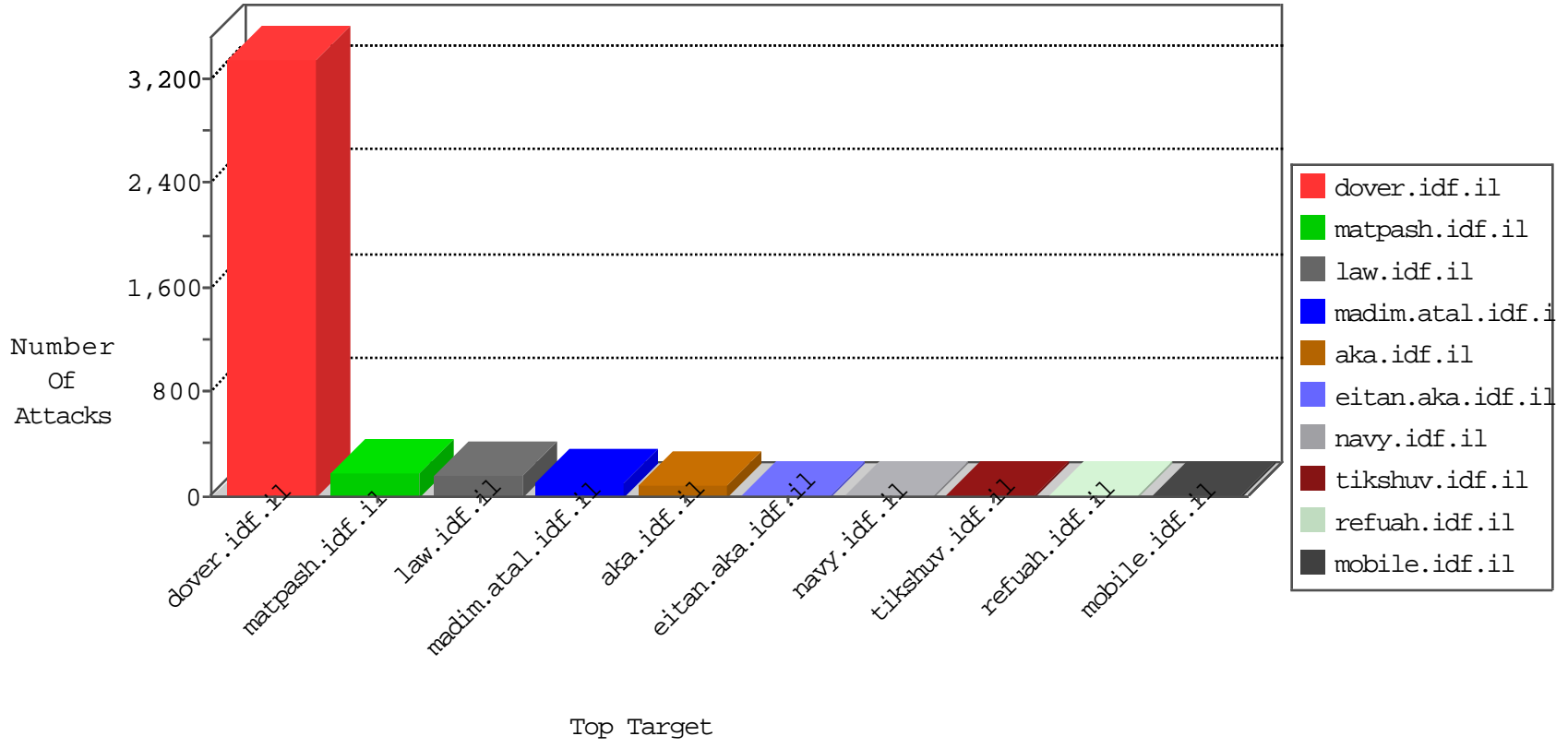


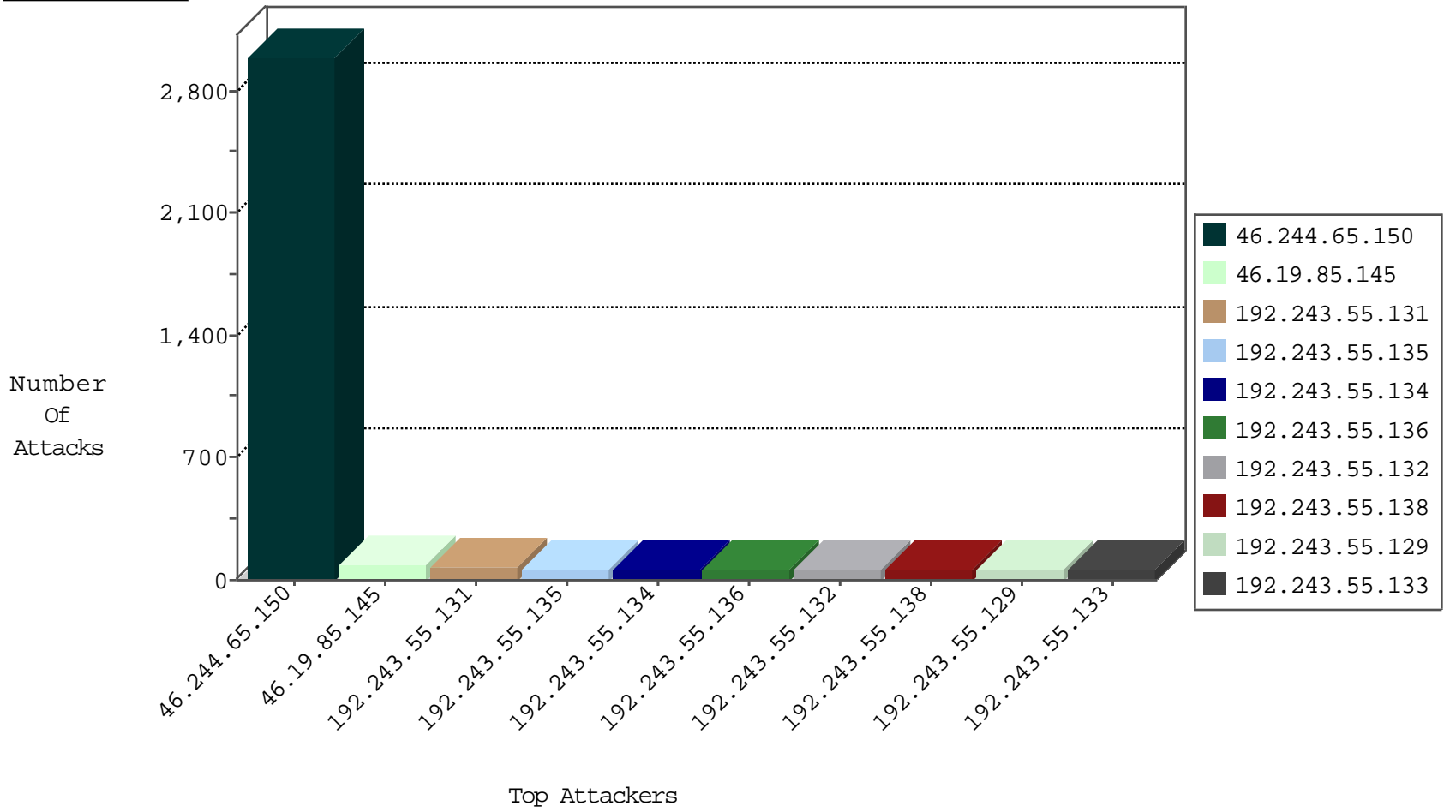
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.244.65.150	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2981
104.245.97.224		147.237.0.33	idf.il	Block_Ntp_All_Net	drop	1
202.58.137.76	Australia	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
104.245.97.224		147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
216.218.206.67	United States	147.237.8.28	e.mobile-ks.idf.il	Block_Udp_All_Nets	drop	1
50.30.37.59	United States	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	1
178.32.222.65	France	147.237.77.179	e.mazi.idf.il	Block_Ntp_All_Net	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.84	United States	147.237.77.234	halag.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
199.30.25.11	United States	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	2
174.136.194.36	United States	147.237.77.216	dover.idf.il	14459: HTTP: Known Skunkx DDOS Bot User-Agent Cyberdog	Block	1
223.73.45.240	China	147.237.77.216	dover.idf.il	C1000125: HTTP: Block admin login to gov.il sites ?q=user	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
207.46.13.96	United States	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
223.73.45.240	China	147.237.77.216	dover.idf.il	0872: HTTP: Apache .htaccess Access	Block	1
157.55.39.210	United States	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	1
223.73.45.240	China	147.237.77.216	dover.idf.il	C1000016: HTTP: administrator in URI	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
172.56.2.7	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
122.228.207.118	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
113.76.90.49	147.237.0.16	China	my-kosher-kravi.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
2.54.133.206	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
198.180.198.185	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 3072	1
187.3.32.186	147.237.76.31	Brazil	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
122.228.207.118	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.118	147.237.8.46	China	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
91.200.165.32	147.237.77.226	Russian Federation	www.chamatz.aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
210.48.146.154	147.237.77.170	Malaysia	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
203.3.24.23	147.237.77.216	Australia	dover.idf.il	portscan: TCP Distributed Portscan	1
193.105.134.220	147.237.0.16	Sweden	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
85.65.87.162	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
192.243.55.136	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
