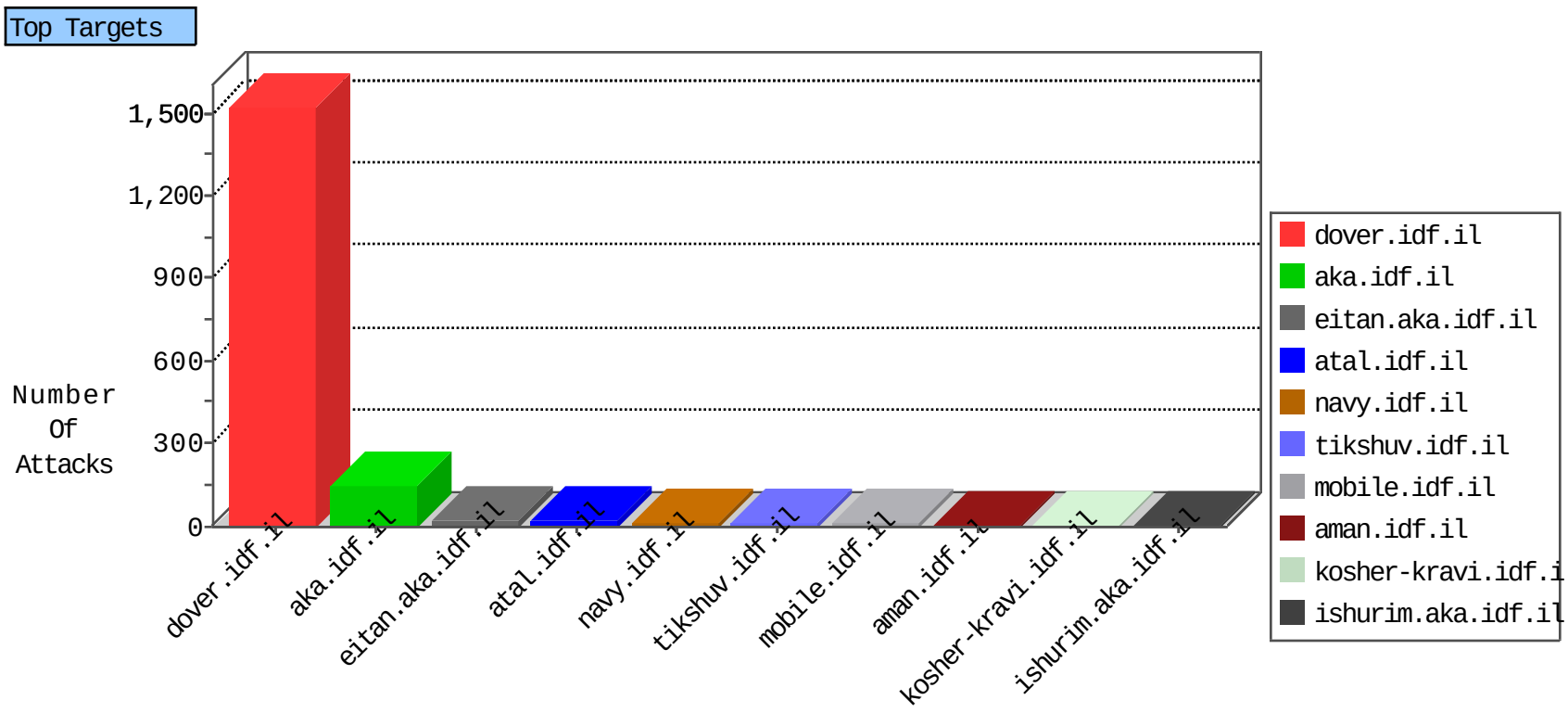
05-02-2016-01:06:41 to 05-02-2016-02:06:41

