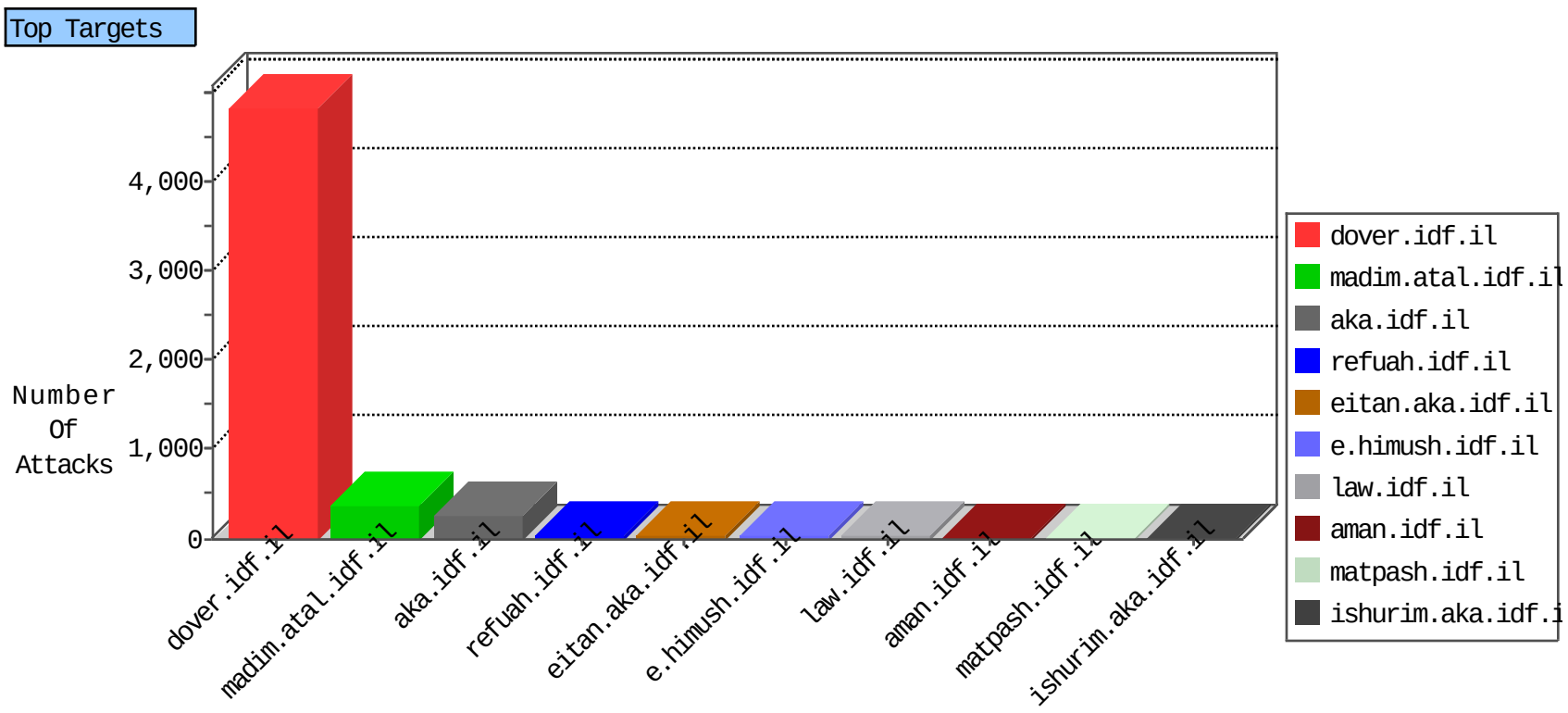
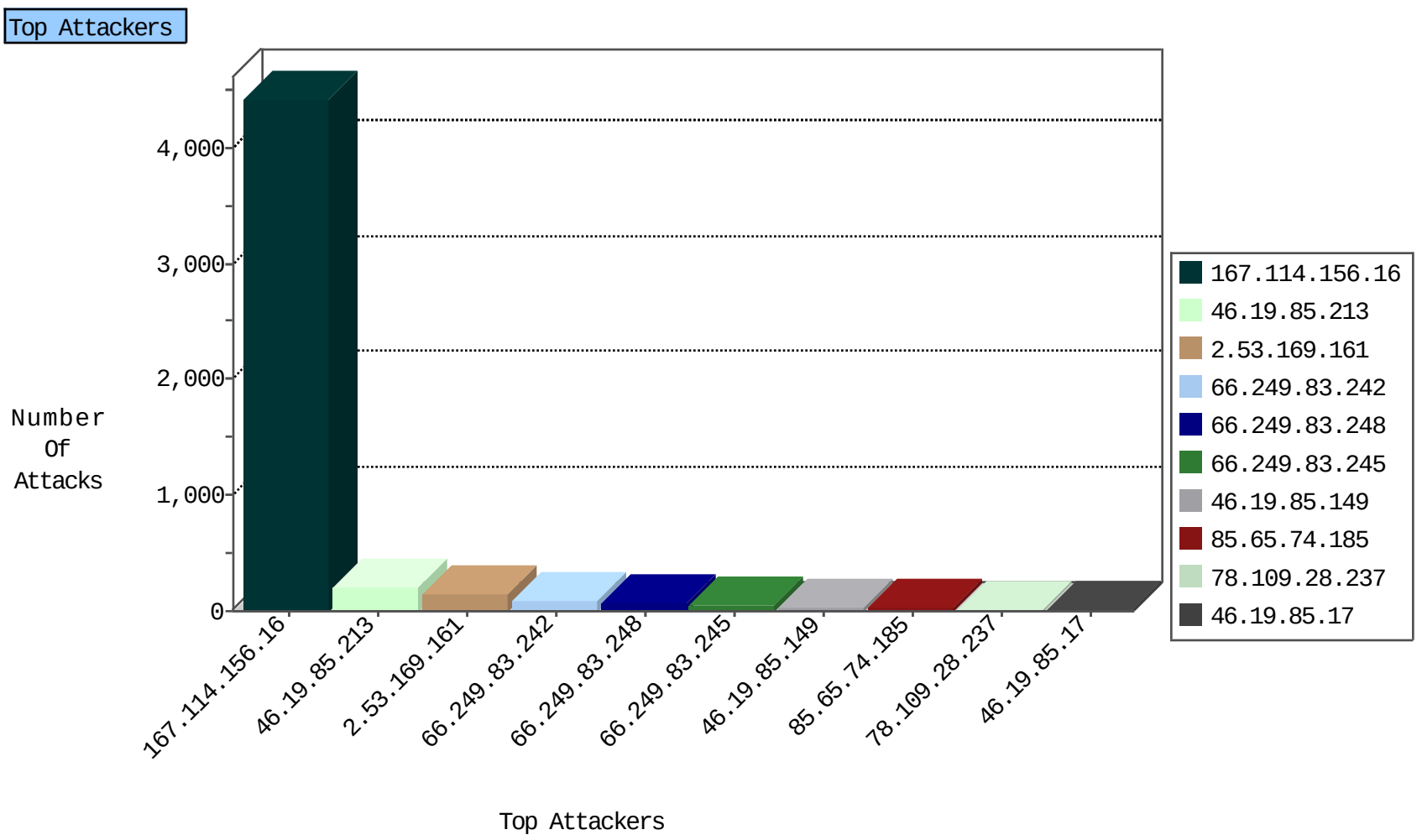
04-18-2016-14:04:02 to 04-18-2016-15:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-18-2016-14:04:02 to 04-18-2016-15:04:02

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	3995
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	658
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	9
212.199.182.150	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
37.46.39.193	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
74.91.23.107	United States	147.237.77.170	maarachot.idf.il	block-sp-traf1	forward	3
204.12.196.235	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	2
107.150.46.36	United States	147.237.76.86	navy.idf.il	block-sp-traf1	forward	2
107.150.46.38	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
101.201.147.32	China	147.237.76.30	himush.idf.il	block-sp-traf1	forward	2
69.30.198.146	United States	147.237.77.19	law-forum.idf.il	block-sp-traf1	forward	2
79.178.169.35	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
107.150.32.58	United States	147.237.72.166	aka.idf.il	block-sp-traf1	forward	2
69.30.226.100	United States	147.237.76.86	navy.idf.il	block-sp-traf1	forward	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
74.82.47.37	United States	147.237.77.234	halag.idf.il	Block_Udp_All_Nets	drop	1
149.78.154.69	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
192.115.177.202	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
80.246.136.213	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

04-18-2016-14:04:02 to 04-18-2016-15:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-18-2016-14:04:02 to 04-18-2016-15:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
54.72.73.168	147.237.77.216	Ireland	dover.idf.il	portscan: TCP Distributed Portscan	1
213.8.173.237	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.149.156	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	1
132.68.129.138	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.22.135.143	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.252.244	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
106.186.113.67	147.237.76.44	Japan	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
91.135.102.191	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.179.69.252	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.105.46	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.64.102	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
46.121.239.176	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
37.26.147.183	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.225.60	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.45.34	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.143.241	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.219.238.10	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
84.228.166.51	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.181.180.112	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.79.107	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1

04-18-2016-14:04:02 to 04-18-2016-15:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	221
66.249.83.242	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	80
66.249.83.248	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	72
66.249.83.245	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
78.109.28.237	Ukraine	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	18
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
109.226.22.157	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
