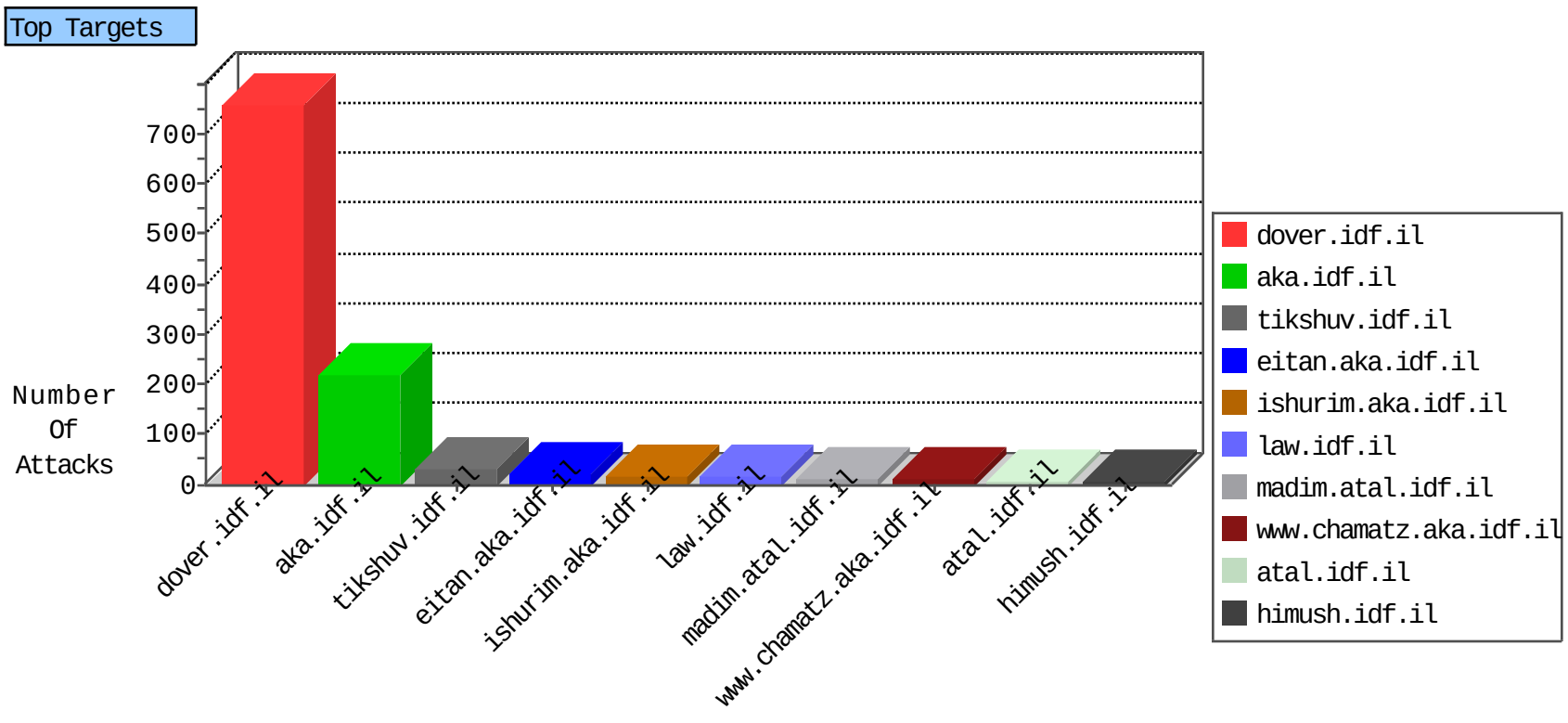
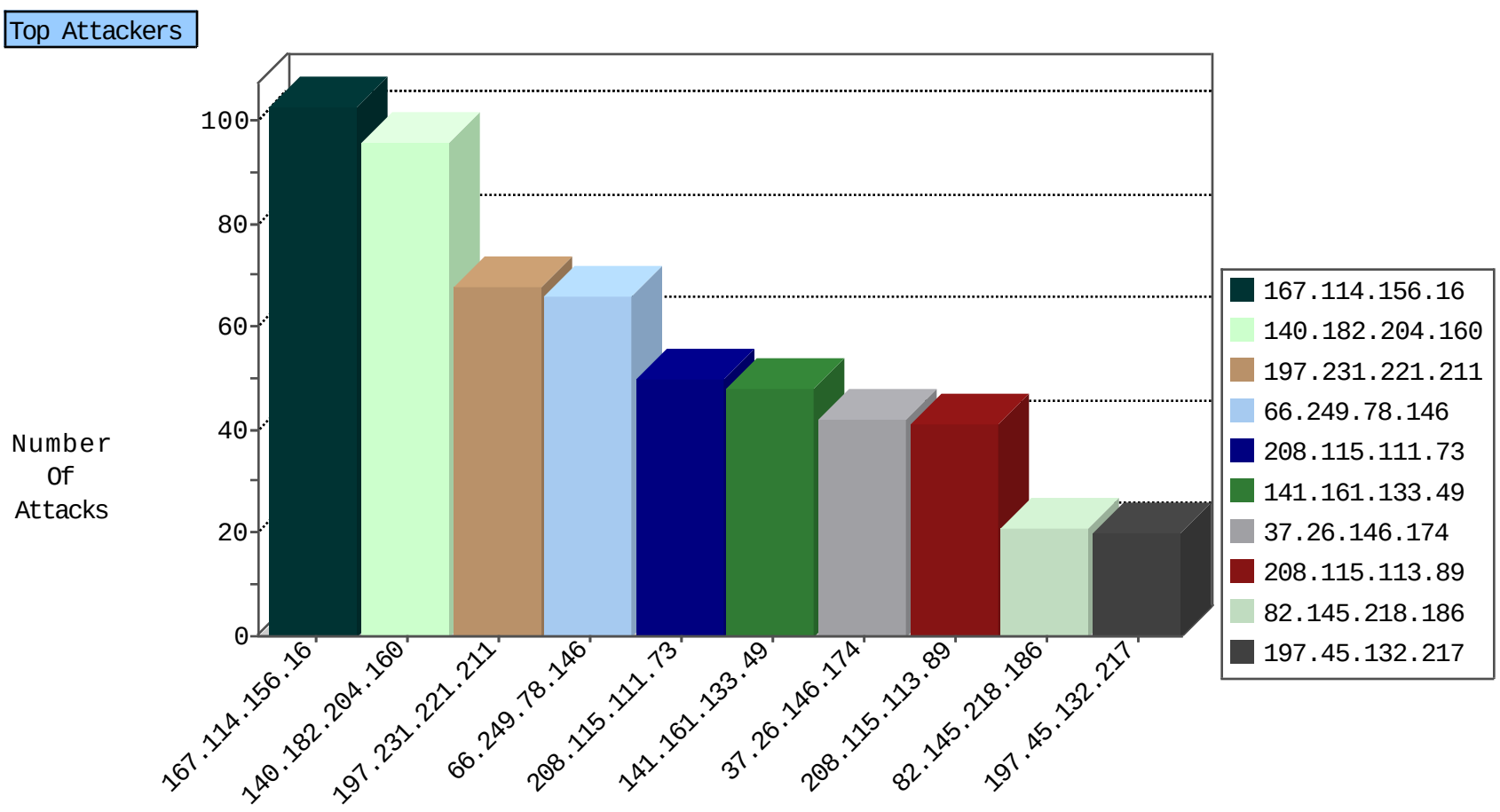
04-26-2016-22:04:04 to 04-26-2016-23:04:04

