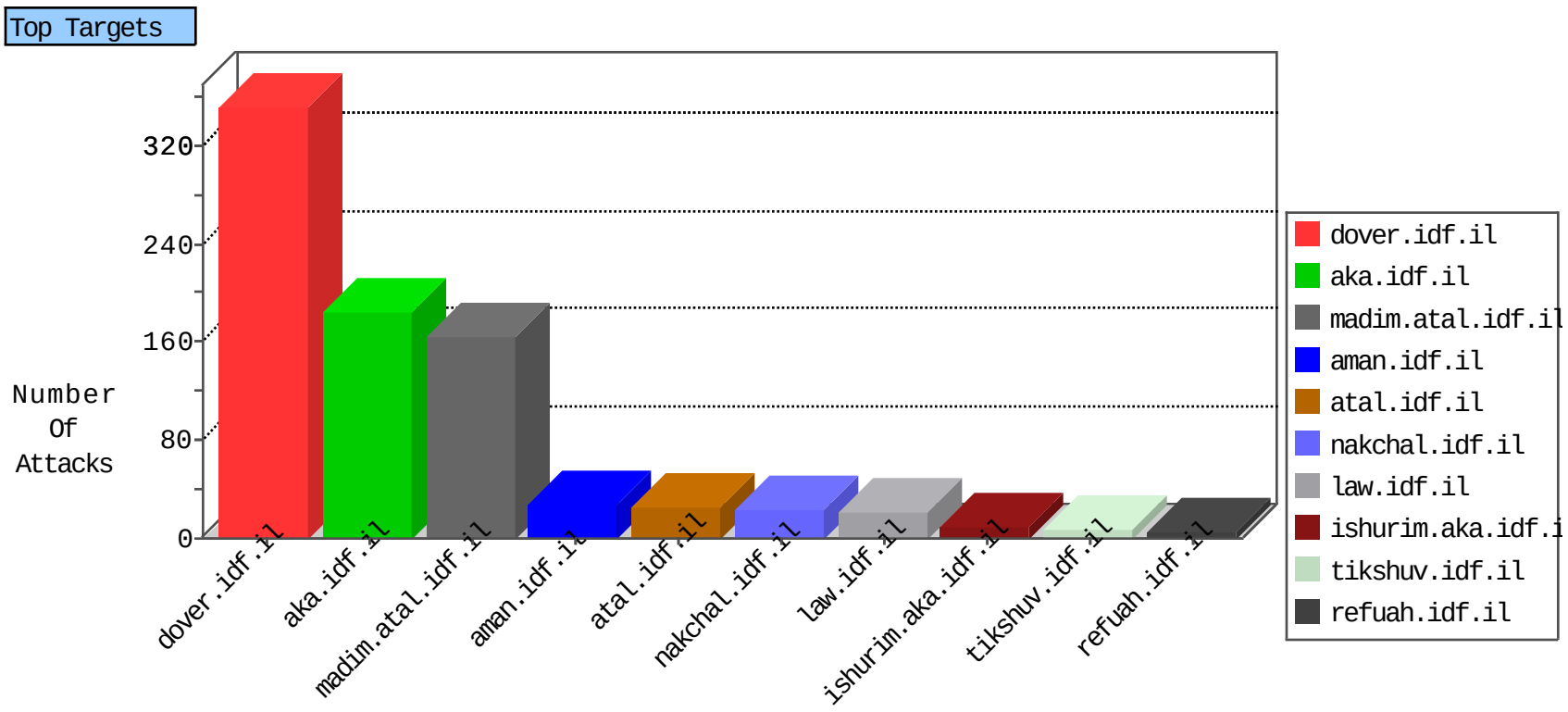
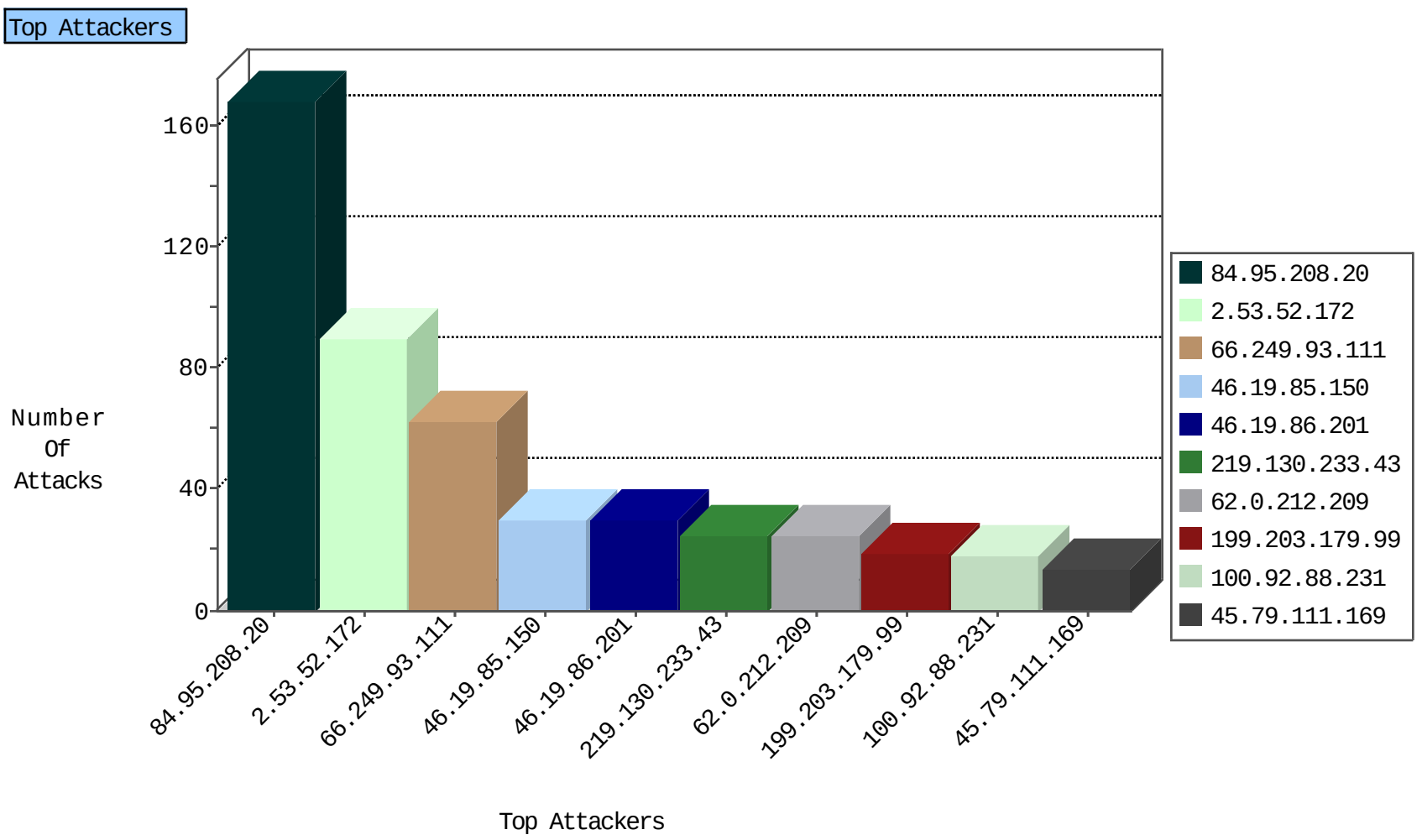
09-04-2016-12:04:03 to 09-04-2016-13:04:03

