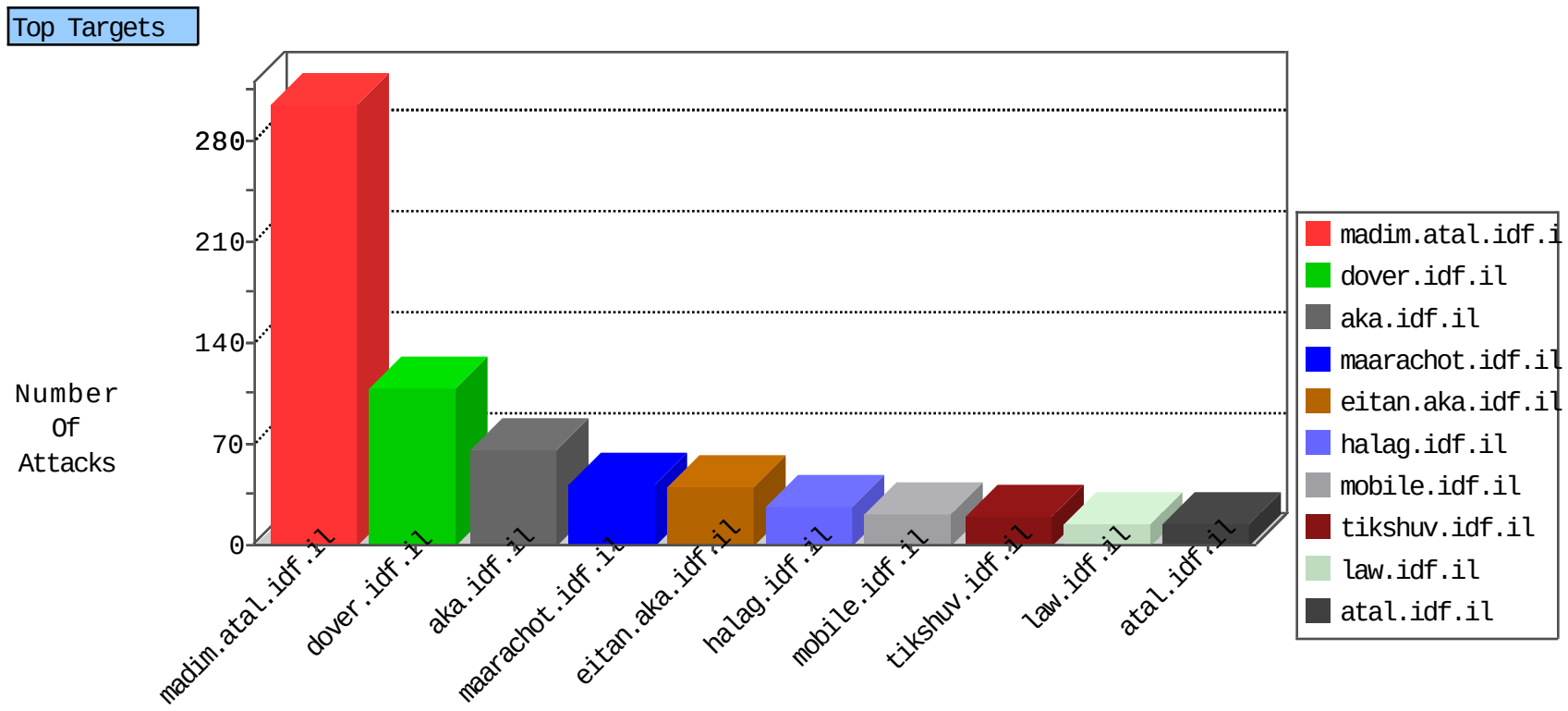
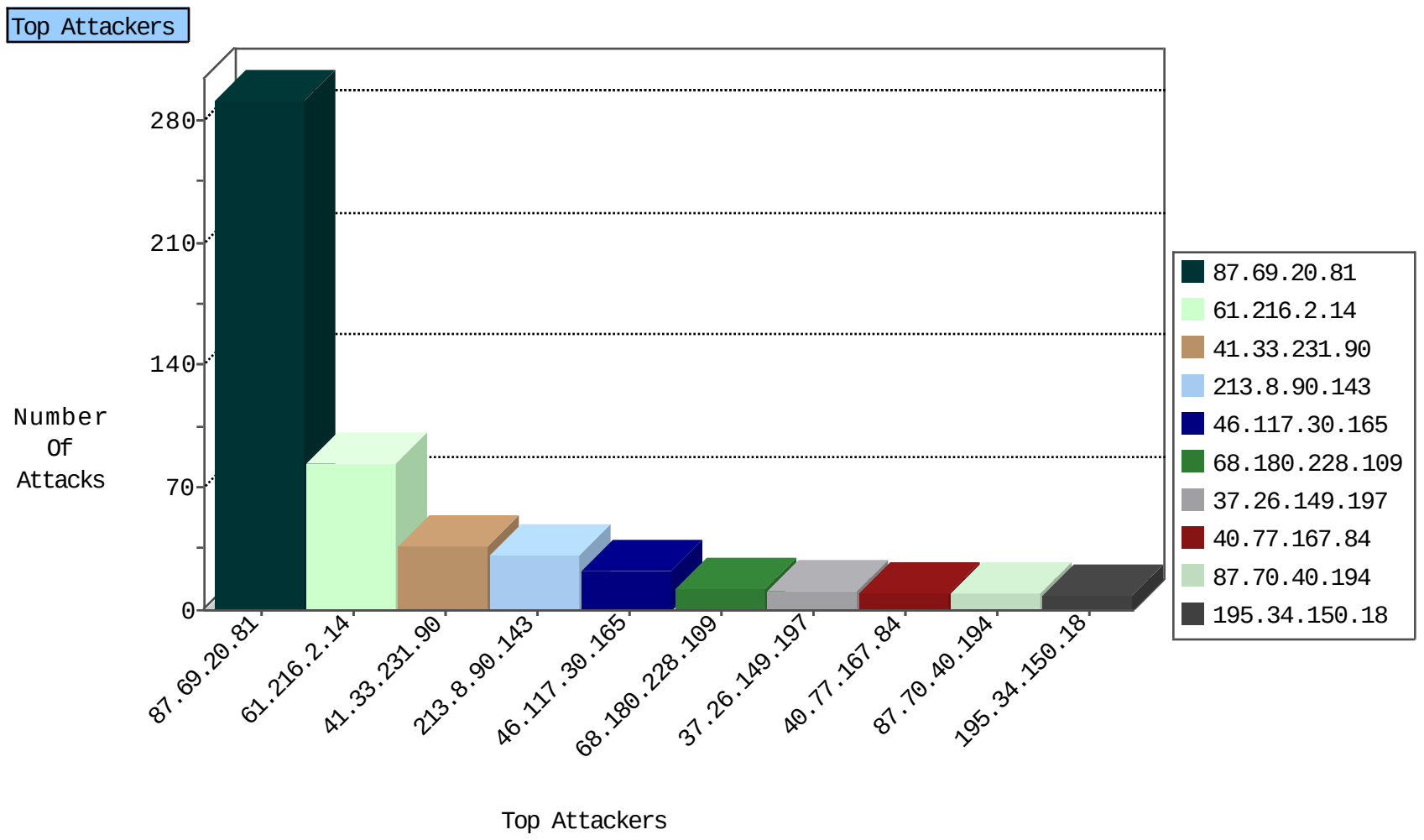
02-26-2016-07:04:04 to 02-26-2016-08:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-26-2016-07:04:04 to 02-26-2016-08:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
198.23.190.39	United States	147.237.77.179	e.mazi.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.116	United States	147.237.77.205	prisha.idf.il	Block_Ntp_All_Net	drop	1
208.100.26.228	United States	147.237.77.227	e.hamaz.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.120	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
198.23.165.141	United States	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1

