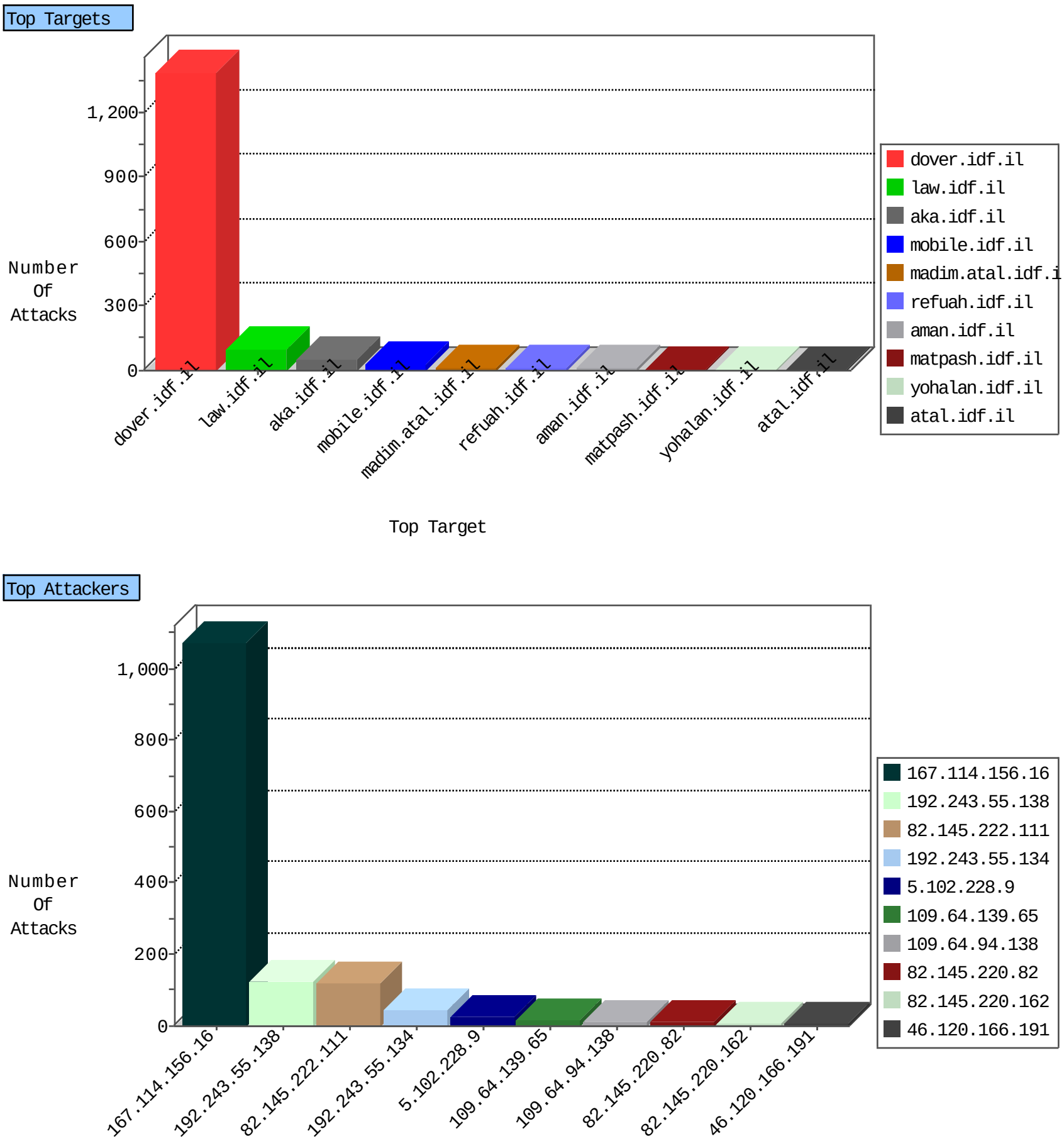
03-12-2016-00:04:07 to 03-12-2016-01:04:07

IDF Under Attack Daily Report



03-12-2016-00:04:07 to 03-12-2016-01:04:07

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	3677
82.145.222.111	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	120
82.145.220.82	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	10
82.145.220.162	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	9
82.145.221.54	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	5
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
94.102.49.206	Netherlands	147.237.0.35	akaws.idf.il	Block_Ntp_All_Net	drop	1
192.243.55.138	Dominica	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1
94.102.49.206	Netherlands	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
217.23.205.97	Bosnia and Herzegovina	147.237.77.19	law-forum.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.0.16	my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1

03-12-2016-00:04:07 to 03-12-2016-01:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.120.173.118	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
207.46.13.70	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-12-2016-00:04:07 to 03-12-2016-01:04:07

