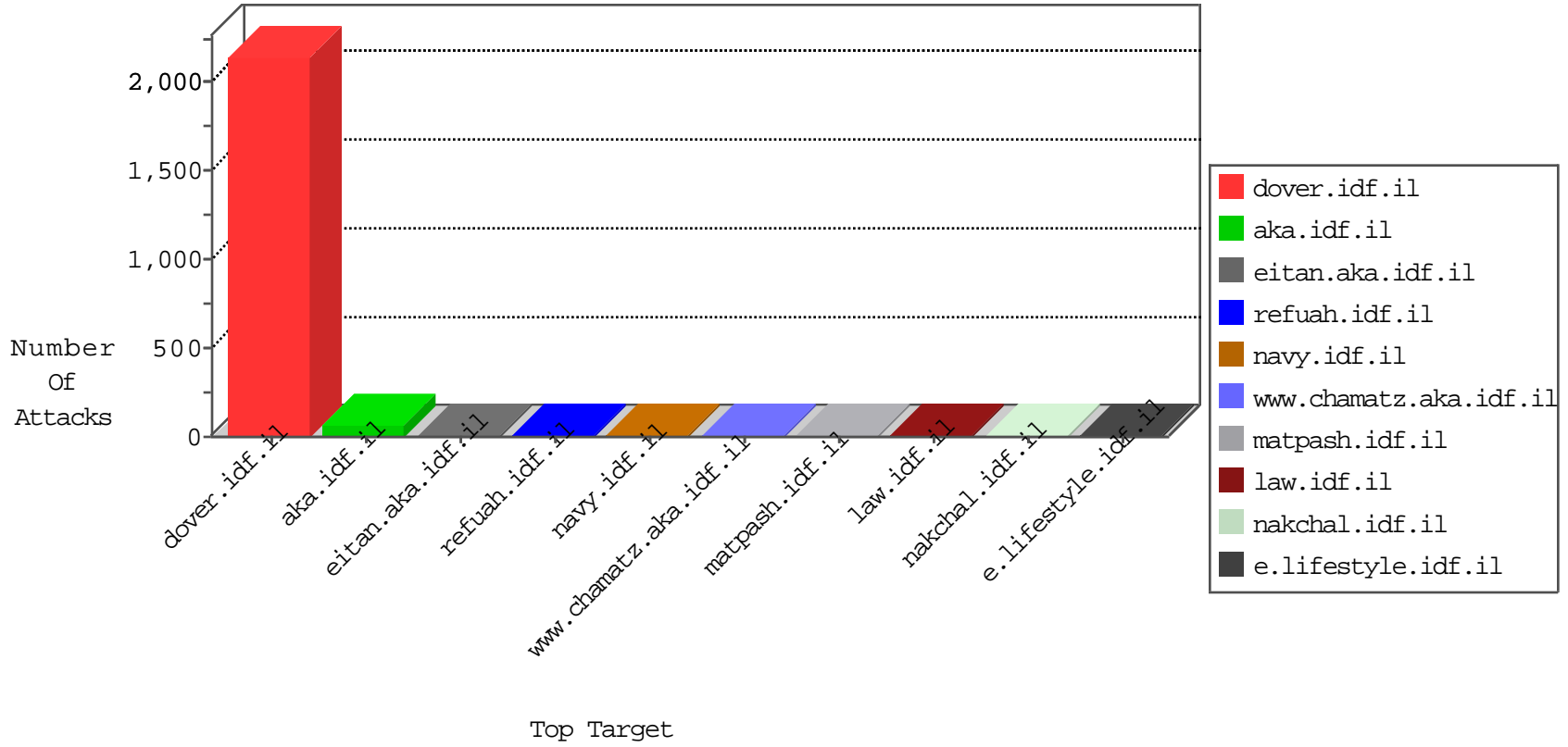


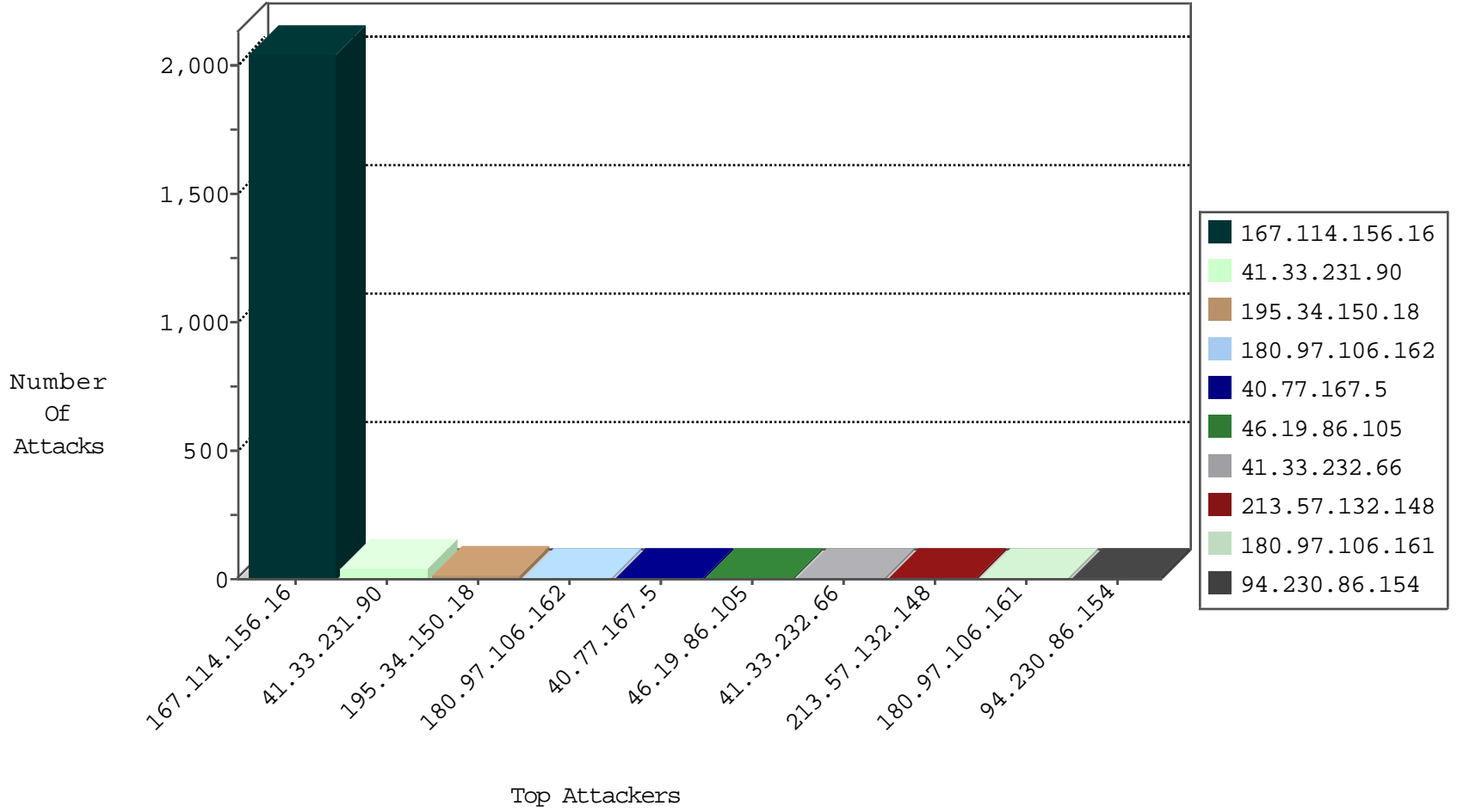
# IDF Under Attack Daily Report



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	3561
204.42.253.2	United States	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	2
180.97.106.162	China	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
111.123.71.35	China	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
171.88.11.214	China	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1

12-25-2015-06:04:09 to 12-25-2015-07:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
108.59.8.70	United States	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	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
66.249.78.69	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
218.104.49.211	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
187.184.244.105	147.237.0.33	Mexico	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
109.235.254.181	147.237.8.24	Turkey	e.lifestyle.idf.il	ET SCAN NMAP -sS window 4096	1
109.235.254.181	147.237.8.24	Turkey	e.lifestyle.idf.il	ET SCAN NMAP -f -sS	1
87.197.159.157	147.237.0.16	Slovakia	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
187.184.244.105	147.237.0.15	Mexico	kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
109.235.254.181	147.237.8.24	Turkey	e.lifestyle.idf.il	ET SCAN NMAP -sS window 2048	1
94.102.48.195	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.78.165	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	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
46.19.86.105	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
94.230.86.154	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
207.233.109.102	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
130.193.51.91	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.146.117	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
141.8.132.112	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	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.229.173.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.57.132.148	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
213.57.132.148	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
157.55.39.53	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
128.232.110.28	United Kingdom	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
157.55.39.178	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
71.59.141.35	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
68.180.229.121	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
68.180.229.239	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
