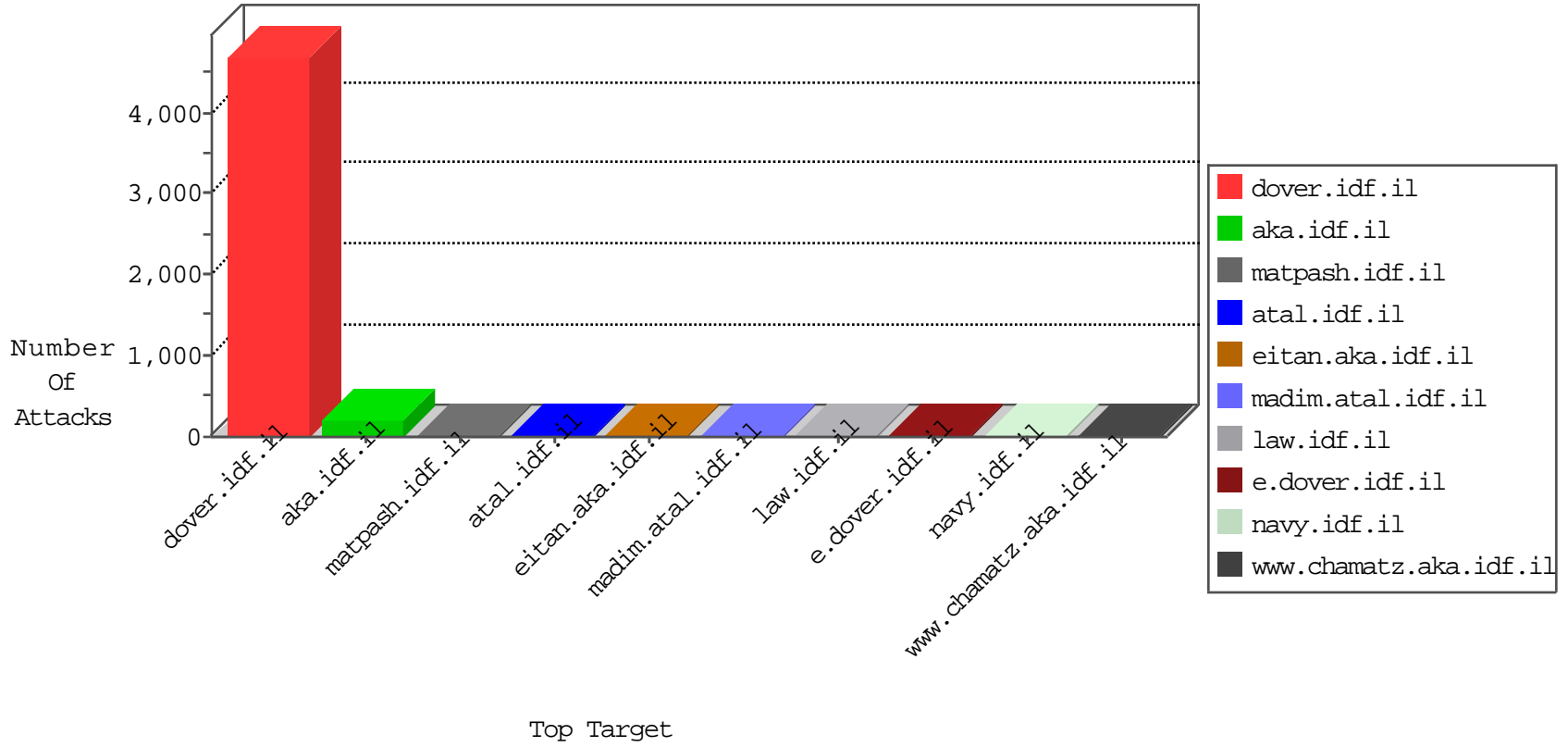


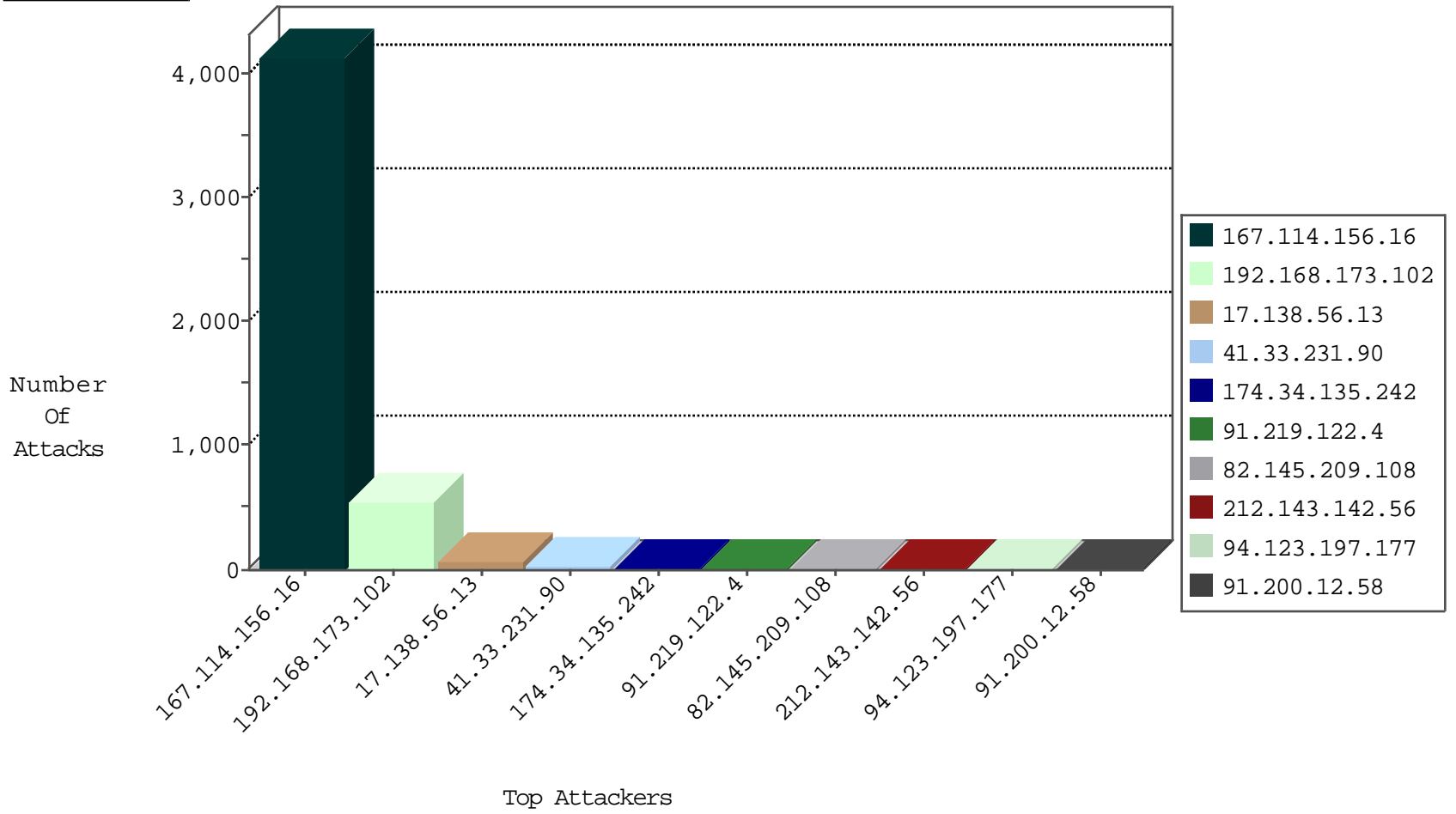
IDF Under Attack Daily Report



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	4136
82.145.209.108	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	10
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	3
184.105.139.108	United States	147.237.8.14	e.orchot.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.80	United States	147.237.8.28	e.mobile-ks.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.92	United States	147.237.77.227	e.hamaz.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.124	United States	147.237.0.19	madim.atal.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.84	United States	147.237.77.74	law.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.96	United States	147.237.8.50	e.tikshuv.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.72	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1	Russian Federation	147.237.77.212	e.dover.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.84	United States	147.237.77.212	e.dover.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.96	United States	147.237.77.243	mobile.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.76	United States	147.237.77.170	maarachot.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.92	United States	147.237.0.35	akaws.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.149	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
91.219.122.4	Poland	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
174.34.135.242	United States	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	4
174.34.135.242	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
174.34.135.242	United States	147.237.0.34	tikshuv.idf.il	C1000074: HTTP: majestic bot	Block	2
174.34.135.242	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
174.34.135.242	United States	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Block	2
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
207.46.13.45	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
91.219.122.4	147.237.77.233	Poland	atal.idf.il	SQL Injection - Select From	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
66.249.69.34	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
180.76.170.207	147.237.76.86	China	navy.idf.il	ET SCAN NMAP -sS window 1024	1
145.132.1.222	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
104.128.144.131	147.237.72.156	Canada	aman.idf.il	ET SCAN NMAP -sS window 4096	1
95.45.254.123	147.237.72.166	Ireland	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
64.31.98.203	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
14.169.75.189	147.237.8.28	Vietnam	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
145.132.1.222	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
