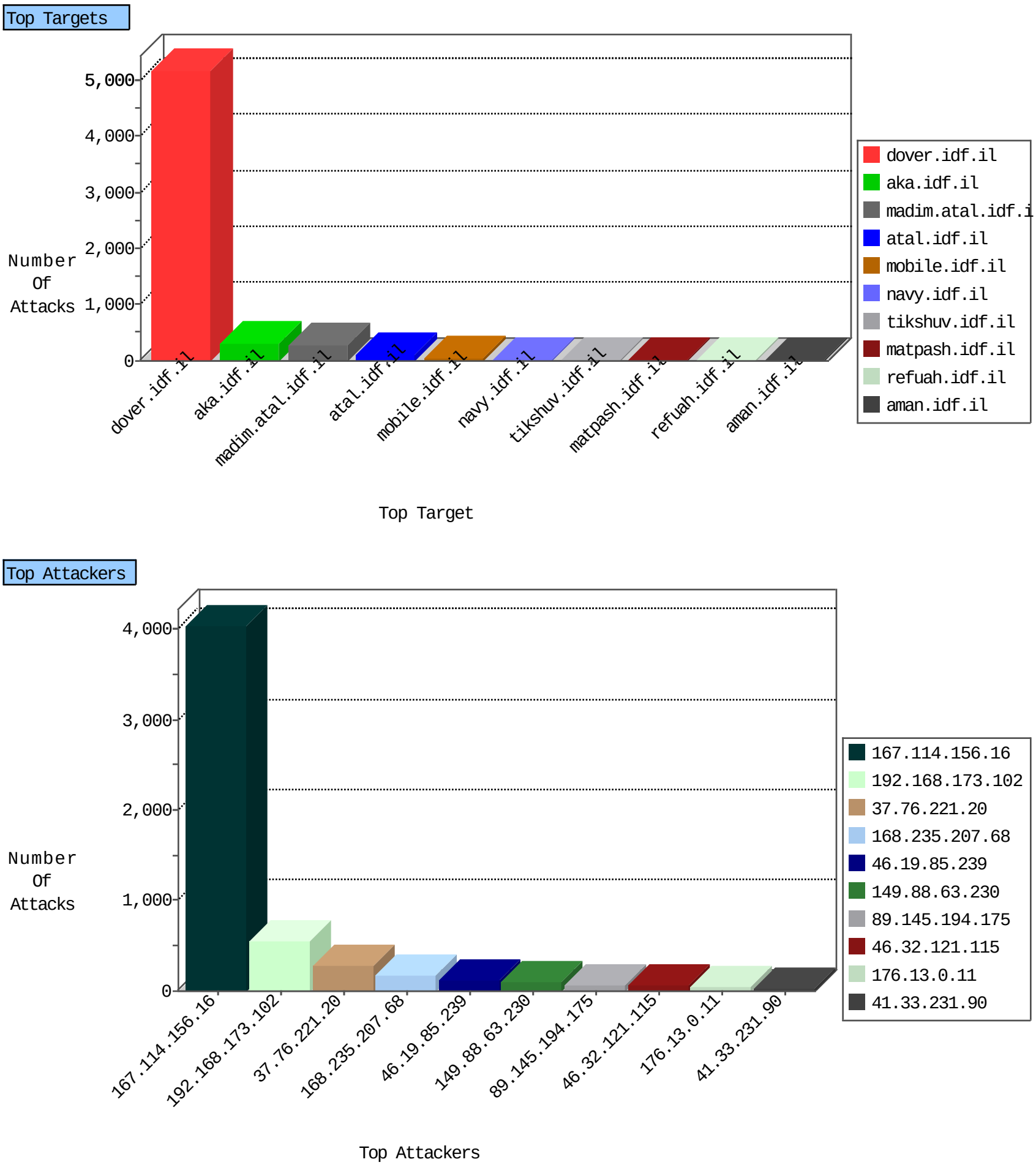
04-08-2016-12:04:05 to 04-08-2016-13:04:05

IDF Under Attack Daily Report



04-08-2016-12:04:05 to 04-08-2016-13:04:05

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	Block_Ip_Web_In	drop	4035
2.53.10.182	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2673
46.32.121.115	Jordan	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	58
37.76.221.20	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	43
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
204.42.253.2	United States	147.237.77.178	e.matpash.idf.il	Block_Ntp_All_Net	drop	2
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
66.249.69.93	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1

04-08-2016-12:04:05 to 04-08-2016-13:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.177.235.221	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
37.26.148.134	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
62.219.180.180	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.78.127	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

