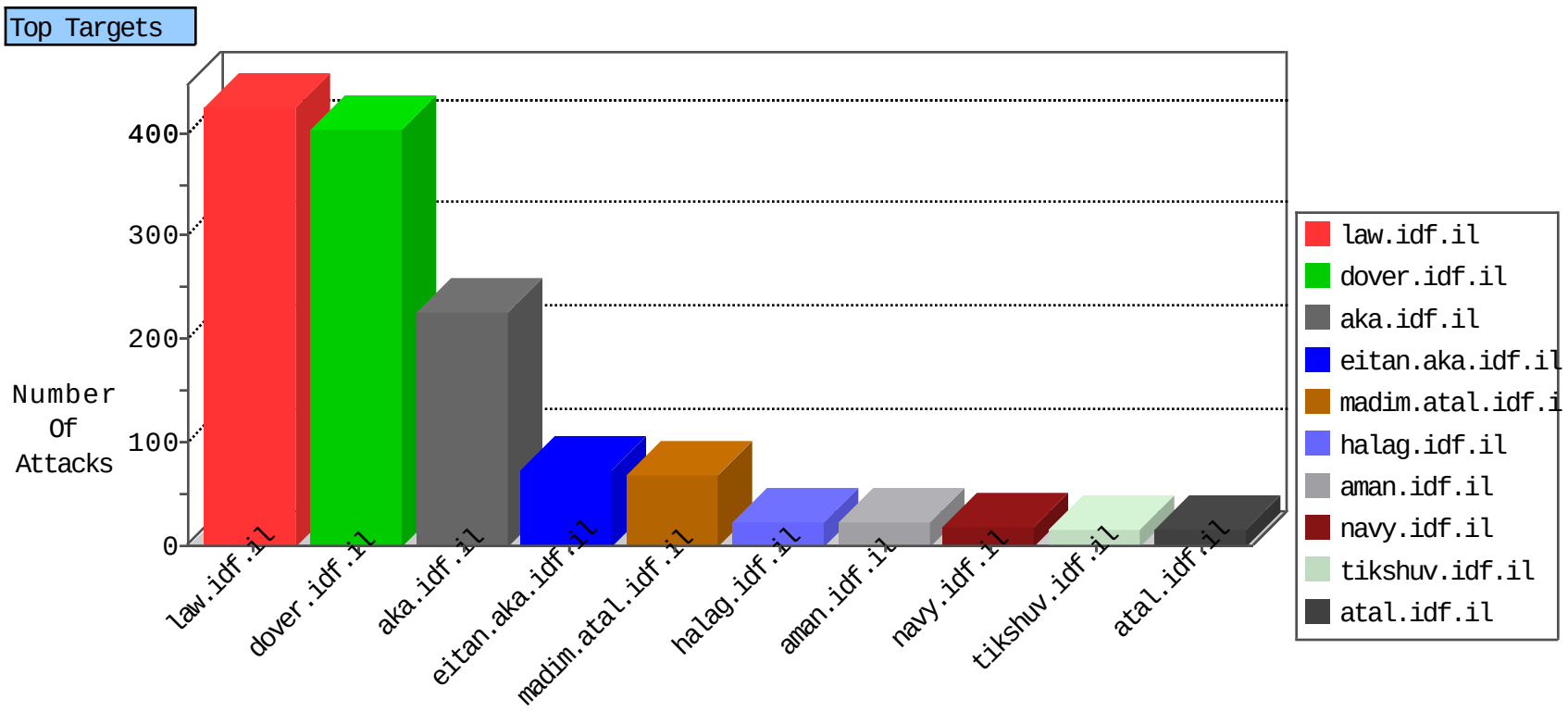
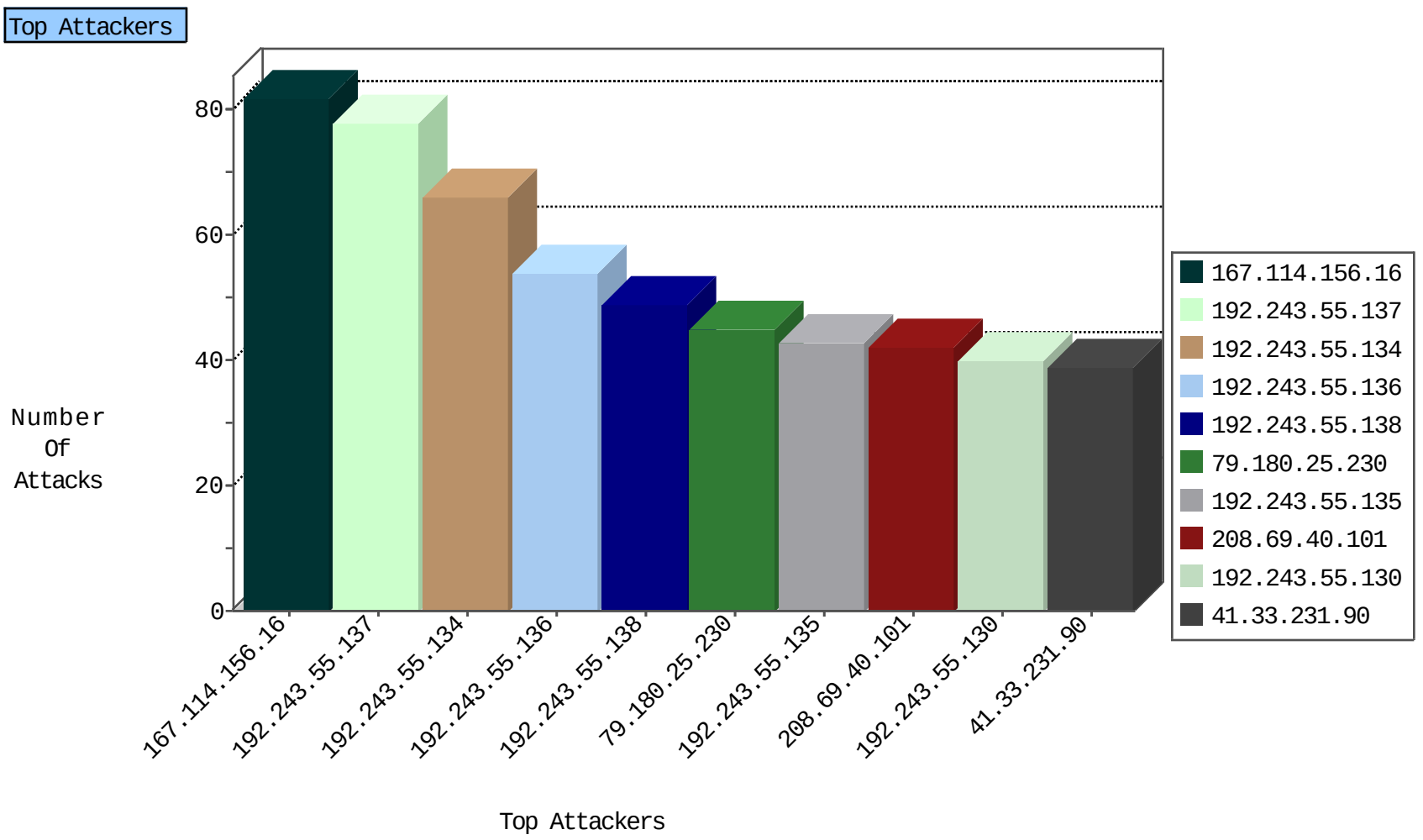
04-23-2016-21:04:03 to 04-23-2016-22:04:03

