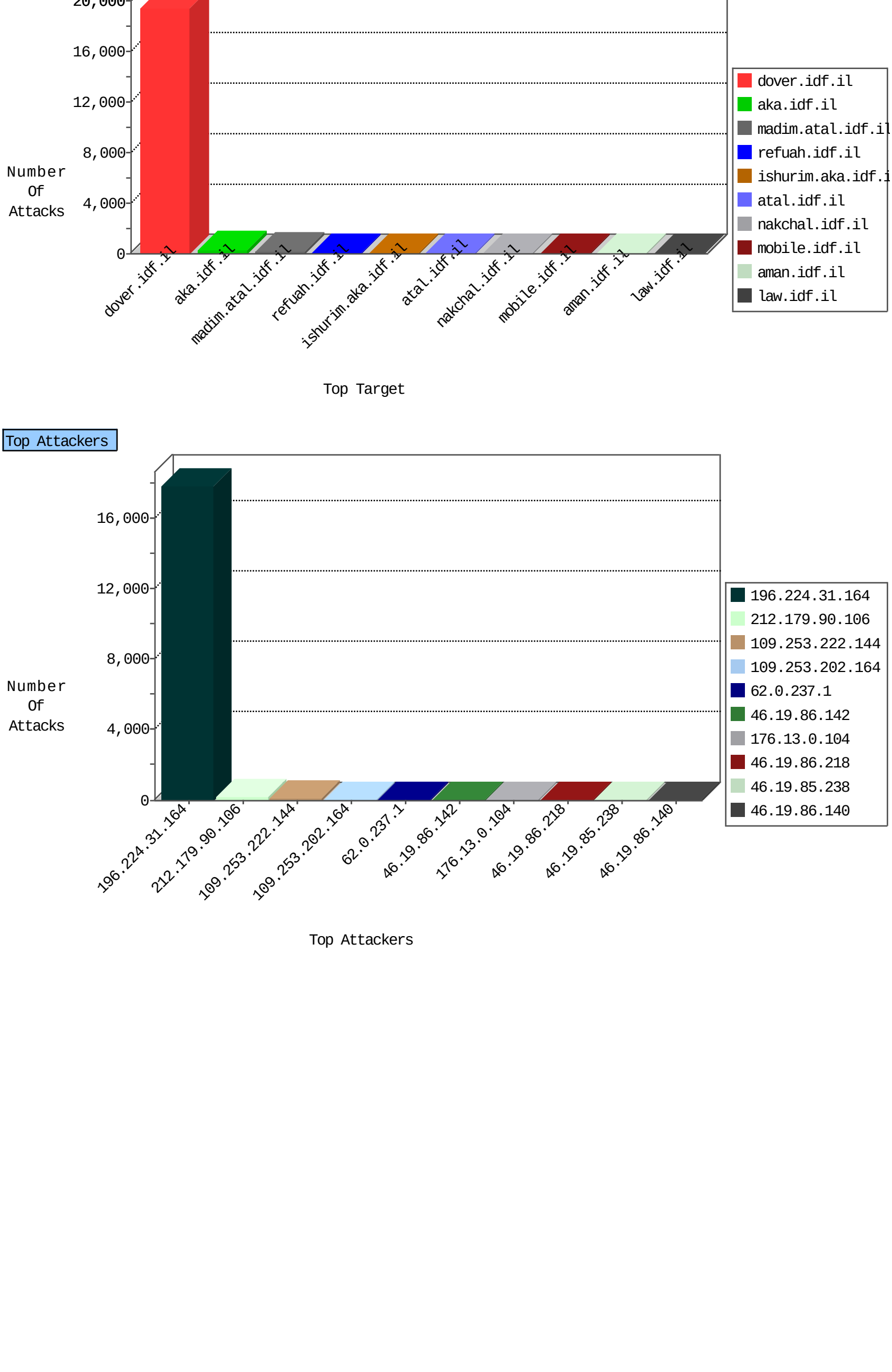
09-12-2016-09:04:01 to 09-12-2016-10:04:01

IDF Under Attack
Daily Report



09-12-2016-09:04:01 to 09-12-2016-10:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
129.97.74.14	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	6
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	6
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
129.10.120.193	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
195.113.161.83	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
129.93.229.138	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
194.29.178.14	Poland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
193.1.13.14	Ireland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
141.22.213.35	Germany	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
201.90.134.51	Brazil	147.237.0.200	m4u.idf.il	JLM_Purple_Con_Limit_Http	drop	1
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
153.90.1.35	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.112	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
208.94.63.194	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
198.133.224.147	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-12-2016-09:04:01 to 09-12-2016-10:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.54.18.219	Saudi Arabia	147.237.76.147	chinuch.aka.idf.il	0854: HTTP: upload* Access	Block	7
106.38.241.105	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	6
77.248.12.153	Netherlands	147.237.76.42	refuah.idf.il	14331: HTTP: Suspicious User-Agent (My Session)	Block	1
106.38.241.105	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1
185.96.92.54	United Kingdom	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

