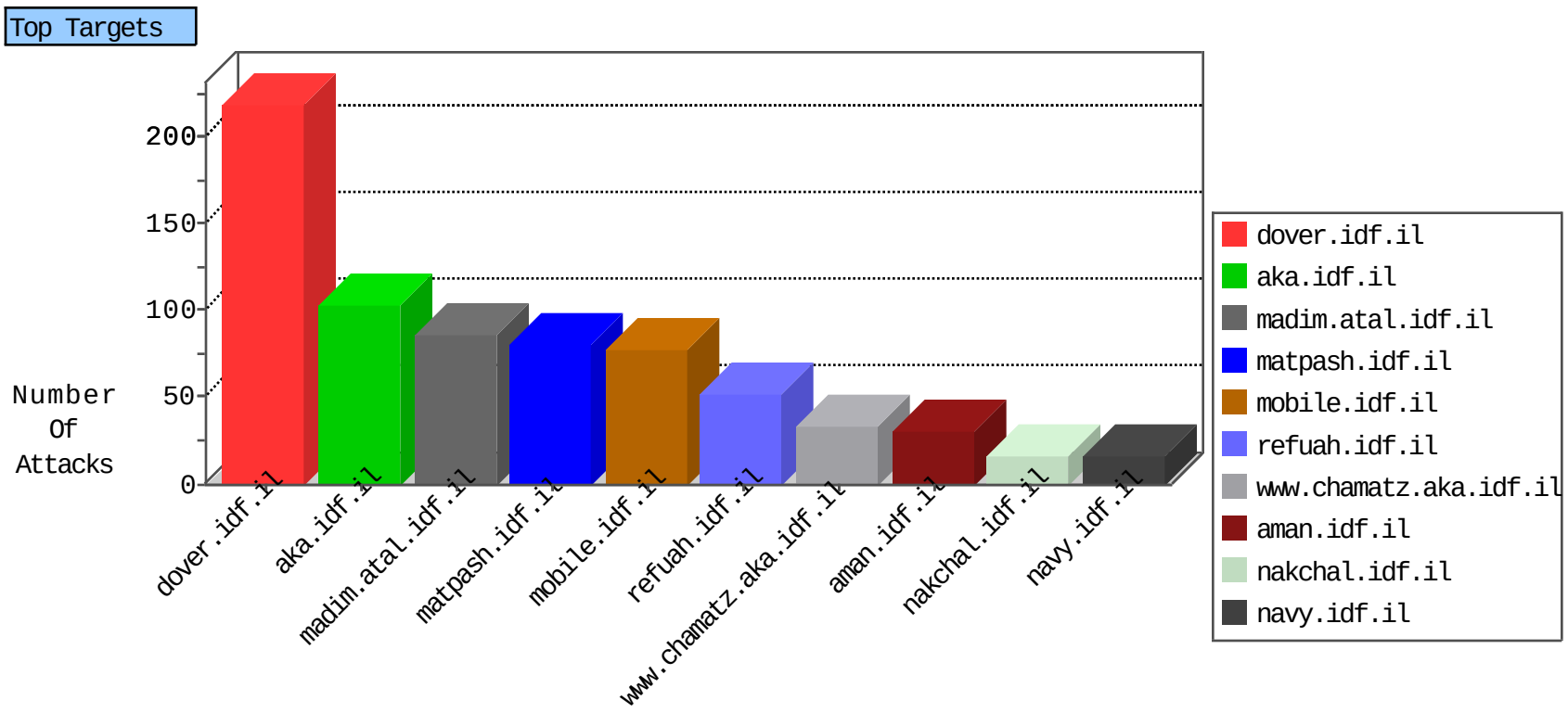
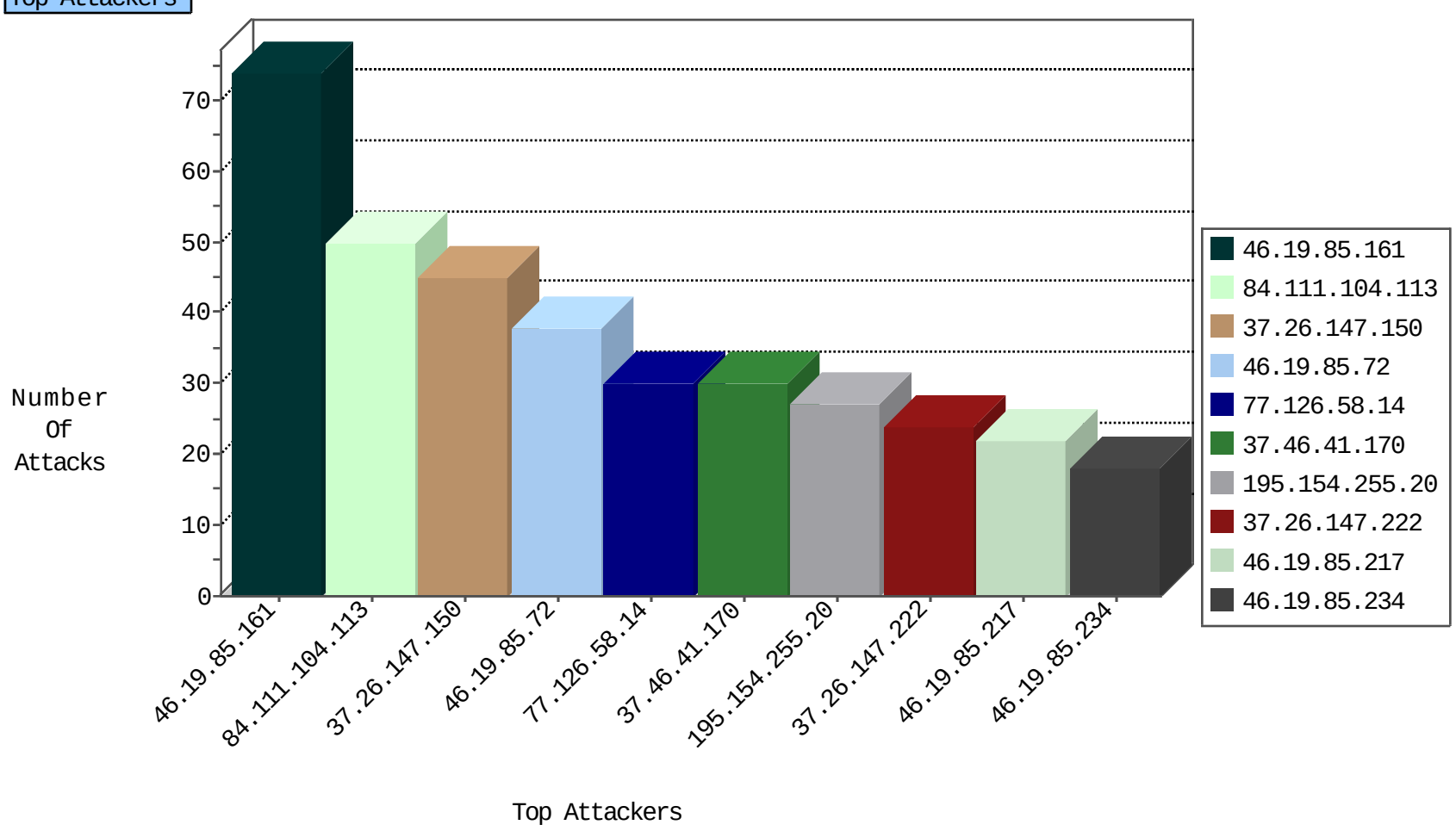
09-30-2016-22:04:01 to 09-30-2016-23:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-30-2016-22:04:01 to 09-30-2016-23:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.111.104.113	Israel	147.237.72.166	aka.idf.il	Black List	drop	22
84.111.104.113	Israel	147.237.77.216	dover.idf.il	Black List	drop	9
185.89.217.225	Netherlands	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
79.178.139.79	Israel	147.237.72.166	aka.idf.il	Black List	drop	6
84.111.104.113	Israel	147.237.77.233	atal.idf.il	Black List	drop	4
84.111.104.113	Israel	147.237.76.200	eitan.aka.idf.il	Black List	drop	4
84.111.104.113	Israel	147.237.77.226	www.chamatz.aka.idf.il	Black List	drop	4
24.133.42.141	Turkey	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
93.158.200.126	Netherlands	147.237.76.86	navy.idf.il	Black List	drop	1
71.6.146.186	United States	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1

09-30-2016-22:04:01 to 09-30-2016-23:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
195.154.255.20	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	21
195.154.255.20	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
195.154.255.20	France	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	2
195.154.255.20	France	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-30-2016-22:04:01 to 09-30-2016-23:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.0.34	Israel	tikshuv.idf.il	Xenu Link Sleuth User Agent	4
109.67.239.218	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	2
202.106.54.203	147.237.76.197	China	e.himush.idf.il	GPL SCAN nmap TCP	2
46.252.49.19	147.237.76.39	Bulgaria	mobile.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
121.164.189.91	147.237.77.234	Korea, Republic of	halag.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
219.142.79.3	147.237.76.197	China	e.himush.idf.il	GPL SCAN nmap TCP	2
121.207.1.156	147.237.77.205	China	prisha.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
94.102.52.55	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
94.102.52.55	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
94.102.52.55	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	147.237.72.217	China	e.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
61.240.144.65	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
124.8.223.198	147.237.76.196	Taiwan	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
124.8.223.198	147.237.0.33	Taiwan	idf.il	ET SCAN Potential SSH Scan	1
106.187.45.144	147.237.76.148	Japan	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
94.102.52.55	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
94.102.52.55	147.237.76.30	Netherlands	himush.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
61.240.144.65	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
124.8.223.198	147.237.76.197	Taiwan	e.himush.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
124.8.223.198	147.237.76.44	Taiwan	e.refuah.idf.il	ET SCAN Potential SSH Scan	1

09-30-2016-22:04:01 to 09-30-2016-23:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.46.41.170	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
77.126.58.14	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
46.19.85.161	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	15
