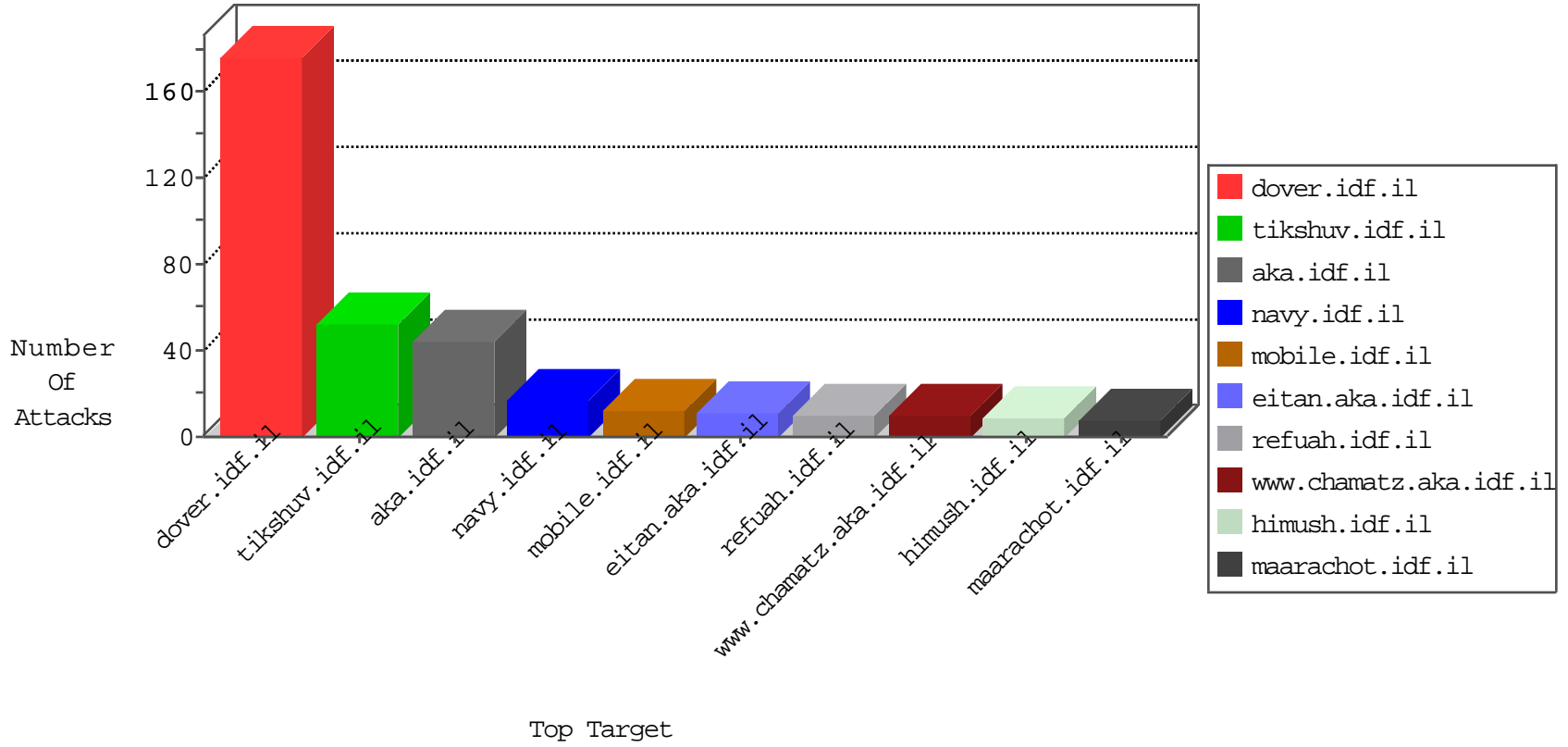


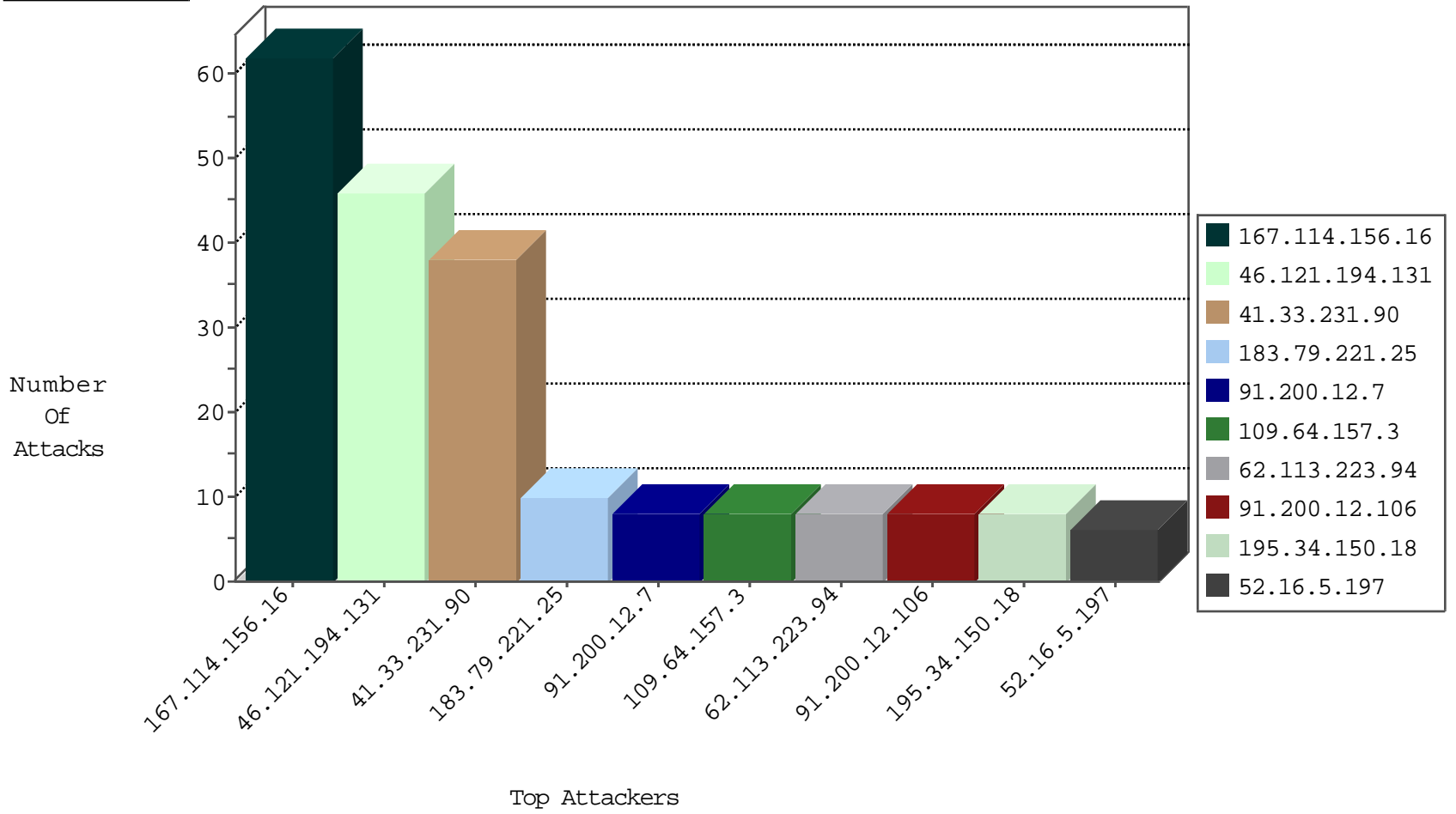
IDF Under Attack Daily Report



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	1315
92.247.181.29	Bulgaria	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
115.239.228.10	China	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Http	drop	2
119.47.101.121	Japan	147.237.76.147	chiruch.aka.idf.il	Block_Udp_All_Nets	drop	2
204.42.253.132	United States	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
66.240.192.138	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
31.148.220.74	Netherlands	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
204.42.253.132	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
89.248.174.4	Netherlands	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
31.148.220.74	Netherlands	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1

01-09-2016-03:04:07 to 01-09-2016-04:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
104.45.132.180	United States	147.237.77.216	dover.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	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
66.249.78.9	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
168.62.238.153	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
112.5.236.194	147.237.8.27	China	e.madim.atal.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
93.174.93.203	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
46.151.53.196	147.237.77.170	Ukraine	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
190.7.56.194	147.237.0.19	Argentina	madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
158.255.2.52	147.237.77.216	Russian Federation	dover.idf.il	ET SCAN NMAP -sS window 1024	1
104.128.144.131	147.237.76.196	Canada	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
183.79.221.25	Japan	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
109.64.157.3	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.86.229	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.168.91.234	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
91.200.12.106	Ukraine	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	4
65.55.210.141	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
199.30.25.226	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
91.200.12.7	Ukraine	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
91.200.12.7	Ukraine	147.237.77.226	www.chamatz.aka.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
91.200.12.106	Ukraine	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
79.176.162.49	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.157.34	Israel	147.237.72.166	aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
174.103.92.62	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
178.154.189.204	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.217.187.39	Poland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
149.88.164.15	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
199.30.24.182	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
