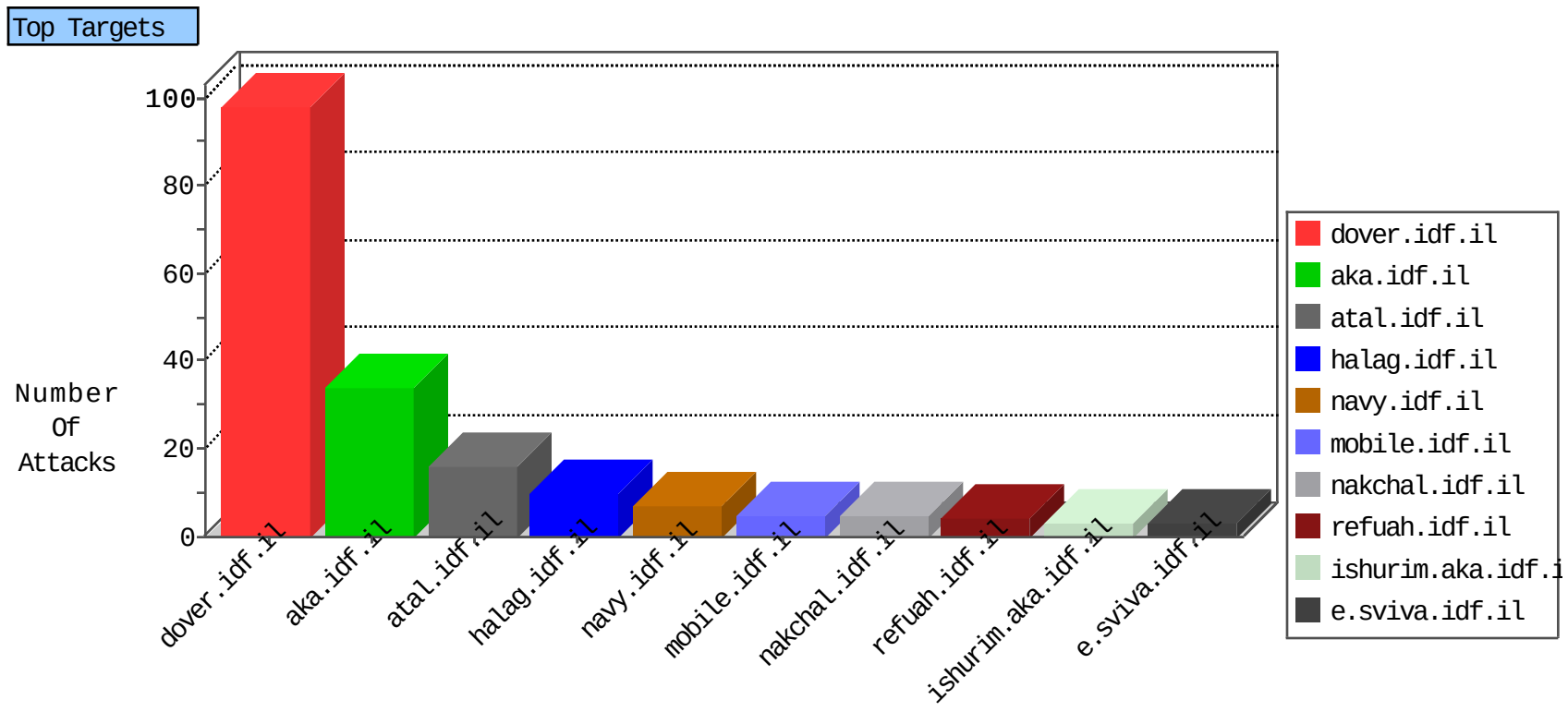
01-09-2016-02:04:04 to 01-09-2016-03:04:04

