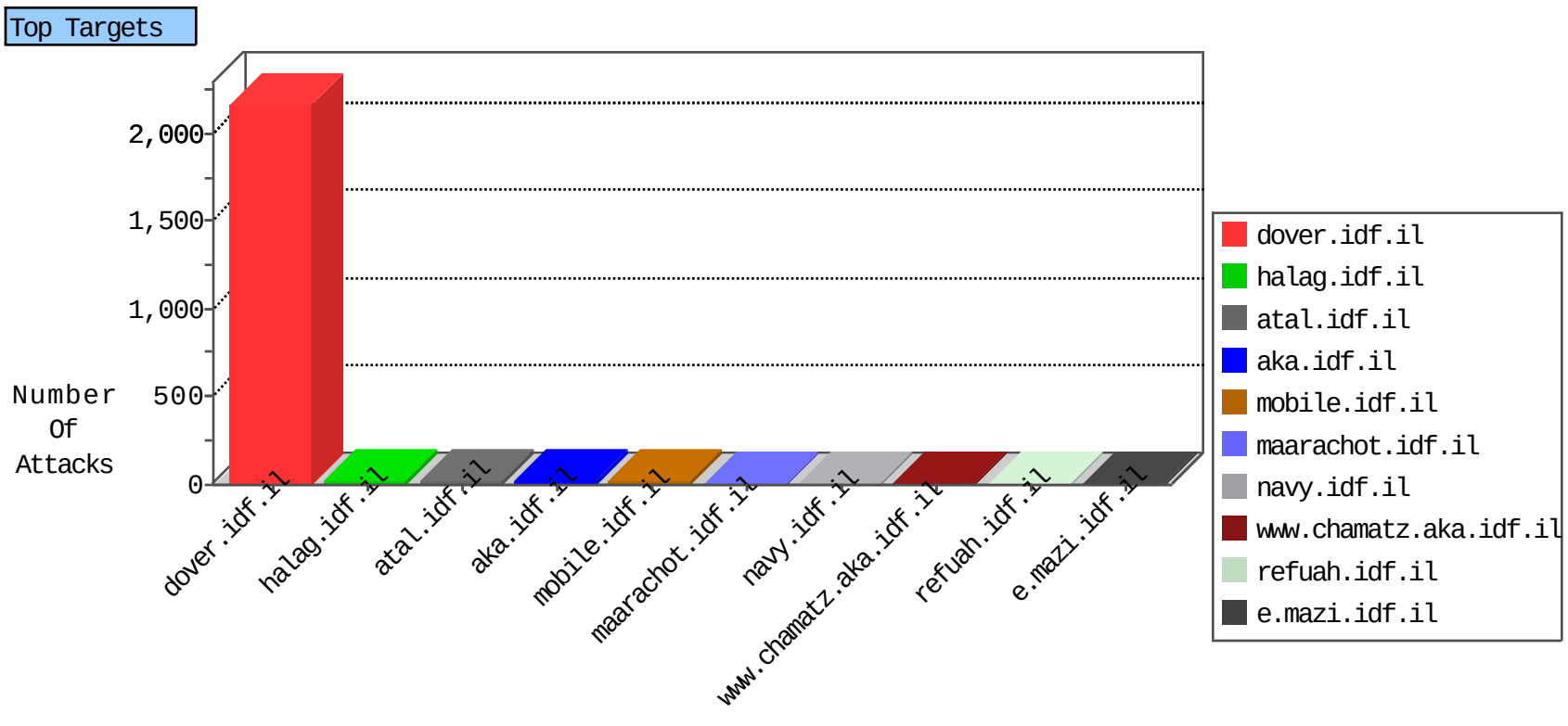
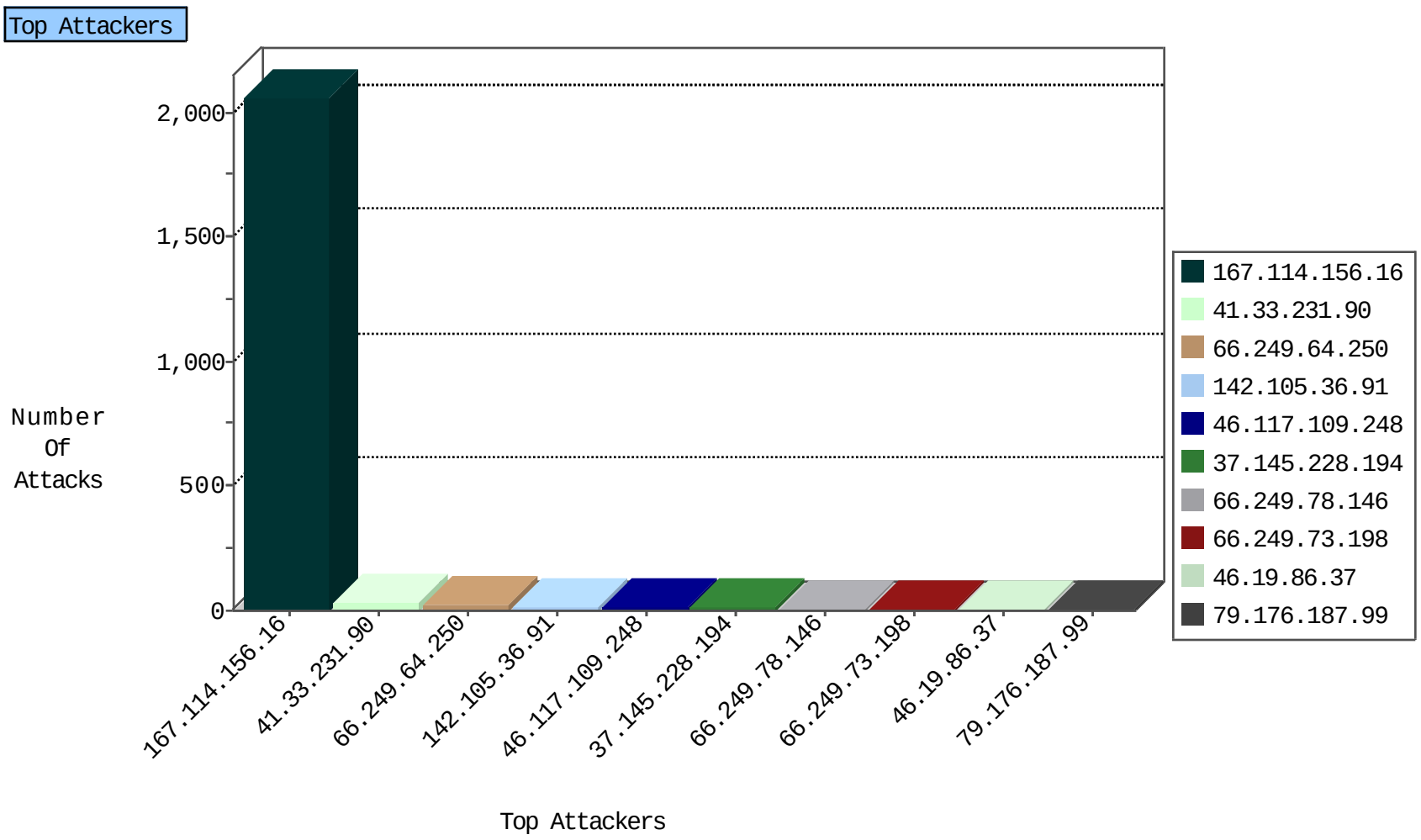
01-13-2016-04:04:00 to 01-13-2016-05:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-13-2016-04:04:00 to 01-13-2016-05:04:00

