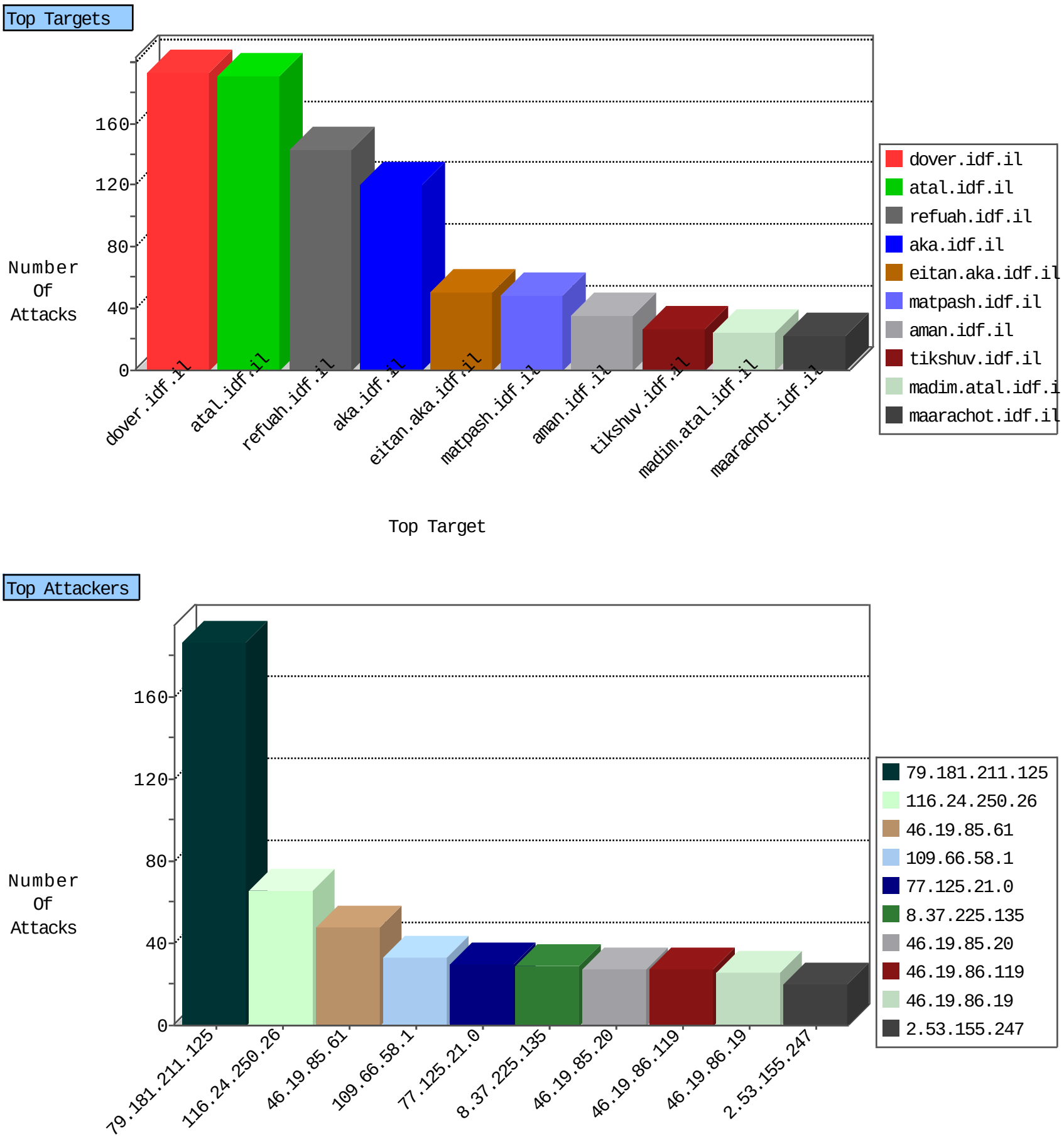
10-04-2016-20:04:06 to 10-04-2016-21:04:06

IDF Under Attack Daily Report



10-04-2016-20:04:06 to 10-04-2016-21:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.94.111.1	Russian Federation	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1
194.177.16.3	Israel	147.237.76.86	navy.idf.il	Black List	drop	1
119.41.216.165	China	147.237.77.121	e.navy.idf.il	Invalid TCP Flags	drop	1
119.41.216.165	China	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

10-04-2016-20:04:06 to 10-04-2016-21:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.243.26.28	Belgium	147.237.77.170	maarachot.idf.il	18160: HTTP: Critroni Likely Malicious Tor Proxy Cookie	Block	1

10-04-2016-20:04:06 to 10-04-2016-21:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.19.85.61	147.237.77.216	Israel	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	48
84.108.214.219	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	4
84.108.214.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	3
91.201.236.50	147.237.77.234	Ukraine	halag.idf.il	ET SCAN NMAP -sS window 4096	1
62.210.243.100	147.237.0.15	France	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
62.150.255.205	147.237.76.148	Kuwait	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.230.71	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
54.147.8.50	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
180.213.5.205	147.237.76.39	China	mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
144.48.2.130	147.237.77.74		law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
40.114.15.49	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.72.217	Netherlands	e.idf.il	ET SCAN NMAP -sS window 1024	1
5.29.167.187	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	1
91.201.236.50	147.237.77.234	Ukraine	halag.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.50	147.237.77.234	Ukraine	halag.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
62.150.255.205	147.237.76.148	Kuwait	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 2048	1
209.126.230.71	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
62.150.255.205	147.237.76.148	Kuwait	gqcenter.aka.idf.il	ET SCAN NMAP -f -sS	1
208.100.26.228	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 1024	1
46.172.91.21	147.237.76.177	Ukraine	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
180.213.5.205	147.237.76.34	China	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
42.112.28.187	147.237.76.176	Vietnam	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
130.193.83.134	147.237.76.30	United Kingdom	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
8.37.225.135	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.195	147.237.72.166	Netherlands	aka.idf.il	ET SCAN NMAP -sS window 1024	1

