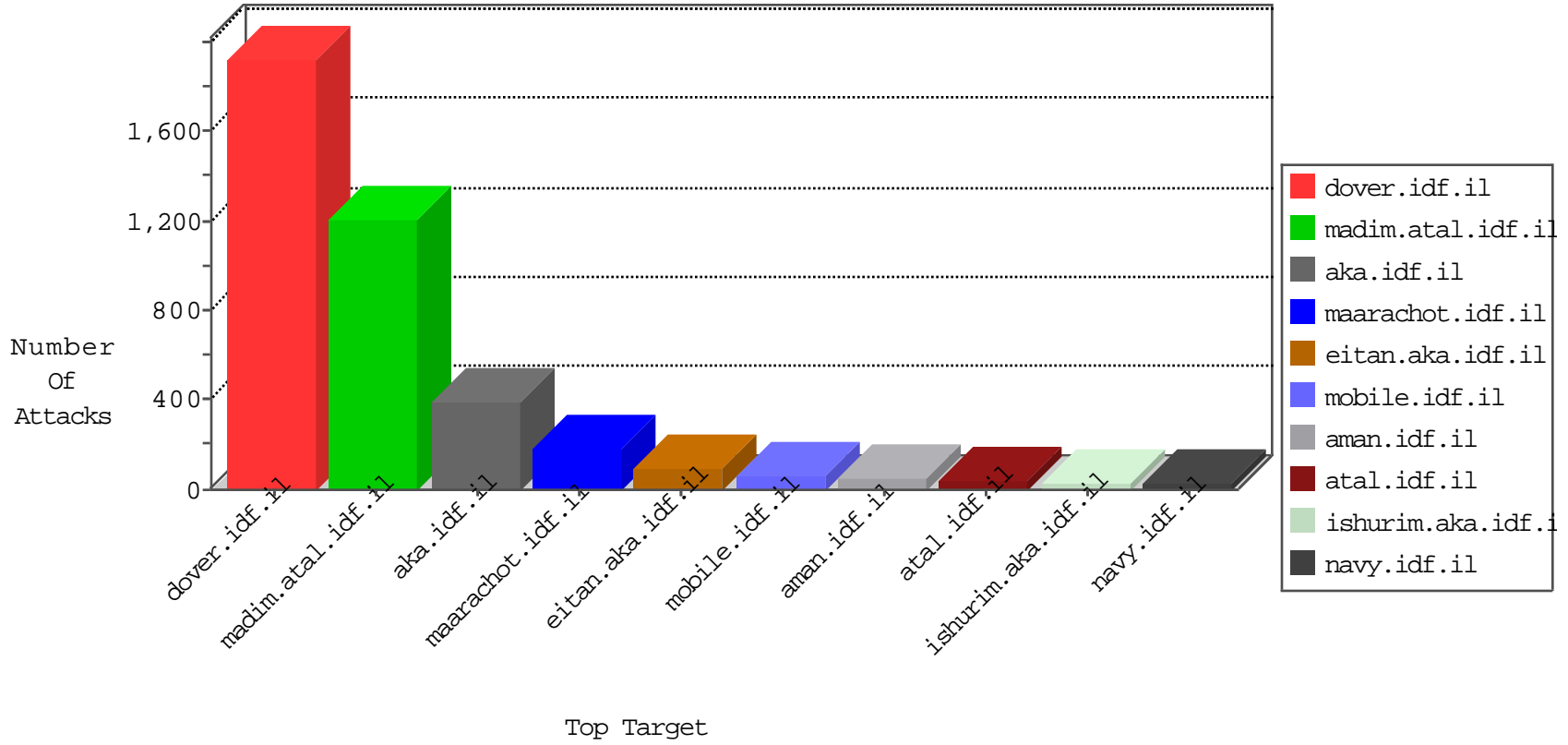


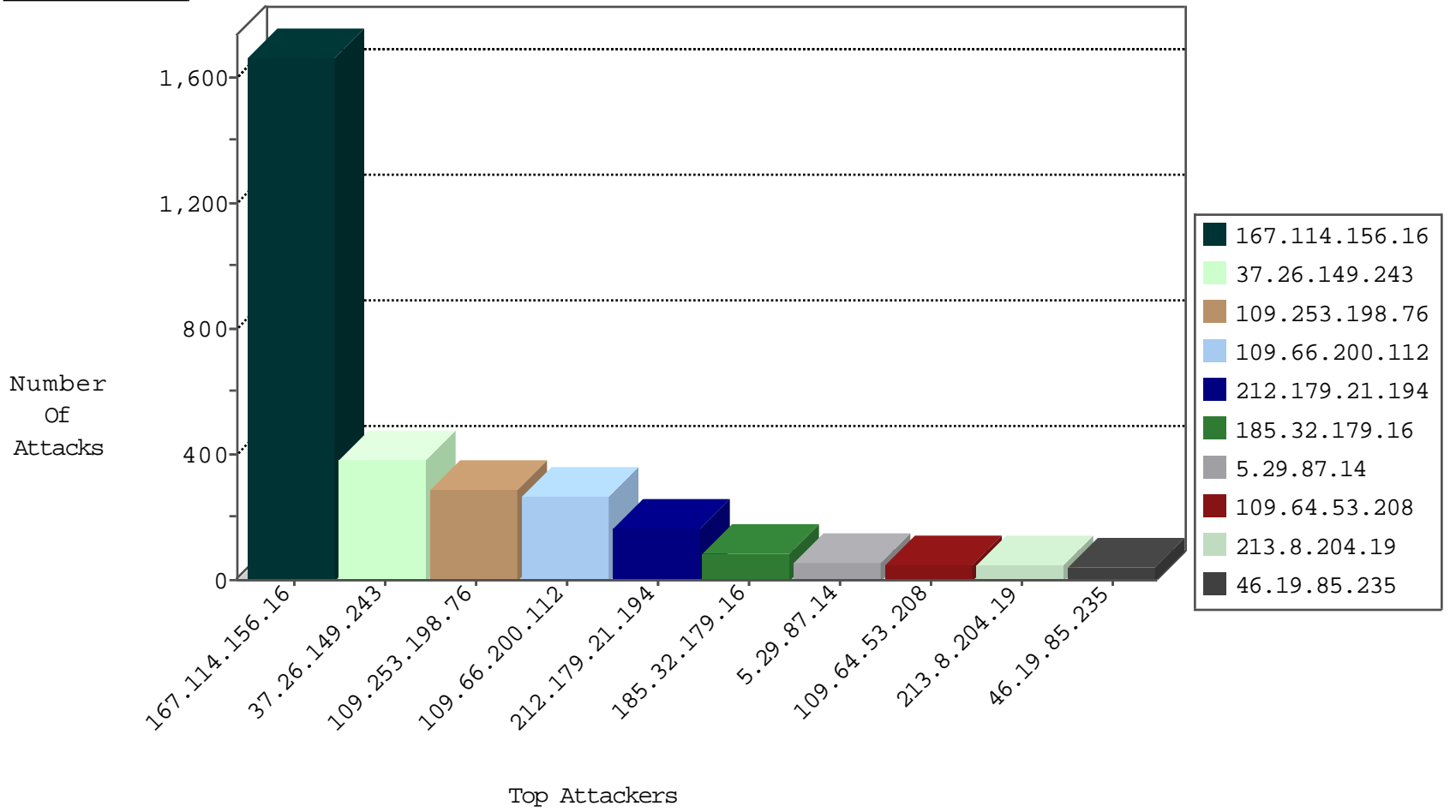
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.73.206	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	3975
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3260
66.249.73.198	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	374
66.249.78.254	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	18
134.147.203.115	Germany	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	2

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
72.9.157.128	United States	147.237.76.86	navy.idf.i	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
109.253.139.53	147.237.77.216	Israel	dover.idf.il	GPL SCAN myscan	2
37.26.149.243	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
109.253.139.53	147.237.77.216	Israel	dover.idf.il	INDICATOR-SCAN myscan	2
79.179.190.181	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.178.59	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
74.91.19.211	147.237.77.216	United States	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
198.20.69.75	147.237.76.42	United States	refuah.idf.il	ET DROP Dshield Block Listed Source	1
36.110.34.116	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
176.13.6.53	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.149.28	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
158.255.6.220	147.237.72.167	Russian Federation	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
109.66.43.187	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
107.191.63.157	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.21.92	147.237.77.216	China	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
79.179.207.99	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
222.186.21.92	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
79.177.52.232	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.39.222.196	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
109.66.132.203	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.194.153	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.108.25.255	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
222.186.21.92	147.237.76.86	China	navy.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
212.179.21.194	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	166
109.64.53.208	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	51
93.172.239.177	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	40
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
46.19.85.112	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	26
92.241.34.224	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
84.94.161.14	Israel	147.237.0.16	my-kosher-kravi.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
112.198.118.64	Philippines	147.237.72.166	aka.idf.il	drop	SAM rule	drop	16
77.127.217.15	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
147.236.232.15	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
84.94.119.85	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	10
