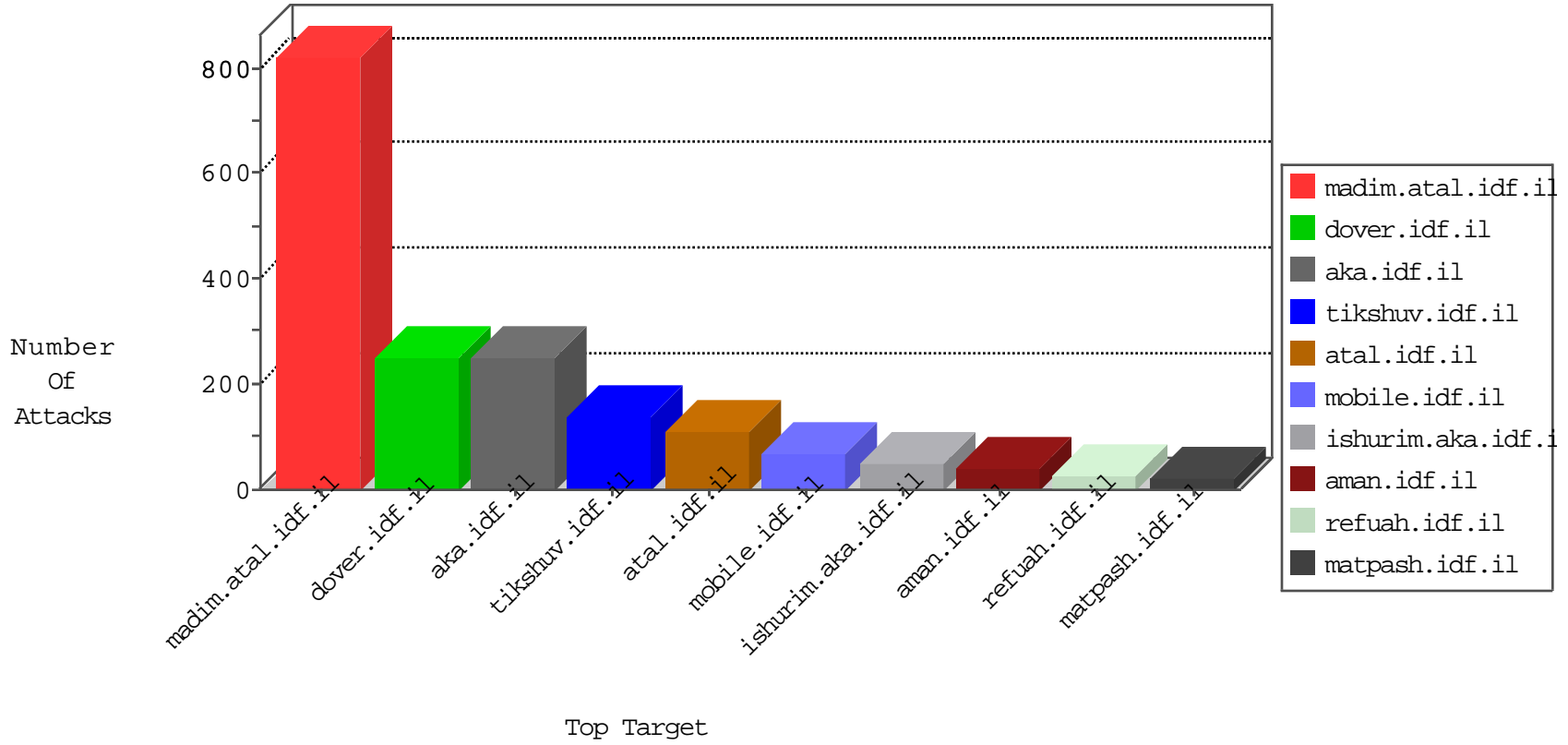


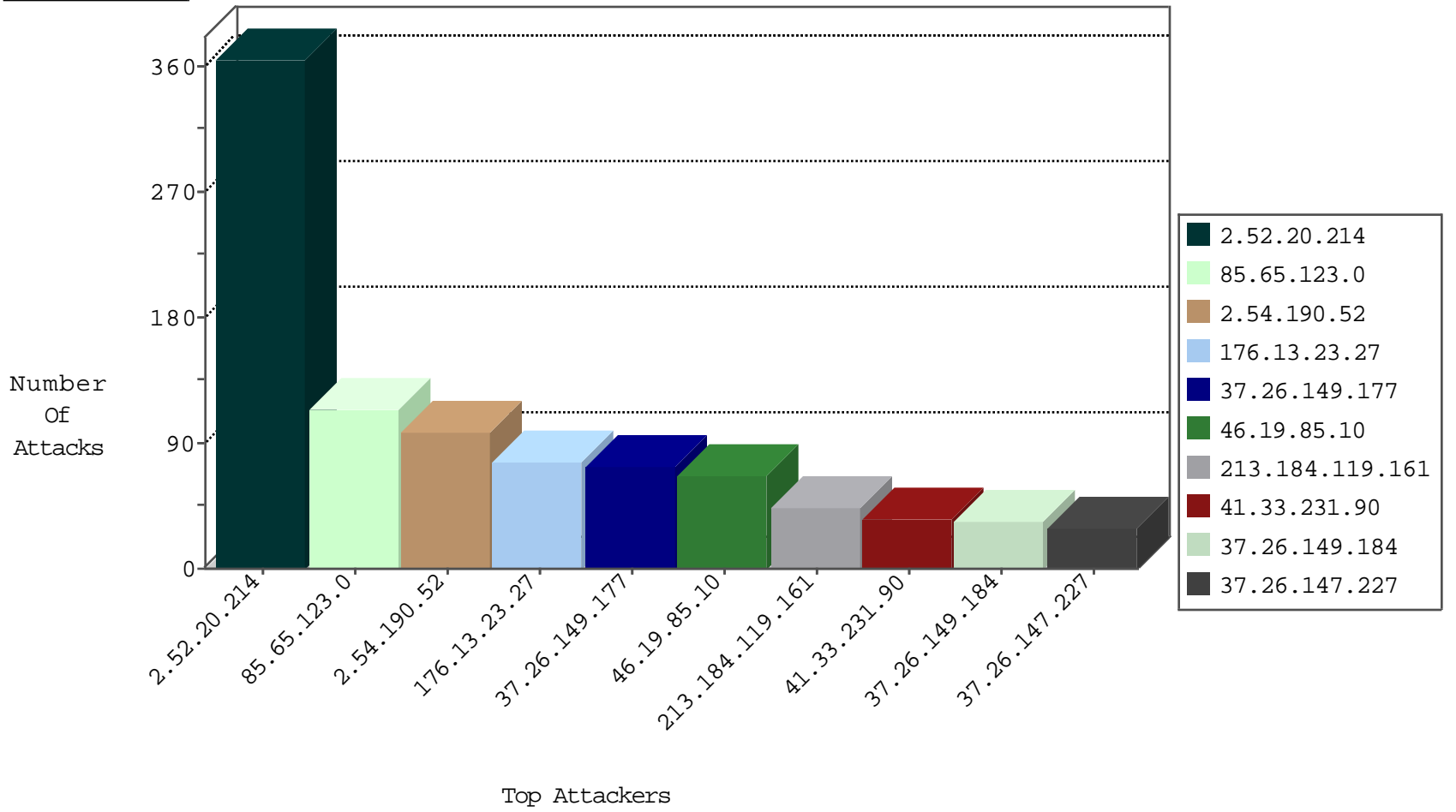
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.241.26	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	90
82.145.33.11	United Kingdom	147.237.76.44	e.refuah.idf.il	Block_Ip_Web_In	drop	1
142.54.169.162	United States	147.237.72.156	aman.idf.il	block-sp-traf1	drop	1
82.145.33.11	United Kingdom	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	1
82.145.33.11	United Kingdom	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	1
89.163.140.157	Germany	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
82.145.33.11	United Kingdom	147.237.76.38	e.e.meitav.idf.il	Block_Ip_Web_In	drop	1
89.163.140.157	Germany	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
81.218.208.46	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.247.80	Israel	147.237.77.176	matpash.idf.il	C008: HTTP: Xenu UserAgent	Block	1
192.240.106.106	United States	147.237.77.233	atal.idf.il	0543: HTTP: php.cgi Access	Block	1
212.154.250.21	Kazakstan	147.237.0.15	kosher-kravi.idf.il	C003: HTTP: phpMyAdmin access	Block	1
212.154.250.21	Kazakstan	147.237.76.31	nakchal.idf.il	C003: HTTP: phpMyAdmin access	Block	1
212.154.250.21	Kazakstan	147.237.76.86	navy.idf.il	C003: HTTP: phpMyAdmin access	Block	1
50.23.43.242	United States	147.237.72.166	aka.idf.il	0543: HTTP: php.cgi Access	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
79.183.242.178	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.45.137.67	147.237.77.179	Turkey	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
2.54.138.58	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.74	147.237.76.177	United States	ncore.idf.il	ET DROP Dshield Block Listed Source	1
109.65.18.166	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.69.200.168	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.45.137.67	147.237.77.233	Turkey	atal.idf.il	ET SCAN NMAP -sS window 1024	1
31.168.0.253	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.146.166	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.226.15.128	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.139.168.219	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
213.184.119.161	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	44
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
80.246.130.49	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	28
2.52.20.214	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
2.54.164.252	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
46.19.85.29	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	17
79.182.238.179	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
79.177.10.131	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
37.26.149.184	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
81.218.251.251	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
87.68.77.21	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
