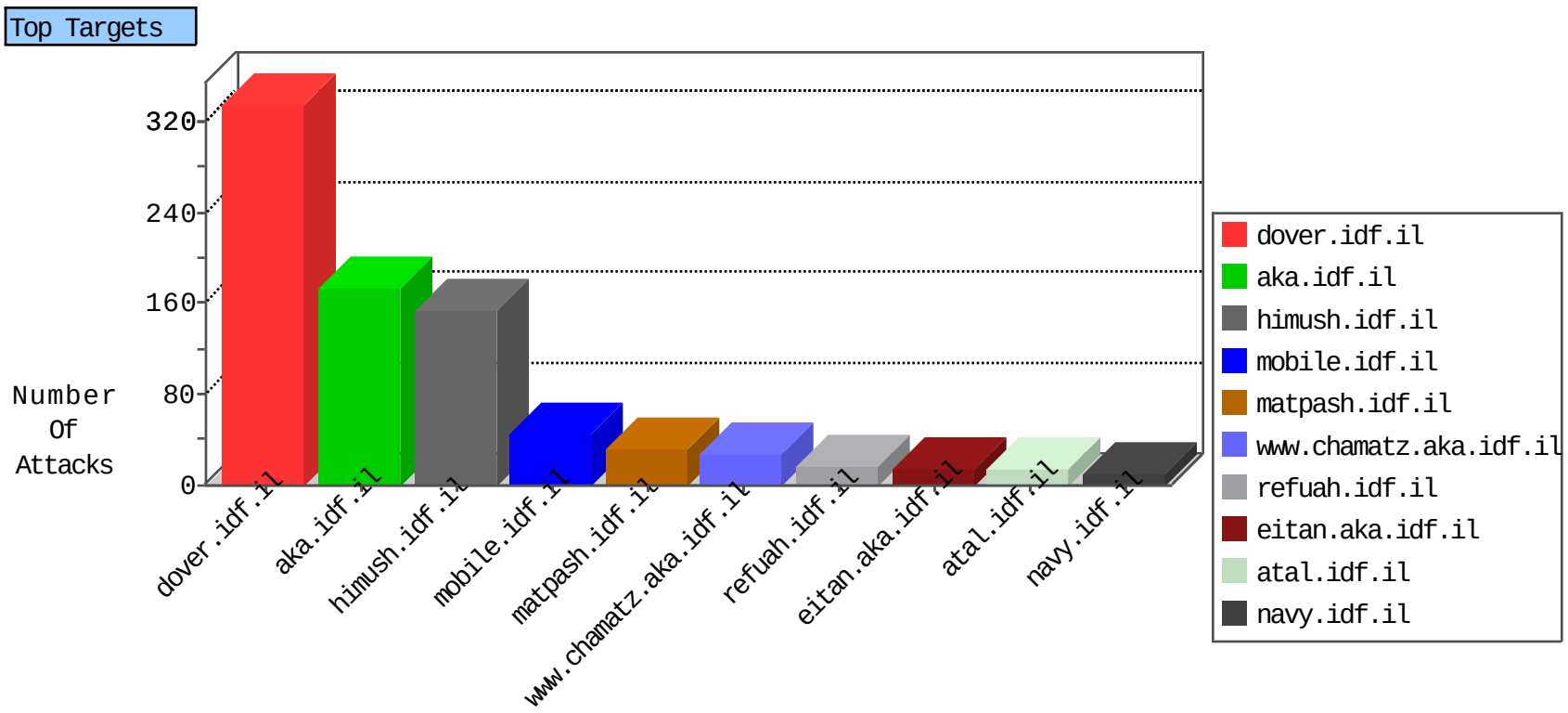
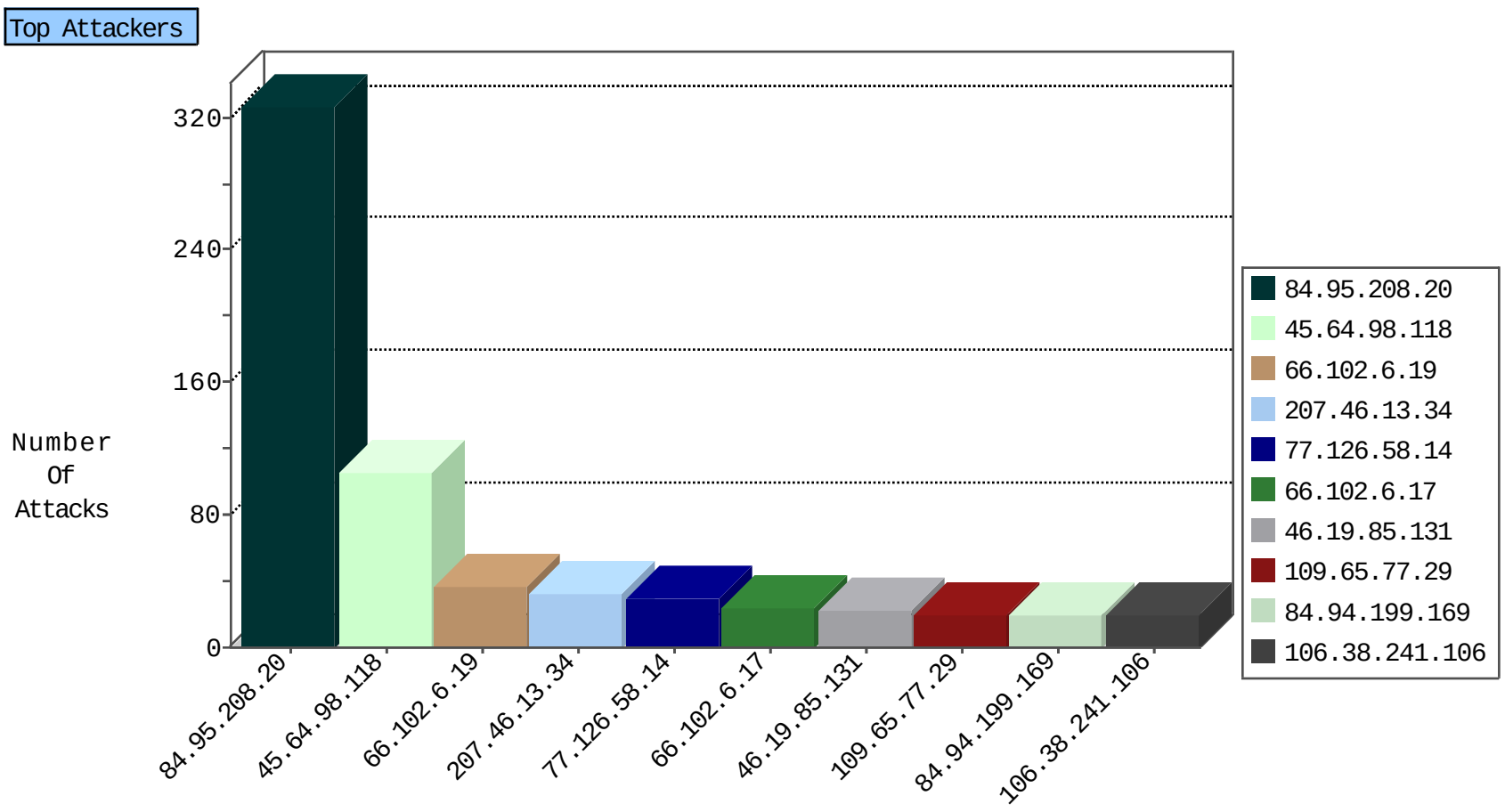
10-03-2016-09:04:08 to 10-03-2016-10:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-03-2016-09:04:08 to 10-03-2016-10:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.102.6.19	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	15
66.102.6.17	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
84.95.208.20	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
66.249.65.51	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
66.249.85.179	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
68.180.231.57	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
77.139.192.75	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
66.249.85.181	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
38.108.35.137	United States	147.237.76.196	e.sviva.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
200.76.129.251	Mexico	147.237.76.147	chinuch.aka.idf.il	L4 Source or Dest Port Zero	drop	1
93.174.94.235	Netherlands	147.237.76.202	e.halag.idf.il	Black List	drop	1
71.6.167.142	United States	147.237.76.31	nakchal.idf.il	Black List	drop	1
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
185.94.111.1	Russian Federation	147.237.76.197	e.himush.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.202	e.halag.idf.il	Black List	drop	1

