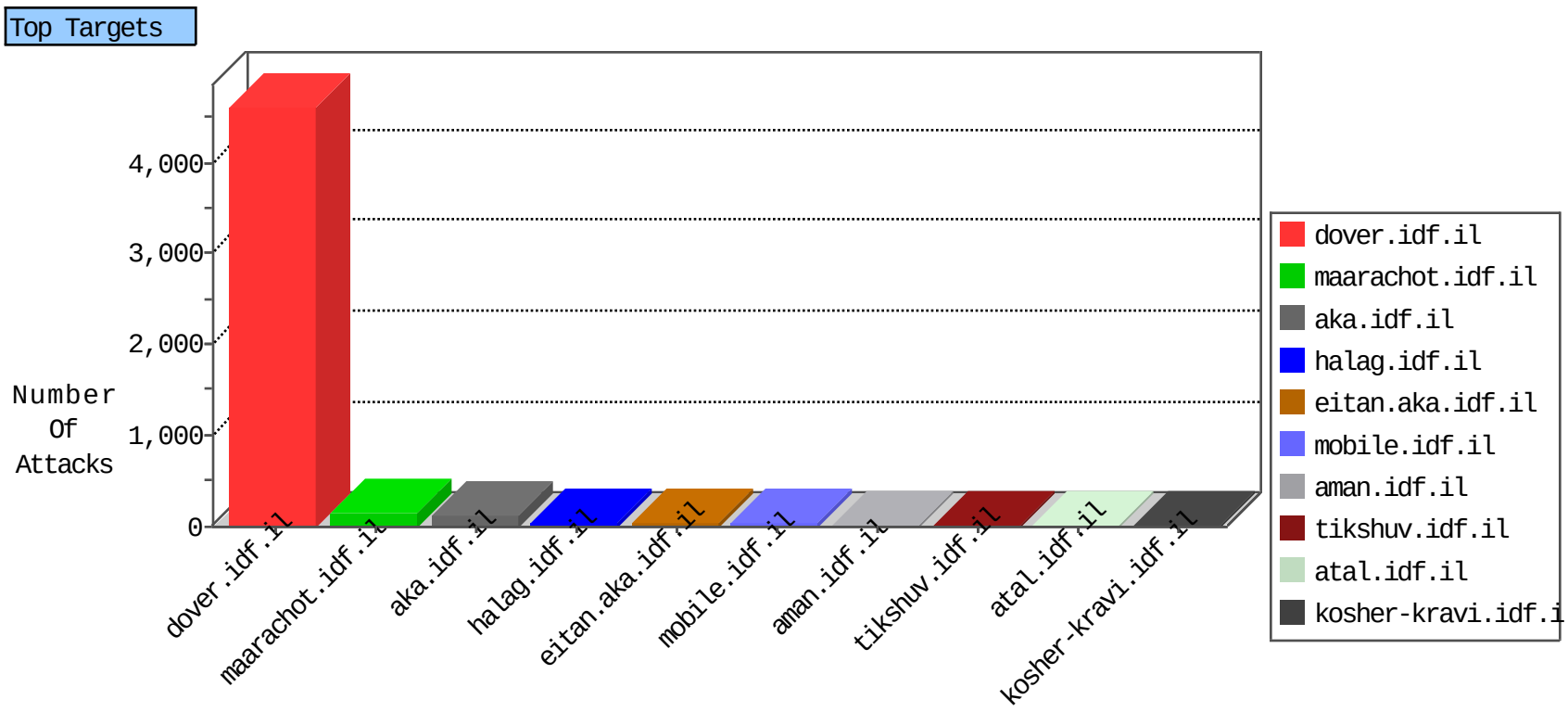
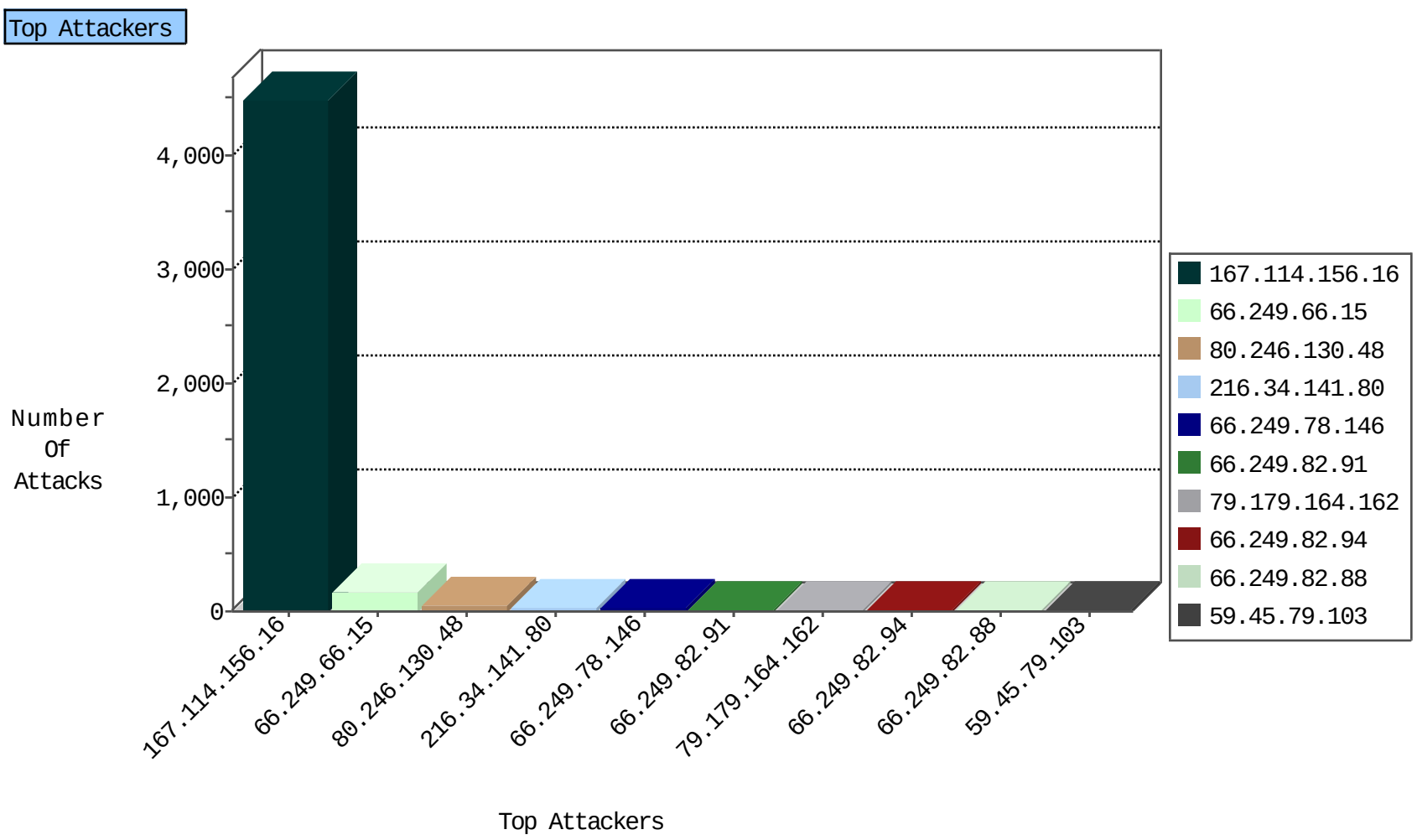
04-20-2016-00:04:05 to 04-20-2016-01:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-20-2016-00:04:05 to 04-20-2016-01:04:05