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
59.45.79.117	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
41.140.253.9	147.237.0.16	Morocco	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
218.246.0.97	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
31.184.195.114	147.237.77.233	Russian Federation	atal.idf.il	ET SCAN Potential SSH Scan	1
210.117.121.60	147.237.76.34	Korea, Republic of	yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
31.184.195.114	147.237.77.178	Russian Federation	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
31.184.195.114	147.237.77.74	Russian Federation	law.idf.il	ET SCAN Potential SSH Scan	1
185.72.179.221	147.237.77.205		prisha.idf.il	ET SCAN NMAP -sS window 1024	1
31.184.195.114	147.237.8.50	Russian Federation	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.194	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
1.52.59.143	147.237.77.170	Vietnam	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
41.140.253.9	147.237.0.16	Morocco	my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
210.117.121.60	147.237.76.34	Korea, Republic of	yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
31.184.195.114	147.237.77.226	Russian Federation	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
210.117.121.60	147.237.76.34	Korea, Republic of	yohalan.idf.il	ET SCAN NMAP -f -sS	1
31.184.195.114	147.237.77.176	Russian Federation	matpash.idf.il	ET SCAN Potential SSH Scan	1
185.106.92.65	147.237.0.34		tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
31.184.195.114	147.237.72.166	Russian Federation	aka.idf.il	ET SCAN Potential SSH Scan	1
178.63.11.208	147.237.76.199	Germany	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
1.52.59.143	147.237.77.170	Vietnam	maarachot.idf.il	ET SCAN NMAP -sS window 3072	1
59.45.79.117	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1

03-12-2016-00:04:07 to 03-12-2016-01:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
192.243.55.138	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
109.64.139.65	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
192.243.55.138	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	15
192.243.55.138	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	15
192.243.55.138	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
192.243.55.138	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.120.166.191	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
79.178.36.198	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
156.204.77.180		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.138	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	6
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.138	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	6
85.64.97.230	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	6
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
126.205.84.174	Japan	147.237.77.176	matpash.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
192.243.55.134	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
5.102.228.9	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.134	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	3
149.78.243.197	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.130.3	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
41.100.95.2	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.64.198.177	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
79.179.225.143	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
109.67.192.196	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.81.48.126	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.56.79	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.2.221	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
213.8.204.2	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
213.8.204.2	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
176.13.11.39	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
89.163.148.58	Germany	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
41.100.95.2	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
141.212.122.172	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
109.253.212.58	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
101.182.94.41	Australia	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
166.175.57.110	United States	147.237.77.216	dover.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
5.102.228.9	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	12
109.64.94.138	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/'	Block	11
5.102.228.9	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 5.102.228.9	Block	9
46.19.86.57	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
82.80.27.121	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
5.102.228.9	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
212.106.71.1	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	2
65.55.210.218	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
194.72.238.241	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xyzzy	Block	1
157.55.2.172	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	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
205.160.241.251	United States	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in Method ¬[[#0]][[#0]][[#0]]A¢	Block	1
37.54.96.72	Ukraine	147.237.77.216	dover.idf.il	Parameter Type Violation l in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
157.55.39.134	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/giyus/leshakot/default.asp	None	1
66.249.65.241	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/modules/forums.frm/frmprintmessage.aspx	Block	1
198.58.102.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
157.55.2.187	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1108-he/nakhal.aspx	Block	1
205.160.241.251	United States	147.237.76.42	refuah.idf.il	Malformed URL	Block	1
176.13.11.39	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
87.71.145.164	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.73.129	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
31.168.31.178	Israel	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	1
199.30.24.99	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
157.55.12.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
77.38.32.182	Slovenia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
205.160.241.251	United States	147.237.76.42	refuah.idf.il	NULL Character in Method ¬[[#0]][[#0]][[#0]]A¢	Block	1
65.55.210.57	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
186.101.55.178	Ecuador	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.54.57.98	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.79.218	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
31.168.31.178	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/xmlrpc.php	Block	1
205.160.241.251	United States	147.237.76.42	refuah.idf.il	Abnormally Long Header Line request header name	Block	1
157.55.12.78	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
77.38.32.182	Slovenia	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
205.160.241.251	United States	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method ¬[[#0]][[#0]][[#0]]A¢ in URL	Block	1
65.55.210.209	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-19239-en/dover.aspx http:/digg.com/submit	Block	1
141.212.122.160	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
66.249.79.225	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/0/310.pdf	Block	1
37.54.96.72	Ukraine	147.237.77.216	dover.idf.il	Parameter Type Violation f in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
205.160.241.251	United States	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in Header Name	Block	1
157.55.39.93	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
79.178.36.198	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
207.46.13.37	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-14886-en/dover.aspx	Block	1

03-12-2016-00:04:07 to 03-12-2016-01:04:07