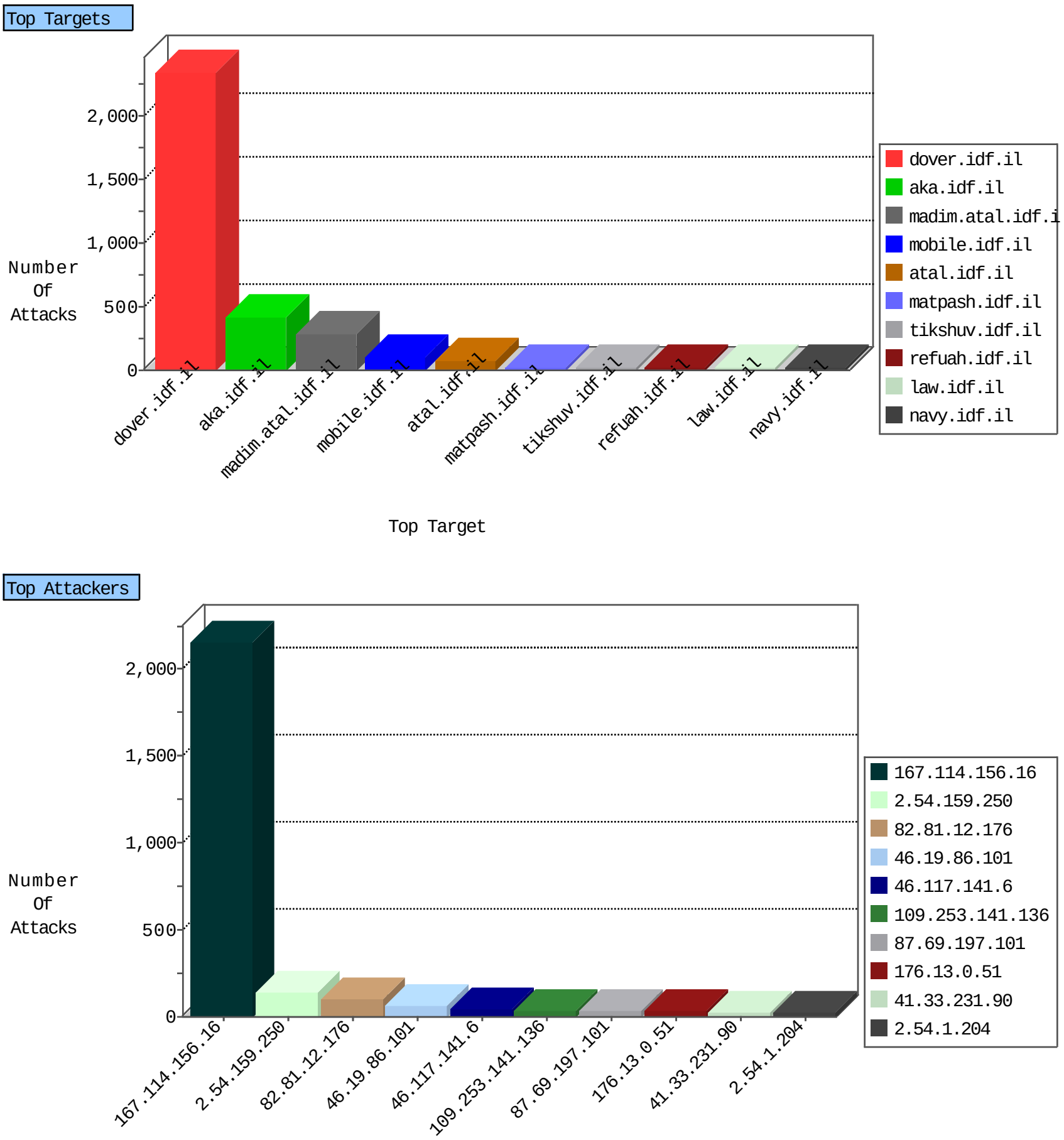
01-21-2016-19:04:05 to 01-21-2016-20:04:05

IDF Under Attack Daily Report



01-21-2016-19:04:05 to 01-21-2016-20:04:05

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	3058
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	105
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
89.248.172.110	Netherlands	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
89.248.172.110	Netherlands	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
89.248.172.110	Netherlands	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
89.248.172.110	Netherlands	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
89.248.172.110	Netherlands	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
80.82.78.39	Netherlands	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
89.248.172.110	Netherlands	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
89.248.172.110	Netherlands	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
89.248.172.110	Netherlands	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
78.184.0.118	Turkey	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
89.248.172.110	Netherlands	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
89.248.172.110	Netherlands	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
80.82.78.39	Netherlands	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
89.248.172.110	Netherlands	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
89.248.172.110	Netherlands	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
89.248.172.110	Netherlands	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
80.82.78.39	Netherlands	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
89.248.172.110	Netherlands	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
89.248.172.110	Netherlands	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
89.248.172.110	Netherlands	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
89.248.172.110	Netherlands	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
89.248.172.110	Netherlands	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
80.82.78.39	Netherlands	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
89.248.172.110	Netherlands	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1