2.54.22.249	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
37.26.149.243	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.14	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
84.228.235.129	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	9
176.13.14.20	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.249	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
84.94.119.85	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
109.66.163.80	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.87	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
85.130.245.195	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
85.65.138.212	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
185.120.125.24		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
187.10.166.71	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.52.7.17	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.65.138.212	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.180.21.168	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.143.242	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.214	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.40.195	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
46.19.85.249	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
185.120.126.122		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.235	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
82.145.209.125	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.214	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.183.137.162	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.65.106.143	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
109.66.3.253	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.53.62	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.249	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
217.132.49.246	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.249	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
109.253.143.242	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
31.210.188.102	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.22.129.136	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
199.30.25.102	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.232	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.190	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.198.76	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	175
37.26.149.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	162
109.66.200.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	129
37.26.149.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	108
109.253.198.76	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
109.66.200.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
37.26.149.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	96
185.32.179.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	81
5.29.87.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	52
213.8.204.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
46.19.85.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	42
2.52.172.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
109.66.200.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	32
2.52.7.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
109.253.198.76	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	5
46.19.85.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
2.54.158.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
80.246.136.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.127.57.123	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.18.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
93.172.181.220	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/size100x0/sip_storage	Block	2
37.26.149.243	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	2
71.215.126.22	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sacher	Block	2
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	2
46.19.85.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.14	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchildsubcategories/1423	Block	2
217.132.156.67	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Method from 217.132.156.67	Block	2
109.160.171.70	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
85.64.16.242	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
46.19.85.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
217.132.156.67	Israel	147.237.72.156	aman.idf.il	Multiple Illegal HTTP Version from 217.132.156.67	Block	2
176.13.14.20	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
84.108.153.250	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.8.204.72	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 213.8.204.72	Block	1
149.88.5.13	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.148.222	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
109.67.2.65	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
77.237.138.202	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to /	Block	1
207.46.13.75	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.75	Block	1
2.54.32.227	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1272-he/atal.aspx	Block	1
217.132.156.67	Israel	147.237.72.156	aman.idf.il	NULL Character in Method Ā°ĀŶZ8tm[[#5]]X%Ā°=Ā°)Ā°ĀĀ?Ā...Ā"ŶĀμĀŶ 9Ā°[[#12]]Ā^Ā°Ā?[[#8]]Ā #E)UĀ°[[#16]]1[[#4]]Ā°ĀŶ?ĀŶXĀ"[[#0]]qR(Ā·D QĀ°Oh4Ā, Ā^Ā^Ā>Ā-mĀ*ĀĀĀ°Ā;ĀŶ!ĀŶĀŶS[[#6]]/Ā@[[#20]]iĀ?k>18Ā+Ā^ EĀ»[[#29]]SĀŶĀĀĀ3Ā&B9ĀĀĀ+PĀ-Ā-+[[#22]]Ā+Ā \$ĀfĀfĀ+ĀŶ [[#4]]ĀŶ@Ā°qĀ°ĀĀĀ;BĀŶĀŶ2SjĀĒ}	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp:list in www.aka.idf.il/chamatz/klali/default.asp	None	1
176.13.19.17	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.111	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/imagevideogallerylobby/	Block	1
84.228.149.164	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
217.132.156.67	Israel	147.237.72.156	aman.idf.il	Illegal Byte Code Character in Header Value	Block	1
212.76.110.98	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1