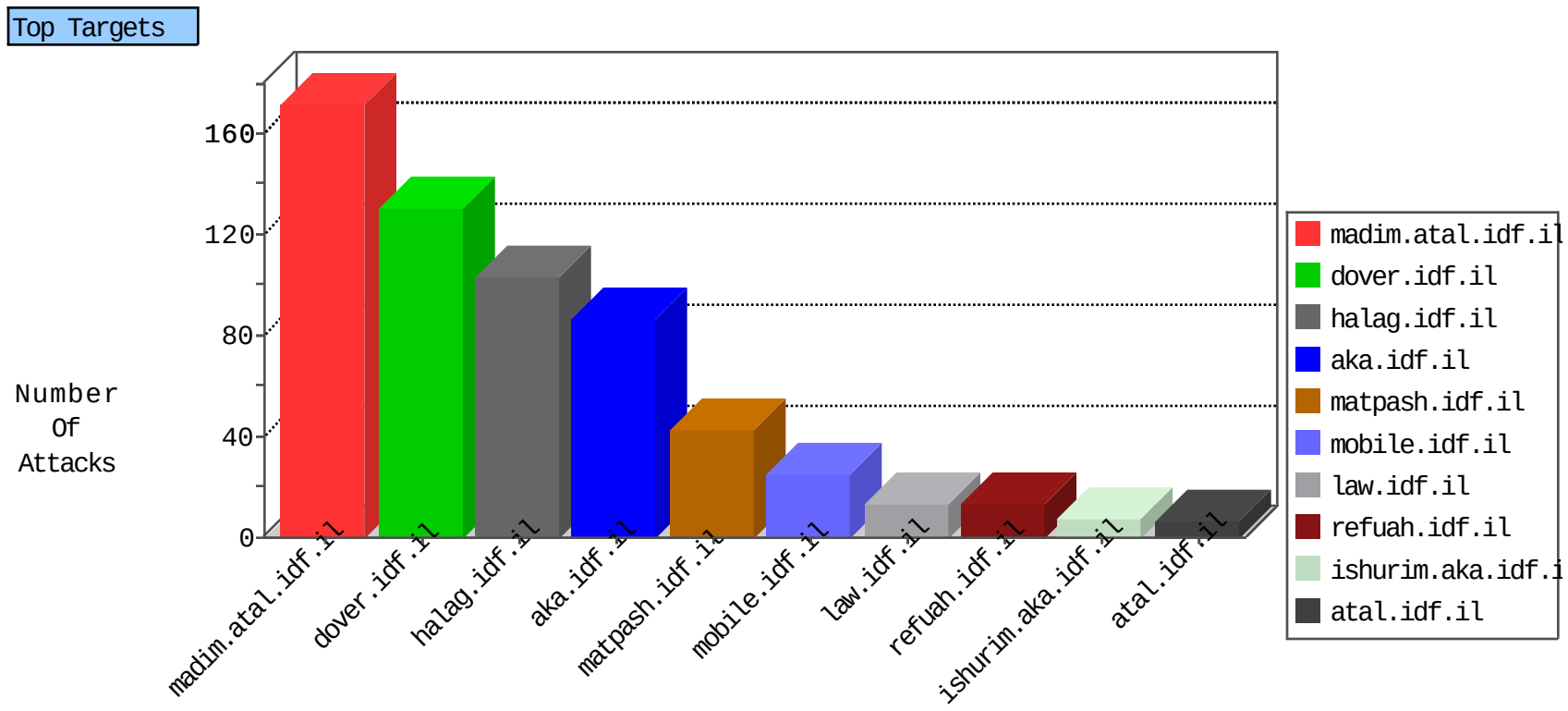
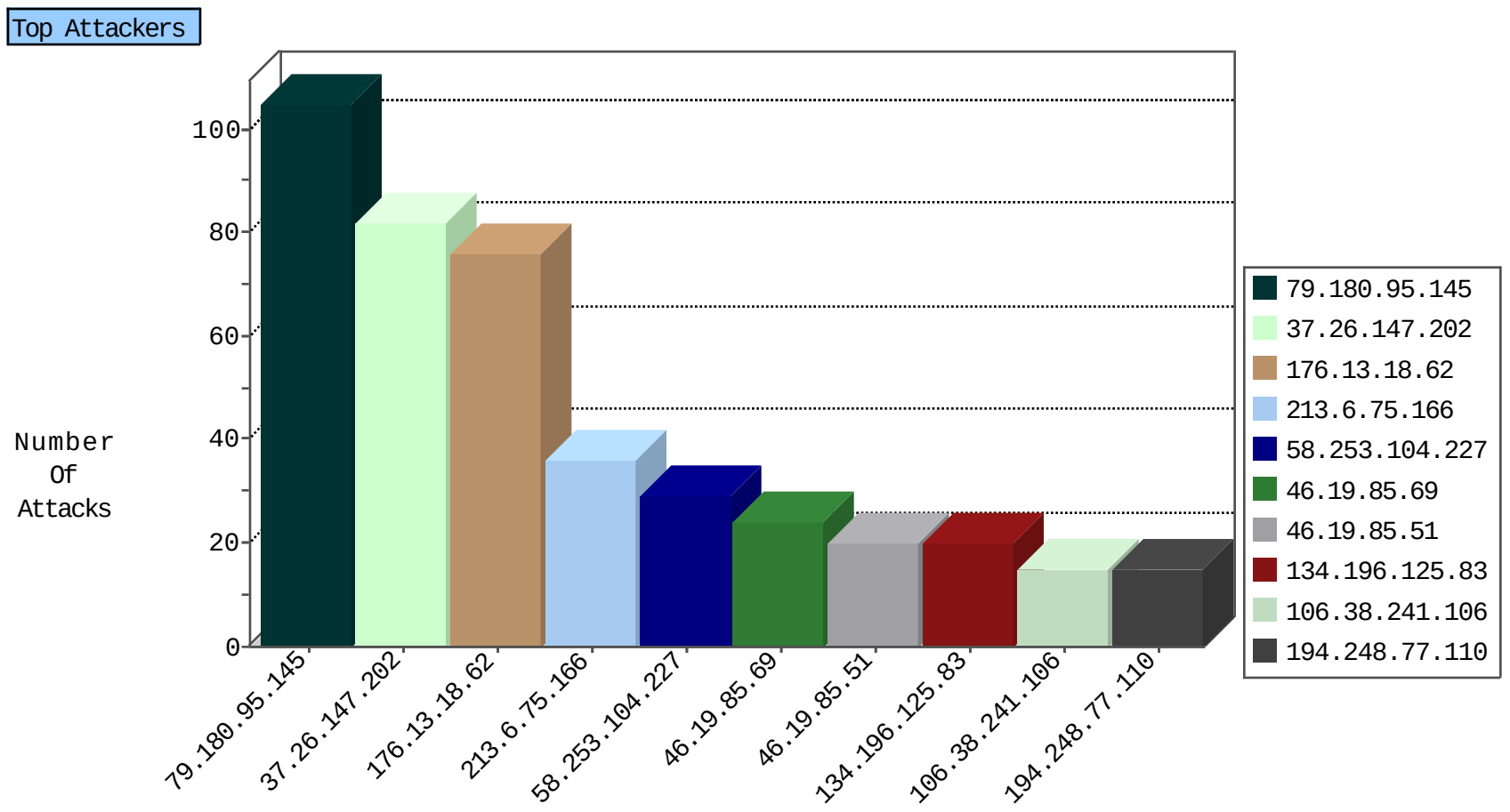
10-04-2016-11:04:04 to 10-04-2016-12:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-04-2016-11:04:04 to 10-04-2016-12:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
173.231.185.150	United States	147.237.76.199	e.nakchal.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
71.6.167.142	United States	147.237.76.44	e.refuah.idf.il	Black List	drop	1
183.60.48.25	China	147.237.76.196	e.sviva.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
71.6.216.40	United States	147.237.76.197	e.himush.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.30	himush.idf.il	Black List	drop	1
71.6.216.41	United States	147.237.76.86	navy.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.31	nakchal.idf.il	Black List	drop	1
71.6.158.166	United States	147.237.76.42	refuah.idf.il	Black List	drop	1

10-04-2016-11:04:04 to 10-04-2016-12:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	14

10-04-2016-11:04:04 to 10-04-2016-12:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
185.110.132.201	147.237.76.86	Ukraine	navy.idf.il	ET SCAN Potential SSH Scan	1
110.186.51.4	147.237.77.178	China	e.matpash.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.110.132.201	147.237.8.28	Ukraine	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
66.249.66.249	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sA (2)	1
185.110.132.201	147.237.0.35	Ukraine	akaws.idf.il	ET SCAN Potential SSH Scan	1
45.76.2.156	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
187.210.101.19	147.237.0.16	Mexico	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.129.15	147.237.8.46	United Kingdom	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
185.110.132.201	147.237.77.74	Ukraine	law.idf.il	ET SCAN Potential SSH Scan	1
128.199.124.88	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
185.110.132.201	147.237.76.196	Ukraine	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
128.199.76.253	147.237.76.30	Singapore	himush.idf.il	ET SCAN NMAP -sS window 1024	1
185.110.132.201	147.237.72.14	Ukraine	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
109.236.86.32	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
185.110.132.201	147.237.0.200	Ukraine	m4u.idf.il	ET SCAN Potential SSH Scan	1
54.242.146.163	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
14.36.6.8	147.237.0.19	Korea, Republic of	madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
183.60.48.25	147.237.0.35	China	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
163.172.169.150	147.237.0.200	United Kingdom	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
185.110.132.201	147.237.77.205	Ukraine	prisha.idf.il	ET SCAN Potential SSH Scan	1
128.199.176.113	147.237.76.202	Singapore	e.halag.idf.il	ET SCAN Potential SSH Scan	1
185.110.132.201	147.237.76.199	Ukraine	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
128.199.76.253	147.237.76.34	Singapore	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1

10-04-2016-11:04:04 to 10-04-2016-12:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.180.95.145	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	100