91.200.12.143	Ukraine	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
109.253.141.6	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
192.243.55.131	Dominica	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
23.25.105.137	United States	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
91.200.12.143	Ukraine	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	2
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
2.52.169.175	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
95.187.205.15	Saudi Arabia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
2.54.157.71	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
104.45.18.178	United States	147.237.77.216	dover.idf.il	Instant Messengers	instant messenger pattern found, application: Skype	monitor	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
24.50.100.36	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
92.247.181.29	Bulgaria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
78.128.40.89	Bulgaria	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
141.212.122.156	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
62.113.223.94	Germany	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
109.66.101.240	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
94.102.51.30	Netherlands	147.237.0.19	madim.atal.idf.il	drop	SAM rule	drop	1
184.105.247.212	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
8.37.231.58	Anonymous Proxy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
62.113.223.94	Germany	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
128.61.240.118	United States	147.237.76.148	ggcenter.aka.idf.il	drop		drop	1
52.16.5.197	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
104.130.78.65	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
93.174.93.203	Netherlands	147.237.0.17	m.my-kosher-kravi.idf.il	drop	SAM rule	drop	1
180.76.15.153	China	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.156	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
62.113.223.94	Germany	147.237.76.86	navy.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
46.121.194.131	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 46.121.194.131	Block	46
37.142.228.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.67.157.34	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	3
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	2
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
184.168.200.28	United States	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
66.147.244.243	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
149.78.87.186	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gius	Block	1
104.232.3.33		147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/./shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
207.46.13.188	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/i/related_users/45666182	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
192.243.55.138	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/general	Block	1
174.19.217.7	United States	147.237.76.42	refuah.idf.il	Malformed URL	Block	1
