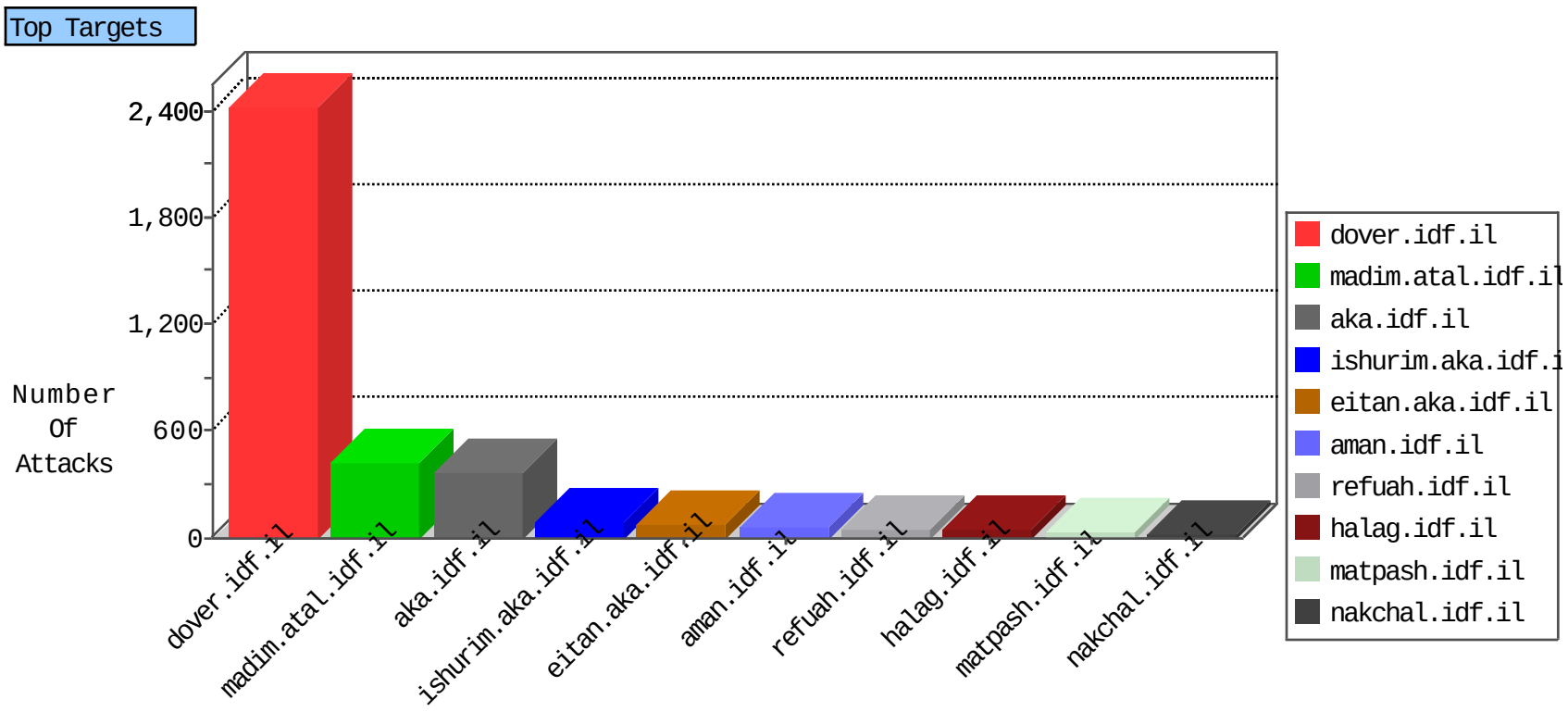
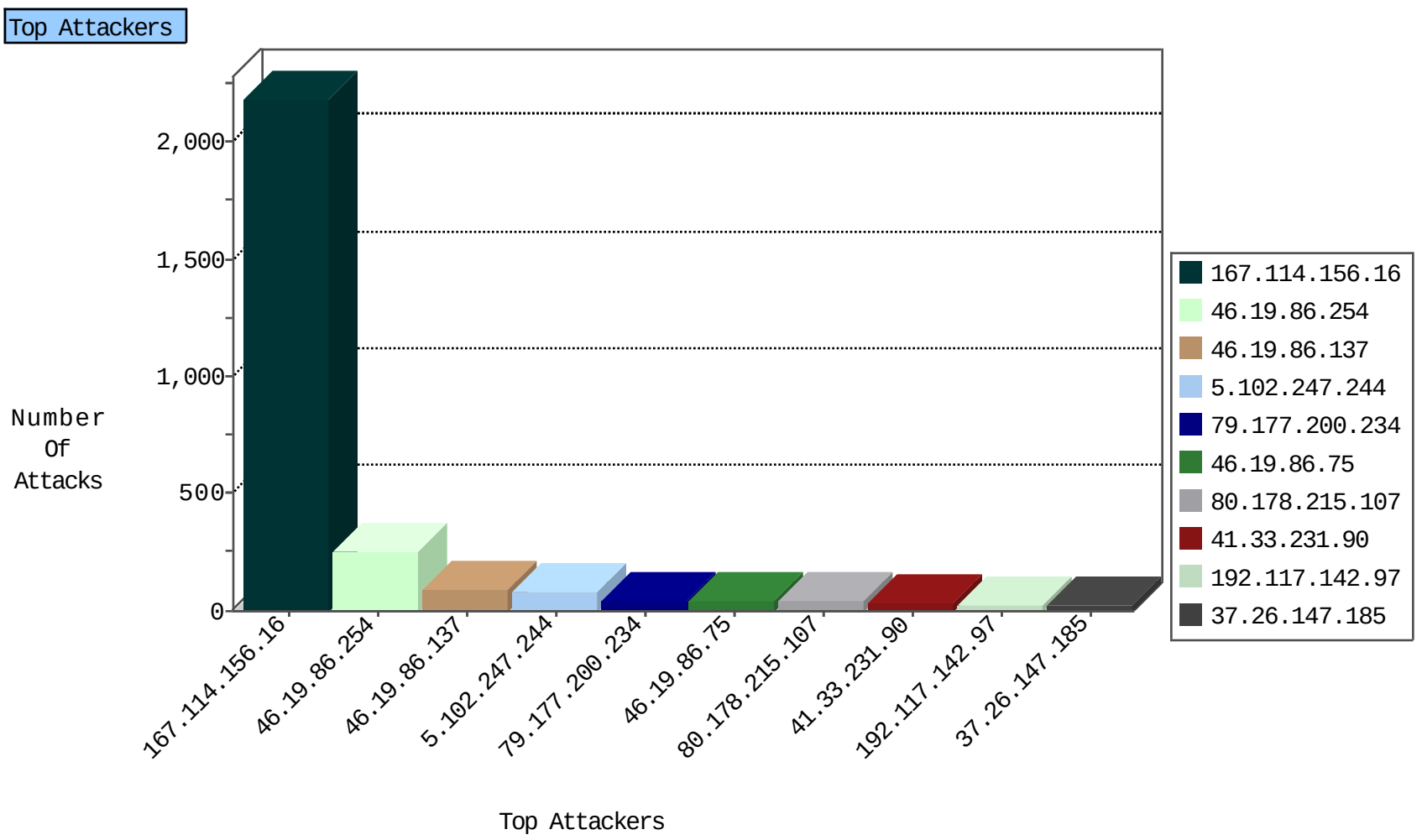
12-17-2015-10:04:01 to 12-17-2015-11:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



