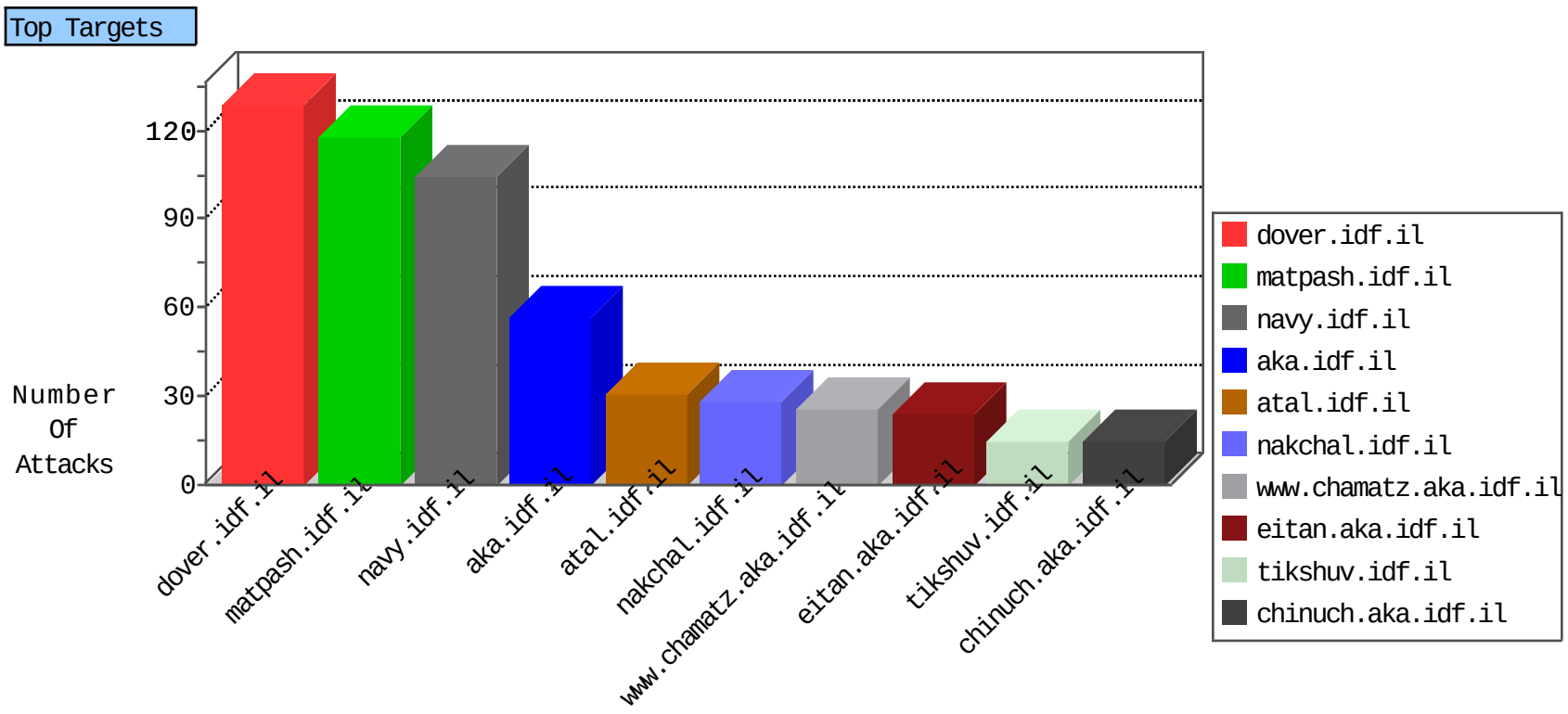
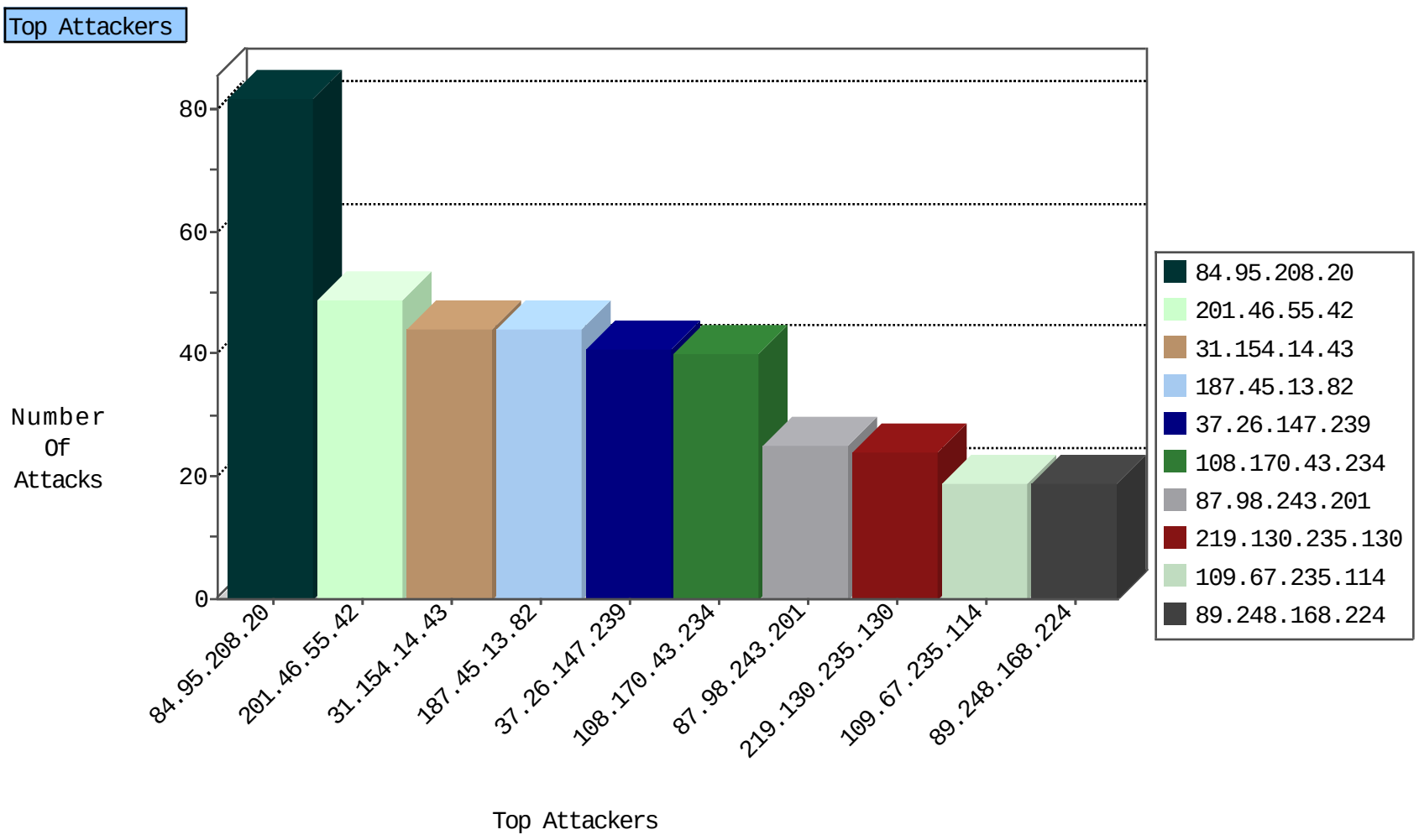
09-10-2016-09:04:08 to 09-10-2016-10:04:08

