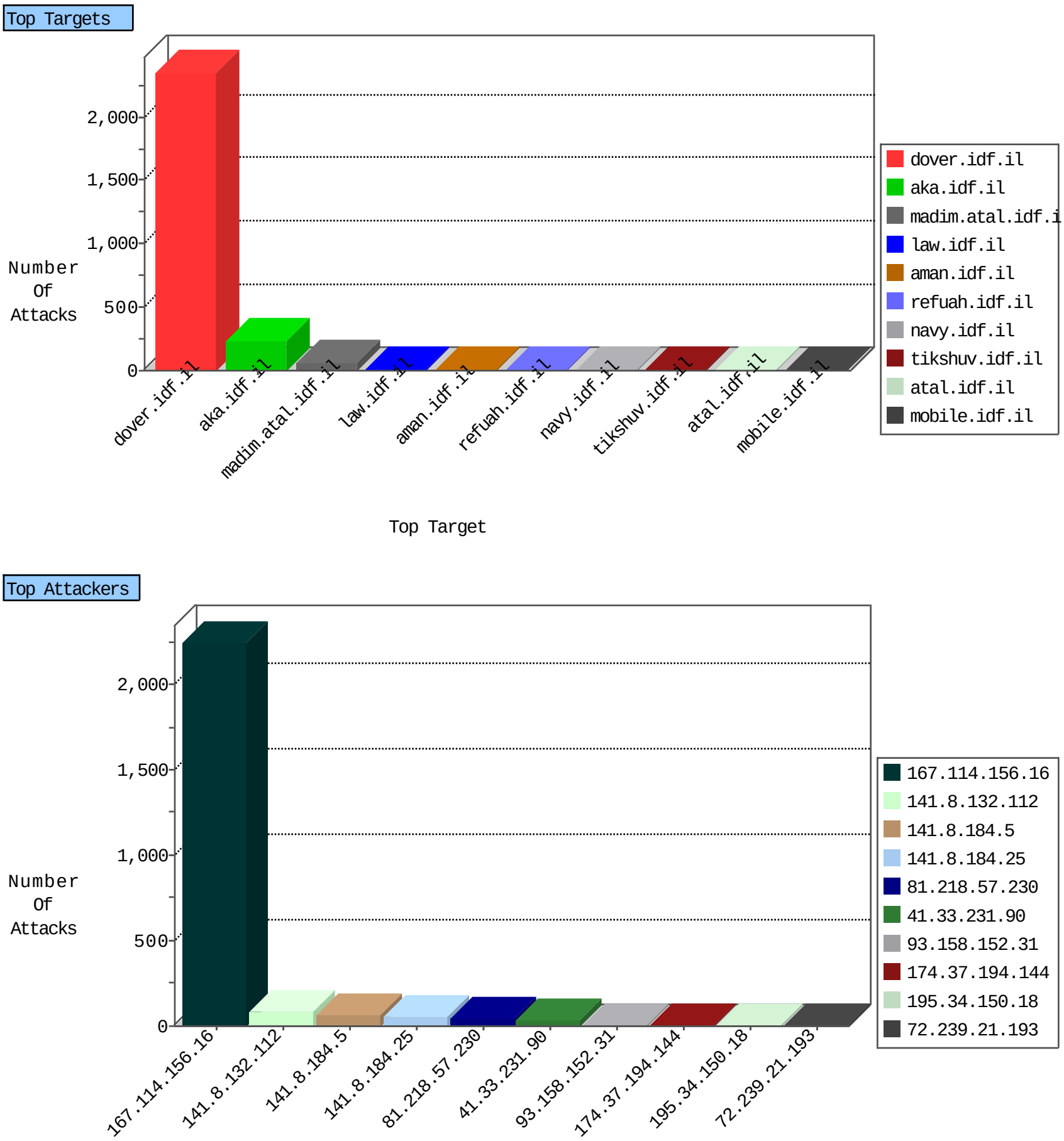
01-21-2016-03:04:01 to 01-21-2016-04:04:01

IDF Under Attack Daily Report



01-21-2016-03:04:01 to 01-21-2016-04:04:01

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	3143
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
42.112.10.81	Vietnam	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	1
42.112.10.66	Vietnam	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	1
42.112.10.74	Vietnam	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	1
42.112.10.87	Vietnam	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	1
42.112.10.68	Vietnam	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	1
42.112.10.75	Vietnam	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	1
23.95.54.18	United States	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
42.112.10.92	Vietnam	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	1
42.112.10.70	Vietnam	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	1
42.112.10.80	Vietnam	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	1
42.112.10.65	Vietnam	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	1
42.112.10.73	Vietnam	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	1

01-21-2016-03:04:01 to 01-21-2016-04:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-21-2016-03:04:01 to 01-21-2016-04:04:01

