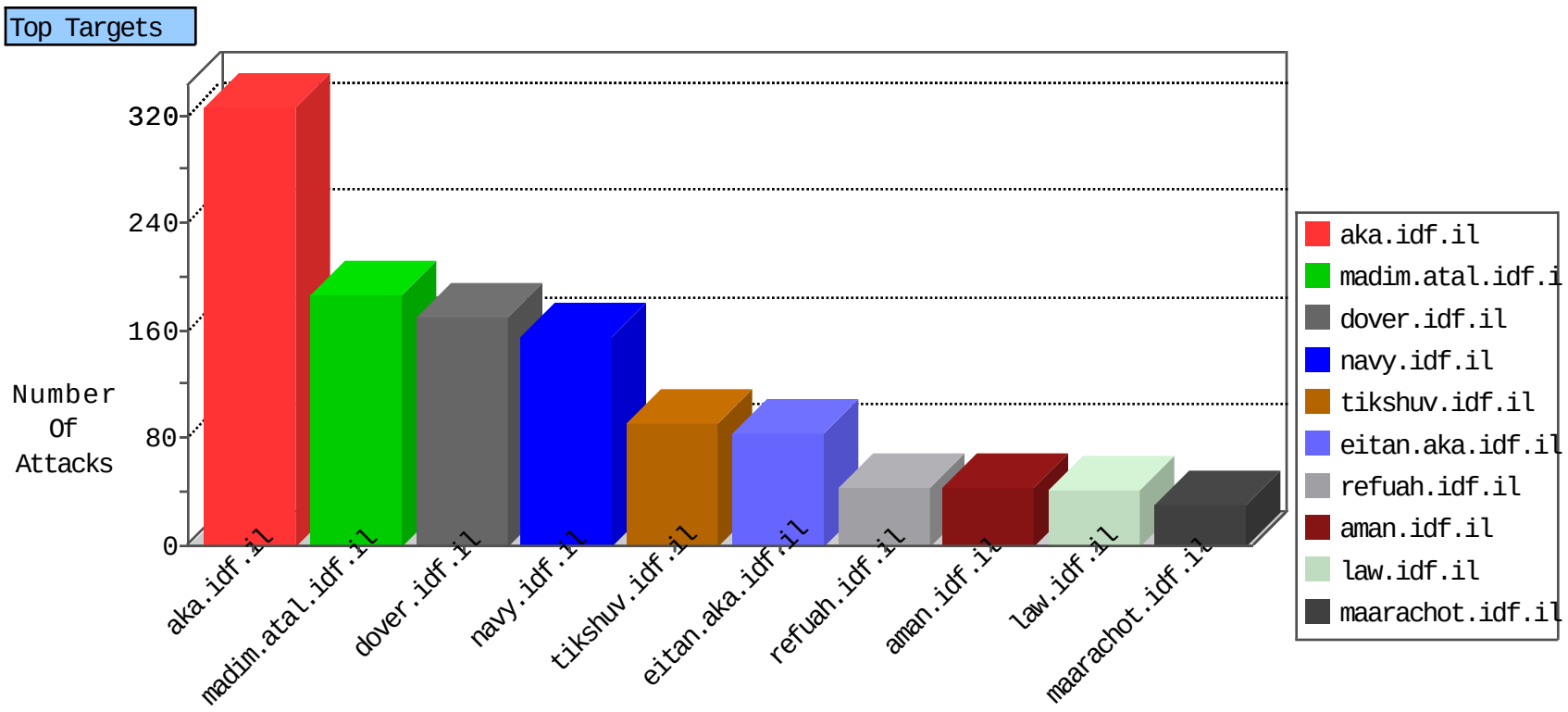
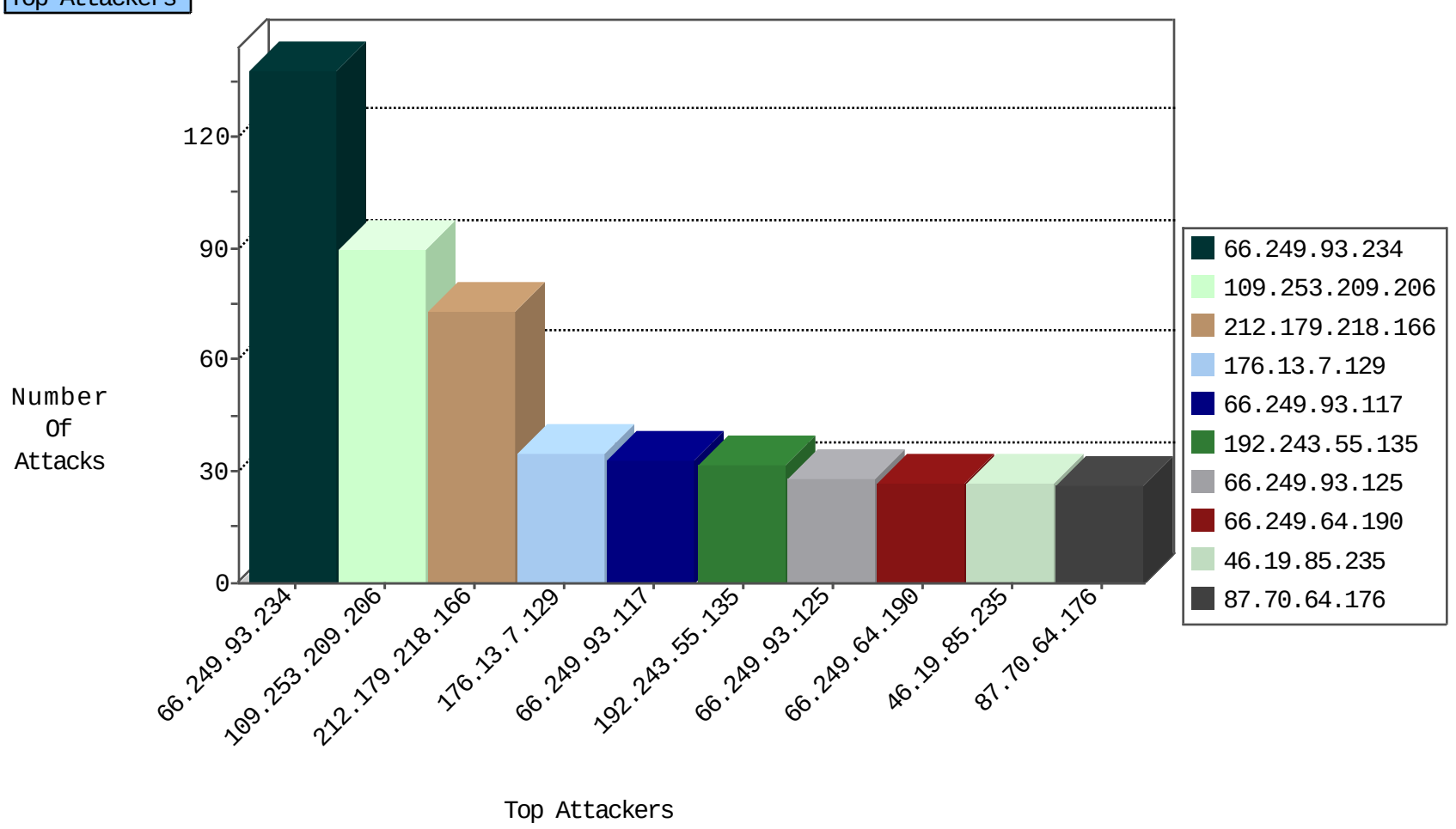
03-03-2016-16:04:06 to 03-03-2016-17:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-03-2016-16:04:06 to 03-03-2016-17:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
79.181.125.32	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
82.145.222.190	Europe	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	5
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
119.93.11.243	Philippines	147.237.0.200	m4u.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
12.152.75.6	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
164.132.54.194	Italy	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
164.132.54.194	Italy	147.237.77.74	law.idf.il	Block_Ntp_All_Net	drop	1
124.232.150.230	China	147.237.77.61	e.cogat.idf.il	Block_Udp_All_Nets	drop	1
79.181.117.197	Israel	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
164.132.54.194	Italy	147.237.77.234	halag.idf.il	Block_Ntp_All_Net	drop	1
115.77.103.234	Vietnam	147.237.8.46	e.chinuch.idf.il	Block_Udp_All_Nets	drop	1
164.132.54.194	Italy	147.237.8.14	e.orchot.idf.il	Block_Ntp_All_Net	drop	1
176.13.9.223	Israel	147.237.72.166	aka.idf.il	DOSS-SSL-ClearText	drop	1
115.239.228.10	China	147.237.0.34	tikshuv.idf.il	JLM_Purple_Con_Limit_Http	drop	1

03-03-2016-16:04:06 to 03-03-2016-17:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.154	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
176.36.80.39	Ukraine	147.237.72.156	aman.idf.il	C1000074: HTTP: majestic bot	Block	3
2.54.142.222	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	2
2.54.159.100	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	2
46.19.86.95	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	2
144.76.29.162	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
144.76.29.162	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
157.55.2.139	United States	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	2
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
157.55.39.210	United States	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	1
212.31.103.50	Cyprus	147.237.77.216	dover.idf.il	12347: HTTP: PHP-CGI Query String Parameter Information Disclosure Vulnerability	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-03-2016-16:04:06 to 03-03-2016-17:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.93.234	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	138
188.120.157.84	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
112.204.24.124	147.237.77.216	Philippines	dover.idf.il	portscan: TCP Distributed Portscan	2
79.182.233.128	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.8.204.55	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.76.39	United States	mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
37.26.147.202	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.145.149	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
137.226.113.7	147.237.76.147	Germany	chinuch.aka.idf.il	ET SCAN Suspicious User-Agent Containing Web Scan/er, Likely Web Scanner	1
95.86.126.119	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.109.9.195	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.81.84.202	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.132.149.16	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.182.39.252	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.149.180	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.74	147.237.76.42	United States	refuah.idf.il	ET DROP Dshield Block Listed Source	1
37.26.146.233	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
177.141.42.13	147.237.0.35	Brazil	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
1.62.116.156	147.237.76.34	China	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
