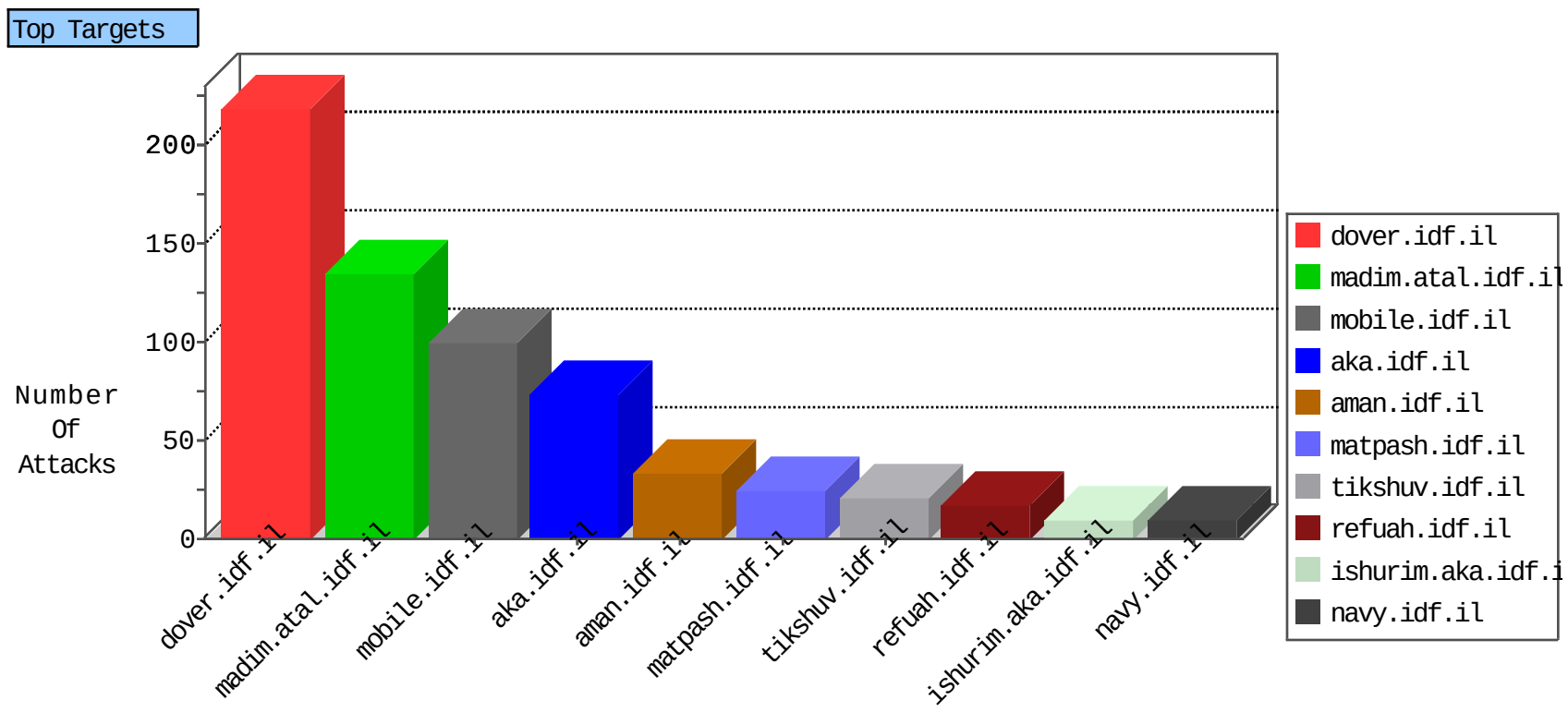
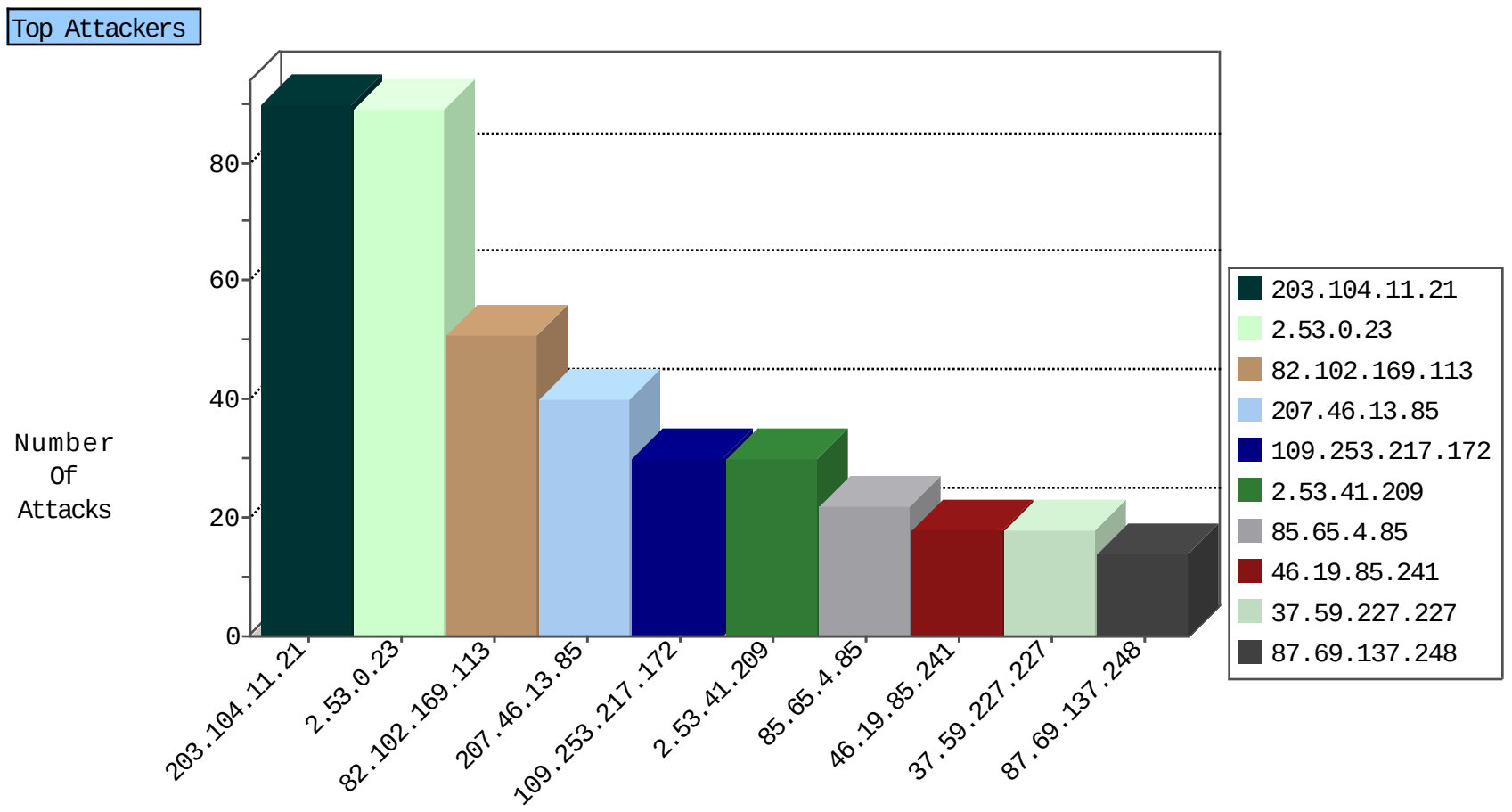
10-05-2016-07:04:01 to 10-05-2016-08:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-05-2016-07:04:01 to 10-05-2016-08:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
195.62.53.168	Russian Federation	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	2
173.208.213.194	United States	147.237.76.86	navy.idf.il	block-sp-traf1	forward	2
204.12.217.2	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	2
69.30.193.254	United States	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	2
66.240.219.146	United States	147.237.76.177	ncore.idf.il	Black List	drop	1
173.208.213.198	United States	147.237.72.166	aka.idf.il	block-sp-traf1	forward	1
82.145.154.60	Sweden	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1
192.187.109.60	United States	147.237.77.176	matpash.idf.il	block-sp-traf1	forward	1
142.54.174.85	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	forward	1

