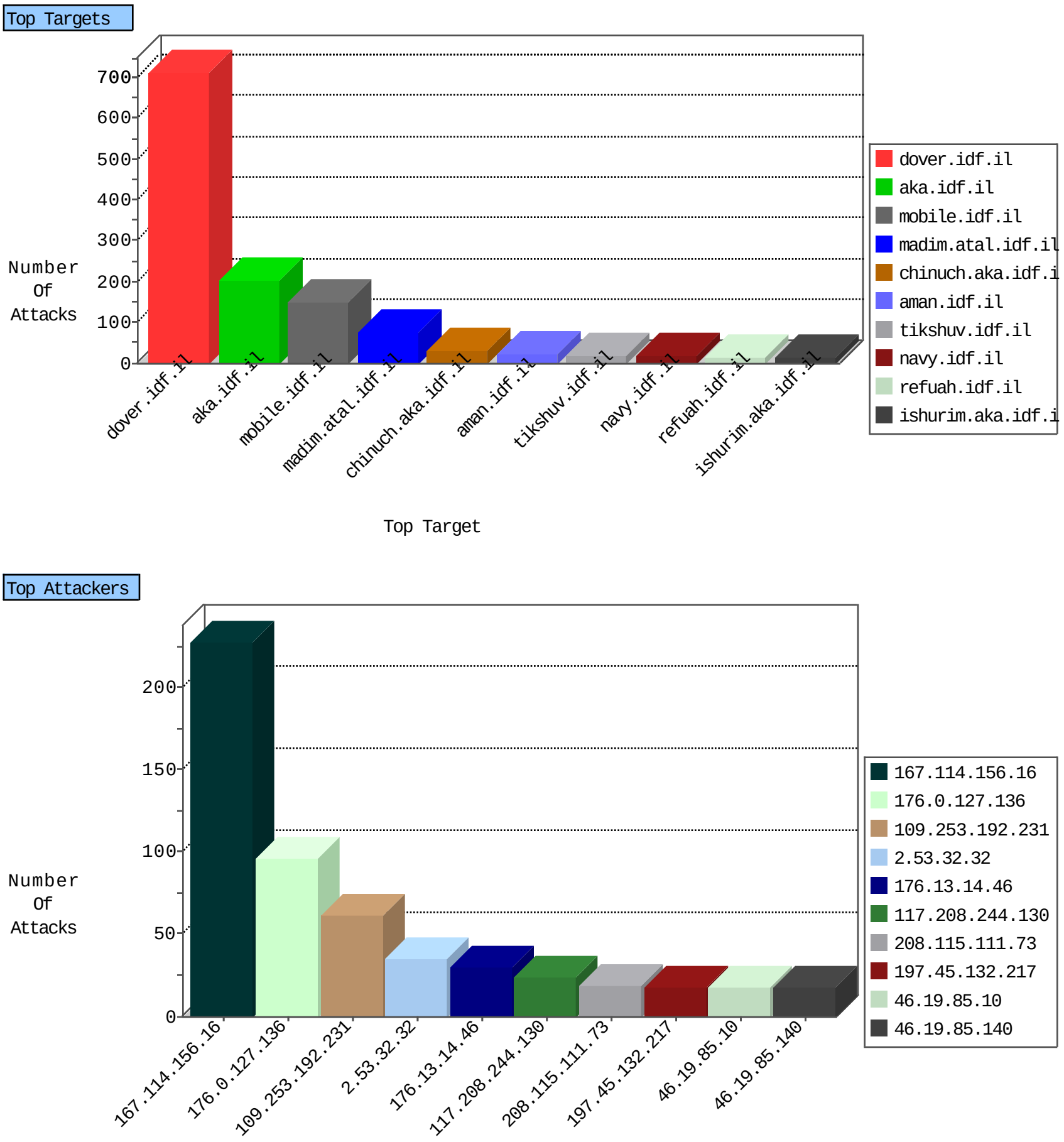
04-28-2016-12:04:01 to 04-28-2016-13:04:01

IDF Under Attack
Daily Report



04-28-2016-12:04:01 to 04-28-2016-13:04:01

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	8435
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	4332
192.115.200.249	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	113
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
185.103.252.96	Russian Federation	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1

04-28-2016-12:04:01 to 04-28-2016-13:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-28-2016-12:04:01 to 04-28-2016-13:04:01

