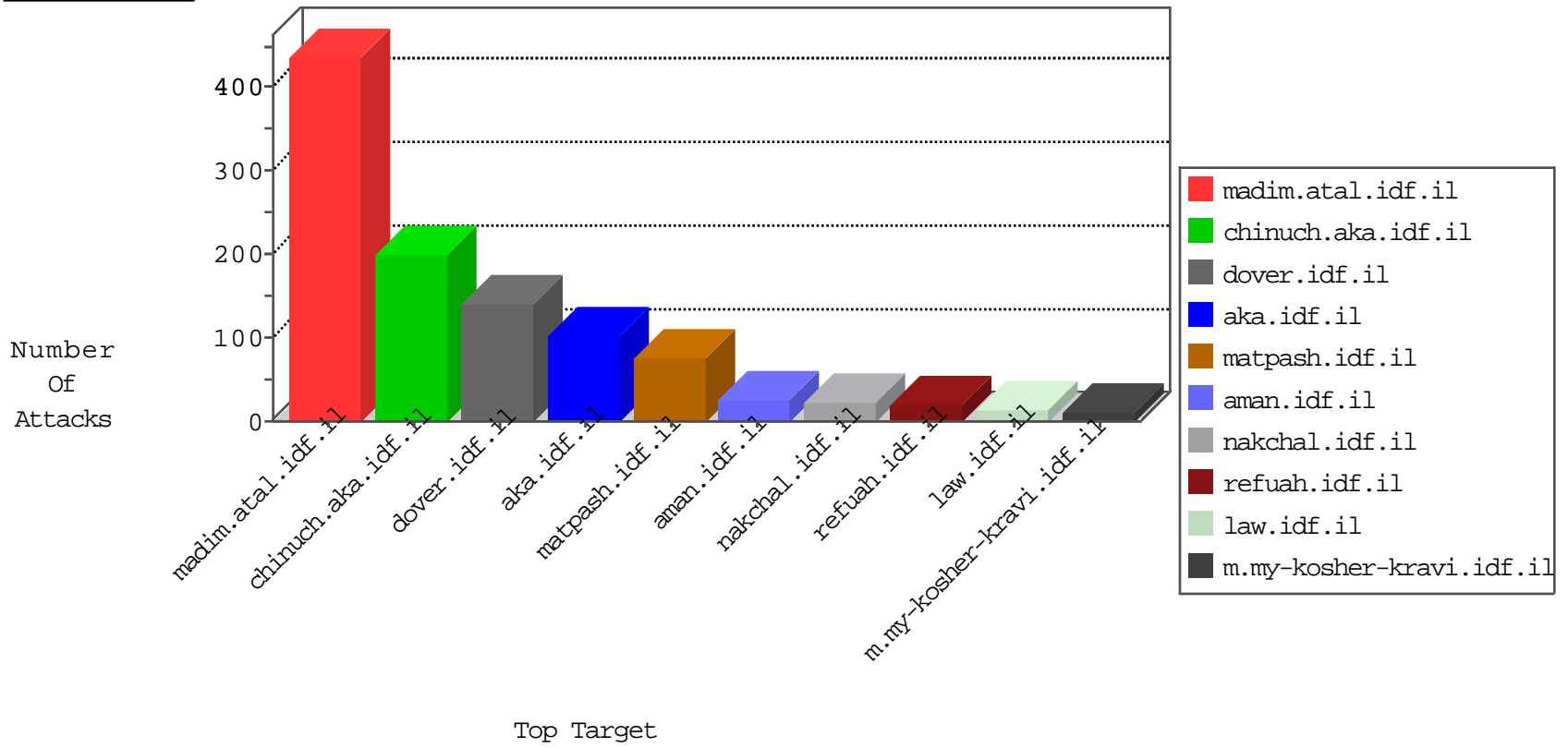


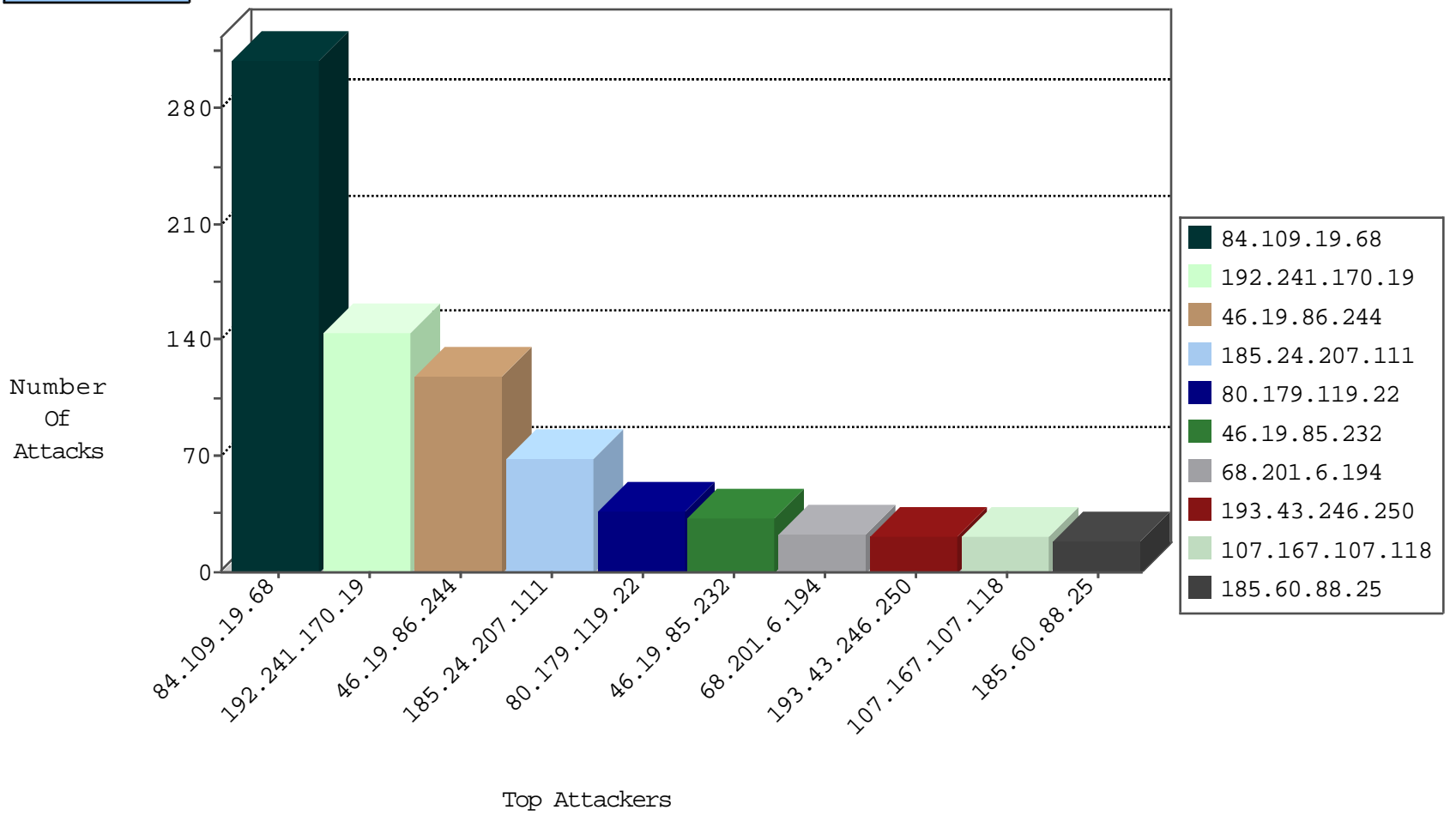
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
42.112.10.75	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1
45.32.193.80	Netherlands	147.237.76.42	refuah.idf.il	Black List	drop	1
42.112.10.70	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1
42.112.10.81	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1
104.238.146.105	United States	147.237.76.42	refuah.idf.il	Black List	drop	1
42.112.10.73	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1
42.112.10.85	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1
42.112.10.66	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1
42.112.10.74	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1
42.112.10.89	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1
42.112.10.69	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.4.123.172	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3
5.9.89.170	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
185.60.88.25	147.237.77.233		atal.idf.il	ET SCAN Potential SSH Scan	2
185.60.88.25	147.237.76.177		ncore.idf.il	ET SCAN Potential SSH Scan	2
185.60.88.25	147.237.76.86		navy.idf.il	ET SCAN Potential SSH Scan	2
185.60.88.25	147.237.76.196		e.sviva.idf.il	ET SCAN Potential SSH Scan	1
220.135.180.51	147.237.77.226	Taiwan	www.chamatz.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.60.88.25	147.237.76.148		ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
204.13.65.204	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
185.60.88.25	147.237.76.39		mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
204.13.65.204	147.237.0.34	United States	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
185.60.88.25	147.237.76.30		himush.idf.il	ET SCAN Potential SSH Scan	1
204.13.65.204	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
185.60.88.25	147.237.72.167		ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
198.199.89.155	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
163.172.238.45	147.237.77.234	United Kingdom	halag.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.129.15	147.237.72.156	United Kingdom	anan.idf.il	ET SCAN NMAP -sS window 1024	1
185.60.88.25	147.237.77.216		dover.idf.il	ET SCAN Potential SSH Scan	1
79.177.14.166	147.237.77.216	Israel	dover.idf.il	ET SCAN NMAP -sA (2)	1
185.60.88.25	147.237.76.199		e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
204.13.65.204	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
204.13.65.204	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
185.60.88.25	147.237.76.34		yohalan.idf.il	ET SCAN Potential SSH Scan	1
204.13.65.204	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
185.60.88.25	147.237.72.217		e.idf.il	ET SCAN Potential SSH Scan	1
201.38.68.132	147.237.77.234	Brazil	halag.idf.il	ET SCAN NMAP -sS window 1024	1
185.60.88.25	147.237.72.166		aka.idf.il	ET SCAN Potential SSH Scan	1
185.60.88.25	147.237.77.235		sviva.idf.il	ET SCAN Potential SSH Scan	1
163.172.169.150	147.237.77.61	United Kingdom	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
185.60.88.25	147.237.77.227		e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
123.206.194.17	147.237.76.202	China	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
185.60.88.25	147.237.77.74		law.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
