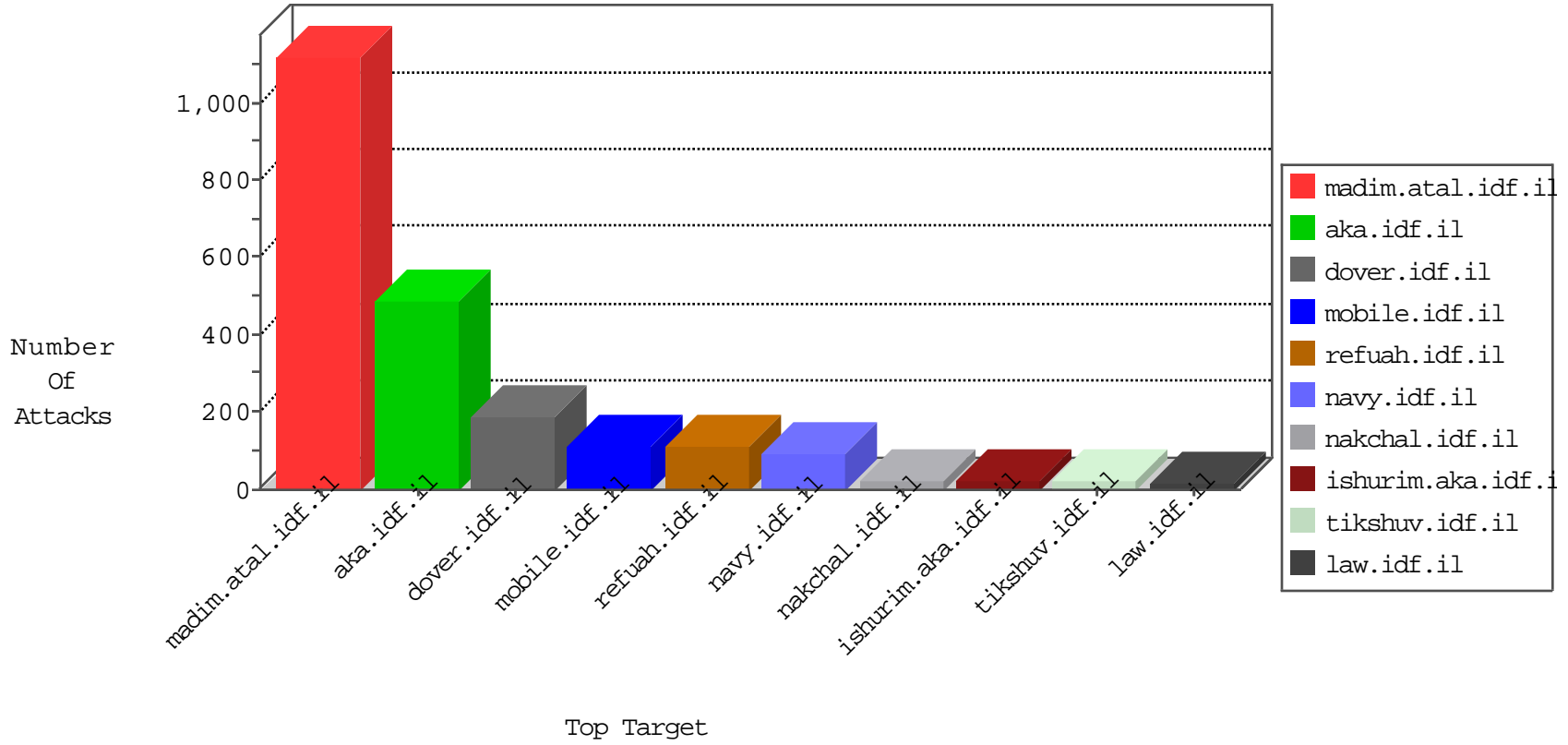


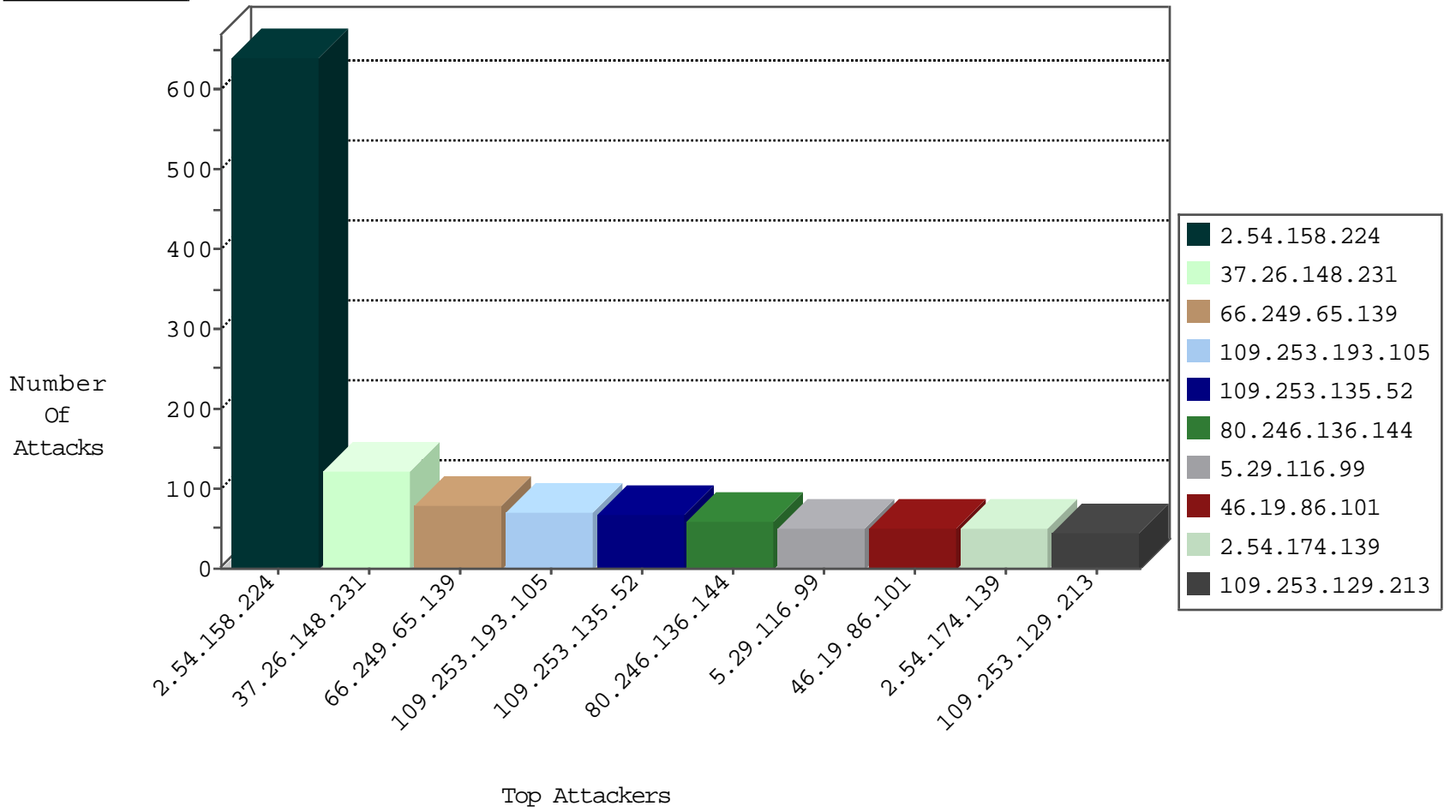
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	9
193.242.218.6	Switzerland	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
199.203.62.54	Israel	147.237.76.200	eitan.aka.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
66.249.65.139	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	80
66.249.93.105	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sA (2)	3
66.249.93.97	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sA (2)	2
209.126.116.147	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	2
46.19.85.218	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.0.40	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.143.233.144	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.112	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.218.241.25	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.182.36.197	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.116.62.149	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.128.233	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
217.132.128.57	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
91.228.248.251	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.183.126.12	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.54.174.139	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	50
62.219.166.143	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	30
5.29.116.99	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	28
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	23
5.29.116.99	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	22
46.19.85.142	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
176.13.18.24	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
2.54.43.21	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
109.66.48.24	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	15
46.19.85.224	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
193.191.219.80	Belgium	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
46.19.85.53	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
85.130.231.75	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
213.8.204.61	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
62.0.200.166	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
212.179.218.166	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.132.127	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.113	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.160	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	11
109.66.48.24	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
188.120.148.197	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
80.246.136.117	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
80.246.139.200	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.255	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.101	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
31.168.65.25	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.178.237.240	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.129	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.212	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
66.249.78.216	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
81.218.147.140	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
37.26.147.240	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.251.81	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
195.160.242.40	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.178.6.76	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.81.18.93	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.158.224	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.235.68.235	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.32.68	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.75	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
188.120.148.27	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.154.102	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
91.200.12.106	Ukraine	147.237.77.74	law.idf.il	drop	SAM rule	drop	4