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	3960
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	793
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
82.166.184.140	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
111.91.235.228	Vietnam	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	1
185.56.28.67	Netherlands	147.237.0.16	my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
23.94.234.122	United States	147.237.77.74	law.idf.il	Block_Udp_All_Nets	drop	1
185.56.28.67	Netherlands	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
82.221.105.6	Iceland	147.237.77.178	e.matpash.idf.il	Block_Udp_All_Nets	drop	1
23.94.234.122	United States	147.237.77.179	e.mazi.idf.il	Block_Udp_All_Nets	drop	1
185.56.28.67	Netherlands	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
94.102.49.116	Netherlands	147.237.72.217	e.idf.il	Block_Ntp_All_Net	drop	1

04-20-2016-00:04:05 to 04-20-2016-01:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-20-2016-00:04:05 to 04-20-2016-01:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.66.15	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	158
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
59.45.79.103	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.155	147.237.0.15	Ukraine	kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
59.45.79.103	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
89.248.172.140	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
59.45.79.103	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
81.27.85.27	147.237.0.35	United Kingdom	akaws.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.103	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
80.82.78.8	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
64.207.180.204	147.237.77.216	United States	dover.idf.il	SERVER-WEBAPP admin.php access	1
179.97.179.148	147.237.8.28	Brazil	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.45.79.103	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
107.158.255.194	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 2048	1
59.45.79.103	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential SSH Scan	1
107.158.255.194	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.103	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.155	147.237.0.15	Ukraine	kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
59.45.79.103	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.155	147.237.0.15	Ukraine	kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
59.45.79.103	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
82.117.208.243	147.237.77.233		atal.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.103	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
80.242.215.82	147.237.8.27	Kazakstan	e.madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.45.79.103	147.237.77.233	China	atal.idf.il	ET SCAN Potential SSH Scan	1
177.193.127.47	147.237.8.27	Brazil	e.madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.45.79.103	147.237.77.176	China	matpash.idf.il	ET SCAN Potential SSH Scan	1
107.158.255.194	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -f -sS	1
59.45.79.103	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
106.38.241.106	147.237.72.166	China	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1

04-20-2016-00:04:05 to 04-20-2016-01:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	480
80.246.130.48	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	45
216.34.141.80	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
79.179.164.162	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
66.249.82.91	Asia/Pacific Region	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
66.249.82.88	Asia/Pacific Region	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
66.249.82.94	Asia/Pacific Region	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
80.246.136.5	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
109.67.130.228	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.43.77.188	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.64.135.221	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
87.70.51.149	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.96.41	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.79.100	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.137.103	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
217.132.234.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.79.102	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.137.148	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
173.249.130.10	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
109.65.98.175	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.137.0	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.135.236	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
185.3.144.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.104	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.144.70	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
149.78.152.115	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.86.45	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
185.3.144.85	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
109.64.197.130	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
37.238.162.40	Iraq	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
149.78.195.30	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
188.120.154.71	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.238.162.40	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
68.180.229.89	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
185.3.144.28	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
216.145.17.190	United States	147.237.72.156	aman.idf.il	Header Rejection	header rejection pattern found in request	monitor	2
62.210.254.52	France	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
141.212.122.202	United States	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
212.181.203.11	Sweden	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
119.81.250.154	Hong Kong	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.120.156.193	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
169.229.3.91	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
37.26.148.185	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.243.31.2	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
66.249.82.91	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.167	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
202.14.148.78	Australia	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

04-20-2016-00:04:05 to 04-20-2016-01:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.126.90.180	Sweden	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	6
188.126.90.180	Sweden	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 188.126.90.180	Block	5
84.94.180.40	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/oprolescategory/oprolescategory.in.aspx	Block	3
66.249.82.94	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
213.8.46.2	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
64.207.180.204	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	2
54.174.60.113	United States	147.237.0.15	kosher-kravi.idf.i	Multiple Unauthorized URL Access from 54.174.60.113	Block	2
223.73.252.20	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
213.8.46.1	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
46.19.85.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
64.207.180.204	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 64.207.180.204	Block	2
95.86.116.99	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/	Block	2
107.77.68.63	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	Block	1
80.246.130.48	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
208.90.57.196	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
157.55.39.146	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/5/109335.pdfצבא-והצלחה	Block	1
95.86.116.99	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$LoginControl$captcha$captchaText in www.aka.idf.il/main/giyus/default.aspx	None	1
213.8.204.71	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
188.126.90.180	Sweden	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/index.php	Block	1
109.64.96.41	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
212.106.88.21	Palestinian Territory, Occupied	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/6/113596.pdf'	Block	1
64.207.180.204	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
5.22.134.215	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.78.252	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/apple-app-site-association	Block	1
54.174.60.113	United States	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to kosher-kravi.idf.il/shared/usercontrols/headerupper/	Block	1
194.28.112.52	Netherlands	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to 147.237.0.15/	Block	1
109.64.197.130	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
84.109.116.244	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
212.106.88.21	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 212.106.88.21	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
40.77.167.5	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/info.aspx	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
223.73.252.20	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 223.73.252.20	Block	1
64.207.180.204	United States	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
194.28.112.52	Netherlands	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
141.212.122.161	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
84.228.41.50	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.idf.il/1038-en/dover.aspx	Block	1
66.249.64.143	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/2/46962.pdf	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-10677-en	Block	1
79.180.29.244	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/bamahane	Block	1
223.73.252.20	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
194.28.112.52	Netherlands	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/hnap1/	Block	1
157.55.39.103	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-12522-he/dover.aspx	Block	1
46.121.104.234	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1

04-20-2016-00:04:05 to 04-20-2016-01:04:05