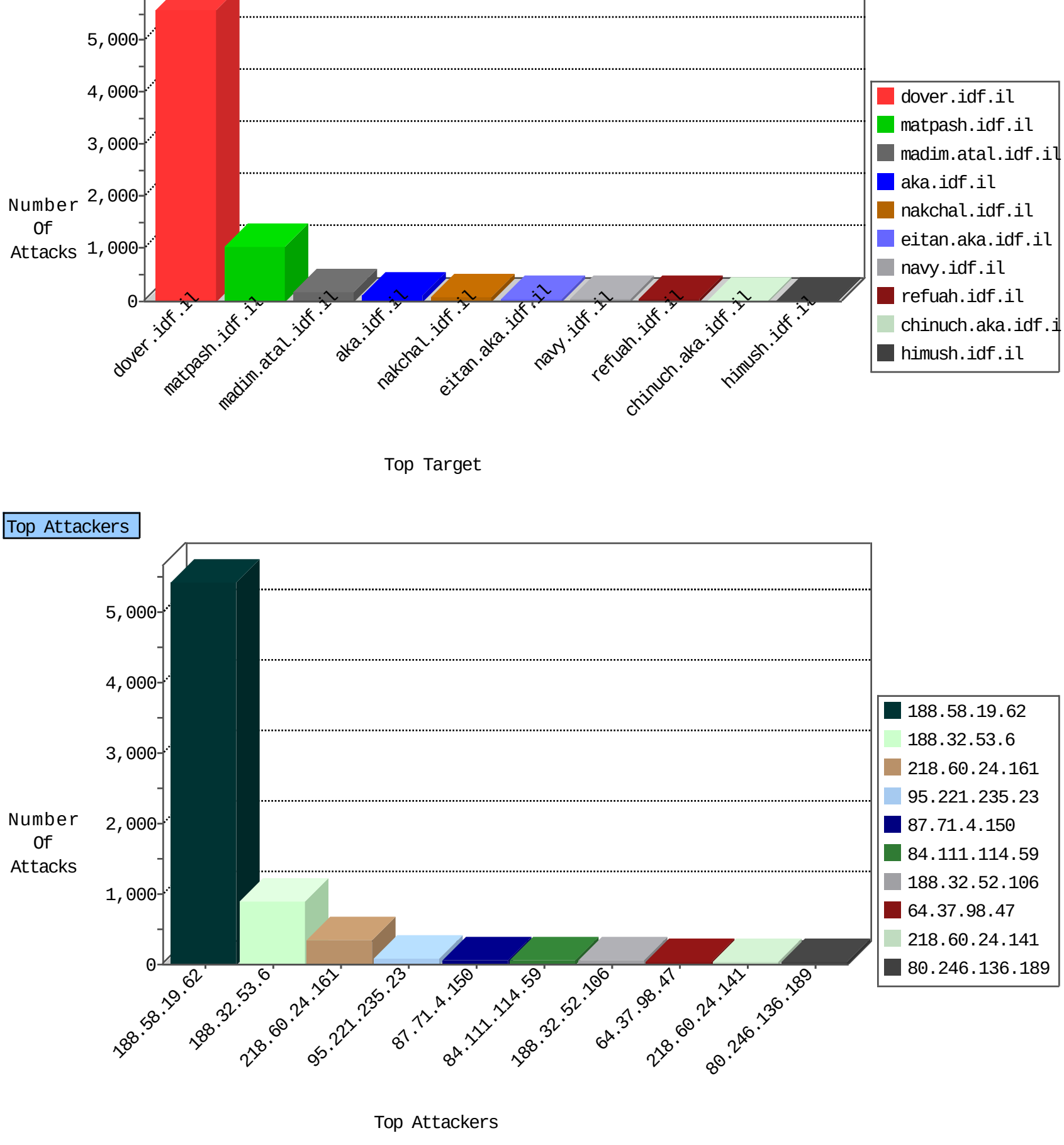
09-07-2016-07:04:03 to 09-07-2016-08:04:03

IDF Under Attack Daily Report



09-07-2016-07:04:03 to 09-07-2016-08:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.51.68	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	247
115.230.125.146	China	147.237.77.61	e.cogat.idf.il	JLM_Purple_Con_Limit_Http	drop	1
115.230.125.146	China	147.237.77.226	www.chamatz.aka.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
66.240.236.119	United States	147.237.76.177	ncore.idf.il	Black List	drop	1
93.158.203.199	Netherlands	147.237.76.42	refuah.idf.il	Black List	drop	1

09-07-2016-07:04:03 to 09-07-2016-08:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
162.210.196.129	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3

