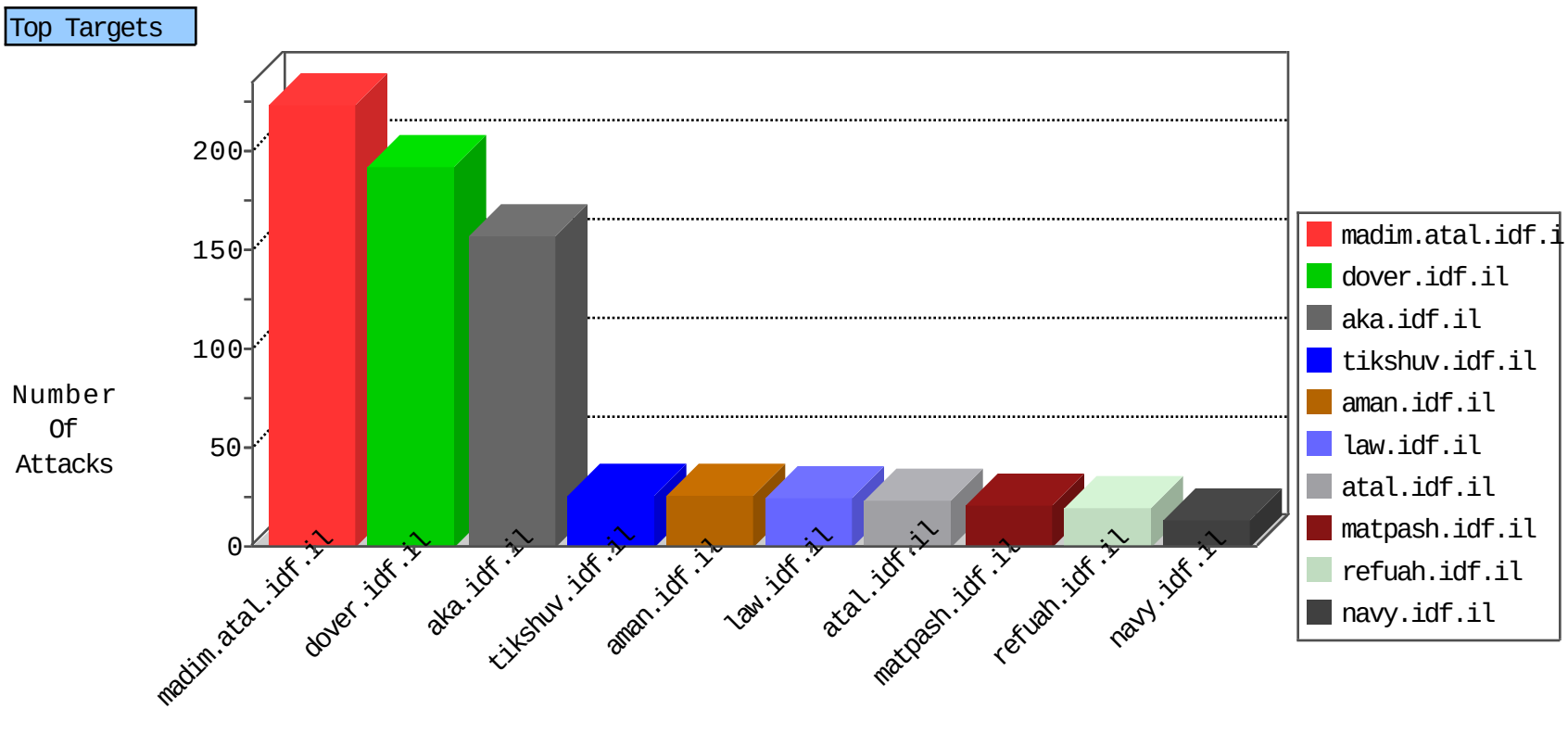
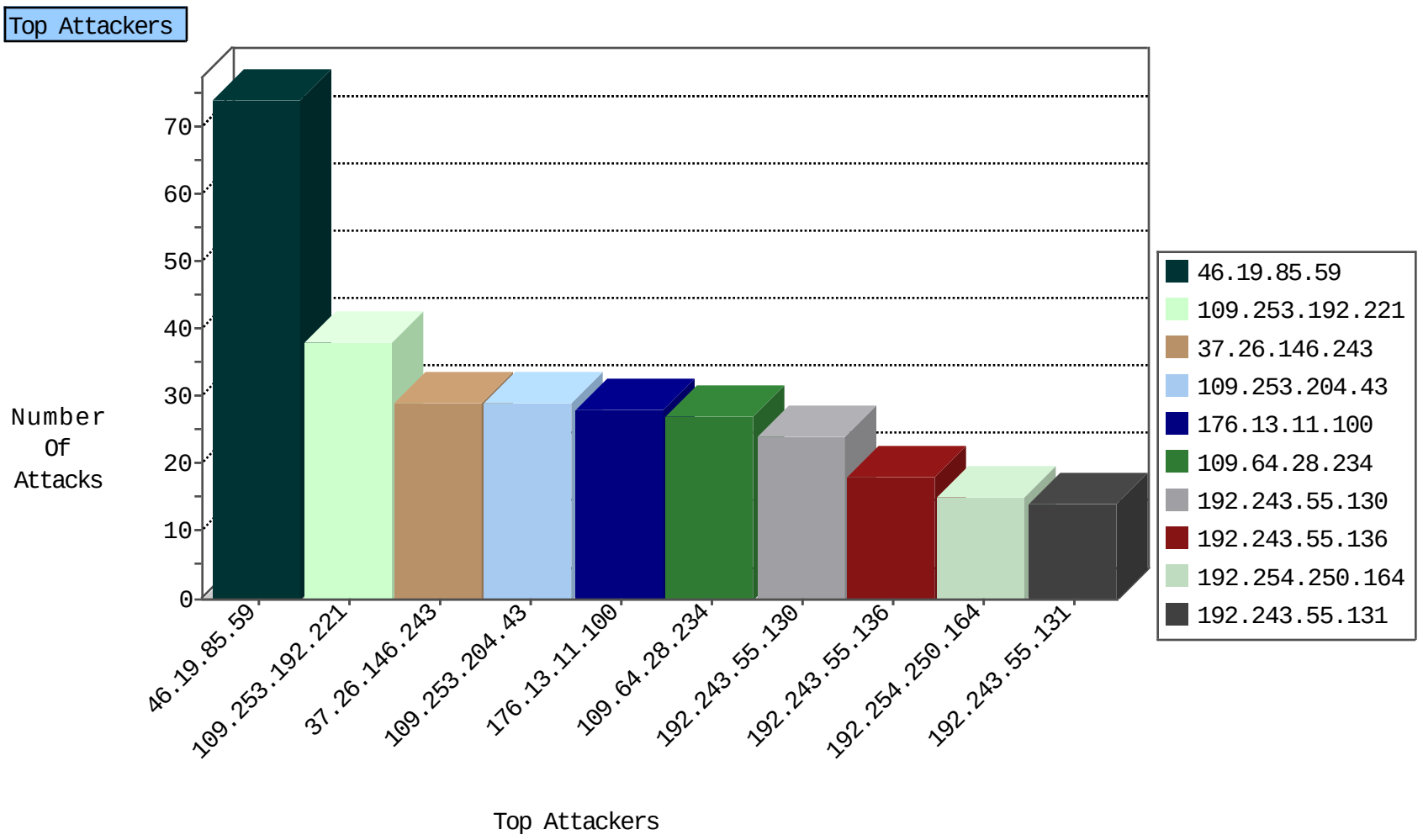
03-09-2016-08:04:07 to 03-09-2016-09:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-09-2016-08:04:07 to 03-09-2016-09:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.139.53	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	65
109.64.28.234	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	17
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	8
176.13.11.21	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
212.179.64.162	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
80.74.102.34	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
216.218.206.67	United States	147.237.8.24	e.lifestyle.idf.i	Block_Udp_All_Nets	drop	1
71.6.216.41	United States	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
23.228.107.104	United States	147.237.8.14	e.orchot.idf.il	Block_Ntp_All_Net	drop	1
184.105.247.219	United States	147.237.8.45	e.eitan.idf.il	Block_Udp_All_Nets	drop	1
23.228.107.104	United States	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1

