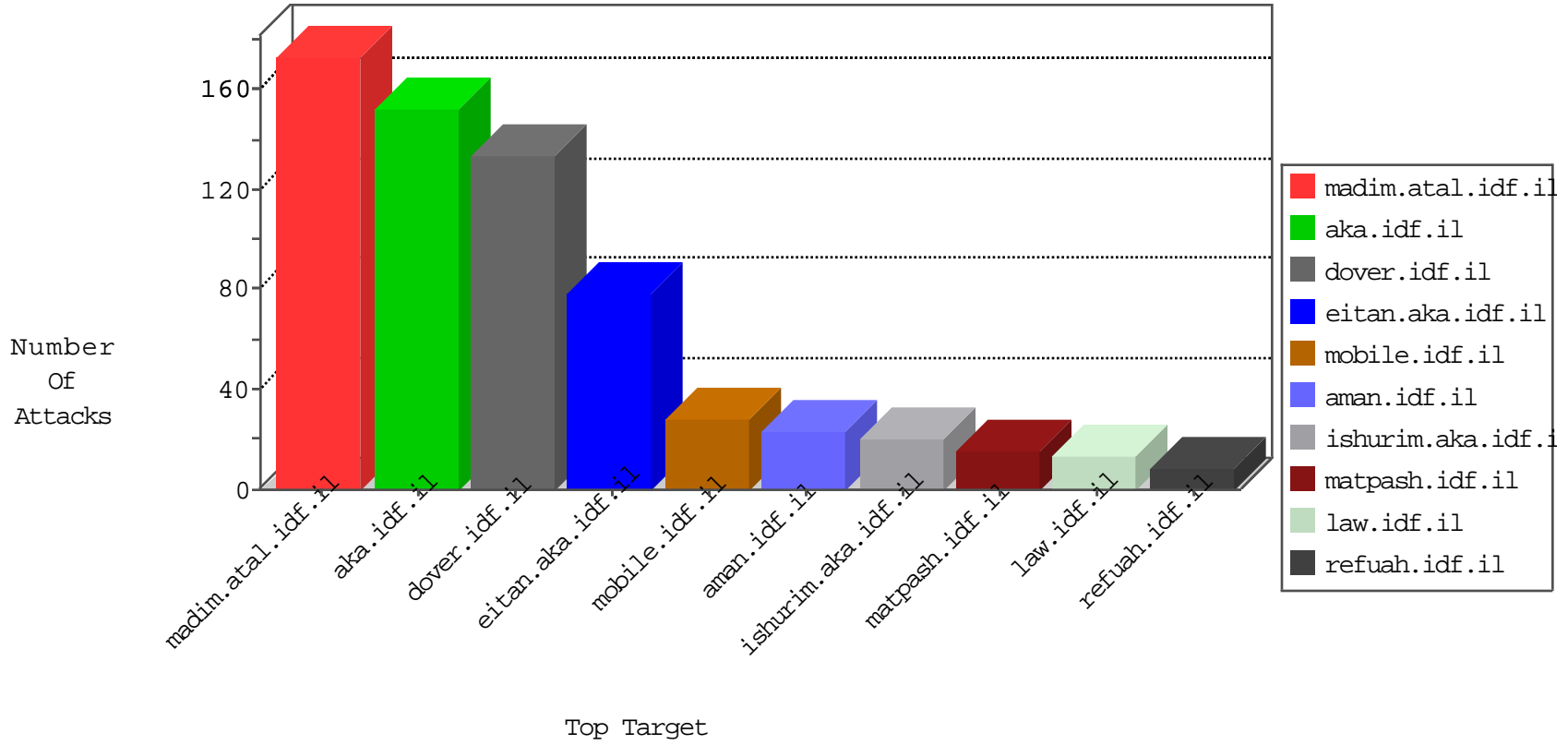


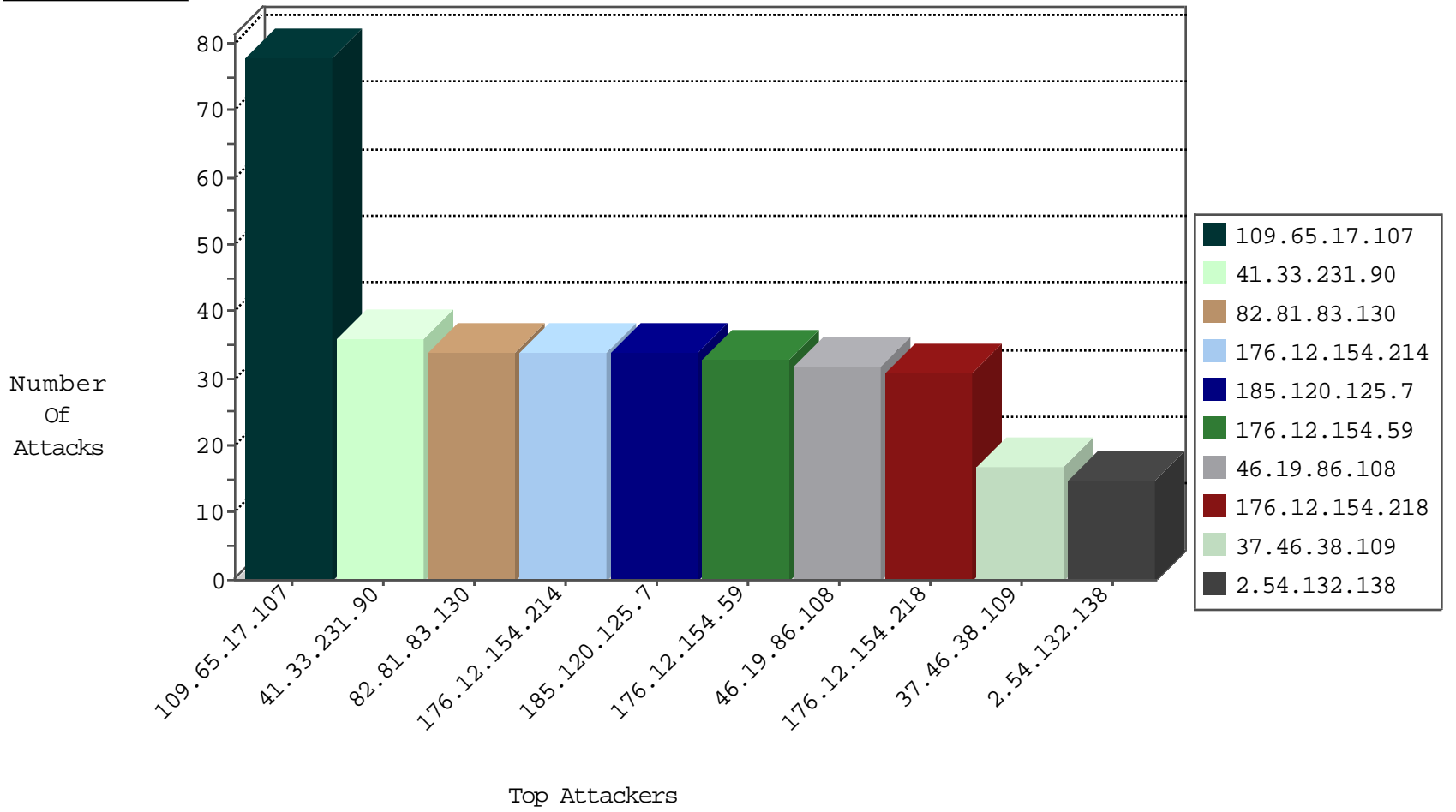
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.215.135.219	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
31.168.240.21	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
89.46.102.242	Romania	147.237.76.198	e.ychalan.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
2.54.30.246	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
195.62.52.41	147.237.76.198	Russian Federation	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.196	147.237.77.176		matpash.idf.il	ET SCAN NMAP -sS window 1024	1
173.55.32.113	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
69.30.254.186	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.18	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.62.52.41	147.237.76.202	Russian Federation	e.halag.idf.il	ET SCAN Potential SSH Scan	1
195.62.52.41	147.237.76.148	Russian Federation	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
192.115.203.25	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
178.162.208.141	147.237.77.233	Germany	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
79.178.123.67	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.0.34.177	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
82.81.83.130	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	34
185.120.125.7		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	22
109.65.17.107	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
185.120.125.7		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
176.12.154.121	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.148.145	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
80.74.105.107	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
138.134.102.15	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
83.250.78.86	Sweden	147.237.77.176	matpash.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.168	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.66.142.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.12.155.35	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
89.138.35.206	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
31.154.135.205	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
46.19.85.172	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
31.154.135.205	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
31.154.135.205	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
2.54.132.138	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
79.182.141.180	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.215.135.219	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
212.179.212.59	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.132.138	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.85.172	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.54.5.139	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.98	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
172.58.153.139	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
2.54.132.138	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
82.102.169.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.179.9.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.132.138	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
84.109.194.242	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
80.246.136.135	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.12.155.125	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.132.138	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.109.194.242	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.26.147.237	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
76.115.96.90	United States	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