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
174.37.194.144	147.237.76.201	United States	e.atal.idf.il	ET SCAN NMAP -sA (2)	2
149.88.164.70	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
174.37.194.144	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sA (2)	2
109.67.149.183	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.104	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
174.37.194.144	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -f -sS	1
104.154.119.160	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
89.248.167.131	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
183.3.202.115	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
79.183.48.179	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
183.3.202.115	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
66.249.78.158	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
183.3.202.115	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.151	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
42.114.176.102	147.237.76.199	Vietnam	e.nakchal.idf.il	ET SCAN NMAP -f -sS	1
174.37.194.144	147.237.76.201	United States	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.140.23	147.237.76.176	United Kingdom	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.248.167.131	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN Potential SSH Scan	1
80.82.78.38	147.237.72.14	Netherlands	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
183.3.202.115	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
79.177.207.110	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
183.3.202.115	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
174.37.194.144	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 2048	1
42.114.176.102	147.237.76.199	Vietnam	e.nakchal.idf.il	ET SCAN NMAP -sS window 2048	1

04-28-2016-12:04:01 to 04-28-2016-13:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.0.127.136	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	96
176.13.14.46	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
2.53.32.32	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
117.208.244.130	India	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	24
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
46.19.85.140	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
85.65.157.152	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
198.58.102.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
79.182.92.156	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
87.70.52.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.102.49	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
37.237.232.21	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
162.244.163.219	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
185.5.220.105	Palestinian Territory, Occupied	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	10
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
185.120.125.70	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.183.107.245	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
37.26.146.204	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.131	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
82.145.216.247	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
185.120.126.14	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	8
157.55.39.106	United States	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
109.253.224.31	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	8
5.102.254.82	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
2.242.84.149	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
83.244.6.239	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.10	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.9.11	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.148	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
92.78.124.182	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.102.242.173	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.10	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.53.38.198	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
50.116.28.209	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
207.46.13.2	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
5.102.254.82	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
213.57.240.232	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.26	Israel	147.237.77.216	dover.idf.il	Block HTTP Non Compliant		monitor	4
45.122.127.112	India	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4

04-28-2016-12:04:01 to 04-28-2016-13:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.192.231	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	62
109.65.208.210	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
2.53.32.32	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
79.182.92.156	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.131	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.140	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
176.13.11.76	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.92	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
87.68.245.30	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 87.68.245.30	Block	2
87.71.100.234	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/homepage/mobile	Block	2
79.182.23.76	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	2
87.68.245.30	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
207.46.13.137	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
5.153.233.130	Sweden	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
87.71.43.9	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/	Block	1
213.57.240.232	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.78.158	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
46.19.85.26	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version deflate, sdch	Block	1
164.132.161.73	Italy	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
92.51.199.202	Ireland	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/6/4616.jpg	Block	1
84.228.63.150	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 84.228.63.150	Block	1
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/site/unselecatble.aspx	Block	1
117.78.13.29	China	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
5.153.233.130	Sweden	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-login.php	Block	1
87.71.100.234	Israel	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/templates/general/mobile	Block	1
217.132.145.86	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: 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/	Block	1
46.19.85.26	Israel	147.237.77.216	dover.idf.il	Multiple Malformed URL from 46.19.85.26	Block	1
176.13.9.11	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
84.228.63.150	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
213.8.204.21	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/7/112217.pdfgoogli.org	Block	1
66.249.64.13	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
146.185.56.226	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/general/mobile	Block	1
40.77.167.9	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
87.71.100.234	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 87.71.100.234	Block	1
79.178.153.50	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/templates/general/mobile	Block	1
46.19.85.26	Israel	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 46.19.85.26	Block	1
109.67.98.51	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/	Block	1
213.8.204.34	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
157.55.2.139	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
41.32.172.181	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
185.120.125.70	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
109.253.159.162	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
2.53.38.198	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
213.8.204.66	Israel	147.237.77.74	law.idf.il	Parameter Type Violation SearchText in www.law.idf.il/657-en/patzar.aspx	Block	1
66.249.66.123	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/6/size100x0/3126.jpg	Block	1
46.19.85.26	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request request version	Block	1
157.55.39.209	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/â€•	Block	1
91.200.14.89	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-en/matpash.aspx/trackback/	Block	1

04-28-2016-12:04:01 to 04-28-2016-13:04:01