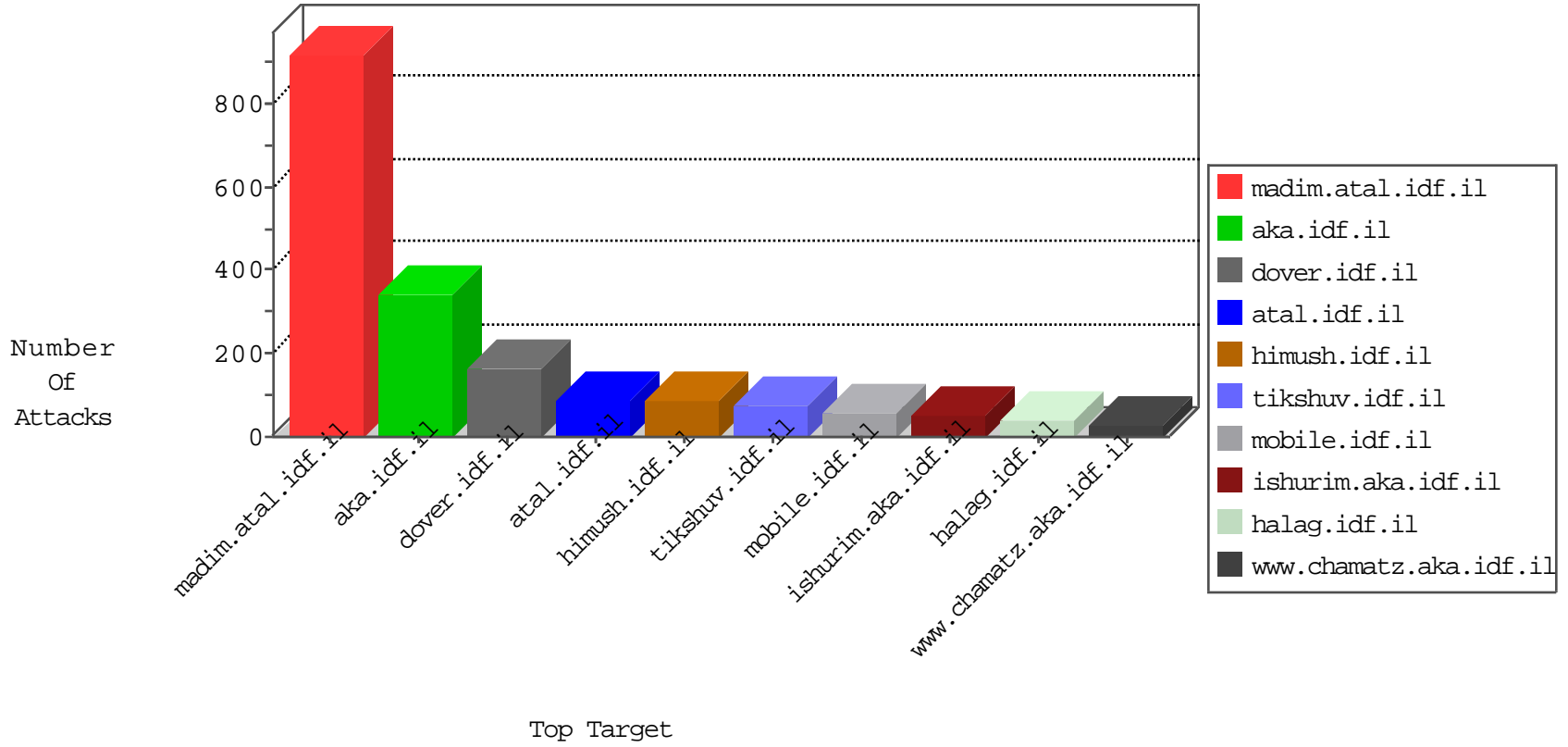


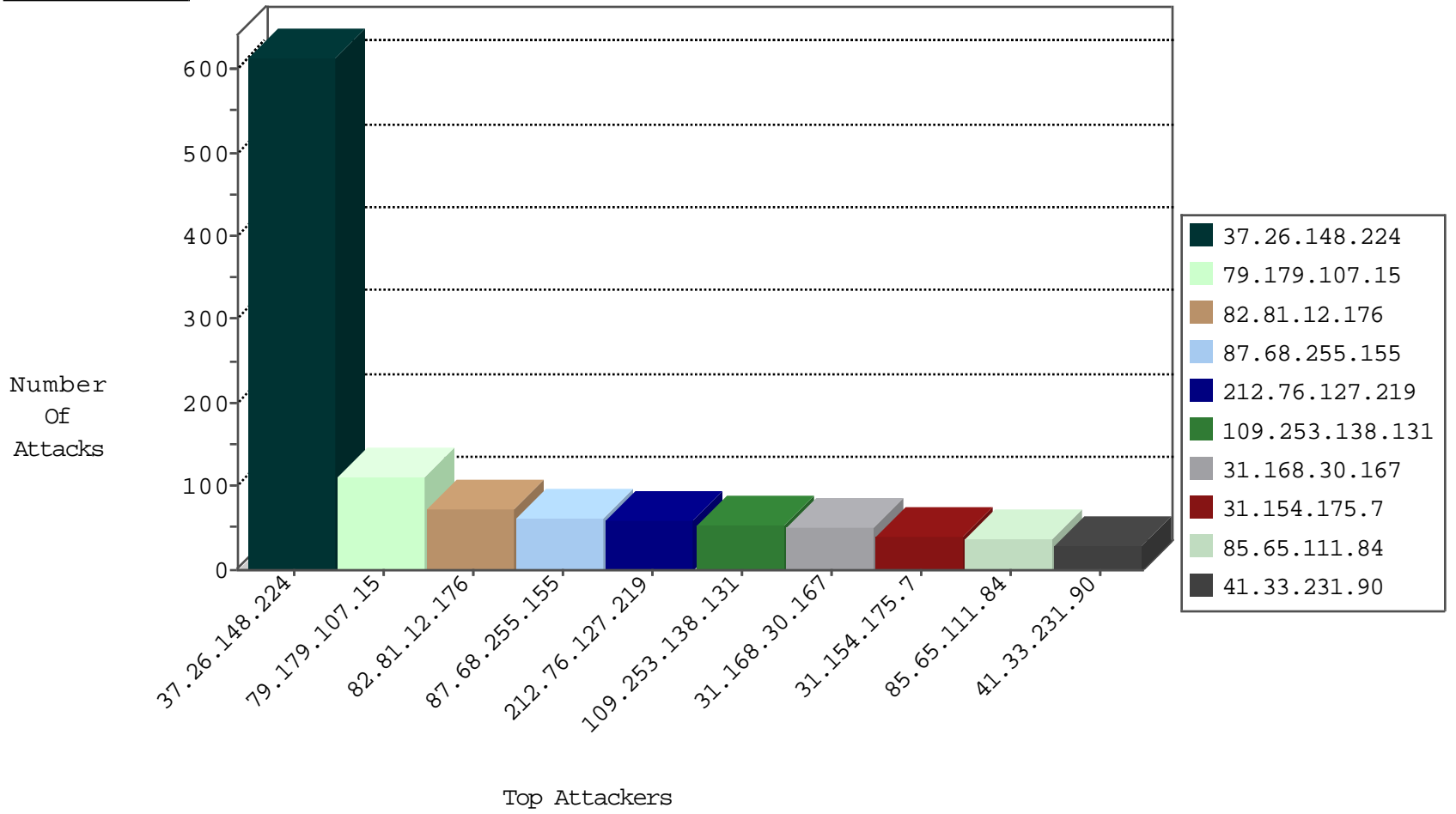
# IDF Under Attack Daily Report



### Top Targets



### Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	73
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
104.233.77.182		147.237.76.198	e.yohanan.idf.il	Block_Ntp_All_Net	drop	1
104.233.77.182		147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
104.233.77.182		147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.9.73.227	Germany	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	1
151.80.31.142	Italy	147.237.72.166	aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
37.26.148.224	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.64.92	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
94.76.9.90	147.237.72.14	Bahrain	dover.idf.il(old)	ET SCAN Potential VNC Scan 5900-5920	1
77.127.183.57	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
196.47.173.21	147.237.77.226	Cote D'Ivoire	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 4096	1
196.47.173.21	147.237.77.226	Cote D'Ivoire	www.chamatz.aka.idf.il	ET SCAN NMAP -f -sS	1
5.239.123.200	147.237.76.34	Iran, Islamic Republic of	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
183.60.48.25	147.237.77.216	China	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
180.97.106.162	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.37	147.237.77.176	China	matpash.idf.il	ET SCAN Potential SSH Scan	1
172.98.200.237	147.237.76.198		e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
94.76.9.90	147.237.72.156	Bahrain	aman.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
94.76.9.90	147.237.72.14	Bahrain	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
199.191.56.188	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 3072	1
196.47.173.21	147.237.77.226	Cote D'Ivoire	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 2048	1
31.168.246.151	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.2.138	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
180.97.106.162	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
172.98.200.237	147.237.76.198		e.yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
116.55.54.115	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.76.127.219	Israel	147.237.76.30	himush.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	60
85.65.111.84	Israel	147.237.72.167	ishurim.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	30
79.179.190.71	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	27
212.76.127.10	Israel	147.237.76.30	himush.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	18
31.154.175.7	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
46.19.85.118	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
31.154.175.7	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
2.52.129.10	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.76.127.44	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	12
46.19.85.195	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
5.29.76.202	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
