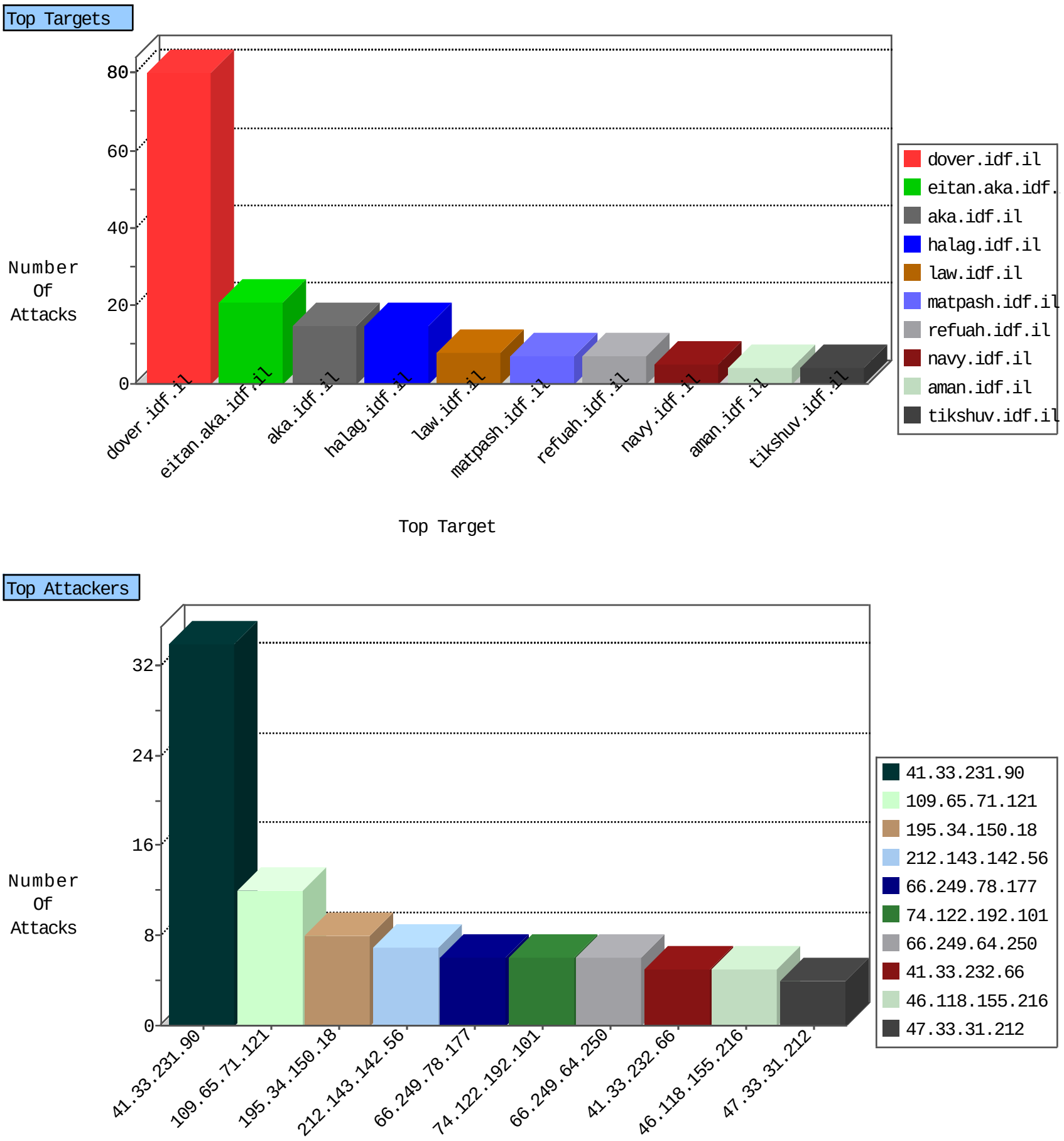
02-12-2016-05:04:01 to 02-12-2016-06:04:01

IDF Under Attack Daily Report



02-12-2016-05:04:01 to 02-12-2016-06:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
142.54.160.211	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	drop	1
185.35.62.164	Switzerland	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
185.35.62.166	Switzerland	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.200		147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1

02-12-2016-05:04:01 to 02-12-2016-06:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.120.173.159	China	147.237.77.233	atal.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

