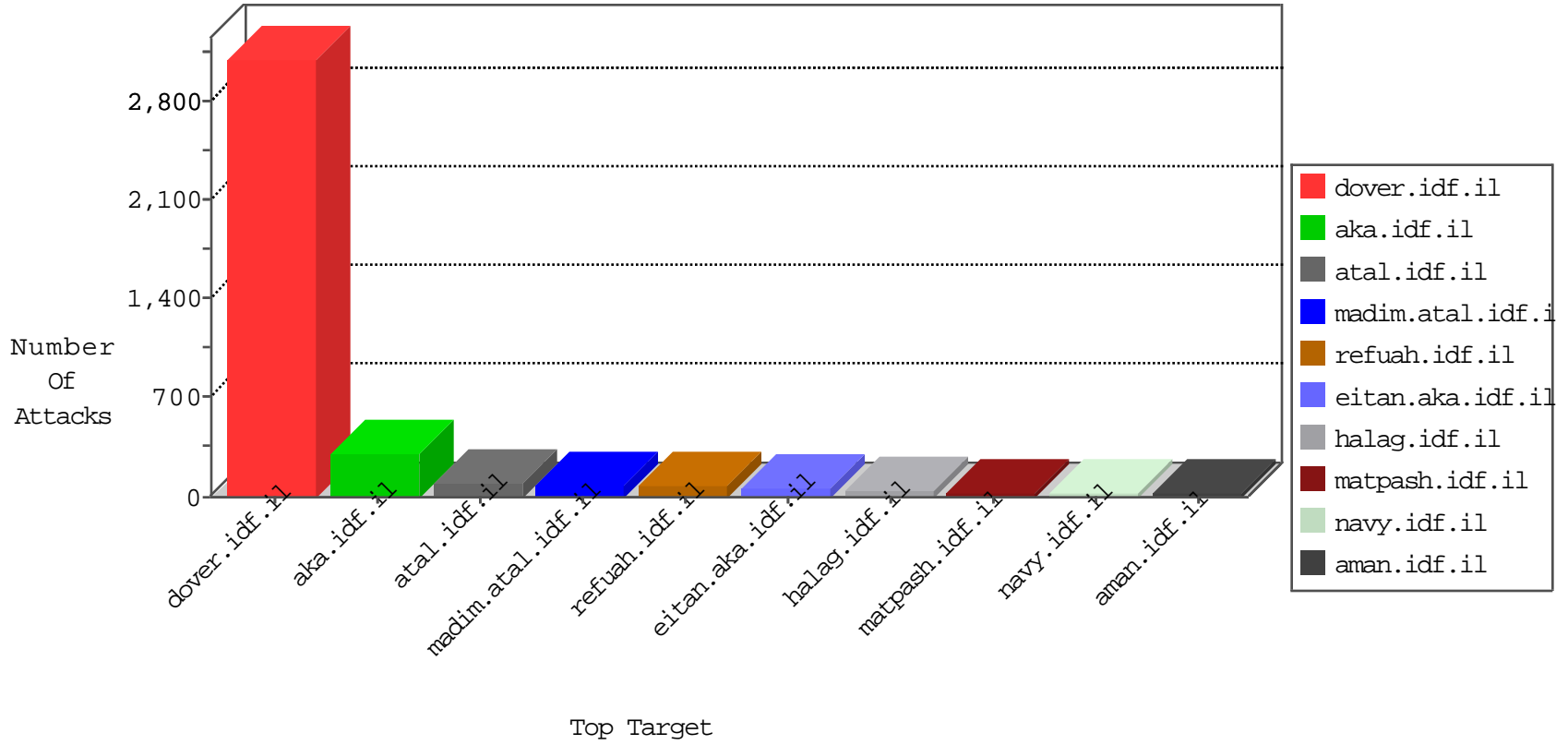


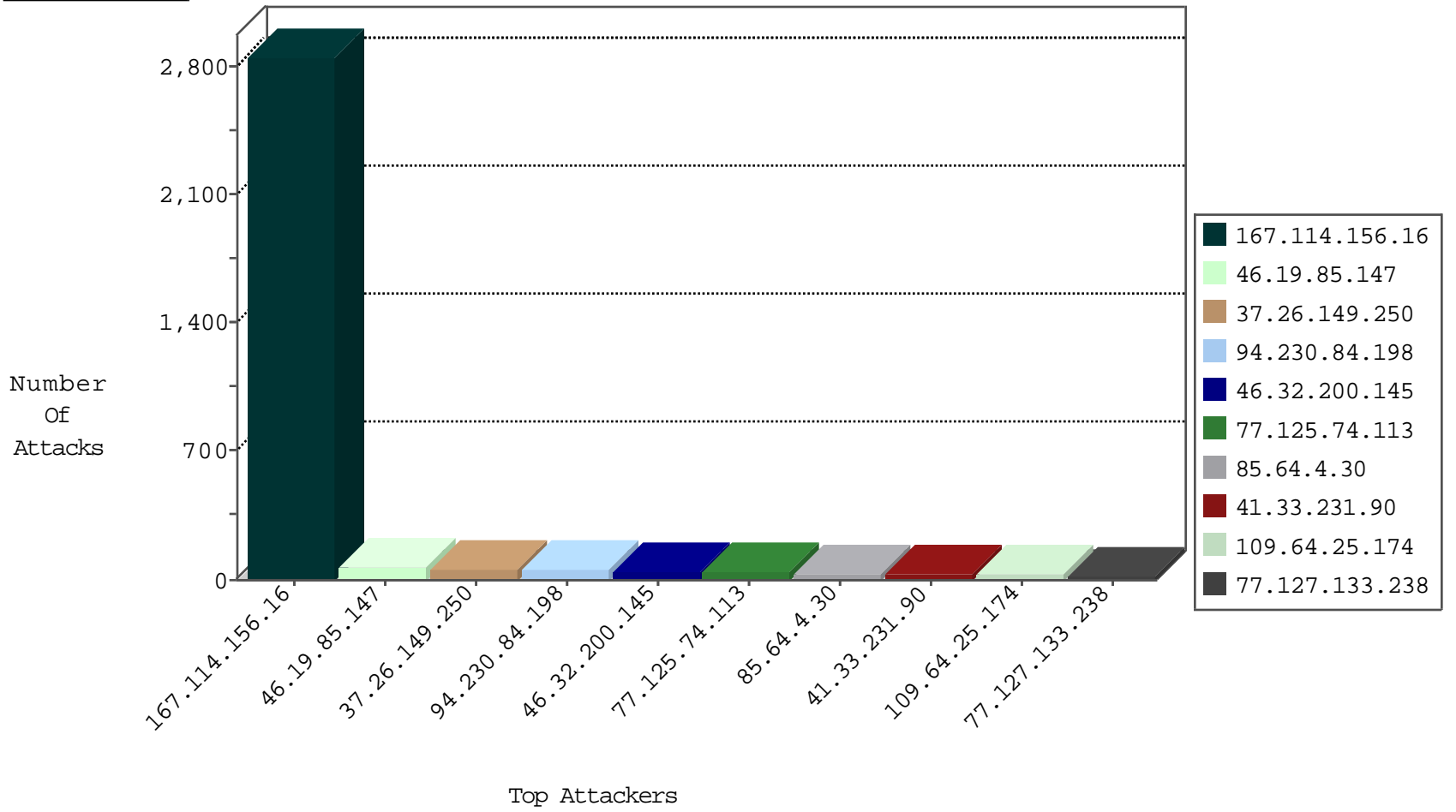
IDF Under Attack Daily Report



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	3590
79.183.27.42	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
198.20.69.98	United States	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
46.186.253.201	Kuwait	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.140.186.251	Morocco	147.237.77.216	dover.idf.il	12373: HTTP: WordPress admin Login	Block	12
78.177.209.255	Turkey	147.237.77.216	dover.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
157.55.39.243	United States	147.237.77.226	www.chamatz.aka.idf.il	C076: HTTP: Access to - action=... (General)	Block	1
167.114.242.198	Canada	147.237.76.86	navy.idf.il	13891: TLS: OpenSSL Encrypted/Unencrypted Heartbeat Packet	Permit	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	3
66.249.66.28	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.65	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
37.157.245.38	147.237.77.176	United Kingdom	matpash.idf.il	ET SCAN NMAP -sS window 4096	1
218.249.175.236	147.237.77.212	China	e.dover.idf.il	ET SCAN NMAP -sS window 4096	1
209.126.116.147	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
199.101.186.178	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 3072	1
108.47.14.226	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
84.61.168.38	147.237.77.178	Germany	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
37.157.245.38	147.237.77.176	United Kingdom	matpash.idf.il	ET SCAN NMAP -sS window 3072	1
219.92.4.74	147.237.0.17	Malaysia	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
218.249.175.236	147.237.77.212	China	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
94.230.84.198	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
82.117.208.243	147.237.77.226		www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.26.149.250	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	57
94.230.84.198	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	52
77.125.74.113	Israel	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
85.64.4.30	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	35
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
109.64.25.174	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	28
46.32.200.145	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
79.177.7.166	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
46.32.200.145	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	20
100.100.86.195		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
66.249.75.94	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
100.100.78.64		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	14
100.100.70.49		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
