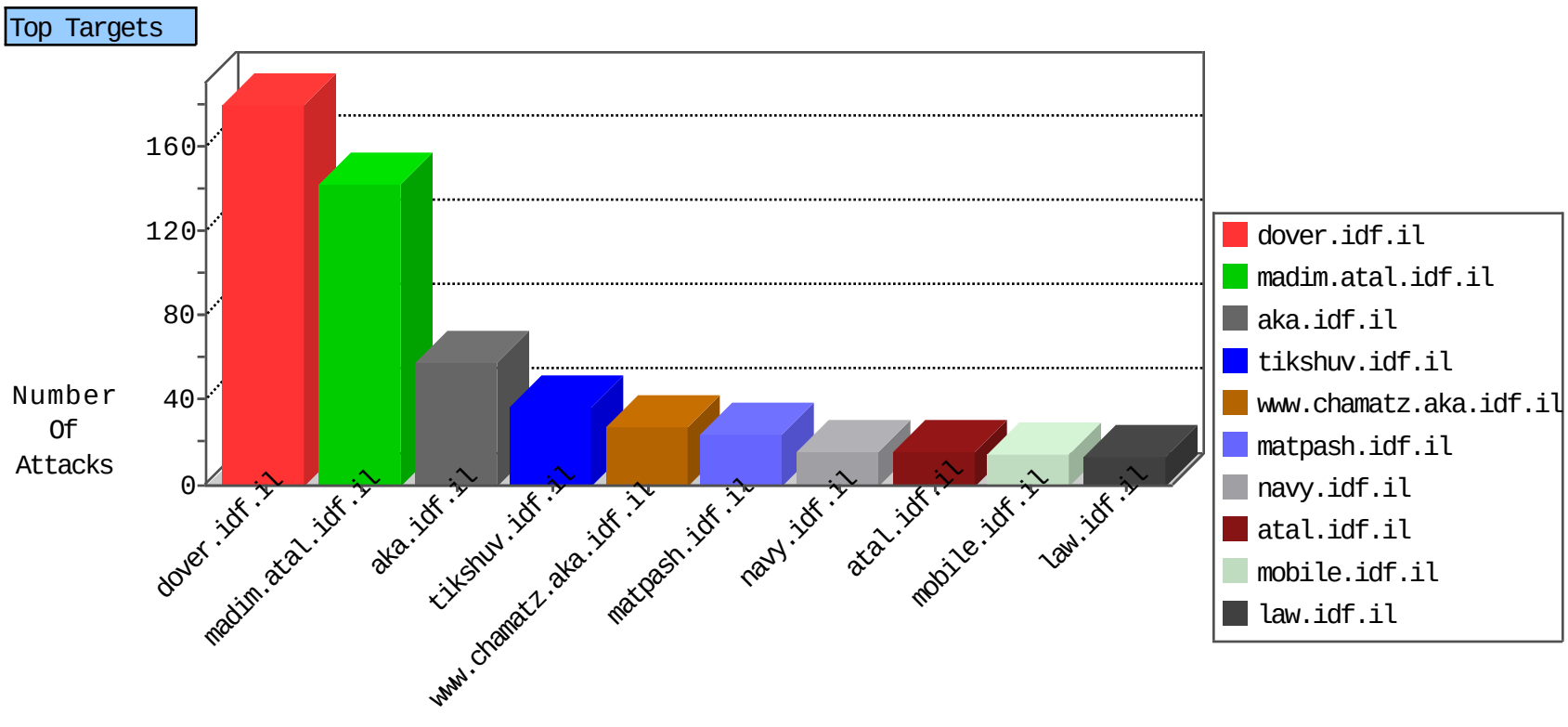
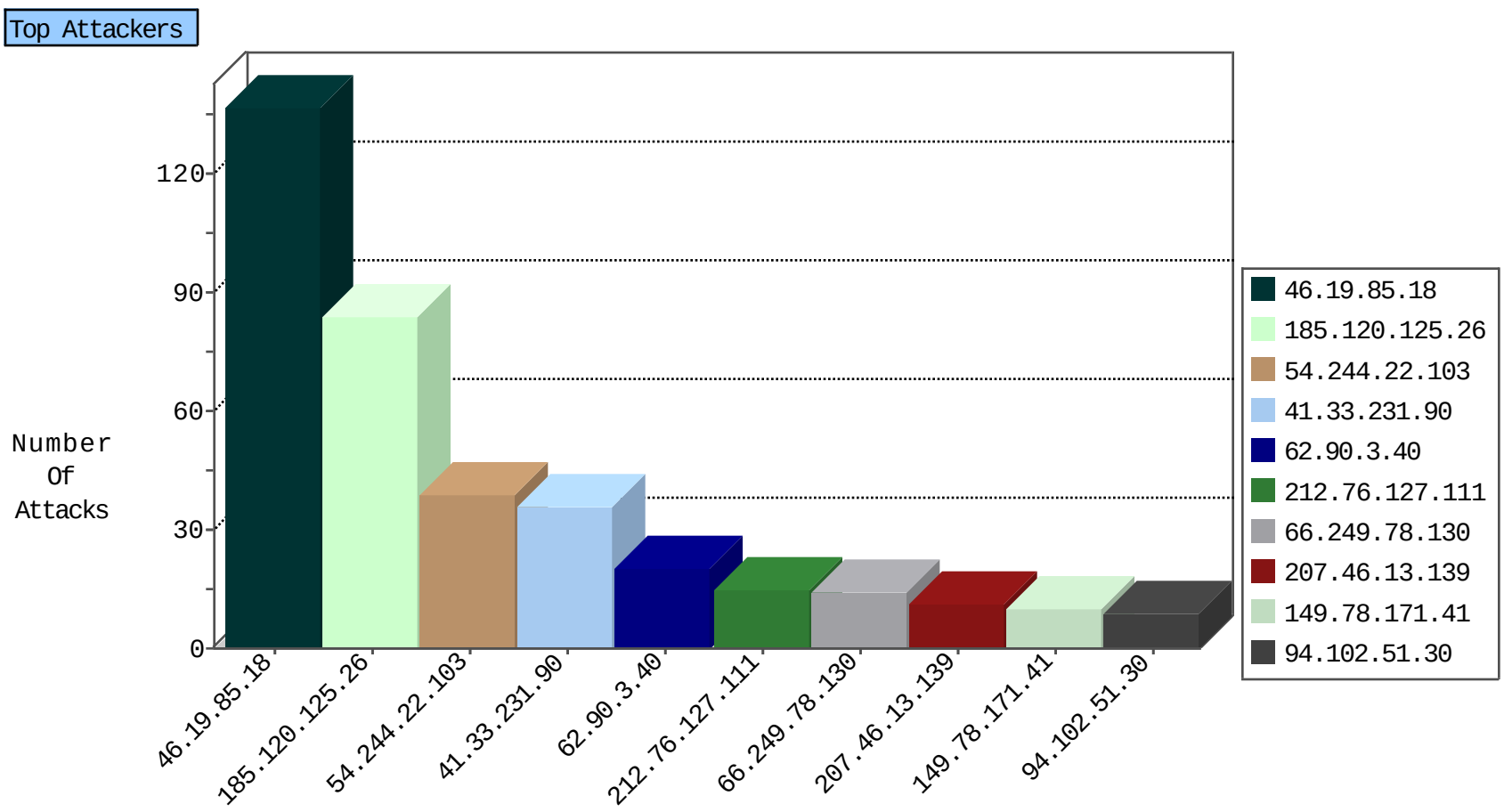
02-08-2016-01:07:32 to 02-08-2016-02:07:32