IDF Under Attack
Daily Report





09-10-2016-09:04:08 to 09-10-2016-10:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
107.189.45.32	United States	147.237.76.199	e.nakchal.idf.il	Black List	drop	1
107.189.45.32	United States	147.237.76.202	e.halag.idf.il	Black List	drop	1

09-10-2016-09:04:08 to 09-10-2016-10:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-10-2016-09:04:08 to 09-10-2016-10:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
211.20.51.57	147.237.77.205	Taiwan	prisha.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
116.12.175.233	147.237.76.30	Singapore	himush.idf.il	ET SCAN NMAP -f -sS	1
202.21.110.212	147.237.0.200	Mongolia	m4u.idf.il	ET SCAN NMAP -sS window 3072	1
78.46.43.18	147.237.77.170	Germany	maarachot.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
176.47.117.79	147.237.77.176	Saudi Arabia	matpash.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
69.24.208.162	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.129.15	147.237.77.216	United Kingdom	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
50.84.213.146	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -sS window 2048	1
163.172.129.15	147.237.77.205	United Kingdom	prisha.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.227.67.158	147.237.0.200	Sweden	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.129.15	147.237.77.121	United Kingdom	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
23.92.20.154	147.237.76.34	United States	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
211.20.51.57	147.237.76.202	Taiwan	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
163.172.129.15	147.237.77.61	United Kingdom	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
211.20.51.57	147.237.76.147	Taiwan	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
139.162.160.132	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
211.20.51.57	147.237.72.217	Taiwan	e.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
116.12.175.233	147.237.76.30	Singapore	himush.idf.il	ET SCAN NMAP -sS window 2048	1
211.20.51.57	147.237.0.15	Taiwan	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.232.98.38	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 1024	1
202.21.110.212	147.237.0.200	Mongolia	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
69.24.208.162	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.129.15	147.237.77.243	United Kingdom	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
50.84.213.146	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -sS window 4096	1
163.172.129.15	147.237.77.216	United Kingdom	dover.idf.il	ET SCAN NMAP -sS window 1024	1
211.20.51.57	147.237.77.234	Taiwan	halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
50.84.213.146	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -f -sS	1
163.172.129.15	147.237.77.179	United Kingdom	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
46.161.40.17	147.237.8.28	Russian Federation	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
211.20.51.57	147.237.77.178	Taiwan	e.matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
163.172.129.15	147.237.77.61	United Kingdom	e.cogat.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
211.20.51.57	147.237.76.196	Taiwan	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
163.172.129.15	147.237.77.19	United Kingdom	law-forum.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
211.20.51.57	147.237.76.31	Taiwan	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
116.12.175.233	147.237.76.30	Singapore	himush.idf.il	ET SCAN NMAP -sS window 4096	1
211.20.51.57	147.237.72.166	Taiwan	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

