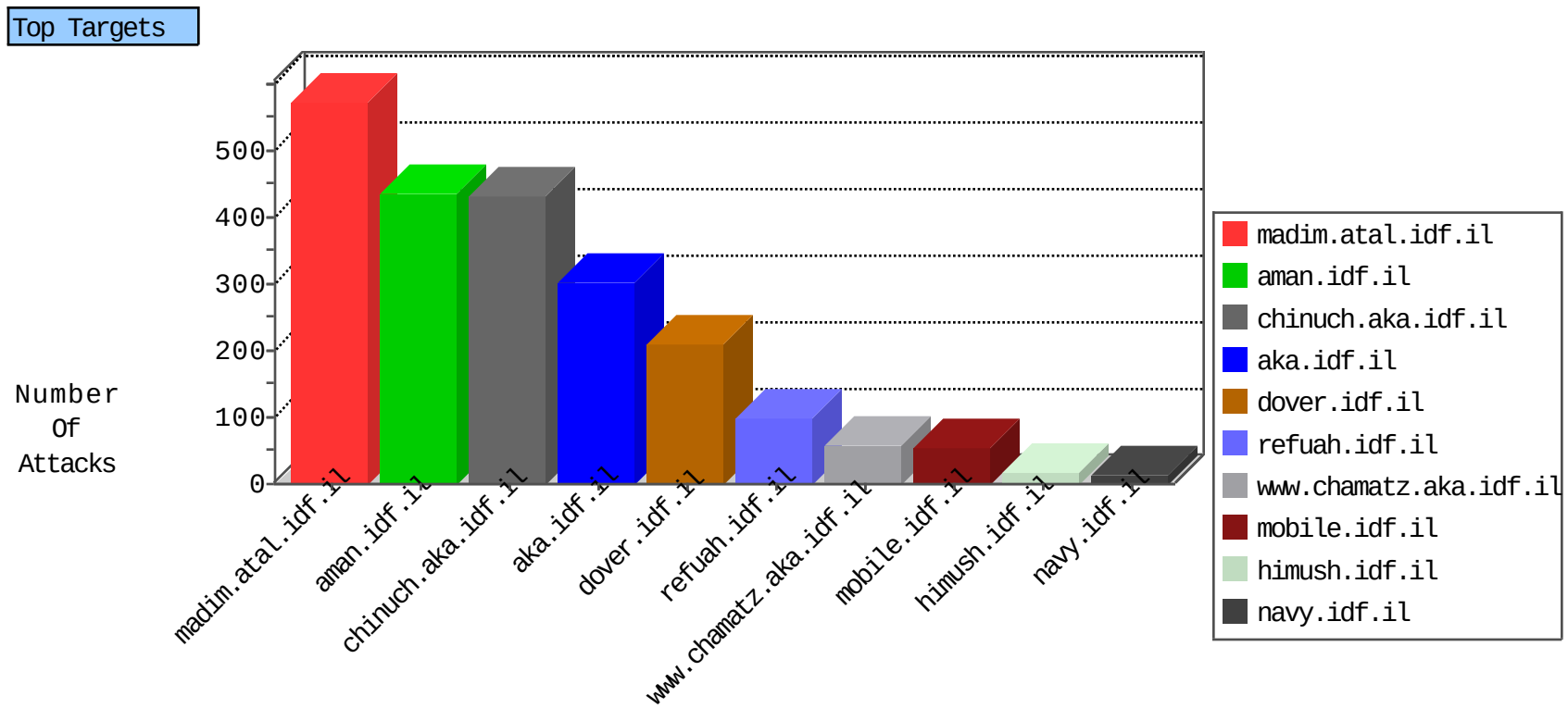
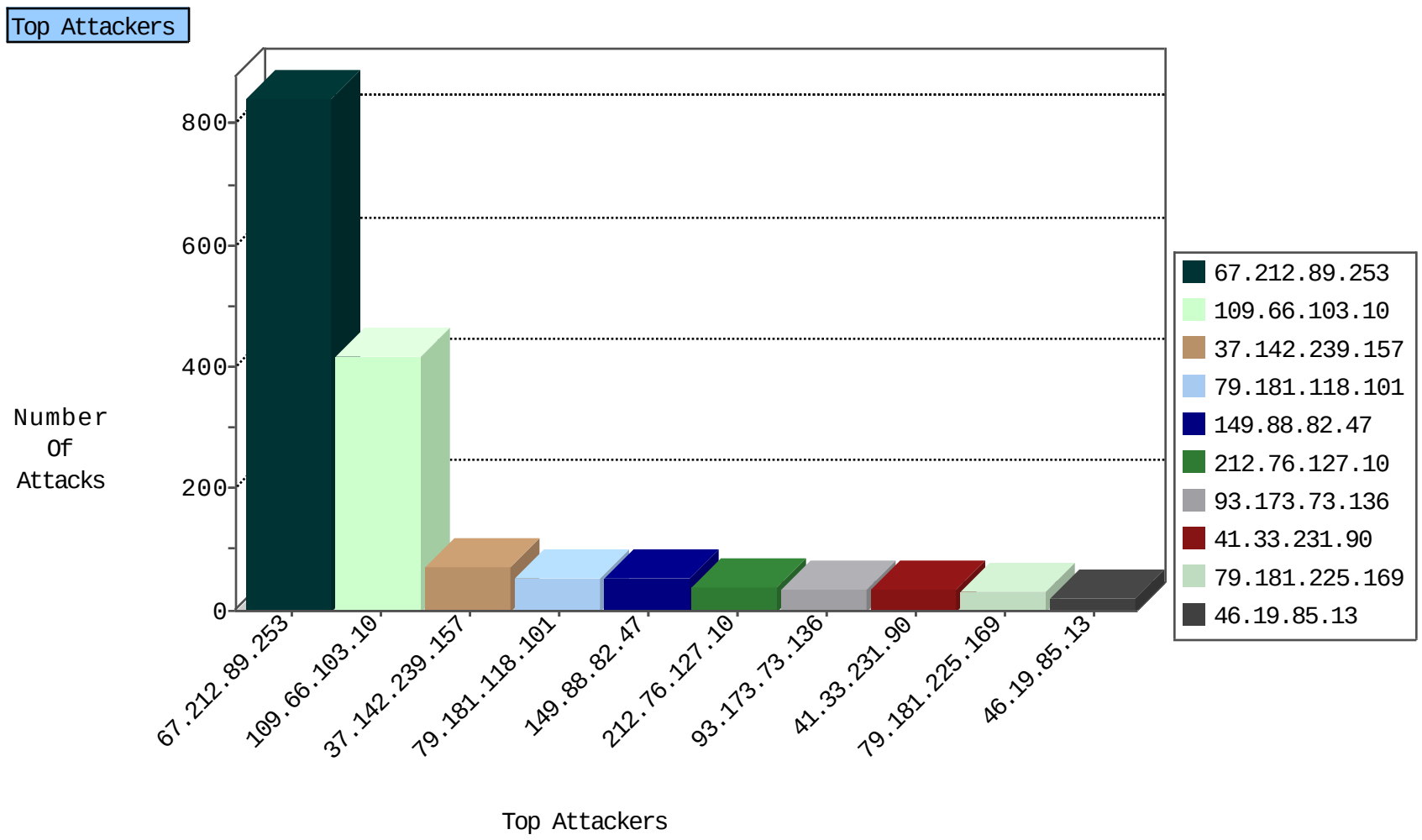
02-06-2016-20:04:06 to 02-06-2016-21:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-06-2016-20:04:06 to 02-06-2016-21:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
14.215.2.162	China	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	2
198.20.99.130	Netherlands	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
74.91.28.59	United States	147.237.76.42	refuah.idf.il	block-sp-traf1	drop	1
94.102.48.195	Netherlands	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
142.54.185.230	United States	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1

