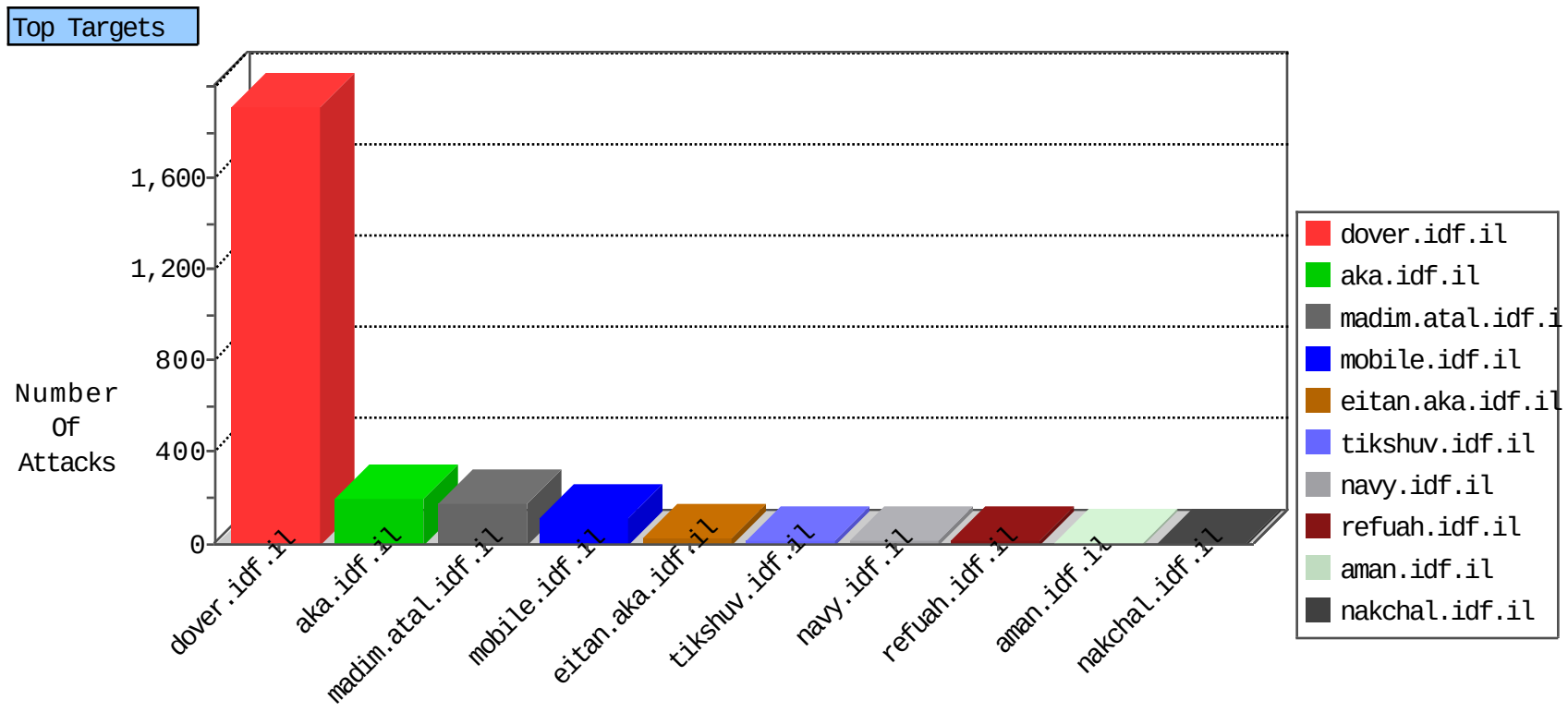
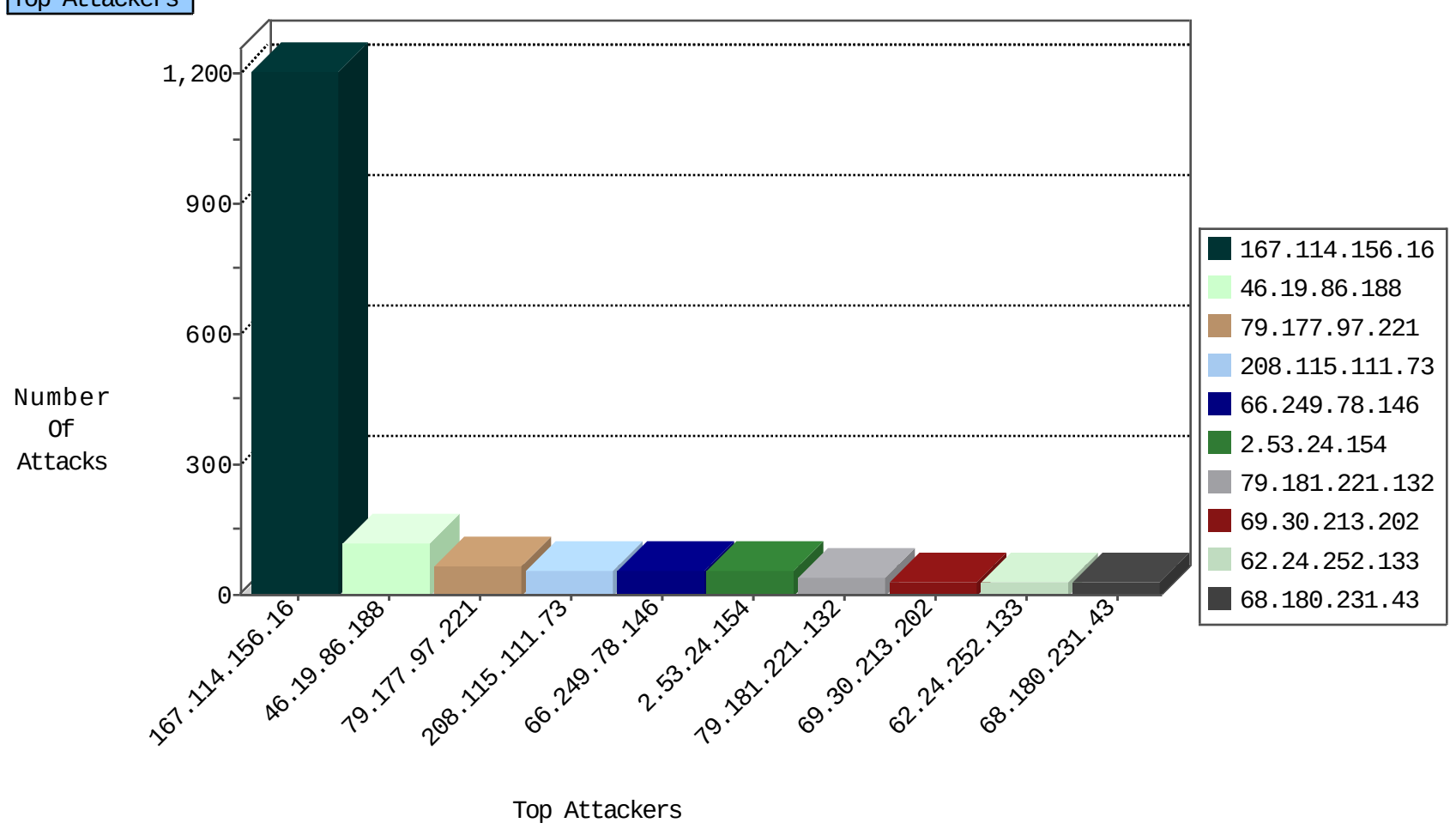
04-28-2016-20:04:07 to 04-28-2016-21:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-28-2016-20:04:07 to 04-28-2016-21:04:07

