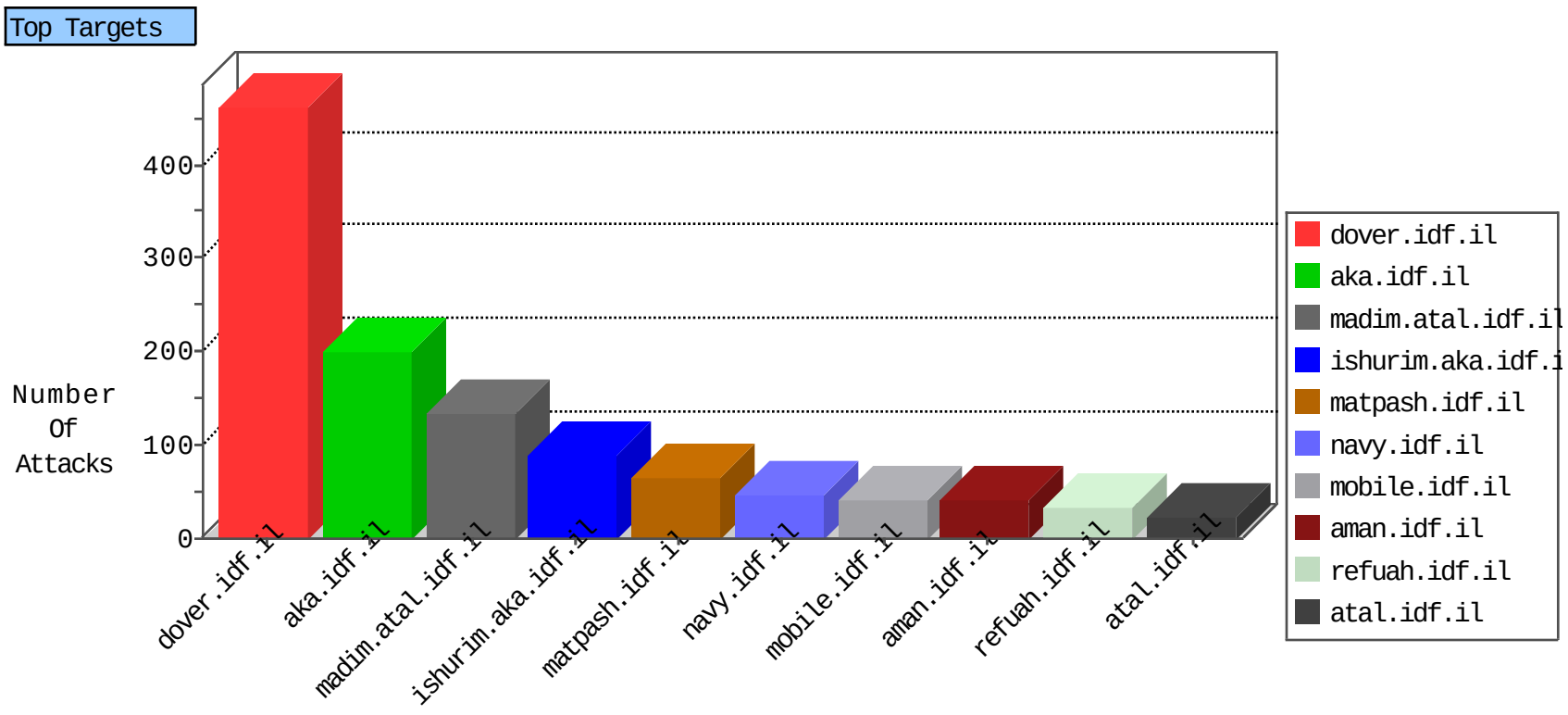
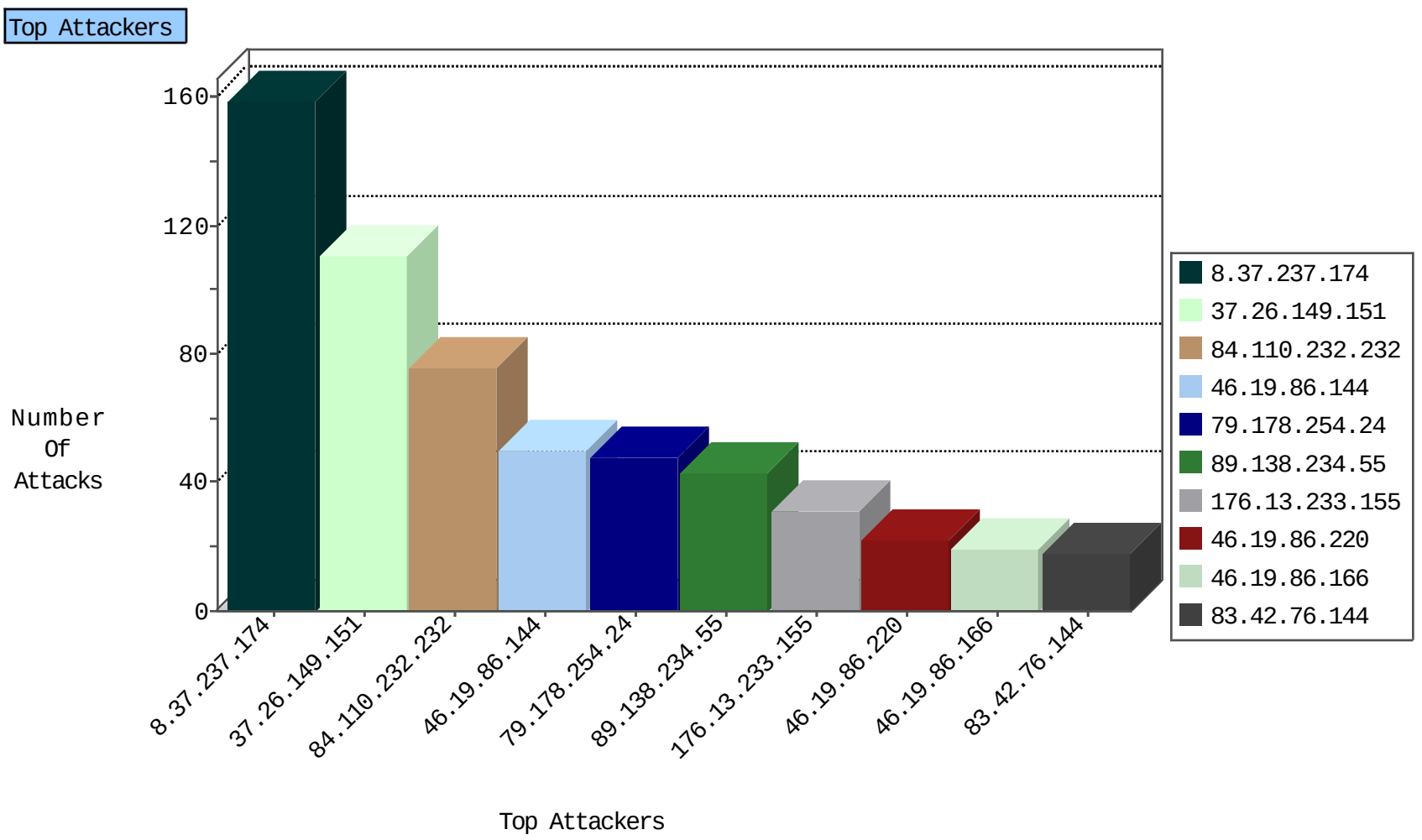
09-04-2016-19:04:02 to 09-04-2016-20:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-04-2016-19:04:02 to 09-04-2016-20:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
8.37.237.174	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	86
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	38
79.180.168.49	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
79.177.34.82	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
79.178.147.153	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
109.226.40.40	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
109.65.113.50	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
109.66.61.189	Israel	147.237.77.216	dover.idf.il	Black List	drop	3
8.37.237.174	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
180.97.106.161	China	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1
180.97.106.161	China	147.237.76.200	eitan.aka.idf.il	Black List	drop	1
217.23.9.123	Netherlands	147.237.76.177	ncore.idf.il	Black List	drop	1
179.99.200.39	Brazil	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	1
37.48.93.217	Netherlands	147.237.76.44	e.refuah.idf.il	Black List	drop	1