IDF Under Attack Daily Report





09-04-2016-12:04:03 to 09-04-2016-13:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.76	Israel	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	34
2.53.37.167	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
120.132.50.135	China	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	1
199.203.179.99	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
212.143.40.198	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
46.19.86.238	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

09-04-2016-12:04:03 to 09-04-2016-13:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
162.210.196.100	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	4

09-04-2016-12:04:03 to 09-04-2016-13:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
80.246.130.35	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	8
45.79.111.169	147.237.0.34	United States	tikshuv.idf.il	WEB-MISC Chunked-Encoding transfer attempt	2
185.32.179.159	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.116.72.226	147.237.76.39	Sweden	mobile.meitav.idf.il	ET SCAN NMAP -f -sS	1
46.19.86.178	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.228.178.105	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.116.166.242	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.210	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
148.251.236.237	147.237.0.16	Germany	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
185.110.132.201	147.237.77.178	Ukraine	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
31.168.135.94	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.212.97	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.102.242.161	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.201	147.237.76.198	Ukraine	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
84.95.208.20	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.201	147.237.76.42	Ukraine	refuah.idf.il	ET SCAN Potential SSH Scan	1
81.218.170.55	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.201	147.237.8.27	Ukraine	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
80.179.184.165	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.132.159.81	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.201	147.237.0.15	Ukraine	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	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
213.8.115.122	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.77.91.109	147.237.77.19	Turkey	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.231	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.116.72.226	147.237.76.39	Sweden	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
185.27.106.15	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
198.50.164.48	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.238.41	147.237.8.28	United Kingdom	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
185.110.132.201	147.237.77.216	Ukraine	dover.idf.il	ET SCAN Potential SSH Scan	1
31.168.232.168	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
117.158.160.211	147.237.77.233	China	atal.idf.il	ET SCAN Potential SSH Scan	1
185.110.132.201	147.237.76.202	Ukraine	e.halag.idf.il	ET SCAN Potential SSH Scan	1
31.154.81.15	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
88.149.249.226	147.237.76.44	Italy	e.refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
2.55.10.138	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.201	147.237.76.197	Ukraine	e.himush.idf.il	ET SCAN Potential SSH Scan	1
84.93.84.77	147.237.77.74	United Kingdom	law.idf.il	Tehila - Perl LWP with fake user agent	1
185.110.132.201	147.237.72.156	Ukraine	aman.idf.il	ET SCAN Potential SSH Scan	1
185.110.132.201	147.237.0.200	Ukraine	m4u.idf.il	ET SCAN Potential SSH Scan	1
79.183.17.146	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.183.183	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.93.185.10	147.237.76.44	Ukraine	e.refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
62.219.44.10	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.116.72.226	147.237.76.39	Sweden	mobile.meitav.idf.il	ET SCAN NMAP -sS window 2048	1

