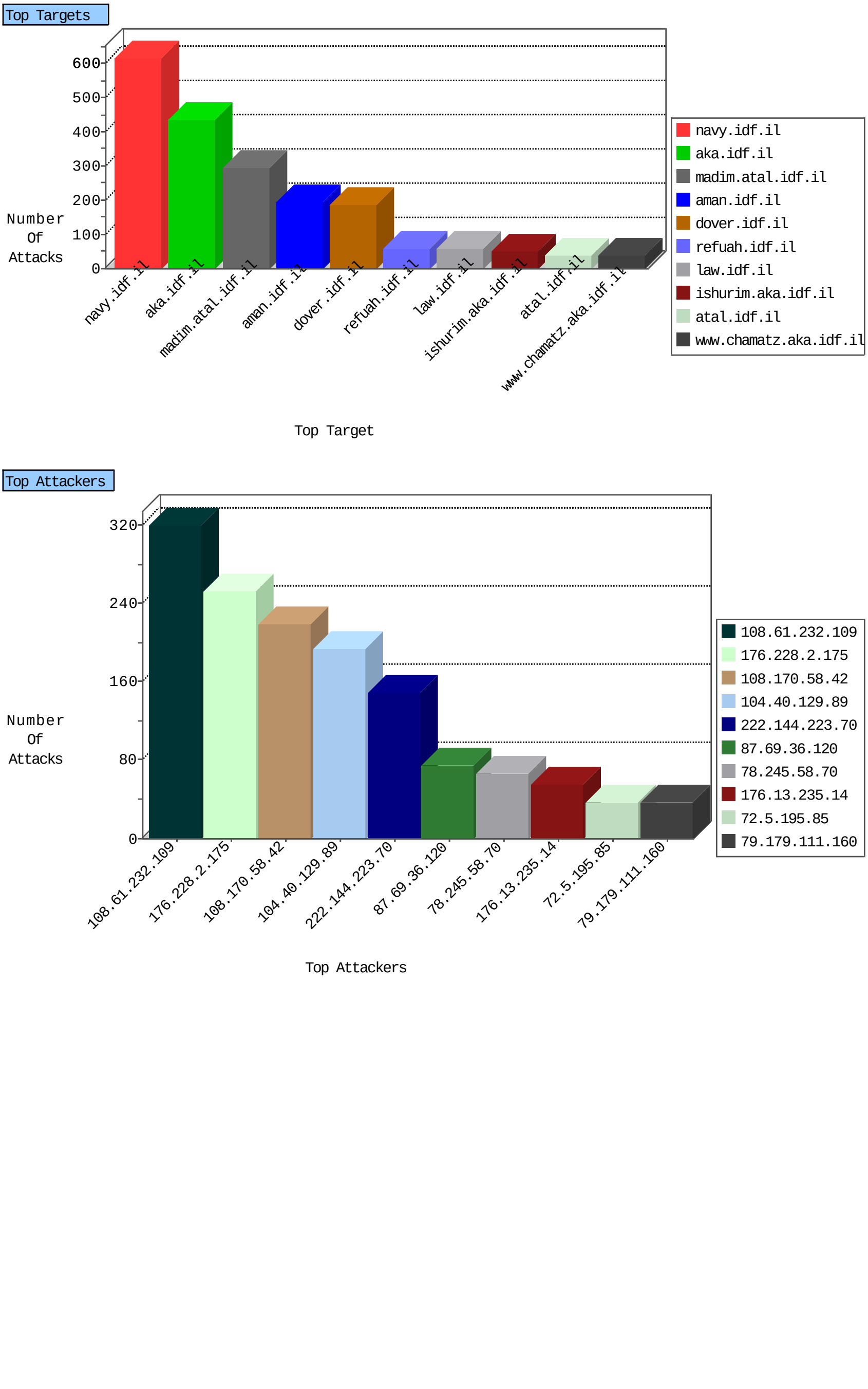
09-07-2016-20:04:04 to 09-07-2016-21:04:04

IDF Under Attack Daily Report



09-07-2016-20:04:04 to 09-07-2016-21:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.179.111.160	Israel	147.237.72.166	aka.idf.il	Black List	drop	37
2.53.28.57	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
185.25.33.139	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
80.82.77.46	Netherlands	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1
185.25.33.140	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
80.82.77.46	Netherlands	147.237.76.86	navy.idf.il	Black List	drop	1
80.82.77.46	Netherlands	147.237.76.199	e.nakchal.idf.il	Black List	drop	1

09-07-2016-20:04:04 to 09-07-2016-21:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
209.17.114.79	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
106.38.241.105	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

