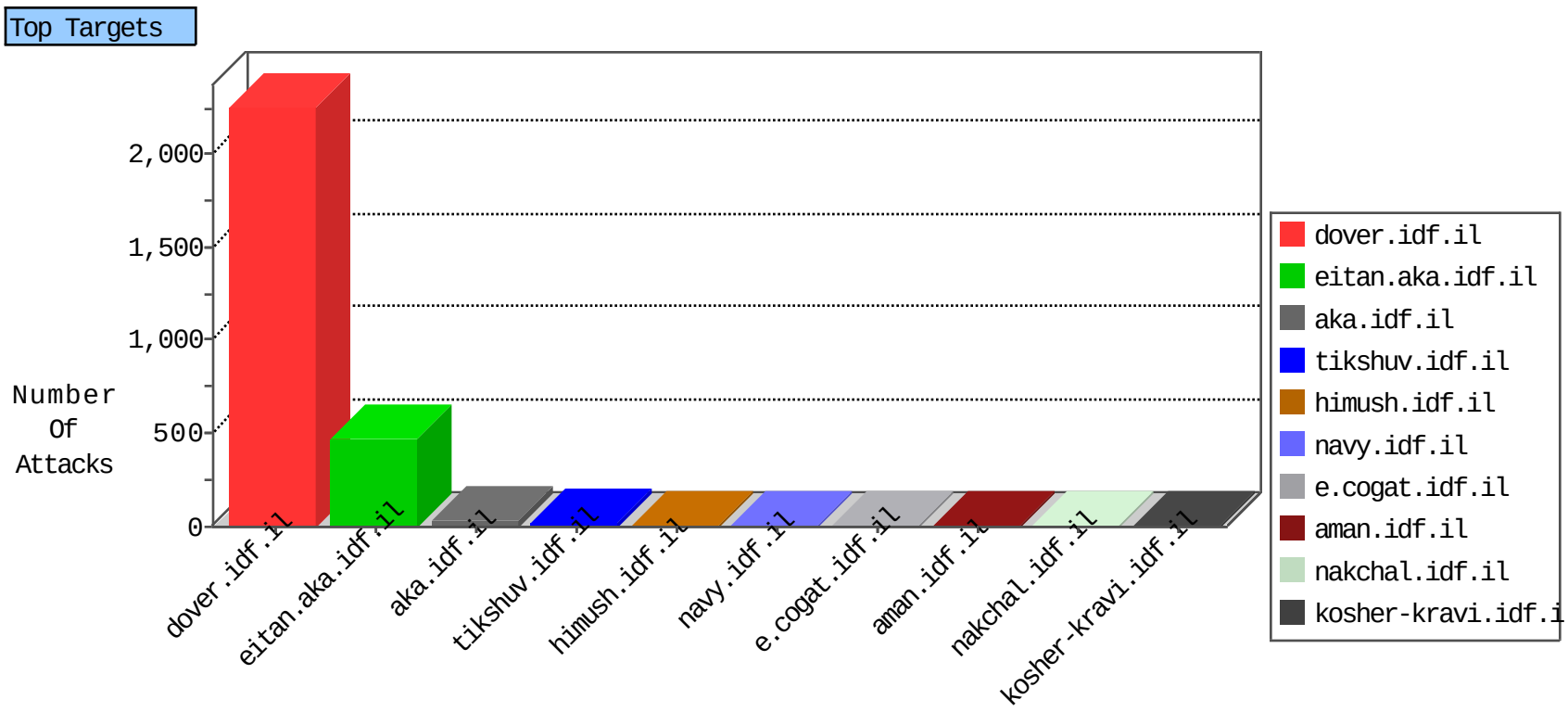
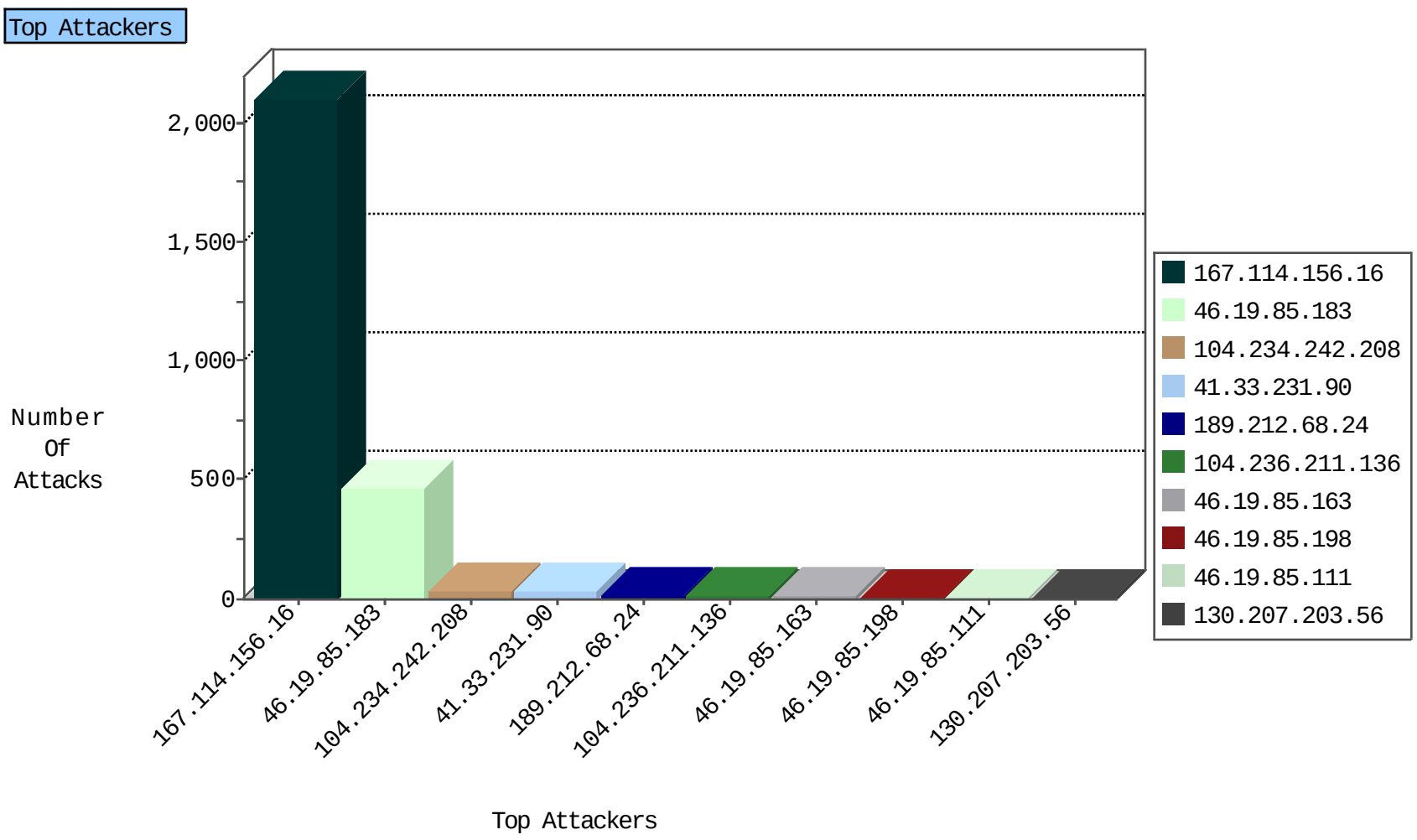
12-18-2015-06:04:06 to 12-18-2015-07:04:06

