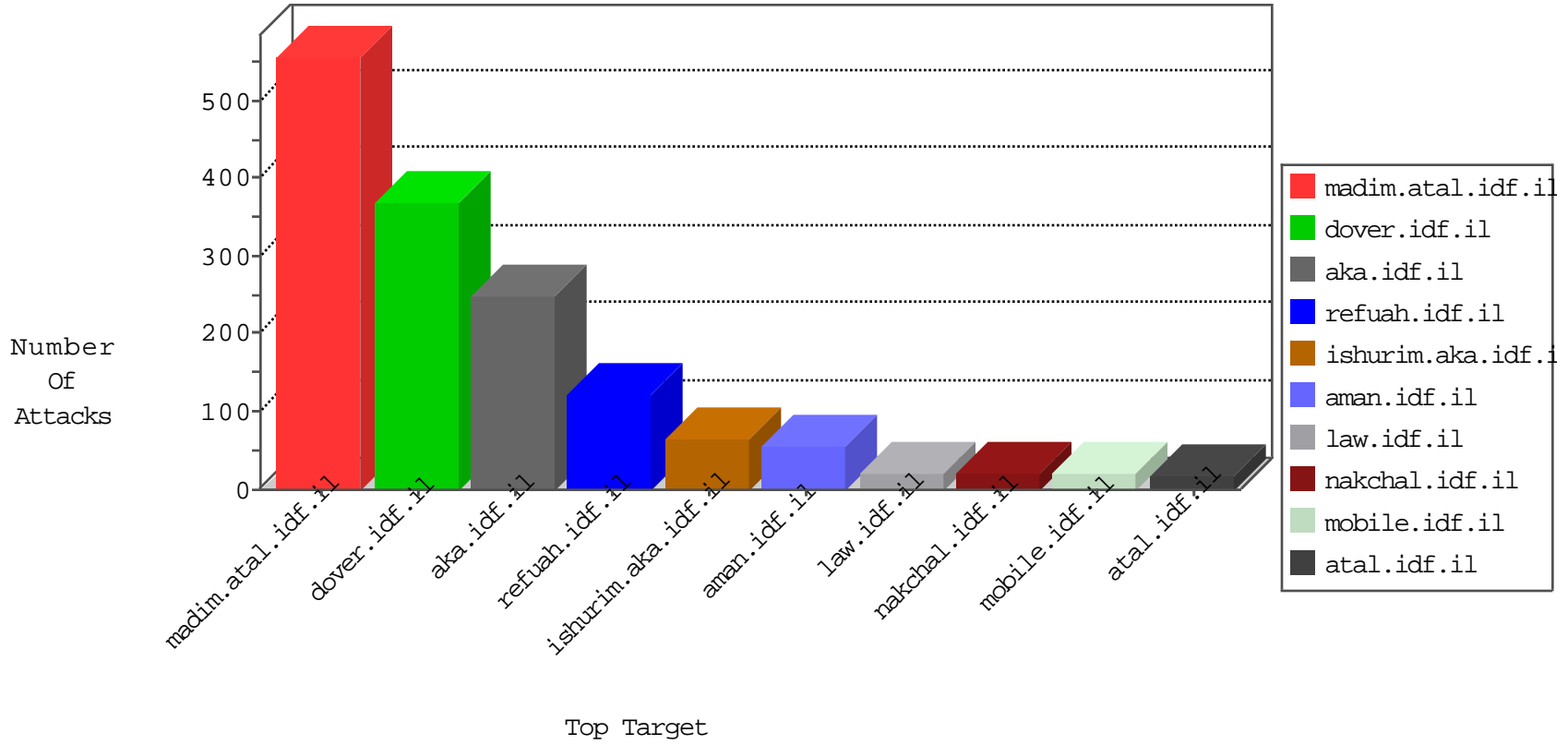


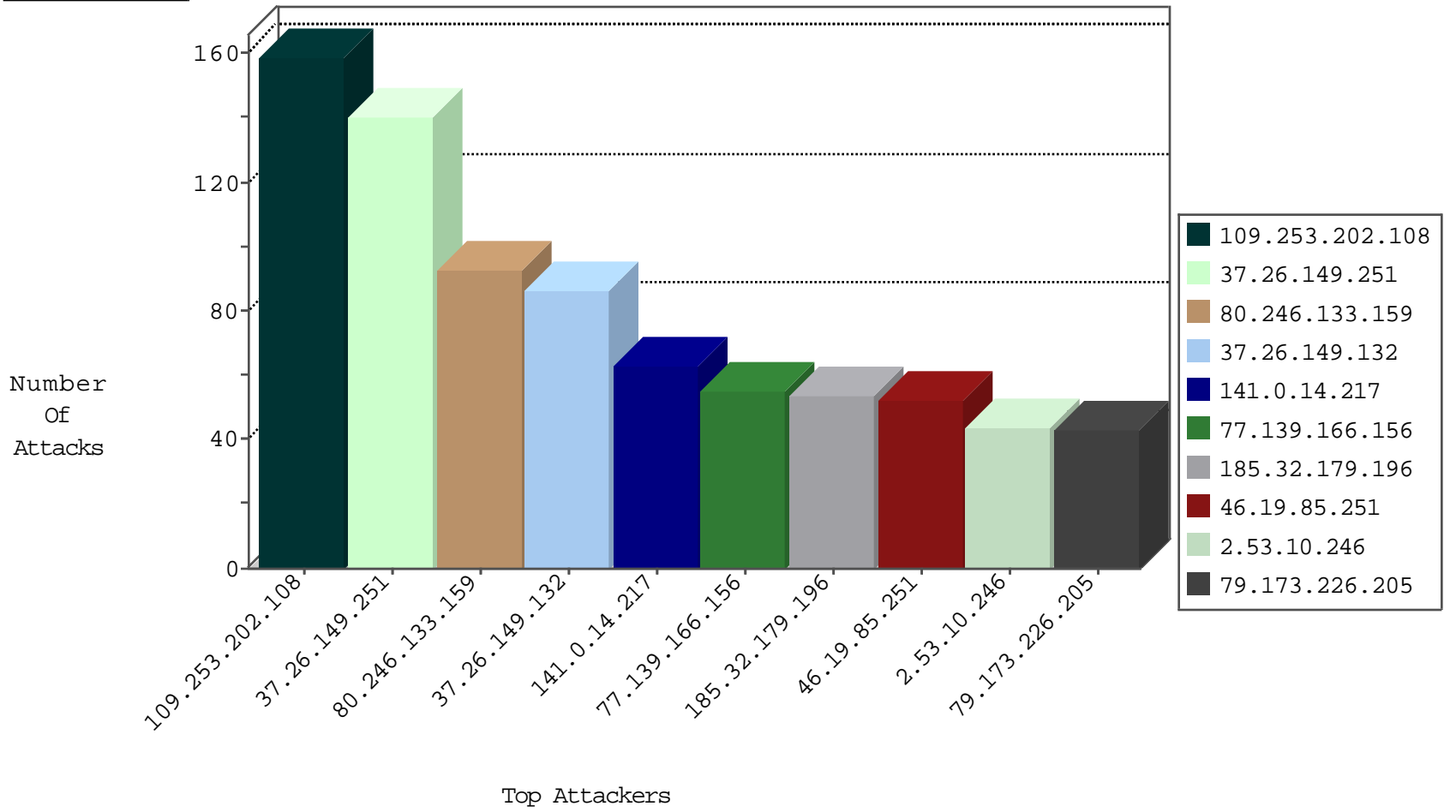
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.173.226.205	Jordan	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-cat	dest-reset	50
145.132.236.165	Netherlands	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	42
2.55.184.96	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	14
5.102.254.119	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	12
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	7
128.42.142.45	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	6
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.32.84.160	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
131.179.150.72	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	2
129.93.229.139	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
204.85.191.11	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.223.8.114	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.217.77.2	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
153.90.1.34	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.97.74.14	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.42.142.45	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.93.229.138	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
204.85.191.10	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.194.252.8	Australia	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.84	Czech Republic	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
141.22.213.34	Germany	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
160.80.221.37	Italy	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.105	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	22
69.30.210.242	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
123.126.113.99	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
151.80.40.87	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
91.224.160.106	147.237.77.233	Netherlands	atal.idf.il	ET SCAN Potential SSH Scan	2
141.226.217.236	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
91.224.160.106	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN Potential SSH Scan	1
185.27.106.104	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.72.156	Netherlands	aman.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
109.65.3.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.69.139.198	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.195	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
79.176.95.191	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.210.162.42	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.77.179	Netherlands	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
36.72.228.72	147.237.76.176	Indonesia	test.ncore.idf.il	ET SCAN NMAP -sS window 3072	1
91.224.160.106	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
23.91.75.231	147.237.76.198	United States	e.yochalan.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.76.34	Netherlands	yochalan.idf.il	ET SCAN Potential SSH Scan	1
2.53.62.175	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.70.2.54	147.237.77.216	Switzerland	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.72.217	Netherlands	e.idf.il	ET SCAN Potential SSH Scan	1
185.3.147.255	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN Potential SSH Scan	1
89.139.207.17	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.60.153.178	147.237.72.14	Russian Federation	dover.idf.il(old)	ET SCAN Potential VNC Scan 5900-5920	1
81.218.251.250	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.158.203.149	147.237.76.148	Netherlands	ggcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
62.0.103.33	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN Potential SSH Scan	1