12-17-2015-10:04:01 to 12-17-2015-11:04:01

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	DOS-Tool-SwitchbladG	dest-reset	3554
212.150.174.90	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	94
162.244.28.120	Canada	147.237.76.201	e.atal.idf.il	L4 Source or Dest Port Zero	drop	1
162.244.28.120	Canada	147.237.76.39	mobile.meitav.idf.il	L4 Source or Dest Port Zero	drop	1
162.244.28.58	Canada	147.237.76.197	e.himush.idf.il	L4 Source or Dest Port Zero	drop	1
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
162.244.28.120	Canada	147.237.76.148	gqcenter.aka.idf.il	L4 Source or Dest Port Zero	drop	1
162.244.28.120	Canada	147.237.76.30	himush.idf.il	L4 Source or Dest Port Zero	drop	1
162.244.28.58	Canada	147.237.76.86	navy.idf.il	L4 Source or Dest Port Zero	drop	1
162.244.28.120	Canada	147.237.76.202	e.halag.idf.il	L4 Source or Dest Port Zero	drop	1
162.244.28.120	Canada	147.237.76.44	e.refuah.idf.il	L4 Source or Dest Port Zero	drop	1
162.244.28.58	Canada	147.237.76.199	e.nakchal.idf.il	L4 Source or Dest Port Zero	drop	1
162.244.28.58	Canada	147.237.76.31	nakchal.idf.il	L4 Source or Dest Port Zero	drop	1
162.244.28.120	Canada	147.237.76.176	test.ncore.idf.il	L4 Source or Dest Port Zero	drop	1
162.244.28.120	Canada	147.237.76.34	yohalan.idf.il	L4 Source or Dest Port Zero	drop	1
162.244.28.58	Canada	147.237.76.147	chinuch.aka.idf.il	L4 Source or Dest Port Zero	drop	1
162.244.28.120	Canada	147.237.77.216	dover.idf.il	L4 Source or Dest Port Zero	drop	1
162.244.28.120	Canada	147.237.76.86	navy.idf.il	L4 Source or Dest Port Zero	drop	1
162.244.28.58	Canada	147.237.76.200	eitan.aka.idf.il	L4 Source or Dest Port Zero	drop	1
162.244.28.58	Canada	147.237.76.34	yohalan.idf.il	L4 Source or Dest Port Zero	drop	1
162.244.28.120	Canada	147.237.76.196	e.sviva.idf.il	L4 Source or Dest Port Zero	drop	1
162.244.28.120	Canada	147.237.76.38	e.e.meitav.idf.il	L4 Source or Dest Port Zero	drop	1
162.244.28.58	Canada	147.237.76.196	e.sviva.idf.il	L4 Source or Dest Port Zero	drop	1
162.244.28.120	Canada	147.237.76.147	chinuch.aka.idf.il	L4 Source or Dest Port Zero	drop	1
162.244.28.58	Canada	147.237.76.202	e.halag.idf.il	L4 Source or Dest Port Zero	drop	1
162.244.28.58	Canada	147.237.76.39	mobile.meitav.idf.il	L4 Source or Dest Port Zero	drop	1

