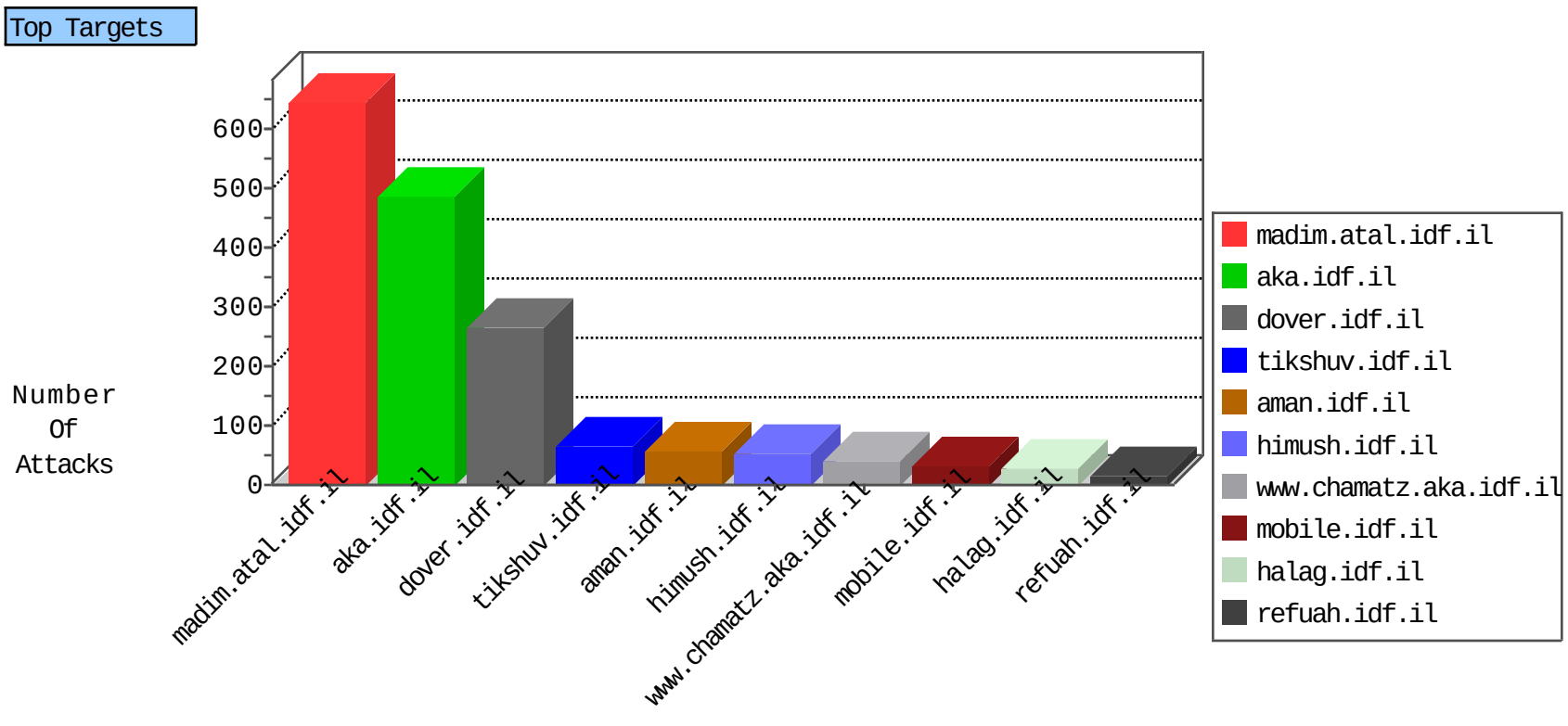
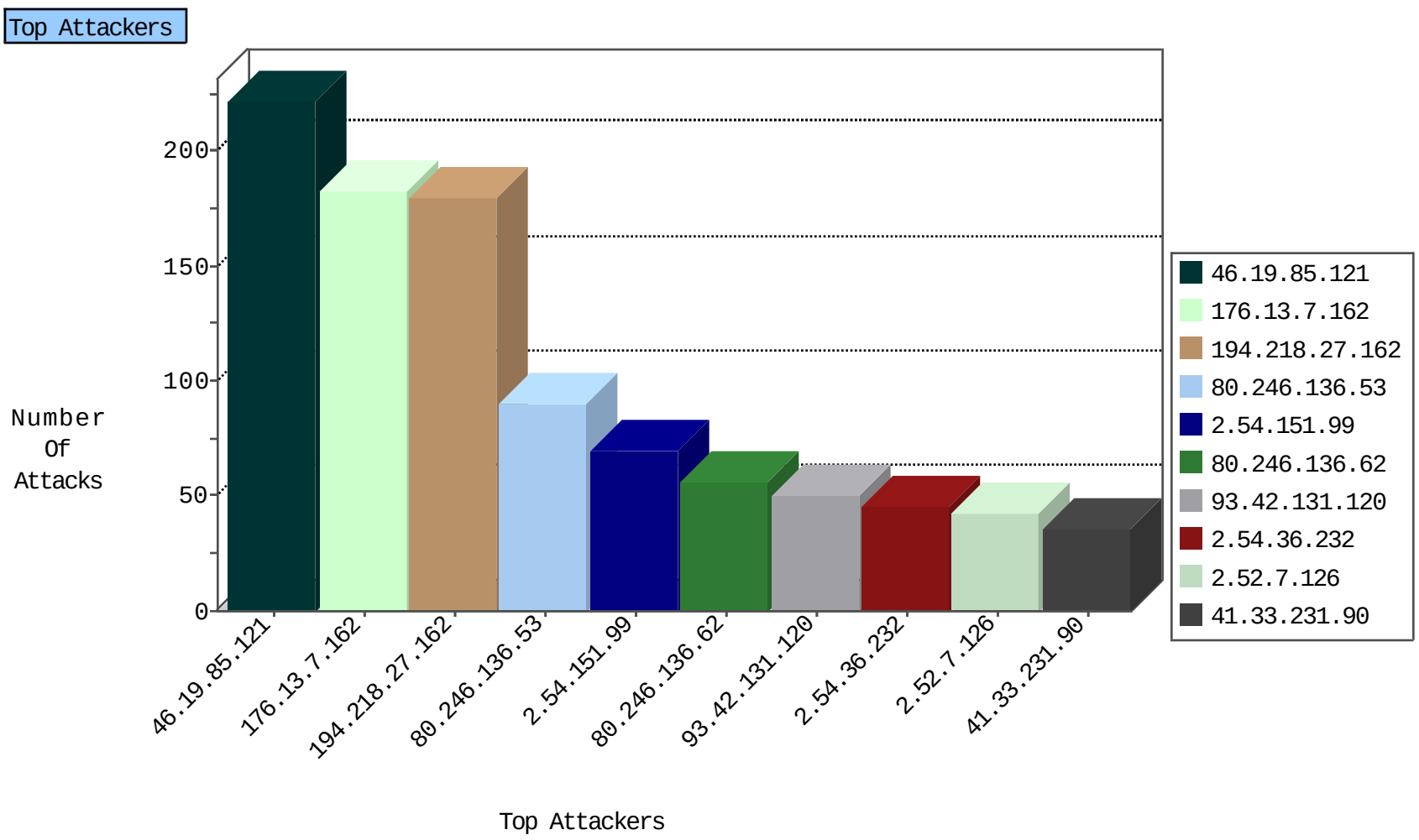
03-02-2016-18:04:02 to 03-02-2016-19:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-02-2016-18:04:02 to 03-02-2016-19:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.151.99	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	27
80.246.138.18	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
176.13.2.33	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
218.93.12.219	China	147.237.72.167	ishurim.aka.idf.il	Invalid TCP Flags	drop	2
59.63.77.94	China	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	1
68.235.61.11	United States	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
85.25.207.231	Germany	147.237.77.121	e.navy.idf.il	Block_Udp_All_Nets	drop	1
59.63.77.94	China	147.237.0.35	akaws.idf.il	Block_Udp_All_Nets	drop	1
68.235.61.11	United States	147.237.77.178	e.matpash.idf.il	Block_Ntp_All_Net	drop	1
110.159.104.106	Malaysia	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
68.235.61.11	United States	147.237.0.19	madim.atal.idf.il	Block_Ntp_All_Net	drop	1
68.235.61.11	United States	147.237.8.27	e.madim.atal.idf.il	Block_Ntp_All_Net	drop	1

03-02-2016-18:04:02 to 03-02-2016-19:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.78.96.54	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
84.108.9.229	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
87.71.90.252	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
46.19.86.230	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
213.57.209.45	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
109.65.110.16	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
109.253.158.198	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
131.253.25.226	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
176.13.14.163	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
212.235.40.29	Israel	147.237.77.216	dover.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-02-2016-18:04:02 to 03-02-2016-19:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
52.48.63.203	147.237.72.166	United States	aka.idf.il	Tehila - Perl LWP with fake user agent	6
77.127.157.235	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.105.134.220	147.237.76.198	Sweden	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
179.154.165.244	147.237.0.34	Brazil	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
5.29.167.68	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.234.124.164	147.237.77.234	Germany	halag.idf.il	ET SCAN NMAP -sS window 1024	1
2.54.3.37	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.171.122.167	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.193	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
89.139.50.95	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.183.149.199	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.176.158.31	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.74	147.237.77.205	United States	prisha.idf.il	ET DROP Dshield Block Listed Source	1
73.76.40.41	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
179.154.165.244	147.237.76.42	Brazil	refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
50.87.144.145	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
132.69.198.157	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.151.99	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
106.78.188.60	147.237.76.44	India	e.refuah.idf.il	GPL SCAN nmap TCP	1
94.102.48.193	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
89.139.142.131	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.108.160.17	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.227.127	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.3.45.125	147.237.76.42	China	refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

