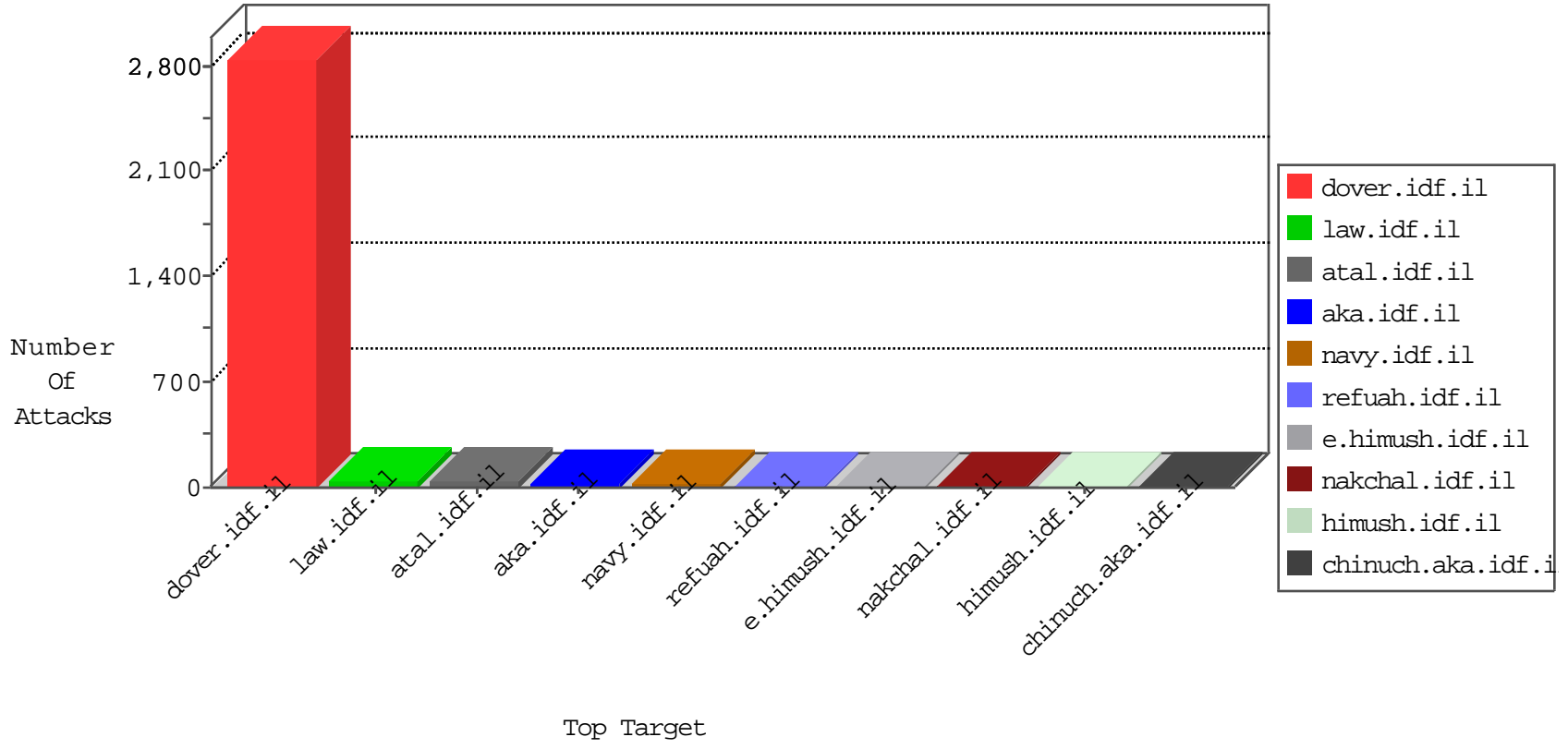


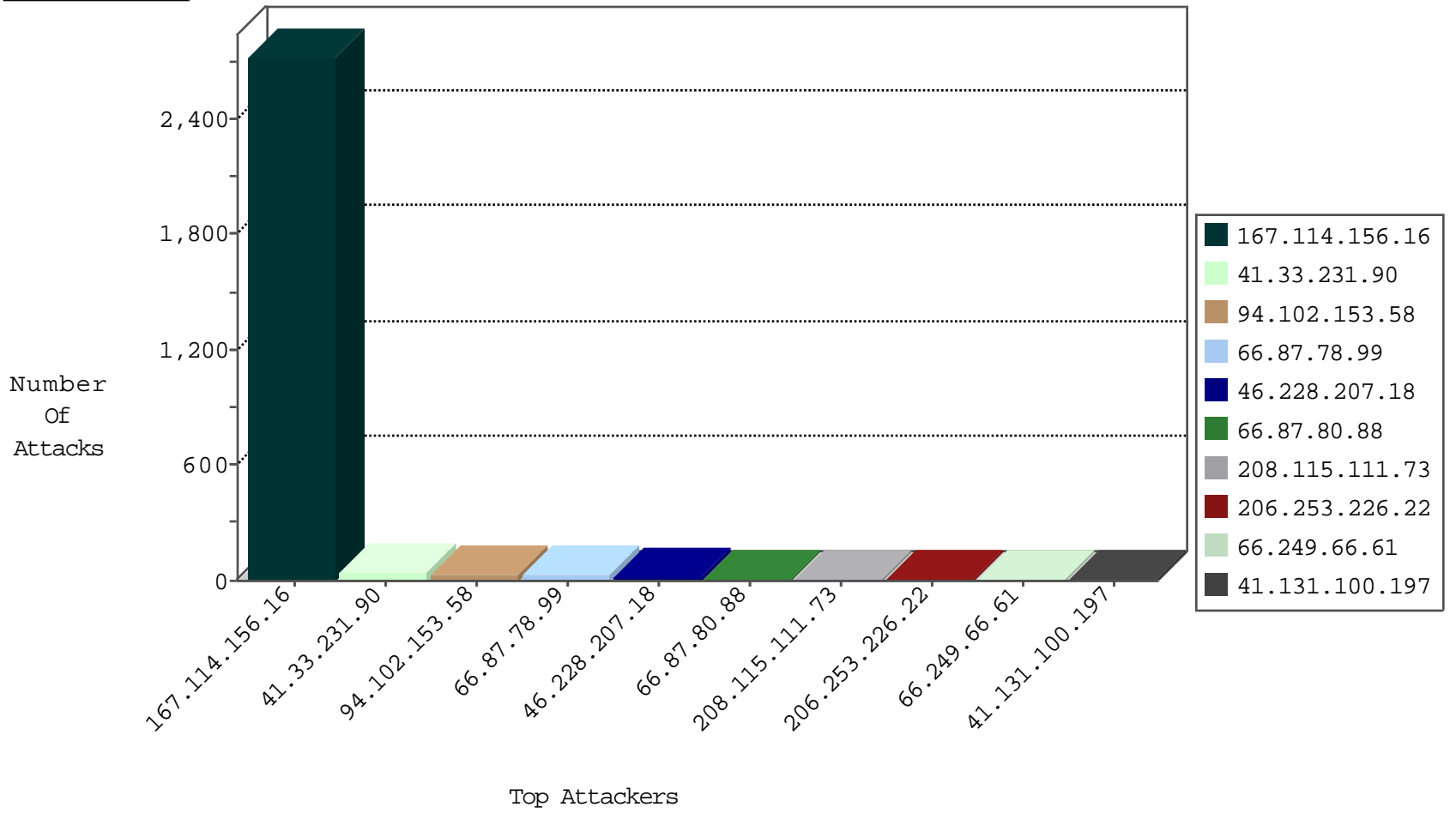
IDF Under Attack Daily Report



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	DOS-Tool-SwitchbladG	dest-reset	3515
66.249.66.61	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	276
202.112.51.96	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1
146.185.239.100	Russian Federation	147.237.77.234	halag.idf.il	block-sp-traf1	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
94.102.153.58	United Kingdom	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
222.84.7.172	China	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
144.76.44.138	Germany	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
105.158.68.33	Morocco	147.237.72.166	aka.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
94.102.153.58	147.237.77.233	United Kingdom	atal.idf.il	SQL Injection - Select From	24
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
46.228.207.18	147.237.76.42	Germany	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
46.228.207.18	147.237.77.216	Germany	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
46.228.207.18	147.237.76.197	Germany	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
46.228.207.18	147.237.76.177	Germany	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.228.207.18	147.237.76.148	Germany	gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.128.144.131	147.237.77.205	Canada	prisha.idf.il	ET SCAN NMAP -sS window 2048	1
46.228.207.18	147.237.76.30	Germany	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.228.207.18	147.237.77.243	Germany	mobile.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.151.55.35	147.237.0.34	Ukraine	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
46.228.207.18	147.237.76.202	Germany	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.228.207.18	147.237.76.198	Germany	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.228.207.18	147.237.76.196	Germany	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
198.20.69.74	147.237.77.74	United States	law.idf.il	ET DROP Dshield Block Listed Source	1
46.228.207.18	147.237.76.176	Germany	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
193.105.134.220	147.237.0.35	Sweden	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
46.228.207.18	147.237.76.86	Germany	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.128.144.131	147.237.77.205	Canada	prisha.idf.il	ET SCAN NMAP -f -sS	1
46.228.207.18	147.237.76.31	Germany	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.248.172.140	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
46.228.207.18	147.237.8.50	Germany	e.tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.228.207.18	147.237.77.235	Germany	sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.228.207.18	147.237.77.212	Germany	e.dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.228.207.18	147.237.76.200	Germany	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