213.6.75.166	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	36
134.196.125.83	Thailand	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
46.19.85.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
194.248.77.110	Norway	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
46.19.85.51	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.19.85.51	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
80.246.136.147	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
141.226.162.39	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
2.53.14.66	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
79.180.76.151	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
79.180.95.145	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
157.55.39.49	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.120.122.219	Israel	147.237.77.74	law.idf.il	Command Injection	command injection detected in URL: 'label'	monitor	4
87.68.55.199	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
77.138.70.20	France	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
154.121.5.243	Algeria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
31.210.187.66	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
77.124.28.160	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.54.75	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.117.76.179	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	3
141.226.162.39	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
77.125.54.143	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
121.74.80.104	New Zealand	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
77.125.54.143	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
173.231.185.150	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
154.121.5.243	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
46.117.76.179	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
121.54.47.25	Philippines	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.85.44	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
5.22.134.251	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
147.235.8.86	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.44	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
176.13.4.32	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.117.76.179	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.117	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
58.253.104.227	China	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
147.235.8.86	Israel	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	2
176.13.244.73	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
31.210.186.52	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
187.61.110.201	Brazil	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
74.82.47.53	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
173.231.185.150	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
5.22.134.221	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.117.76.179	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
147.235.8.86	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
46.19.86.115	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
