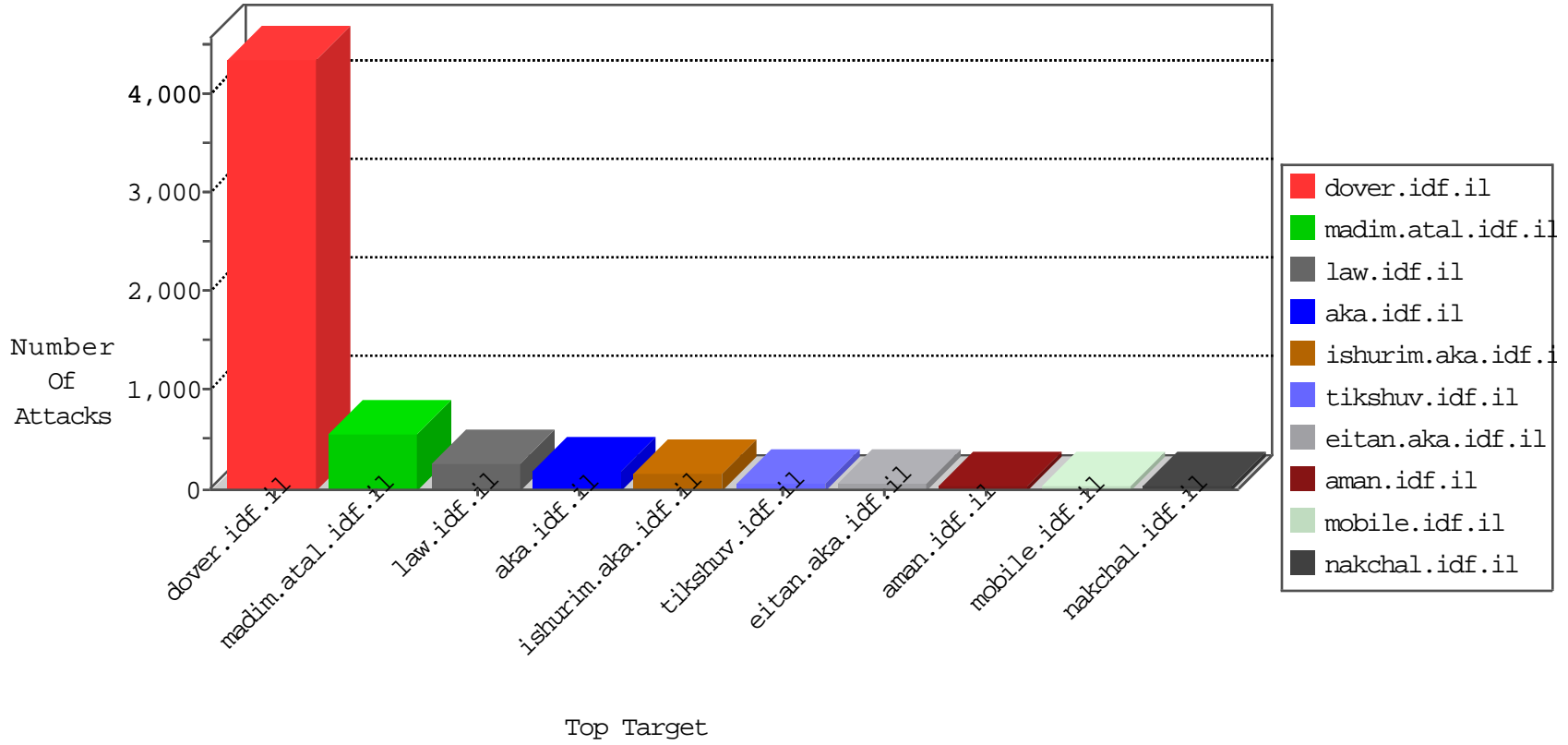




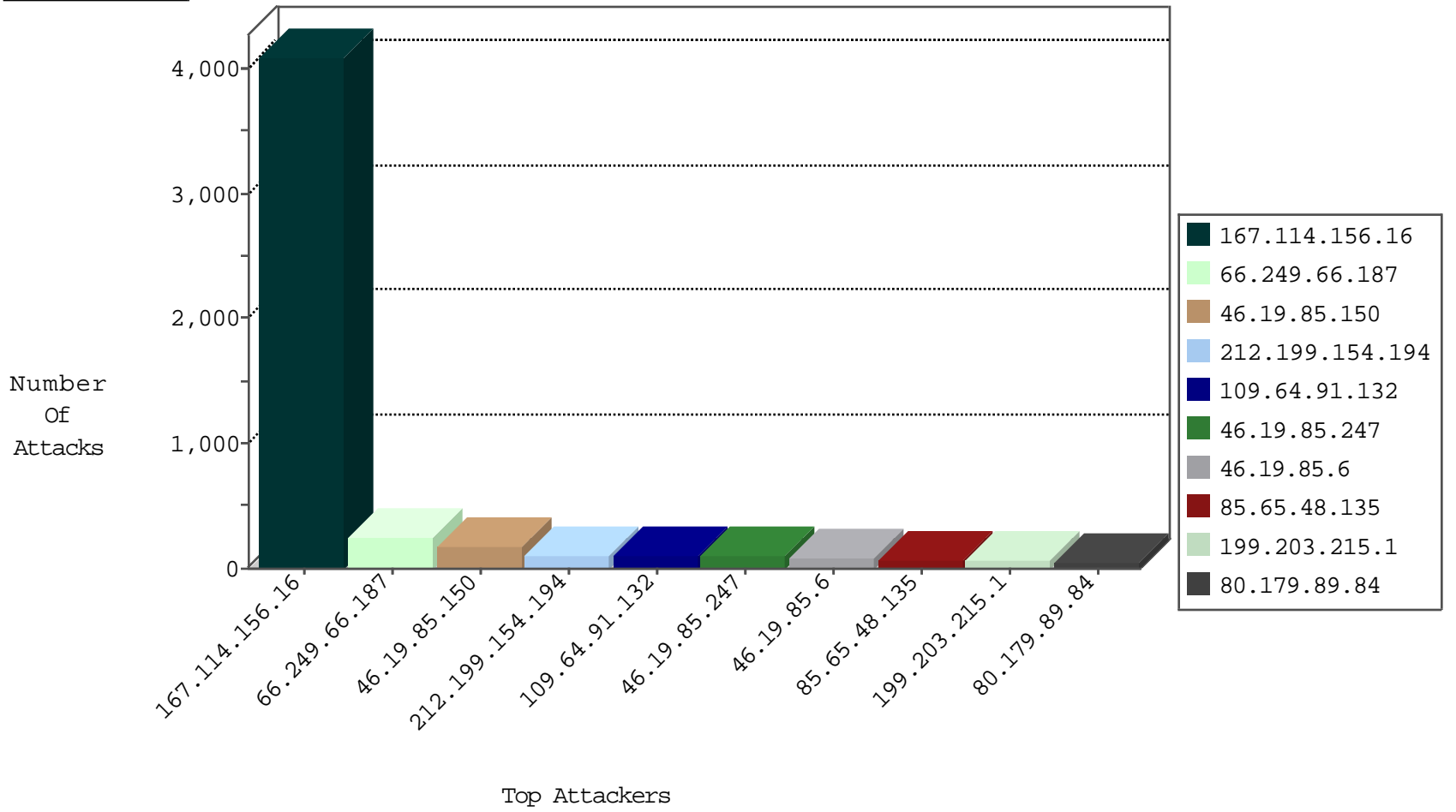
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4072
212.199.154.194	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	707
80.179.89.84	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	55
79.176.76.154	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	18
2.53.145.202	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
79.178.205.207	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
185.94.111.1	Russian Federation	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
84.87.210.52	Netherlands	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
94.102.49.116	Netherlands	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
93.174.93.50	Netherlands	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
45.32.231.87	Netherlands	147.237.76.176	test.noore.idf.il	Block_Ntp_All_Net	drop	1
123.30.183.145	Vietnam	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
94.102.49.116	Netherlands	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
45.32.231.87	Netherlands	147.237.77.235	sviva.idf.il	Block_Ntp_All_Net	drop	1
94.102.49.116	Netherlands	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.103.252.98	Russian Federation	147.237.76.30	himush.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	1
192.187.114.11	United States	147.237.76.86	navy.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.66.187	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	239
82.166.204.70	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.82.78.38	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.76.176	Netherlands	test.noore.idf.il	ET SCAN NMAP -sS window 1024	1
213.151.32.163	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
125.212.232.165	147.237.8.45	Vietnam	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
37.142.208.153	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
118.26.143.50	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
109.160.164.192	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.65.151.232	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.64.88.14	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.130.177	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.82.78.38	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
79.177.214.13	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.235.98.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
42.113.132.39	147.237.8.24	Vietnam	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
118.26.143.50	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1
2.53.184.223	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
118.26.143.50	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
89.138.48.65	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.64.191.7	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
199.203.215.1	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	52
212.199.154.194	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	29
2.53.190.17	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
85.130.231.164	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.85.248	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
185.32.179.87	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
80.179.197.6	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
