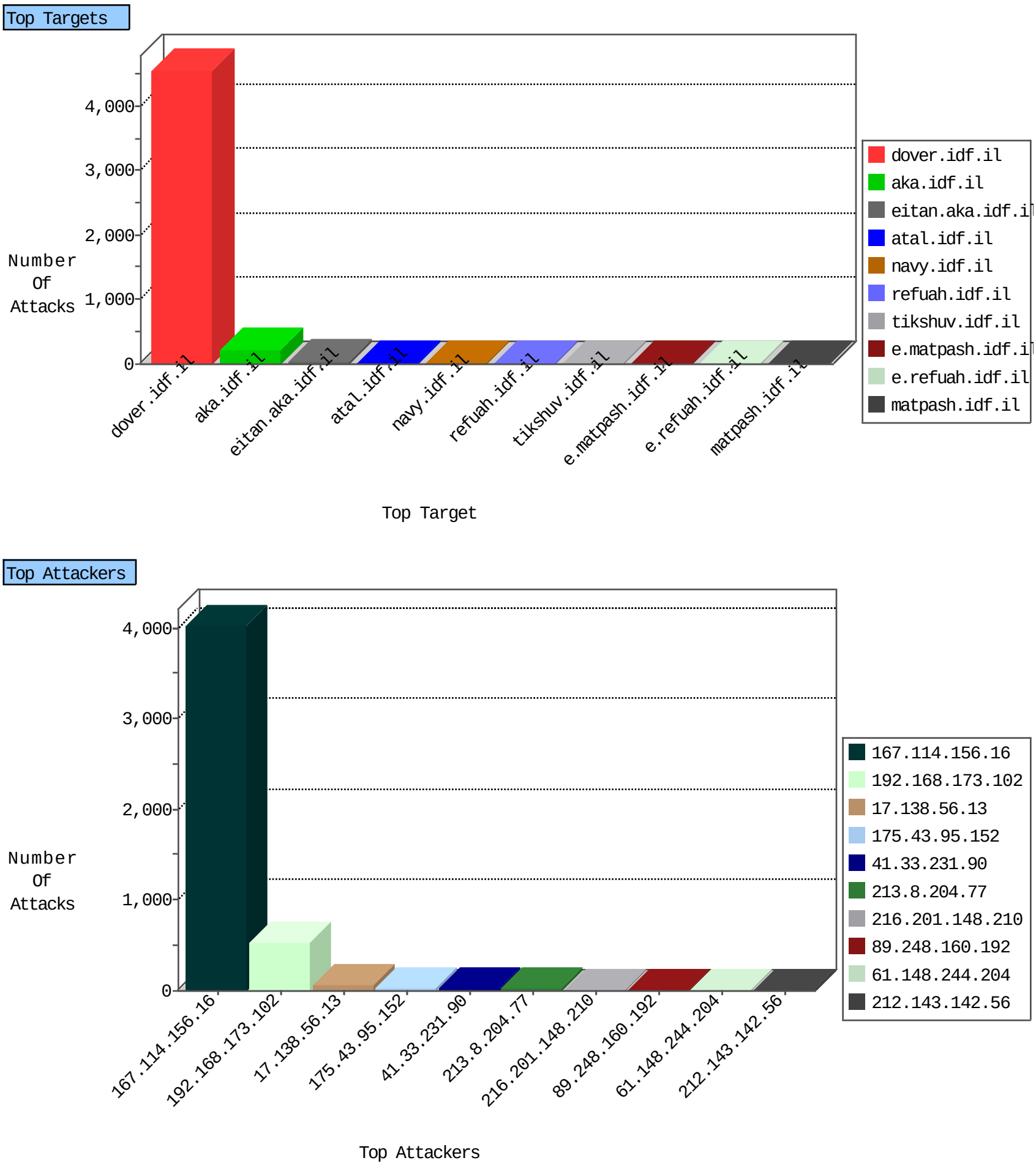
04-09-2016-07:04:05 to 04-09-2016-08:04:05

IDF Under Attack Daily Report



04-09-2016-07:04:05 to 04-09-2016-08:04:05

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	4021
123.59.59.52	China	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	4
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
209.126.127.17	United States	147.237.8.45	e.eitan.idf.il	Block_Udp_All_Nets	drop	2
209.126.127.17	United States	147.237.8.14	e.orchot.idf.il	Block_Udp_All_Nets	drop	2
209.126.127.17	United States	147.237.8.28	e.mobile-ks.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.120	United States	147.237.77.19	law-forum.idf.il	Block_Ntp_All_Net	drop	1
123.151.42.61	China	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Udp_All_Nets_Con_Limit	drop	1
209.126.127.17	United States	147.237.8.27	e.madim.atal.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.67	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Udp_All_Nets	drop	1

