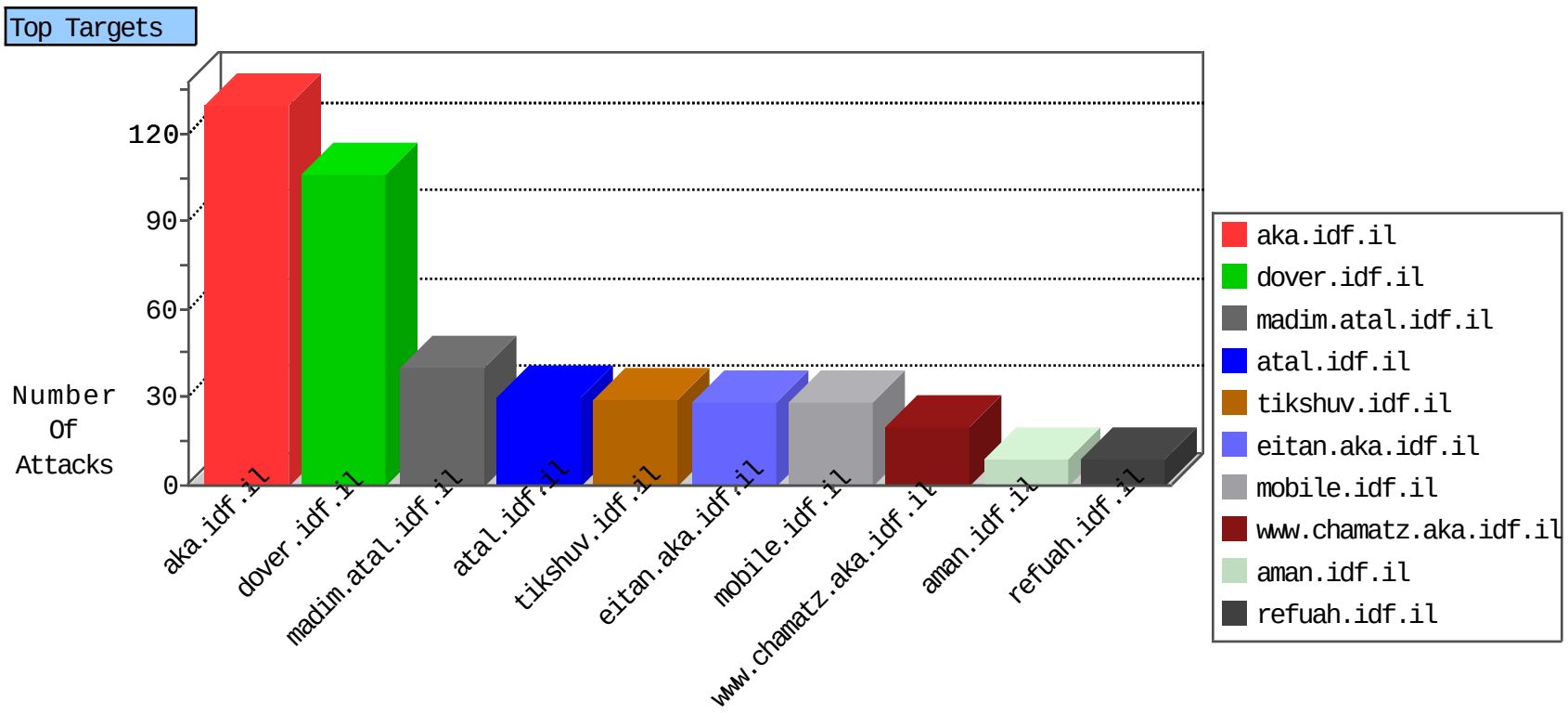
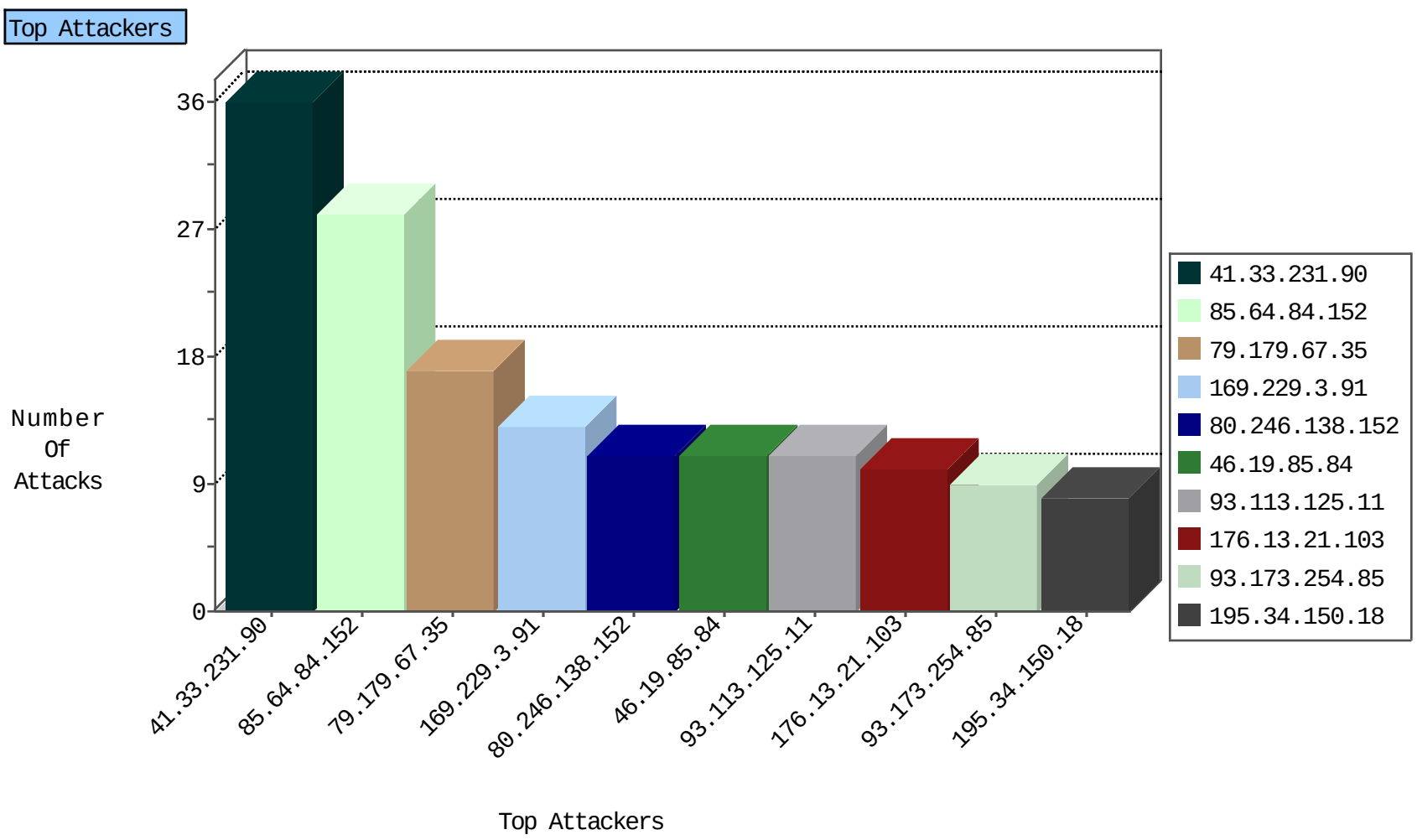
02-20-2016-11:04:07 to 02-20-2016-12:04:07

