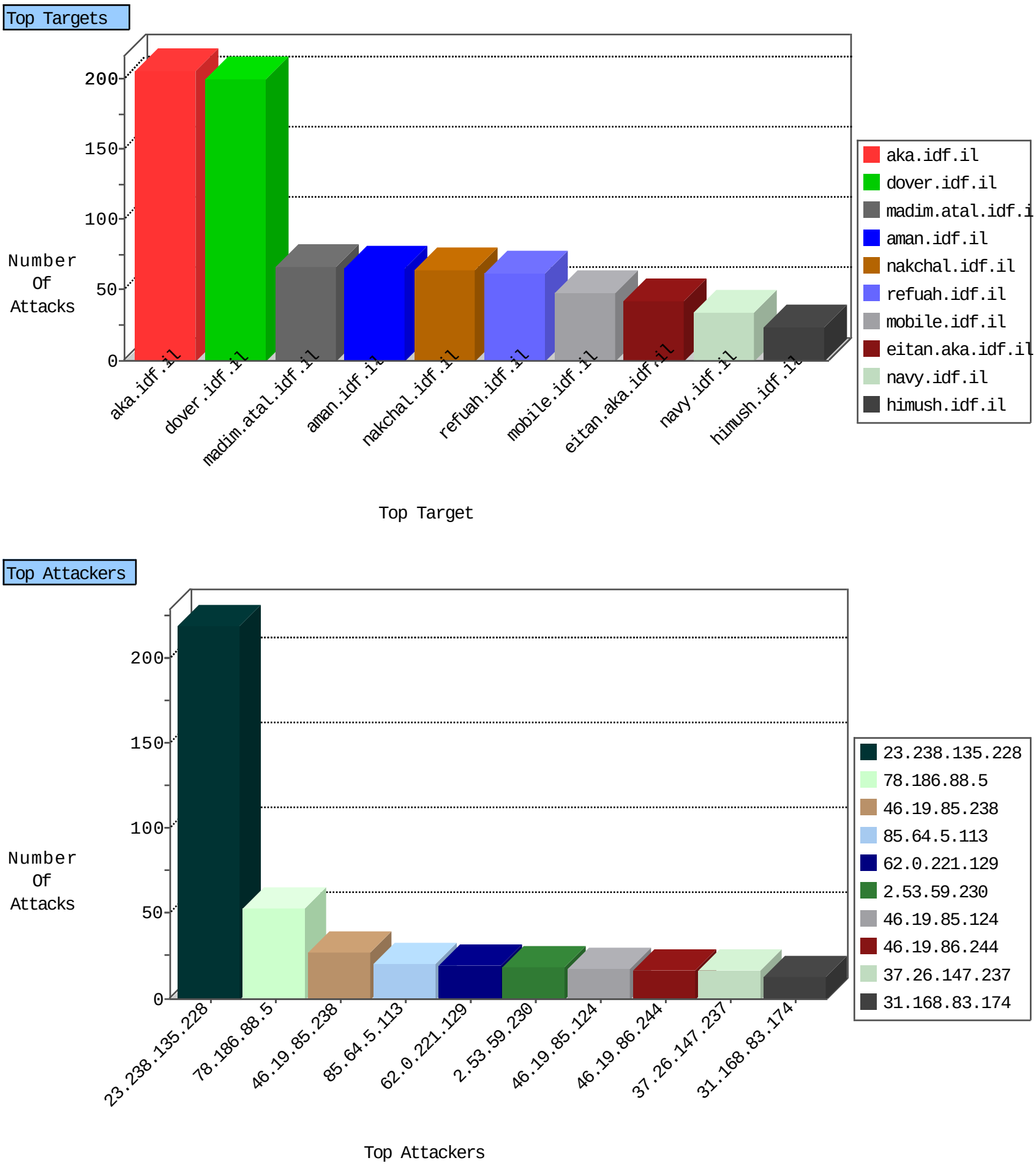
09-08-2016-09:04:05 to 09-08-2016-10:04:05

IDF Under Attack
Daily Report



09-08-2016-09:04:05 to 09-08-2016-10:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.226.40.40	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
58.218.200.137	China	147.237.76.176	test.ncore.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
71.6.216.57	United States	147.237.76.201	e.atal.idf.il	Black List	drop	1
85.64.16.40	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
10.0.0.2		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

09-08-2016-09:04:05 to 09-08-2016-10:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.29.217.24	Israel	147.237.72.156	aman.idf.il	32390: HTTP: Suspicious User-Agent (Mozilla)	Block	2