04-09-2016-07:04:05 to 04-09-2016-08:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
216.201.148.210	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	8
106.38.241.149	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
62.210.143.245	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
66.249.66.59	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.66.56	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

04-09-2016-07:04:05 to 04-09-2016-08:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
216.201.148.210	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	10
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
89.248.160.192	147.237.8.28	Netherlands	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
141.101.178.137	147.237.76.44	Russian Federation	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.72.156	Netherlands	aman.idf.il	ET SCAN NMAP -sS window 1024	1
122.52.139.2	147.237.76.42	Philippines	refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
23.102.168.255	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 2048	1
89.248.160.192	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
89.248.160.192	147.237.76.198	Netherlands	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
89.248.160.192	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN Potential SSH Scan	1
89.248.160.192	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
89.248.160.192	147.237.76.30	Netherlands	himush.idf.il	ET SCAN Potential SSH Scan	1
208.100.26.228	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.160.192	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
141.101.178.137	147.237.76.147	Russian Federation	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.79.104	147.237.77.176	Netherlands	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
141.101.178.137	147.237.76.39	Russian Federation	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
23.102.168.255	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 4096	1
89.248.160.192	147.237.77.179	Netherlands	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
23.102.168.255	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -f -sS	1
89.248.160.192	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN Potential SSH Scan	1
89.248.160.192	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
89.248.160.192	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
89.248.160.192	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN Potential SSH Scan	1
89.248.160.192	147.237.72.14	Netherlands	dover.idf.il(old)	ET SCAN Potential SSH Scan	1

04-09-2016-07:04:05 to 04-09-2016-08:04:05

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	327
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	197
17.138.56.13	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	56
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
213.8.204.77	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
61.148.244.204	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
87.71.52.126	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.211.228.121	Qatar	147.237.77.216	dover.idf.il	drop	SAM rule	drop	5
5.22.129.103	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
66.249.66.59	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.28.175.186	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.178.6.63	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
146.88.40.124	Thailand	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
66.249.64.163	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
157.55.39.241	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
85.65.134.251	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
62.128.45.194	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
2.53.57.134	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
98.207.17.78	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
5.22.129.95	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
98.220.216.178	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
84.109.28.234	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
157.55.12.92	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
123.59.59.68	China	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
85.93.91.84	Germany	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	1
141.101.178.137	Russian Federation	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
106.184.3.122	Japan	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
85.65.134.251	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
52.68.136.185	Japan	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.101.178.137	Russian Federation	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
87.69.19.217	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.217	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
106.186.113.132	Japan	147.237.76.34	yohalan.idf.il	drop		drop	1
184.105.247.199	United States	147.237.8.46	e.chinuch.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.101.178.137	Russian Federation	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.14	United States	147.237.0.33	idf.il	drop		drop	1
141.212.122.218	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
106.186.113.132	Japan	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
85.65.134.251	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.101.178.137	Russian Federation	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.100	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
123.59.59.64	China	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
85.65.134.251	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
66.240.213.93	United States	147.237.77.170	maarachot.idf.il	Scanner Enforcement Violation	Masscan Port Scanner	reject	1
141.101.178.137	Russian Federation	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

04-09-2016-07:04:05 to 04-09-2016-08:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
175.43.95.152	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 175.43.95.152	Block	29
175.43.95.152	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	6
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	6
185.89.217.234	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
185.89.217.227	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
185.89.217.224	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
185.89.217.228	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
123.59.59.52	China	147.237.76.200	eitan.aka.idf.i	Unauthorized URL Access to www.qyer.com/894-he/eitan.aspx	Block	1
66.249.66.26	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
208.115.125.36	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	1
175.43.95.152	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-9703-en/contact.php	Block	1
66.249.75.52	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
45.243.98.11	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
185.89.217.231	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
157.55.39.205	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/&q=الاسرائيلي &sa=x&ei=oed5t-rlm4-r-gbqp8hkbg&ved=0cc0qfjag	Block	1
66.249.66.53	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
178.162.45.2	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1044-he/ishurim.aspx	Block	1
85.93.91.84	Germany	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/robots.txt	Block	1
45.243.98.11	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
185.89.217.232	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
157.55.39.241	United States	147.237.72.166	aka.idf.il	Unknown Parameter sorderby in aka.idf.il/iturim/asp/displayallsoldiers.asp	None	1
66.249.69.10	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1
109.67.11.48	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.64.101	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
66.249.69.34	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/yohalan/home/home.asphttps:/www.aka.idf.il/yohalan/home/home.asp	Block	1
5.22.129.103	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
114.97.56.215	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/896-he/idfg.aspx/trackback/	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/french/nahal.stm.	Block	1
66.249.75.44	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
38.111.147.88	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1

04-09-2016-07:04:05 to 04-09-2016-08:04:05