03-02-2016-18:04:02 to 03-02-2016-19:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	120
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	60
93.42.131.120	Italy	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	50
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
2.54.151.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
87.71.77.28	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	23
66.249.81.144	United States	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	19
66.249.81.148	United States	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	13
68.105.166.106	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.210.219.83	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
2.52.7.126	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
79.180.127.122	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.151.99	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
46.19.86.98	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
79.177.151.124	Israel	147.237.76.147	chinuch.aka.idf.il	drop	First packet isn't SYN	drop	8
2.52.7.126	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
2.52.7.126	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
185.3.144.99	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
185.3.147.238	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
66.249.81.152	United States	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	6
79.182.183.233	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
77.126.209.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.156.135	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
188.161.186.44	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.86.241	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	6
109.253.129.237	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.147	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
188.161.186.44	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
2.52.7.126	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	5
162.129.251.19	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
37.163.54.135	France	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.52.7.126	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
185.3.147.20	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.10.28	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
188.120.148.255	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.40.161	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
37.163.54.135	France	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
81.192.111.212	Morocco	147.237.77.216	dover.idf.il	drop		drop	4
85.64.112.17	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.52.7.126	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
89.139.145.95	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
109.65.110.16	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.54.50.132	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.4.13	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.215.203	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.64.11.8	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
109.66.16.77	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.164.202	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
46.19.85.36	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3

03-02-2016-18:04:02 to 03-02-2016-19:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.121	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	222
176.13.7.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	173
80.246.136.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	90
80.246.136.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	56
2.54.36.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	43