09-10-2016-09:04:08 to 09-10-2016-10:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
31.154.14.43	Israel	147.237.77.176	matpash.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	44
91.141.2.117	Austria	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	19
77.42.252.199	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
89.248.168.224	Netherlands	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	14
104.34.143.59	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
109.67.235.114	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
46.243.150.194	Bahrain	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
216.52.148.4	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
46.121.98.249	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
37.26.147.239	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
93.172.130.234	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
216.52.148.4	United States	147.237.76.86	navy.idf.il	SYN Attack		monitor	7
77.42.252.195	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
185.89.217.232	Netherlands	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
185.89.217.234	Netherlands	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
37.26.147.239	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.89.217.235	Netherlands	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
185.89.217.230	Netherlands	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
213.8.204.56	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
109.67.235.114	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
108.170.43.234	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
108.170.43.234	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
108.170.43.234	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
108.170.43.234	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
185.89.217.226	Netherlands	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
37.26.147.239	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
187.45.13.82	Brazil	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
185.89.217.227	Netherlands	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
201.46.55.42	Brazil	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
85.64.122.38	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
201.46.55.42	Brazil	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
108.170.43.234	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
37.26.147.239	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid sequence number	alert	4
37.26.147.239	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
185.89.217.225	Netherlands	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
185.89.217.231	Netherlands	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
201.46.55.42	Brazil	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
37.26.147.239	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
201.46.55.42	Brazil	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
187.45.13.82	Brazil	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
37.26.147.239	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
108.170.43.234	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
187.45.13.82	Brazil	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
108.170.43.234	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
89.248.168.224	Netherlands	147.237.76.86	navy.idf.il	SYN Attack		monitor	3
176.13.235.165	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.126.6.214	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
187.45.13.82	Brazil	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
201.46.55.42	Brazil	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3

09-10-2016-09:04:08 to 09-10-2016-10:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	18
219.130.235.130	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 219.130.235.130	Block	17
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	11
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	7
219.130.235.130	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	6
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	5
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	5
87.71.69.237	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	5
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	4
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
84.95.208.20	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
176.13.235.165	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
87.71.50.98	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in atal.idf.il/1440-he/atal.aspx	Block	2
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
46.19.85.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	PHP Attempt	Block	1
195.154.41.132	France	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to 147.237.76.147/	Block	1
93.172.130.234	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1133-he/atal.aspx	Block	1
66.102.9.2	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
66.249.66.174	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/1/71621.pdf	Block	1
157.55.39.244	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1133-he/atal.aspx	Block	1
84.95.208.20	Israel	147.237.77.234	halag.idf.il	PHP Attempt	Block	1
212.129.62.79	France	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to 147.237.76.200/	Block	1
94.234.170.84	Sweden	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtContent in www.idf.il/1038-en/dover.aspx	Block	1
66.102.9.26	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
66.249.66.177	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/tmuna/	Block	1
172.246.118.178	United States	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	1
85.64.151.237	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
2.53.149.176	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/.здесь	Block	1
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	PHP Attempt	Block	1
109.67.235.114	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
66.249.64.30	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/3044.jpg	Block	1
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/div.item	Block	1
66.249.79.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/tags/tags.aspx	Block	1
172.246.118.178	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/blog/wp-login.php	Block	1
31.154.39.187	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus	Block	1
84.95.208.20	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
109.253.194.237	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
66.249.64.220	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/9/239.doc	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/piwik.php	Block	1
219.130.235.130	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.asp	Block	1
84.95.208.20	Israel	147.237.72.156	aman.idf.il	PHP Attempt	Block	1
66.249.64.224	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/templatecontrols/pictureinfo/pictureinfo.aspx	Block	1
109.253.214.110	Israel	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/894-ar	Block	1
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1

09-10-2016-09:04:08 to 09-10-2016-10:04:08