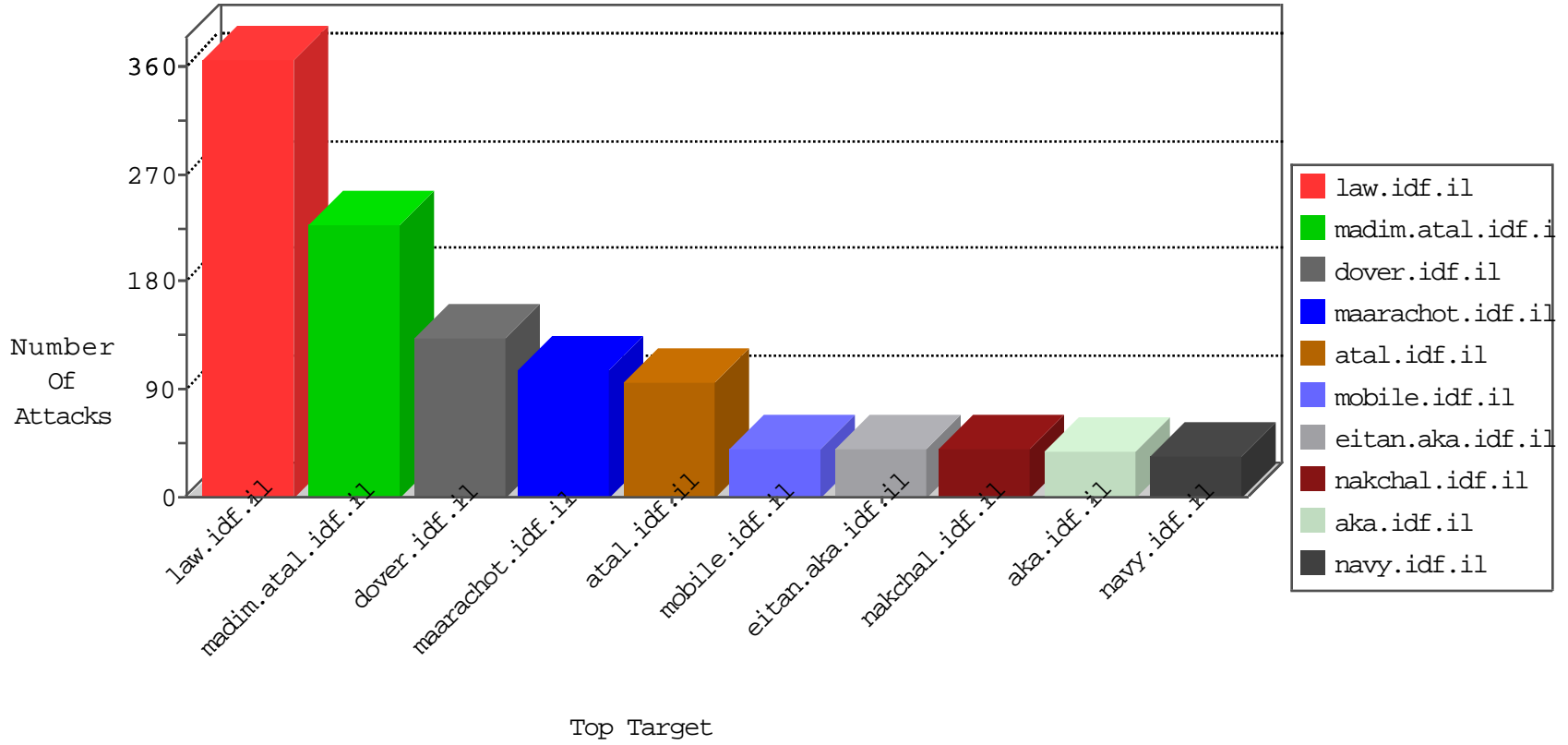


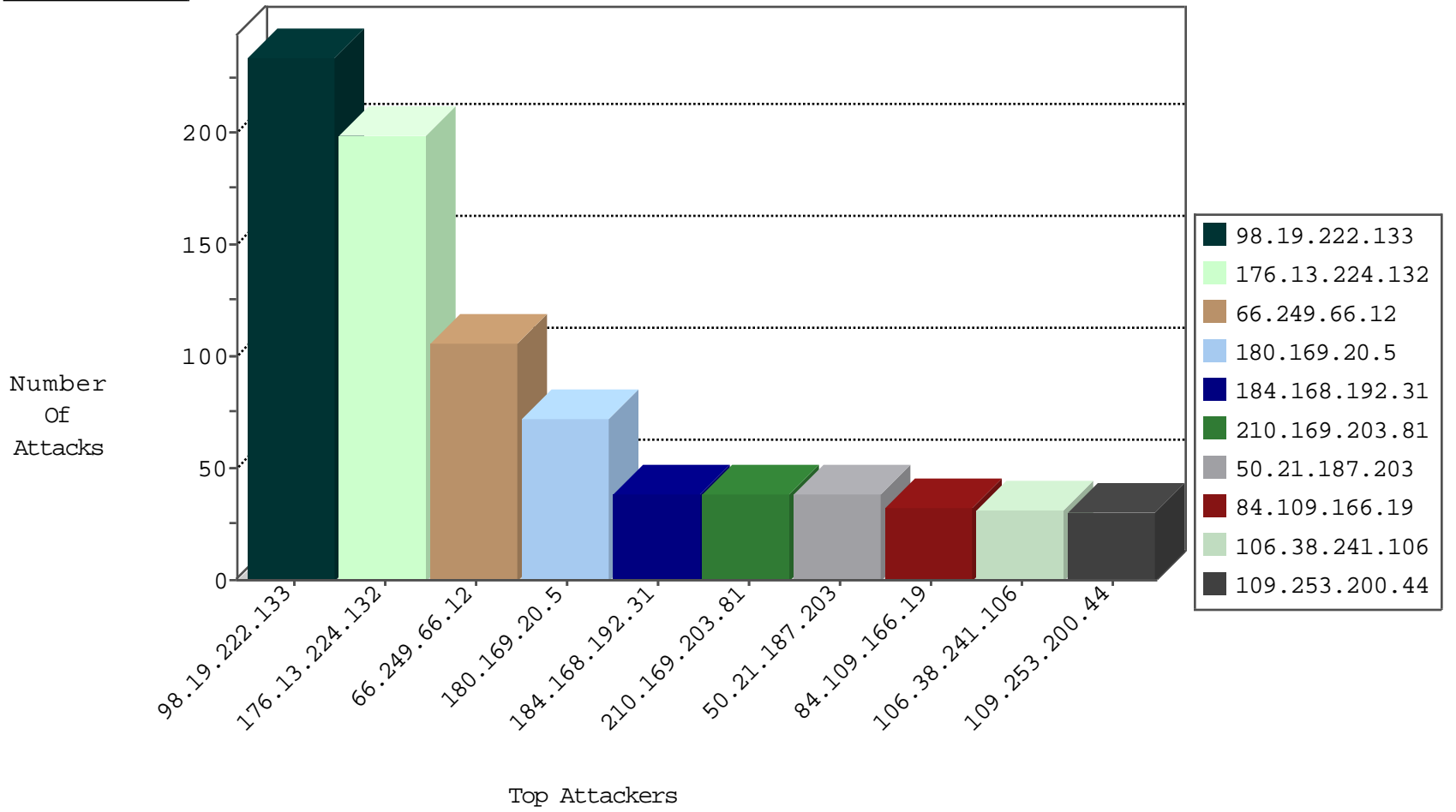
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
134.147.203.115	Germany	147.237.76.177	ncore.idf.il	Black List	drop	2
71.6.135.131	United States	147.237.76.176	test.ncore.idf.il	Black List	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
98.19.222.133	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	36
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	29
98.19.222.133	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	18
184.168.192.31	United States	147.237.76.31	nakchal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
210.169.203.81	Japan	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
50.21.187.203	United States	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
180.169.20.5	China	147.237.77.216	dover.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
98.19.222.133	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	9
66.135.63.82	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
184.168.192.31	United States	147.237.76.31	nakchal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
210.169.203.81	Japan	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
74.208.154.12	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
50.21.187.203	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
180.169.20.5	China	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
74.208.218.66	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
195.8.208.118	Netherlands	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
216.58.230.159	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
84.245.33.104	Netherlands	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
66.29.211.141	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
217.37.125.121	United Kingdom	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
184.168.152.45	United States	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
89.44.144.244	Romania	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	5
121.40.25.174	China	147.237.0.34	tikshuv.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	5
199.58.86.206	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
199.58.86.206	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
27.159.237.68	China	147.237.77.216	dover.idf.il	22611: HTTP: WordPress LoginWall Fake Plugin Usage	Block	1
151.80.31.108	France	147.237.72.156	aman.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
98.19.222.133	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	144
66.249.66.12	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	106
180.169.20.5	147.237.77.216	China	dover.idf.il	SQL Injection - Select From	54
98.19.222.133	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	24
184.168.192.31	147.237.76.31	United States	nakchal.idf.il	SQL Injection - Select From	20
50.21.187.203	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	20
210.169.203.81	147.237.77.74	Japan	law.idf.il	SQL Injection - Select From	20
66.29.211.141	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	18
74.208.218.66	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	18
195.8.208.118	147.237.77.74	Netherlands	law.idf.il	SQL Injection - Select From	14
216.58.230.159	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
74.208.154.12	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
84.245.33.104	147.237.77.74	Netherlands	law.idf.il	SQL Injection - Select From	8
217.37.125.121	147.237.72.166	United Kingdom	aka.idf.il	SQL Injection - Select From	8
184.168.152.45	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	8
66.135.63.82	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
89.44.144.244	147.237.77.233	Romania	atal.idf.il	SQL Injection - Select From	8
