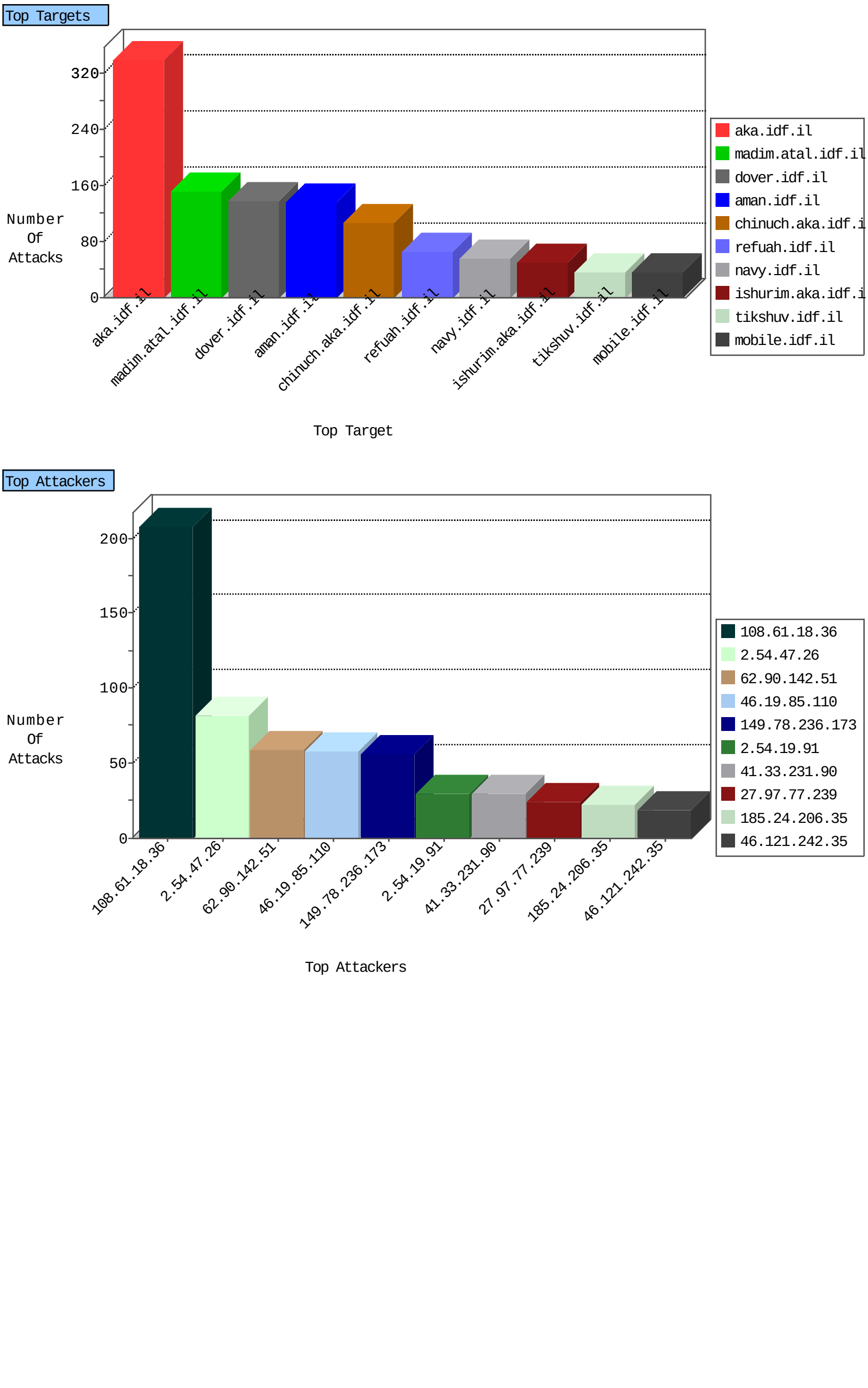
02-11-2016-19:04:01 to 02-11-2016-20:04:01

IDF Under Attack
Daily Report



02-11-2016-19:04:01 to 02-11-2016-20:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
185.94.111.1		147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
1.33.83.219	Japan	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
74.91.28.58	United States	147.237.77.205	prisha.idf.il	block-sp-traf1	drop	1
185.130.5.224		147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1

02-11-2016-19:04:01 to 02-11-2016-20:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
31.168.13.78	Israel	147.237.72.166	aka.idf.il	C008: HTTP: Xenu UserAgent	Block	1
31.168.13.78	Israel	147.237.76.86	navy.idf.il	C008: HTTP: Xenu UserAgent	Block	1
31.168.13.78	Israel	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
155.94.254.143	United States	147.237.77.176	matpash.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1
188.165.15.129	France	147.237.0.34	tikshuv.idf.il	C228: HTTP: AhrefBot crawler	Block	1