09-07-2016-20:04:04 to 09-07-2016-21:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
209.17.114.79	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
91.121.222.79	147.237.77.74	France	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	4
45.79.71.122	147.237.72.166	United States	aka.idf.il	WEB-MISC Chunked-Encoding transfer attempt	2
106.38.241.105	147.237.72.166	China	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
104.232.98.38	147.237.76.176	United States	test.ncore.idf.i	ET SCAN NMAP -sS window 1024	1
104.192.0.20	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
104.128.144.131	147.237.77.61	Canada	e.cogat.idf.il	ET SCAN NMAP -sS window 2048	1
106.186.20.183	147.237.0.34	Japan	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
104.232.98.38	147.237.76.176	United States	test.ncore.idf.i	ET SCAN NMAP -sS window 2048	1
104.232.98.38	147.237.76.176	United States	test.ncore.idf.i	ET SCAN NMAP -f -sS	1
104.192.0.20	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
104.128.144.131	147.237.77.61	Canada	e.cogat.idf.il	ET SCAN NMAP -f -sS	1
66.249.93.135	147.237.77.233	Europe	atal.idf.il	ET SCAN NMAP -sA (2)	1

09-07-2016-20:04:04 to 09-07-2016-21:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
108.61.232.109	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	321
222.144.223.70	Japan	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	147
78.245.58.70	France	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	67
87.69.36.120	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	35
87.69.36.120	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	35
72.5.195.85	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	34
176.44.144.203	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
185.93.35.174	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
176.13.235.14	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
108.170.58.42	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
108.170.58.42	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
108.170.58.42	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
108.170.58.42	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
108.170.58.42	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
108.170.58.42	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
108.170.58.42	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
108.170.58.42	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
104.40.129.89	Netherlands	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
108.170.58.42	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
104.40.129.89	Netherlands	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
104.40.129.89	Netherlands	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
108.170.58.42	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
104.40.129.89	Netherlands	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
104.40.129.89	Netherlands	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
104.40.129.89	Netherlands	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
104.40.129.89	Netherlands	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
104.40.129.89	Netherlands	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
108.170.58.42	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
104.40.129.89	Netherlands	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
104.40.129.89	Netherlands	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
104.40.129.89	Netherlands	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
46.120.195.136	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
77.139.184.240	France	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
108.170.58.42	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
108.170.58.42	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
108.170.58.42	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
46.19.85.200	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
104.40.129.89	Netherlands	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
108.170.58.42	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
108.170.58.42	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
104.40.129.89	Netherlands	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
104.40.129.89	Netherlands	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
104.40.129.89	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
108.170.58.42	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
77.139.184.240	France	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
176.13.235.14	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
104.40.129.89	Netherlands	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
104.40.129.89	Netherlands	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
104.40.129.89	Netherlands	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
176.13.235.14	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	8

09-07-2016-20:04:04 to 09-07-2016-21:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.228.2.175	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	254
212.76.120.127	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/general.aspx	Block	14
77.139.170.208	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	13
84.111.241.194	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	12
79.182.61.127	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	12
176.13.245.192	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	7
212.76.120.127	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 212.76.120.127	Block	6
46.121.115.171	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.121.115.171	Block	6
79.183.15.78	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	5
85.250.78.118	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
176.13.6.48	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
88.128.80.195	Germany	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/giyus/	Block	2
46.215.116.191	Poland	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
185.93.245.74	United Arab Emirates	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en	Block	2
77.138.70.173	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/patzar/home/default.asp	Block	2
94.230.86.98	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
2.53.149.34	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
212.76.111.5	Israel	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	2
66.147.244.101	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	2
80.246.140.64	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.86.148	Israel	147.237.76.31	nakchal.idf.il	Abnormally Long Request method	Block	1
37.26.148.138	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
77.139.17.239	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
66.249.76.79	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/pratim/pirteychayal/	Block	1
2.53.18.195	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.121.115.171	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/login.aspx	Block	1
79.181.97.242	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl33 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
45.79.71.122	United States	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 45.79.71.122	Block	1
77.138.57.9	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/brothers/kurs/default.asp	Block	1
2.53.191.239	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
180.76.15.144	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9182-he/refuah.aspx	Block	1
109.66.191.232	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/giyus	Block	1
66.249.69.216	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/forums/asp/showforum.asp	Block	1
81.218.225.134	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
46.19.86.148	Israel	147.237.76.31	nakchal.idf.il	Malformed URL	Block	1
45.79.71.122	United States	147.237.72.166	aka.idf.il	Malformed HTTP Header Line 3	Block	1
77.139.17.239	France	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
68.180.230.47	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1395-en/dover.aspx	Block	1
2.53.52.160	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
176.13.228.147	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
89.139.155.106	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.182.57.82	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
45.79.71.122	United States	147.237.72.166	aka.idf.il	Unknown HTTP Request Method 1 in URL	Block	1
5.22.134.207	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/favicon.ico	Block	1
109.253.218.64	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.69.218	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	Block	1
46.19.86.148	Israel	147.237.76.31	nakchal.idf.il	Unknown HTTP Request Method endToFriend.aspx?&l=he&f=894 in URL	Block	1
45.79.71.122	United States	147.237.72.166	aka.idf.il	Malformed URL	Block	1
212.76.120.127	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/default.aspx	Block	1
77.139.91.31	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	1

09-07-2016-20:04:04 to 09-07-2016-21:04:04