02-06-2016-20:04:06 to 02-06-2016-21:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.203.18.169	Netherlands	147.237.77.216	dover.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
93.142.189.206	Croatia	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
136.243.103.157	Germany	147.237.72.166	aka.idf.il	C106: HTTP: majestic bot	Block	1
186.151.63.89	Guatemala	147.237.72.166	aka.idf.il	C008: HTTP: Xenu UserAgent	Block	1
186.151.63.89	Guatemala	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1

02-06-2016-20:04:06 to 02-06-2016-21:04:06

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
59.45.79.117	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.77.227	China	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
176.13.22.143	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.85.35.211	147.237.77.216	Bulgaria	dover.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
213.57.235.73	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
192.80.65.177	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
101.108.103.216	147.237.76.34	Thailand	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.45.79.117	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1

02-06-2016-20:04:06 to 02-06-2016-21:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
67.212.89.253	Canada	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	419
67.212.89.253	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	419
109.66.103.10	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
212.76.127.10	Israel	147.237.77.226	www.chamatz.aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	39
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
93.173.73.136	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	35
79.181.225.169	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	31
149.88.82.47	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	26
212.76.127.219	Israel	147.237.77.226	www.chamatz.aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	15
46.19.86.91	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
46.120.190.75	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
149.88.82.47	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
46.19.86.182	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
109.65.188.118	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
213.8.204.19	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
154.118.111.15		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
77.125.114.235	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
37.46.39.204	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
5.29.201.220	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	7
212.179.212.215	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.29.201.220	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.13	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.13	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
62.19.59.171	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.54.158.9	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.115.67	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.40.37	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.68.160.35	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
149.88.82.47	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.21	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.183.178.205	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
52.49.79.6	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
46.19.86.193	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
5.22.131.125	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.13	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
2.52.190.75	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
84.95.57.146	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.22	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
50.18.94.121	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
188.120.148.210	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.22	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
91.200.12.141	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
46.19.85.13	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
68.180.229.121	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.28	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
31.210.187.58	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.28	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

02-06-2016-20:04:06 to 02-06-2016-21:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.66.103.10	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	222
109.66.103.10	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
79.181.118.101	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	55
37.142.239.157	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	52
109.66.103.10	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 109.66.103.10	Block	36
37.142.239.157	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	19
185.32.179.52	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
192.243.55.136	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.136	Block	6
109.65.80.7	Israel	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	4
109.65.80.7	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/xmlrpc.php	Block	4
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	3
109.253.145.250	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.142.230.17	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.176.125.67	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
37.26.146.225	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
176.13.22.13	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
46.120.190.75	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	2
95.86.107.125	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/4/113414.pdf&sa=u&ved=0ahukewilnsck6epkahvdiiwkhz5jcgoqfggymaq&usg=afqjcnfmwyykfodfyysnfh8l8iajntl-zq	Block	2
164.138.118.222	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 164.138.118.222	Block	2
109.64.225.130	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â	Block	2
46.120.191.110	Israel	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	1
31.168.3.188	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$78 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
93.173.73.136	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
79.179.99.243	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in www.atal.idf.il/1440-he/atal.aspx	Block	1
192.243.55.133	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/faq.aspx	Block	1
164.138.118.222	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/&sa=u&ved=0ahukewir4i623epkahvd9g4khag9cxcqfggimaa&usg=afqjcnhcvyyg7w1cq-yhd5_ammzoyodtwa	Block	1
46.19.85.191	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl38$ctl01$ctl03$cblQuestion$0 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
2.54.40.37	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
213.8.204.66	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/controls/atuda/Â	Block	1
79.182.64.11	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
185.89.217.226		147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
46.120.236.155	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
109.67.133.253	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
95.86.97.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
68.180.230.244	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
46.120.190.75	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 46.120.190.75	Block	1
5.22.131.86	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.182.207.82	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
185.89.217.235		147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
79.176.125.67	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	1
46.121.136.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mivtza	Block	1
95.86.105.200	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/	Block	1
79.181.124.22	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gen204	Block	1
207.46.13.192	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/robots.txt	Block	1
176.221.124.42	Poland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/dover.aspx/	Block	1
5.102.234.64	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
80.246.136.89	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$117 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
79.176.168.63	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl38$ctl01$ctl03$cblQuestion$6 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
188.143.232.21	Russian Federation	147.237.77.176	matpash.idf.il	Parameter Type Violation fromDate in www.cogat.idf.il/901-en/cogat.aspx	Block	1

02-06-2016-20:04:06 to 02-06-2016-21:04:06