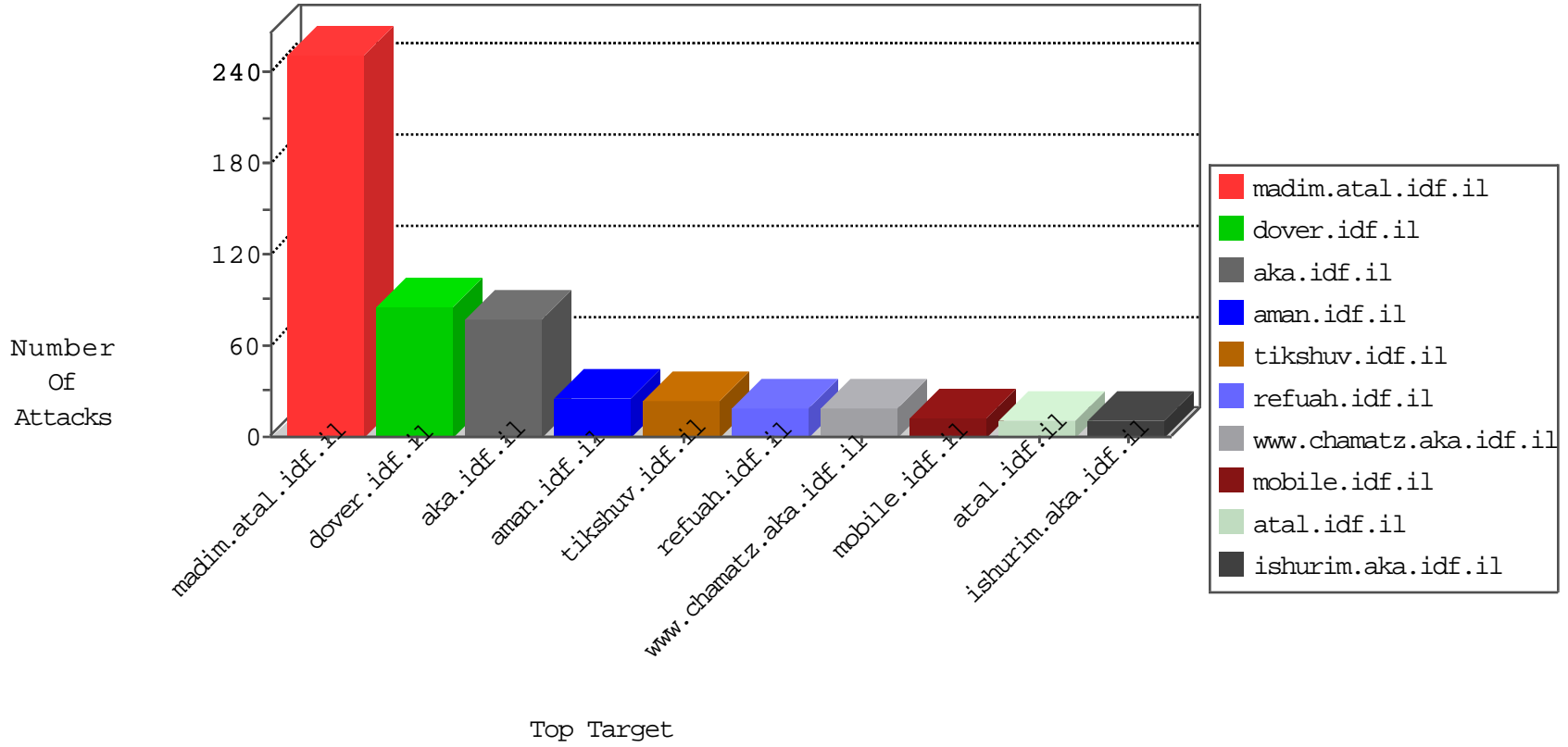


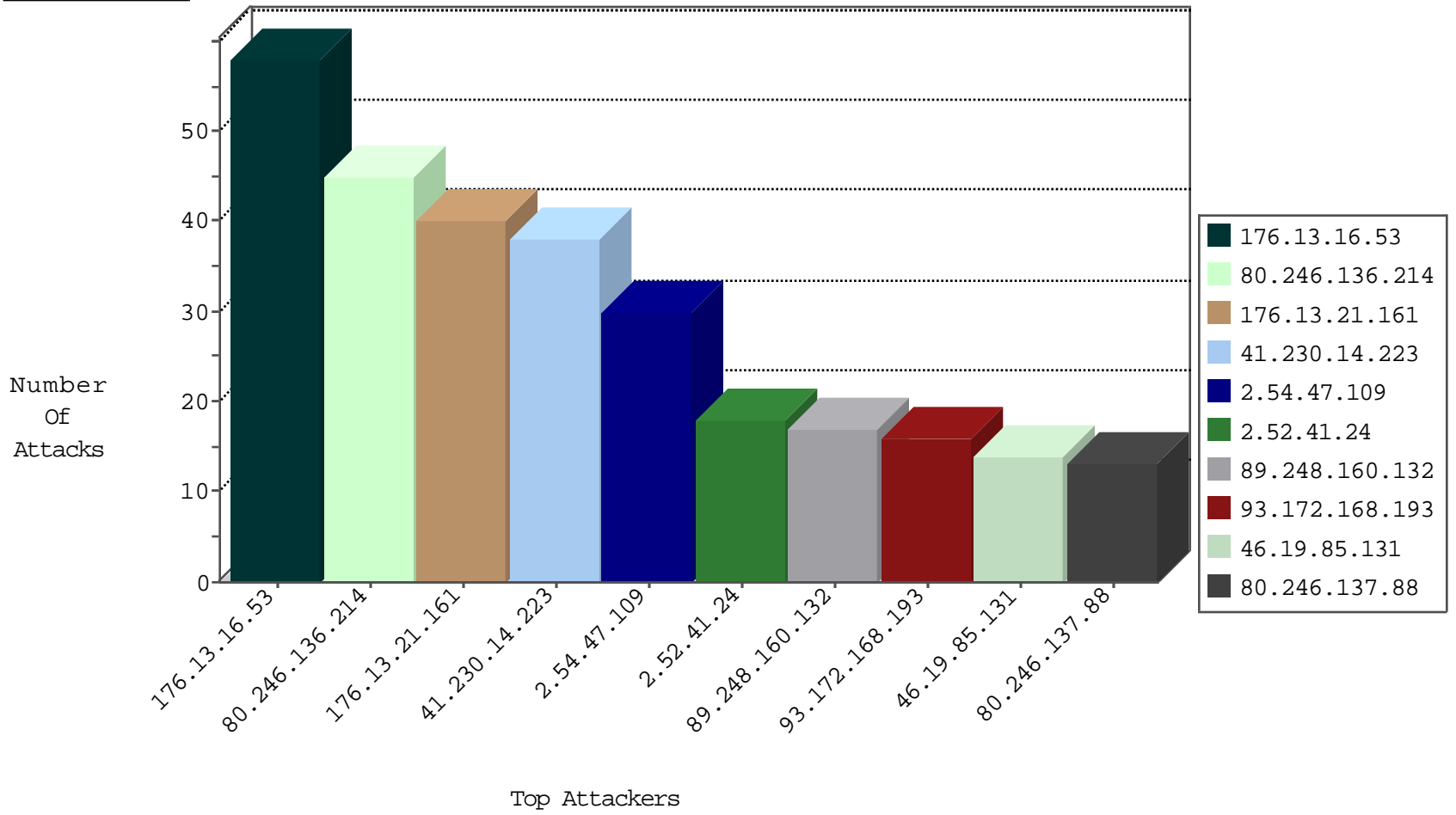
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
5.28.174.238	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
134.147.203.115	Germany	147.237.72.217	e.idf.il	Block_Ntp_All_Net	drop	2
216.218.206.75	United States	147.237.77.227	e.hamaz.idf.il	Block_Udp_All_Nets	drop	1
95.9.238.146	Turkey	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
85.105.106.121	Turkey	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
14.207.92.97	Thailand	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
85.105.106.121	Turkey	147.237.77.226	www.chamatz.aka.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.100	United States	147.237.72.166	aka.idf.il	Block_Ntp_All_Net	drop	1
36.234.185.133	Taiwan	147.237.77.205	prisha.idf.il	Block_Udp_All_Nets	drop	1
85.105.106.121	Turkey	147.237.77.227	e.hamaz.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.11	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
199.58.86.211	United States	147.237.77.216	doover.idf.il	C1000074: HTTP: majestic bot	Block	2
207.46.13.70	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
212.235.56.185	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
66.249.66.184	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
207.46.13.98	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
80.246.130.34	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

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
218.246.0.97	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
200.58.174.134	147.237.76.44	Bolivia	e.refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
113.76.90.223	147.237.72.156	China	aman.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
104.45.210.69	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.193	147.237.8.14	Netherlands	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.149.135	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
198.20.69.74	147.237.77.19	United States	law-forum.idf.il	ET DROP Dshield Block Listed Source	1
189.218.187.24	147.237.76.199	Mexico	e.nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.45.210.69	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 2048	1
104.45.210.69	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -f -sS	1
66.249.64.190	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
5.39.222.253	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.230.14.223	Tunisia	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
82.81.83.130	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
41.230.14.223	Tunisia	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.131	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.131	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.98	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
41.230.14.223	Tunisia	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
46.19.85.98	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
82.81.161.130	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
79.177.61.74	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.135	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.178	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.57.63	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