IDF Under Attack Daily Report





02-20-2016-11:04:07 to 02-20-2016-12:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
183.60.48.25	China	147.237.76.201	e.atal.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
216.99.159.226	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
185.130.5.201		147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
23.228.199.38	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
203.187.95.124	Taiwan	147.237.8.46	e.chinuch.idf.il	Invalid L4 Header Length	drop	1
176.103.72.75	Poland	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
216.145.14.142	United States	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	drop	1
185.130.5.201		147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
23.228.199.39	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
216.99.149.203	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
190.116.133.247	Peru	147.237.0.15	kosher-kravi.idf.il	Invalid TCP Flags	drop	1
77.50.246.44	Russian Federation	147.237.76.38	e.e.meitav.idf.il	L4 Source or Dest Port Zero	drop	1
216.99.149.204	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
185.130.5.201		147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
23.228.199.37	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
190.116.133.247	Peru	147.237.0.33	idf.il	Invalid TCP Flags	drop	1
176.103.72.75	Poland	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1

02-20-2016-11:04:07 to 02-20-2016-12:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.78.146.134	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	6
77.127.208.77	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	6
46.19.85.226	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	5
106.38.241.144	China	147.237.77.216	dover.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	4
89.138.105.117	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	4
84.228.195.205	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	1
84.228.9.151	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
149.50.125.54	United States	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	1