02-11-2016-19:04:01 to 02-11-2016-20:04:01

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
37.161.157.142	147.237.77.216	France	dover.idf.il	ET SCAN NMAP -sA (2)	2
2.54.16.164	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
180.97.106.161	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.36	147.237.77.243	China	mobile.idf.il	ET SCAN Potential SSH Scan	1
123.195.130.67	147.237.76.31	Taiwan	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
89.255.21.58	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
222.186.56.42	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
75.148.3.165	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
198.12.82.58	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
51.254.23.230	147.237.8.50	United Kingdom	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.149	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
31.168.21.176	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
180.97.106.162	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.37	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.36	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
109.65.203.214	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
222.186.56.42	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
77.127.178.105	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
75.148.3.165	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
198.12.82.58	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 1024	1
51.254.23.230	147.237.8.28	United Kingdom	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.77.216	China	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

02-11-2016-19:04:01 to 02-11-2016-20:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
108.61.18.36	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	104
108.61.18.36	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	103
46.19.85.110	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	38
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
62.90.142.51	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	22
62.90.142.51	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	21
46.19.85.110	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
27.97.77.239	India	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	18
62.90.142.51	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
31.168.66.62	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
79.183.147.128	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
185.24.206.35	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	12
46.19.86.12	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
2.54.19.91	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
79.181.126.69	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
185.3.147.247	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.121.242.35	Israel	147.237.76.30	himush.idf.il	drop	First packet isn't SYN	drop	9
46.19.86.82	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
50.182.230.239	United States	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
2.54.21.48	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
77.127.209.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
93.173.231.229	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
79.178.126.73	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.145.55	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	6
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.187.231	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
149.88.216.160	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.222.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.229.131.179	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.215.59	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
37.26.146.218	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
185.24.206.35	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
5.102.242.190	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.82	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.19.91	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
109.67.121.158	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
2.54.19.91	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.57	Israel	147.237.77.233	atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	5
31.210.187.33	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.19.91	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
185.24.206.35	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
141.0.14.119	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
31.210.186.62	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
87.69.99.215	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.121.242.35	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence		monitor	4
128.194.3.195	United States	147.237.72.166	aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
198.204.249.34	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4

02-11-2016-19:04:01 to 02-11-2016-20:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.47.26	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	82
149.78.236.173	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	56
84.109.104.237	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 84.109.104.237	Block	11
66.249.65.14	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.65.14	Block	7
161.10.157.37	Colombia	147.237.0.34	tikshuv.idf.il	Distributed PHP Attempt	Block	6
79.179.142.164	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	5
161.10.157.37	Colombia	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 161.10.157.37	Block	5
46.19.86.86	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
95.86.88.91	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.54.186.106	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
79.181.240.223	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.63.246.103	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	2
46.116.114.246	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.52.22.204	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
165.91.12.184	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il/robots.txt	Block	1
85.250.187.6	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$71 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
128.194.131.138	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il/robots.txt	Block	1
62.114.167.92	Egypt	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	1
109.65.121.76	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â	Block	1
92.53.114.87	Russian Federation	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
31.168.66.62	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/matash	Block	1
218.38.33.24	Korea, Republic of	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
161.10.157.37	Colombia	147.237.0.34	tikshuv.idf.il	Admin Blocking	Block	1
84.108.204.229	Israel	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
119.94.183.37	Philippines	147.237.77.74	law.idf.il	PHP Attempt	Block	1
66.249.66.131	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/2359.jpg	Block	1
50.63.138.151	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
185.110.109.103		147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
85.250.221.196	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
79.180.114.154	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/register/mailingsignup.asp	Block	1
149.78.37.172	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
109.66.141.188	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.171	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/templates/events/events.aspx	Block	1
93.141.190.14	Croatia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
37.46.251.236	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi'a=0	Block	1
218.38.33.24	Korea, Republic of	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
84.108.204.229	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/xmlrpc.php	Block	1
119.94.183.37	Philippines	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
66.249.66.191	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/2372.jpg	Block	1
54.163.91.231	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 54.163.91.231	Block	1
95.154.214.2	United Kingdom	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	Block	1
186.202.151.18	Brazil	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
86.174.191.160	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
79.181.101.172	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl38$ctl01$ctl03$cblQuestion$2 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
149.78.37.172	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 149.78.37.172	Block	1
109.160.242.221	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gius	Block	1
93.141.190.14	Croatia	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
46.19.85.57	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1135-he/atal.aspx	Block	1
128.194.3.195	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il/robots.txt	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-en/matpash.aspx	Block	1

02-11-2016-19:04:01 to 02-11-2016-20:04:01