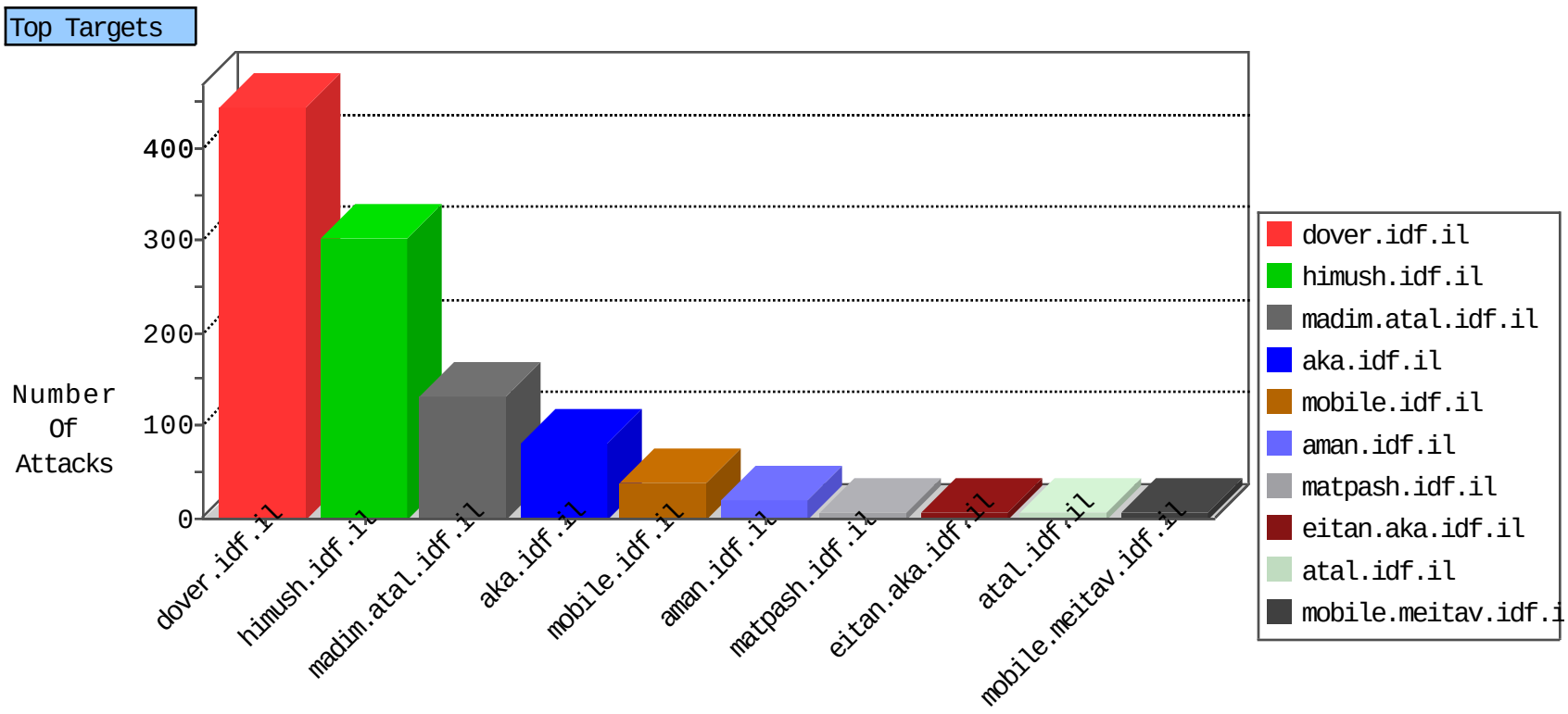
10-03-2016-20:04:06 to 10-03-2016-21:04:06