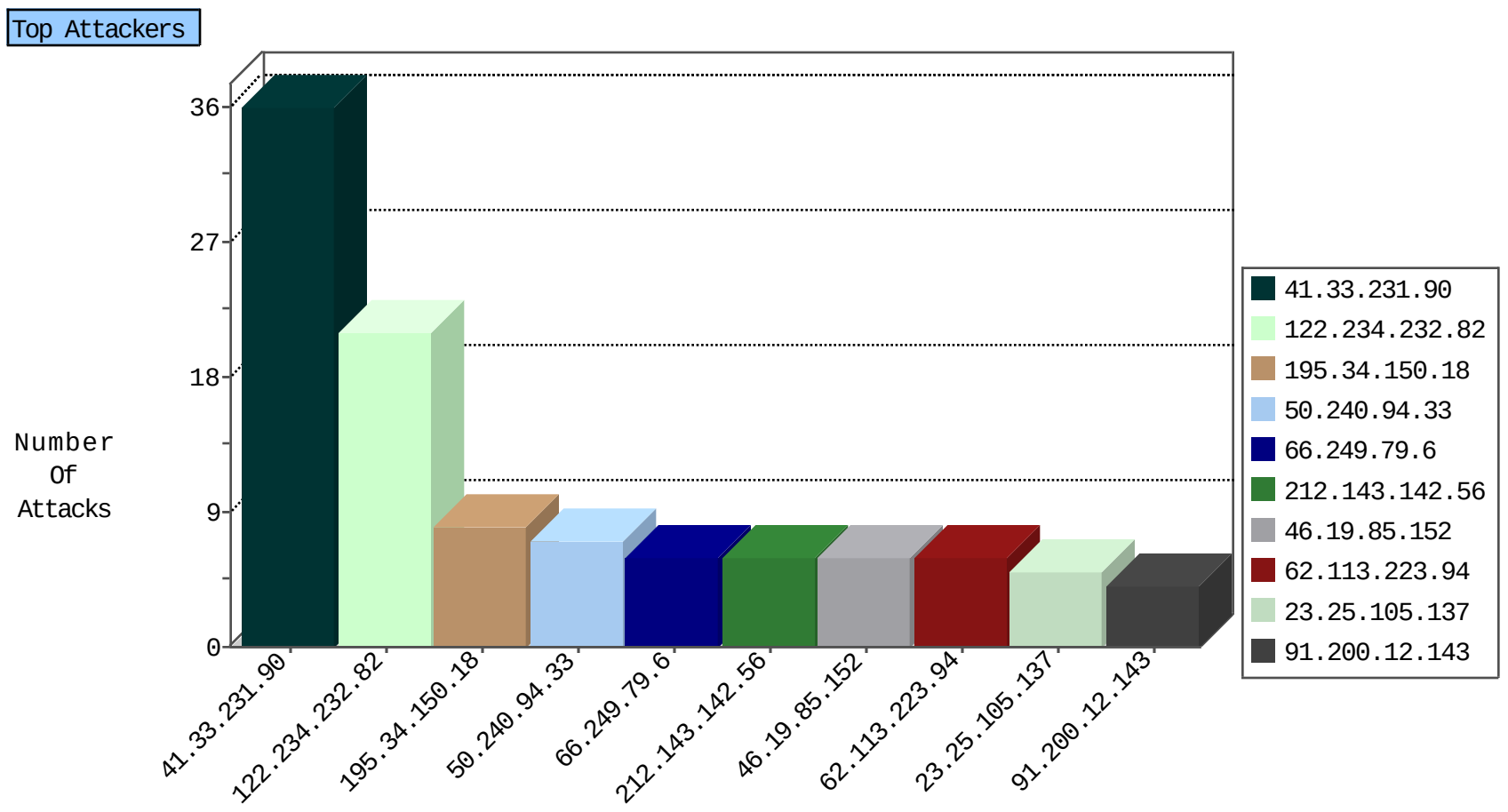
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

01-09-2016-02:04:04 to 01-09-2016-03:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.240.236.119	United States	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
80.82.64.177	Netherlands	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
89.248.174.4	Netherlands	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1

01-09-2016-02:04:04 to 01-09-2016-03:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-09-2016-02:04:04 to 01-09-2016-03:04:04

