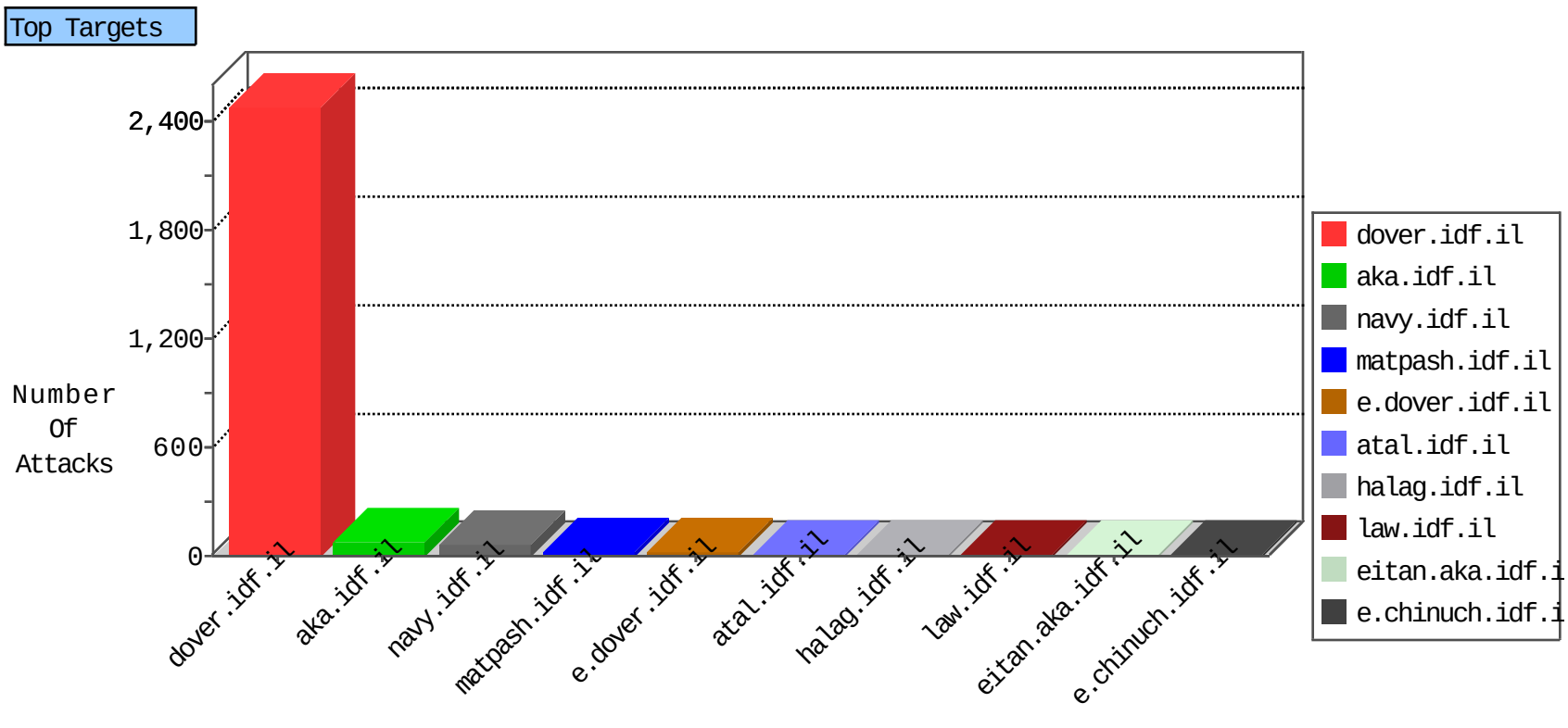
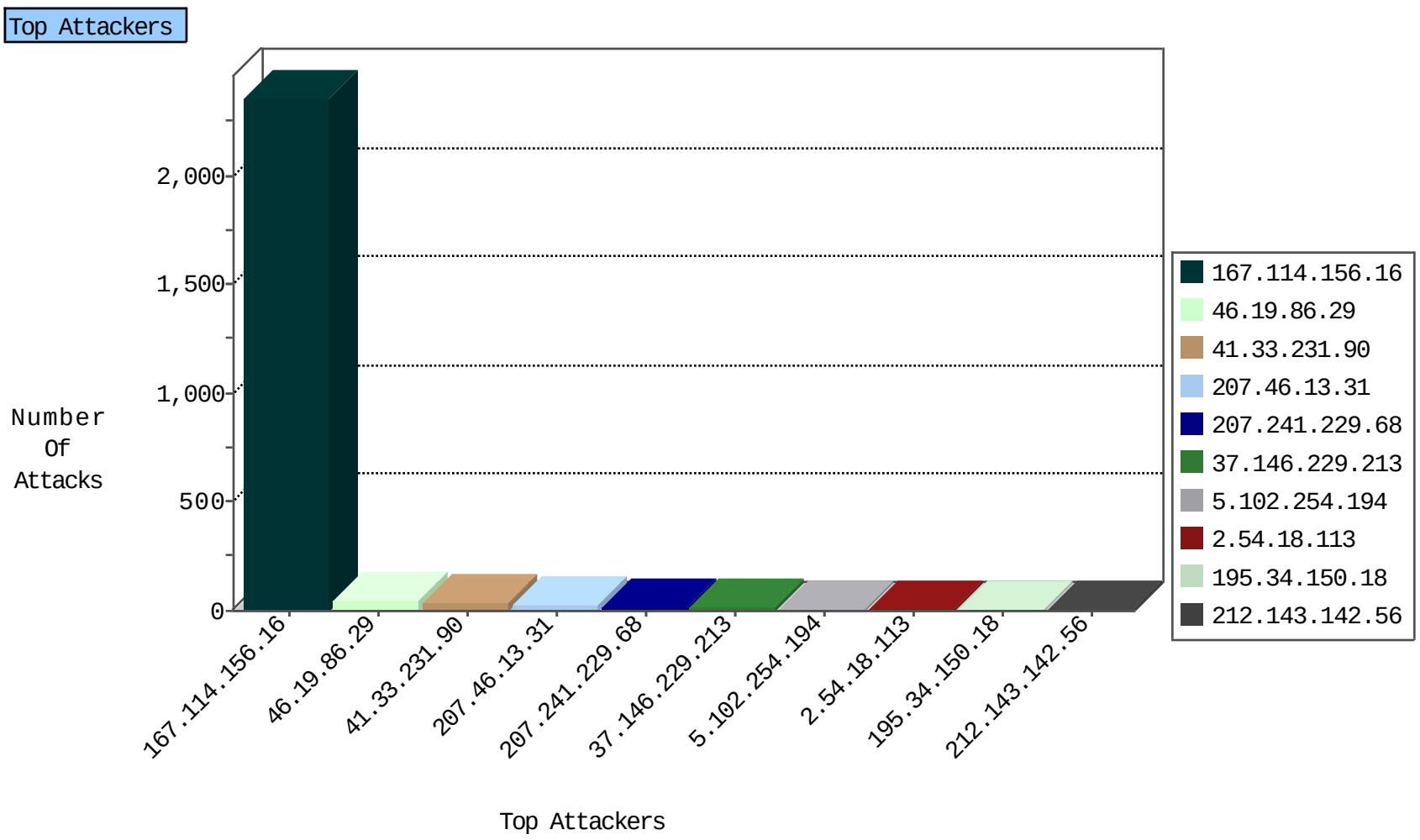
12-19-2015-08:04:05 to 12-19-2015-09:04:05

