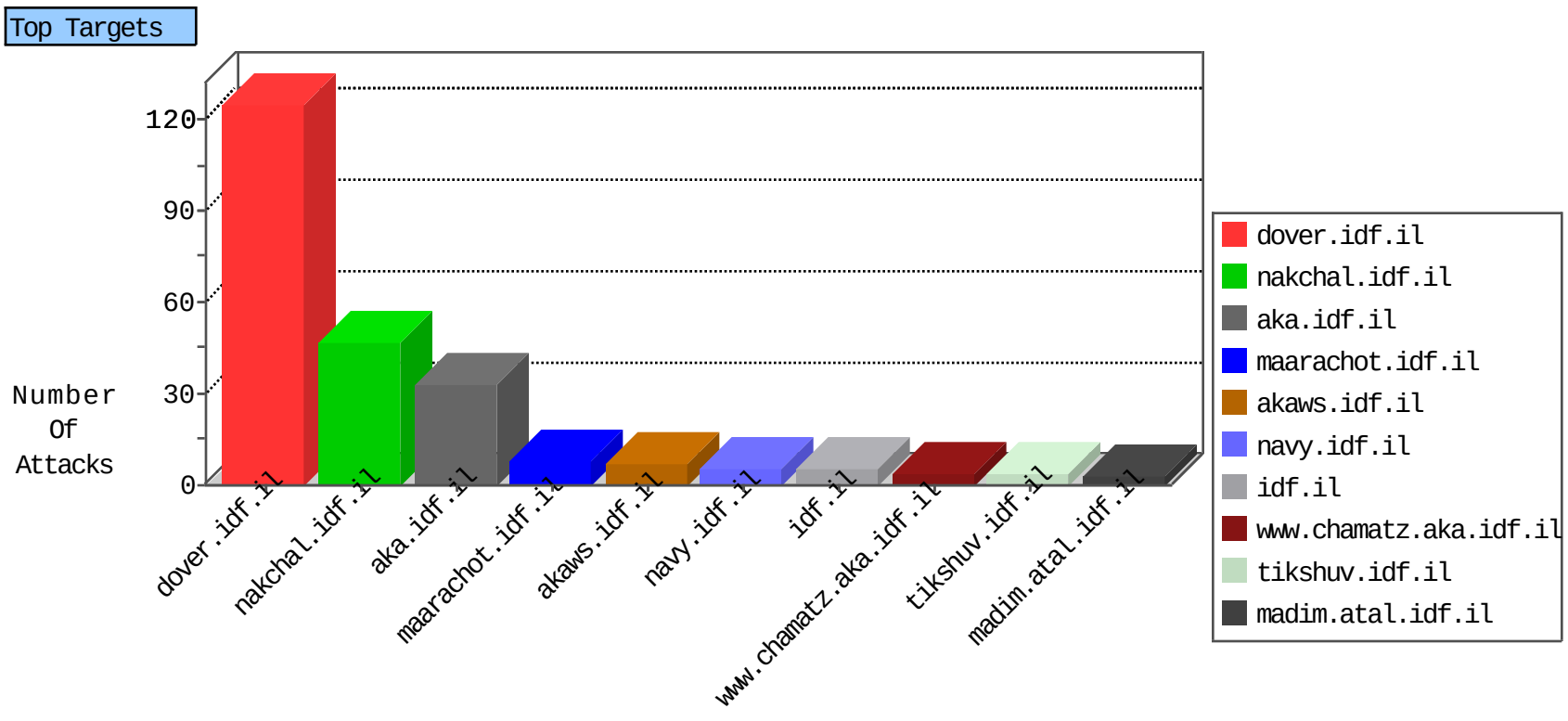
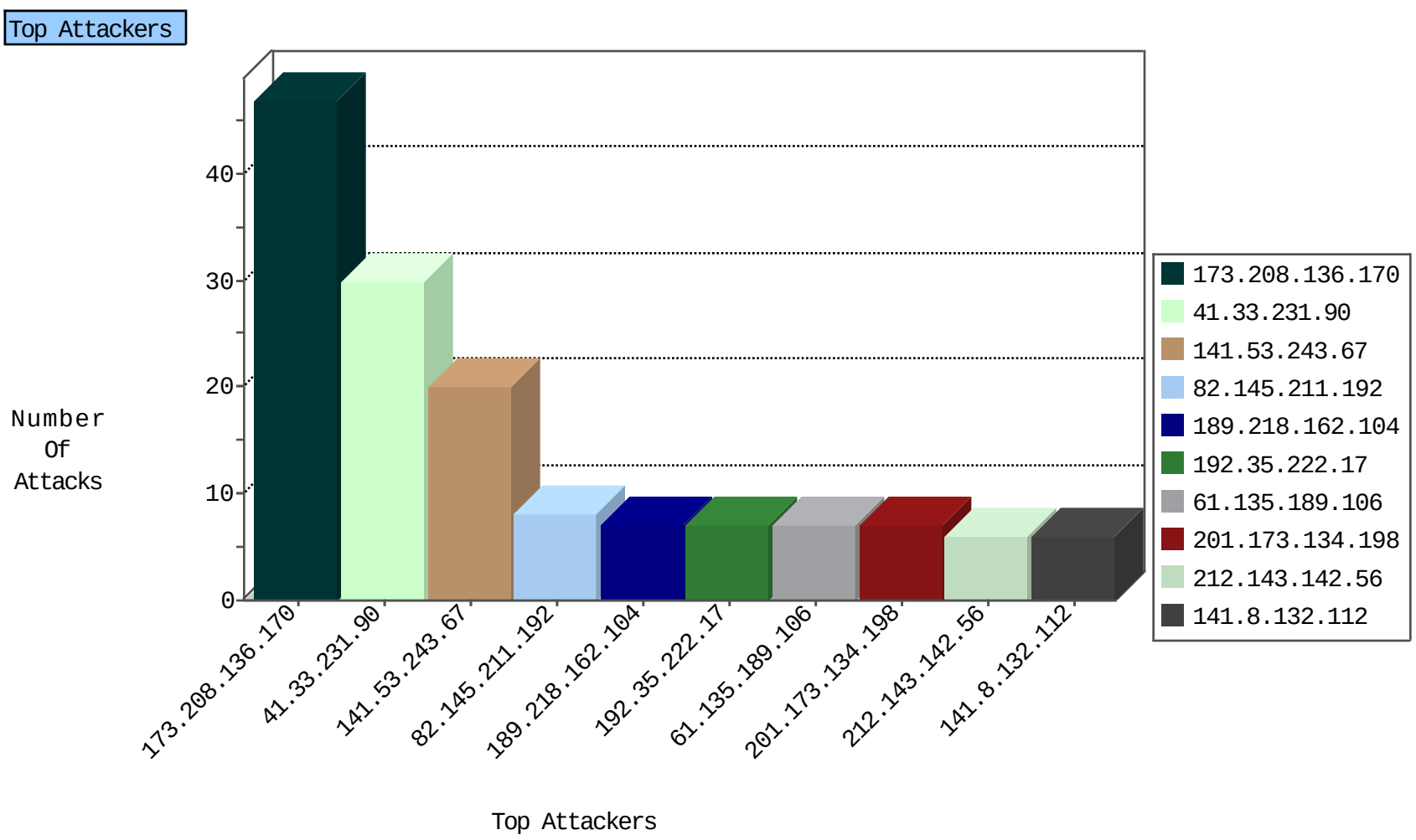
03-04-2016-01:12:13 to 03-04-2016-02:12:13