192.241.170.19	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	142
185.24.207.111	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	24
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
107.167.107.118	India	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	22
185.24.207.111	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	20
109.253.147.175	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	17
185.24.207.111	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
80.179.119.22	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
80.179.119.22	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
46.19.85.232	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.19.85.232	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
185.24.207.111	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	10
176.228.158.118	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
176.228.158.118	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
91.225.132.102	Poland	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
84.111.63.58	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.85.232	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.232	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
87.70.39.231	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.85.250	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
68.201.6.194	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	5
79.179.14.172	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
185.24.207.110	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.250	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.121	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
68.201.6.194	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	5
68.201.6.194	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.121	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	5
80.179.119.22	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	5
46.19.85.250	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
85.64.228.85	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
68.201.6.194	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.19.86.59	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.121	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
80.179.119.22	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
68.201.6.194	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
192.241.170.19	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
195.90.103.48	Poland	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
195.90.103.48	Poland	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
100.92.184.126		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
195.90.103.48	Poland	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
202.83.122.30	Indonesia	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.26.149.200	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.96.191	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.167.98	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
157.55.39.25	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
195.90.103.48	Poland	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.86.59	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
202.83.122.30	Indonesia	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.109.19.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	310
46.19.86.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	118
46.19.86.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.224	Block	3
66.249.64.112	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.64.112	Block	2
2.53.161.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.138.177.181	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/pniotanswer.aspx	Block	2
213.57.43.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
40.77.167.90	United States	147.237.72.166	aka.idf.il	Abnormally Long Request URL	Block	1
180.76.15.145	China	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/templates/shared/usercontrols/headerupper/	Block	1
79.178.211.140	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
66.249.75.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-8583-he/dover.aspx	Block	1
213.197.164.46	Lithuania	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 213.197.164.46	Block	1
109.253.201.217	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.76.80	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
66.249.69.228	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to ww.idf.il/atal1/izkor/view_text.asp	Block	1
185.32.179.195	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.179.14.172	Israel	147.237.72.166	aka.idf.il	Unknown Parameter in www.aka.idf.il/main/giyus/general.aspx	None	1
66.249.75.46	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/general/general.aspx	Block	1
213.197.164.46	Lithuania	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1
66.249.64.112	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/m/	Block	1
113.103.86.243	China	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
66.249.69.229	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1
204.79.180.201	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/miluum/templates/inner.asp	Block	1
84.108.70.15	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.75.172	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/templates/homepage/homepage.aspx	Block	1
113.103.86.243	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/wp-login.php	Block	1
66.249.69.232	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_bottom.asp	Block	1
46.117.28.61	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https://www.aman.idf.il/	Block	1
66.249.76.71	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/robots.txt	Block	1
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
37.26.148.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ctl00\$c in www.aka.idf.il/main/giyus/userdetails/updateuserdetails.aspx	None	1
176.9.29.147	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
77.139.47.167	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/miyun/miyunlobby.aspx	Block	1
66.249.75.4	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8870-he/refuah.aspx	Block	1
213.197.164.46	Lithuania	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012ources/images/innerpage/goback.gif	Block	1
66.249.64.108	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/israeliinkalkilia04012011.aspx	Block	1
85.64.24.221	Israel	147.237.72.166	aka.idf.il	Unknown Parameter asm in www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	None	1
66.249.76.76	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
66.249.69.228	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.228	Block	1