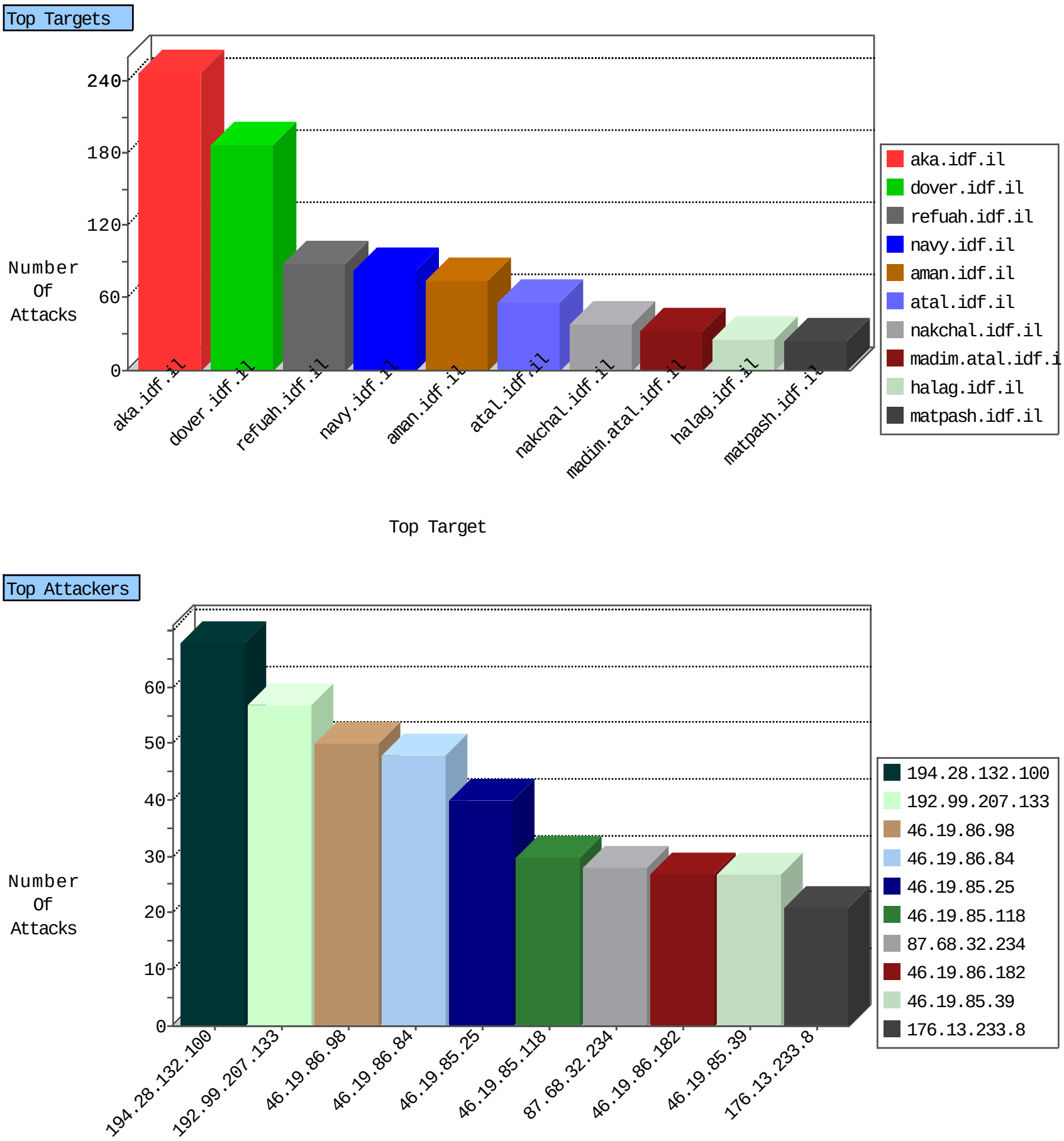
09-08-2016-18:04:00 to 09-08-2016-19:04:00

IDF Under Attack
Daily Report



09-08-2016-18:04:00 to 09-08-2016-19:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.142.8.209	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
89.248.167.131	Netherlands	147.237.76.198	e.yohalan.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.177	ncore.idf.il	Black List	drop	1

09-08-2016-18:04:00 to 09-08-2016-19:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
61.135.189.125	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1
106.38.241.105	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

