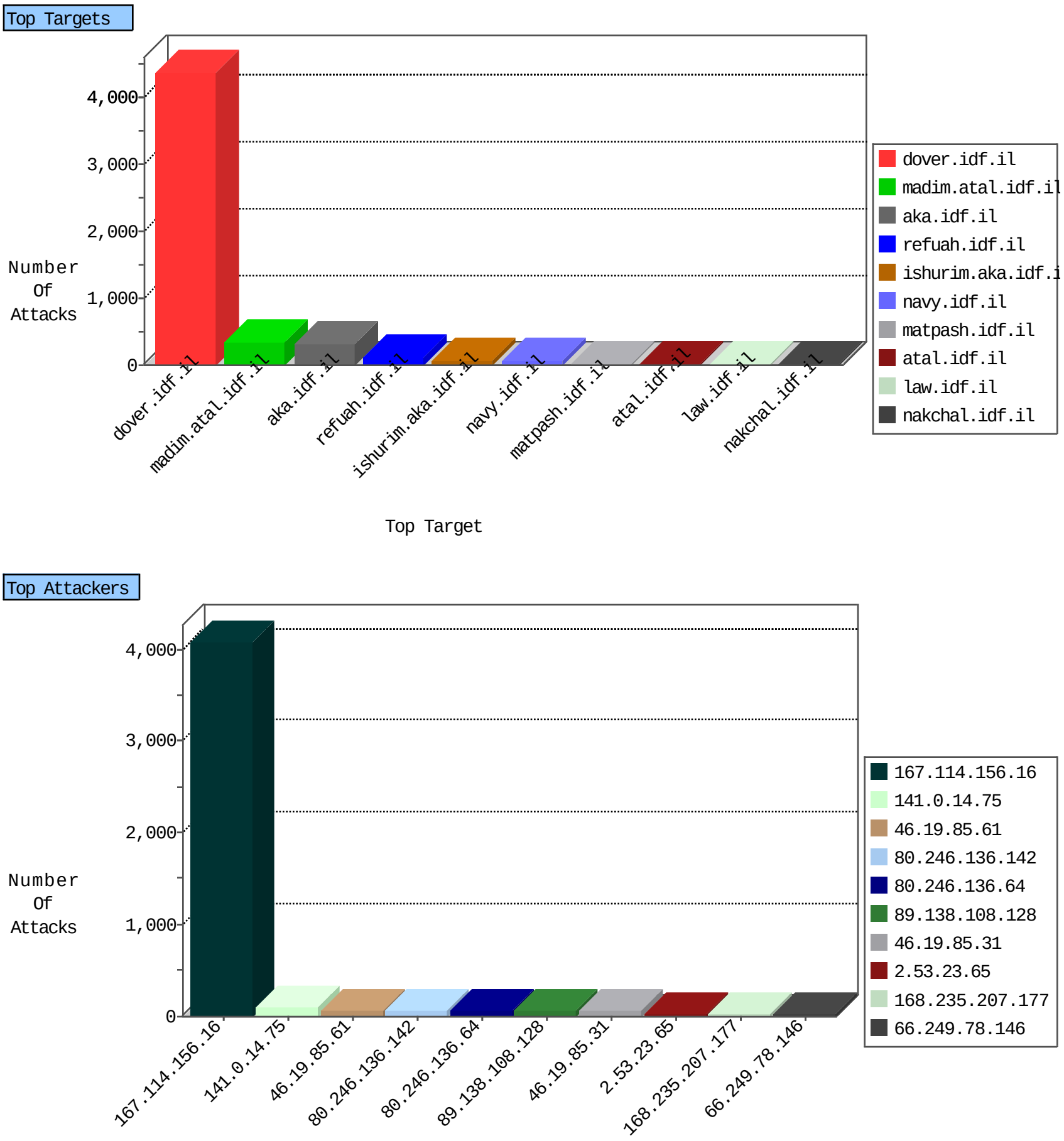
04-19-2016-16:04:03 to 04-19-2016-17:04:03