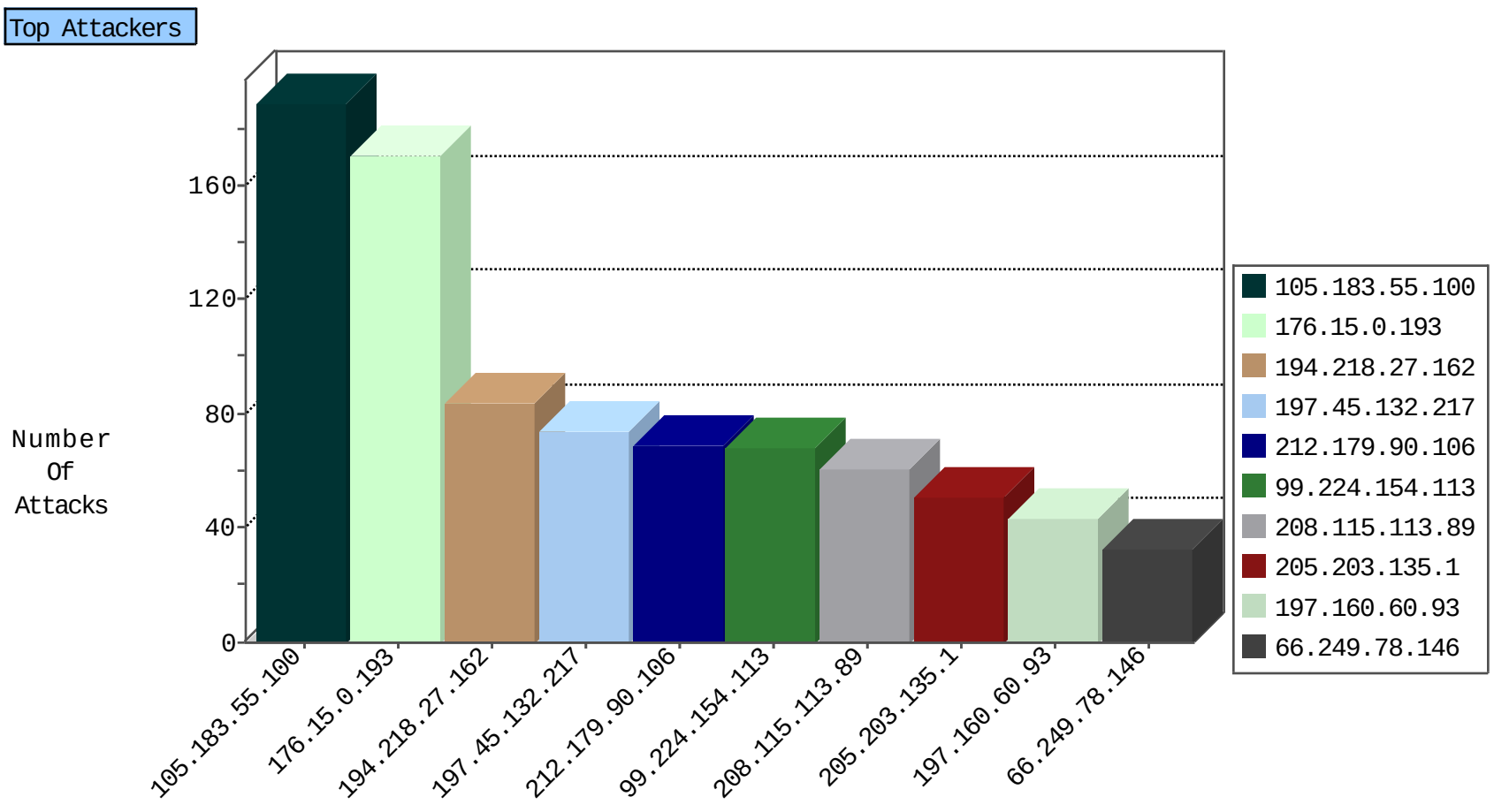
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

05-02-2016-01:06:41 to 05-02-2016-02:06:41

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
197.160.73.40	Egypt	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	14
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
71.6.135.131	United States	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
94.102.52.10	Netherlands	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
71.6.165.200	United States	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
112.169.100.157	Korea, Republic of	147.237.76.202	e.halag.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
217.112.96.194	Italy	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
89.46.102.242	Romania	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
141.212.122.206	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
94.102.52.10	Netherlands	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1

05-02-2016-01:06:41 to 05-02-2016-02:06:41

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.210.226.9	France	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
197.160.73.40	Egypt	147.237.77.216	dover.idf.i	12026: HTTP: LOIC DDoS Tool (ONLY enable when under DoS attack)	Block	2

