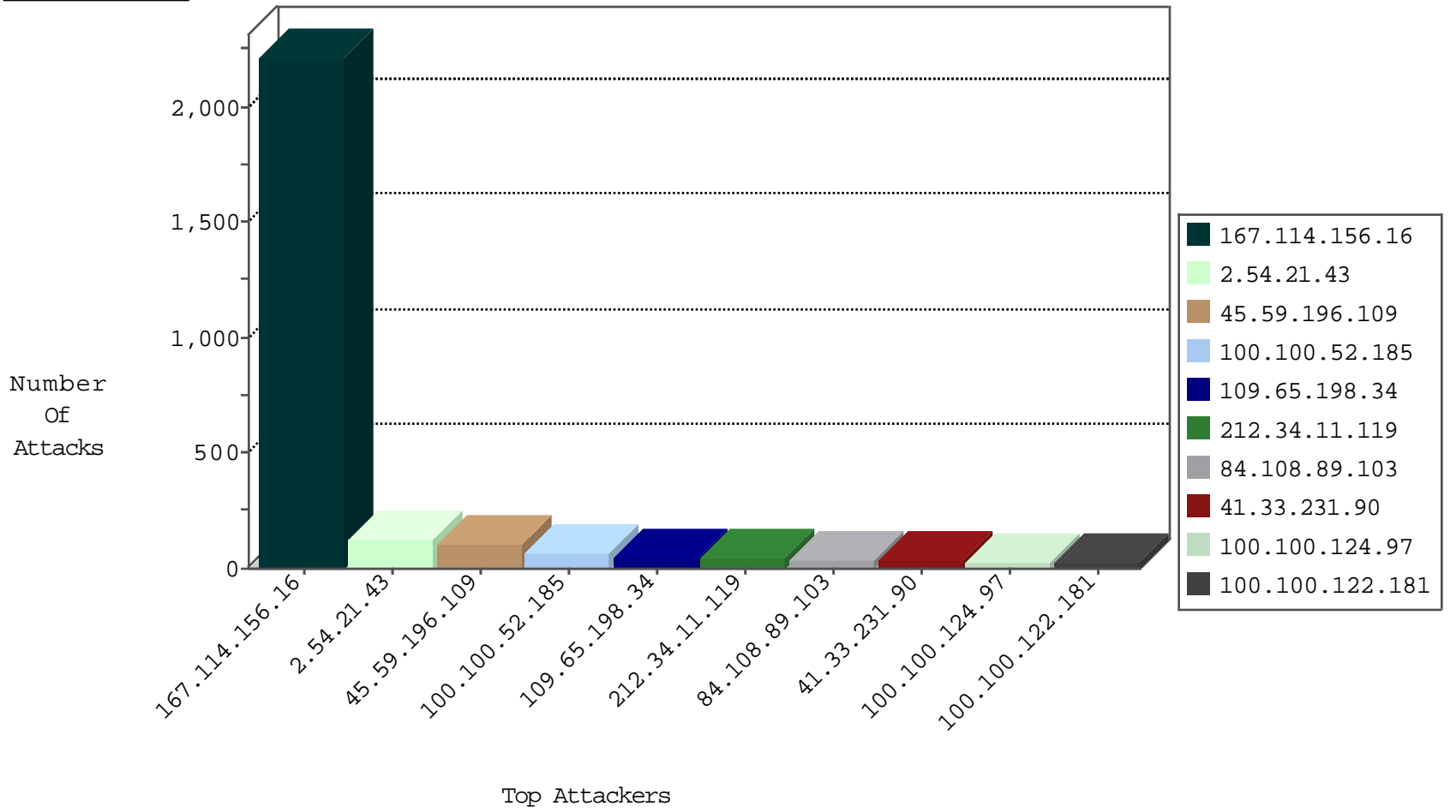
# IDF Under Attack Daily Report



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	3288
66.249.75.106	Israel	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	1103
79.176.205.103	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
204.42.253.2	United States	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	2
223.242.12.133	China	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
113.17.175.198	China	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
45.59.196.109		147.237.77.216	dover.idf.i	C1000108: HTTP: Trying to locate existing FCKeditor	Block	36
45.59.196.109		147.237.77.216	dover.idf.i	0854: HTTP: upload* Access	Block	12
109.67.27.70	Israel	147.237.76.42	refuah.idf.i	C1000004: HTTP: options method (Microsoft)	Block	5
115.42.137.250	Singapore	147.237.77.216	dover.idf.i	12347: HTTP: PHP-CGI Query String Parameter Information Disclosure Vulnerability	Block	1
79.178.101.190	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	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
66.249.73.185	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.190	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.81.196	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
66.249.66.39	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
162.222.185.165	147.237.76.31	United States	nakchal.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
196.47.173.21	147.237.76.200	Cote D'Ivoire	eitan.aka.idf.il	ET SCAN NMAP -sS window 2048	1
46.228.207.18	147.237.76.202	Germany	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
5.142.239.84	147.237.0.15	Russian Federation	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
182.132.24.252	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
162.222.185.165	147.237.76.202	United States	e.halag.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.76.30	United States	himush.idf.il	ET SCAN Potential SSH Scan	1
196.47.173.21	147.237.76.200	Cote D'Ivoire	eitan.aka.idf.il	ET SCAN NMAP -sS window 4096	1
50.204.188.142	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
196.47.173.21	147.237.76.200	Cote D'Ivoire	eitan.aka.idf.il	ET SCAN NMAP -f -sS	1
46.172.71.252	147.237.0.17	Ukraine	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.80.162.188	147.237.77.227	Vietnam	e.hamaz.idf.il	ET SCAN NMAP -sS window 4096	1
182.84.232.140	147.237.0.35	China	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
162.222.185.165	147.237.76.201	United States	e.atal.idf.il	ET SCAN Potential SSH Scan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
45.59.196.109		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
100.100.52.185		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
100.100.124.97		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	22
100.100.122.181		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
100.100.52.185		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	20
100.100.52.185		147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	18
66.249.73.185	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
109.64.155.239	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
84.108.89.103	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	12
46.120.227.134	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
100.100.106.220		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
109.64.18.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.65.198.34	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
109.64.106.56	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
100.100.77.111		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
31.154.92.244	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
84.110.145.203	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.65.198.34	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
173.252.114.118	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	8
2.52.137.211	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.85.129	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
5.102.254.50	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.220	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.198.34	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
173.252.114.117	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.194	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
31.210.186.209	Israel	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	6
84.108.89.103	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
85.130.172.84	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.184.137	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.198.34	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
