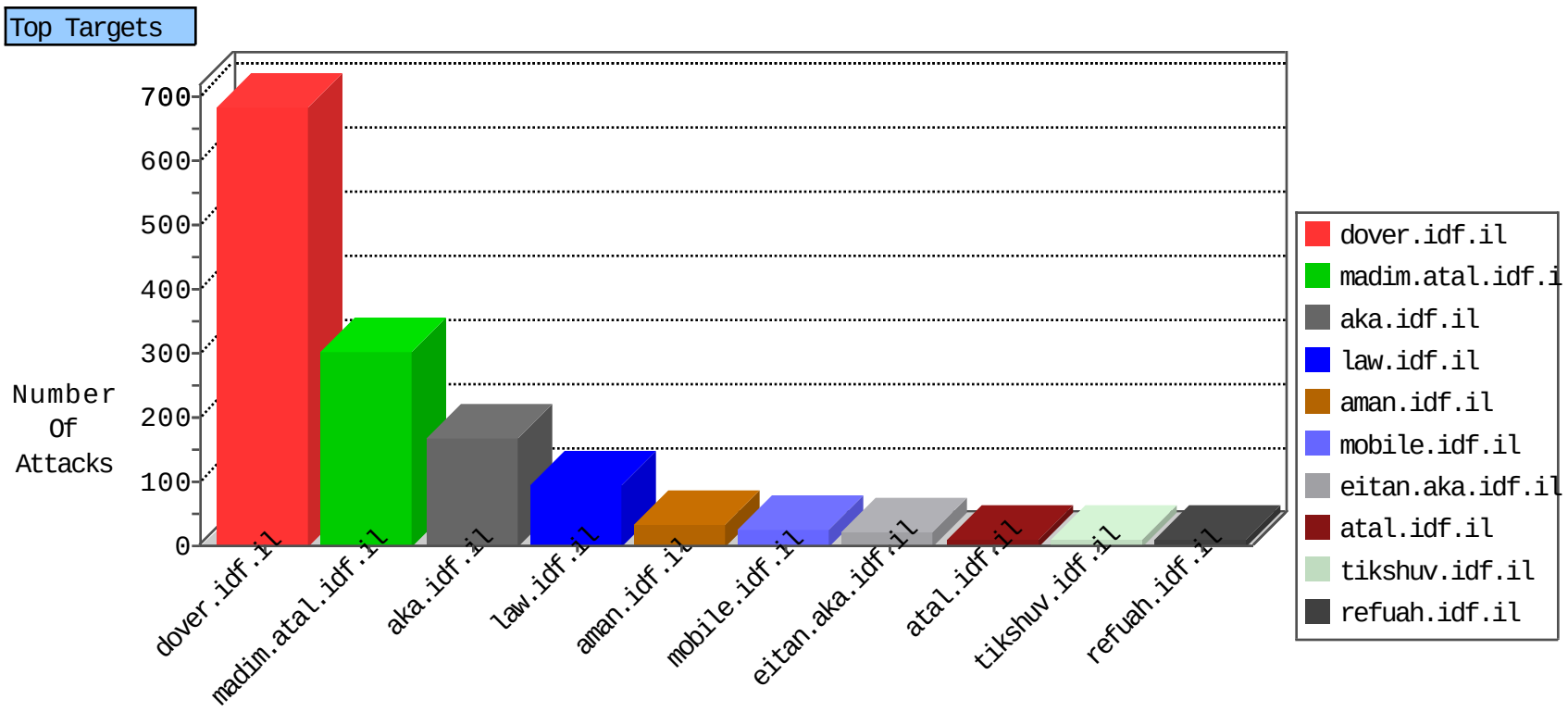
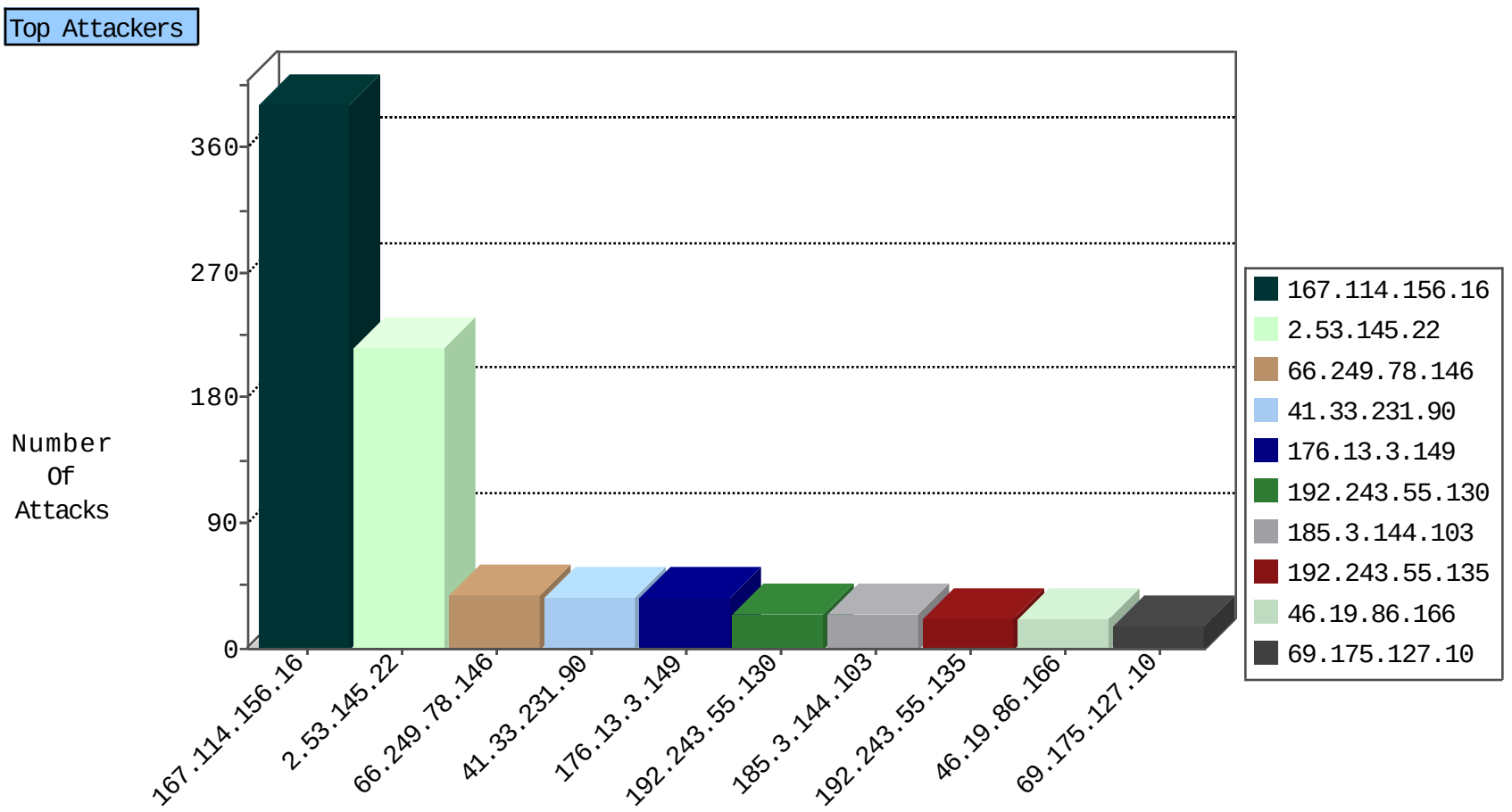
04-22-2016-15:04:00 to 04-22-2016-16:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-22-2016-15:04:00 to 04-22-2016-16:04:00