09-08-2016-09:04:05 to 09-08-2016-10:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
92.45.158.230	147.237.77.216	Turkey	dover.idf.il	portscan: TCP Distributed Portscan	1
82.166.94.133	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
61.163.52.38	147.237.76.196	China	e.sviva.idf.il	ET SCAN NMAP -f -sS	1
37.26.147.249	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.88.208.193	147.237.72.166	Russian Federation	aka.idf.il	ET SCAN NMAP -sS window 1024	1
2.53.137.214	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
150.242.238.99	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
117.159.34.194	147.237.76.196	China	e.sviva.idf.il	ET SCAN NMAP -sS window 2048	1
109.67.157.28	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.32.107.194	147.237.77.235	Italy	sviva.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
85.158.48.35	147.237.76.30	Russian Federation	himush.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
61.163.52.38	147.237.76.196	China	e.sviva.idf.il	ET SCAN NMAP -sS window 2048	1
58.218.200.137	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
212.182.116.196	147.237.72.166	Poland	aka.idf.il	portscan: TCP Distributed Portscan	1
2.53.163.135	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
163.172.169.150	147.237.8.27	United Kingdom	e.madim.atal.idf.i	ET SCAN NMAP -sS window 1024	1
150.242.238.99	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
117.159.34.194	147.237.76.196	China	e.sviva.idf.il	ET SCAN NMAP -f -sS	1
109.67.117.85	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-08-2016-09:04:05 to 09-08-2016-10:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
23.238.135.228	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	23
23.238.135.228	United States	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	23
23.238.135.228	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	22
23.238.135.228	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	22
23.238.135.228	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	22
23.238.135.228	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	22
23.238.135.228	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	22
78.186.88.5	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
85.64.5.113	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	21
23.238.135.228	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	21
62.0.221.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	20
46.19.85.238	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
78.186.88.5	Turkey	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
62.0.200.125	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.238	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
2.53.17.16	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
132.76.61.52	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
62.0.205.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
62.0.225.254	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
46.19.86.244	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
37.26.147.237	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
85.65.171.88	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
37.26.147.237	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.124	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
78.186.88.5	Turkey	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.13.237.248	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.119.168	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.179.21.194	Israel	147.237.76.177	ncore.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
78.186.88.5	Turkey	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.223.5	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
78.186.88.5	Turkey	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.86.244	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
87.69.36.210	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.45	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.114	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.85.45	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.114	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
2.53.167.42	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
2.53.178.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
87.69.36.210	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
185.32.179.73	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
193.43.246.250	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
109.253.145.88	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	4
62.0.203.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.124	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.91	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
185.86.140.230	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
213.8.98.193	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
79.176.33.146	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.59.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	19
31.168.83.174	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	13
46.19.86.178	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	11
109.253.241.146	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
2.53.48.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
2.53.145.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
46.19.86.65	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
31.168.71.114	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	4
212.179.21.194	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 212.179.21.194	Block	4
109.253.140.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
46.19.85.62	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	4
46.19.85.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.241.127	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	3
2.53.47.76	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
109.253.138.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.34	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.139.3.72	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	3
2.55.20.168	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
212.29.224.216	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 212.29.224.216	Block	2
109.67.157.28	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	1
2.53.61.144	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.178.204.71	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
180.97.106.161	China	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple NULL Character in Method from 180.97.106.161	Block	1
66.249.66.174	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/5/71545.pdf	Block	1
94.32.107.194	Italy	147.237.77.235	sviva.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
77.126.47.99	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
164.138.119.106	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
46.19.86.219	Israel	147.237.77.216	dover.idf.il	Malformed URL __atuvc=1	Block	1
109.253.135.17	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$btnSend.x in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
37.26.149.199	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
80.246.130.19	Israel	147.237.76.42	refuah.idf.il	Distributed Suspicious Response Code	Block	1
66.249.66.177	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/2/71562.pdf	Block	1
185.24.207.101	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __EVENTARGUMENT in www.aka.idf.il/main/giyus/	None	1
109.65.160.100	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
77.138.57.9	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
212.31.101.54	Cyprus	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash/sheelon.aspx	Block	1
176.13.2.178	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.86.219	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method ET_SessionId=ftcnmobv1l1zwsrhzec5eony; in URL __atuvc=1	Block	1
40.77.167.49	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
2.53.152.200	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
82.81.142.140	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;t in www.aka.idf.il/main/sachar/scriptresource.axd	None	1
66.249.66.180	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/1/71081.doc	Block	1
204.79.180.25	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/templates/home.asp	Block	1
132.74.56.157	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/iturim/asp/	Block	1
109.65.160.100	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
31.168.71.114	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 31.168.71.114	Block	1
77.138.249.220	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/faq.aspx	Block	1
176.13.248.215	Israel	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/894-ar	Block	1
46.19.86.244	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
2.53.156.254	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1