09-12-2016-09:04:01 to 09-12-2016-10:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
185.96.92.54	147.237.72.166	United Kingdom	aka.idf.il	SQL Injection - Select From	2
93.174.91.29	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
82.128.161.253	147.237.77.227	Finland	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
79.177.11.96	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.25.69.41	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
65.60.36.203	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
52.166.249.197	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.129.15	147.237.77.235	United Kingdom	sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.19.85.186	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.129.15	147.237.76.198	United Kingdom	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
31.168.169.122	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.195	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
93.174.91.29	147.237.77.19	Netherlands	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
89.138.177.209	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.128.161.253	147.237.77.176	Finland	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.66.240	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
191.96.249.18	147.237.72.217	Chile	e.idf.il	ET SCAN Potential SSH Scan	1
62.219.255.166	147.237.77.233	Israel	atal.idf.il	ET SCAN NMAP -sA (2)	1
185.32.179.97	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.158	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.129.15	147.237.77.235	United Kingdom	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
37.218.214.188	147.237.77.176	Palestinian Territory, Occupied	matpash.idf.il	ET SCAN NMAP -sA (2)	1
163.172.129.15	147.237.0.16	United Kingdom	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
5.29.249.97	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.195	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN NMAP -sS window 1024	1

09-12-2016-09:04:01 to 09-12-2016-10:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
196.224.31.164	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17885
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	173
62.0.237.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	35
46.19.86.142	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
176.13.236.74	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
46.19.85.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
37.8.48.136	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
109.226.40.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
82.166.219.154	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
68.180.229.190	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
46.19.86.140	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
62.219.237.170	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
46.19.86.130	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
109.253.206.5	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
79.181.123.230	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
46.19.86.191	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
132.66.255.253	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
5.102.195.5	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.53.30.218	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.86.158	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	12
176.13.231.97	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
37.26.148.221	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
46.24.20.52	Spain	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
37.26.148.221	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
176.13.237.206	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
176.13.16.36	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.33	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
31.168.11.202	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.186	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.219	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
147.236.238.22	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.82	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.110	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
156.204.212.202	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
109.253.203.217	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
82.80.196.44	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
109.253.150.105	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
192.115.177.202	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
79.181.100.38	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
109.253.156.79	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
31.154.7.4	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
2.53.129.236	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
2.55.181.142	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.149	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
199.203.215.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8

09-12-2016-09:04:01 to 09-12-2016-10:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.222.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	89
109.253.202.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	75
176.13.0.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	34
46.19.86.233	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	4
109.253.128.76	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
176.13.230.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
212.199.76.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/4/	Block	3
176.13.250.71	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
209.88.173.130	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 209.88.173.130	Block	3
2.55.181.142	Israel	147.237.76.42	refuah.idf.il	Distributed Parameter Type Violation on www.refua.atal.idf.il/1518-he/refuah.aspx parameter ctl00$ContentPlaceHolder1$txtLastName	Block	2
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
109.253.201.141	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
80.74.118.200	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/2/	Block	2
46.19.85.253	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
17.78.149.78	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	2
37.26.148.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
194.114.146.227	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
80.74.118.200	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	2
176.13.250.71	Israel	147.237.0.19	madim.atal.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.85.238	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method .xml in URL	Block	1
2.53.7.196	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
217.132.36.190	Israel	147.237.77.216	dover.idf.il	Illegal Parameter Encoding ctl00$ContentPlaceHolder1$txtContent in www.idf.il/1038-he/dover.aspx	None	1
46.121.15.82	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
183.160.115.35	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1694-11766-he/cogat.aspx/trackback/	Block	1
46.4.74.42	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/iturim/asp/displayonesoldier.asp	Block	1
2.53.155.232	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
212.179.21.194	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/step3.aspx	None	1
176.13.251.66	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
5.28.180.57	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.253.246.88	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
82.166.219.154	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
2.53.11.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/ghttps:/photos.google.com/share/af1qipmchh_7cgqzaunpocr4rnzhxlbaydkw0rle1hp8i6s33brdkzh-xki8bern8-cmqq	Block	1
66.147.244.101	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/general.aspx	Block	1
192.243.55.129	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/eitan/listpage/?catid=32659	Block	1
176.13.231.23	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.53.163.101	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
212.199.76.9	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.199.76.9	Block	1
80.246.133.176	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
46.19.86.184	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
176.13.251.66	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
157.55.39.236	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
95.189.172.244	Russian Federation	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
2.53.25.254	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
192.243.55.135	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.135	Block	1
66.249.66.240	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
176.13.238.121	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.85.227	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.53.178.228	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.253.202.164	Israel	147.237.0.19	madim.atal.idf.il	Untraceable SSL Sessions: Open Mode	None	1

09-12-2016-09:04:01 to 09-12-2016-10:04:01