02-26-2016-07:04:04 to 02-26-2016-08:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.65.136.140	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
51.255.65.4	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
51.255.65.5	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
157.55.39.92	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
51.255.65.46	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
207.46.13.145	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
51.255.65.80	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

02-26-2016-07:04:04 to 02-26-2016-08:04:04

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	4
185.95.255.42	147.237.76.30		himush.idf.il	ET SCAN NMAP -sA (2)	4
198.54.90.200	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	2
185.95.255.42	147.237.76.86		navy.idf.il	ET SCAN NMAP -sA (2)	2
79.138.70.153	147.237.0.19	Sweden	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.179	147.237.72.156		aman.idf.il	ET SCAN Potential SSH Scan	1
62.169.239.185	147.237.76.30	Greece	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.130.5.179	147.237.0.34		tikshuv.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
159.203.250.214	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 1024	1
114.249.143.244	147.237.76.30	China	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.215.89.20	147.237.72.156	United States	aman.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.42.206	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.144	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
79.138.70.153	147.237.0.33	Sweden	idf.il	ET SCAN Potential SSH Scan	1
185.130.5.179	147.237.77.61		e.cogat.idf.il	ET SCAN Potential SSH Scan	1
79.138.70.153	147.237.0.16	Sweden	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.179	147.237.72.14		dover.idf.il(old)	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
180.150.177.188	147.237.8.45	China	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
40.113.118.99	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 4096	1
146.185.250.2	147.237.72.156	Russian Federation	aman.idf.il	ET SCAN Potential SSH Scan	1
104.215.89.20	147.237.72.156	United States	aman.idf.il	ET SCAN NMAP -sS window 4096	1
93.174.93.144	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.8.46	China	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
82.117.208.243	147.237.77.178		e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1