91.135.102.172	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.227.172	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.139	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.138.220	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.147.226	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.8.113.121	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.194.75	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
202.175.135.13	New Zealand	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
2.54.150.185	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
37.142.239.72	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
119.94.196.130	Philippines	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
192.118.60.69	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
157.55.39.183	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
37.26.147.171	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
2.54.150.185	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.218	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
2.54.150.185	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid sequence number	monitor	2
176.13.14.188	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
37.142.68.54	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
62.212.73.211	Netherlands	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
2.54.150.185	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
46.19.86.84	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
188.120.148.160	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
31.168.170.54	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
202.175.135.13	New Zealand	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
37.142.68.54	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
192.118.60.69	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
2.54.150.185	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
46.19.85.97	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
37.26.147.134	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.22	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
103.41.177.26		147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	illegal header format detected: Malformed HTTP protocol name in request	monitor	1
2.54.186.207	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.158	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
89.248.160.132	Netherlands	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.19.85.131	Israel	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	illegal header format detected: Illegal start line in request	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.16.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	51
80.246.136.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
176.13.21.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
2.54.47.109	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
2.52.41.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
80.246.137.88	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
80.246.138.28	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
109.253.200.120	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
41.230.14.223	Tunisia	147.237.77.216	doover.idf.il	Multiple Unauthorized URL Access from 41.230.14.223	Block	9