109.160.142.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
2.54.156.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
52.48.63.203	United States	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	8
52.48.63.203	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 52.48.63.203	Block	7
46.118.158.214	Ukraine	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	6
46.118.158.214	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.118.158.214	Block	5
37.26.148.160	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
109.253.194.249	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
199.30.24.145	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
176.13.8.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.178.98.12	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	3
37.26.148.160	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	2
149.78.59.121	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	2
81.218.241.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.26	Block	2
2.54.28.37	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
157.55.39.81	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
37.26.148.160	Israel	147.237.0.19	madim.atal.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.19.85.36	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
79.181.4.13	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
188.120.152.217	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
140.123.101.42	Taiwan	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
37.26.148.160	Israel	147.237.76.39	mobile.meitav.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.64.12.5	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
213.151.62.104	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/71804-he/maarachot.aspx&sa=u&ved=0ahukewj_5m3bu6llahxb7a4khxpaa5uqfgggmak&usg=afqjcnh_rgasmwcw42tir4byhqfrgpozrg	Block	1
46.19.85.110	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files	Block	1
95.86.101.5	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-21253-he/idfgdover.aspx&sa=u&ved=0ahukewi0wfbatkllahxdbswkhrgyctkqfggpmai&usg=afqjcnhvb6z831le-179ylcsf6iihgngnw	Block	1
2.54.150.181	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
79.183.59.19	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
142.54.166.170	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1927-en/cogat.aspxgazasemanales	Block	1
46.118.158.214	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/index.php	Block	1
109.65.60.210	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/requestpayslipexplanation.aspx	None	1
2.52.6.199	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
81.218.241.26	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/images/1.he/topcap.gif	Block	1
66.249.64.176	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/1464-he/אגף הטכנולוגיה והל וגיסטיקה.aspx	Block	1
109.253.220.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
95.86.115.144	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
207.46.13.101	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
46.121.111.141	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 46.121.111.141 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
37.142.64.106	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.66.25	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
185.32.179.246	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	1
114.40.114.154	Taiwan	147.237.72.166	aka.idf.il	Admin Blocking	Block	1
46.117.123.149	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl51 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
95.141.29.55	Luxembourg	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/band	Block	1

03-02-2016-18:04:02 to 03-02-2016-19:04:02