66.87.78.99	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	26
66.87.80.88	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
157.55.39.153	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
41.131.100.197	Egypt	147.237.77.74	law.idf.il	drop	SAM rule	drop	4
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
157.55.39.165	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
157.55.39.219	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
157.55.39.55	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
208.115.111.73	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
222.84.7.172	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
78.186.2.212	Turkey	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	2
66.249.75.102	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
206.253.226.22	United States	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
206.253.226.22	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
119.94.218.44	Philippines	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
202.112.51.96	China	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.78	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.104	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.34	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.211	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.121.180	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
208.115.111.73	United States	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	1
202.112.51.96	China	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.75	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.79	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
208.115.111.73	United States	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	1
41.131.100.197	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
184.105.247.228	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.121.181	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.139.107	United States	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
146.185.239.102	Russian Federation	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
104.128.144.131	Canada	147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
208.115.111.73	United States	147.237.76.200	eitan.aka.idf.il	drop	SAM rule	drop	1
50.16.27.108	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.247	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
141.212.122.66	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.86	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.18	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.120	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
115.230.124.164	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
208.115.111.73	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
199.203.122.61	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.67	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
162.203.2.233	United States	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationsevice.aspx/getauthuser	Block	6
199.30.25.229	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	3
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
74.6.53.166	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 74.6.53.166	Block	1
66.249.66.28	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
141.212.122.64	United States	147.237.0.15	kosher-kravi.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
78.186.2.212	Turkey	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
66.249.78.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/5/size100x0/3365.jpg	Block	1
74.6.53.167	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 74.6.53.167	Block	1
66.249.66.43	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20191-he/dover.aspx	Block	1
78.186.2.212	Turkey	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/xmlrpc.php	Block	1
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 66.249.78.248	Block	1
206.253.226.22	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
40.77.167.83	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/1106-7.stm.	Block	1
74.6.53.167	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wordpress/wp-admin/	Block	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
199.16.156.124	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/7/size220x0/17467.jpg	Block	1
105.158.68.33	Morocco	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
73.5.149.74	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
206.253.226.22	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
46.117.81.206	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
119.94.218.44	Philippines	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
74.6.53.168	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 74.6.53.168	Block	1
66.249.66.75	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.66.75	Block	1
199.16.156.125	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/sip_storage/files/7/size220x0/17467.jpg	Block	1
105.158.68.33	Morocco	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/wp-login.php	Block	1
73.5.149.74	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
46.236.24.53	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
119.94.218.44	Philippines	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	1
74.6.53.168	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/test/wp-admin/	Block	1
66.249.67.250	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/tmuna/	Block	1
107.130.127.80	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1