185.57.213.39		147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.19.86.205	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	9
37.26.147.173	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
46.19.86.27	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.131.28	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.232	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.253.214.7	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.249	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.52	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.120.126.82	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.232	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.116.218.69	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.51	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	alert	6
46.19.85.0	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
81.218.51.218	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
176.13.12.96	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.232	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.0	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
66.249.66.20	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.119	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
149.88.188.223	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.119	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
87.69.208.74	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
149.88.188.223	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.162	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.85.119	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.119	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.145	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
185.32.179.87	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
109.253.200.69	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.142.119	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.159.150.241	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.154.189.8	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.205	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.64.183.11	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.162.149	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.33	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.66.22	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.251	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-19-2016-13:04:04 to 04-19-2016-14:04:04

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.86.50	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	180
109.64.91.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	108
46.19.85.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
46.19.85.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	81
85.65.48.135	Israel	147.237.0.34	tikshuv.idf.il	Automated Vulnerability Scanning V1	Block	61
2.53.171.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	46
109.253.215.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
179.36.193.101	Argentina	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 179.36.193.101	Block	11
46.19.86.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
192.116.232.69	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	6
8.37.232.238	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
192.116.232.69	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	4
37.239.68.125	Iraq	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 37.239.68.125	Block	3
2.55.43.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
194.90.128.185	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 194.90.128.185	Block	3
109.253.200.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	2
192.41.140.67	Netherlands	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00\$ContentPlaceHolder1\$txtEmail in www.idf.il/1038-en/dover.aspx	Block	2
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/nakhal	Block	2
87.69.85.182	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
54.193.120.63	United States	147.237.77.234	halag.idf.il	PHP Attempt	Block	1
31.168.100.81	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/4/112304.pdf	Block	1
80.246.133.30	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
212.179.21.194	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqquantity.aspx	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
176.13.5.198	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
2.53.171.82	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/mobile/templates/catalog/catalog.aspx	Block	1
82.110.109.210	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.181.179.222	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMai in www.aka.idf.il/main/sachar/	None	1
192.116.232.69	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakchal.idf.il/sip_storage/files/5/1475.png	Block	1
54.193.120.63	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/wp-login.php	Block	1
109.253.130.99	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/894-he/nakhal.aspx	Block	1
81.169.144.135	Germany	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to chinuch.aka.idf.il/wp/wp-admin/	Block	1
212.199.112.144	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 212.199.112.144	Block	1
68.180.231.62	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/yohalan/main0926.html	Block	1
46.235.44.54	Netherlands	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to chinuch.aka.idf.il/old/wp-admin/	Block	1
80.149.240.82	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	Block	1
66.249.66.123	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9698-he/refuah.aspx	Block	1
81.218.147.226	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/[=	Block	1
77.124.17.236	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
52.25.193.162	United States	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	1
85.250.16.228	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
80.246.130.37	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.66.177	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/4/70454.pdf	Block	1
82.109.66.146	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
77.125.122.120	Israel	147.237.72.166	aka.idf.il	Unknown Parameter _e_pi_ in www.aka.idf.il/main/gyus/default.aspx	None	1
52.25.193.162	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp-login.php	Block	1
192.115.190.190	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/homepage/mobile	Block	1
31.154.155.67	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/contactus.aspx	Block	1
80.246.130.45	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/faq/mobile	Block	1