IDF Under Attack Daily Report





02-08-2016-01:07:32 to 02-08-2016-02:07:32

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.64.133	Israel	147.237.77.234	halag.idf.il	TCP handshake violation, first packet not syn	drop	6450
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	4
203.166.137.11	Singapore	147.237.77.74	law.idf.il	Invalid TCP Flags	drop	1
203.166.137.11	Singapore	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
185.130.5.201		147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1

02-08-2016-01:07:32 to 02-08-2016-02:07:32

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
198.20.69.74	United States	147.237.8.46	e.chinuch.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

02-08-2016-01:07:32 to 02-08-2016-02:07:32

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
185.130.5.165	147.237.76.200		eitan.aka.idf.il	ET SCAN Potential SSH Scan	2
185.130.5.165	147.237.72.166		aka.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.165	147.237.8.24		e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
125.212.232.144	147.237.76.176	Vietnam	test.ncore.idf.il	ET SCAN NMAP -sS window 2048	1
125.212.232.144	147.237.76.176	Vietnam	test.ncore.idf.il	ET SCAN NMAP -f -sS	1
125.212.232.144	147.237.0.35	Vietnam	akaws.idf.il	ET SCAN NMAP -sS window 3072	1
218.246.0.97	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
81.183.168.243	147.237.77.233	Hungary	atal.idf.il	ET SCAN NMAP -sS window 1024	1
192.241.253.62	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.165	147.237.77.74		law.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.165	147.237.72.217		e.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.165	147.237.8.28		e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
179.43.141.234	147.237.0.17	Switzerland	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
125.212.232.144	147.237.76.176	Vietnam	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
125.212.232.144	147.237.0.35	Vietnam	akaws.idf.il	ET SCAN NMAP -sS window 4096	1
218.246.0.97	147.237.76.198	China	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
88.249.106.23	147.237.76.196	Turkey	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
46.45.137.67	147.237.8.45	Turkey	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
192.241.253.62	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 1024	1

