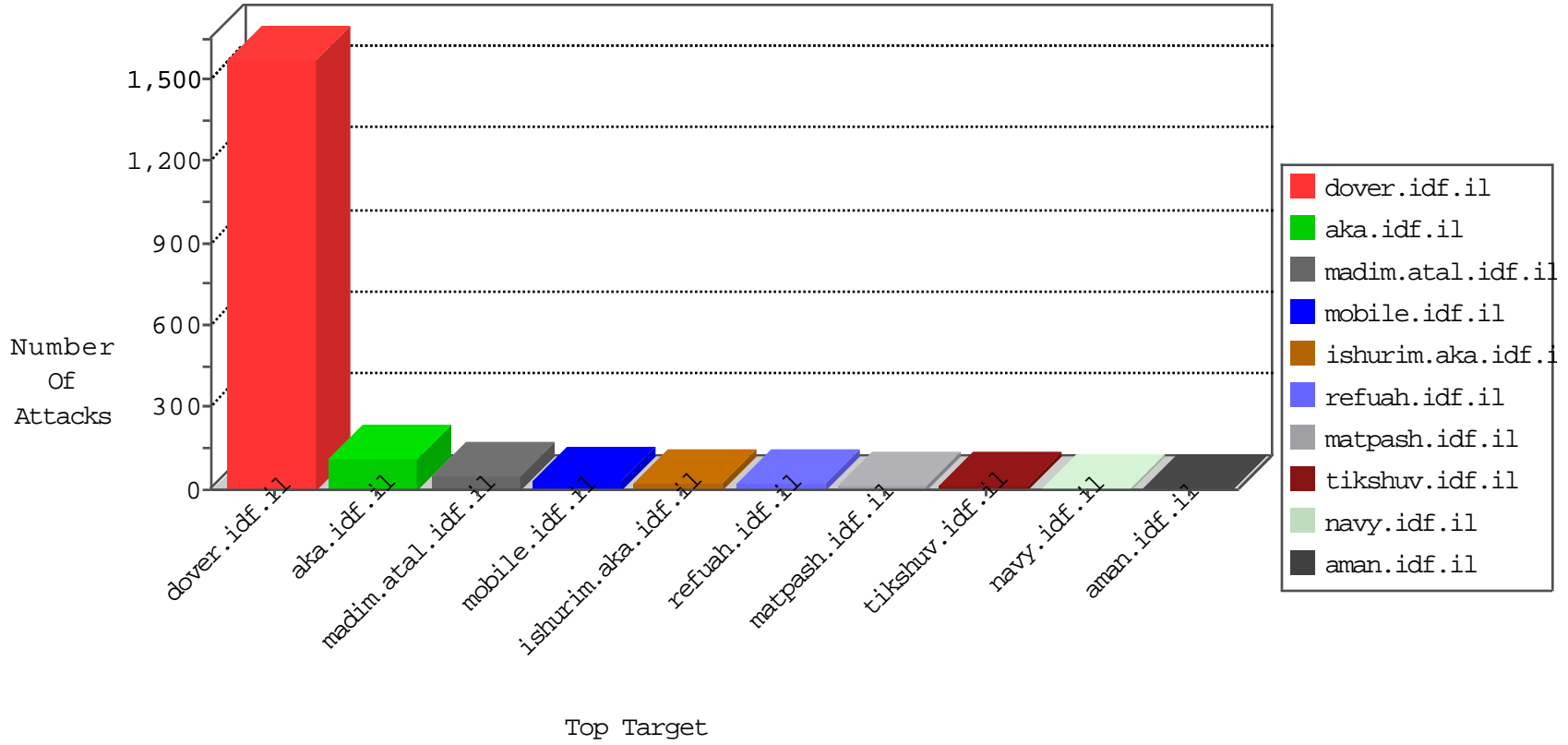


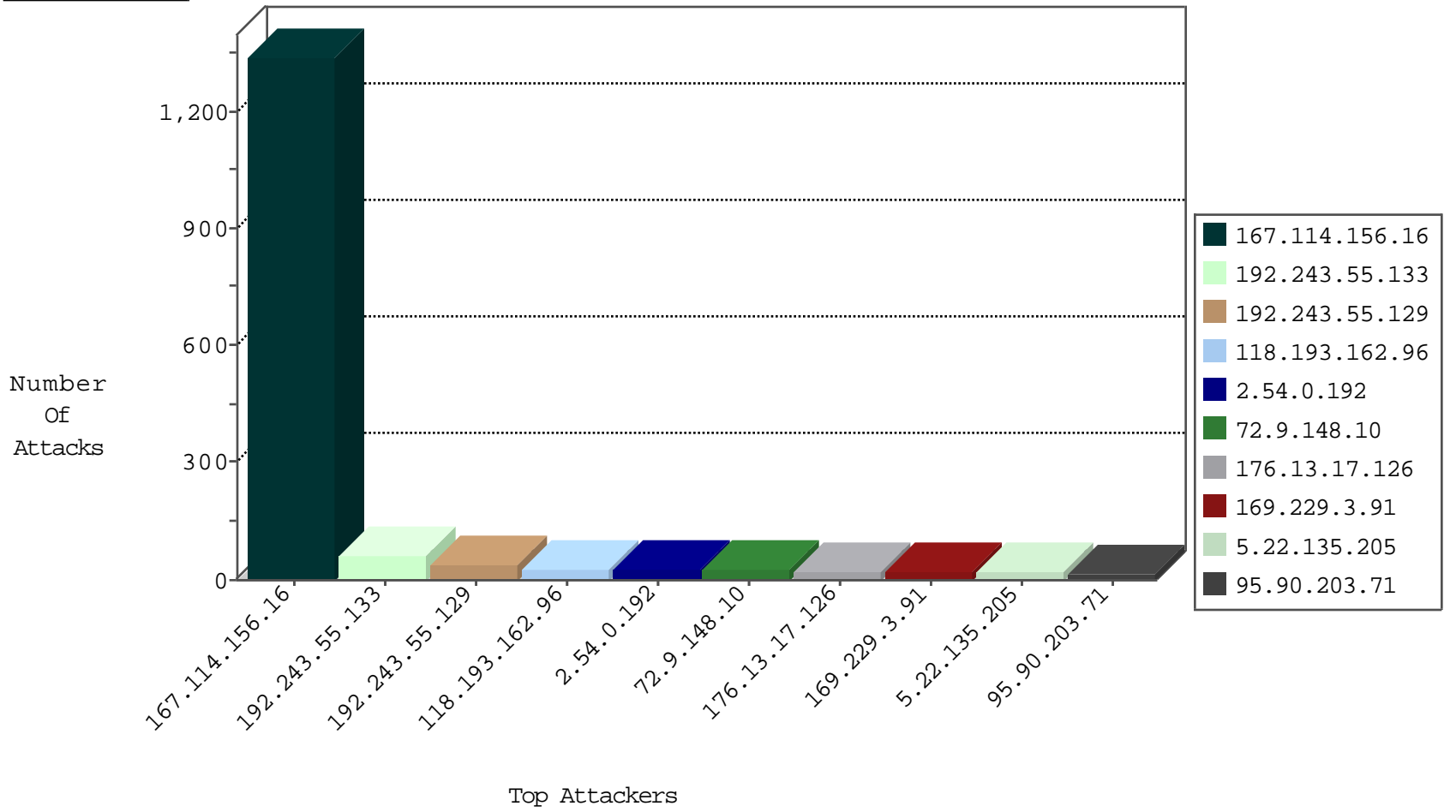
IDF Under Attack Daily Report



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	4000
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
134.147.203.115	Germany	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	2
179.43.144.33	Switzerland	147.237.77.179	e.mazi.idf.il	Block_Ntp_All_Net	drop	1
152.178.71.13	United States	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	1
179.43.144.33	Switzerland	147.237.8.45	e.eitan.idf.il	Block_Ntp_All_Net	drop	1
66.240.192.138	United States	147.237.77.170	maarachot.idf.il	Block_Udp_All_Nets	drop	1
179.43.144.33	Switzerland	147.237.8.50	e.tikshuv.idf.il	Block_Ntp_All_Net	drop	1
179.43.144.33	Switzerland	147.237.8.27	e.madim.atal.idf.il	Block_Ntp_All_Net	drop	1
179.43.144.33	Switzerland	147.237.77.121	e.navy.idf.il	Block_Ntp_All_Net	drop	1
179.43.144.33	Switzerland	147.237.8.28	e.mobile-ks.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.36.3	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
144.76.61.21	Germany	147.237.77.216	doover.idf.il	C1000074: HTTP: majestic bot	Block	2
109.65.13.106	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
151.80.31.152	Italy	147.237.77.176	matpash.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
188.165.15.105	France	147.237.76.31	nakchal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
118.193.162.96	China	147.237.77.216	doover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	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
109.64.149.100	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
66.249.66.25	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.68	147.237.76.39	United States	mobile.meitav.idf.i	ET SCAN NMAP -sA (2)	2
196.47.173.21	147.237.8.45	Cote D'Ivoire	e.eitan.idf.il	ET SCAN NMAP -sS window 4096	1
196.47.173.21	147.237.8.45	Cote D'Ivoire	e.eitan.idf.il	ET SCAN NMAP -f -sS	1
202.71.25.29	147.237.76.201	India	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
196.47.173.21	147.237.8.45	Cote D'Ivoire	e.eitan.idf.il	ET SCAN NMAP -sS window 2048	1
91.201.236.114	147.237.77.74	Ukraine	law.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
202.71.25.29	147.237.76.201	India	e.atal.idf.il	ET SCAN NMAP -sS window 4096	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.54.0.192	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	22
5.22.135.205	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	15
95.90.203.71	Germany	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
109.253.132.240	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.11.159	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	6
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.213	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.65.94.9	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.136.46	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
