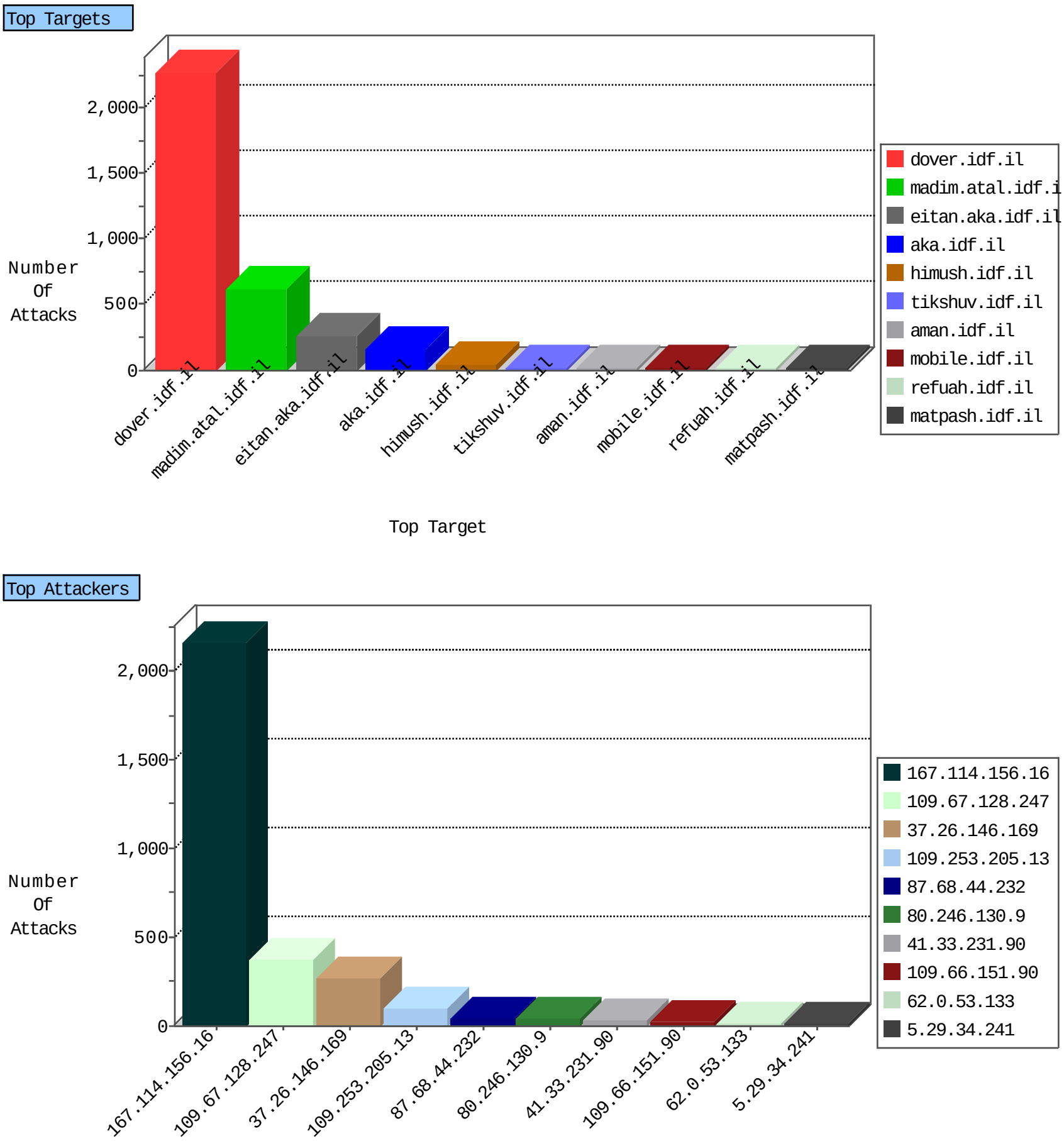
01-22-2016-10:04:00 to 01-22-2016-11:04:00

IDF Under Attack Daily Report



01-22-2016-10:04:00 to 01-22-2016-11:04:00

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	3074
109.67.128.247	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	481
5.189.169.156	Germany	147.237.8.27	e.madim.atal.idf.il	L4 Source or Dest Port Zero	drop	1
5.189.169.156	Germany	147.237.77.234	halag.idf.il	L4 Source or Dest Port Zero	drop	1
5.189.169.156	Germany	147.237.76.196	e.sviva.idf.il	L4 Source or Dest Port Zero	drop	1
5.189.169.156	Germany	147.237.77.178	e.matpash.idf.il	L4 Source or Dest Port Zero	drop	1
5.189.169.156	Germany	147.237.72.217	e.idf.il	L4 Source or Dest Port Zero	drop	1
89.248.172.201	Netherlands	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
5.189.169.156	Germany	147.237.76.198	e.yohalan.idf.il	L4 Source or Dest Port Zero	drop	1
5.189.169.156	Germany	147.237.0.34	tikshuv.idf.il	L4 Source or Dest Port Zero	drop	1
5.189.169.156	Germany	147.237.77.212	e.dover.idf.il	L4 Source or Dest Port Zero	drop	1
5.189.169.156	Germany	147.237.76.30	himush.idf.il	L4 Source or Dest Port Zero	drop	1
104.255.70.247		147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
5.189.169.156	Germany	147.237.76.202	e.halag.idf.il	L4 Source or Dest Port Zero	drop	1
5.189.169.156	Germany	147.237.8.14	e.orchot.idf.il	L4 Source or Dest Port Zero	drop	1
5.189.169.156	Germany	147.237.77.226	www.chamatz.aka.idf.il	L4 Source or Dest Port Zero	drop	1
5.189.169.156	Germany	147.237.76.44	e.refuah.idf.il	L4 Source or Dest Port Zero	drop	1
5.189.169.156	Germany	147.237.77.121	e.navy.idf.il	L4 Source or Dest Port Zero	drop	1