10-03-2016-09:04:08 to 10-03-2016-10:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	13
220.181.125.23	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

10-03-2016-09:04:08 to 10-03-2016-10:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
120.33.120.66	147.237.72.217	China	e.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
42.115.126.16	147.237.77.235	Vietnam	sviva.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
124.8.223.198	147.237.76.38	Taiwan	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
122.230.216.69	147.237.76.197	China	e.himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
101.24.189.34	147.237.0.34	China	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
85.143.216.168	147.237.72.167	Russian Federation	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
58.63.69.176	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
183.129.160.229	147.237.77.74	China	law.idf.il	ET SCAN Potential SSH Scan	1
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	1
139.162.160.132	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
14.152.59.11	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
124.8.223.198	147.237.76.201	Taiwan	e.atal.idf.il	ET SCAN Potential SSH Scan	1
124.8.223.198	147.237.0.19	Taiwan	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
122.72.53.188	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
116.28.77.156	147.237.0.33	China	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
94.102.48.194	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
61.221.69.222	147.237.72.217	Taiwan	e.idf.il	ET SCAN NMAP -sS window 1024	1
46.121.112.167	147.237.0.15	Israel	kosher-kravi.idf.il	ET SCAN NMAP -sA (2)	1
176.58.124.35	147.237.8.24	United Kingdom	e.lifestyle.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
139.162.13.205	147.237.77.226	Singapore	www.chamatz.aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1

10-03-2016-09:04:08 to 10-03-2016-10:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
207.46.13.34	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
77.126.58.14	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
45.64.98.118	Indonesia	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	25
45.64.98.118	Indonesia	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	24
45.64.98.118	Indonesia	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	24
45.64.98.118	Indonesia	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
84.94.199.169	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	15
45.64.98.118	Indonesia	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	14
46.19.86.135	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
66.102.6.19	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.177.205.135	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.102.6.19	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.85.131	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.131	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.131	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.156	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.131	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
115.28.218.121	China	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
66.102.6.19	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
84.95.208.20	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
185.110.108.165	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.156	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
115.28.218.121	China	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	4
66.102.6.17	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.102.6.19	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
115.28.218.121	China	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	4
84.94.199.169	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
176.13.19.74	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
164.132.202.49	Italy	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.179.42.227	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
66.102.6.17	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
2.53.190.9	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
164.132.204.198	Italy	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	3
164.132.202.49	Italy	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	3
164.132.204.198	Italy	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	3
46.19.86.99	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
31.168.166.178	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.204	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
115.28.218.121	China	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
37.26.146.244	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
79.61.203.98	Italy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
164.132.202.49	Italy	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
202.136.81.103	India	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
5.22.134.221	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
82.102.215.21	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
141.226.217.250	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
109.64.159.86	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
79.61.203.98	Italy	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2

10-03-2016-09:04:08 to 10-03-2016-10:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	134
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	91
109.65.77.29	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.65.77.29	Block	18
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	13
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	12
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	9
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	8
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	5
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
84.95.208.20	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
85.132.77.12	Azerbaijan	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	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	3
85.132.77.12	Azerbaijan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/images/	Block	3
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	3
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
68.81.201.57	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	2
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
84.95.208.20	Israel	147.237.77.234	halag.idf.il	PHP Attempt	Block	1
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	PHP Attempt	Block	1
68.81.201.57	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 68.81.201.57	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
79.181.66.83	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
141.226.218.13	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mas.aspx	None	1
66.249.64.56	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1250-he/atal.aspx	Block	1
84.95.208.20	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
109.65.77.29	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
157.55.39.145	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/â€ž	Block	1
66.249.64.58	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1249-he/atal.aspx	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/piwik.php	Block	1
84.95.208.20	Israel	147.237.72.156	aman.idf.il	PHP Attempt	Block	1
128.72.229.15	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Unauthorized Method POST for www.chinuch.aka.idf.il/1163-he/chinuch.aspx	None	1
68.180.228.60	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation PageNum in www.tikshuv.idf.il/901-he/tikshuv.aspx	Block	1
2.53.166.252	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 2.53.166.252	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	PHP Attempt	Block	1
216.244.66.241	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 106.38.241.106	Block	1
66.249.64.60	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1486-he/atal.aspx	Block	1
139.162.13.205	Singapore	147.237.76.42	refuah.idf.il	Multiple Untraceable SSL Sessions from 139.162.13.205 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1824-he/dover.aspx	Block	1
2.53.166.252	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	1
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-10046-en	Block	1
66.249.65.59	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8759-he/refuah.aspx	Block	1
139.162.13.205	Singapore	147.237.76.42	refuah.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
77.139.25.104	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/haredim/general.aspx	Block	1

10-03-2016-09:04:08 to 10-03-2016-10:04:08