87.70.39.76	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
87.69.11.237	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
183.250.209.101	China	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
197.35.215.226	Egypt	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
93.158.152.49	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.116.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.46.41.242	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.54.0.192	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.180.127.230	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.154.166.11	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
156.204.142.26		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.64.191.195	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.22.148	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.178.231.122	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.166	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.39.76	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
176.67.100.198	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	3
79.178.176.104	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.69.38	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.62.103	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.136.217	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.67.100.198	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
109.64.33.106	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

03-12-2016-14:04:03 to 03-12-2016-15:04:03

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
217.132.14.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
72.9.148.10	United States	147.237.76.86	navy.idf.il	drop	SAM rule	drop	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
118.193.162.96	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 118.193.162.96	Block	25
176.13.17.126	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
46.19.86.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
8.37.235.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
46.19.86.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
37.142.183.65	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00\$ContentPlaceholder\$txtFirstName in madim.atal.idf.il/1088-he/meretz.aspx	Block	4
80.246.130.99	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
89.138.6.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
149.88.222.235	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 149.88.222.235	Block	3
80.246.130.226	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
149.88.222.235	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
79.181.210.106	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.181.210.106	Block	2
121.34.192.190	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 121.34.192.190	Block	1
82.205.14.176	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/clashaclers.php	Block	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	Multiple Abnormally Long Request from 169.229.3.91	Block	1
66.249.66.182	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/2827.jpg	Block	1
157.55.39.49	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
150.70.173.8	Japan	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/clientscripts.js	Block	1
118.193.162.96	China	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 118.193.162.96	Block	1
183.250.209.101	China	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/./shared/usercontrols/headerupper/	Block	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in URL ;r,"¶ \$7[["+#25]] o,f ;'7" <]#21[[!\$]]#4[[3]]#21[[Block	1
79.181.210.106	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/gyus/general.aspx	Block	1
150.70.173.53	Japan	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/scroller/jquery.jcarousel.js	Block	1
131.253.25.183	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.229.1.194	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
66.249.66.188	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/3142.jpg	Block	1
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.il	Illegal Byte Code Character in Method	Block	1
150.70.173.9	Japan	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery/jquery-ui.js	Block	1
37.26.146.191	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	Malformed URL ;r,"¶ \$7[["+#25[[]#21]]³[[#4[[!\$]]#21 <]]" f,o ; 7	Block	1
46.43.115.227	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
150.70.173.55	Japan	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery.plugins/jquery.equal heights.js	Block	1
149.88.71.234	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	NULL Character in Method	Block	1
66.249.69.2	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/9/70239.pdf	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
150.70.173.10	Japan	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery.plugins/slider.js	Block	1
212.179.159.253	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
118.193.162.96	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/fck/	Block	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method 19^@f&w;r[[#16]]•br•• in URL ;r,"¶ \$7[["+#25[[]#21]]³[[#4[[!\$]]#21" <]]" ;'o,f	Block	1
150.70.173.56	Japan	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery.plugins/jquery.charts.js	Block	1
109.177.232.81	United Arab Emirates	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	Abnormally Long Request request version	Block	1
68.180.228.96	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
150.70.173.46	Japan	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/sa_swfobject.js	Block	1
46.19.85.213	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
121.34.192.190	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	1