106.184.2.29	147.237.72.156	Japan	aman.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.131	147.237.8.28	Canada	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 3072	1
93.183.201.2	147.237.0.200	Ukraine	m4u.idf.il	ET SCAN Potential SSH Scan	1
49.149.137.178	147.237.76.31	Philippines	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
208.100.26.228	147.237.8.28	United States	e.mobile-ks.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
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	369
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	175
17.138.56.13	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	57
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
94.123.197.177	Turkey	147.237.77.216	dover.idf.il	drop	SAM rule	drop	8
155.254.215.182	Bahrain	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
73.171.202.86	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
66.249.65.16	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.244.118.251	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
213.244.118.251	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
79.181.231.193	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
207.241.229.237	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
199.30.24.136	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
199.30.25.29	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
157.55.2.143	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
104.148.44.149	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
74.82.47.31	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.133.98.138	Ukraine	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1
180.76.170.207	China	147.237.76.86	navy.idf.il	drop	SAM rule	drop	1
106.184.3.122	Japan	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
216.218.206.79	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
85.104.154.209	Turkey	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.215	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
157.55.39.205	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
104.148.44.149	United States	147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
213.244.119.251	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
195.62.53.168	Russian Federation	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.31	United States	147.237.76.148	ggqcenter.aka.idf.il	drop		drop	1
65.31.129.157	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
180.76.170.207	China	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
106.184.3.122	Japan	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.115	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
208.115.111.68	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