192.243.55.129	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.133	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.243.55.137	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.132	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.135	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.136	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.132	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.134	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.131	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.243.55.136	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.243.55.132	Dominica	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.137	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.135	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.132	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.131	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
203.3.24.23	Australia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.131	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence		monitor	4
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.130	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
192.243.55.132	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
192.243.55.138	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
192.243.55.131	Dominica	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
46.19.85.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	79
2.52.172.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	28
192.115.64.250	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 192.115.64.250	Block	17
199.30.25.68	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
176.13.12.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
65.54.247.156	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 65.54.247.156	Block	3
207.46.13.107	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
37.26.148.157	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	2
192.115.64.250	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	2
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.66.184	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/default.aspx	Block	1
66.249.64.190	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;docId in www.aka.idf.il/brothers/klali/default.asp	None	1
192.243.55.131	Dominica	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 192.243.55.131	Block	1
113.76.90.49	China	147.237.0.16	my-kosher-kravi.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.64.190	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;sideScroll in www.aka.idf.il/giyus/leshakot/	None	1
66.249.64.165	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/1056-ar/hamaz.aspx	Block	1
68.180.229.173	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/yohalan/main0926.html	Block	1
66.249.64.190	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;docId in www.aka.idf.il/giyus/leshakot/default.asp	None	1
46.19.86.58	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/iraq/english/media.asp	Block	1
134.191.232.70	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.190	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;sidescroll in www.aka.idf.il/giyus/kadatz/	None	1
66.249.64.190	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/general	Block	1
77.125.6.20	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/idkunpratimishiyim.aspx	Block	1
66.249.64.190	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;docId in www.aka.idf.il/tizmoret/klali/default.asp	None	1
192.243.55.133	Dominica	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/shared/usercontrols/lobbyinfocenteritem/	Block	1
46.19.86.121	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
134.191.232.71	Israel	147.237.76.30	himush.idf.il	Unknown Parameter amp;rnd in www.chimush.atal.idf.il/shared/ajax/createcaptchaimage.aspx	None	1
66.249.66.76	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.76	Block	1
223.73.45.240	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 223.73.45.240	Block	1
66.249.64.190	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;amp;list in www.aka.idf.il/chamatz/klali/default.asp	None	1
37.26.148.180	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 37.26.148.180 (Open Mode)	None	1
192.115.64.250	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
80.246.130.251	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.64.190	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;docid in www.aka.idf.il/giyus/syyarot/	None	1
192.243.55.135	Dominica	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 192.243.55.135	Block	1
134.191.232.71	Israel	147.237.76.30	himush.idf.il	Unknown Parameter amp;t in www.chimush.atal.idf.il/webresource.axd	None	1
66.249.66.105	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/templatecontrols/news/	Block	1
223.73.45.240	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
66.249.64.190	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;catId in www.aka.idf.il/giyus/general/default.asp	None	1
37.26.148.180	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
107.150.42.34	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.yun.ph/	Block	1
66.249.64.190	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;pageNum in www.aka.idf.il/iturim/asp/displayallsoldiers.asp	None	1
192.243.55.137	Dominica	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-he	Block	1
66.249.64.74	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakchal.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1