37.26.146.210	Israel	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
82.80.64.158	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
2.54.128.233	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.34.16	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-03-2016-12:04:05 to 02-03-2016-13:04:05

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.253.142.217	Israel	147.237.72.166	aka.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
2.54.158.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	364
2.54.158.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	153
2.54.158.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	116
37.26.148.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	87
109.253.135.52	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	67
80.246.136.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	58
46.19.86.101	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	50
109.253.193.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	48
109.253.129.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	44
109.253.159.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	34
109.253.193.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
167.114.0.27	Canada	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 167.114.0.27	Block	21
109.253.215.45	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 109.253.215.45	Block	20
37.26.148.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	19
37.26.148.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
37.26.148.231	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 37.26.148.231	Block	15
149.88.28.41	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	14
85.250.25.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
109.253.132.127	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
85.250.25.2	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	4
46.19.86.113	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
79.178.165.168	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/gyus/authentication-service.aspx/getauthuser	Block	3
109.253.159.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.15.68	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
2.54.158.224	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.43.21	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
176.13.18.24	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
188.143.232.11	Russian Federation	147.237.76.30	himush.idf.il	Multiple Unauthorized URL Access from 188.143.232.11	Block	3
176.13.2.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	3
185.120.125.48		147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 185.120.125.48	Block	2
84.109.73.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.148.198	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
188.143.232.11	Russian Federation	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 188.143.232.11	Block	2
81.218.57.61	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
80.246.136.117	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
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	2
138.134.192.10	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	2
185.120.125.24		147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
84.108.110.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
209.88.196.250	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	2
188.143.232.11	Russian Federation	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 188.143.232.11	Block	2
192.198.151.44	Europe	147.237.72.166	aka.idf.il	Unknown Parameter amp;t in www.aka.idf.il/main/kapatz/scriptresource.axd	None	1
5.29.116.99	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
95.86.69.95	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/sip_storage/files/4/2924.pdf&sa=u&ved=0ahukewilq7mzrdvkahvb2hokhtiadskqfggymac&sig2=cpxzucukywit-nge0y6hbg&usg=afqjcnvnbdezptltdpil8i4caxmd_al-a	Block	1
66.249.93.99	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
46.19.86.244	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
167.114.0.27	Canada	147.237.77.216	dover.idf.il	Parameter Type Violation Language in www.idf.il/shared/ajax/getemergencybanner.aspx	Block	1