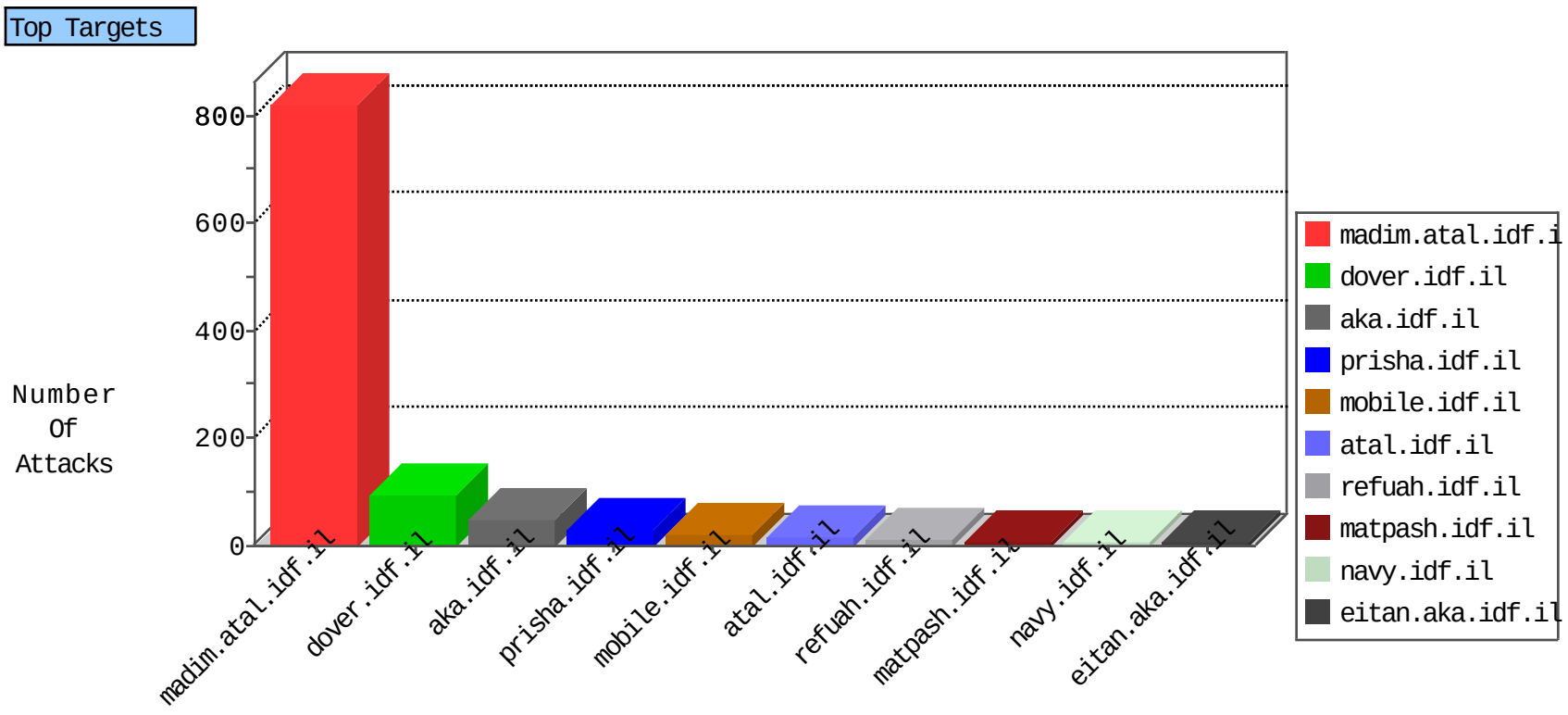
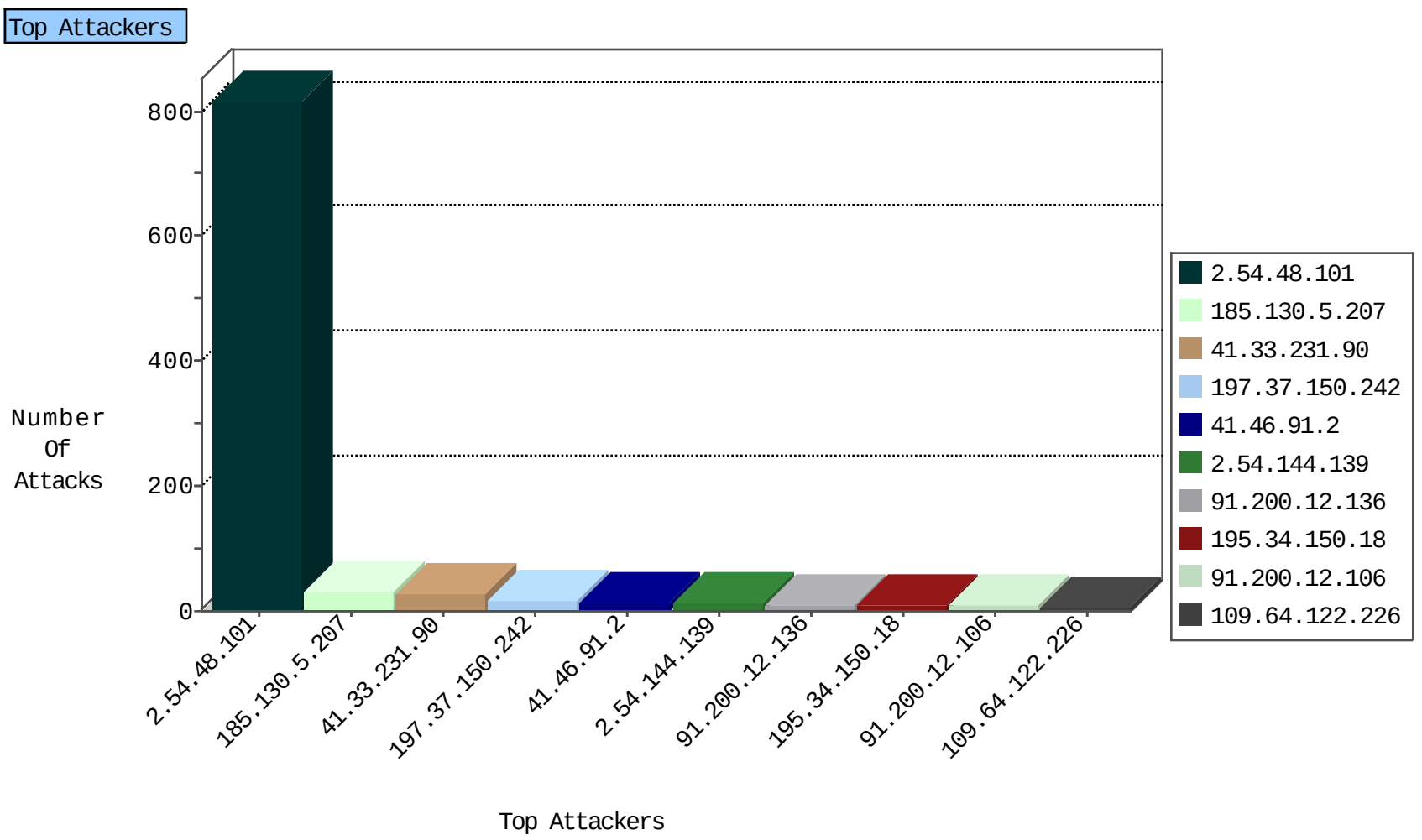
02-06-2016-02:04:07 to 02-06-2016-03:04:07

