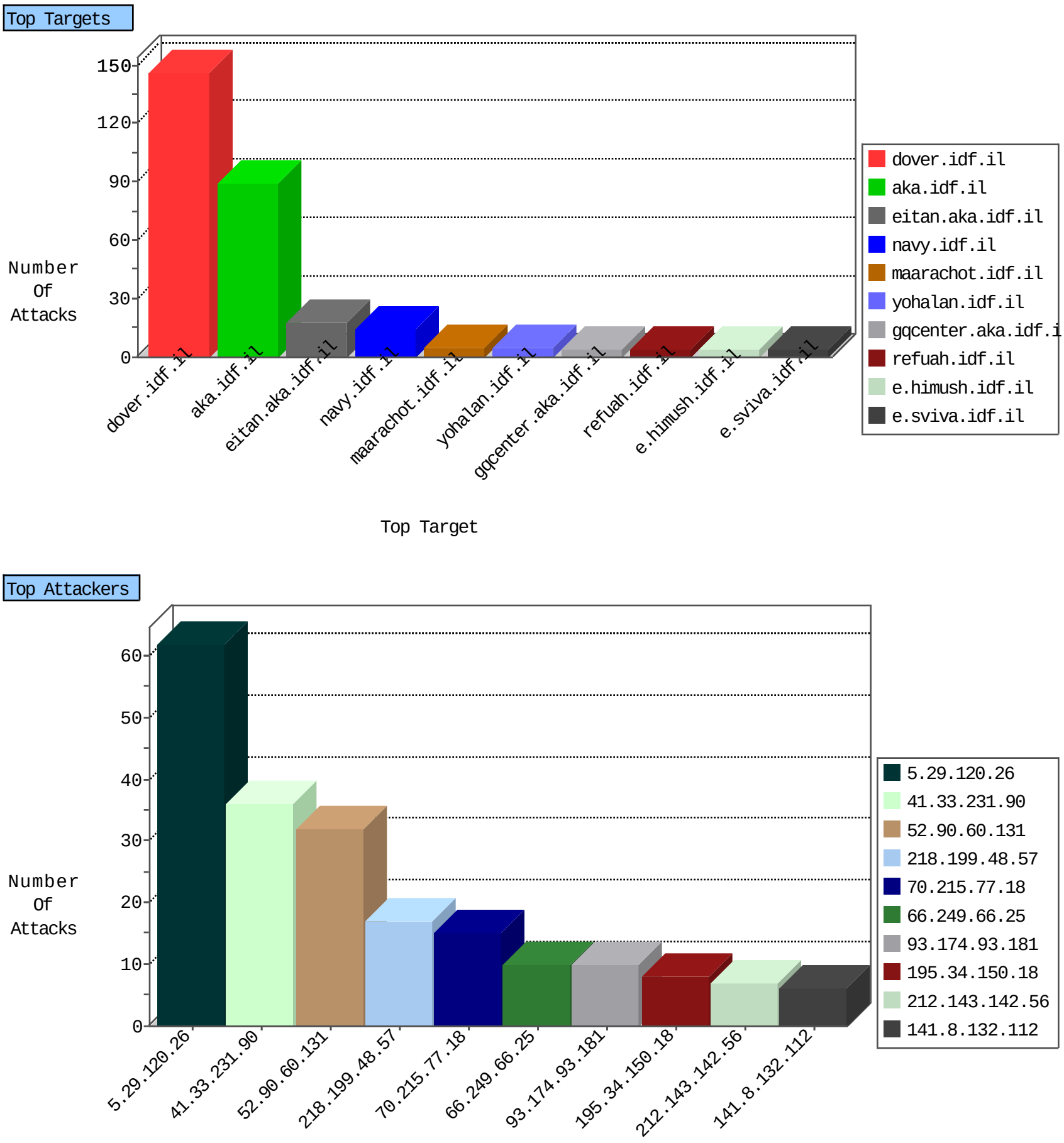
02-15-2016-05:04:01 to 02-15-2016-06:04:01

IDF Under Attack
Daily Report



02-15-2016-05:04:01 to 02-15-2016-06:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.54.237	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
68.116.5.134	United States	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	2
123.151.42.61	China	147.237.76.30	himush.idf.il	Block_Udp_All_Nets_Con_Limit	drop	1
185.130.5.224		147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1

