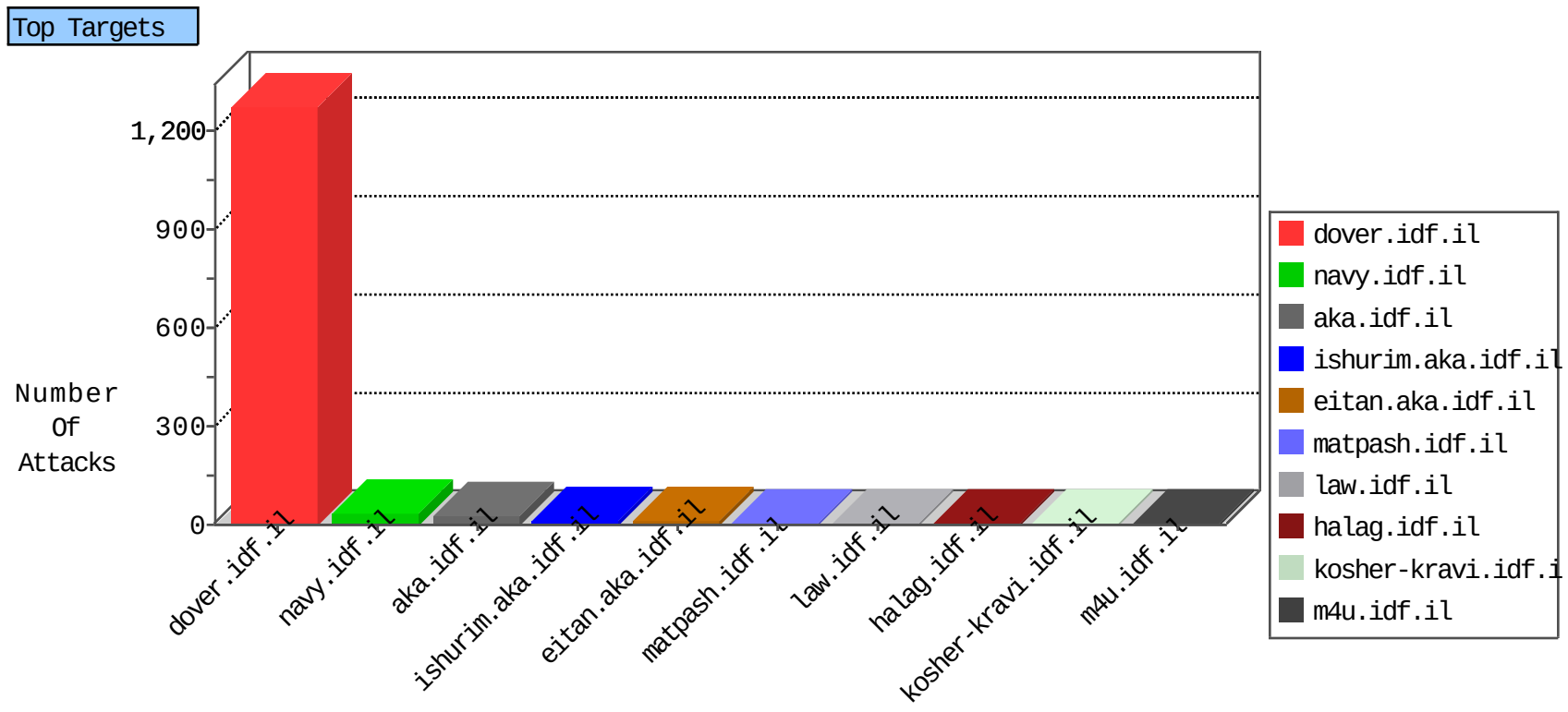
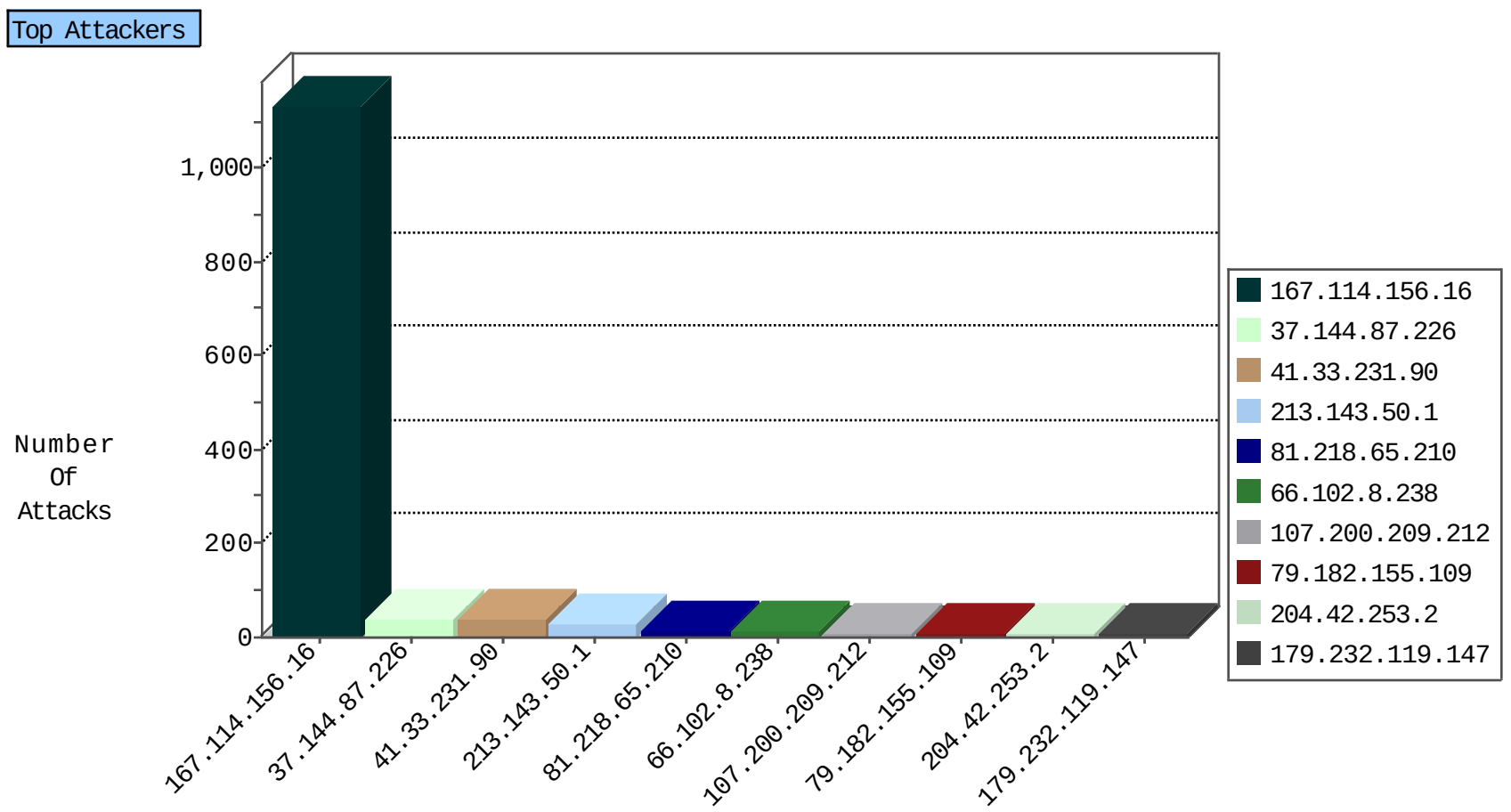
04-15-2016-04:04:09 to 04-15-2016-05:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-15-2016-04:04:09 to 04-15-2016-05:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	1135
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	6
37.144.87.226	Russian Federation	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Http	drop	3
204.42.253.2	United States	147.237.8.28	e.mobile-ks.idf.il	Block_Ntp_All_Net	drop	2
37.144.87.226	Russian Federation	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Http	drop	2
204.42.253.2	United States	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.0.35	akaws.idf.il	Block_Ntp_All_Net	drop	2
209.126.127.16	United States	147.237.0.16	my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
209.126.127.16	United States	147.237.0.35	akaws.idf.il	Block_Udp_All_Nets	drop	1
38.229.1.13	United States	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
218.23.79.217	China	147.237.72.217	e.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
209.126.127.16	United States	147.237.0.15	kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1