176.13.21.166	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
84.108.35.92	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	10
176.13.21.166	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.19.85.84	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
87.68.255.155	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.84	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
62.0.200.202	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
37.26.147.210	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.162	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
63.246.61.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.121.123.18	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.64.4.12	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.125	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.117.98.67	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
31.154.167.26	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
31.154.167.26	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.197	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
188.120.148.197	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.102.198.201	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.197	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.228.231.43	Bulgaria	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.179.114.11	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.149.239	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.29.247.44	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
80.179.114.11	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.134.30	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.197	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
31.210.188.25	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
195.60.232.57	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
84.108.35.92	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.76.127.111	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
37.46.38.73	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.179.137.82	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
84.108.35.92	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
66.249.64.172	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.121.140.64	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
91.200.12.136	Ukraine	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.148.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	382
37.26.148.224	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 37.26.148.224	Block	159
79.179.107.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	96
37.26.148.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	67
87.68.255.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	53
109.253.138.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	53
31.168.30.167	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 31.168.30.167	Block	51
149.78.206.56	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
46.19.86.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
109.253.220.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
79.179.107.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	7
109.253.207.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
176.13.11.34	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
109.253.134.117	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.148.130	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 37.26.148.130	Block	3
2.54.34.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.181.61.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.136.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
31.168.243.88	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.0.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.160.166.9	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/about.aspx	Block	2
84.109.152.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
185.120.126.37		147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.120.227.178	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	2
84.228.231.43	Bulgaria	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/faq.aspx	Block	2
93.172.243.17	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	2
5.22.134.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.149.133	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
79.179.107.15	Israel	147.237.0.19	madim.atal.idf.il	Untraceable SSL Sessions: Open Mode	None	2
213.57.189.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.0.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.52.56.75	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.181.172.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
87.69.34.200	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	2
37.26.149.198	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
151.75.224.245	Italy	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/wp-admin/includes/index.php	Block	1
84.108.139.154	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.147.195	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.179.190.71	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
217.132.125.110	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/mas.aspx	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
185.32.179.4	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
31.154.175.7	Israel	147.237.72.166	aka.idf.il	Illegal HTTP Version Â°Â?[[#8]]Â@7_TÂ,u[[#18]]Â...[[#31]]Â... _[[#18]]~&[[#30]][[#26]]Â>Â*(QÂ..Â<Â³[[#22]]N[[#6]]],Â%Â+Â%Â%Â?Â*Â+ Â+*Â`Â-Â"v)Â-Â GÂ =TÂ.ZÂ%Â>Â%hsÂ... aÂ?Â^Â t<Â`EkAisÂCÂž	Block	1
105.110.72.60	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/wp-content/index.php	Block	1
46.19.85.195	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
2.52.135.31	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
87.68.85.250	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.183.52.233	Israel	147.237.72.166	aka.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 79.183.52.233	Block	1
79.178.60.234	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	1
207.46.13.87	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/900-he/atal.aspx	Block	1