176.13.0.181	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
74.82.47.30	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
180.97.106.161	China	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	1
63.143.231.49	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
207.233.109.102	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.187.114.171	France	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.139.104	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
92.222.242.102	France	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
180.97.106.161	China	147.237.77.243	mobile.idf.il	drop	SAM rule	drop	1
68.187.88.6	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
176.13.14.223	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
216.218.206.70	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.85.122	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.133	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.3.144.57	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
2.54.164.139	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
94.242.228.108	Luxembourg	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
180.97.106.162	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
80.246.136.111	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
180.97.106.161	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
66.249.64.143	Israel	147.237.0.33	idf.il	drop		drop	1
37.187.114.171	France	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.110	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
92.222.242.102	France	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
180.97.106.162	China	147.237.0.19	madim.atal.idf.il	drop	SAM rule	drop	1
180.97.106.36	China	147.237.0.15	kosher-kravi.idf.il	drop	SAM rule	drop	1
216.218.206.82	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.134	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
2.54.164.139	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
40.77.167.5	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1515-en/show-image.asp	Block	4
207.46.13.21	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1515-en/show-image.asp	Block	3
40.77.167.5	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 40.77.167.5	Block	3
85.64.52.49	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.66.183	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/tmuna/	Block	1
40.77.167.11	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-12847-he/dover.aspx?x3A;?x3D?x3E'0Qae03ae x'a, -a,,c03E'x'a, -A 03Açx'aešA-x'aeZAc03E'0Qae03Açx'aešA-0uA;03E' x'a, -Aš03aeš02A-03E'0Qae03ae x'a, -a,,c03E'02Ac03Açx'a, -Aš 02A-03ae 02A;03E'0Qae03Açx'aešA-0uA;03E'x'a, -Aš03aeš02Aç03E' 0Qae03ae x'a, -a,,c03E'02Ac03Açx'a, -Aš02A-03ae 02A;03E'0Qae0 03Açx'aešA-0uA;03E'x'a, -Aš03aeš02Aç	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
141.212.122.129	United States	147.237.76.200	eitan.aka.idf.il	Malformed URL proxystest.zmap.io:80	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	1
66.147.244.101	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	1
31.154.152.77	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 31.154.152.77	Block	1
185.100.85.61		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
85.64.170.91	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 85.64.170.91 (sigalgs DoS Attack)	None	1
66.249.78.67	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
41.203.18.134	South Africa	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
207.46.13.9	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/dynamic_map/dynamic_map.aspx	Block	1
141.212.122.129	United States	147.237.77.226	www.chamatz.aka.idf.il	Multiple Malformed URL from 141.212.122.129	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mivtza	Block	1
66.249.64.118	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/164-5160-he/patzar.aspx	Block	1
31.154.152.77	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/gen_204	Block	1
195.154.194.111	France	147.237.77.74	law.idf.il	PHP Attempt	Block	1
85.64.170.91	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/forums/asp/showforum.asp	Block	1
41.203.18.134	South Africa	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
157.55.39.54	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/faq.aspx	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-ar/cogat.aspx	Block	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-13907-he/dover.aspx	Block	1
195.154.194.111	France	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/wp-login.php	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/prisha/	Block	1
45.35.71.181		147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	1
157.55.39.186	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
80.246.136.38	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.28	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
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	1
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	1
66.249.78.165	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.147.244.101	United States	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
185.3.146.117	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/apple-touch-icon-precomposed.png	Block	1