121.40.25.174	147.237.0.34	China	tikshuv.idf.il	SQL Injection - Select From	7
77.252.26.51	147.237.72.166	Poland	aka.idf.il	ET SCAN NMAP -f -sS	1
210.121.115.200	147.237.0.17	Korea, Republic of	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
106.38.241.106	147.237.72.166	China	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
46.161.40.17	147.237.76.200	Russian Federation	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
77.252.26.51	147.237.72.166	Poland	aka.idf.il	ET SCAN NMAP -sS window 2048	1
66.249.69.224	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	1
139.162.187.89	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
60.246.192.153	147.237.77.178	Macau	e.matpash.idf.il	ET SCAN NMAP -sS window 4096	1
115.211.39.196	147.237.76.44	China	e.refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.183.223.228	147.237.76.38	Latvia	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
46.161.40.17	147.237.76.196	Russian Federation	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
77.252.26.51	147.237.72.166	Poland	aka.idf.il	ET SCAN NMAP -sS window 3072	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
84.109.166.19	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	32
109.253.200.44	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
178.20.235.164	Russian Federation	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	24
158.85.253.245	United States	147.237.76.86	navy.idf.il	drop	SAM rule	drop	18
5.22.134.207	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
81.88.48.113	Italy	147.237.77.233	atal.idf.il	drop	SAM rule	drop	6
176.13.235.108	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
158.85.253.245	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.2	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
185.110.108.165	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.165	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
96.224.230.17	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
98.19.222.133	United States	147.237.77.233	atal.idf.il	drop	SAM rule	drop	3
66.249.64.89	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.2	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
2.53.140.74	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
172.217.29.51	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
101.184.159.194	Australia	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
74.125.206.121	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	2
172.217.17.83	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	2
2.55.160.91	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
216.58.212.179	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
74.125.206.121	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
172.217.17.83	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
110.66.127.82	Japan	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
103.21.166.9	Sri Lanka	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
79.183.8.135	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.86.26	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
172.217.17.51	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
139.162.37.147	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
216.58.212.147	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
74.82.47.49	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.96	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
172.217.17.51	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
109.253.139.157	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1
216.58.211.83	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	1
37.26.147.231	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