81.218.241.26	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	10
109.253.212.103	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
109.253.212.103	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
2.52.20.214	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
85.130.219.78	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
85.130.219.78	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.86.73	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	7
46.19.86.73	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
62.90.131.78	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
46.19.85.201	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.183.219.19	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.29	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.130.177.9	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.11.171	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.73	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
46.19.85.237	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.74	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
80.179.17.183	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
95.35.210.184	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.14.122	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.245	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.74	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.39.150	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.150	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.54.152.33	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.245	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.32.179.167	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.80	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.25.76	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.127.10.35		147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.80	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
208.115.111.73	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
79.179.131.108	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.81.227	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
62.219.166.203	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.54.42.222	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
81.218.241.25	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.52.20.214	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	171
2.52.20.214	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	159
85.65.123.0	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 85.65.123.0	Block	113
2.54.190.52	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	95
37.26.149.177	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	73
176.13.23.27	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	65
46.19.85.10	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	65
37.26.147.227	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
37.26.149.184	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	21
46.19.85.217	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	15
82.80.17.163	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	11
176.13.23.27	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	11
82.80.193.236	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	10
95.35.210.184	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
176.13.17.156	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
2.54.186.88	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
213.57.168.222	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
2.54.22.245	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	4
2.54.164.252	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
176.13.2.46	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
192.240.106.106	United States	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 192.240.106.106	Block	3
37.26.148.183	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/\$\$\$&?&?\$\$\$	Block	3
46.210.157.48	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.243	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.52.40.230	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.61	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
50.23.43.242	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 50.23.43.242	Block	3
79.182.217.144	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/8/	Block	3
212.179.21.194	Israel	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqantity.aspx	Block	2
109.253.204.130	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
37.46.39.147	Israel	147.237.0.19	madim.atal.idf.i	Distributed Unauthorized URL Access on madim.atal.idf.il/shared/ajax/updatemakatqantity.aspx	Block	2
37.26.149.160	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
167.114.156.198	Canada	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 167.114.156.198	Block	2
176.13.14.122	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
2.54.152.33	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
2.54.190.52	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	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
89.161.201.67	Poland	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/xmlrpc.php	Block	1
50.23.43.242	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/cgi-bin/php	Block	1
180.76.15.142	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
2.50.2.113	United Arab Emirates	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
81.218.251.250	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
46.19.85.170	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.46.39.123	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.179.223.31	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
5.22.130.68	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1