12-17-2015-10:04:01 to 12-17-2015-11:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.80	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

12-17-2015-10:04:01 to 12-17-2015-11:04:01

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	2
188.42.136.164	147.237.8.28	Luxembourg	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
166.63.125.149	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
109.67.129.55	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.182.39.243	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.75	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.17.127	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
188.42.136.164	147.237.8.45	Luxembourg	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
176.12.151.182	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.220.82	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.113	147.237.72.217	Ukraine	e.idf.il	ET SCAN NMAP -sS window 1024	1
79.177.34.144	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.39.222.253	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
2.52.21.177	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.177.148	147.237.77.216	Israel	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
188.42.136.164	147.237.8.46	Luxembourg	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1

12-17-2015-10:04:01 to 12-17-2015-11:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.177.200.234	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	42
46.19.86.75	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	40
80.178.215.107	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	39
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	28
192.117.142.97	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
107.167.99.113	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	23
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
5.102.247.244	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
5.102.254.189	Israel	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
207.241.229.104	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	15
79.183.3.244	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
94.230.93.239	Israel	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
157.55.2.166	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.65.26.24	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	10
37.26.148.140	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	10
37.26.146.165	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	10
59.38.97.59	China	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
2.52.49.198	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
37.26.147.185	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
46.19.85.112	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.103	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
207.241.229.104	United States	147.237.77.216	dover.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	7
84.228.151.180	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.178.144.212	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.102.99	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.182.195.80	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
94.230.93.229	Israel	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.118.27.253	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
80.179.204.11	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.103	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	6
62.219.110.116	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.178.161.140	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.108.192.240	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.102	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
80.179.209.168	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.183	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.182.39.243	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	6
80.178.97.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.39.243	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.19.85.148	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.86.103	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
91.135.102.191	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
37.26.147.185	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	5
46.19.85.120	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.26.147.185	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
217.194.199.124	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.85.27	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.52.49.198	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
37.46.39.248	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.52.49.198	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4

12-17-2015-10:04:01 to 12-17-2015-11:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	124
46.19.86.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	100
5.102.247.244	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	63
46.19.86.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	58
46.19.86.137	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.137	Block	35
46.19.86.254	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 46.19.86.254	Block	30
109.253.195.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
2.52.26.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
46.19.85.72	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
37.26.148.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
37.26.148.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
192.117.142.97	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
2.54.171.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
93.172.191.135	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/2/	Block	3
46.19.86.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.18.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.148.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.211.107	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
207.46.13.180	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/cmspages/getresource.ashx	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
209.88.198.1	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
93.172.191.135	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 93.172.191.135	Block	2
183.83.48.154	India	147.237.77.176	matpash.idf.il	PHP Attempt	Block	2
37.26.148.224	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
207.46.13.128	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.128	Block	2
2.54.22.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
212.25.102.57	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.25.102.57	Block	2
5.22.134.76	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.22.134.76	Block	2
183.83.48.154	India	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	2
193.34.57.101	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
212.25.102.57	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/faqselection.aspx	Block	2
45.55.165.208		147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to /	Block	1
2.52.25.16	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.179.37.247	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
212.179.177.148	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
77.125.155.110	Israel	147.237.0.16	my-kosher-kravi.idf.il	Parameter Type Violation Master$ContentPlaceHolder1$remark in my-kosher-kravi.idf.il/ajax/reserveschedule/trainingformiframe.aspx	Block	1
66.249.64.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/9/63009.doc	Block	1
5.29.1.89	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
95.90.224.124	Germany	147.237.77.216	dover.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 95.90.224.124	Block	1
2.52.174.228	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
84.108.192.240	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.221	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
192.114.23.211	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/resources/images/favicon/favicon.png	Block	1
79.182.39.243	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
37.142.239.122	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.12.145.217	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
31.168.21.77	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.64.98.213	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

12-17-2015-10:04:01 to 12-17-2015-11:04:01