176.12.154.143	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.146.198	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.80.196.44	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
37.26.147.254	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	2
176.12.154.156	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
62.0.75.197	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
37.26.147.178	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		alert	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.12.154.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	34
176.12.154.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
46.19.86.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
176.12.154.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
37.46.38.109	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	17
80.246.136.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
40.77.167.68	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/modiin/modiin/default.aspx	Block	4
37.26.148.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
188.143.232.35	Russian Federation	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 188.143.232.35	Block	3
46.19.85.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
93.173.49.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.223	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
37.26.148.216	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
176.12.154.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.12.154.121	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
76.115.96.90	United States	147.237.77.74	law.idf.il	Suspicious Response Code	Block	2
188.143.232.35	Russian Federation	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 188.143.232.35	Block	2
176.12.154.130	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	2
79.180.97.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
149.78.169.23	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	2
37.26.148.165	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
93.173.143.143	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1115-ar/dover.aspx	Block	1
38.81.65.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
110.93.217.10	Pakistan	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
80.246.136.24	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
212.5.158.158	Bulgaria	147.237.77.74	law.idf.il	PHP Attempt	Block	1
95.86.98.216	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/453-he/patzar.aspx&sa=u&ved=0ahukewja15y_rtjkahujohokhsc6agqgfggamac&sig2=jrhujonb8-tewueqaeayenq&usg=afqjcnfiffgetm5mw_ditcksrtaotsonngw	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9330-he/refuah.aspx	Block	1
40.77.167.34	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/smalim/smalim.aspx	None	1
110.93.217.10	Pakistan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
212.5.158.158	Bulgaria	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
95.86.98.216	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 95.86.98.216	Block	1
149.78.25.64	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
84.108.76.198	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/sachar/undefined	Block	1
66.249.78.4	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1237-he/atal.aspx	Block	1
95.86.98.216	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1279-he/cogat.aspx&sa=u&ved=0ahukewignqaf9jka hwg2rokhb9qcxgqfggimaa&usg=afqjcnun8bgj6tyzckq_loom0posduz2a	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
176.12.154.193	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
37.46.39.173	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/	Block	1
109.66.195.54	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mivtza	Block	1
80.74.105.107	Israel	147.237.72.167	ishurim.aka.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 80.74.105.107	Block	1
191.232.136.126	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1