02-08-2016-01:07:32 to 02-08-2016-02:07:32

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
185.120.125.26		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	56
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	32
185.120.125.26		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	28
212.76.127.111	Israel	147.237.77.226	www.chamatz.aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	15
66.249.78.130	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
207.46.13.139	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	11
149.78.171.41	Israel	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	10
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
212.76.127.44	Israel	147.237.77.226	www.chamatz.aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
24.148.13.209	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
66.249.78.223	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	6
109.65.166.55	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.43.126.31	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
66.249.78.177	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
62.90.3.40	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
107.107.62.157	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
62.90.3.40	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
2.54.168.59	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.40.33	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.183.168.243	Hungary	147.237.77.233	atal.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
46.19.86.226	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
208.52.154.240	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
62.90.3.40	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	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
37.26.148.252	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.90.3.40	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
209.140.43.126	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
185.32.179.213	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
62.90.3.40	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
66.249.78.170	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
62.90.3.40	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
136.243.67.234	Germany	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
66.249.66.90	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
177.240.111.115	Mexico	147.237.0.33	idf.il	drop		drop	2
5.189.165.244	Germany	147.237.0.33	idf.il	drop		drop	2
66.249.66.182	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	2
177.240.111.115	Mexico	147.237.0.35	akaws.idf.il	drop		drop	2
5.189.165.244	Germany	147.237.77.216	dover.idf.il	Block HTTP Non Compliant		monitor	2
66.249.66.186	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	2
5.189.165.244	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
54.158.6.83	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
95.180.14.182		147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.216	United States	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
45.63.97.227		147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
94.102.51.30	Netherlands	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
23.20.210.230	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	84
46.19.85.18	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.18	Block	53
219.94.128.197	Japan	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 219.94.128.197	Block	5
79.182.96.209	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/7/112297.pdf	Block	1
46.19.85.253	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
5.29.154.92	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$61 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
177.240.111.115	Mexico	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
109.65.166.55	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.78.80	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	1
219.94.128.197	Japan	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
41.238.122.164	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
146.185.234.48	Russian Federation	147.237.76.42	refuah.idf.il	Parameter Type Violation searchText in www.refua.atal.idf.il/994-he/refuah.aspx	Block	1
81.183.168.243	Hungary	147.237.77.233	atal.idf.il	Abnormally Long Request request version	Block	1
46.19.85.253	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1
5.189.165.244	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
177.240.111.115	Mexico	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
141.212.122.81	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to /x	Block	1
66.249.78.223	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
146.185.234.48	Russian Federation	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/news/news.in.aspx/templates/sendtofriend/sendtofriend.aspx	Block	1
81.183.168.243	Hungary	147.237.77.233	atal.idf.il	Illegal HTTP Version the green fields outside. Watch the goats chewing the grass. What is the meaning of life? Life isn't about getting to the end. Goats know this. You should know too. Goats are wise. Goats are cute. Listen to them! This is the message. Love goats, love the Internet! ðŸ?? Kecske. HTTP/1.0	Block	1
46.19.85.253	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method nd/SendToFriend.aspx?&l=he&f=894 in URL	Block	1
37.142.136.37	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
180.76.15.158	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
141.212.122.81	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to /x	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9736-he/refuah.aspx	Block	1
157.55.39.48	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/size220x0/sip_storage	Block	1
81.183.168.243	Hungary	147.237.77.233	atal.idf.il	Malformed URL towards	Block	1
62.90.3.40	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
208.52.154.240	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to /pma/scripts/setup.php	Block	1
41.225.222.199	Tunisia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/ping-t=admin.1.2.3.4.5.6.7.8.9=pasword	Block	1
141.212.122.81	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to /x	Block	1
68.180.230.244	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
46.19.85.152	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
177.240.111.115	Mexico	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
104.131.127.187	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to www.m.my-kosher-kravi.idf.il/	Block	1
66.249.66.142	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/favicon.ico	Block	1
41.238.122.164	Egypt	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
146.185.234.48	Russian Federation	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 146.185.234.48	Block	1

02-08-2016-01:07:32 to 02-08-2016-02:07:32