04-08-2016-12:04:05 to 04-08-2016-13:04:05

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	5
85.250.87.19	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	2
192.169.188.231	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
124.105.55.87	147.237.76.34	Philippines	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
198.20.69.98	147.237.77.227	United States	e.hamaz.idf.il	ET DROP Dshield Block Listed Source	1
111.118.150.57	147.237.0.33	Cambodia	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
195.216.176.244	147.237.0.19	Latvia	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
192.169.188.231	147.237.77.179	United States	e.mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
192.169.188.231	147.237.77.19	United States	law-forum.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
192.169.188.231	147.237.76.44	United States	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
220.231.195.122	147.237.8.45	China	e.eitan.idf.il	ET SCAN NMAP -sS window 3072	1
192.169.188.231	147.237.72.156	United States	aman.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
208.100.26.228	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
124.105.37.130	147.237.76.44	Philippines	e.refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
195.216.176.244	147.237.72.14	Latvia	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
106.184.2.29	147.237.76.147	Japan	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
195.216.176.244	147.237.0.15	Latvia	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
192.169.188.231	147.237.77.243	United States	mobile.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
192.169.188.231	147.237.77.216	United States	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
192.169.188.231	147.237.77.176	United States	matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
192.169.188.231	147.237.76.86	United States	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
220.231.195.122	147.237.8.45	China	e.eitan.idf.il	ET SCAN NMAP -sS window 4096	1
192.169.188.231	147.237.76.34	United States	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
208.100.26.228	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sS window 1024	1

04-08-2016-12:04:05 to 04-08-2016-13:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	362
37.76.221.20	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	215
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	191
168.235.207.68	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	175
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
89.145.194.175	United Kingdom	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	35
89.145.194.175	United Kingdom	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	35
192.114.5.10	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
5.79.68.161	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
50.50.1.9	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	14
62.90.81.186	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
46.19.86.38	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
217.132.128.58	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
2.52.136.163	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.142.72.86	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
66.249.64.163	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
37.76.221.20	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.253.150.115	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.180.160.239	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.76.221.20	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.197.2	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.166.5	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.114.23.208	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.69.93	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
85.130.234.210	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.46.39.154	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.148	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
149.88.176.109	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
85.64.13.126	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
82.152.180.203	United Kingdom	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
178.255.215.87	France	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.36.61	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.175.214	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.179	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.151.31	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.118.108	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.96.173	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.179.121.84	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.67.221	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.71.66.35	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.173.80.93	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-08-2016-12:04:05 to 04-08-2016-13:04:05

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
84.228.14.160	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.248	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.147.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.152.180.203	United Kingdom	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	124
149.88.63.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
176.13.0.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
176.13.7.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
176.13.12.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
82.81.23.242	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	3
37.26.147.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
91.200.12.106	Ukraine	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
91.200.12.106	Ukraine	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.idf.il/1038-en/dover.aspx	Block	2
46.19.86.38	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
2.54.189.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
85.65.88.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.76.221.20	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
207.46.13.71	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	Illegal Byte Code Character in URL	Block	1
66.249.78.20	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/style/1.he/popup.css	Block	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Unknown HTTP Request Method qËŽœŽ4qc–[[#29]]9ãŠ“ïrðú[[#4]]ü([[#19]]."D•»ÏæÑ[[#2]]Um\-(Ç¬£€e•ô[[#27]]¦¢•[[#4]]ß[[#20]]©-¹LQ¨d_«#¯ in URL	Block	1
5.22.129.88	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl59 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
156.211.77.152	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/favicon.ico	Block	1
82.80.196.44	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/sip_storage/files/5/	Block	1
66.249.69.2	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
169.229.3.91	United States	147.237.76.200	eitan.aka.idf.il	Illegal Byte Code Character in Method i[[#18]]¦ê–íY[[#21]]$LÕÓîI<™…ÂÜ[[#1]]£Œ[[#31]]+[[#18]]ºT—[[#21]]W@çú–…Œ%»&1ùönT>ü¡xfZ[[#28]]K;Ó	Block	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unknown HTTP Request Method éÊµ¹[[#22]]5JF•ksÓh in URL	Block	1
41.36.131.71	Egypt	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
2.52.143.56	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	NULL Character in URL	Block	1
66.249.78.27	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/style/1.he/style.css	Block	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	Abnormally Long Request method	Block	1
5.143.70.180	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1564-en/dover.aspx'	Block	1
157.55.39.8	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/templates/inner.asp	Block	1
66.249.69.10	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
169.229.3.91	United States	147.237.76.200	eitan.aka.idf.il	Malformed URL	Block	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Malformed URL	Block	1
41.36.131.71	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/admin	Block	1
109.65.109.131	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
2.52.166.5	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	Unknown HTTP Request Method ÛÅßw$: in URL	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1395-en/dover.aspx	Block	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
62.90.81.186	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1462-he/atal.aspx	Block	1
157.55.39.241	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/default.asp	Block	1
84.200.45.157	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1153-20127-he/kkkkkkk=bc69e9b3kkkkkkk_bc69e9b3	Block	1
66.249.69.18	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/4/71614.pdf	Block	1
169.229.3.91	United States	147.237.76.200	eitan.aka.idf.il	Unknown HTTP Request Method i[[#18]]¦ê–íY[[#21]]$LÕÓîI<™…ÂÜ[[#1]]£Œ[[#31]]+[[#18]]ºT—[[#21]]W@çú–…Œ%»&1ùönT>ü¡xfZ[[#28]]K;Ó in URL	Block	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Multiple Abnormally Long Request from 169.229.3.91	Block	1
41.102.248.172	Algeria	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
109.253.197.2	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1