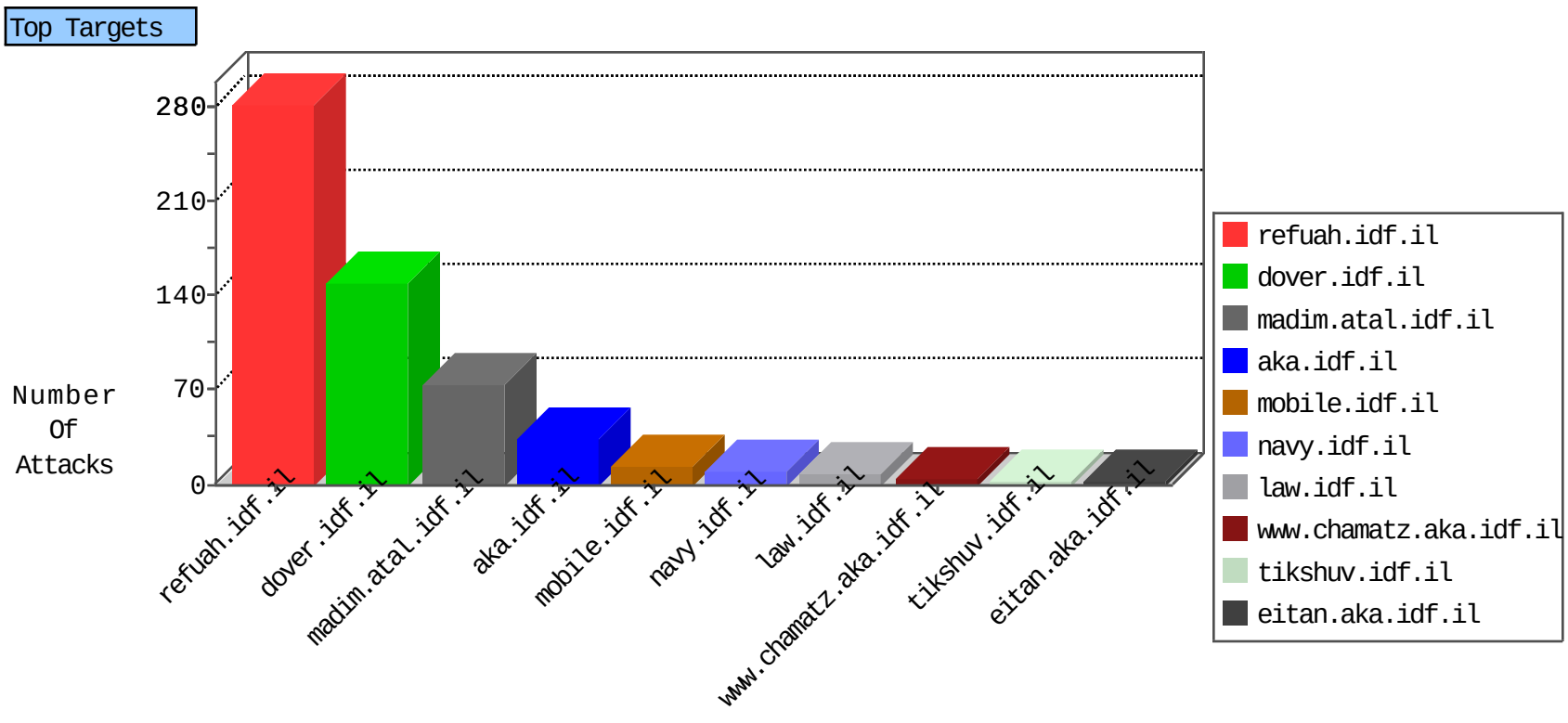
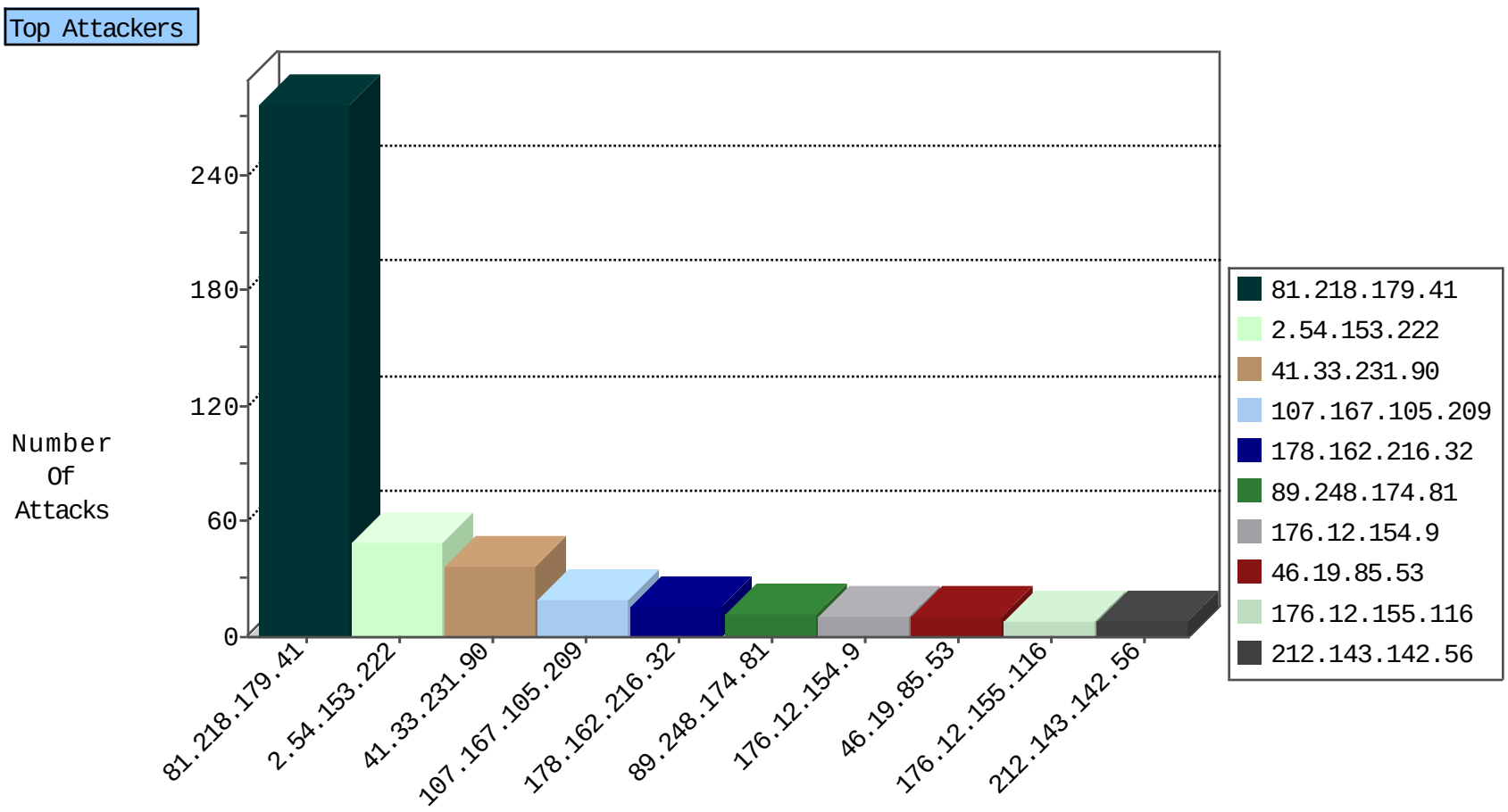
02-03-2016-01:06:57 to 02-03-2016-02:06:57

