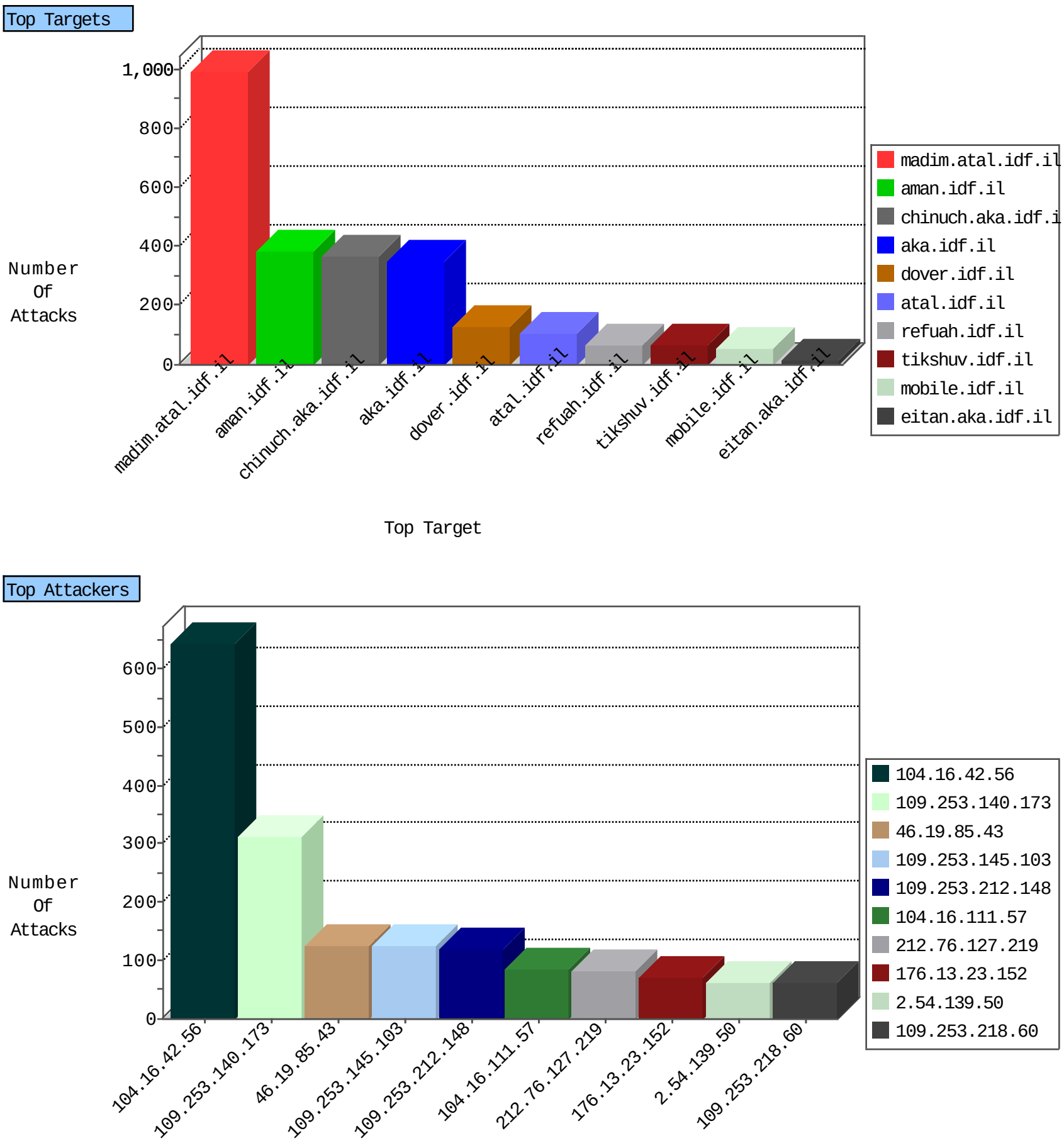
02-07-2016-13:04:08 to 02-07-2016-14:04:08

IDF Under Attack
Daily Report



02-07-2016-13:04:08 to 02-07-2016-14:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.182.106.124	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	30
31.168.96.254	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
185.115.126.8		147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
185.115.126.8		147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1