09-07-2016-07:04:03 to 09-07-2016-08:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	14
77.126.80.246	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	2
84.93.84.77	147.237.77.74	United Kingdom	law.idf.il	Tehila - Perl LWP with fake user agent	2
66.249.66.10	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	1
46.120.122.219	147.237.77.170	Israel	maarachot.idf.il	Xenu Link Sleuth User Agent	1
142.54.191.210	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 4096	1
42.112.28.187	147.237.8.27	Vietnam	e.madim.atal.idf.i	ET SCAN NMAP -sS window 1024	1
142.54.191.210	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -f -sS	1
104.232.98.38	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
104.232.98.38	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -f -sS	1
94.102.48.195	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.66.191	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	1
161.10.17.156	147.237.0.33	Colombia	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.120.122.219	147.237.77.74	Israel	law.idf.il	Xenu Link Sleuth User Agent	1
142.54.191.210	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 2048	1
116.7.243.198	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 1024	1
104.232.98.38	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.93.139	147.237.77.233	Europe	atal.idf.il	ET SCAN NMAP -sA (2)	1

09-07-2016-07:04:03 to 09-07-2016-08:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
188.58.19.62	Turkey	147.237.77.216	dover.idf.il	drop	SAM rule	drop	5430
188.32.53.6	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	903
95.221.235.23	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	86
188.32.52.106	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	53
218.60.24.161	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	25
218.60.24.161	China	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	24
107.167.112.18	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	23
218.60.24.161	China	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	22
218.60.24.161	China	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
82.145.220.219	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	19
218.60.24.161	China	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
218.60.24.161	China	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	18
218.60.24.161	China	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
175.100.61.185	Cambodia	147.237.77.216	dover.idf.il	Header Rejection	header rejection pattern found in request	monitor	14
218.60.24.161	China	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
218.60.24.161	China	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
218.60.24.161	China	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
218.60.24.161	China	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.86.120	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
218.60.24.161	China	147.237.76.200	eitan.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	6
80.246.136.189	Israel	147.237.72.166	aka.idf.il	drop		drop	6
80.246.136.189	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.86.120	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
218.60.24.161	China	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
218.60.24.161	China	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
218.60.24.161	China	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
218.60.24.161	China	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
218.60.24.161	China	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
218.60.24.161	China	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
218.60.24.161	China	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
80.246.136.189	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
218.60.24.161	China	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
80.246.136.189	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
218.60.24.161	China	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
218.60.24.161	China	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	5
218.60.24.161	China	147.237.76.200	eitan.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	5
218.60.24.161	China	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
80.246.136.189	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
80.246.136.189	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
66.249.93.139	Europe	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.86.110	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
213.8.84.204	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.55.17.111	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
64.37.98.47	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
218.60.24.161	China	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
218.60.24.161	China	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	4
37.247.36.115	Netherlands	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
218.60.24.141	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
218.60.24.161	China	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
2.54.195.198	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3

09-07-2016-07:04:03 to 09-07-2016-08:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.71.4.150	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	68
84.111.114.59	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	62
134.191.232.69	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	14
134.191.232.69	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 134.191.232.69	Block	13
176.13.227.36	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	7
185.32.179.208	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
37.26.147.249	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.149.135	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
80.246.139.253	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
24.87.137.101	Canada	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 24.87.137.101	Block	2
212.179.28.34	Israel	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	2
176.13.247.77	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
207.46.13.111	United States	147.237.72.166	aka.idf.il	Unknown Parameter 4f9c0c80 in www.aka.idf.il/main/home/default.aspx	None	1
144.76.96.81	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
2.54.195.198	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
109.173.70.137	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
2.53.1.192	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
212.179.28.34	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 212.179.28.34	Block	1
148.251.2.180	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/miluim/templates/inner.asp	Block	1
87.68.34.182	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
188.32.230.241	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
46.4.74.42	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
2.53.51.68	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 2.53.51.68	Block	1
24.87.137.101	Canada	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	1
204.79.180.198	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/portalmiluim/templates/inner.asp	Block	1
46.19.85.10	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
2.53.51.68	Israel	147.237.72.166	aka.idf.il	Unknown Parameter d in www.aka.idf.il/main/giyus/general.aspx	None	1
212.179.28.34	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/5/	Block	1
95.221.248.220	Russian Federation	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
37.26.146.254	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/images/1.he/infocenteritem/	Block	1
207.46.13.93	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
134.191.232.69	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/2/	Block	1
2.53.167.174	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
183.160.115.123	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1956-he/cogat.aspx/trackback/	Block	1
109.66.161.98	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1

09-07-2016-07:04:03 to 09-07-2016-08:04:03