IDF Under Attack
Daily Report

Top Targets



Top Attackers



04-26-2016-22:04:04 to 04-26-2016-23:04:04

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	4583
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	105
180.153.91.183	China	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	5
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
109.64.39.18	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
80.70.128.129	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
123.59.59.52	China	147.237.77.233	atal.idf.il	block-sp-traf1	drop	1
38.229.1.13	United States	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1	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
62.210.107.57	France	147.237.0.200	m4u.idf.il	JLM_Purple_Con_Limit_Http	drop	1
94.102.49.116	Netherlands	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
66.240.192.138	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1

04-26-2016-22:04:04 to 04-26-2016-23:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-26-2016-22:04:04 to 04-26-2016-23:04:04

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
39.49.19.166	147.237.77.74	Pakistan	law.idf.il	Xenu Link Sleuth User Agent	4
185.3.144.38	147.237.77.216	Israel	dover.idf.il	GPL SCAN myscan	2
185.3.144.38	147.237.77.216	Israel	dover.idf.il	INDICATOR-SCAN myscan	2
222.186.42.248	147.237.0.33	China	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
13.92.103.193	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
109.235.254.181	147.237.8.27	Turkey	e.madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
104.215.90.42	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 3072	1
104.171.122.176	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
82.117.208.243	147.237.77.176		matpash.idf.il	ET SCAN NMAP -sS window 1024	1
66.240.213.93	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.42.248	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
13.92.103.193	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
208.80.155.214	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	1
13.92.103.193	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -f -sS	1
109.235.254.181	147.237.8.27	Turkey	e.madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1
104.219.238.10	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
104.215.90.42	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
104.171.122.176	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
80.82.78.38	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1

04-26-2016-22:04:04 to 04-26-2016-23:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
140.182.204.160	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	96
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	67
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	66
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
141.161.133.49	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
37.26.146.174	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
82.145.218.186	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	21
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
95.86.83.56	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
109.253.203.113	Israel	147.237.72.166	aka.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	14
64.14.237.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
207.46.13.49	United States	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
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
212.179.212.59	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.55.138.160	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.103.91	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
37.237.193.48	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.64.233	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
198.58.102.158	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
207.46.13.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
5.22.129.85	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
66.249.66.190	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
92.247.181.31	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.175	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
82.81.27.137	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.85.123	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.76.123.213	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
157.55.39.147	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.67.209.246	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
89.145.95.42	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
93.173.23.134	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
82.81.27.137	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.85.123	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
185.3.144.38	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.181.149.70	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
203.133.169.231	Korea, Republic of	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
87.71.14.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.161.207	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.245	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.81.27.137	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.76.101.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.118.156.3	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1556-en/	Block	5
2.53.25.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.78.147	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	2
2.53.163.3	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
52.12.235.71	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/newsite/english/main.asp	Block	1
212.199.143.202	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
149.50.2.79	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
79.179.152.33	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	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
5.29.105.160	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/mobile	Block	1
187.20.215.252	Brazil	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 187.20.215.252	Block	1
89.138.110.245	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/4/	Block	1
68.180.229.24	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/templates/shared/usercontrols/navmenu/	Block	1
54.210.18.124	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
151.80.31.176	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/giyus/asp/rec.asp	Block	1
80.18.127.118	Italy	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.66.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/2391.jpg	Block	1
5.39.222.159	Netherlands	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
187.20.215.252	Brazil	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/	Block	1
93.115.95.216	Anonymous Proxy	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
68.180.229.89	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/תאתר	Block	1
54.214.136.228	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/newsite/english/main.asp	Block	1
157.55.39.147	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
80.178.120.14	Israel	147.237.72.166	aka.idf.il	Post Request - Missing Content Type	Block	1
66.249.78.130	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/navy/searchpage.aspx	Block	1
109.72.215.18	United Kingdom	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/index.php	Block	1
77.124.7.38	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined	Block	1
65.55.210.220	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
164.132.161.78	Italy	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/movies/yassin7.	Block	1
80.178.120.14	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/general.aspx	Block	1
51.255.65.67	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/shared/usercontrols/headerupper/	Block	1
212.179.212.59	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	1
149.50.2.79	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 149.50.2.79	Block	1
79.179.152.33	Israel	147.237.77.234	halag.idf.il	Parameter Type Violation search in www.logistics.atal.idf.il/1213-he/halag.aspx	Block	1
65.208.151.116	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/4/	Block	1
176.13.2.67	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
89.138.110.245	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized HTTP Method	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/sachar/faq.aspx	Block	1

04-26-2016-22:04:04 to 04-26-2016-23:04:04