41.77.138.90	Egypt	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	14
46.19.85.149	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
46.19.85.42	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
2.53.158.135	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.149	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
194.90.66.9	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
87.71.26.91	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
46.19.85.17	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
192.115.177.202	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
31.168.247.70	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
89.138.115.115	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.149	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.182.107.91	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.33.52	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.227	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.3.180	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.32.179.186	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
176.13.5.195	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.117.136.6	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.17	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
62.219.239.102	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
66.102.9.91	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.149	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
212.143.134.129	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
94.159.178.70	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
37.26.147.147	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
31.168.133.226	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.102.9.101	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.93.93	Europe	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
31.168.227.138	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
107.6.123.226	Singapore	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
46.19.85.239	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
147.235.8.51	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
37.26.147.147	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.199.195.166	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.55.188.183	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.13.203	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.248	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.137.192	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
176.13.10.10	Israel	147.237.72.166	aka.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
46.19.85.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	209
2.53.169.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	154
46.19.86.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
213.57.91.199	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized HTTP Method	Block	5
212.199.93.122	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 212.199.93.122	Block	5
2.55.10.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
46.19.86.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
46.19.86.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.65.74.185	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
65.55.213.31	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
40.77.167.25	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
176.13.13.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.65.74.185	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 85.65.74.185	Block	2