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-04-2016-01:12:13 to 03-04-2016-02:12:13

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.145.211.192	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	8
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
109.253.143.214	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
46.116.114.154	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
179.43.144.33	Switzerland	147.237.77.227	e.hamaz.idf.il	Block_Ntp_All_Net	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
114.99.179.11	China	147.237.0.16	my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
31.170.164.244	United Kingdom	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.196		147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
162.216.114.158	United States	147.237.8.27	e.madim.atal.idf.il	Block_Udp_All_Nets	drop	1
46.17.40.227	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
162.216.114.158	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

03-04-2016-01:12:13 to 03-04-2016-02:12:13

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
61.135.189.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
91.121.169.194	France	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
157.55.39.179	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
207.46.13.96	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

03-04-2016-01:12:13 to 03-04-2016-02:12:13

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
192.35.222.17	147.237.77.216	United States	dover.idf.il	ET DOS SSL Bomb DoS Attempt	5
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
61.240.144.65	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
202.71.25.29	147.237.76.44	India	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
196.203.83.25	147.237.77.226	Tunisia	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
185.72.179.221	147.237.0.16		my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
185.56.82.54	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
119.188.4.9	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
61.240.144.65	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
202.71.25.29	147.237.76.44	India	e.refuah.idf.il	ET SCAN NMAP -sS window 4096	1
196.203.83.25	147.237.77.226	Tunisia	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 3072	1
185.72.179.221	147.237.0.35		akaws.idf.il	ET SCAN NMAP -sS window 1024	1
185.56.82.54	147.237.0.33	Netherlands	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
119.188.4.9	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
119.188.4.9	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential VNC Scan 5800-5820	1

03-04-2016-01:12:13 to 03-04-2016-02:12:13

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	30
141.53.243.67	Germany	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
91.200.12.106	Ukraine	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	4
91.200.12.136	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
93.146.44.155	Italy	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.19.229	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.51.91	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
61.135.189.106	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
46.19.85.207	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.35.222.17	United States	147.237.77.216	dover.idf.il	SSL Enforcement Violation	TLS Servers Cipher Suites Vulnerability Scanning Tools	reject	2
91.200.12.7	Ukraine	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	2
201.173.134.198	Mexico	147.237.0.33	idf.il	drop		drop	2
201.173.134.198	Mexico	147.237.0.35	akaws.idf.il	drop		drop	2
189.218.162.104	Mexico	147.237.0.33	idf.il	drop		drop	2
157.55.39.58	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
91.200.12.141	Ukraine	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	2
189.218.162.104	Mexico	147.237.0.35	akaws.idf.il	drop		drop	2
89.139.231.238	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
198.20.70.114	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.121.77.17	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
172.56.39.194	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.142.64.75	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.78	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
70.193.103.90	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.116.114.154	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.199	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
50.141.76.0	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
185.106.94.49		147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.113	United States	147.237.0.35	akaws.idf.il	drop		drop	1
109.64.32.75	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
75.40.20.134	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
192.115.177.203	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.116.114.154	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.200	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
8.37.227.70	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
141.212.122.69	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
50.141.76.0	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
188.32.55.220	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.188	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.114	United States	147.237.0.35	akaws.idf.il	drop		drop	1
109.253.143.214	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
195.60.232.57	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.116.234.159	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
146.185.239.102	Russian Federation	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
24.114.84.200	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.70	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.121	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
123.126.113.80	China	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

03-04-2016-01:12:13 to 03-04-2016-02:12:13

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
173.208.136.170	United States	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 173.208.136.170	Block	38
173.208.136.170	United States	147.237.76.31	nakchal.idf.il	Multiple Admin Blocking from 173.208.136.170	Block	7
131.253.25.152	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
189.218.162.104	Mexico	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
23.81.70.3	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/shared/usercontrols/headerupper/	Block	1
201.173.134.198	Mexico	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on /tmunblock.cgi	Block	1
91.109.30.95	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	1
189.218.162.104	Mexico	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
157.55.39.41	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
37.142.64.99	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
212.182.119.147	Poland	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
173.208.136.170	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/admin/asset/assetmanager/assetmanager.asp	Block	1
95.0.35.167	Turkey	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	1
189.218.162.104	Mexico	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
168.235.206.230	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
37.236.8.16	Iraq	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/navmenu/kkkkkkk=cd07baa9kkkkkkk_cd07baa9	Block	1
109.64.10.40	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	1
201.173.134.198	Mexico	147.237.0.15	kosher-kravi.idf.il	Distributed Unauthorized URL Access on /tmunblock.cgi	Block	1
173.208.136.170	United States	147.237.76.31	nakchal.idf.il	Admin Blocking	Block	1
66.249.64.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
185.13.112.60	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1044-he/ishurim.aspx	Block	1
130.49.75.73	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.png	Block	1
201.173.134.198	Mexico	147.237.0.19	madim.atal.idf.il	Distributed Unauthorized URL Access on /tmunblock.cgi	Block	1
66.249.66.60	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1

03-04-2016-01:12:13 to 03-04-2016-02:12:13