01-22-2016-10:04:00 to 01-22-2016-11:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
91.228.196.139	Poland	147.237.77.216	dover.idf.i	C076: HTTP: Access to - action=... (General)	Block	1
172.245.218.130	United States	147.237.77.216	dover.idf.i	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1

01-22-2016-10:04:00 to 01-22-2016-11:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
80.246.130.9	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	17
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.66.75	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	2
66.249.66.33	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
88.204.187.90	147.237.72.14	Kazakstan	dover.idf.il(old)	ET SCAN NMAP -sS window 4096	1
50.23.96.210	147.237.0.33	United States	idf.il	ET SCAN Potential SSH Scan	1
195.216.176.244	147.237.76.177	Latvia	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
50.23.96.210	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
183.3.202.115	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
183.3.202.115	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
169.50.77.72	147.237.77.216	Switzerland	dover.idf.il	ET SCAN NMAP -sS window 1024	1
159.8.109.19	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.76.198	Netherlands	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
50.23.96.210	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
183.3.202.115	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
183.3.202.115	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
163.172.13.173	147.237.72.166	United Kingdom	aka.idf.il	ET SCAN NMAP -sS window 1024	1
108.168.185.133	147.237.76.201	United States	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1

01-22-2016-10:04:00 to 01-22-2016-11:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
37.26.146.169	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	249
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
109.66.151.90	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
62.0.53.133	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
80.246.130.9	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
80.246.130.9	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
2.54.51.109	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
37.26.146.169	Israel	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
46.19.85.108	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
5.29.127.89	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
37.26.149.150	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
81.218.63.91	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
172.250.65.69	United States	147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
185.38.14.215	Netherlands	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
79.183.207.92	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.0.73.124	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
157.55.39.173	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.136.29	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
109.253.202.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.117.197	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.144.25	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.230.86.247	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.0.80.195	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.38.66	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.203	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.136.29	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
130.193.37.16	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.147.143	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
62.219.213.133	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.171.157	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.160.210.220	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.137.217	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.180.215	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.232.158	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.121.123.18	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
80.246.137.217	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
40.77.167.64	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.86.140	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
77.87.228.70	Germany	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
54.183.174.52	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
77.87.228.70	Germany	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
54.183.189.218	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
149.78.198.160	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
46.19.85.254	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
84.108.118.66	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.233	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
188.120.148.170	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
40.77.167.57	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2

01-22-2016-10:04:00 to 01-22-2016-11:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.67.128.247	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	182
109.67.128.247	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	145
109.253.205.13	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	64
87.68.44.232	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	44
109.253.205.13	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	35
5.29.34.241	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	15
176.13.20.159	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
93.172.117.219	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	11
176.13.3.175	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
80.246.136.111	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	7
87.68.156.149	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
80.246.139.36	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
2.54.33.139	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
109.65.175.246	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	4
172.250.65.69	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized HTTP Method	Block	4
172.250.65.69	United States	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 172.250.65.69	Block	4
46.116.151.201	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.160.42	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
87.69.197.101	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.147.160	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
85.64.32.214	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
93.172.255.125	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
5.29.225.47	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	3
84.109.149.39	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
109.65.175.246	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.54.14.208	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	2
84.94.33.117	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
37.26.149.138	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
95.86.118.204	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-18416-he/dover.aspx&sa=u&ved=0ahukewinqq-yhr3kahviyq4khsszdqwqfggzma4&usg=afqjcnf1lwaepxrqmvsoysizszlop2txsq	Block	2
62.128.41.133	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
184.105.139.67	United States	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to 147.237.0.19/	Block	1
40.77.167.57	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/misrot.aspx	Block	1
79.182.63.87	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.120.56.7	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
207.46.13.36	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
46.19.85.19	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
176.13.1.14	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	1
37.26.146.169	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/1117-en/eitan/more information.aspx	Block	1
109.160.173.110	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
74.82.47.2	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
2.52.160.227	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
95.86.121.29	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/&sa=u&ved=0ahukewjkgouvgl3kahvjohqkhwl5da8qfggimaa&usg=afqjcnhcvyyg7w1cq-yhd5_ammzoyodtwa	Block	1
62.219.98.201	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/matash/payslips/payslipslist.asp	Block	1
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
185.32.179.104	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.228.12.214	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1

01-22-2016-10:04:00 to 01-22-2016-11:04:00