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	HTTP-POST-Segmented-DoS	dest-reset	16955
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	613
46.121.152.86	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	203
85.64.79.176	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	101
94.102.49.116	Netherlands	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
94.102.49.116	Netherlands	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1	Russian Federation	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
94.102.52.10	Netherlands	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1	Russian Federation	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
85.250.169.120	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1
94.102.52.10	Netherlands	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
31.148.219.86	Netherlands	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1

04-22-2016-15:04:00 to 04-22-2016-16:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-22-2016-15:04:00 to 04-22-2016-16:04:00

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
66.102.6.131	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
109.64.35.136	147.237.76.42	Israel	refuah.idf.il	ET SCAN NMAP -sA (2)	2
109.236.94.216	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
188.14.242.67	147.237.76.202	Italy	e.halag.idf.il	ET SCAN NMAP -f -sS	1
93.174.88.102	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potentia Scan or Infection	1
185.130.5.99	147.237.77.233	Lithuania	atal.idf.il	ET SCAN Potential SSH Scan	1
85.131.208.140	147.237.77.178	Germany	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.99	147.237.76.44	Lithuania	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
85.131.208.140	147.237.76.148	Germany	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.99	147.237.76.39	Lithuania	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
85.131.208.140	147.237.76.34	Germany	yohalan.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.99	147.237.72.167	Lithuania	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.99	147.237.72.156	Lithuania	aman.idf.il	ET SCAN Potential SSH Scan	1
64.20.48.41	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 2048	1
195.216.176.244	147.237.77.212	Latvia	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
149.78.154.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
64.20.48.41	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -f -sS	1
109.236.94.216	147.237.72.156	Netherlands	aman.idf.il	ET SCAN NMAP -sS window 1024	1
188.14.242.67	147.237.76.202	Italy	e.halag.idf.il	ET SCAN NMAP -sS window 2048	1
185.130.5.99	147.237.77.235	Lithuania	sviva.idf.il	ET SCAN Potential SSH Scan	1
85.131.208.140	147.237.77.235	Germany	sviva.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.99	147.237.77.178	Lithuania	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
85.131.208.140	147.237.77.61	Germany	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.99	147.237.76.42	Lithuania	refuah.idf.il	ET SCAN Potential SSH Scan	1
85.131.208.140	147.237.76.44	Germany	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.99	147.237.72.217	Lithuania	e.idf.il	ET SCAN Potential SSH Scan	1
85.131.208.140	147.237.8.46	Germany	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.99	147.237.72.166	Lithuania	aka.idf.il	ET SCAN Potential SSH Scan	1
65.55.210.58	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.99	147.237.0.15	Lithuania	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
64.20.48.41	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 1024	1
195.154.54.169	147.237.76.44	France	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
109.236.94.216	147.237.77.176	Netherlands	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
188.14.242.67	147.237.76.202	Italy	e.halag.idf.il	ET SCAN NMAP -sS window 3072	1

04-22-2016-15:04:00 to 04-22-2016-16:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	29
185.3.144.103	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
136.0.99.15	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	16
69.175.127.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
66.102.6.131	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
153.31.112.24	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
162.243.126.57	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
72.9.148.10	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	12
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
79.182.26.104	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
109.64.41.84	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.121.193.94	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
208.115.113.89	United States	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	7
92.241.37.230	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
157.55.39.241	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
84.228.220.167	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.4.11.215	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
95.86.104.64	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
5.29.246.216	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.78.252	United States	147.237.0.19	madim.atal.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
95.86.104.64	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.130	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
47.53.143.214	Italy	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
37.46.39.111	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.53.27.232	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
66.102.7.233	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
192.243.55.135	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
5.29.190.239	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	4
82.6.49.138	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
2.53.170.223	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	4
91.200.12.141	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
37.26.149.130	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
37.46.41.201	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
85.130.225.96	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
176.31.224.223	France	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
157.55.39.129	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
149.78.179.201	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.137	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
185.120.125.88	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.145.22	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	217
176.13.3.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
46.19.86.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
46.19.85.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
80.246.136.115	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	3
37.26.147.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
212.235.28.4	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 212.235.28.4	Block	3
101.255.56.138	Indonesia	147.237.0.34	tikshuv.idf.il	Distributed PHP Attempt	Block	2
37.26.146.230	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	2
66.102.6.188	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.86.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.102.7.240	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.55.15.41	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in atal.idf.il/1440-he/atal.aspx	Block	2
151.80.31.176	France	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
5.29.246.216	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1283-19206-en/dover.aspx	Block	1
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation docId in tikshuv.idf.il/site/story.aspx	Block	1
109.254.29.48	Ukraine	147.237.77.74	law.idf.il	PHP Attempt	Block	1
46.121.81.174	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
213.8.204.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
157.55.39.200	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
101.255.56.138	Indonesia	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 101.255.56.138	Block	1
46.19.85.171	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
212.44.9.122	United Kingdom	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
109.254.29.48	Ukraine	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/wp-login.php	Block	1
81.177.254.105	Russian Federation	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
160.178.154.166	Morocco	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 160.178.154.166	Block	1
101.255.56.138	Indonesia	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/wp-login.php	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
212.44.9.122	United Kingdom	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
141.212.122.161	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1
81.177.254.105	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
160.178.154.166	Morocco	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
41.254.2.129	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
109.64.250.227	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
66.249.66.17	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/general/general.aspx	Block	1
149.88.177.19	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
95.86.68.6	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/h	Block	1
66.249.64.198	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
41.254.2.129	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/admin	Block	1
109.111.26.23	Russian Federation	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/general.aspx	Block	1
79.178.22.224	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	1
46.116.73.98	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/milluim/index	Block	1
212.235.28.4	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/site/templates/controller.asp	Block	1

04-22-2016-15:04:00 to 04-22-2016-16:04:00