173.252.114.114	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.97	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
31.210.186.209	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
84.108.89.103	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
217.194.202.150	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
84.108.89.103	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.152	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.12.93	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.198.34	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.86.246	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.108.89.103	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
31.154.92.244	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.52.5.121	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
79.177.159.161	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
31.210.186.154	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.234.217	Israel	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
79.178.96.251	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.21.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	71
2.54.21.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	49
212.34.11.119	Jordan	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	12
212.34.11.119	Jordan	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 212.34.11.119	Block	11
46.19.85.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
212.34.11.119	Jordan	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 212.34.11.119	Block	10
212.34.11.119	Jordan	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 212.34.11.119	Block	6
79.182.222.75	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	4
212.150.128.10	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	4
84.111.38.154	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	3
45.59.196.109		147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 45.59.196.109	Block	3
85.250.138.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
45.59.196.109		147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
109.64.218.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.137.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
213.57.160.146	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.109	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.34.11.119	Jordan	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	1
185.32.179.169	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.109.40.104	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
46.19.85.40	Israel	147.237.77.216	dover.idf.il	Distributed Abnormally Long Request	Block	1
37.26.149.233	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	Block	1
212.143.234.217	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
2.54.27.102	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
93.172.145.114	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
84.111.184.168	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
82.80.196.44	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
41.228.167.4	Tunisia	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
176.12.138.54	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.127.232.233	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https://www.aka.idf.il/	Block	1
217.194.202.150	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
31.154.156.99	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
95.108.158.144	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
86.98.97.73	United Arab Emirates	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
46.117.109.228	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/894-he/nakchal.aspx	Block	1
46.19.85.40	Israel	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	1
199.59.148.211	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/6/size220x0/4636.jpg	Block	1
40.77.167.20	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/templates/departmentslobby/	Block	1
109.64.106.56	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.137.68	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 4d9c6f40 in www.aka.idf.il/main/kapatz/contactus.aspx	None	1
2.54.150.69	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
94.159.204.122	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cpMain\$cpMain\$employmentStatusDay in www.aka.idf.il/main/sachar/payslips.aspx	None	1
46.19.86.39	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
84.228.255.214	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	1