130.211.152.118	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
109.64.179.124	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.248.174.37	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
82.81.163.138	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

03-03-2016-16:04:06 to 03-03-2016-17:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.179.218.166	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
66.249.93.117	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	33
66.249.93.125	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	28
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
80.246.133.37	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
46.116.26.190	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
66.249.93.121	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	17
2.54.59.21	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
2.54.145.149	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.1.206	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.173	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
2.52.45.220	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.19.86.70	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	10
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.235	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
77.125.116.16	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.182.134.173	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.179.218.166	Israel	147.237.76.200	eitan.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.102.9.115	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	7
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
109.67.136.153	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.235	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.183.38.64	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.221.86	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.1.5	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.130.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.215.178	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.235	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.97	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.45.220	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.235	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.178.191.183	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.161	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
188.120.154.203	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.116.96.156	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
192.243.55.133	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.6	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.52.48.241	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.173	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.146.177	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
212.179.218.166	Israel	147.237.76.200	eitan.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.86.181	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.102.254.116	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
82.80.179.140	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
199.203.111.183	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.235.47	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.209.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	87
176.13.7.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
87.70.64.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
46.19.86.229	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 46.19.86.229	Block	22
109.253.136.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
66.249.64.190	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.190	Block	14
109.253.223.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
192.115.64.250	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 192.115.64.250	Block	5
81.218.97.45	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	5
37.26.149.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
81.218.97.45	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 81.218.97.45	Block	3
82.80.179.140	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
118.193.161.67	China	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 118.193.161.67	Block	2
46.19.85.51	Israel	147.237.76.39	mobile.meitav.idf.il	Distributed Suspicious Response Code	Block	2
46.117.116.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
87.69.210.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
213.151.32.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
208.115.113.89	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1065-en/dover.aspx	Block	1
79.182.134.173	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.64.190	United States	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/shalishut/site/faq.aspx	None	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	Multiple Unknown HTTP Request Method from 169.229.3.91	Block	1
46.43.96.119	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.52.40.16	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.151.60.207	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/994-9050-he/atal.aspx&sa=u&ved=0ahukewizq6yi3ktlahwknpokhya8agiqqoubccywbq&sig2=ro4a39c5-jb67qmu_fpodq&usg=afqjcnevkby_ltgkmtejoas1waf8hgsodg	Block	1
66.249.66.176	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/7/307.pdf	Block	1
149.88.150.162	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/1070-he/nakhal.aspx	Block	1
66.249.64.190	United States	147.237.72.166	aka.idf.il	Unknown Parameter catI.. in www.aka.idf.il/main/giyus/general.aspx	None	1
109.186.163.32	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1065-he/dover.aspx	Block	1
80.246.133.37	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.64.190	United States	147.237.72.166	aka.idf.il	Unknown Parameter itemid in www.aka.idf.il/kamlar/gallery/showpicture.asp	None	1
46.116.26.190	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
84.108.77.157	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$85 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
5.29.171.117	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/sachar/	Block	1
192.115.64.250	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1384-he/dover.aspx	Block	1
157.55.39.152	United States	147.237.77.233	atal.idf.il	Abnormally Long Request URL	Block	1
66.249.64.190	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/giyus/leshakot/default.asp	None	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1133-he/dover.aspx	Block	1
66.249.64.233	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-13959-he/dover.aspxהגדוד	Block	1
185.25.148.240	Poland	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to testp2.czar.bielawa.pl/testproxy.php	Block	1
130.193.50.33	Russian Federation	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/8/638.pdf	Block	1
8.18.120.151	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
207.46.13.101	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
76.24.62.130	United States	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
66.249.64.190	United States	147.237.72.166	aka.idf.il	Unknown Parameter d.. in www.aka.idf.il/giyus/general/	None	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	Abnormally Long Request method	Block	1
212.179.21.194	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl23 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.66.69	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/29022011yezu.aspx	Block	1
185.25.148.240	Poland	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to testp3.pospr.waw.pl/testproxy.php	Block	1