01-21-2016-19:04:05 to 01-21-2016-20:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
198.50.134.71	Canada	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
208.69.31.10	United States	147.237.0.15	kosher-kravi.idf.il	10711: HTTP: ZmEu Vulnerability Scanner	Block	1
208.69.31.10	United States	147.237.0.17	m.my-kosher-kravi.idf.il	10711: HTTP: ZmEu Vulnerability Scanner	Block	1

01-21-2016-19:04:05 to 01-21-2016-20:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	12
109.253.141.136	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
109.253.143.166	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
222.186.58.169	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
108.168.185.133	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.76.197	China	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
104.219.238.10	147.237.76.176		test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
94.138.215.138	147.237.72.156	Turkey	aman.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
193.105.134.220	147.237.72.166	Sweden	aka.idf.il	ET SCAN NMAP -sS window 1024	1
37.142.68.63	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
180.97.106.161	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.36	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
168.62.238.153	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
113.59.33.61	147.237.8.14	China	e.orchot.idf.il	ET SCAN NMAP -f -sS	1
222.186.58.169	147.237.76.42	China	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
222.186.58.169	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.219.238.10	147.237.77.233		atal.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.72.166	China	aka.idf.il	ET SCAN NMAP -sS window 1024	1
94.138.215.138	147.237.72.166	Turkey	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
192.115.67.55	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
31.210.188.111	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
180.97.106.37	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.36	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
113.59.33.61	147.237.8.14	China	e.orchot.idf.il	ET SCAN NMAP -sS window 2048	1

01-21-2016-19:04:05 to 01-21-2016-20:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.86.101	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
2.54.1.204	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
82.145.217.217	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	23
46.19.85.225	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
109.253.141.136	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
185.120.125.25		147.237.72.166	aka.idf.il	drop	SAM rule	drop	13
31.168.93.54	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.178.155.150	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.141.136	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	12
94.159.150.177	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
94.159.150.177	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
79.182.174.105	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
79.182.119.250	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
77.127.177.115	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.142.68.63	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
95.97.13.10	Netherlands	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
94.230.86.237	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
104.187.110.229	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.85.140	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.22.135.231	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.15	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
192.114.105.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
80.249.75.230	Algeria	147.237.77.216	dover.idf.il	drop		drop	6
46.19.85.15	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.108.172.100	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
66.249.78.12	United States	147.237.0.19	madim.atal.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.136.165	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.140	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.178.154.45	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
91.200.12.7	Ukraine	147.237.77.74	law.idf.il	drop	SAM rule	drop	5
37.26.149.215	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
213.57.182.163	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
213.57.182.163	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.104	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
213.57.34.81	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
109.65.139.40	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
79.178.229.83	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
91.200.12.7	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
188.120.148.192	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
91.200.12.136	Ukraine	147.237.77.74	law.idf.il	drop	SAM rule	drop	4
149.50.101.66	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
85.64.29.229	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.104	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
77.125.8.211	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.135.72	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.212.45	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.159.250	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
46.117.141.6	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	47
87.69.197.101	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	30
176.13.0.51	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
2.54.159.250	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	28
46.19.85.175	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	10
176.13.17.232	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
109.253.212.45	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
80.246.136.224	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.142.234.2	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 37.142.234.2	Block	3
213.8.204.55	Israel	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	2
104.187.110.229	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	2
89.139.143.155	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
84.109.178.170	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â	Block	2
2.54.147.77	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.15.163	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
79.182.174.105	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.85.140	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.120.125.105		147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
89.138.127.8	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
80.246.137.136	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	1
68.180.229.173	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.157.81	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.108.172.100	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.142.234.2	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/6/110476.pdf	Block	1
176.228.52.3	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.54.141.243	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
149.88.25.91	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.181.162.117	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/general.aspx	Block	1
109.64.26.191	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.161	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/tizmoret/gallery/showpicture.asp	Block	1
188.166.40.236	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
31.154.162.133	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.1.20	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.137.241	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.125.158.220	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
104.194.26.205	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
62.219.193.62	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/general.aspx	Block	1
213.57.182.163	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.38	Israel	147.237.76.42	refuah.idf.il	Malformed URL	Block	1
178.155.24.170	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi'a=0	Block	1
149.88.48.164	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
79.182.119.250	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
109.64.199.34	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/iraq/english/info07.asp	Block	1
46.19.86.54	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
204.13.201.138	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
93.173.161.204	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
83.130.107.10	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
31.168.201.225	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1