02-12-2016-05:04:01 to 02-12-2016-06:04:01

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
91.201.236.114	147.237.76.44	Ukraine	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
74.122.192.101	147.237.76.196	United States	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
74.122.192.101	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
74.122.192.101	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.77.74	China	law.idf.il	ET SCAN NMAP -sS window 1024	1
1.54.210.107	147.237.77.234	Vietnam	halag.idf.il	ET SCAN NMAP -sS window 4096	1
193.105.134.220	147.237.8.14	Sweden	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
168.63.200.101	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
115.236.75.201	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
74.122.192.101	147.237.76.201	United States	e.atal.idf.il	ET SCAN Potential SSH Scan	1
74.122.192.101	147.237.76.86	United States	navy.idf.il	ET SCAN Potential SSH Scan	1
74.122.192.101	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential SSH Scan	1
14.113.221.50	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
198.20.69.74	147.237.77.19	United States	law-forum.idf.il	ET DROP Dshield Block Listed Source	1
1.54.210.107	147.237.77.234	Vietnam	halag.idf.il	ET SCAN NMAP -sS window 3072	1
193.105.134.220	147.237.76.200	Sweden	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
168.63.200.101	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
168.63.200.101	147.237.76.30	United States	himush.idf.il	ET SCAN Potential SSH Scan	1

02-12-2016-05:04:01 to 02-12-2016-06:04:01

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
109.65.71.121	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
66.249.64.250	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.78.177	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	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
47.33.31.212	Canada	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	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
173.183.52.172	Canada	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
66.249.64.139	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
130.203.136.75	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
212.143.76.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.127.193.91	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
157.55.39.92	United States	147.237.0.15	kosher-kravi.idf.il	drop	SAM rule	drop	3
94.159.178.5	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
31.168.206.96	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
208.115.113.89	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.77	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.249.64.133	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
74.82.47.30	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.239	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.114	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.128	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
2.54.133.206	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
216.218.206.96	United States	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
198.1.101.123	United States	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
37.187.114.171	France	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.143	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.69	United States	147.237.77.61	e.cogat.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.36	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.231	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
2.54.133.206	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.128	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
122.3.152.159	Philippines	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
198.20.69.74	United States	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
154.103.202.214	Sudan	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
141.212.122.70	United States	147.237.77.61	e.cogat.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.239	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
2.54.173.133	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP anomaly detected	Non-compliant TCP packets coming from multiple external sources were detected. This may result from potential network configuration problem.	drop	1
141.212.122.129	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
123.125.71.106	China	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
201.141.15.185	Mexico	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
66.249.85.170	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.75	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.74	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

02-12-2016-05:04:01 to 02-12-2016-06:04:01

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
141.212.122.137	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
124.124.48.38	India	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.19	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
208.115.113.89	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
41.218.223.38	Ghana	147.237.77.216	dover.idf.il	Header Rejection	header rejection pattern found in request	monitor	1

02-12-2016-05:04:01 to 02-12-2016-06:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.118.155.216	Ukraine	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	2
92.240.253.126	Slovakia	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/wp-admin/	Block	1
41.218.223.38	Ghana	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
218.65.149.155	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 218.65.149.155	Block	1
157.55.39.66	United States	147.237.72.166	aka.idf.il	Unknown Parameter 136cd360 in www.aka.idf.il/main/home/default.aspx	None	1
66.249.64.191	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
37.142.68.19	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
213.8.204.18	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
93.115.108.210	Romania	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/test/wp-admin/	Block	1
46.118.155.216	Ukraine	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1
218.65.149.155	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/u+	Block	1
157.55.39.209	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/toolfs.asp	Block	1
66.249.66.136	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/2401.jpg	Block	1
40.77.167.17	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/robots.txt	Block	1
213.8.204.18	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/xmlrpc.php	Block	1
142.167.135.21	Canada	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
46.118.155.216	Ukraine	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on www.refua.atal.idf.il/xmlrpc.php	Block	1
198.20.69.74	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-he/cogat.aspx	Block	1
40.77.167.32	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/chamatz/kurs/default.asp	None	1
213.8.204.18	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
142.167.135.21	Canada	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
207.46.13.31	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.31	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
41.218.223.38	Ghana	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1
213.8.204.18	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
157.55.39.39	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_pictures.asp	Block	1
46.118.155.216	Ukraine	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/blog/	Block	1
37.142.68.19	Israel	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
207.46.13.31	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/trajector/	Block	1

02-12-2016-05:04:01 to 02-12-2016-06:04:01