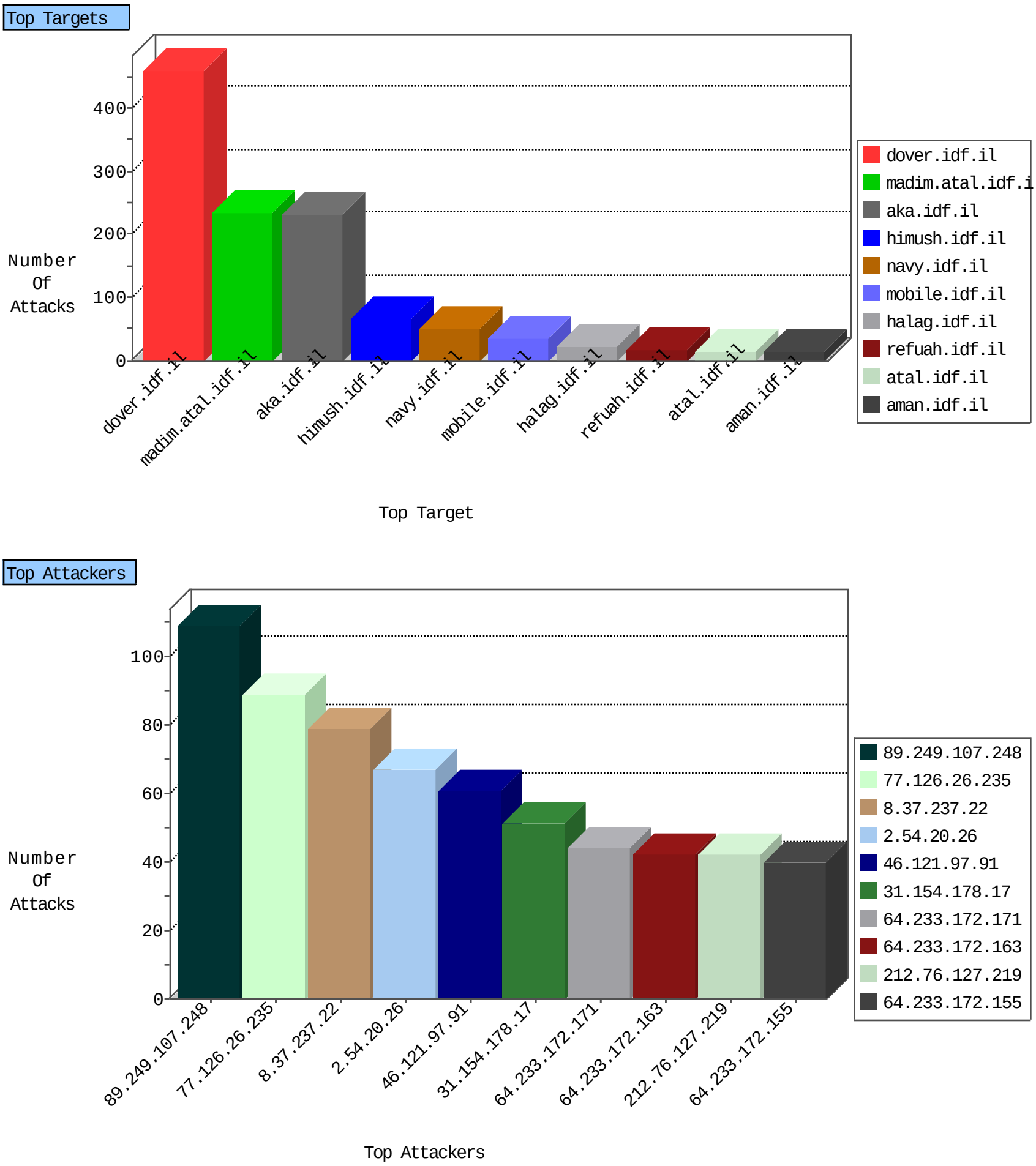
02-05-2016-15:04:04 to 02-05-2016-16:04:04

IDF Under Attack Daily Report



02-05-2016-15:04:04 to 02-05-2016-16:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.178.13.103	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
79.176.127.112	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
66.249.81.206	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
66.249.93.180	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
104.207.128.23	United States	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
76.169.1.130	United States	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
138.75.133.73	Singapore	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

02-05-2016-15:04:04 to 02-05-2016-16:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-05-2016-15:04:04 to 02-05-2016-16:04:04

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
37.26.148.152	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
93.189.26.18	147.237.76.31	Austria	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
50.204.188.142	147.237.72.156	United States	aman.idf.il	ET SCAN NMAP -sS window 3072	1
46.166.129.183	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN NMAP -sS window 3072	1
218.246.0.97	147.237.77.176	China	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
95.86.124.131	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
91.201.236.114	147.237.0.17	Ukraine	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
46.166.129.183	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN NMAP -sS window 4096	1
46.19.85.249	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
218.246.0.97	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1