02-26-2016-07:04:04 to 02-26-2016-08:04:04

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	36
213.8.90.143	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid sequence number	monitor	31
46.117.30.165	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
68.180.228.109	United States	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	12
40.77.167.84	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
87.70.40.194	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
40.77.167.10	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.121.61.19	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
79.177.204.91	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
40.77.167.90	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
172.56.26.95	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
109.253.129.245	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
61.216.2.14	Taiwan	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	6
95.35.175.172	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
204.12.251.37	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
40.77.167.83	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
79.176.167.132	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
61.216.2.14	Taiwan	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
108.46.225.81	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
61.216.2.14	Taiwan	147.237.76.86	navy.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
37.26.149.197	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.16	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.46.41.145	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
61.216.2.14	Taiwan	147.237.76.39	mobile.meitav.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
37.26.148.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.192.136	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
61.216.2.14	Taiwan	147.237.77.176	matpash.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
61.216.2.14	Taiwan	147.237.77.226	www.chamatz.aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
178.255.215.87	France	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
61.216.2.14	Taiwan	147.237.77.170	maarachot.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
61.216.2.14	Taiwan	147.237.77.233	atal.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
217.69.133.227	Russian Federation	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
82.81.78.139	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
61.216.2.14	Taiwan	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
217.69.133.228	Russian Federation	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
136.243.67.234	Germany	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
61.216.2.14	Taiwan	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
61.216.2.14	Taiwan	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.102.242.91	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
61.216.2.14	Taiwan	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
82.81.78.139	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
61.216.2.14	Taiwan	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.120.198.128	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
61.216.2.14	Taiwan	147.237.76.200	eitan.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
172.56.26.95	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2

02-26-2016-07:04:04 to 02-26-2016-08:04:04

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
61.216.2.14	Taiwan	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
37.26.149.197	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		alert	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.69.20.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	292
66.249.83.155	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
66.249.83.161	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
79.183.199.21	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
176.13.15.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
80.12.42.36	France	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.117.161.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.8.204.53	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1641	Block	2
78.108.161.226	Lebanon	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
66.249.78.242	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/3/2153.doc	Block	1
203.133.170.143	Korea, Republic of	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
61.216.2.14	Taiwan	147.237.77.170	maarachot.idf.il	Multiple Illegal Byte Code Character in Method from 61.216.2.14	Block	1
46.161.40.120	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation l in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
5.39.222.159	Netherlands	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/rom-0	Block	1
74.82.47.3	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
66.249.64.48	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/6/105796.pdf	Block	1
61.216.2.14	Taiwan	147.237.76.86	navy.idf.il	Multiple Illegal Byte Code Character in Method from 61.216.2.14	Block	1
175.156.130.240	Singapore	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.78.248	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/2154.doc	Block	1
61.216.2.14	Taiwan	147.237.77.176	matpash.idf.il	Multiple Illegal Byte Code Character in Method from 61.216.2.14	Block	1
148.251.13.51	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
54.244.22.103	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.26.146.243	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
77.127.183.83	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
66.249.69.26	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	1
61.216.2.14	Taiwan	147.237.76.86	navy.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
80.246.130.218	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$captchaText in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
46.161.40.120	Russian Federation	147.237.77.74	law.idf.il	Parameter Type Violation FileName in www.law.idf.il/templates/getfile/getfile.aspx	Block	1
61.216.2.14	Taiwan	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
157.55.2.179	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
61.216.2.14	Taiwan	147.237.0.19	madim.atal.idf.il	Multiple Untraceable SSL Sessions from 61.216.2.14 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
37.26.148.155	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/home/giyus	Block	1
66.249.78.65	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/5/110865.pdf	Block	1
61.216.2.14	Taiwan	147.237.76.147	chinuch.aka.idf.il	Multiple Illegal Byte Code Character in Method from 61.216.2.14	Block	1
176.109.248.123	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/894-he/chinuch.aspx	Block	1
84.94.114.184	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
46.161.40.120	Russian Federation	147.237.77.74	law.idf.il	Parameter Type Violation InfoCenterItem in www.law.idf.il/templates/getfile/getfile.aspx	Block	1
66.249.83.158	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
61.216.2.14	Taiwan	147.237.77.226	www.chamatz.aka.idf.il	Multiple Illegal Byte Code Character in Method from 61.216.2.14	Block	1
61.216.2.14	Taiwan	147.237.0.34	tikshuv.idf.il	Multiple Untraceable SSL Sessions from 61.216.2.14 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
157.55.39.105	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.117.30.165	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
79.177.204.91	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.78.236	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
61.216.2.14	Taiwan	147.237.76.200	eitan.aka.idf.il	Illegal Byte Code Character in Method	Block	1
184.105.247.195	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
85.250.82.155	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
46.161.40.120	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation f in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
2.52.173.71	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
61.216.2.14	Taiwan	147.237.77.233	atal.idf.il	Illegal Byte Code Character in Method	Block	1