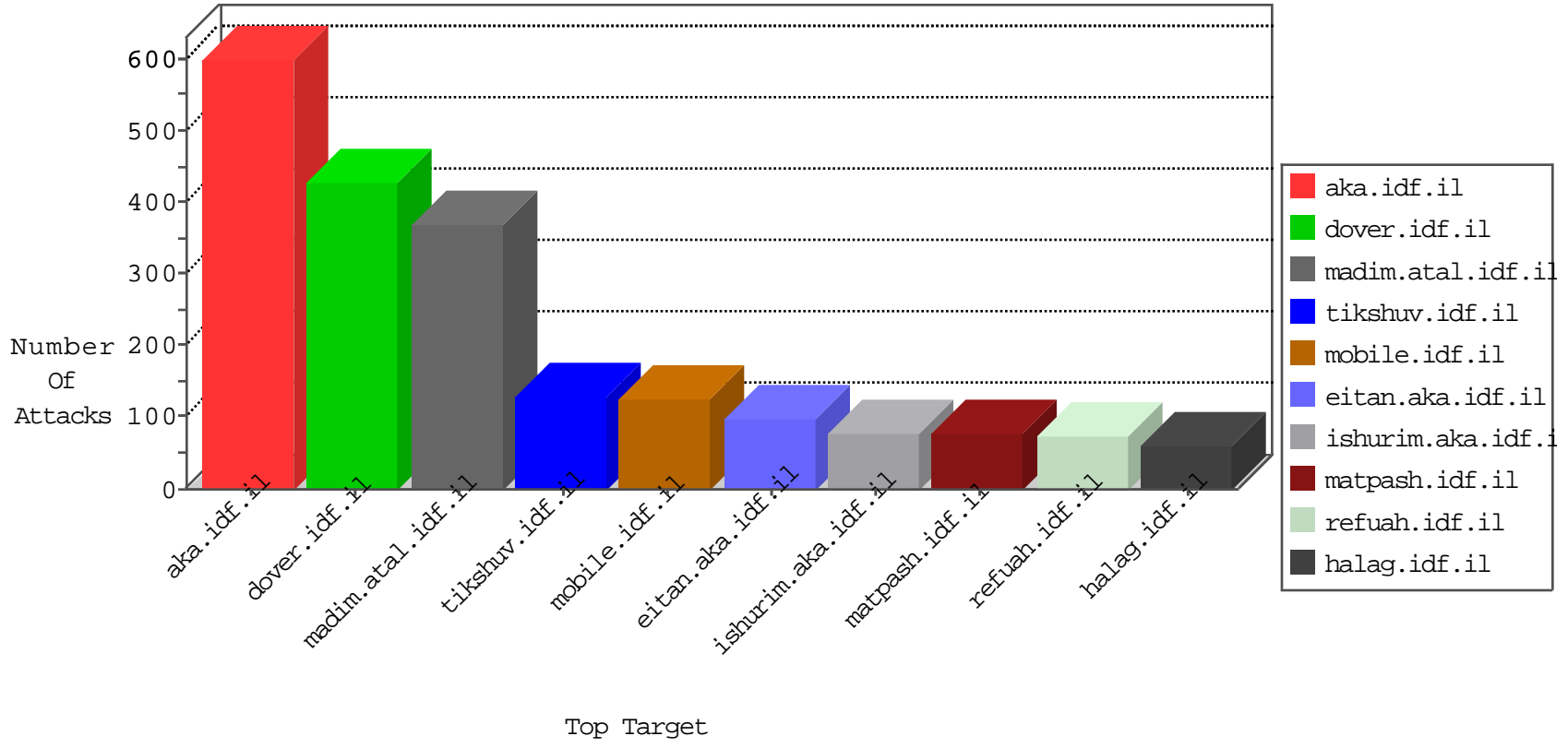


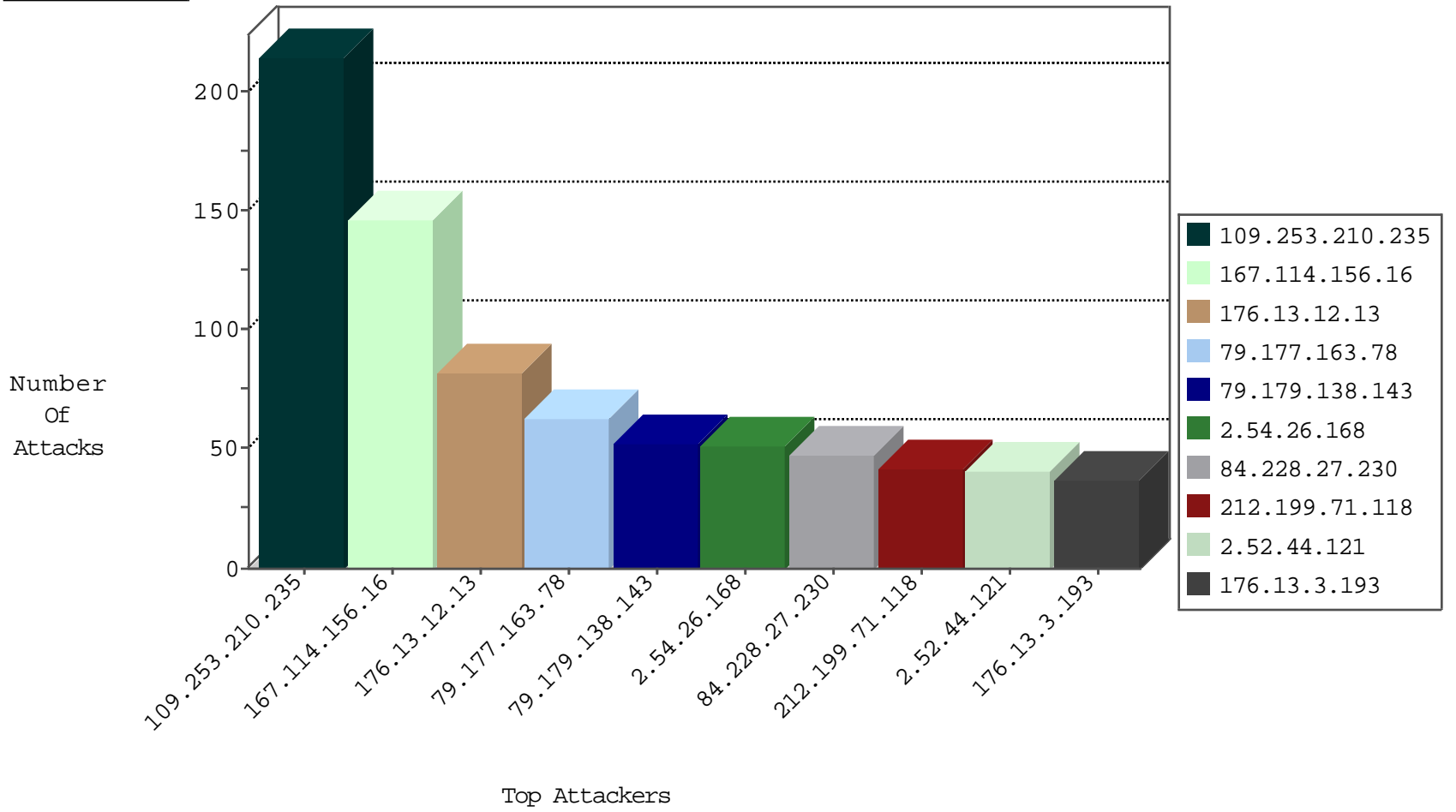
IDF Under Attack Daily Report



Top Targets



Top Attackers



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	2784
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	125
79.179.52.174	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
109.200.30.168	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
167.114.156.16	Canada	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	6
80.246.136.41	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	5
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
52.33.66.29	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
207.46.13.142	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
105.96.73.11	Algeria	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
31.168.240.21	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
162.213.153.152	United States	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
66.240.236.119	United States	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
151.217.178.35		147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
80.246.136.41	147.237.77.216	Israel	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	5
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
66.249.78.2	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
62.219.99.130	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
132.74.213.111	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
62.0.103.156	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
98.211.117.184	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.108	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.173.187.114	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.128.66	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.250.114.20	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.8.204.35	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.181.108.120	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
178.169.143.78	147.237.77.179	Bulgaria	e.mazi.idf.il	ET SCAN NMAP -sS window 4096	1
77.127.149.202	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
151.217.178.88	147.237.77.233		atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
62.219.164.244	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
151.217.178.88	147.237.0.16		my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
62.90.192.226	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
108.61.164.250	147.237.76.201	United States	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
46.121.142.11	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
95.156.251.10	147.237.0.17	Germany	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
36.37.149.245	147.237.77.216	Cambodia	dover.idf.il	portscan: TCP Distributed Portscan	1
93.173.27.64	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.64.5.161	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.183.181.210	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.180.204.97	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
151.217.178.88	147.237.77.234		halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
151.217.178.88	147.237.72.166		aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.177.163.78	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	63
2.54.26.168	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	51