09-04-2016-12:04:03 to 09-04-2016-13:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.93.111	Europe	147.237.77.216	dover.idf.il	drop	SAM rule	drop	48
46.19.86.201	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
62.0.212.209	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	25
100.92.88.231		147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	18
199.203.179.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
62.0.197.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
66.249.93.111	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	14
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
62.0.251.201	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
213.8.204.28	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	12
62.0.197.85	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
185.89.217.226	Netherlands	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	8
212.179.223.52	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.185	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
46.19.86.243	Israel	147.237.77.233	atal.idf.il	drop	SAM rule	drop	6
37.26.148.199	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
122.57.7.118	New Zealand	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.180	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
46.19.86.151	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
37.26.148.199	Israel	147.237.72.156	aman.idf.il	drop	SAM rule	drop	3
176.13.241.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
176.13.14.241	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.44	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	3
87.69.37.129	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
77.126.53.183	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.185	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
212.29.223.233	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
62.0.207.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
216.243.31.2	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
185.89.217.226	Netherlands	147.237.72.156	aman.idf.il	drop	SAM rule	drop	1
176.13.7.113	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.241.150	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	1
176.13.14.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
80.178.101.40	Israel	147.237.0.15	kosher-kravi.idf.il	drop	First packet isn't SYN	drop	1
46.43.99.252	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1
109.253.197.32	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	1
46.19.86.7	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
80.178.204.69	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
212.235.34.5	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.249.227	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.229.248	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
80.179.16.170	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
185.24.207.112	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	1
176.13.6.134	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
176.13.232.208	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	1

09-04-2016-12:04:03 to 09-04-2016-13:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.52.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	90
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	88
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	62
46.19.85.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
219.130.233.43	China	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 219.130.233.43	Block	17
46.19.85.84	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	12
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	7
2.53.7.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
82.80.198.164	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for aka.idf.il/	Block	6
93.172.200.28	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
85.64.146.247	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	6
219.130.233.43	China	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	6
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	5
176.13.241.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.179.255.6	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	3
2.53.14.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
82.80.198.164	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/4/	Block	3
46.19.86.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.55.41.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.125.28.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.27	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
109.253.130.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	3
66.249.93.107	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
80.246.136.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.154.19.5	Block	2
37.26.146.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
62.219.139.8	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
176.13.1.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
85.64.146.247	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/2/	Block	2
37.26.146.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.138.140.102	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
45.79.111.169	United States	147.237.0.34	tikshuv.idf.il	Multiple Malformed URL from 45.79.111.169	Block	1
31.168.16.234	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
85.130.216.49	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
66.249.76.74	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/apple-app-site-association	Block	1
2.53.136.167	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
45.79.111.169	United States	147.237.72.167	ishurim.aka.idf.il	Multiple Malformed HTTP Header Line from 45.79.111.169	Block	1
212.199.224.24	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 212.199.224.24	Block	1
80.179.255.6	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 80.179.255.6	Block	1
37.46.35.61	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
148.251.2.180	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
74.91.23.166	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
66.249.64.144	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/general/general.aspx	Block	1
5.29.101.211	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.229.14.112	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
219.130.233.43	China	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
77.138.251.117	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/klali.aspx	Block	1
45.79.111.169	United States	147.237.0.34	tikshuv.idf.il	Multiple Unknown HTTP Request Method from 45.79.111.169	Block	1

09-04-2016-12:04:03 to 09-04-2016-13:04:03