10-05-2016-07:04:01 to 10-05-2016-08:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.59.227.227	France	147.237.77.176	matpash.idf.il	C1000016: HTTP: administrator in URI	Permit	6
209.58.178.49	Singapore	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

10-05-2016-07:04:01 to 10-05-2016-08:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
124.8.223.198	147.237.76.201	Taiwan	e.atal.idf.il	ET SCAN Potential SSH Scan	1
106.75.9.82	147.237.0.19	China	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
124.8.223.198	147.237.76.147	Taiwan	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
103.208.244.223	147.237.76.42		refuah.idf.il	ET SCAN Potential SSH Scan	1
124.8.223.198	147.237.0.17	Taiwan	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
103.208.244.223	147.237.0.35		akaws.idf.il	ET SCAN Potential SSH Scan	1
123.31.34.190	147.237.76.34	Vietnam	yohalan.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
123.31.34.190	147.237.72.156	Vietnam	aman.idf.il	ET SCAN Potential SSH Scan	1
54.235.19.162	147.237.77.216	United States	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
121.46.106.5	147.237.72.156	India	aman.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
5.255.90.133	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.98	147.237.77.235	United States	sviva.idf.il	ET DROP Dshield Block Listed Source	1
109.236.86.32	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
125.65.82.44	147.237.72.156	China	aman.idf.il	ET SCAN NMAP -sS window 1024	1
109.236.86.32	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
124.8.223.198	147.237.76.202	Taiwan	e.halag.idf.il	ET SCAN Potential SSH Scan	1
109.64.152.251	147.237.76.86	Israel	navy.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
124.8.223.198	147.237.76.200	Taiwan	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
103.208.244.223	147.237.76.86		navy.idf.il	ET SCAN Potential SSH Scan	1
124.8.223.198	147.237.76.31	Taiwan	nakchal.idf.il	ET SCAN Potential SSH Scan	1
103.208.244.223	147.237.76.38		e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
123.31.34.190	147.237.76.44	Vietnam	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
103.208.244.223	147.237.0.15		kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
123.31.34.190	147.237.72.166	Vietnam	aka.idf.il	ET SCAN Potential SSH Scan	1
62.210.243.100	147.237.76.42	France	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
123.31.34.190	147.237.0.15	Vietnam	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
50.19.25.51	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
208.100.26.228	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 1024	1
109.236.86.32	147.237.77.74	Netherlands	law.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
163.172.129.15	147.237.77.178	United Kingdom	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
5.255.90.133	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
109.236.86.32	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
125.65.82.44	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
109.236.86.32	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

10-05-2016-07:04:01 to 10-05-2016-08:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
203.104.11.21	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	90
207.46.13.85	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	39
109.253.217.172	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
2.53.41.209	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
85.65.4.85	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
82.102.169.113	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	16
2.53.150.116	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	11
46.19.85.241	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
46.19.85.241	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
84.94.35.50	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
87.69.137.248	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
175.0.172.192	China	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.114	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.111.54.30	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
176.13.246.214	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
141.226.162.57	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.246.140.41	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.69.137.248	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.253.213.68	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
80.246.136.169	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.14.161.10	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.253.199.165	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
109.253.139.59	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
82.102.169.113	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.86.124	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
212.199.65.218	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
185.14.161.10	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
2.53.52.3	Israel	147.237.76.42	refuah.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
37.142.242.165	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.86.191	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
82.102.169.113	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
2.53.23.247	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
87.69.137.248	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
213.151.32.163	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
77.138.188.178	France	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
109.253.135.247	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
5.22.134.183	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.163	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
37.26.146.243	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
72.173.128.245	United States	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
2.54.104.81	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	2
187.61.122.117	Brazil	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
46.19.86.195	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
85.130.176.102	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
80.246.133.169	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.85.85	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
187.61.124.31	Brazil	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
79.178.28.36	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
46.19.86.195	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2

10-05-2016-07:04:01 to 10-05-2016-08:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.0.23	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	89
82.102.169.113	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	27
109.253.214.250	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
37.59.227.227	France	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 37.59.227.227	Block	4
37.59.227.227	France	147.237.77.176	matpash.idf.il	PHP Attempt	Block	3
80.246.136.181	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.59.227.227	France	147.237.77.176	matpash.idf.il	Multiple Admin Blocking from 37.59.227.227	Block	3
80.246.140.41	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
88.202.218.236	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/contactus.aspx	Block	2
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	2
80.74.107.118	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
212.199.118.19	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/bottomcap.gif	Block	1
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/8/5328.png	Block	1
66.249.64.45	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/.well-known/apple-app-site-association	Block	1
31.154.101.236	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
176.13.246.214	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
80.246.136.3	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/news.aspx	Block	1
37.59.227.227	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/admin.php	Block	1
66.249.76.70	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/mobile/modiin/general.aspx	Block	1
37.59.227.227	France	147.237.77.176	matpash.idf.il	Admin Blocking	Block	1
194.90.99.193	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 194.90.99.193	Block	1
46.19.86.13	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
82.102.169.113	Israel	147.237.0.19	madim.atal.idf.i	SSL Untraceable Connection - Open Mode	None	1
66.249.79.59	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18287-he/dover.aspx	Block	1
195.62.53.168	Russian Federation	147.237.76.42	refuah.idf.il	Unauthorized URL Access to gmail.com/engine/log.txt	Block	1
66.102.9.5	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/sitemap.aspx	Block	1
78.46.21.97	Germany	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
207.46.13.109	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
66.102.9.8	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1

10-05-2016-07:04:01 to 10-05-2016-08:04:01