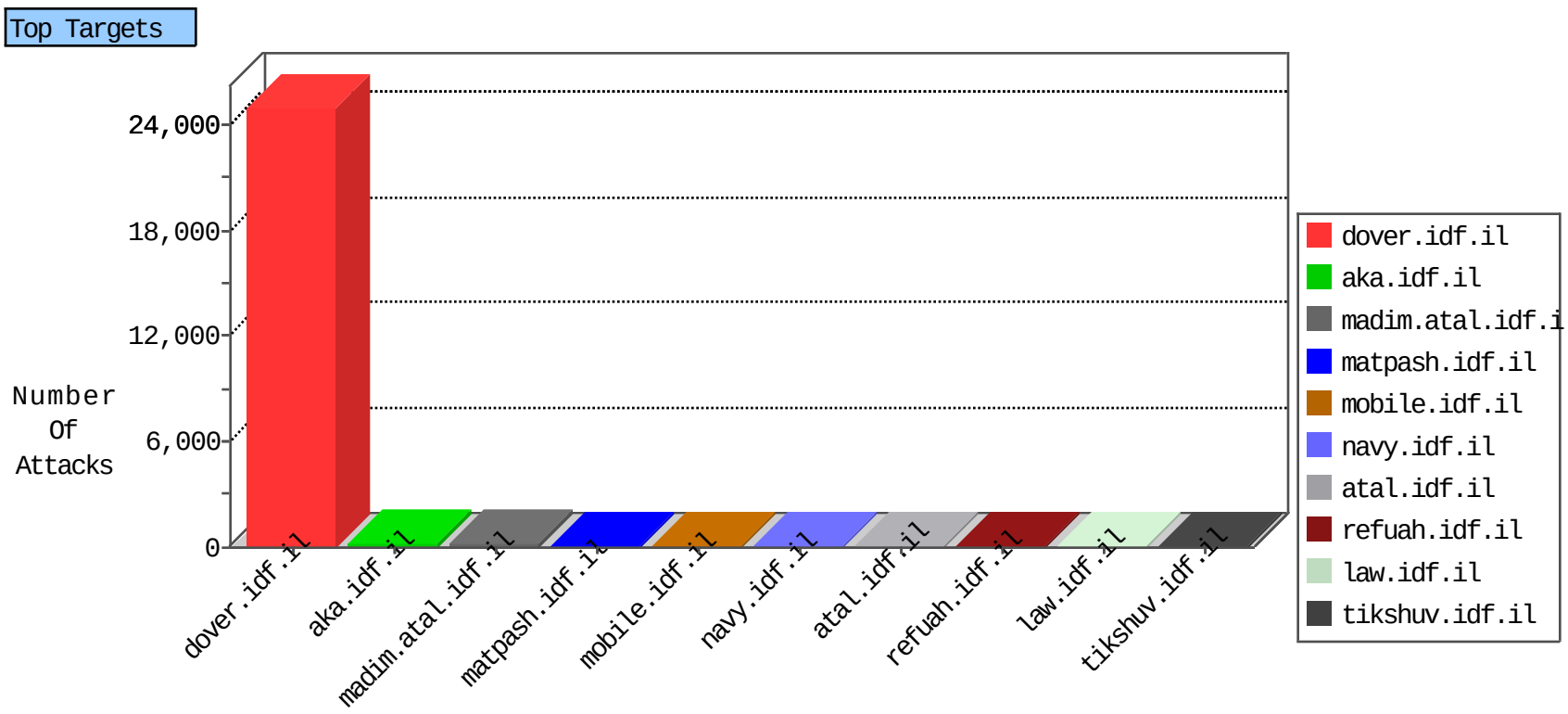
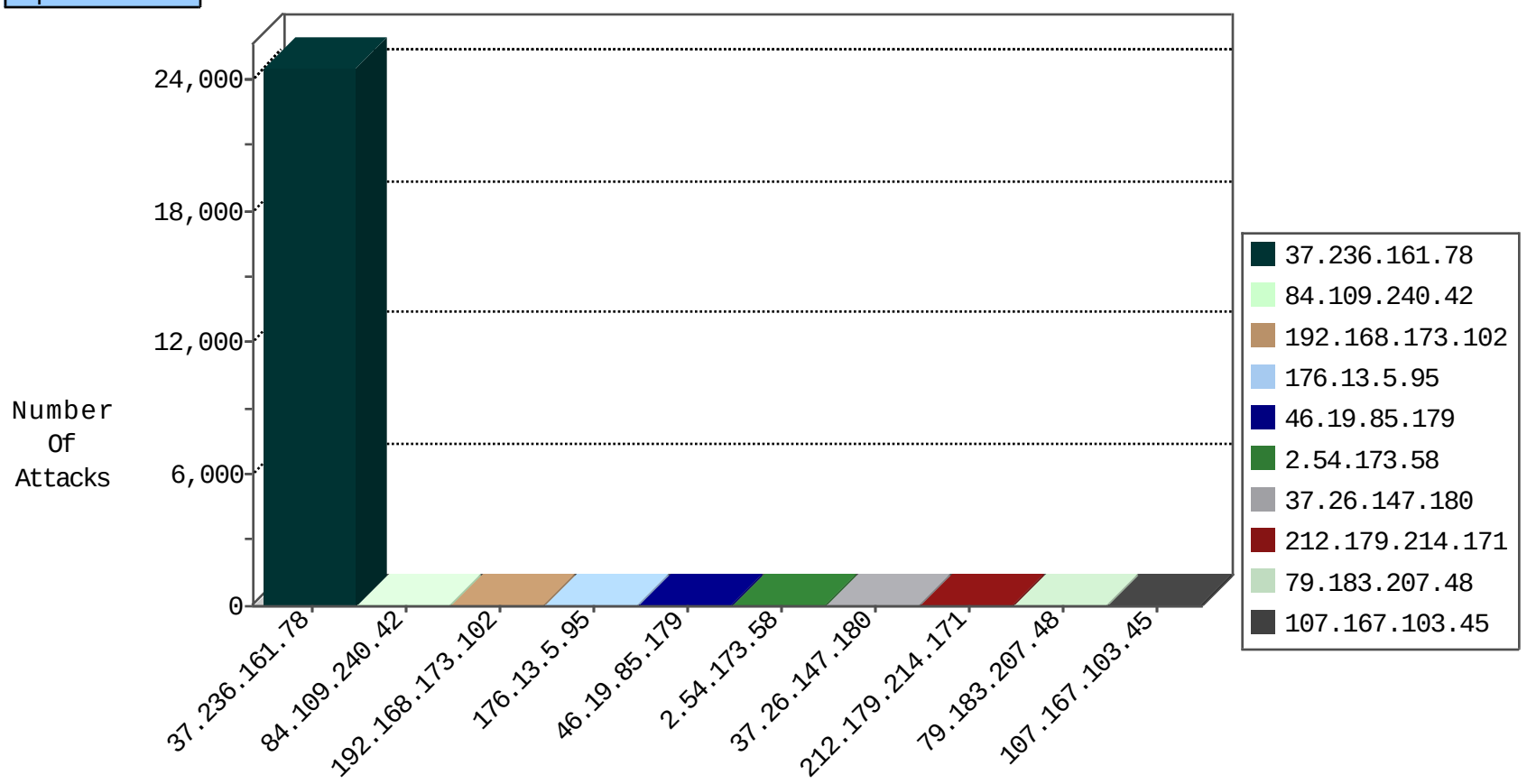
03-07-2016-22:04:01 to 03-07-2016-23:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-07-2016-22:04:01 to 03-07-2016-23:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.236.161.78	Iraq	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
37.236.161.78	Iraq	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
46.19.85.133	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
89.248.174.4	Netherlands	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
71.6.216.38	United States	147.237.72.217	e.idf.il	Block_Ntp_All_Net	drop	1
212.124.126.46	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
78.152.21.90	Poland	147.237.77.243	mobile.idf.il	Block_Udp_All_Nets	drop	1
149.50.90.216	United States	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
71.6.216.38	United States	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
185.35.62.78	Switzerland	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	1
78.152.21.90	Poland	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	1
84.108.76.71	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
46.19.85.179	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
185.130.5.224		147.237.77.233	atal.idf.il	Block_Udp_All_Nets	drop	1
78.152.21.90	Poland	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1

