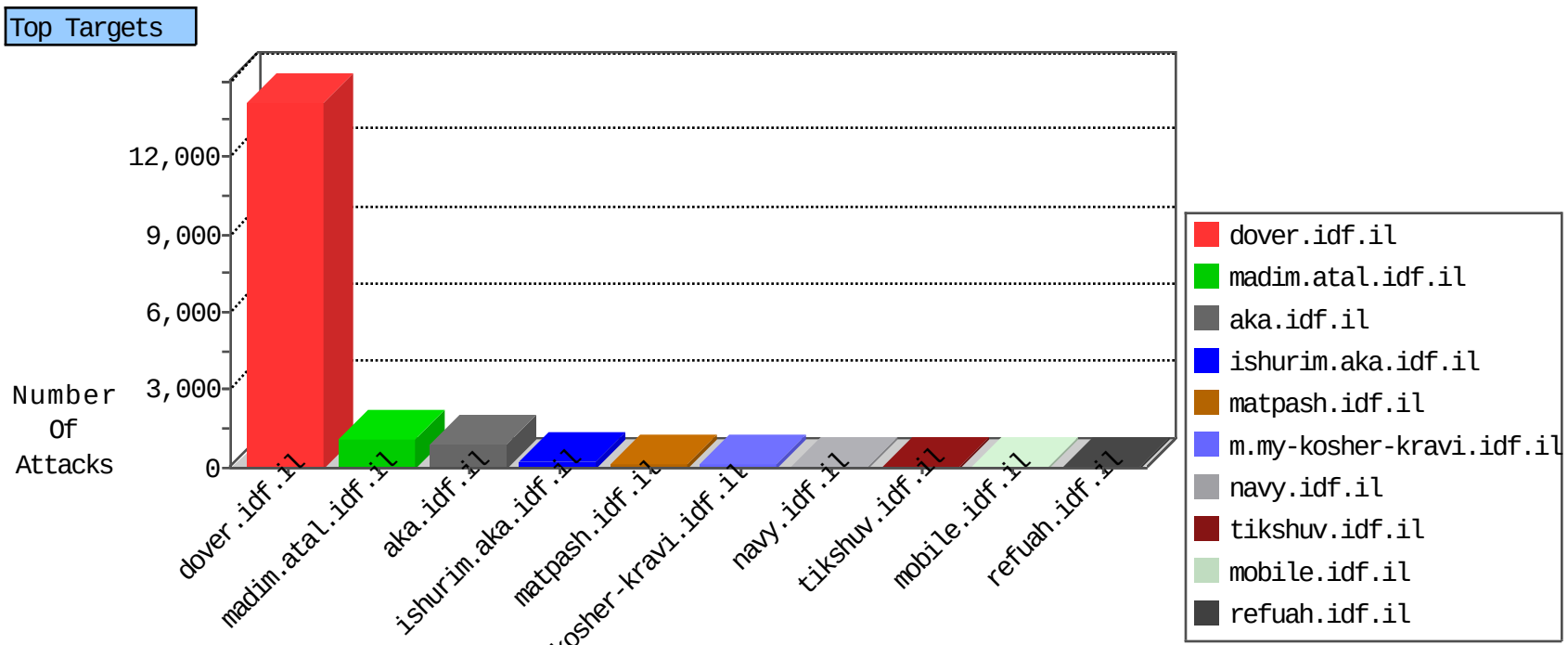
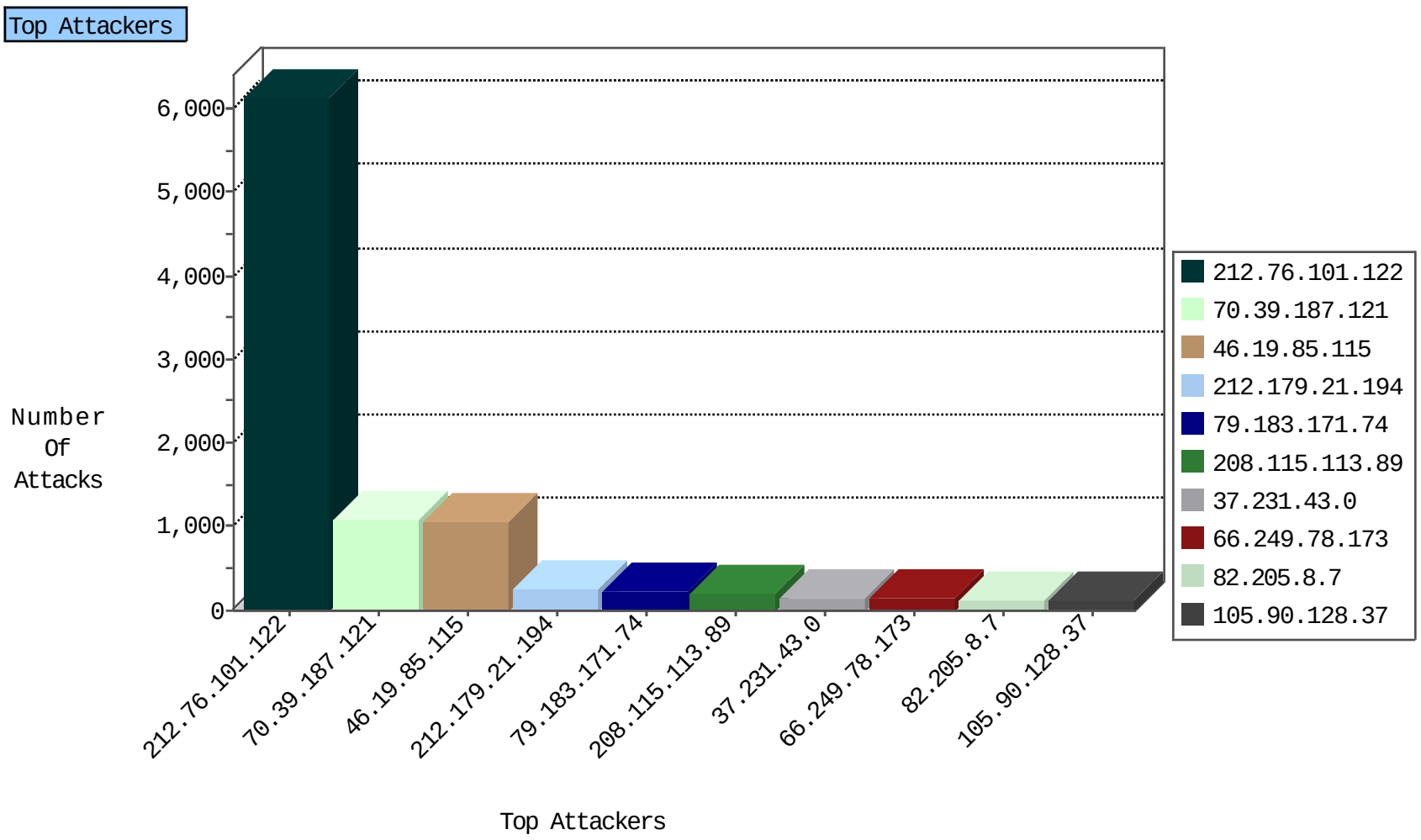
10-21-2015-16:04:06 to 10-21-2015-17:04:06