05-02-2016-01:06:41 to 05-02-2016-02:06:41

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
62.210.226.9	147.237.77.233	France	atal.idf.il	SQL Injection - Select From	12
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
195.154.54.169	147.237.76.44	France	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
81.80.189.107	147.237.76.197	France	e.himush.idf.il	ET SCAN NMAP -f -sS	1
183.60.48.25	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.211	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
173.218.197.121	147.237.76.31	United States	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
58.218.204.211	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
119.10.114.32	147.237.72.14	China	dover.idf.il(old)	ET SCAN NMAP -sS window 2048	1
46.228.207.18	147.237.76.200	Germany	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
112.169.100.157	147.237.76.200	Korea, Republic of	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
46.228.207.18	147.237.76.39	Germany	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.197.72.206	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
46.228.207.18	147.237.76.31	Germany	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.201.236.158	147.237.77.61	Ukraine	e.cogat.idf.il	ET SCAN NMAP -f -sS	1
222.186.42.248	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
88.249.106.23	147.237.76.201	Turkey	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.42.248	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
81.80.189.107	147.237.76.197	France	e.himush.idf.il	ET SCAN NMAP -sS window 2048	1
183.60.48.25	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.211	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
139.217.27.204	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
46.228.207.18	147.237.77.216	Germany	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
119.10.114.32	147.237.72.14	China	dover.idf.il(old)	ET SCAN NMAP -f -sS	1
46.228.207.18	147.237.76.199	Germany	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
112.169.100.157	147.237.76.86	Korea, Republic of	navy.idf.il	ET SCAN Potential SSH Scan	1
46.228.207.18	147.237.76.38	Germany	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.201.236.158	147.237.77.61	Ukraine	e.cogat.idf.il	ET SCAN NMAP -sS window 2048	1
46.228.207.18	147.237.76.30	Germany	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
222.186.42.248	147.237.76.42	China	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.201.236.158	147.237.77.61	Ukraine	e.cogat.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
222.186.42.248	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
81.80.189.107	147.237.76.197	France	e.himush.idf.il	ET SCAN NMAP -sS window 3072	1

05-02-2016-01:06:41 to 05-02-2016-02:06:41

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
105.183.55.100	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	189
176.15.0.193	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	171
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	74
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	69
99.224.154.113	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	56
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
197.160.60.93	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	28
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
157.55.39.53	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
198.58.103.92	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
207.46.13.22	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
66.249.93.111	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
66.249.93.119	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
198.58.102.158	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
66.249.93.115	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
192.115.61.75	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.115	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
144.76.30.236	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
54.189.199.157	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
87.203.102.200	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
149.202.98.160	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
173.55.114.156	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
128.242.249.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
85.65.105.227	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
98.177.199.154	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.0.86.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
45.55.61.39	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
41.40.233.169	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
41.40.197.76	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
81.132.124.61	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
41.40.130.88	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.55.21.163	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

05-02-2016-01:06:41 to 05-02-2016-02:06:41

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.65.105.227	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
79.182.47.171	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	3
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
17.142.156.171	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/apple-app-site-association	Block	1
207.46.13.178	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-12847-he/dover.aspx„'"•'¡'ƒ¯„,¬¿„,½	Block	1
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-he/cogat.aspx	Block	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
82.80.230.228	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
54.185.204.250	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1398-en/dover.aspx	Block	1
212.179.21.194	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/div.item	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/	Block	1
190.234.106.56	Peru	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
77.58.27.167	Switzerland	147.237.77.74	law.idf.il	PHP Attempt	Block	1
207.46.13.22	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-15858-he/dover.aspx„'ƒ¯„,¬¿„,½„'§'₪'ƒ¯„,¬¿„,½	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/default.aspx	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/0/71550.pdf	Block	1
119.127.241.250	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
77.58.27.167	Switzerland	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/wp-login.php	Block	1
207.46.13.178	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.178	Block	1
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1
148.102.19.181	Peru	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1

05-02-2016-01:06:41 to 05-02-2016-02:06:41