185.89.217.234	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
185.89.217.232	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.72	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.19.85.72	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
46.19.85.234	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.161	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	10
186.13.6.149	Argentina	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	10
46.19.85.161	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.161	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
46.19.85.234	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
46.19.85.72	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
46.19.85.72	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.161	Israel	147.237.77.176	matpash.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	8
185.89.217.227	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.12	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
109.160.213.184	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.161	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
185.89.217.233	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
185.89.217.225	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
77.126.14.141	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.204.182	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.89.217.226	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.12	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.86	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
2.55.157.103	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.161	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.86	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
79.181.99.166	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	6
185.89.217.228	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.26.147.191	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
2.55.143.4	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
79.177.55.181	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
37.46.35.124	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	5
2.53.167.86	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
37.46.35.124	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
46.19.85.217	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
185.89.217.229	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.55.143.4	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.194	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
185.89.217.230	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
176.13.249.163	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
185.89.217.235	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.161	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
185.89.217.231	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.166.190.184	Netherlands	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
109.160.213.184	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
106.38.241.106	China	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	4

09-30-2016-22:04:01 to 09-30-2016-23:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.147.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
37.26.147.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
37.26.147.222	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	12
2.53.160.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.51	Block	3
185.32.179.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.136.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.138.83.68	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	2
2.53.152.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.138.185.39	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/smalim/smalim.aspx	Block	2
77.138.185.39	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/	Block	2
176.13.11.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.55.21.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.67.239.218	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/ishurim	Block	1
2.87.238.142	Greece	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.237.138.202	Czech Republic	147.237.77.234	halag.idf.il	Unauthorized URL Access to /	Block	1
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mobile/main/haredim/general.aspx	Block	1
188.120.134.208	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
37.46.35.124	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
2.53.53.111	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.65.59	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9711-he/refuah.aspx	Block	1
109.253.204.182	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
5.255.253.75	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
79.1.7.180	Italy	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1399-en/dover.aspx	Block	1
66.249.64.105	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mobile/main/giyus/general.aspx	Block	1
192.243.55.135	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/templates/shared/usercontrols/lobbyinfocenteritem/	Block	1
104.153.224.168	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 104.153.224.168	Block	1
66.249.73.143	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx	Block	1
157.55.39.128	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
79.179.132.189	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
77.125.29.16	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
66.249.65.21	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/mobile/	Block	1
204.79.180.81	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on aka.idf.il/miluim/templates/inner.asp	Block	1
104.153.224.168	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/sachar	Block	1
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/edim/theproj/	Block	1
79.181.17.141	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	None	1
77.125.86.225	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
213.8.204.17	Israel	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
109.67.136.49	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/homepage.aspx	Block	1
77.139.93.39	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catId\u003d59116\u0026pageNum\u003d3 in www.aka.idf.il/edim/yoman/yoman.asp	None	1
80.178.85.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
77.138.16.63	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	Block	1
66.249.65.58	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9757-he/refuah.aspx	Block	1
213.8.204.17	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1

09-30-2016-22:04:01 to 09-30-2016-23:04:01