74.82.47.10	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.252	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
169.229.3.90	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
104.156.240.216	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
213.244.119.251	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
74.82.47.47	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
195.62.53.168	Russian Federation	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.139.75	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
117.114.135.68	China	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
104.128.144.131	Canada	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.18	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
186.143.131.125	Argentina	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
169.229.3.90	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
106.38.241.149	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
216.218.206.70	United States	147.237.76.198	e.yohalan.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
107.77.72.125	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
91.200.12.58	Ukraine	147.237.77.176	matpash.idf.il	PHP Attempt	Block	4
91.200.12.58	Ukraine	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 91.200.12.58	Block	3
157.55.39.108	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/kamlar/news/www.idf.il/mivtza	Block	1
188.214.14.52	Romania	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
130.185.155.10	Sweden	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
66.249.69.2	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
157.55.39.205	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
194.187.168.208	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
130.185.155.10	Sweden	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/wp-login.php	Block	1
66.249.69.18	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
157.55.39.243	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
91.200.12.58	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
23.81.235.118	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
157.55.39.21	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.69.34	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.69.34	Block	1
169.229.3.90	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/ts.php	Block	1
95.45.254.123	Ireland	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
62.210.77.51	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1008-en/+navmenu.qc+	Block	1
157.55.39.29	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/site/links.aspx	Block	1
74.82.47.3	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
169.229.3.90	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/ts.php	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17551-en/dover.aspxand	Block	1