IDF Under Attack Daily Report



04-19-2016-16:04:03 to 04-19-2016-17:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4079
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	178
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	6
168.235.207.177	United States	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
84.111.65.41	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
37.187.39.228	France	147.237.77.205	prisha.idf.il	Block_Udp_All_Nets_Con_Limit	drop	2
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
168.235.207.177	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
185.94.111.1	Russian Federation	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	1
141.0.14.75	Europe	147.237.76.42	refuah.idf.il	JLM_Under_Attack_Con_Http	drop	1
208.73.206.243	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
141.0.14.216	Europe	147.237.76.42	refuah.idf.il	JLM_Under_Attack_Con_Http	drop	1
208.73.206.243	United States	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
94.102.49.116	Netherlands	147.237.8.50	e.tikshuv.idf.il	Block_Ntp_All_Net	drop	1
194.69.127.148	United Kingdom	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1
185.94.111.1	Russian Federation	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	1
123.30.183.145	Vietnam	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
194.69.127.150	United Kingdom	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
82.145.217.212	Europe	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	1

04-19-2016-16:04:03 to 04-19-2016-17:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-19-2016-16:04:03 to 04-19-2016-17:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
115.72.13.23	147.237.0.19	Vietnam	madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
85.131.208.140	147.237.77.176	Germany	matpash.idf.il	ET SCAN Potential SSH Scan	1
85.131.208.140	147.237.0.19	Germany	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
62.219.173.210	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.144	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
201.212.108.174	147.237.0.16	Argentina	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.130.5.88	147.237.76.42	Lithuania	refuah.idf.il	ET SCAN Potential SSH Scan	1
158.255.5.147	147.237.8.46	Russian Federation	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
132.76.10.42	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.219.238.10	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 1024	1
85.131.208.140	147.237.76.198	Germany	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
70.66.93.30	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
46.120.106.223	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.53.185.3	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.0.136	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.50.12.242	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

04-19-2016-16:04:03 to 04-19-2016-17:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
141.0.14.75	Europe	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	94
46.19.85.61	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	30
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
46.19.85.61	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	19
168.235.207.177	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
77.234.45.133	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
109.253.226.47	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
46.19.85.61	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
80.246.137.89	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
46.19.86.11	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.61	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
212.179.21.194	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence		monitor	8
84.228.41.50	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
46.43.96.13	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
84.111.141.143	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.253.142.73	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.55.167.185	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
185.120.125.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
199.203.93.50	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.164.7	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
168.235.207.177	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
85.130.248.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.215.187	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
84.111.141.143	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.26	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.26	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
77.234.45.133	Germany	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.100	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
84.94.105.30	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
66.102.9.117	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.100	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
66.102.9.127	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	4
2.53.164.7	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
77.234.45.139	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.177.216.95	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
91.200.12.141	Ukraine	147.237.77.74	law.idf.il	drop	SAM rule	drop	4
2.53.164.7	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
84.228.41.50	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
212.179.21.194	Israel	147.237.0.19	madim.atal.idf.il	drop	First packet isn't SYN	drop	4
79.177.216.95	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
91.200.12.141	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
149.88.128.242	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
212.179.21.194	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
79.177.216.95	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
199.30.25.157	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
212.179.21.194	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
62.90.167.94	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.136.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	66
80.246.136.64	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	63
89.138.108.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	59
46.19.85.31	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	55
2.53.23.65	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	34
109.253.132.33	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	21
109.253.203.13	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	9
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	7
46.19.86.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
173.236.187.27	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 173.236.187.27	Block	5
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
2.53.184.88	Israel	147.237.76.42	refuah.idf.il	Distributed Suspicious Response Code	Block	4
87.71.3.162	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 87.71.3.162	Block	4
84.111.242.12	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/images/1.he/infocenteritem/	Block	4
2.53.0.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
46.119.112.23	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.119.112.23	Block	3
176.13.6.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 141.8.132.78	Block	3
176.13.17.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.20.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.5.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
207.46.13.176	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.85.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
46.120.210.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
104.128.144.131	Canada	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
79.183.222.21	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl13 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
31.168.179.101	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_FINISH_RESUMED_SESSION)	None	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
66.249.64.137	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
106.186.113.132	Japan	147.237.76.39	mobile.meitav.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
46.19.85.100	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
84.228.41.50	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-ar/www.idf.il/ar	Block	1
66.249.75.118	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/	Block	1
104.128.144.131	Canada	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/	Block	1
46.119.112.23	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
37.48.65.71	Netherlands	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
66.249.64.238	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/templates/news/news.aspx	Block	1
87.68.19.198	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
176.13.7.171	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17570-	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
106.186.113.132	Japan	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Untraceable SSL Sessions from 106.186.113.132 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
38.111.147.83	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
173.236.187.27	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-15044-he/dover.aspx	Block	1
109.253.142.73	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
74.82.47.2	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1