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	DOS-Tool-SwitchbladG	dest-reset	868
84.110.82.166	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
188.138.17.205	France	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
212.143.254.66	Israel	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
123.151.42.61	China	147.237.76.44	e.refuah.idf.il	JLM_Purple_Con_Limit_Udp	drop	1

04-28-2016-20:04:07 to 04-28-2016-21:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
24.71.248.218	Canada	147.237.76.31	nakchal.idf.i	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	8262: HTTP: Slowloris DoS Tool	Block	1

04-28-2016-20:04:07 to 04-28-2016-21:04:07

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
187.185.100.209	147.237.0.34	Mexico	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
183.60.48.25	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
180.97.106.36	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
104.219.238.10	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.8.14	Ukraine	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.77.227	Netherlands	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
66.240.213.93	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
190.153.238.58	147.237.0.17	Chile	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
180.97.106.161	147.237.8.45	China	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
176.53.0.79	147.237.72.14	Turkey	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.8.14	Ukraine	e.orchot.idf.il	ET SCAN NMAP -sS window 2048	1
91.201.236.155	147.237.8.14	Ukraine	e.orchot.idf.il	ET SCAN NMAP -f -sS	1
80.82.78.38	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
13.92.178.142	147.237.76.201	United States	e.atal.idf.il	ET SCAN NMAP -sS window 3072	1
190.153.238.58	147.237.72.14	Chile	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1

04-28-2016-20:04:07 to 04-28-2016-21:04:07

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	742
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
2.53.24.154	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
79.181.221.132	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
62.24.252.133	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
37.26.148.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
37.26.149.224	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
213.55.114.230	Ethiopia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
37.237.177.88	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
119.131.39.64	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
52.70.160.253	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.53.19.251	Israel	147.237.76.200	eitan.aka.idf..	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.177.97.221	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.103.114	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.158	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
207.46.13.137	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
52.70.178.172	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.158	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
66.249.93.115	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.158	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
109.253.224.63	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
69.30.213.202	United States	147.237.76.200	eitan.aka.idf..	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
79.181.35.26	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
138.91.55.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
52.70.181.32	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
52.70.181.44	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
52.29.21.27	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
41.210.129.101	Uganda	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
69.30.213.202	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
79.178.186.190	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.189	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
213.247.64.13	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.102.6.188	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
92.247.181.29	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.102.254.140	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.189	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
52.70.175.45	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.79	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6

04-28-2016-20:04:07 to 04-28-2016-21:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.188	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	119
79.177.97.221	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	53
79.181.221.132	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
37.26.149.224	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
52.70.180.16	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
52.3.106.144	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
46.19.85.95	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	3
52.70.158.226	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
185.32.179.16	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
52.70.178.172	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
79.180.169.66	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
199.30.24.90	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
52.70.181.32	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.253.224.63	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
79.177.97.221	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
54.210.12.89	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.120.168.168	Israel	147.237.72.166	aka.idf.il	Double URL Encoding - parameter: search in www.aka.idf.il/main/giyus/pniothandler1.asmx/search	Block	1
92.53.98.245	Russian Federation	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/old/wp-admin/	Block	1
23.91.70.36	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/test/wp-admin/	Block	1
68.180.229.154	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/5/109335.pdfצבא-ההצלה	Block	1
207.46.13.2	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.2	Block	1
157.55.39.106	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
39.44.191.54	Pakistan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1
51.255.65.44	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/golani/	Block	1
197.221.14.66	South Africa	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/wordpress/wp-admin/	Block	1
109.253.224.45	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
37.26.146.165	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/general/mobile	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1781-he/dover.aspx	Block	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
157.55.39.209	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.209	Block	1
45.55.181.223	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/894-he/tikshuv.aspxshared/usercontrols/headerupper/	Block	1
79.180.169.66	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.79.89	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.253.224.60	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
71.225.0.46	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
212.227.119.14	Germany	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/blog/wp-admin/	Block	1
157.55.39.209	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-16775-en/dover.aspx-title=chief	Block	1
66.249.79.89	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
52.70.108.216	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
199.30.24.135	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
37.26.149.245	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
52.70.181.44	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
164.132.161.27	Italy	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/prisha	Block	1
84.108.62.107	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl33 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed URL is Above Root Directory	Block	1
199.30.25.131	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
149.88.37.219	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main-sachar	Block	1
39.44.191.54	Pakistan	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1

04-28-2016-20:04:07 to 04-28-2016-21:04:07