66.249.64.233	United States	147.237.77.216	doover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	9
37.26.147.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
2.54.167.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
109.253.212.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.185.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.10.176	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
46.19.86.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.102.7.226	United States	147.237.77.216	doover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.102.7.233	United States	147.237.77.216	doover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
176.13.14.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
89.138.109.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.120.160.88	Israel	147.237.77.216	doover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
93.172.168.193	Israel	147.237.77.216	doover.idf.il	Distributed PHP Attempt	Block	1
91.189.41.165	Sweden	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on refua.atal.idf.il/wordpress/wp-admin/	Block	1
184.105.139.68	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
68.180.230.240	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/5/112745.pdf	Block	1
93.172.168.193	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	1
64.19.78.243	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
208.113.197.86	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
93.172.168.193	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
23.101.61.176	Ireland	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/1048-7668-he/tikshuv.aspx#.vqutgvkrlcs	Block	1
66.249.66.26	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1133-he/atal.aspx	Block	1
103.41.177.26		147.237.76.42	refuah.idf.il	Abnormally Long Request request version	Block	1
93.172.168.193	Israel	147.237.77.216	doover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
46.120.160.88	Israel	147.237.77.233	atal.idf.il	Distributed PHP Attempt	Block	1
93.172.168.193	Israel	147.237.0.15	kosher-kravi.idf.il	PHP Attempt	Block	1
43.252.214.185	Japan	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
184.168.200.96	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on refua.atal.idf.il/test/wp-admin/	Block	1
113.76.90.223	China	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
77.221.130.140	Russian Federation	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
93.172.168.193	Israel	147.237.77.234	halag.idf.il	Distributed PHP Attempt	Block	1
46.120.160.88	Israel	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
93.172.168.193	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 93.172.168.193	Block	1
87.71.6.125	Israel	147.237.0.34	tikshuv.idf.il	Distributed PHP Attempt	Block	1
66.249.66.64	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	1
103.41.177.26		147.237.76.42	refuah.idf.il	Illegal HTTP Version instanceof HTML element	Block	1
93.172.168.193	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed PHP Attempt	Block	1
46.120.160.88	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/xmlrpc.php	Block	1
93.172.168.193	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/xmlrpc.php	Block	1
46.19.85.131	Israel	147.237.77.216	doover.idf.il	Illegal HTTP Version	Block	1
198.20.69.74	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1