139.162.37.147	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
216.58.212.179	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
185.3.147.75	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
216.58.211.83	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
72.229.180.147	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
176.13.224.132	Israel	147.237.0.19	madim.atal.idf.il	drop	First packet isn't SYN	drop	1
46.19.85.139	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
101.184.159.194	Australia	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
46.19.86.3	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
2.55.170.158	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
91.185.190.172	Poland	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
216.58.212.147	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.224.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	198
109.253.220.0	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
24.73.225.146	United States	147.237.76.86	navy.idf.il	Unauthorized HTTP Method	Block	9
24.73.225.146	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/8/	Block	2
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.224	Block	2
46.19.86.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
103.21.166.9	Sri Lanka	147.237.77.216	dover.idf.il	Parameter Type Violation ct100\$ContentPlaceholder1\$txtEmail in www.idf.il/1038-en/dover.aspx	Block	2
2.55.167.55	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 2.55.167.55	Block	2
2.55.167.55	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
68.180.230.216	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakchal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.66.117	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Byte Code Character in Parameter Name Gb&T907@)DKd&f^z^H!lkR[[#28]]{	Block	1
100.13.130.4	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/index.php	Block	1
66.249.75.12	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/3369.jpg	Block	1
66.249.65.156	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1412-he/atal.aspx	Block	1
192.115.248.2	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
2.55.167.55	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/promotioncube/	Block	1
66.249.76.61	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/.well-known/apple-app-site-association	Block	1
66.249.65.160	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
84.229.94.102	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-ar/www.idf.il/ar	Block	1
66.102.9.5	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	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
66.249.76.62	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/apple-app-site-association	Block	1
66.249.66.113	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rmd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
5.22.134.207	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/apple-touch-icon-precomposed.png	Block	1
98.139.14.249	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized Method HEAD for www.eitan.aka.idf.il/1103-8363-he/eitan.aspx	None	1
66.249.69.232	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atall/izkor/view_img.asp	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/.well-known/assetlinks.json	Block	1
66.249.76.81	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
66.249.66.117	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	1
100.13.130.4	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/index.php	Block	1
66.249.75.4	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/3272.jpg	Block	1
66.249.64.158	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/robots.txt	Block	1