79.179.138.143	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
84.228.27.230	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
46.19.86.120	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	27
80.179.7.163	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	26
77.126.221.124	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	26
109.64.159.67	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	24
212.199.34.114	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	24
213.57.143.65	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	23
79.181.160.73	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
80.246.136.60	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
77.127.174.190	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
149.154.245.31	Belgium	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	18
15.90.166.12	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	17
5.102.105.230	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	16
31.168.180.89	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
46.19.85.17	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
2.54.128.66	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.17	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
2.52.159.188	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.140	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.199.71.118	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
212.199.71.118	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
2.52.162.149	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
2.52.44.121	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
92.74.93.104	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.86.100	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.200	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.167.157	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
46.19.85.74	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.179.28.34	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
130.203.136.75	United States	147.237.77.74	law.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	8
113.22.40.65	Vietnam	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
109.253.142.189	Israel	147.237.76.30	hinush.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
46.19.85.222	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	8
5.29.142.44	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.253.142.189	Israel	147.237.76.30	hinush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
212.199.71.118	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
195.160.240.11	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
149.78.251.10	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.126	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.44.121	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.127.230.249	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.21.28	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.158.169	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.208	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		alert	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.210.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	134
109.253.210.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	81
176.13.12.13	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	80
176.13.3.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
79.179.138.143	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
84.108.139.53	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	13
84.228.27.230	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	12
213.8.204.58	Israel	147.237.0.34	tikshuv.idf.il	Distributed Suspicious Response Code	Block	12
37.26.147.161	Israel	147.237.0.34	tikshuv.idf.il	Distributed Suspicious Response Code	Block	12
80.246.136.60	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	10
109.253.211.60	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
217.194.193.245	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	6
80.246.136.163	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
31.168.137.108	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 31.168.137.108	Block	5
176.13.11.158	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	4
46.19.86.140	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	4
176.13.11.158	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
176.13.15.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.195	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	3
185.32.179.69	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.121.213.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.34	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.11.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.34	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
109.65.176.189	Israel	147.237.0.34	tikshuv.idf.il	Distributed Suspicious Response Code	Block	3
176.13.16.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.23.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.142.68.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.38	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
93.173.161.139	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
109.226.44.76	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/	Block	3
176.12.142.50	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
40.77.167.105	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	2
109.253.131.29	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.29.142.44	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
2.54.32.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.181.160.73	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/shared/ajax/lightboxmediagallery.aspx	Block	2
109.253.137.40	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	2
194.114.146.227	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
185.3.144.32	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.182.77	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
79.177.97.111	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
185.32.179.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.78.111	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
173.252.89.56	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.149.184	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
87.69.155.138	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https://www.idf.il/	Block	1
185.50.251.115	Ukraine	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-en/dover.aspx	Block	1
15.90.166.12	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;t in www.aka.idf.il/main/kapatz/scriptresource.axd	None	1
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1