IDF Under Attack
Daily Report





04-23-2016-21:04:03 to 04-23-2016-22:04:03

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	TCP handshake violation, first packet not syn	drop	6043
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	5095
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	913
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	9
74.91.17.180	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	2
112.119.243.239	Hong Kong	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	2
104.238.135.152	United States	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
123.59.59.52	China	147.237.77.233	atal.idf.il	block-sp-traf1	drop	1
94.102.52.10	Netherlands	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
104.238.135.152	United States	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
94.102.52.10	Netherlands	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
104.238.135.152	United States	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
94.102.52.10	Netherlands	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
74.91.23.109	United States	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	drop	1

04-23-2016-21:04:03 to 04-23-2016-22:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-23-2016-21:04:03 to 04-23-2016-22:04:03

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
98.126.212.154	147.237.0.34	United States	tikshuv.idf.i	ET SCAN NMAP -sS window 1024	1
40.114.42.13	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
190.124.35.115	147.237.72.156	Nicaragua	aman.idf.il	ET SCAN NMAP -sS window 3072	1
174.37.194.144	147.237.77.61	United States	e.cogat.idf.i	ET SCAN NMAP -sS window 4096	1
106.38.241.144	147.237.72.166	China	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
98.126.212.154	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 1024	1
190.124.35.115	147.237.72.156	Nicaragua	aman.idf.il	ET SCAN NMAP -sS window 1024	1
174.37.194.144	147.237.77.61	United States	e.cogat.idf.i	ET SCAN NMAP -sS window 3072	1

04-23-2016-21:04:03 to 04-23-2016-22:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.180.25.230	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
208.69.40.101	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	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	27
87.70.52.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
207.241.231.194	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	18
85.76.17.197	Finland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	17
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	17
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
89.138.227.121	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	15
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
192.243.55.137	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
192.243.55.134	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
63.153.217.245	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
85.65.203.89	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
192.243.55.137	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	11
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
84.108.121.163	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.19.86.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	9
81.57.210.33	France	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	9
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
192.243.55.138	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
77.126.82.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.136	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
85.64.16.126	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
85.250.128.80	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
198.58.103.28	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.135	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
87.69.25.217	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.135	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
192.243.55.132	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
85.65.203.89	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7

04-23-2016-21:04:03 to 04-23-2016-22:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.19.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	37
212.76.109.76	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
47.90.1.211	Canada	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/yohalan/forums/asp/	Block	3
37.46.41.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.248.253.133	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1556-en/	Block	3
208.54.86.151	United States	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
199.30.25.92	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
117.135.251.134	China	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/yohalan/forums/asp/	Block	2
203.127.58.237	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.186.2.168	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/general/mobile	Block	2
109.253.225.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
220.255.148.10	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1361-he/dover.aspx	Block	1
199.30.24.77	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
130.193.50.33	Russian Federation	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/261-6958-	Block	1
109.49.64.245	Portugal	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
79.181.245.89	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/yoman.asp	Block	1
157.55.39.191	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in tikshuv.idf.il/site/general.aspx	Block	1
46.19.85.239	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
117.135.250.130	China	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/yohalan/forums/asp/	Block	1
103.231.241.40	Philippines	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
2.53.16.142	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/an..	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 141.8.132.78	Block	1
62.219.227.44	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 62.219.227.44 (Protocol violation (SSL_CONN_CLIENT_KEY_EXCHANGE))	None	1
37.142.64.129	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/newsflash/mobile	Block	1
109.64.131.147	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/https:/mobile.idf.il/	Block	1
84.109.81.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
169.229.3.91	United States	147.237.77.234	halag.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
46.19.86.22	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
103.231.241.40	Philippines	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/wp-login.php	Block	1
74.91.17.180	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to www.gege1.com/	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/9/16919.pdf.	Block	1
65.55.210.242	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
40.77.167.65	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	1
212.76.119.180	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/elram/site/templates/controller.asp	Block	1
85.64.66.85	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 85.64.66.85 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
192.243.55.137	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/327-he/patzar.aspx?pagenum=2	Block	1
117.177.250.152	China	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/yohalan/forums/asp/	Block	1
46.28.136.28	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	Distributed Suspicious Response Code	Block	1
106.38.241.144	China	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
203.127.96.199	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.178.53.217	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
157.55.39.56	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/misrot.aspx	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
40.77.167.72	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/meitav@idf.gov.il	Block	1

04-23-2016-21:04:03 to 04-23-2016-22:04:03