02-05-2016-15:04:04 to 02-05-2016-16:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
89.249.107.248	Croatia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	86
8.37.237.22	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	79
31.154.178.17	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
212.76.127.219	Israel	147.237.76.30	himush.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	42
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
5.29.131.215	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	24
77.126.26.235	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
46.121.156.188	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
141.0.14.166	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
64.233.172.171	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
64.233.172.171	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	18
212.76.127.10	Israel	147.237.76.30	himush.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	18
77.127.209.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
64.233.172.163	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
64.233.172.163	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	15
64.233.172.155	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
64.233.172.155	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	15
192.116.94.220	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
64.233.172.163	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
89.249.107.248	Croatia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
64.233.172.155	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
77.125.86.246	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
89.249.107.248	Croatia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	9
185.3.147.205	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
82.166.148.146	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
54.172.96.232	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
64.233.172.171	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
188.120.148.253	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
77.125.109.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.22	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.22	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
84.95.209.201	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.125.226	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
54.164.131.187	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
2.52.177.231	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
66.249.81.182	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.19.86.252	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.116.86.14	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
80.246.139.11	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
37.26.147.234	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.8.85	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
149.78.43.54	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.209.83	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.167	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.126.26.235	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-05-2016-15:04:04 to 02-05-2016-16:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.20.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	67
46.121.97.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	61
77.126.26.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	61
46.210.243.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
176.13.15.127	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
109.67.9.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
192.243.55.134	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.134	Block	2
77.126.26.235	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
192.116.94.220	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Multiple Unknown HTTP Request Method from 169.229.3.91	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/null	Block	1
169.229.3.91	United States	147.237.76.39	mobile.meitav.idf.il	Multiple Unknown HTTP Request Method from 169.229.3.91	Block	1
128.232.110.29	United Kingdom	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to 147.237.76.147/	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx	Block	1
169.229.3.91	United States	147.237.77.234	halag.idf.il	Unknown HTTP Request Method 7:6ÃŽ`!Ã?Ã«Ã¿LÂ?bÃˆÃ…Ã‰1Â?Ã³ÂžZZ<[[#24]]7Ã?Â²Ã±\D[[#22]]Â•~tlÂœoÂ¥\Ã±Ã”&Â?[[#22]]Ãž[[#16]]ÂŽÂžÃ‡ÂŽÃ©[[#30]]^[[#7]]Â¹ in URL	Block	1
54.172.96.232	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/sitemap/piwik.php	Block	1
169.229.3.91	United States	147.237.76.86	navy.idf.il	Unknown HTTP Request Method ÃŒnÃ¢[[#31]]VÃ½[[#31]]kÃŸÃ†[[#7]]Ã»3Â‘[[#29]]Ã ÃœÂ»ZÂƒÃŒ in URL Ã?Â¸<Â?×¨Ã™Â¬;yÂ¬Ã?Ö´	Block	1
169.229.3.91	United States	147.237.76.39	mobile.meitav.idf.il	Illegal Byte Code Character in Header Name	Block	1
79.181.162.133	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
192.243.55.129	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/general	Block	1
169.229.3.91	United States	147.237.77.234	halag.idf.il	Abnormally Long Request method	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-15430-en/dover.aspxbedouin	Block	1
46.117.190.22	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
169.229.3.91	United States	147.237.76.86	navy.idf.il	Abnormally Long Request method	Block	1
192.243.55.135	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/tizmoret/printpreview/default.asp	Block	1
157.55.39.138	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/61998	Block	1
77.125.86.246	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.65.82	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter searchText in eitan.aka.idf.il/916-en/eitan.aspx	None	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Illegal Byte Code Character in URL	Block	1
169.229.3.91	United States	147.237.76.39	mobile.meitav.idf.il	Malformed URL	Block	1
41.82.0.80	Senegal	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1
192.243.55.130	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=58570&docid=65110	Block	1
85.65.15.29	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
169.229.3.91	United States	147.237.77.234	halag.idf.il	Illegal Byte Code Character in Header Name	Block	1
66.249.78.177	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter SearchText in www.eitan.aka.idf.il/938-he/eitan.aspx	None	1
169.229.3.91	United States	147.237.76.86	navy.idf.il	Illegal Byte Code Character in Method ÃŒnÃ¢[[#31]]VÃ½[[#31]]kÃŸÃ†[[#7]]Ã»3Â‘[[#29]]Ã ÃœÂ»ZÂƒÃŒ	Block	1
192.243.55.136	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.136	Block	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	Abnormally Long Request method	Block	1
77.125.109.191	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
185.3.147.205	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Multiple Abnormally Long Request from 169.229.3.91	Block	1
66.249.65.122	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter PageNum in www.eitan.aka.idf.il/1103-en/eitan.aspx	None	1
169.229.3.91	United States	147.237.76.39	mobile.meitav.idf.il	Multiple Abnormally Long Request from 169.229.3.91	Block	1
41.82.0.80	Senegal	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
192.243.55.132	Dominica	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/tizmoret/printpreview/default.asp	Block	1
109.64.182.124	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
169.229.3.91	United States	147.237.77.234	halag.idf.il	Illegal Byte Code Character in Method 7:6ÃŽ`!Ã?Ã«Ã¿LÂ?bÃˆÃ…Ã‰1Â?Ã³ÂžZZ<[[#24]]7Ã?Â²Ã±\D[[#22]]Â•~tlÂœoÂ¥\Ã±Ã”&Â?[[#22]]Ãž[[#16]]ÂŽÂžÃ‡ÂŽÃ©[[#30]]^[[#7]]Â¹	Block	1
66.249.78.177	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter SortDir in www.eitan.aka.idf.il/1103-en/eitan.aspx	None	1
169.229.3.91	United States	147.237.76.86	navy.idf.il	Illegal Byte Code Character in Query String on Ã?Â¸<Â?×¨Ã™Â¬;yÂ¬Ã?Ö´	Block	1

02-05-2016-15:04:04 to 02-05-2016-16:04:04