04-15-2016-04:04:09 to 04-15-2016-05:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.149	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	3
185.106.92.47	Russian Federation	147.237.77.234	halag.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	3
69.30.214.38	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
199.30.24.96	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
68.64.168.82	United States	147.237.77.170	maarachot.idf.il	C1000016: HTTP: administrator in URI	Block	1
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	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
185.106.92.47	Russian Federation	147.237.77.234	halag.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
106.38.241.106	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-15-2016-04:04:09 to 04-15-2016-05:04:09

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
106.186.113.132	147.237.76.200	Japan	eitan.aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
97.74.4.26	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
87.229.116.42	147.237.76.202	Hungary	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.205.69	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
220.179.172.185	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
218.23.79.217	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
195.216.176.244	147.237.76.86	Latvia	navy.idf.il	ET SCAN NMAP -sS window 1024	1
185.106.92.47	147.237.77.234	Russian Federation	halag.idf.il	ET WEB_SERVER Muieblackcat scanner	1
97.74.4.26	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 1024	1
97.74.4.26	147.237.8.14	United States	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
58.218.205.69	147.237.8.14	China	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
46.151.52.139	147.237.76.38	Ukraine	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
220.133.23.113	147.237.0.19	Taiwan	madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
198.20.69.98	147.237.76.197	United States	e.himush.idf.il	ET DROP Dshield Block Listed Source	1

04-15-2016-04:04:09 to 04-15-2016-05:04:09

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	36
37.144.87.226	Russian Federation	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	31
66.102.8.238	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
213.143.50.1	Spain	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
79.182.155.109	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
172.56.36.177	United States	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.143.50.1	Spain	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
213.143.50.1	Spain	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
123.126.113.101	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	5
213.143.50.1	Spain	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
213.143.50.1	Spain	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.53.142.15	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
179.232.119.147	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
172.56.12.141	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
179.232.119.147	Brazil	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
46.117.58.55	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
199.30.24.201	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
213.143.50.1	Spain	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
177.75.229.28	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
141.212.122.131	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
141.212.122.112	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.80	United States	147.237.0.35	akaws.idf.il	drop		drop	1
159.226.95.66	China	147.237.0.33	idf.il	drop		drop	1
141.212.122.136	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.121	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.228	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
106.186.113.132	Japan	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
62.210.129.246	France	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
141.212.122.213	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
218.22.211.69	China	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
2.53.154.20	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.132	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.114	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.111	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.53.232.154	Russian Federation	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
46.105.61.138	France	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
141.212.122.136	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.122	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.243	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
120.132.84.157	China	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.214	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
37.48.74.44	Netherlands	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
141.212.122.132	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
200.74.240.180	Panama	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.115	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.112	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.94.165.139	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.137	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

04-15-2016-04:04:09 to 04-15-2016-05:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
199.30.25.90	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
199.30.24.220	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.102.8.238	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
199.30.24.35	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
107.200.209.212	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	2
107.200.209.212	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 107.200.209.212	Block	1
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter SearchText in www.eitan.aka.idf.il/938-he/eitan.aspx	None	1
40.77.167.78	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/chamatz/klali/default.asp	None	1
147.9.98.104	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
107.200.209.212	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/wp-login.php	Block	1
66.249.78.89	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
107.200.209.212	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/wp-login.php	Block	1
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
40.77.167.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
157.55.39.55	United States	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/robots.txt	Block	1
107.200.209.212	United States	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
204.236.235.245	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
109.86.72.163	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1116-en/	Block	1
106.186.113.132	Japan	147.237.76.200	eitan.aka.idf.il	Multiple Untraceable SSL Sessions from 106.186.113.132 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
198.58.96.215	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
107.200.209.212	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/wp-login.php	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1381-he/dover.aspx	Block	1
123.59.59.52	China	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.mafengwo.cn/894-he/orchot.aspx	Block	1
106.186.113.132	Japan	147.237.76.200	eitan.aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.102.8.243	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/kesher	Block	1
37.48.74.44	Netherlands	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
128.232.110.28	United Kingdom	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
107.200.209.212	United States	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	Block	1

04-15-2016-04:04:09 to 04-15-2016-05:04:09