IDF Under Attack Daily Report





10-21-2015-16:04:06 to 10-21-2015-17:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.186.61.126	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2544
192.116.190.74	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	748
46.19.86.243	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	129
192.168.8.100		147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	91
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	83
109.65.28.124	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
188.120.148.211	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
82.205.8.7	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
176.13.2.211	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
82.145.209.106	Europe	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	7
213.57.195.81	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
213.151.46.230	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
79.176.36.139	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	5
2.54.182.0	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
176.13.22.143	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
37.26.146.216	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.13.6.142	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
201.151.106.81	Mexico	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
46.19.86.20	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
46.19.85.56	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
85.130.201.77	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
81.218.67.234	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
87.69.22.254	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
2.54.149.210	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
189.207.130.242	Mexico	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
79.178.110.48	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
81.218.50.26	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
60.169.74.168	China	147.237.76.202	e.halag.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
14.215.176.20	China	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
144.162.213.207	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
46.19.85.248	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
31.168.96.58	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1

10-21-2015-16:04:06 to 10-21-2015-17:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.120.240.53	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
217.132.65.124	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2

10-21-2015-16:04:06 to 10-21-2015-17:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
194.90.134.229	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.154.92.152	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.6.55	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.194	147.237.77.227	Netherlands	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
87.69.168.138	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.82.78.169	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN Potential SSH Scan	1
80.82.78.169	147.237.76.86	Netherlands	navy.idf.il	ET SCAN Potential SSH Scan	1
79.182.4.19	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.140	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
37.19.127.127	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
194.30.41.129	147.237.77.216	Spain	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.135.157	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
130.193.190.143	147.237.77.216	Iraq	dover.idf.il	portscan: TCP Distributed Portscan	1
89.139.164.118	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.136.219	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.82.78.169	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
80.82.78.169	147.237.8.24	Netherlands	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
69.58.181.15	147.237.77.216	United States	dover.idf.il	ET DOS SSL Bomb DoS Attempt	1
37.142.213.109	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

10-21-2015-16:04:06 to 10-21-2015-17:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.76.101.122	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6148
70.39.187.121	Satellite Provider	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1091
79.183.171.74	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	221
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	214
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	206
37.231.43.0	Kuwait	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	142
105.90.128.37	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	116
91.138.71.58	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	110
5.109.38.141	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	106
37.161.125.227	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	98
144.162.213.207	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	85
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	81
192.118.78.57	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	78
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	71
62.90.219.27	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
66.249.93.200	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	62
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
190.24.146.71	Colombia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
109.186.61.126	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
109.65.105.78	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
109.160.142.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
46.19.86.231	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
46.19.86.99	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
81.218.44.11	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
176.13.0.161	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
2.54.52.101	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
79.183.116.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
79.183.218.20	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
109.64.197.195	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
37.26.146.187	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
151.80.31.115	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
176.12.157.214	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
109.67.202.14	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
82.205.8.7	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
93.172.184.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
100.100.115.157		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	38
79.180.32.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
89.139.39.186	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
2.54.6.18	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
31.168.89.122	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
85.64.249.42	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
46.19.86.9	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
176.12.136.201	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
66.249.78.159	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.115	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1050
82.205.8.7	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	84
80.230.23.70	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	84
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	56
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	28
66.249.67.192	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	28
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	28
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	28
192.116.190.74	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	28
79.181.188.127	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
213.57.155.196	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	14
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/idf_in_pictures/images/2002/march/balatadotjpg	Block	14
5.29.136.5	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
157.55.39.173	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	14
81.218.251.251	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	14
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/idf/templates/album.aspx	Block	14
193.205.142.192	Italy	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ https:/twitter.com/	Block	14
66.249.67.155	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	14
92.113.154.3	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/7/13037.jpg	Block	14
79.183.116.165	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	14
176.13.8.236	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14
207.46.13.141	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/general.aspx	Block	14
149.78.108.217	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	14
79.183.116.165	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$btnSubmit.x in www.aka.idf.il/main/sachar/payslips.aspx	None	14
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	14
46.19.85.131	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	14
188.120.135.12	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/viewpniot.aspx	None	14
84.110.55.101	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
79.177.28.171	Israel	147.237.0.19	madim.atal.idf.il	Cookie Tampering on cookie _pk_ref.322.9cd2: Expected ["","",1445421715,"https://www.google.co.il/"], Observed ["","",1445433187,"https://www.google.co.il/"]	None	14
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	14
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/templates/sendtofriend/sendtofriend.aspx	Block	14
5.18.97.212	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation part in www.idf.il/hebrew/nakhal/page.asp	Block	14
149.78.138.203	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/maim/kapatz	Block	14
79.183.200.141	Israel	147.237.72.166	aka.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 79.183.200.141	Block	14
188.143.232.15	Russian Federation	147.237.77.176	matpash.idf.il	Parameter Type Violation fromDate in www.cogat.idf.il/901-en/cogat.aspx	Block	14
46.117.27.127	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
87.68.30.65	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	14
79.179.167.141	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
212.143.3.44	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	14
5.29.60.156	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	14
151.80.31.115	Italy	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
87.68.67.216	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtPassword in m.my-kosher-kravi.idf.il/templates/login.aspx	Block	14
213.57.155.196	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 213.57.155.196	Block	13