03-09-2016-08:04:07 to 03-09-2016-09:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.29.131.168	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
176.13.1.181	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
37.26.149.234	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
66.249.66.190	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
69.30.214.38	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	2
79.177.115.236	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	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

03-09-2016-08:04:07 to 03-09-2016-09:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
209.126.116.147	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
176.13.1.181	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.199.213	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.193	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
81.218.190.42	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
40.121.136.51	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
216.170.120.121	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
176.13.21.174	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
139.196.57.234	147.237.77.205	China	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
109.186.50.192	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.174.93.181	147.237.8.28	Netherlands	e.mobile-ks.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.19.85.155	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

03-09-2016-08:04:07 to 03-09-2016-09:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
192.254.250.164	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	15
46.19.85.188	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
111.199.82.251	China	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
62.0.200.215	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
46.19.86.186	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
185.32.179.184	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.137	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.217.108	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.12.91	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.100	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.46.41.111	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.179.53.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.217.108	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
62.0.200.170	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
37.26.147.195	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
87.69.48.74	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.64.28.234	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
2.54.10.128	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
87.69.48.74	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
109.64.28.234	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.147.197	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
192.243.55.132	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.86.56	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
109.65.189.99	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.94.121.186	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.188.234	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
106.39.60.188	China	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
2.54.7.24	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.243	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
147.236.238.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.191.172	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.147.210	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
213.8.204.16	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
2.53.10.138	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.80.139.237	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
109.253.210.134	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
46.19.86.229	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.7.202	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.136.58	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
37.26.148.211	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.177.179.13	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.215.224	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

03-09-2016-08:04:07 to 03-09-2016-09:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	74
109.253.192.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	38
109.253.204.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
176.13.11.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	28
37.26.146.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	27
2.52.138.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
176.13.4.123	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
109.253.144.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
192.115.252.2	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.115.252.2	Block	3
109.65.61.107	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 109.65.61.107	Block	3
46.19.86.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.146.243	Israel	147.237.0.19	madim.atal.idf.il	Untraceable SSL Sessions: Open Mode	None	2
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
80.179.9.7	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
183.206.165.99	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/editorold/editor/	Block	1
46.19.85.137	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
84.109.90.4	Israel	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
207.46.13.187	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/smalim/faq.aspx	None	1
66.249.64.51	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/size100x0/3250.jpg	Block	1
183.206.173.99	China	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/editorold/editor/	Block	1
157.55.39.93	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
109.65.161.65	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationexplanation.aspx	None	1
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/getfile.aspx?filename=xhllytaxltawms5kb2m=&infocenteritem=true	Block	1
80.179.9.115	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
183.206.165.99	China	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 183.206.165.99	Block	1
109.253.209.64	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
84.109.90.4	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
212.68.157.162	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	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
185.89.217.231		147.237.76.86	navy.idf.il	URL is Above Root Directory www.navy.idf.il/../images/shared/home.png	Block	1
109.65.161.65	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$employmentStatesMonth in www.aka.idf.il/main/sachar/payslips.aspx	None	1
192.243.55.136	Dominica	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/getfile.aspx?filename=xgf5b3nolwrvy3ncdghpa2fcdhphdmltxdewodcuzg9j&infocenteritem=true	Block	1
80.179.223.31	Israel	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	1
46.120.76.200	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$38 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
183.206.165.99	China	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 183.206.165.99	Block	1
111.199.82.251	China	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/usercontrols/headerupper/	Block	1
87.70.33.152	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	1
212.179.159.253	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/סו'ג	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1399-en/dover.aspx	Block	1
193.201.227.152	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1044-he/ishurim.aspx	Block	1
81.218.136.207	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/moreinfo/tichnun.yosh@gmail.com	Block	1
46.121.136.206	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ishurim/mai	Block	1
183.206.173.99	China	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 183.206.173.99	Block	1
2.54.188.92	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
141.212.122.209	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/	Block	1
95.86.83.206	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1086-20722-he/dover.aspx&sa=u&ved=0ahukewio_n2ngbplahvdipokhclcbsyqfggtmai&usg=afqjcnf5embshtqth8k1egco9nl8punkba	Block	1
217.69.133.10	Russian Federation	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
192.115.252.2	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/doctrine/doctrine.stm"	Block	1
183.206.165.99	China	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 183.206.165.99	Block	1

03-09-2016-08:04:07 to 03-09-2016-09:04:07