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
122.234.232.82	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	2
122.234.232.82	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	2
122.234.232.82	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
122.234.232.82	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
189.254.90.133	147.237.8.46	Mexico	e.chinuch.idf.il	ET SCAN NMAP -sS window 3072	1
122.234.232.82	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
189.254.90.133	147.237.8.46	Mexico	e.chinuch.idf.il	ET SCAN NMAP -f -sS	1
122.234.232.82	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1
122.234.232.82	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1
122.234.232.82	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
122.234.232.82	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.203	147.237.76.197	Netherlands	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
122.234.232.82	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
61.182.170.38	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
122.234.232.82	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	1
122.234.232.82	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
122.234.232.82	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
189.254.90.133	147.237.8.46	Mexico	e.chinuch.idf.il	ET SCAN NMAP -sS window 2048	1
122.234.232.82	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
122.234.232.82	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
122.234.232.82	147.237.77.233	China	atal.idf.il	ET SCAN Potential SSH Scan	1
122.234.232.82	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
122.234.232.82	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential SSH Scan	1
61.182.170.38	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
122.234.232.82	147.237.77.74	China	law.idf.il	ET SCAN Potential SSH Scan	1
61.182.170.38	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1

01-09-2016-02:04:04 to 01-09-2016-03:04:04

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
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.79.6	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
134.191.232.94	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.189	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
50.240.94.33	United States	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.152	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.85.152	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.183.16.85	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
50.240.94.33	United States	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
91.200.12.143	Ukraine	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	2
31.210.188.60	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
157.55.39.2	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
185.3.144.22	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
217.132.42.204	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
91.200.12.143	Ukraine	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
23.25.105.137	United States	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
62.113.223.94	Germany	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.206	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.85.141	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
27.46.137.20	China	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
208.115.113.89	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
176.13.15.61	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.157	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
128.61.240.118	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
2.54.24.248	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
81.44.224.176	Spain	147.237.76.147	chinuch.aka.idf.il	drop	SAM rule	drop	1
62.113.223.94	Germany	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.207	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.144	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
93.174.93.203	Netherlands	147.237.0.16	my-kosher-kravi.idf.il	drop	SAM rule	drop	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
74.94.211.209	United States	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
178.32.53.94	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
60.234.101.54	New Zealand	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.159	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.51	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
128.61.240.118	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.39.93.143	France	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
81.44.224.176	Spain	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	1
195.154.146.225	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
62.113.223.94	Germany	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.147	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.46.39.194	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
94.102.51.30	Netherlands	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	1
74.94.211.209	United States	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
62.113.223.94	Germany	147.237.0.33	idf.il	drop		drop	1
141.212.122.198	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
128.61.240.118	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

01-09-2016-02:04:04 to 01-09-2016-03:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
208.115.113.88	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on navy.idf.il/giyus/forum/asp/showforum.asp	Block	3
176.13.1.214	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
94.230.85.81	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
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	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
94.223.91.240	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
207.46.13.157	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/w/load.php	Block	1
66.249.65.51	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/templates/general/general.aspx	Block	1
192.243.55.137	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=58564&docid=35722	Block	1
2.52.53.78	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.140.228	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
77.40.129.123	Norway	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
46.166.137.217	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
185.104.120.4		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
150.70.173.10	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.69.38	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1877	Block	1
192.243.55.137	Dominica	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 192.243.55.137	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-16744-ar/mmmmmmm=5d8b9a65mmmmmmm_5d8b9a65	Block	1
23.25.105.137	United States	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 23.25.105.137	Block	1
141.212.122.145	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/	Block	1
207.46.13.75	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.75	Block	1
77.40.129.123	Norway	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
46.166.186.204	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
188.143.232.21	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
157.55.39.2	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
95.175.97.229	Finland	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	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
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/movies/yassin2.wmv http:/apexvid.com/t8p746bln3qp	Block	1
66.249.69.46	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.69.46	Block	1
183.79.221.25	Japan	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
23.25.105.137	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/gen204	Block	1
150.70.97.84	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
207.46.13.75	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-12085-he/captcha/captcha_image.asp	Block	1
88.75.184.195	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
46.166.186.209	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
188.143.232.21	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
157.55.39.2	United States	147.237.72.166	aka.idf.il	Unknown Parameter KEY in www.aka.idf.il/ishurim/cityofficers/	None	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
195.154.226.90	France	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 195.154.226.90	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
184.168.200.150	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
46.19.85.215	Israel	147.237.76.42	refuah.idf.il	Illegal HTTP Version	Block	1
150.70.97.84	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
207.46.13.157	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
94.191.186.77	Denmark	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
50.240.94.33	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
192.243.55.134	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/eitan/pratim/pirteytkufa	Block	1
157.55.39.245	United States	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to kosher-kravi.idf.il/templates/general/	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

01-09-2016-02:04:04 to 01-09-2016-03:04:04