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
174.37.194.144	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
201.173.72.4	147.237.77.74	Mexico	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
103.7.12.5	147.237.0.19	Indonesia	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
93.174.93.17	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
78.46.218.161	147.237.77.216	Germany	dover.idf.il	Tehila - Perl LWP with fake user agent	1
46.161.40.120	147.237.77.212	Russian Federation	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
212.179.227.181	147.237.77.205	Israel	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.13.173	147.237.76.86	United Kingdom	navy.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
93.85.93.3	147.237.0.15	Belarus	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
46.161.40.120	147.237.77.234	Russian Federation	halag.idf.il	ET SCAN NMAP -sS window 1024	1

01-21-2016-03:04:01 to 01-21-2016-04:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	81
141.8.184.5	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	66
141.8.184.25	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	51
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
93.158.152.31	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	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
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
79.178.109.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
197.47.107.52	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.66.15	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
65.8.86.65	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
77.77.76.3	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
172.58.137.234	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
8.37.227.81	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	2
37.46.39.225	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
174.37.194.144	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	2
91.200.12.136	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
207.46.13.108	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
37.46.39.250	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
207.46.13.108	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
65.8.86.65	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
174.37.194.144	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.203	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.168.152.9	United States	147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
54.176.17.88	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.62.155.52	Russian Federation	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
141.212.122.199	United States	147.237.8.46	e.chinuch.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
94.230.95.115	Israel	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
207.237.82.50	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
65.8.86.65	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
174.37.194.144	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.204	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.199	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
104.128.144.131	Canada	147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
208.115.111.68	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
65.8.86.65	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
174.37.194.144	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.19.85.85	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.206	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
81.169.237.146	Germany	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	1
63.143.229.176	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
174.37.194.144	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.202	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
107.85.106.12	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.85	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.207	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.57.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
37.26.146.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
199.30.16.175	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
91.143.80.201	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
79.178.204.23	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
207.232.55.134	Israel	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
78.46.218.161	Germany	147.237.77.216	dover.idf.il	EXPDB-17602:WordPress-TimThumb-Plugin-RCE	Block	1
184.172.55.140	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/blog/wp-admin/	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1927-he/cogat.aspx	Block	1
46.135.232.255	Czech Republic	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
141.8.184.25	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mail/kapats	Block	1
79.183.148.166	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
72.239.21.193	United States	147.237.76.86	navy.idf.il	NULL Character in Header Name at Ã.Âˆ Â?fÂ¬Ã°Âª[[#2]]Â?[[#4]][Â»Â€Ã¢Â½%$[[#11]]l[[#20]][[#0]]Â¢0=Ãž Â£[[#12]][[#16]][8Ã«Ã„Ã˜\Ãº	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/faq.aspx	Block	1
178.17.174.99	Moldova, Republic of	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
78.46.218.161	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-content/themes/estore/timthumb.php "deals of the day"	Block	1
195.62.53.168	Russian Federation	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to /admin/login	Block	1
72.239.21.193	United States	147.237.76.86	navy.idf.il	Illegal Byte Code Character in Header Name Ã.Âˆ Â?fÂ¬Ã°Âª[[#2]]Â?[[#4]][Â»Â€Ã¢Â½%$[[#11]]l[[#20]][[#0]]Â¢0=Ãž Â£[[#12]][[#16]][8Ã«Ã„Ã˜\Ãº	Block	1
50.62.161.29	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
142.4.213.25	Canada	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
79.183.148.166	Israel	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
72.239.21.193	United States	147.237.76.86	navy.idf.il	NULL Character in Method Â,[[#0]][[#0]][[#0]][[#22]]Â¡	Block	1
199.116.253.200	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
182.50.151.12	Singapore	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
66.249.78.235	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 5cf35968 in aka.idf.il/news/	None	1
104.128.144.131	Canada	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/redirect.php	Block	1
196.22.132.203	South Africa	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
72.239.21.193	United States	147.237.76.86	navy.idf.il	Illegal Byte Code Character in Header Value	Block	1
50.62.161.29	United States	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
150.70.173.52	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
72.239.21.193	United States	147.237.76.86	navy.idf.il	Unknown HTTP Request Method Â,[[#0]][[#0]][[#0]][[#22]]Â¡ in URL	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
182.50.151.12	Singapore	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
66.249.79.75	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
79.183.148.166	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed PHP Attempt	Block	1
72.239.21.193	United States	147.237.76.86	navy.idf.il	Illegal Byte Code Character in Method Â,[[#0]][[#0]][[#0]][[#22]]Â¡	Block	1
196.22.132.203	South Africa	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
50.62.177.130	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	Block	1
150.70.173.53	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
91.72.142.163	United Arab Emirates	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
77.247.181.165	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
207.232.55.134	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
184.168.46.19	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1379-he/dover.aspx	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
46.135.232.255	Czech Republic	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
79.183.148.166	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/xmlrpc.php	Block	1
72.239.21.193	United States	147.237.76.86	navy.idf.il	Malformed URL	Block	1