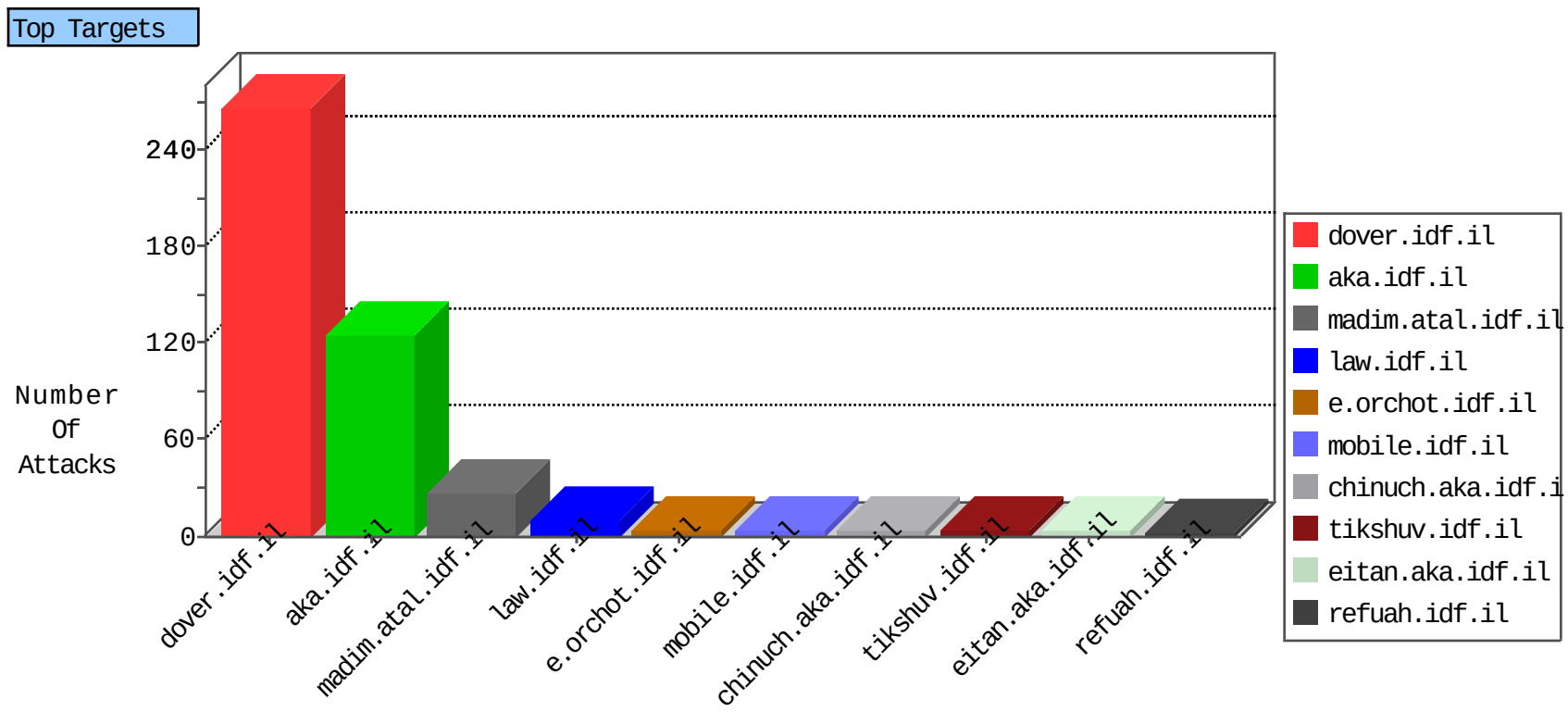
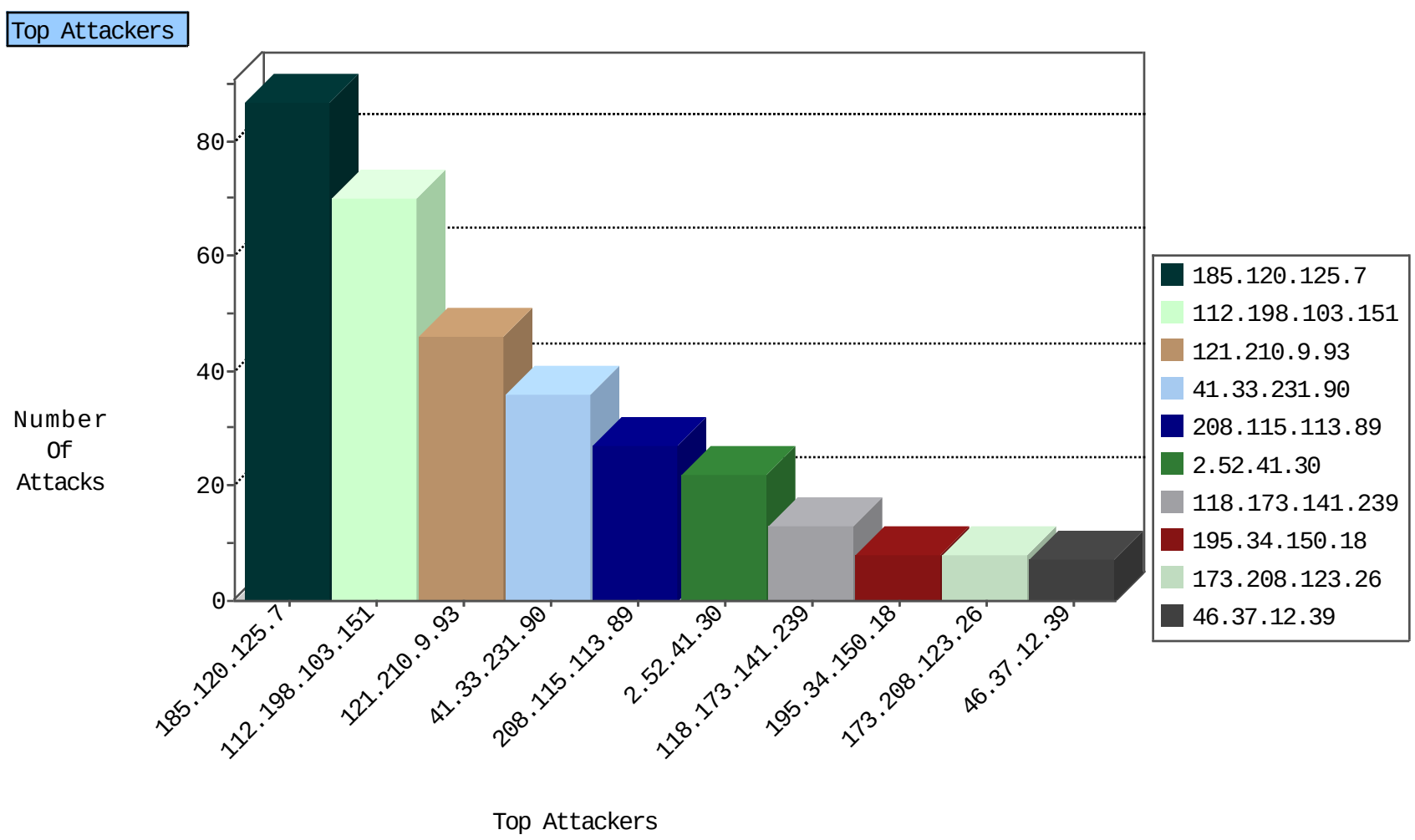
02-01-2016-05:04:09 to 02-01-2016-06:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-01-2016-05:04:09 to 02-01-2016-06:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
121.210.9.93	Australia	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	129
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	6
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	5
212.179.54.237	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
50.206.89.77	United States	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	2
183.60.48.25	China	147.237.76.201	e.atal.idf.il	JLM_Under_Attack_Con_Tcp	drop	2