89.108.144.115	Lebanon	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.18.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	76
37.26.147.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	73
58.253.104.227	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 58.253.104.227	Block	17
79.180.183.24	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.180.183.24	Block	11
58.253.104.227	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	6
46.120.122.219	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/726-en/patzar.aspx200oktext/html34445 idf law review 3200:00.359utf-8	Block	4
2.53.137.106	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
31.154.81.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
62.117.59.18	Egypt	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/homepage.aspx	Block	2
176.13.13.21	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.181.9.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
136.243.16.208	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
66.249.69.72	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8919-he/refuah.aspx	Block	1
94.142.238.190	Czech Republic	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/general.aspx	Block	1
77.138.175.13	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/9/71729.pdf	Block	1
2.53.137.106	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
79.180.183.24	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/kiosk/kiosk.aspx	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/8/71768.pdf	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
77.138.231.208	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/cityofficers/	Block	1
66.249.64.43	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/8/71748.pdf	Block	1
68.180.228.174	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
117.213.194.115	India	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/sip_storage/files/2/2792.ppt	Block	1
79.178.26.30	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/faq.aspx	Block	1
66.249.66.180	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation aspxerrorpath in www.idf.il/error.htm	Block	1
176.13.244.73	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
89.139.117.216	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
77.138.70.20	France	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/sip_storage/files/3/1773.jpg	Block	1
58.253.104.227	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.asp	Block	1
130.193.50.33	Russian Federation	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/487-	Block	1
2.53.16.14	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
79.180.95.145	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.66.202	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20581-he/dover.aspx	Block	1
217.132.110.81	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$cb15224782 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
46.19.86.115	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
91.240.78.14	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/chamatz	Block	1
77.138.104.63	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1

10-04-2016-11:04:04 to 10-04-2016-12:04:04