02-07-2016-13:04:08 to 02-07-2016-14:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-07-2016-13:04:08 to 02-07-2016-14:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
188.126.77.138	147.237.72.166	Sweden	aka.idf.il	ET SCAN NMAP -sS window 1024	1
94.233.194.48	147.237.0.15	Russian Federation	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
89.248.168.218	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN Potential SSH Scan	1
81.218.66.107	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.182.208.201	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.25.91.30	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
45.35.64.142	147.237.77.216		dover.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.74	147.237.77.235	United States	sviva.idf.il	ET DROP Dshield Block Listed Source	1
194.90.241.40	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.117.103.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
179.43.141.234	147.237.76.201	Switzerland	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
93.189.26.18	147.237.72.217	Austria	e.idf.il	ET SCAN NMAP -sS window 1024	1
84.25.222.53	147.237.77.216	Netherlands	dover.idf.il	portscan: TCP Distributed Portscan	1
80.179.37.129	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.199.57.203	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.176.210.183	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
199.203.226.21	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.134.164	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
193.34.57.101	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

02-07-2016-13:04:08 to 02-07-2016-14:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
104.16.42.56	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	324
104.16.42.56	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	321
212.76.127.219	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	73
104.16.111.57	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	40
104.16.111.57	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	39
77.126.104.242	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	21
2.54.0.37	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
77.126.104.242	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	11
77.126.104.242	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
46.19.85.98	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
212.199.103.79	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
94.230.93.230	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
94.230.93.134	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.26.149.235	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
94.230.93.217	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
149.88.219.8	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
212.76.127.219	Israel	147.237.77.234	halag.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
176.13.20.31	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
46.19.86.164	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.183.49.120	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.7.12	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
94.230.93.227	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.45.143	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
213.8.125.176	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.125.103	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.134.164	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
212.76.127.111	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
2.54.34.164	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
94.230.93.137	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.84.94	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
80.178.136.242	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.210.186.41	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.226.20.135	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.10.206	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
80.246.137.96	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
2.54.171.163	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
2.54.171.163	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
80.246.137.96	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.171.163	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
80.246.137.96	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
2.52.134.164	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.54.171.163	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
80.246.137.96	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.54.171.163	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.54.43.52	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
176.228.90.12	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.171.163	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
80.178.157.42	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4

02-07-2016-13:04:08 to 02-07-2016-14:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.140.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	163
109.253.140.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	150
109.253.212.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	121
109.253.145.103	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	110
176.13.23.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	67
46.19.85.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	67
109.253.218.60	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	62
2.54.139.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	58
46.19.85.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	58
2.54.5.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
2.54.183.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
212.116.164.20	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	16
109.253.145.103	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	14
176.13.3.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
81.218.241.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.26	Block	8
37.26.146.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
87.145.87.53	Germany	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	6
46.19.85.98	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
37.26.149.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
2.52.2.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
132.72.99.129	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	3
45.114.127.237		147.237.76.42	refuah.idf.il	PHP Attempt	Block	3
84.228.98.148	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	3
2.52.33.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
45.114.127.237		147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	3
37.26.148.225	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	3
109.253.222.216	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.250.199.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.139.50	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	3
37.26.146.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.153.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.54.177	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
77.247.181.162	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-ar	Block	2
46.19.86.223	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	2
79.177.223.64	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 79.177.223.64	Block	2
82.102.136.67	Israel	147.237.76.42	refuah.idf.il	Distributed Parameter Type Violation on www.refua.atal.idf.il/1518-he/refuah.aspx parameter ctl00$ContentPlaceHolder1$txtContent	Block	2
2.54.139.50	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCity in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	2
62.219.228.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.33.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.228.98.148	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 84.228.98.148	Block	2
81.218.241.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/searchback.png	Block	1
46.19.85.227	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
79.178.18.179	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.85.60	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
109.67.120.114	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
87.69.210.76	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$83 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
66.249.65.193	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/shared/usercontrols/headerupper/	Block	1
185.32.179.174	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl38$ctl01$ctl03$cblQuestion$1 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
61.135.190.71	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/shared/clientscripts/sa_swfobject.js	Block	1
176.13.3.75	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/	Block	1

02-07-2016-13:04:08 to 02-07-2016-14:04:08