10-04-2016-20:04:06 to 10-04-2016-21:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
79.181.211.125	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	187
109.66.58.1	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	32
77.125.21.0	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
8.37.225.135	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
46.19.86.119	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	23
46.19.85.20	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	23
185.120.124.87	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	10
46.19.86.19	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	10
66.102.9.159	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	8
79.178.27.63	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	7
46.19.85.1	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
141.226.161.226	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.55.148.101	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
2.53.40.103	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.89	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.85.1	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.19	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.19.86.159	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
110.168.203.25	Thailand	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
52.64.53.229	Australia	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	5
46.19.86.19	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	5
46.19.85.137	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
174.89.234.10	Canada	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.85	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.197	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
199.30.16.186	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.76	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
197.48.191.242	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.81	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.137	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.86.85	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
51.255.47.108	France	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
79.181.254.211	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
89.138.93.188	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
213.8.204.44	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.197	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
109.253.212.232	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.85.70	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.85.217	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
207.46.13.116	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.136.220	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
5.22.134.75	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
31.210.186.35	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
5.22.134.99	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.181.254.211	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.46.38.97	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
37.26.146.191	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
46.19.86.19	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

10-04-2016-20:04:06 to 10-04-2016-21:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
116.24.250.26	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 116.24.250.26	Block	30
2.53.155.247	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 2.53.155.247	Block	19
116.24.250.26	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 116.24.250.26	Block	17
116.24.250.26	China	147.237.77.176	matpash.idf.il	PHP Attempt	Block	11
46.19.86.205	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
79.177.37.124	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	9
116.24.250.26	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	6
62.122.180.137	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation lang in www.idf.il/1398-en/dover.aspx	Block	5
62.122.180.137	Russian Federation	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2113-en/cogat.aspx	Block	4
80.246.136.148	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	3
2.53.49.42	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
82.166.240.201	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.10	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.53.143.22	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
77.138.165.207	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/	Block	2
37.142.182.251	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.120.113.100	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 46.120.113.100	Block	2
46.19.85.74	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
2.53.55.47	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 2.53.55.47	Block	2
2.53.55.47	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	1
73.232.44.60	United States	147.237.76.86	navy.idf.il	NULL Character in Method ,[[#0]][[#0]][[#0]][[#19]]ñ[ÉÙÏ`¿ª•¾ŸHfÔ6[[#16]][[#7]]•¹,ÃÂ×õSS,6À[[#30]]©'[[#25]]ª±VcK¼ü•Ë[[#16]]-½-$Lur8ù²!ÒÜƒ:[[#1]]Ä%•[[#12]]ç[[#28]]Ðqëð•[[#29]]"•Êýú[[#2]]Ü[[#25]]	Block	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.177	Block	1
46.120.113.100	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
109.253.218.17	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
79.180.36.35	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl09 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
5.22.134.99	Israel	147.237.72.166	aka.idf.il	Unknown Parameter asm in www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	None	1
73.232.44.60	United States	147.237.76.86	navy.idf.il	Abnormally Long Request method	Block	1
116.24.250.26	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.asp	Block	1
66.249.64.30	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
109.66.58.1	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
46.19.86.19	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
66.249.66.242	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/164-3447-he	Block	1
79.183.39.16	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/kiosk/kiosk.aspx	Block	1
73.232.44.60	United States	147.237.76.86	navy.idf.il	Illegal Byte Code Character in Header Name	Block	1
176.13.0.189	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/9/71579.pdf	Block	1
109.66.150.241	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
77.139.180.13	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/4/69314.pdf	Block	1
62.122.180.137	Russian Federation	147.237.77.176	matpash.idf.il	Parameter Type Violation lang in www.cogat.idf.il/2113-en/cogat.aspx	Block	1
40.77.167.66	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
73.232.44.60	United States	147.237.76.86	navy.idf.il	Illegal Byte Code Character in Method ,[[#0]][[#0]][[#0]][[#19]]ñ[ÉÙÏ`¿ª•¾ŸHfÔ6[[#16]][[#7]]•¹,ÃÂ×õSS,6À[[#30]]©'[[#25]]ª±VcK¼ü•Ë[[#16]]-½-$Lur8ù²!ÒÜƒ:[[#1]]Ä%•[[#12]]ç[[#28]]Ðqëð•[[#29]]"•Êýú[[#2]]Ü[[#25]]	Block	1
185.27.105.85	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/requestpayslipexplanation.aspx	None	1
66.249.64.145	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/templatecontrols/links/undefined	Block	1
109.253.140.241	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
2.53.155.247	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/6/112306.pd	Block	1
66.249.76.79	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/9/71549.pdf	Block	1
73.232.44.60	United States	147.237.76.86	navy.idf.il	Illegal HTTP Version	Block	1
66.249.65.20	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/9/69409.pdf	Block	1
46.120.113.100	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1

10-04-2016-20:04:06 to 10-04-2016-21:04:06