02-20-2016-11:04:07 to 02-20-2016-12:04:07

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
93.113.125.11	147.237.77.205	Romania	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.0.35	China	akaws.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
177.243.148.144	147.237.76.31	Mexico	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
128.127.0.45	147.237.8.45	Italy	e.eitan.idf.il	ET SCAN NMAP -sS window 2048	1
104.44.133.108	147.237.76.39	United States	mobile.meitav.idf.i	ET SCAN NMAP -sS window 3072	1
94.102.48.193	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
70.97.186.107	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
183.60.48.25	147.237.76.30	China	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
128.127.0.45	147.237.8.45	Italy	e.eitan.idf.il	ET SCAN NMAP -sS window 4096	1
128.127.0.45	147.237.8.45	Italy	e.eitan.idf.il	ET SCAN NMAP -f -sS	1
104.44.133.108	147.237.76.39	United States	mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1

02-20-2016-11:04:07 to 02-20-2016-12:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
85.64.84.152	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	28
79.179.67.35	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
109.253.215.135	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.47.30	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.126.190	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.248	Israel	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	5
97.114.102.234	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
77.125.94.102	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
176.13.20.239	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
91.200.12.143	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
176.13.20.239	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.178.98.91	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.25.158	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.232.192	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.134.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.147.11	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.147.114	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
216.145.14.142	United States	147.237.0.15	kosher-kravi.idf.il	Header Rejection	header rejection pattern found in request	monitor	3
46.19.86.100	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.250.60	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.126.190.188	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.179	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
82.81.24.59	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.4.181	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.150.225	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.135.189	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.25.133	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.42.149	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.32.161	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
79.181.187.149	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.101.52	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.174.23	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-20-2016-11:04:07 to 02-20-2016-12:04:07

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
82.166.131.119	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
116.58.205.107	Bangladesh	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
5.22.131.24	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
2.54.173.108	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
213.8.204.12	Israel	147.237.72.166	aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
116.58.205.107	Bangladesh	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
5.22.130.239	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
212.14.243.234	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
185.3.144.112	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
89.138.6.87	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
94.230.86.157	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
212.14.243.234	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2

02-20-2016-11:04:07 to 02-20-2016-12:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.84	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
80.246.138.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
80.246.137.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
93.173.254.85	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 93.173.254.85	Block	5
176.13.21.103	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 176.13.21.103	Block	5
46.121.93.35	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 46.121.93.35	Block	4
46.19.86.156	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.19.86.156	Block	3
2.54.164.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.121.93.35	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	3
46.19.86.38	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.19.86.38	Block	3
176.13.21.103	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
93.173.254.85	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	3
109.67.101.52	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	2
176.13.21.103	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
5.22.130.239	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	2
80.246.137.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
213.8.204.12	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/home/default.aspx	Block	2
125.78.220.178	China	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
109.67.101.52	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 109.67.101.52	Block	2
39.46.59.182	Pakistan	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
125.78.220.178	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/portalmiluim/templates/home.asp/xmlrpc.php	Block	1
77.127.57.8	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$98 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
199.16.156.126	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-18021en/dover.aspx	Block	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	Illegal Byte Code Character in Method Â¿#Â‡Â˜@Ãœ xgG[[#14]]1•Ã§Â¯ÃŒ:Â„=j	Block	1
84.108.205.197	Israel	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
66.240.219.146	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
39.46.59.182	Pakistan	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1
157.55.39.159	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
93.173.254.85	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/updatestatus.php	Block	1
79.179.67.35	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
207.46.13.29	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/site/unselecatble.aspx	Block	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	Malformed URL	Block	1
109.253.135.83	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
84.108.205.197	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/xmlrpc.php	Block	1
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1108-he/nakhal.aspx	Block	1
184.105.139.68	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	Illegal Byte Code Character in Method	Block	1
95.32.82.25	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/wp-config.bkp	Block	1
207.241.231.248	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;docId in www.aka.idf.il/brothers/skira/default.asp	None	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	Unknown HTTP Request Method Â¿#Â‡Â˜@Ãœ xgG[[#14]]1•Ã§Â¯ÃŒ:Â„=j in URL	Block	1
17.138.56.26	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.138.56.26	Block	1
125.78.220.178	China	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 125.78.220.178	Block	1
85.64.210.78	Israel	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
74.82.47.4	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
185.3.147.235	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 185.3.147.235	Block	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	Abnormally Long Request method	Block	1
109.67.23.212	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
2.52.41.242	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
61.3.129.70	India	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
37.146.111.38	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	1

02-20-2016-11:04:07 to 02-20-2016-12:04:07