109.65.173.4	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.116.124.237	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
100.100.17.237		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
100.100.32.98		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
149.78.119.22	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
213.57.138.102	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
79.179.165.123	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.183.28.187	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.70	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
79.180.155.187	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
77.127.133.238	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	8
213.57.138.102	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
2.54.174.144	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.58	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.181	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.182.165.169	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
212.150.62.145	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.58	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.181	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
85.250.123.117	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
84.108.1.162	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
172.56.21.69	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
85.65.17.228	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
77.127.133.238	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
77.127.133.238	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
80.246.133.249	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
77.127.133.238	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
5.102.254.231	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
85.65.17.228	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
77.127.133.238	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
66.249.75.102	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
87.68.46.218	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
37.26.148.133	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.86.81	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	63
109.66.81.64	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
23.254.201.150	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
80.178.157.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
176.12.146.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.106.227.27	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	3
176.12.145.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
149.88.100.84	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
46.19.86.73	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
95.108.158.144	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
89.138.32.143	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Parameter Type Violation ct100\$ContentPlaceholder1\$txtAreaRemarks in m.my-kosher-kravi.idf.il/templates/training/training.aspx	Block	2
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
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-he/cogat.aspx	Block	1
213.57.189.170	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
46.121.68.45	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
199.59.148.210	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/size220x0/13032.jpg	Block	1
85.250.154.200	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
82.205.125.83	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
37.26.148.217	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
77.125.160.160	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
109.64.119.242	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
89.145.108.202	United Kingdom	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1153-8890-he/dover.aspx	Block	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
84.111.161.205	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
185.32.179.138	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
5.102.254.86	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.176.174.96	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.57.206.248	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
70.39.157.198	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
54.153.33.152	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	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
89.138.32.143	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
84.108.36.89	Israel	147.237.72.166	aka.idf.il	MSSQL Data Retrieval with Implicit Conversion Errors	None	1
37.26.149.163	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.126.40.195	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
94.230.84.198	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
187.63.7.99	Brazil	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
85.64.4.30	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
5.255.253.151	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.17	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
79.177.7.166	Israel	147.237.72.166	aka.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 79.177.7.166	Block	1
70.39.157.199	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
217.132.208.137	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.64.3.164	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
62.219.130.24	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/1133-22638-he/dover.aspx.	Block	1