46.166.190.138	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
131.253.25.181	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized HTTP Method	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
79.181.55.225	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.131	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/size100x0/2427.jpg	Block	1
184.168.200.28	United States	147.237.77.170	maarachot.idf.il	Distributed Unauthorized URL Access on www.maarachot.idf.il/xmlrpc.php	Block	1
40.77.167.42	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
157.55.39.2	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/Ã-â€-Ã-Ã-Ã-â„ çÃ-â€-Ã-â€?	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
69.195.106.239	United States	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
195.64.164.134	France	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
174.19.217.7	United States	147.237.76.42	refuah.idf.il	NULL Character in Method Ã-[[#0]][[#0]][[#0]]A&ç	Block	1
50.62.176.229	United States	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
17.138.59.136	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/apple-app-site-association	Block	1
131.253.25.181	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/i/jot	Block	1
207.46.13.121	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
80.246.133.81	Israel	147.237.77.176	matpash.idf.il	Suspicious Response Code	Block	1
66.249.69.38	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.69.38	Block	1
192.243.55.131	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/kadatz	Block	1
40.77.167.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/user/js.php	Block	1
174.19.217.7	United States	147.237.76.42	refuah.idf.il	Abnormally Long Header Line request header name	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
195.64.164.134	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
69.195.106.239	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/xmlrpc.php	Block	1
174.19.217.7	United States	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method Ã-[[#0]][[#0]][[#0]]A&ç in URL	Block	1
50.62.176.229	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/xmlrpc.php	Block	1
17.138.60.156	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/apple-app-site-association	Block	1
141.0.23.8	Germany	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
207.46.13.157	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.157	Block	1
91.92.198.5	Bulgaria	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
66.249.69.46	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.69.46	Block	1
192.243.55.135	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?docid=64966	Block	1
174.19.217.7	United States	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in Header Name	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
198.154.225.251	United States	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
71.210.247.162	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
184.105.139.68	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1