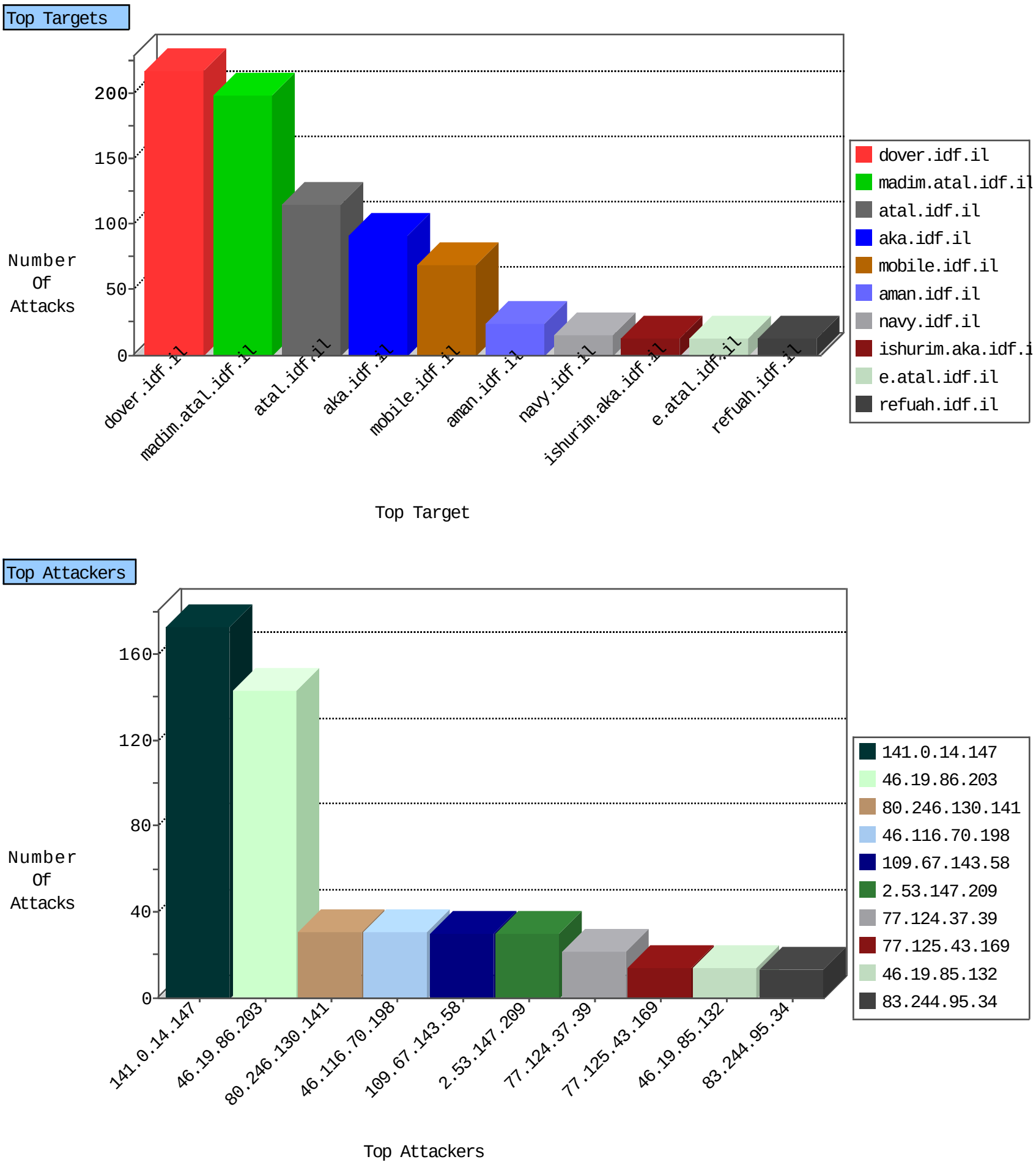
09-24-2016-20:04:01 to 09-24-2016-21:04:01

IDF Under Attack Daily Report



09-24-2016-20:04:01 to 09-24-2016-21:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.82.81	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	12
194.177.16.3	Israel	147.237.76.86	navy.idf.il	Black List	drop	3
111.72.252.91	China	147.237.76.147	chinuch.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
45.63.53.164	United States	147.237.76.30	himush.idf.il	Black List	drop	1
122.224.153.109	China	147.237.0.19	madim.atal.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
104.238.146.105	United States	147.237.76.38	e.e.meitav.idf.il	Black List	drop	1

09-24-2016-20:04:01 to 09-24-2016-21:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
199.58.86.211	United States	147.237.72.156	aman.idf.il	C1000074: HTTP: majestic bot	Permit	2
52.1.90.117	United States	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