09-04-2016-19:04:02 to 09-04-2016-20:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.134.218.13	Russian Federation	147.237.72.166	aka.idf.il	5119: HTTP: Cross Site Scripting (HTML in HTTP Headers)	Block	1

09-04-2016-19:04:02 to 09-04-2016-20:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	7
91.121.135.78	147.237.72.166	France	aka.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	6
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	4
45.79.71.122	147.237.72.166	United States	aka.idf.il	WEB-MISC Chunked-Encoding transfer attempt	2
94.156.128.25	147.237.76.34	Bulgaria	yohalan.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.0.33	Netherlands	idf.il	ET SCAN NMAP -sS window 1024	1
77.124.23.63	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
211.23.156.152	147.237.72.14	Taiwan	dover.idf.il(old	ET SCAN Potential SSH Scan	1
64.137.171.55	147.237.76.31	Canada	nakchal.idf.il	ET SCAN Potential SSH Scan	1
192.114.3.241	147.237.0.34	Israel	tikshuv.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
114.233.54.8	147.237.76.30	China	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
103.207.36.84	147.237.76.196	Vietnam	e.sviva.idf.il	ET SCAN NMAP -sS window 2048	1
94.156.128.25	147.237.77.19	Bulgaria	law-forum.idf.il	ET SCAN Potential SSH Scan	1
94.102.52.71	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.158	147.237.8.45	Ukraine	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
79.177.6.77	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
64.137.171.55	147.237.77.19	Canada	law-forum.idf.il	ET SCAN Potential SSH Scan	1
208.100.26.228	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 1024	1
186.170.213.135	147.237.0.34	Colombia	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
103.207.36.84	147.237.76.196	Vietnam	e.sviva.idf.il	ET SCAN NMAP -sS window 3072	1
103.207.36.84	147.237.76.196	Vietnam	e.sviva.idf.il	ET SCAN NMAP -f -sS	1

09-04-2016-19:04:02 to 09-04-2016-20:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
8.37.237.174	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	75
84.110.232.232	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	37
84.110.232.232	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	monitor	36
8.37.237.174	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	23
89.138.234.55	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
79.178.254.24	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
79.178.254.24	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	19
176.13.236.18	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
176.13.233.155	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	15
46.19.86.144	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
176.228.136.129	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
46.19.86.144	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
109.65.183.177	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
62.0.234.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
46.19.86.144	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
46.19.86.220	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
46.19.86.220	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.19.86.144	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
176.13.233.155	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
46.19.86.166	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
79.178.254.24	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
37.26.149.151	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence		monitor	10
176.13.246.160	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.243.194.244	Poland	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
89.138.234.55	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
109.253.143.73	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
83.42.76.144	Spain	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
37.26.149.151	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence		alert	8
46.19.85.244	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.133.98.5	Ukraine	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.96	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
195.60.235.57	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
46.19.85.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
177.72.17.91	Brazil	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
46.19.85.206	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.185	Israel	147.237.76.86	navy.idf.il	drop	SAM rule	drop	6
37.26.146.192	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
89.138.234.55	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	6
46.19.85.206	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.13.16.118	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
141.226.217.96	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
37.26.149.151	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.185	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	5
77.127.32.39	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.166	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.109	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
89.139.151.92	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
2.53.143.90	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.85.109	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.123	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4

09-04-2016-19:04:02 to 09-04-2016-20:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.149.151	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	86
80.246.130.24	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.120.122.219	Block	4
77.138.134.62	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	3
109.253.147.32	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.215.244	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1381	Block	3
2.55.5.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.126.33.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.246.160	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.64.135.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.57.165.51	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	3
2.53.13.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
217.153.185.109	Poland	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
207.46.13.90	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
37.46.41.132	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
212.199.57.202	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
79.180.250.232	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
2.55.176.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.65.129.245	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
192.114.3.241	Israel	147.237.0.34	tikshuv.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	2
80.74.101.10	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationexplanation.aspx	None	1
68.180.229.49	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
207.46.13.78	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/robots.txt	Block	1
157.55.39.111	United States	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to kosher-kravi.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
46.19.86.166	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
93.173.165.19	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
66.249.64.223	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1462-he/atal.aspx	Block	1
180.76.15.144	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english	Block	1
45.79.71.122	United States	147.237.72.166	aka.idf.il	Multiple Malformed URL from 45.79.71.122	Block	1
2.53.146.57	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
68.180.229.153	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in nakhal.idf.il/1073-he/nakhal.aspx	Block	1
176.13.233.155	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
46.116.64.142	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
95.86.86.3	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/https:/www.aman.idf.il/	Block	1
79.176.25.83	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage	Block	1
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/rights/asp/info.asp?moduleid=2&catid=22703&docid=22721	Block	1
192.114.3.241	Israel	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to 147.237.0.15/	Block	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
80.246.138.133	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
45.79.71.122	United States	147.237.72.166	aka.idf.il	Malformed HTTP Header Line 2	Block	1
66.249.79.21	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
192.114.3.241	Israel	147.237.0.19	madim.atal.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
131.253.24.157	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
45.79.71.122	United States	147.237.72.166	aka.idf.il	Unknown HTTP Request Method 1 in URL	Block	1
82.166.158.124	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
77.127.0.244	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 77.127.0.244	Block	1
176.13.246.160	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/portalmiluim/templates/inner.asp	Block	1
45.79.71.122	United States	147.237.72.166	aka.idf.il	Malformed URL	Block	1
79.181.251.139	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$passwordUpdate$hiddenUpdatePassword in www.aka.idf.il/main/giyus/faq.aspx	None	1

09-04-2016-19:04:02 to 09-04-2016-20:04:02