02-15-2016-05:04:01 to 02-15-2016-06:04:01

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
151.80.31.132	Italy	147.237.72.166	aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1

02-15-2016-05:04:01 to 02-15-2016-06:04:01

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
218.199.48.57	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.181	147.237.77.176	Netherlands	matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.199.48.57	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.181	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.199.48.57	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.181	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.77.121	China	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
218.199.48.57	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.181	147.237.0.33	Netherlands	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.199.48.57	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.98	147.237.76.30	United States	himush.idf.il	ET DROP Dshield Block Listed Source	1
93.174.93.181	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
218.199.48.57	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
115.236.75.201	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
218.199.48.57	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
115.214.71.31	147.237.76.197	China	e.himush.idf.il	ET SCAN NMAP -sS window 2048	1
218.199.48.57	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
94.102.51.30	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
218.199.48.57	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.181	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.199.48.57	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.181	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.199.48.57	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.181	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.199.48.57	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.181	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.246.0.97	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
218.199.48.57	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.181	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.199.48.57	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
218.199.48.57	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
93.113.125.11	147.237.76.34	Romania	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
115.214.71.31	147.237.76.197	China	e.himush.idf.il	ET SCAN NMAP -sS window 3072	1
218.199.48.57	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
115.214.71.31	147.237.76.197	China	e.himush.idf.il	ET SCAN NMAP -f -sS	1
218.199.48.57	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
94.102.51.30	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN Potential SSH Scan	1

02-15-2016-05:04:01 to 02-15-2016-06:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.29.120.26	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	62
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
52.90.60.131	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	32
70.215.77.18	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.66.3	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
157.55.39.238	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
103.50.11.142		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
54.241.198.78	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
52.49.79.6	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
66.249.66.60	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
54.151.42.39	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
2.54.17.61	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.184.5	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.18.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.134.144	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.66.134	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.86.157	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
23.96.208.137	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
66.249.66.63	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
184.105.247.216	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.145	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
109.186.129.58	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
2.52.178.98	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
75.131.101.103	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.155	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
93.113.125.11	Romania	147.237.76.198	e.yohalan.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.247.216	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.116.6.24	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.146	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
109.186.129.58	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
195.60.232.57	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
75.131.101.103	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
93.113.125.11	Romania	147.237.76.199	e.nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
74.82.47.26	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.220	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.153	United States	147.237.0.33	idf.il	drop		drop	1
122.201.19.100	Mongolia	147.237.77.216	dover.idf.il	Header Rejection	header rejection pattern found in request	monitor	1
176.106.40.172	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
141.212.122.116	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
93.113.125.11	Romania	147.237.76.201	e.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
74.82.47.43	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.247	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.154	United States	147.237.0.33	idf.il	drop		drop	1
2.54.36.140	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
128.232.110.28	United Kingdom	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
93.113.125.11	Romania	147.237.76.34	yohalan.idf.il	drop		drop	1

02-15-2016-05:04:01 to 02-15-2016-06:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.25	Block	7
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
109.253.204.209	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
66.102.8.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
91.206.110.69	Ukraine	147.237.77.216	dover.idf.il	Parameter Type Violation f in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
66.249.66.21	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
122.201.19.100	Mongolia	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
37.142.68.19	Israel	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
180.180.170.91	Thailand	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
91.206.110.69	Ukraine	147.237.77.216	dover.idf.il	Parameter Type Violation l in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
157.55.39.73	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
67.222.134.19	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/test/wp-admin/	Block	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
180.180.170.91	Thailand	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
98.130.0.140	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/blog/wp-admin/	Block	1
157.55.39.105	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	Parameter Type Violation PageNum in www.idf.il/1115-ar/dover.aspx	Block	1
64.71.32.30	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp-admin/	Block	1
184.154.225.3	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wordpress/wp-admin/	Block	1
66.249.66.40	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19666-he/idfgdover.aspx	Block	1
173.252.79.116	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.178.62.21	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	1
207.46.13.111	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
122.201.19.100	Mongolia	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1
23.254.201.89	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp/wp-admin/	Block	1
173.252.114.117	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1

02-15-2016-05:04:01 to 02-15-2016-06:04:01