IDF Under Attack Daily Report





02-06-2016-02:04:07 to 02-06-2016-03:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
146.185.239.100	Russian Federation	147.237.0.34	tikshuv.idf.il	block-sp-traf1	drop	1
94.102.48.195	Netherlands	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
183.60.48.25	China	147.237.76.42	refuah.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
94.102.48.195	Netherlands	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
94.102.48.195	Netherlands	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1

02-06-2016-02:04:07 to 02-06-2016-03:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-06-2016-02:04:07 to 02-06-2016-03:04:07

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
66.249.78.89	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
104.128.144.131	147.237.72.14	Canada	dover.idf.il(old)	ET SCAN NMAP -sS window 2048	1
211.215.19.235	147.237.76.199	Korea, Republic of	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
104.214.148.178	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
104.128.144.131	147.237.72.14	Canada	dover.idf.il(old)	ET SCAN NMAP -f -sS	1
43.252.199.202	147.237.76.30	Japan	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
211.215.19.235	147.237.76.201	Korea, Republic of	e.atal.idf.il	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
115.188.207.222	147.237.76.30	New Zealand	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

02-06-2016-02:04:07 to 02-06-2016-03:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
185.130.5.207		147.237.77.205	prisha.idf.il	drop	SAM rule	drop	30
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
197.37.150.242	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
2.54.144.139	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
77.126.203.40	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.130.241	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
91.200.12.106	Ukraine	147.237.77.233	atal.idf.il	drop	SAM rule	drop	4
91.200.12.136	Ukraine	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	4
91.200.12.136	Ukraine	147.237.77.233	atal.idf.il	drop	SAM rule	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
91.200.12.106	Ukraine	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	4
79.180.228.60	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.220.239	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.64.203	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.122.226	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
89.238.166.141	United Kingdom	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
105.90.145.8	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
31.154.8.70	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
157.55.39.81	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
23.99.122.165	United States	147.237.72.14	dover.idf.il(old)	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
41.46.91.2	Egypt	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	2
109.64.122.226	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
66.249.65.122	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
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	2
41.46.91.2	Egypt	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	1
146.185.239.102	Russian Federation	147.237.76.148	gqcenter.aka.idf.i	drop		drop	1
23.99.122.165	United States	147.237.72.14	dover.idf.il(old)	Bad TCP sequence	SYN retransmit with different window scale	alert	1
107.182.20.202	United States	147.237.72.156	aman.idf.il	Header Rejection	header rejection pattern found in request	monitor	1
46.19.85.97	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
37.26.147.197	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
109.73.127.69	United Kingdom	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
73.134.111.103	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
203.127.96.216	Singapore	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
41.46.91.2	Egypt	147.237.76.200	eitan.aka.idf.il	drop	First packet isn't SYN	drop	1
108.180.24.186	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.109.2.237	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
46.19.85.237	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
198.20.69.74	United States	147.237.77.243	mobile.idf.il	drop	SAM rule	drop	1
23.101.61.176	Ireland	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
84.109.2.237	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
203.127.96.216	Singapore	147.237.77.216	dover.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
77.201.201.147	France	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
45.246.45.34	Uruguay	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
195.28.180.101	Israel	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
24.0.239.209	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
203.127.96.216	Singapore	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

02-06-2016-02:04:07 to 02-06-2016-03:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.48.101	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.48.101	Block	477
2.54.48.101	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 2.54.48.101	Block	228
2.54.48.101	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	111
192.243.55.132	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.132	Block	5
192.243.55.138	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.138	Block	4
188.143.232.70	Russian Federation	147.237.77.176	matpash.idf.il	Parameter Type Violation fromDate in www.cogat.idf.il/901-en/cogat.aspx	Block	3
37.24.151.174	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	2
41.46.91.2	Egypt	147.237.77.233	atal.idf.il	PHP Attempt	Block	2
17.138.55.213	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.138.55.213	Block	2
213.163.66.185	Netherlands	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 213.163.66.185	Block	2
41.46.91.2	Egypt	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/xmlrpc.php	Block	2
46.19.86.84	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
192.243.55.131	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.131	Block	2
58.63.53.185	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	2
192.243.55.137	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.137	Block	2
107.182.20.202	United States	147.237.72.156	aman.idf.il	eMail Hoarding	Block	1
212.97.132.209	Denmark	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/old/wp-admin/	Block	1
66.249.78.233	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/templates/news/news.in.aspx	Block	1
192.243.55.132	Dominica	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/promotioncube/	Block	1
157.55.39.79	United States	147.237.72.166	aka.idf.il	Unknown Parameter tm in www.aka.idf.il/main/giyus/	None	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-he/cogat.aspx	Block	1
58.63.53.185	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
192.243.55.137	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/eitan/listpage	Block	1
192.243.55.129	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=58560&docid=73184	Block	1
41.46.91.2	Egypt	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 41.46.91.2	Block	1
109.64.122.226	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.79.228	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
192.243.55.133	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/general.aspx?catid=59630	Block	1
31.180.44.182	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1397-en/dover.aspx	Block	1
157.55.39.143	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
70.79.93.159	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.78.13	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
192.243.55.130	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=59268&docid=65415	Block	1
41.46.91.2	Egypt	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
2.54.48.101	Israel	147.237.0.19	madim.atal.idf.il	Too Many 403: Response Code per Session	Block	1
109.253.220.239	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	1
213.163.66.185	Netherlands	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	1
66.249.79.235	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/1.he/scroller/skin.css	Block	1
192.243.55.134	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/tizmoret/faq/default.asp?catid=49388	Block	1
31.180.44.182	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1397-en/dover.aspx	Block	1
157.55.39.145	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/sip_storage/files/3/2493.jpg	Block	1
84.228.205.135	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
192.243.55.138	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/smalim/smalim.aspx?catid=58629	Block	1
66.249.78.82	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
41.46.91.2	Egypt	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 41.46.91.2	Block	1
109.253.220.247	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$26 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
66.249.79.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/1.he/langstyle.css	Block	1
58.63.53.185	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 58.63.53.185	Block	1
192.243.55.136	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/kadatz	Block	1
162.203.2.233	United States	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1

02-06-2016-02:04:07 to 02-06-2016-03:04:07