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	3221
66.249.73.198	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1864
37.145.228.194	Russian Federation	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
185.130.5.224		147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
63.141.227.98	United States	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1

01-13-2016-04:04:00 to 01-13-2016-05:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
177.185.194.92	Brazil	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
202.124.109.87	New Zealand	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

01-13-2016-04:04:00 to 01-13-2016-05:04:00

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	3
202.124.109.87	147.237.77.74	New Zealand	law.idf.il	SQL Injection - Select From	3
177.185.194.92	147.237.77.233	Brazil	atal.idf.il	SQL Injection - Select From	3
220.231.195.122	147.237.77.243	China	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
172.98.200.238	147.237.77.170		maarachot.idf.il	ET SCAN NMAP -sS window 4096	1
172.98.200.238	147.237.77.170		maarachot.idf.il	ET SCAN NMAP -f -sS	1
151.11.201.3	147.237.76.86	Italy	navy.idf.il	ET SCAN NMAP -sS window 2048	1
98.119.105.221	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 4096	1
98.119.105.221	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -f -sS	1
5.39.222.196	147.237.8.14	Netherlands	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
220.231.195.122	147.237.77.243	China	mobile.idf.il	ET SCAN NMAP -sS window 3072	1
172.98.200.238	147.237.77.170		maarachot.idf.il	ET SCAN NMAP -sS window 2048	1
151.11.201.3	147.237.76.86	Italy	navy.idf.il	ET SCAN NMAP -sS window 4096	1
151.11.201.3	147.237.76.86	Italy	navy.idf.il	ET SCAN NMAP -f -sS	1
98.119.105.221	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 2048	1
61.182.170.38	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1