IDF Under Attack Daily Report



Top Target



Top Attackers

02-03-2016-01:06:57 to 02-03-2016-02:06:57

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	8
212.179.54.237	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
61.160.215.88	China	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
142.54.169.162	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	drop	1
158.69.123.26	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1

02-03-2016-01:06:57 to 02-03-2016-02:06:57

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
216.17.111.245	United States	147.237.72.167	ishurim.aka.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1
69.197.177.26	United States	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	1
151.80.31.141	Italy	147.237.76.30	himush.idf.il	C228: HTTP: AhrefBot crawler	Block	1

02-03-2016-01:06:57 to 02-03-2016-02:06:57

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
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
187.105.21.152	147.237.76.86	Brazil	navy.idf.il	ET SCAN NMAP -sA (2)	2
89.248.174.81	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.248.174.81	147.237.76.198	Netherlands	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.248.174.81	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.248.174.81	147.237.72.156	Netherlands	aman.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
220.231.195.122	147.237.77.227	China	e.hamaz.idf.il	ET SCAN NMAP -sS window 3072	1
80.82.78.8	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potentia Scan or Infection	1
61.240.144.65	147.237.77.243	China	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
106.38.241.106	147.237.72.166	China	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
89.248.174.81	147.237.77.233	Netherlands	atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.248.174.81	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.248.174.81	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.248.174.81	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.248.174.81	147.237.76.39	Netherlands	mobile.meitav.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
89.248.174.81	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
220.231.195.122	147.237.77.227	China	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.174.81	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.248.174.81	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

02-03-2016-01:06:57 to 02-03-2016-02:06:57

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
81.218.179.41	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	276
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
107.167.105.209	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
176.12.155.116	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
178.162.216.32	Germany	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
31.210.188.122	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
84.108.32.84	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
149.78.11.123	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
176.228.201.125	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
149.200.203.133	Jordan	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
82.145.223.36	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
176.12.154.220	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.26.94	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
76.115.96.90	United States	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
79.178.5.78	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.141.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.46.39.227	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
178.162.216.32	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
176.12.155.116	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
31.210.186.20	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
178.162.216.32	Germany	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
31.210.188.122	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
199.30.16.172	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
104.236.10.137		147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
178.162.216.32	Germany	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
178.162.216.32	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
91.200.12.106	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
2.54.160.33	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
115.230.124.164	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
178.162.216.32	Germany	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
141.212.122.196	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
96.21.101.19	Canada	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.206	United States	147.237.8.46	e.chinuch.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.28.129.18	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
137.116.71.170	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.197	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
96.21.101.19	Canada	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
147.75.194.73	Switzerland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
5.28.129.18	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
84.108.100.240	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.111	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
31.210.187.170	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.204	United States	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
79.180.245.17	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
31.210.188.122	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

02-03-2016-01:06:57 to 02-03-2016-02:06:57

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.153.222	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	46
176.12.154.9	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
176.12.154.100	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
46.28.105.84	Czech Republic	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.28.105.84	Block	5
104.236.10.137		147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 104.236.10.137	Block	4
76.115.96.90	United States	147.237.77.74	law.idf.il	Suspicious Response Code	Block	3
176.12.154.9	Israel	147.237.0.19	madim.atal.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in madim.atal.idf.il/mobile/login.aspx	Block	2
46.19.85.53	Israel	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 46.19.85.53	Block	2
176.12.154.220	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.85.53	Israel	147.237.77.216	dover.idf.il	Multiple Malformed URL from 46.19.85.53	Block	2
46.19.85.53	Israel	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 46.19.85.53	Block	2
2.54.153.222	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.54.153.222	Block	2
109.67.51.116	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
79.170.44.126	United Kingdom	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	Block	1
46.19.85.53	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method 0; in URL __atssc=google	Block	1
31.210.186.20	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$38 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
104.131.245.20	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/	Block	1
66.249.78.134	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.chimush.atal.idf.il/console/core/doc_mgr/null	Block	1
46.19.85.53	Israel	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 46.19.85.53	Block	1
109.103.118.137	Romania	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
81.218.179.41	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
41.36.138.206	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
68.180.228.102	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/templates/shared/usercontrols/trajector/	Block	1
109.103.118.137	Romania	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
84.108.32.84	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
46.28.105.84	Czech Republic	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
41.36.138.206	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
104.236.10.137		147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1395-en/dover.aspx	Block	1
149.78.11.123	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
2.54.153.222	Israel	147.237.0.19	madim.atal.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCity in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	1
103.250.69.70	Bangladesh	147.237.77.74	law.idf.il	PHP Attempt	Block	1
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.25	Block	1
46.19.85.53	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
103.250.69.70	Bangladesh	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/daily_statistics/english/5.doc statistics about idf ratio of thwarting suicide bombing attacks	Block	1
46.19.85.53	Israel	147.237.77.216	dover.idf.il	Malformed URL __atssc=google;2	Block	1

02-03-2016-01:06:57 to 02-03-2016-02:06:57