09-08-2016-18:04:00 to 09-08-2016-19:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.77.176	Israel	matpash.idf.il	Xenu Link Sleuth User Agent	8
46.120.122.219	147.237.77.74	Israel	law.idf.il	Xenu Link Sleuth User Agent	8
66.249.79.103	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	2
46.120.122.219	147.237.77.170	Israel	maarachot.idf.il	Xenu Link Sleuth User Agent	2
113.240.250.154	147.237.76.177	China	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.67.13	147.237.77.235	United Kingdom	sviva.idf.il	ET SCAN Potential SSH Scan	1
163.172.67.13	147.237.77.74	United Kingdom	law.idf.il	ET SCAN Potential SSH Scan	1
163.172.67.13	147.237.76.199	United Kingdom	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
163.172.67.13	147.237.72.14	United Kingdom	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
42.116.29.68	147.237.0.19	Vietnam	madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
163.172.67.13	147.237.8.14	United Kingdom	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
37.26.147.161	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
128.199.58.67	147.237.77.234	Netherlands	halag.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
123.249.27.241	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
182.254.131.170	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
123.249.27.241	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
178.220.165.231	147.237.76.196		e.sviva.idf.il	ET SCAN NMAP -sS window 3072	1
106.186.20.183	147.237.0.33	Japan	idf.il	ET SCAN Potential SSH Scan	1
163.172.67.13	147.237.77.233	United Kingdom	atal.idf.il	ET SCAN Potential SSH Scan	1
163.172.67.13	147.237.77.61	United Kingdom	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
163.172.67.13	147.237.76.196	United Kingdom	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
42.116.29.68	147.237.0.19	Vietnam	madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
163.172.67.13	147.237.8.24	United Kingdom	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
42.116.29.68	147.237.0.19	Vietnam	madim.atal.idf.il	ET SCAN NMAP -f -sS	1
163.172.67.13	147.237.0.200	United Kingdom	m4u.idf.il	ET SCAN Potential SSH Scan	1
123.249.27.241	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
123.249.27.241	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
178.220.165.231	147.237.76.196		e.sviva.idf.il	ET SCAN NMAP -sS window 4096	1

09-08-2016-18:04:00 to 09-08-2016-19:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
194.28.132.100	Ukraine	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	66
5.102.198.137	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
46.19.85.118	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
46.19.86.98	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	15
87.68.32.234	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
46.19.85.25	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
87.68.32.234	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
46.19.85.25	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
46.19.86.84	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
46.19.86.84	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.86.84	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
185.120.126.10	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.86.84	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.86.98	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
46.19.85.118	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
46.19.86.98	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
185.32.179.87	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.66.60.166	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	9
81.218.66.107	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
84.94.46.44	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
46.19.86.182	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
109.67.118.243	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	7
46.19.86.182	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
109.67.118.243	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
46.19.85.39	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.98	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	7
192.99.207.133	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
46.19.86.182	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
80.246.133.164	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
109.253.131.149	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
80.246.138.120	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
77.138.102.39	France	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	6
192.99.207.133	Canada	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
192.99.207.133	Canada	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.85.39	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.39	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
37.26.148.167	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
80.246.138.120	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.182	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
80.246.138.120	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
192.99.207.133	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.86.222	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
192.99.207.133	Canada	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.85.25	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.99.207.133	Canada	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
192.99.207.133	Canada	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.85.25	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
185.120.126.10	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	4
80.246.137.35	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.85.45	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

09-08-2016-18:04:00 to 09-08-2016-19:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.233.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
85.65.149.230	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 85.65.149.230	Block	16
213.57.168.41	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	6
84.108.101.215	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	5
5.102.195.247	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	5
77.139.168.158	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	4
185.32.179.87	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
84.109.113.192	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	3
37.26.149.246	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	3
109.253.131.149	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
2.53.51.237	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	2
76.14.80.216	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
106.184.21.28	Japan	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/giyus/	Block	2
109.67.143.49	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_KEY_EXCHANGE)	None	1
66.249.64.124	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/yohalan/main.main.asp	Block	1
85.64.1.249	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 85.64.1.249	Block	1
46.43.70.206	Palestinian Territory, Occupied	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
37.142.239.32	Israel	147.237.72.166	aka.idf.il	Double URL Encoding - parameter: search in www.aka.idf.il/main/giyus/pniothandler1.asmx/search	Block	1
80.74.125.36	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ...9&sideScroll in www.aka.idf.il/giyus/kadatz/	None	1
77.138.54.20	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/giyus/kadatz/	Block	1
61.135.189.125	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
108.21.193.119	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
46.19.86.98	Israel	147.237.77.233	atal.idf.il	Abnormally Long Request request version	Block	1
79.176.146.28	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
12.151.244.133	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
109.186.76.154	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
74.91.23.166	United States	147.237.72.167	ishurim.aka.idf.i	Unauthorized URL Access to 147.237.72.167/	Block	1
46.117.24.178	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
46.19.85.175	Israel	147.237.77.233	atal.idf.il	Distributed Abnormally Long Request	Block	1
80.246.133.164	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
77.138.208.32	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/	Block	1
2.53.17.123	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	Block	1
108.161.241.24	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/favicon.ico	Block	1
46.19.86.98	Israel	147.237.77.233	atal.idf.il	Illegal HTTP Version _pk_ref.117.aa59=%5B%22%22%2C%22%22%2C1473347120%2C%22https%3A%2F%2Fwww.google.co.il%2F%22%5D; _pk_id.117.aa59=b2e29e375e25a9ad.1473347120.1.1473347120.1473347120.; _pk_ses.117.aa59=*	Block	1
79.180.218.242	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
31.210.187.75	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
74.91.23.166	United States	147.237.77.216	dover.idf.il	Unauthorized Method HEAD for 147.237.77.216/	Block	1
85.65.149.230	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
46.120.54.51	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
46.19.85.175	Israel	147.237.77.233	atal.idf.il	Distributed Illegal HTTP Version	Block	1
81.98.163.96	United Kingdom	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
77.138.222.58	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.41	Block	1
109.67.118.243	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
84.109.113.192	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.86.98	Israel	147.237.77.233	atal.idf.il	Malformed URL __atuvs=57d17df14f1cad83000;	Block	1
79.182.138.23	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.253.192.251	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
46.121.115.171	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.121.115.171	Block	1

09-08-2016-18:04:00 to 09-08-2016-19:04:00