02-01-2016-05:04:09 to 02-01-2016-06:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.63.108.252	Spain	147.237.77.74	law.idf.il	0527: HTTP: formmail.pl Access	Block	1
212.63.108.252	Spain	147.237.77.74	law.idf.il	3885: HTTP: PHP File Include Exploit	Block	1

02-01-2016-05:04:09 to 02-01-2016-06:04:09

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
183.60.48.25	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
36.72.228.72	147.237.76.42	Indonesia	refuah.idf.il	ET SCAN NMAP -sS window 4096	1
36.72.228.72	147.237.76.42	Indonesia	refuah.idf.il	ET SCAN NMAP -f -sS	1
183.60.48.25	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.76.86	China	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
36.72.228.72	147.237.76.42	Indonesia	refuah.idf.il	ET SCAN NMAP -sS window 2048	1

02-01-2016-05:04:09 to 02-01-2016-06:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
185.120.125.7		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	58
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
112.198.103.151	Philippines	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	31
185.120.125.7		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	29
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	17
118.173.141.239	Thailand	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
173.208.123.26	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
121.210.9.93	Australia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.176.55.13	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
208.115.113.89	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	5
208.115.113.89	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	5
91.200.12.143	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
64.233.172.179	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
91.200.12.106	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
37.247.36.74	Netherlands	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
172.58.17.106	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
91.200.12.136	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
46.19.85.162	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
130.193.37.16	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
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
2.54.153.237	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.6	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.187.6	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
71.6.165.200	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
74.82.47.47	United States	147.237.0.35	akaws.idf.il	drop		drop	1
184.105.139.102	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
37.26.147.133	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
217.148.45.113	United Kingdom	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
74.82.47.10	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
176.13.21.149	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.220.215.81	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
216.218.206.107	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
64.233.172.155	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
184.105.247.200	United States	147.237.0.33	idf.il	drop		drop	1
37.142.139.230	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
130.193.50.33	Russian Federation	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
74.82.47.11	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
45.79.168.168		147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
184.105.139.67	United States	147.237.76.39	mobile.meitav.idf.i	drop	SAM rule	drop	1
216.218.206.118	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.251	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.142.139.230	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
149.88.239.130	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
109.253.193.249	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
74.82.47.18	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.75	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
5.22.135.144	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

02-01-2016-05:04:09 to 02-01-2016-06:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.52.41.30	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	17
46.19.85.17	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
112.198.103.151	Philippines	147.237.72.166	aka.idf.il	Distributed Abnormally Long Request	Block	4
112.198.103.151	Philippines	147.237.72.166	aka.idf.il	Distributed Unknown HTTP Request Method	Block	4
112.198.103.151	Philippines	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Header Name	Block	4
112.198.103.151	Philippines	147.237.72.166	aka.idf.il	Distributed Malformed URL	Block	4
112.198.103.151	Philippines	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Method	Block	4
112.198.103.151	Philippines	147.237.72.166	aka.idf.il	Distributed NULL Character in Header Name	Block	4
46.19.86.213	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.37.12.39	Italy	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.37.12.39	Block	3
112.198.103.151	Philippines	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Header Value	Block	3
2.52.41.30	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	3
112.198.103.151	Philippines	147.237.72.166	aka.idf.il	Distributed NULL Character in Method	Block	2
2.52.41.30	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
112.198.103.151	Philippines	147.237.72.166	aka.idf.il	Distributed Malformed HTTP Header Line	Block	2
5.29.164.247	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.37.12.39	Italy	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	2
112.198.103.151	Philippines	147.237.72.166	aka.idf.il	Distributed Abnormally Long Header Line	Block	2
112.198.103.151	Philippines	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
66.249.65.37	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
191.232.136.8	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/null	Block	1
2.52.56.210	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1
204.13.201.138	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
77.40.129.123	Norway	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
125.212.121.13	Philippines	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
112.198.103.151	Philippines	147.237.72.166	aka.idf.il	Distributed Illegal HTTP Version	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.78.187	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
192.99.41.217	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
2.52.56.210	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
204.13.201.138	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
77.40.129.123	Norway	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
125.212.121.13	Philippines	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
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
66.249.79.202	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
195.254.135.76	Romania	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
112.198.103.151	Philippines	147.237.72.166	aka.idf.il	Illegal URL Path Encoding ×§c[[#4]]Ö³coÂ¬h-58jÃš×• ^u,/i[[#20]]×?×£•6%[[#12]]Ã›×´×ƒm 7Â?×šÂ±6×“Æ’Â§ÃŸe[[#25]]1Âž×•=Ö¹g[[#0]]Ö²ÃŸâ„¢Ã›/tÃ·Â¸.hw	Block	1
77.127.23.26	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/idkunpratimishiyim.aspx	Block	1
162.243.175.201	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
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	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
204.13.201.137	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
112.198.103.151	Philippines	147.237.72.166	aka.idf.il	NULL Character in URL ×§c[[#4]]Ö³coÂ¬h-58jÃš×• ^u,/i[[#20]]×?×£•6%[[#12]]Ã›×´×ƒm 7Â?×šÂ±6×“Æ’Â§ÃŸe[[#25]]1Âž×•=Ö¹g[[#0]]Ö²ÃŸâ„¢Ã›/tÃ·Â¸.hw	Block	1
36.2.9.139	Japan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	Block	1
54.243.53.148	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1283-12386-en/dover.aspx	Block	1
173.252.90.90	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.229.173	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
204.13.201.137	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22638-he/dover.aspx.	Block	1
112.198.103.151	Philippines	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1

02-01-2016-05:04:09 to 02-01-2016-06:04:09