01-13-2016-04:04:00 to 01-13-2016-05:04:00

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	32
66.249.64.250	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	22
142.105.36.91	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.117.109.248	Israel	147.237.77.233	atal.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	6
79.176.187.99	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.117.109.248	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
212.76.127.219	Israel	147.237.77.226	www.chamatz.aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
177.185.192.50	Brazil	147.237.77.233	atal.idf.il	drop	SAM rule	drop	4
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
81.169.237.146	Germany	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	3
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
178.154.189.201	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
95.26.231.188	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
37.145.228.194	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.249.64.139	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
84.109.96.202	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
81.169.237.146	Germany	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	2
141.212.122.186	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
95.26.231.188	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.3.144.18	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.26	United States	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.100	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
158.255.6.220	Russian Federation	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.186	United States	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
104.130.78.65	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
188.143.232.19	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
74.82.47.28	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
61.240.144.67	China	147.237.76.200	eitan.aka.idf.il	Web Server Enforcement Violation	Masscan Port Scanner	reject	1
158.255.6.220	Russian Federation	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.145.228.194	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
141.212.122.177	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.70	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.118	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
158.255.6.220	Russian Federation	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
46.19.86.36	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.187	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
106.75.199.187	China	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.47	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.80	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
61.240.144.67	China	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
158.255.6.220	Russian Federation	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.145.228.194	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.178	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.208	United States	147.237.76.177	ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.36	Israel	147.237.77.216	dover.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
46.19.86.37	Israel	147.237.77.243	mobile.idf.i	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	7
84.108.32.126	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
8.37.70.71	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1395-en/dover.aspx?pagenum=2&lang=en&sortdir=asc&usg=alkjrhiosuo8w-pi4juryd4w51_pt5f6ow	Block	1
188.143.232.19	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.143.232.19	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/salah.stm" target="_blank	Block	1
8.37.71.30	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 8.37.71.30	Block	1
207.46.13.180	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	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
37.187.129.166	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
8.37.70.72	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1395-en/dover.aspx&usg=alkjrhiz3e6wai7-w4spouucpboq43xgjq	Block	1
188.143.232.19	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/article.in.aspx/templates/sendtofriend/sendtofriend.aspx	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.i	Unauthorized URL Access to 147.237.76.42/templates/shared/usercontrols/headerupper/	Block	1
8.37.71.30	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/&usg=alkjrhhrvywoidsb7pl81jcyo5_5on2nsq	Block	1
208.184.112.74	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/1133-22638-he/dover.aspx.	Block	1
8.37.70.139	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1395-en/dover.aspx?pagenum=3&lang=en&sortdir=asc&usg=alkjrhi6miyjcadvx9lhldixezmshy5x6g	Block	1
195.154.227.118	France	147.237.77.216	dover.idf.il	Illegal HTTP Version HTTP/	Block	1
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	1
8.37.71.91	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-18154-en/dover.aspx&usg=alkjrhg0qvgkv0zbhp71rzol6ccwcd1qog	Block	1
5.255.253.47	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
219.133.153.216	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
117.78.13.54	China	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
66.249.64.172	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/894-en	Block	1
8.37.71.15	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 8.37.71.15	Block	1
199.30.24.227	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.176.187.99	Israel	147.237.77.243	mobile.idf.i	Distributed Suspicious Response Code	Block	1
17.138.55.165	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
8.37.70.43	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-19259-en/dover.aspx&usg=alkjrhgygzlcans2kuj4irhbjyh_mkmdea	Block	1
157.55.39.156	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/chamatz/kurs/default.asp	None	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	1
8.37.71.15	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-18098-en/dover.aspx&usg=alkjrhimoybhjnyldxhdov560qbonofudq	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
37.187.129.166	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1