46.117.107.241	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN Potential SSH Scan	1
23.91.75.231	147.237.77.179	United States	e.mazi.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
91.224.160.106	147.237.76.86	Netherlands	navy.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.98	147.237.77.226	United States	www.chamatz.aka.idf.il	ET DROP Dshield Block Listed Source	1
2.55.40.118	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
80.246.133.159	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	93
141.0.14.217	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
62.0.208.254	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	30
46.19.85.251	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	26
46.19.85.251	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	26
107.167.98.61	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	23
107.167.112.50	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	23
192.118.78.198	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
185.32.179.196	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
185.32.179.196	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	17
77.124.244.99	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
207.241.226.144	United States	147.237.72.166	aka.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	16
62.0.221.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	16
185.32.179.196	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	16
2.53.145.25	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
145.132.236.165	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.178	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
2.53.188.203	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	12
79.182.113.239	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.41	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.53.145.25	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
2.53.145.25	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	7
37.76.202.82	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
195.60.235.57	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
77.240.179.195	Czech Republic	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.192.127	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.178	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.77	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.253.211.17	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.86.41	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
185.3.147.162	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.53.145.11	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
176.13.15.222	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
176.13.15.222	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
109.253.200.181	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
176.13.19.96	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.235.98.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
185.32.179.196	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	4
37.26.149.181	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
212.179.214.29	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
2.53.145.25	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
185.27.106.104	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	3
62.0.200.202	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	3
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
185.27.106.104	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.68	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
79.173.226.205	Jordan	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