09-24-2016-20:04:01 to 09-24-2016-21:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
78.97.159.124	147.237.0.33	Romania	idf.il	ET SCAN Potential SSH Scan	2
58.218.200.137	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
163.172.169.150	147.237.76.176	United Kingdom	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.200.137	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
125.77.28.26	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
201.150.38.110	147.237.77.226	Mexico	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 4096	1
125.77.28.26	147.237.8.45	China	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
5.29.117.65	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.143.227.35	147.237.76.202	United Kingdom	e.halag.idf.il	ET SCAN NMAP -sS window 4096	1
118.99.219.161	147.237.76.197	Taiwan	e.himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
195.143.227.35	147.237.76.202	United Kingdom	e.halag.idf.il	ET SCAN NMAP -f -sS	1
78.129.171.173	147.237.77.243	United Kingdom	mobile.idf.il	ET SCAN Potential SSH Scan	1
185.129.148.230	147.237.76.198	Latvia	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
78.97.159.124	147.237.0.17	Romania	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
185.129.148.230	147.237.76.147	Latvia	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.76.117	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
183.60.48.25	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
163.172.169.150	147.237.76.197	United Kingdom	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.200.137	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
132.74.95.19	147.237.77.170	Israel	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
58.218.200.137	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
211.149.197.148	147.237.77.19	China	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
125.77.28.26	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
201.150.38.110	147.237.77.226	Mexico	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 3072	1
125.77.28.26	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
195.143.227.35	147.237.76.202	United Kingdom	e.halag.idf.il	ET SCAN NMAP -sS window 2048	1
113.73.168.119	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.129.148.230	147.237.76.199	Latvia	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
185.129.148.230	147.237.76.148	Latvia	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
78.97.159.124	147.237.0.16	Romania	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
58.220.2.5	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
176.47.10.56	147.237.77.216	Saudi Arabia	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1

09-24-2016-20:04:01 to 09-24-2016-21:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
141.0.14.147	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	104
141.0.14.147	Europe	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	60
80.246.130.141	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	30
109.67.143.58	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
2.53.147.209	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
83.244.95.34	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
106.39.60.189	China	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	13
46.19.85.132	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	12
176.58.72.52	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
77.124.37.39	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
77.124.37.39	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
106.39.60.184	China	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	6
77.125.43.169	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
77.125.43.169	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.92	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
84.111.100.99	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.86.237	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.85.196	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.200	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
95.86.80.173	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
14.139.222.72	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
101.167.172.37	Australia	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
213.8.204.41	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
66.249.82.81	Asia/Pacific Region	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
85.65.194.115	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
2.55.169.79	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.86.200	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
51.254.217.34	France	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.85.205	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
80.246.139.221	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.86.200	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
109.253.192.202	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.138.60.225	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
37.26.148.139	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
77.124.37.39	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
128.232.110.28	United Kingdom	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
84.108.69.197	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
2.53.4.123	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
109.253.200.44	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	2
77.124.37.39	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
176.13.226.3	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
80.246.136.214	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
91.143.234.207	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
141.0.14.147	Europe	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
176.13.251.175	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
81.218.66.211	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
77.138.181.58	France	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
141.226.218.11	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

09-24-2016-20:04:01 to 09-24-2016-21:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.203	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	143
46.116.70.198	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	31
109.253.139.224	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.179.196.221	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
89.138.231.251	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
77.139.47.167	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/miyun/miyunlobby.aspx	Block	3
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.224	Block	3
93.172.145.227	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	3
46.121.139.173	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
84.109.241.17	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 84.109.241.17	Block	2
66.249.69.228	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	2
79.178.187.138	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	2
66.102.9.5	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	2
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	2
182.232.72.40	Thailand	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
77.139.239.216	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	1
66.249.75.8	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/6/2826.jpg	Block	1
199.58.86.211	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1
77.126.66.157	Israel	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
37.142.2.111	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
66.249.75.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
213.151.42.2	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
87.70.12.26	Israel	147.237.72.166	aka.idf.il	Unknown Parameter y in www.aka.idf.il/main/sachar/payslips.aspx	None	1
77.126.66.157	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/wp-login.php	Block	1
66.249.69.228	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.228	Block	1
40.77.167.34	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/daily_statistics/english/1.doc.	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/.well-known/apple-app-site-association	Block	1
66.249.64.2	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/iturim/asp/displayallsoldiers.asp	Block	1
77.138.82.7	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
66.249.69.232	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	1
157.55.39.183	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/scripts.asmx/getjs	Block	1
80.246.130.141	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
66.249.76.98	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
93.172.125.6	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.75.4	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/6/2976.jpg	Block	1
80.246.138.157	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/cityofficers/	Block	1
66.249.76.117	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1

09-24-2016-20:04:01 to 09-24-2016-21:04:01