IDF Under Attack Daily Report





12-19-2015-08:04:05 to 12-19-2015-09:04:05

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	3402
81.218.169.64	Israel	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1

12-19-2015-08:04:05 to 12-19-2015-09:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-19-2015-08:04:05 to 12-19-2015-09:04:05

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
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
131.109.15.15	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -f -sS	1
94.102.60.89	147.237.72.217	Netherlands	e.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.60.89	147.237.8.27	Netherlands	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
61.244.49.137	147.237.0.35	Hong Kong	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.21.196	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
134.213.133.4	147.237.77.234	United Kingdom	halag.idf.il	ET SCAN NMAP -sS window 4096	1
134.213.133.4	147.237.77.234	United Kingdom	halag.idf.il	ET SCAN NMAP -f -sS	1
131.109.15.15	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 2048	1
125.65.165.215	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
94.102.60.89	147.237.8.28	Netherlands	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
5.39.222.253	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
134.213.133.4	147.237.77.234	United Kingdom	halag.idf.il	ET SCAN NMAP -sS window 2048	1
131.109.15.15	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 3072	1

12-19-2015-08:04:05 to 12-19-2015-09:04:05

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	34
46.19.86.29	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	22
207.46.13.31	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	21
207.241.229.68	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	18
37.146.229.213	Russian Federation	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	16
46.19.86.29	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
2.54.18.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.76	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
176.107.10.154	Russian Federation	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
5.102.254.194	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.29	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	4
84.109.5.33	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.29	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.86.29	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	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
5.102.254.194	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
92.96.74.124	United Arab Emirates	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
109.66.97.154	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.247	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	3
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
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
40.77.167.105	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
208.115.113.89	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
208.115.111.73	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
95.38.61.199	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
95.38.61.199	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
2.52.36.188	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
184.105.247.212	United States	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
146.185.239.102	Russian Federation	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
45.79.87.95		147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
92.96.74.124	United Arab Emirates	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
79.180.48.155	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.19.86.247	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.87	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
99.244.46.3	Canada	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
2.52.36.188	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.34	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.216	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.4.109.148	Germany	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
212.28.230.202	Lebanon	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
5.144.131.170	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
84.94.22.193	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.86.247	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.139.88	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
99.244.46.3	Canada	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

12-19-2015-08:04:05 to 12-19-2015-09:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
207.46.13.143	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 207.46.13.143	Block	4
40.77.167.38	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/online/webresource.axd	Block	3
207.46.13.11	United States	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/online/webresource.axd	Block	3
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	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
192.117.101.225	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
192.69.255.198	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.69.255.198	Block	2
157.55.39.162	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/general.aspx	Block	1
77.38.32.182	Slovenia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
207.46.13.131	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/count.asp	Block	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1086-13893-en/dover.aspx	Block	1
5.102.254.194	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
192.69.255.198	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	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
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter sOpenLinkIn in www.aka.idf.il/eitan/pratim/pirteychayal/	None	1
40.77.167.105	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
192.171.243.203	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1395-en/dover.aspx','_self')	Block	1
176.13.6.57	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
77.237.138.51	Czech Republic	147.237.77.234	halag.idf.il	Unauthorized URL Access to /	Block	1
66.249.69.40	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19412-he/idfgdover.aspx	Block	1
31.168.197.86	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
192.69.255.217	United States	147.237.77.216	dover.idf.il	Parameter Type Violation Language in www.idf.il/shared/ajax/getemergencybanner.aspx	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
46.116.233.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage	Block	1
185.32.179.159	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.182.217.137	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
207.46.13.143	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1035-he/csshandler.ashx	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
37.26.148.214	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.117	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/3/size100x0/2413.jpg	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
66.102.9.91	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
192.69.255.193	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.69.255.193	Block	1
104.131.215.64	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/14-he	Block	1
207.46.13.190	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/robots.txt	Block	1
66.249.78.104	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
192.171.243.154	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1008-en/navmenu.aspx'	Block	1
157.55.39.160	United States	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/online/webresource.axd	Block	1
77.38.32.182	Slovenia	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	Block	1
5.29.234.82	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	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
66.249.78.111	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	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
40.77.167.73	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
192.171.243.203	United States	147.237.77.216	dover.idf.il	Parameter Type Violation lang in www.idf.il/templates/navmenu/navmenu.css.aspx	Block	1

12-19-2015-08:04:05 to 12-19-2015-09:04:05