79.173.226.205	Jordan	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.85.135	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.53.145.25	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.202.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	159
37.26.149.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	140
37.26.149.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	86
77.139.166.156	France	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	55
2.53.10.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
176.13.228.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
46.19.85.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
2.53.34.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
87.69.252.138	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	10
77.138.142.147	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/kapatz/	Block	4
2.55.135.127	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.232.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
147.236.38.168	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/0/	Block	3
46.19.85.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.182.113.239	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
87.69.252.138	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakchal.idf.il/sip_storage/files/2/	Block	3
109.253.207.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.53.54.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.147.162	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
176.13.236.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.23.38	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
77.124.244.99	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
147.236.38.168	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for aka.idf.il/	Block	1
87.70.36.151	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
207.46.13.110	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
77.139.220.180	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Abnormally Long Request method	Block	1
66.249.64.105	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/m/main/giyus/general.aspx	Block	1
87.68.55.246	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	NULL Character in Header Name at	Block	1
37.47.1.217	Poland	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/miyun/miyunlobby.aspx	Block	1
104.128.144.131	Canada	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/redirect.php	Block	1
212.143.138.230	Israel	147.237.77.74	law.idf.il	Parameter Type Violation Master\$Header1\$ucHeaderSearch\$txtSearch in www.law.idf.il/602-6434-he/patzar.aspx	Block	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	Multiple Unknown HTTP Request Method from 169.229.3.91	Block	1
79.176.5.209	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Illegal Byte Code Character in Header Name	Block	1
66.249.66.62	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/contactus/contactus.aspx	Block	1
141.226.217.236	Israel	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/894-ar	Block	1
87.69.252.138	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 87.69.252.138	Block	1
77.138.142.147	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Unknown HTTP Request Method !e~ðóóááájWfš•#012~ in URL	Block	1
159.203.102.112	United States	147.237.76.39	mobile.meitav.idf.il	SSL Untraceable Connection - Unsupported Cipher	None	1
109.64.61.231	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
2.53.160.66	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
213.8.204.19	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Malformed HTTP Header Line 1	Block	1
66.249.76.53	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
37.26.147.162	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1