03-07-2016-22:04:01 to 03-07-2016-23:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.120.173.109	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	6
82.166.69.222	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
66.249.93.125	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	2
109.253.156.112	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
66.249.93.121	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-07-2016-22:04:01 to 03-07-2016-23:04:01

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
217.66.232.187	147.237.77.176	Palestinian Territory, Occupied	matpash.idf.il	ET SCAN NMAP -sA (2)	2
162.213.154.10	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
104.215.89.20	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
94.102.48.193	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
210.212.236.235	147.237.76.199	India	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
37.1.209.203	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 1024	1
210.212.236.235	147.237.0.34	India	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
210.212.236.235	147.237.0.15	India	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
199.255.137.113	147.237.77.226	Belgium	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 3072	1
199.255.137.113	147.237.77.226	Belgium	www.chamatz.aka.idf.il	ET SCAN NMAP -f -sS	1
186.205.48.210	147.237.76.30	Brazil	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.215.89.20	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
104.215.89.20	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -f -sS	1
210.212.236.235	147.237.76.200	India	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.193	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
210.212.236.235	147.237.76.38	India	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
5.39.222.253	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
210.212.236.235	147.237.0.16	India	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.76.34	United States	yohalan.idf.il	ET SCAN Potential SSH Scan	1
199.255.137.113	147.237.77.226	Belgium	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 2048	1

03-07-2016-22:04:01 to 03-07-2016-23:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.236.161.78	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23292
37.236.161.78	Iraq	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1064
37.236.161.78	Iraq	147.237.77.216	dover.idf.il	drop		drop	200
192.168.173.102		147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	50
37.26.147.180	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	31
107.167.103.45	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	23
46.19.85.179	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
192.168.173.102		147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	17
212.179.214.171	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
212.179.214.171	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	15
79.183.207.48	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	14
37.26.147.180	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
212.179.214.171	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	13
46.19.86.88	Israel	147.237.77.176	matpash.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.147.140	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.183.207.48	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
37.142.198.183	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
46.19.85.1	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
37.142.198.183	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
84.111.108.176	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
46.19.85.179	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.179	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
46.19.85.133	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.105	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.45	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.180.20.13	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.46.39.151	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
87.71.82.250	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.179	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.105	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
217.194.193.26	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.139.243	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.1	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.46.39.225	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
84.109.112.219	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
5.102.254.208	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.42	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.179	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
5.102.254.208	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
31.154.159.248	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
31.154.159.248	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.86.130	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
5.102.254.206	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
213.57.196.35	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
50.97.138.113	United States	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	4
79.183.202.47	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.142.231.210	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4

03-07-2016-22:04:01 to 03-07-2016-23:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.109.240.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	71
176.13.5.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	60
2.54.173.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	44
185.32.179.1	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	15
109.253.157.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
66.249.64.50	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.50	Block	10
37.26.149.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.50.60	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
79.178.25.28	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.108.232.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.174.84	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
82.166.242.20	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
109.66.17.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.183.207.48	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
212.143.38.222	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
66.249.64.131	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
109.160.207.184	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
84.109.112.219	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
77.247.181.162	Netherlands	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
52.37.168.145	United States	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 52.37.168.145	Block	1
94.230.86.136	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
31.168.31.178	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/xmlrpc.php	Block	1
80.246.130.145	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
213.57.142.180	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/	Block	1
66.249.64.233	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1514-en/dover.aspx.	Block	1
40.77.167.92	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
52.37.168.145	United States	147.237.77.226	www.chamatz.aka.idf.il	Distributed PHP Attempt	Block	1
98.183.230.213	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
37.26.148.168	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
80.246.139.243	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.64.240	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
46.117.43.117	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
109.253.157.248	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
84.110.34.142	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/main/sachar/faq.aspx	None	1
79.178.175.53	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
193.201.227.152	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1044-he/ishurim.aspx	Block	1
52.37.168.145	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/wp-login.php	Block	1
37.26.148.168	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
98.183.230.213	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
66.249.73.190	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/2/242.doc	Block	1
52.37.168.145	United States	147.237.0.19	madim.atal.idf.il	Distributed PHP Attempt	Block	1
157.55.39.183	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/main/haredim/general.aspx	None	1
85.181.50.81	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
8.37.230.115	Anonymous Proxy	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.178.175.53	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	1
212.143.38.222	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1
37.26.148.215	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.52.157.109	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.73.204	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
175.139.159.50	Malaysia	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/163-7183-en/patzar.aspx+www.163.com	Block	1

03-07-2016-22:04:01 to 03-07-2016-23:04:01