IDF Under Attack Daily Report





12-18-2015-06:04:06 to 12-18-2015-07:04:06

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	3230
66.249.69.93	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	451
66.249.78.146	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	218
204.42.253.2	United States	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	2
190.236.194.53	Peru	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
190.236.194.53	Peru	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
115.182.21.40	China	147.237.76.30	himush.idf.il	L4 Source or Dest Port Zero	drop	1

12-18-2015-06:04:06 to 12-18-2015-07:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.154	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

12-18-2015-06:04:06 to 12-18-2015-07:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
189.212.68.24	147.237.72.156	Mexico	aman.idf.il	ET SCAN Potential SSH Scan	3
189.212.68.24	147.237.0.33	Mexico	idf.il	ET SCAN Potential SSH Scan	2
66.249.75.201	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
189.212.68.24	147.237.76.196	Mexico	e.sviva.idf.il	ET SCAN Potential SSH Scan	2
79.182.124.60	147.237.72.156	Israel	aman.idf.il	ET SCAN NMAP -sA (2)	2
189.212.68.24	147.237.8.24	Mexico	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
189.212.68.24	147.237.0.16	Mexico	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
112.196.49.101	147.237.76.30	India	himush.idf.il	ET SCAN NMAP -sS window 4096	1
94.102.48.195	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
189.212.68.24	147.237.8.50	Mexico	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
189.212.68.24	147.237.0.34	Mexico	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
189.212.68.24	147.237.0.17	Mexico	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
116.233.79.200	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
112.196.49.101	147.237.76.30	India	himush.idf.il	ET SCAN NMAP -sS window 3072	1
37.143.82.50	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
189.212.68.24	147.237.76.201	Mexico	e.atal.idf.il	ET SCAN Potential SSH Scan	1

12-18-2015-06:04:06 to 12-18-2015-07:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
46.19.85.183	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	429
104.234.242.208		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
104.236.211.136		147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.198	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
205.252.110.19	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.163	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
130.207.203.56	United States	147.237.77.61	e.cogat.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	6
84.110.83.244	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.163	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.111	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.111	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
91.200.12.106	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
46.19.85.22	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.22.193	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
46.19.86.56	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	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
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
101.226.166.244	China	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
157.55.39.194	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
40.77.167.7	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
68.65.120.48		147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
180.97.106.162	China	147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	1
141.212.122.127	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
125.206.236.61	Japan	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
82.221.105.6	Iceland	147.237.8.27	e.madim.atal.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.89.217.225		147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
180.97.106.37	China	147.237.0.19	madim.atal.idf.il	drop	SAM rule	drop	1
141.212.122.116	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.89.217.234		147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
74.82.47.34	United States	147.237.0.33	idf.il	drop		drop	1
184.105.139.82	United States	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.56	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
46.19.85.24	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.89.217.227		147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
68.65.120.48		147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
180.97.106.37	China	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	1
141.212.122.117	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.89.217.235		147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
74.82.47.38	United States	147.237.76.148	gqcenter.aka.idf.i	drop		drop	1
184.105.139.103	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.86.192	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.121.181	United States	147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.17.111.245	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.89.217.231		147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
68.65.120.48		147.237.0.19	madim.atal.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
46.19.85.183	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.183	Block	38
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
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
77.237.138.51	Czech Republic	147.237.77.234	halag.idf.il	Unauthorized URL Access to /	Block	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19372-he/idfgdover.aspx	Block	1
40.77.167.39	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/tizmoret/klali/default.asp	None	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
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international-training	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
66.249.66.136	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8718-he/refuah.aspx	Block	1
141.212.122.112	United States	147.237.0.34	tikshuv.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
91.145.144.112	Poland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.69.40	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19396-he/idfgdover.aspx	Block	1
40.77.167.45	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
207.46.13.169	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/feeds/posts/default/-/artikel kesehatan	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
68.180.229.31	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/templates/shared/usercontrols/headerupper/	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
66.249.69.2	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
157.55.39.194	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.194	Block	1
96.250.109.35	United States	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to www.kosher-kravi.idf.il/sip_storage/files/3/1773.jpg	Block	1
66.249.69.77	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/news/news.aspx	Block	1
207.46.13.169	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/smalim/faq.aspx	None	1
46.19.85.183	Israel	147.237.76.200	eitan.aka.idf.il	Too Many 404: Response Code per Session	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
68.180.229.239	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gyuis	Block	1
173.252.90.110	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
101.226.166.244	China	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.111	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
207.46.13.169	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/chamatz/miktzoa/default.asp	None	1
109.64.1.183	Israel	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
68.180.230.244	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/movies/strike_heb2.asf	Block	1
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	1
104.236.211.136		147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/894-he/tikshuv.aspxshared/usercontrols/headerupper/	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
207.46.13.180	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/jom2.5/materialy-2.feed	Block	1
66.249.66.131	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/3208.pdf	Block	1
109.64.1.183	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/xmlrpc.php	Block	1

12-18-2015-06:04:06 to 12-18-2015-07:04:06