77.127.160.188	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	2
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	2
85.65.74.185	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 85.65.74.185	Block	2
85.65.74.185	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 85.65.74.185	Block	2
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/nakhal	Block	2
213.8.63.16	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
87.71.74.170	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined	Block	2
46.19.85.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
85.65.74.185	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 85.65.74.185	Block	2
85.65.74.185	Israel	147.237.72.166	aka.idf.il	NULL Character in Method üGzä>»§ÈÁ[[#27]]xÕ˜ñ[[#19]]G1)[[#26]]}MèÚ- rÙœ[[#16]][[#0]]¶dÖ>m Œe/\44†îìHÕ¨ýˆWÏJ•ÍF¥r[[#27]]ncúedµWµJ©`Íyå¶›®	Block	1
46.222.186.24	Spain	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/71929-he/	Block	1
212.143.134.129	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter &l in www.eitan.aka.idf.il/templates/sendtofriend/sendtofriend.aspx	None	1
85.65.74.185	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Parameter Name Zß£7Fn–«,bף•ה£nÝV¸±QÞ, ut„ך"וו¨<X½>2<צ]]#1[[]]#2[[6‘6פÚx¬פ]]jx$±5XUg[[#12:½ @[[#14]];ÞŠ[[#24]]’[[#29]]<[[Žק#1ל#˜]]pם†”aj^[[ם#15[[·]]#28½]]-0מרי˛`‹ •)–•µw	Block	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	Malformed URL	Block	1
74.91.23.107	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to www.app-softwares.com/	Block	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/2347.jpg	Block	1
89.139.154.225	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
212.199.93.122	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/login.aspx	Block	1
80.246.130.244	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/faq/mobile	Block	1
185.27.105.179	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/	Block	1
66.249.83.248	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.253.208.180	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
85.65.74.185	Israel	147.237.72.166	aka.idf.il	NULL Character in URL n¸don[[#19]]˛˙¸″Û>[[#1]]Ÿf[[#22]]¯ [[#23]]³ÿ¿i}[[#28]][[#7]]c˛£€`6[[#0]]71#[[ez]]'8Ÿri‘¹¨•Ù65š[[#12]]pŽ¦÷8„ ž[[#8]]‘„f[["#5^-go-û}]]א″'3210#ƒ'ר:wfŒ9[[#17]]dr˙šl”•„ytn[[#31]]qÚˆ «¸µ<:₪,	Block	1
50.62.161.6	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/wordpress/wp-admin/	Block	1
213.57.91.199	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/sip_storage/files/0/	Block	1
2.55.185.8	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
212.143.134.129	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter amp;rnd in www.eitan.aka.idf.il/shared/ajax/createcaptchaimage.aspx	None	1
85.65.74.185	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Parameter Value at 8 for m„[[#16]]domת·'pע ß•g3	Block	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	Unknown HTTP Request Method ÷õ«8[[#8]] in URL	Block	1
66.249.78.253	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
98.130.0.237	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/wp/wp-admin/	Block	1
85.14.244.114	Germany	147.237.77.176	matpash.idf.il	Distributed Suspicious Response Code	Block	1
195.160.242.40	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	Block	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
67.212.234.44	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/blog/wp-admin/	Block	1
85.65.74.185	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
62.210.152.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/wp-login.php	Block	1