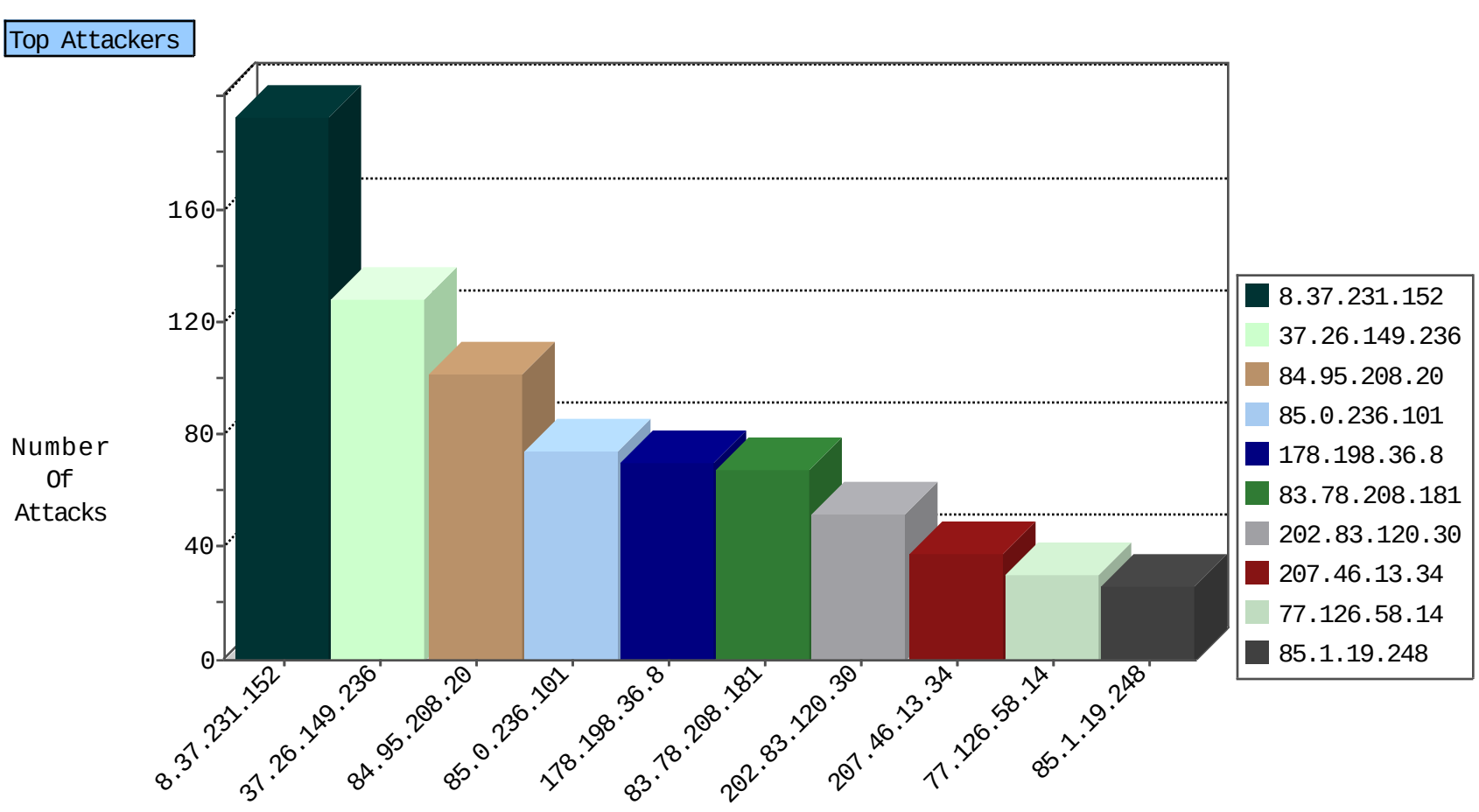
IDF Under Attack
Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

10-03-2016-20:04:06 to 10-03-2016-21:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.95.208.20	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
109.226.40.40	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
50.87.144.145	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
8.37.231.152	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	3
71.6.216.42	United States	147.237.76.31	nakchal.idf.il	Black List	drop	1

10-03-2016-20:04:06 to 10-03-2016-21:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
51.254.32.77	France	147.237.77.170	maarachot.idf.il	C1000074: HTTP: majestic bot	Permit	2
195.154.187.115	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
195.154.187.115	France	147.237.77.233	atal.idf.il	C1000074: HTTP: majestic bot	Permit	2

10-03-2016-20:04:06 to 10-03-2016-21:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
96.37.146.131	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 2048	1
78.129.171.173	147.237.76.148	United Kingdom	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
27.12.211.101	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
14.152.59.11	147.237.77.176	China	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
2.53.59.12	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
201.114.60.162	147.237.76.38	Mexico	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.0.35	China	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
96.37.146.131	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 4096	1
96.37.146.131	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -f -sS	1
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	1
14.152.59.11	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 1024	1
2.53.147.26	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
201.114.60.162	147.237.76.38	Mexico	e.e.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
198.20.69.98	147.237.76.39	United States	mobile.meitav.idf.i	ET DROP Dshield Block Listed Source	1
183.60.48.25	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
177.154.52.42	147.237.0.33	Brazil	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

10-03-2016-20:04:06 to 10-03-2016-21:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
8.37.231.152	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	141
8.37.231.152	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	49
207.46.13.34	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	38
77.126.58.14	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
66.249.65.53	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	19
85.0.236.101	Switzerland	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
178.198.36.8	Switzerland	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
83.78.208.181	Switzerland	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	15
85.0.236.101	Switzerland	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	15
83.78.208.181	Switzerland	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
85.0.236.101	Switzerland	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	15
178.198.36.8	Switzerland	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	15
85.0.236.101	Switzerland	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	15
83.78.208.181	Switzerland	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	14
178.198.36.8	Switzerland	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	14
178.198.36.8	Switzerland	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	13
202.83.120.30	Indonesia	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
46.19.86.5	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
85.0.236.101	Switzerland	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
83.78.208.181	Switzerland	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	13
202.83.120.30	Indonesia	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	12
178.198.36.8	Switzerland	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
202.83.120.30	Indonesia	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	12
83.78.208.181	Switzerland	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.19.86.5	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
202.83.120.30	Indonesia	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
80.246.138.15	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
85.1.19.248	Switzerland	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
202.83.120.30	Indonesia	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
147.236.72.197	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
85.1.19.248	Switzerland	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	6
147.236.72.197	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.95.37.89	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
85.1.19.248	Switzerland	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
85.1.19.248	Switzerland	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	5
193.5.216.100	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
5.22.134.72	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
85.1.19.248	Switzerland	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
85.64.73.89	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.121.120.89	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
37.46.41.245	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.175	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.226.40.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
54.82.56.247	United States	147.237.76.39	mobile.meitav.idf.i	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
185.3.147.75	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.109.102.202	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
134.35.236.233	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
84.95.208.20	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3

10-03-2016-20:04:06 to 10-03-2016-21:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.149.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	128
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	71
2.53.179.222	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 2.53.179.222	Block	8
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	5
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	5
213.57.229.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
2.53.141.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
79.183.39.16	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.183.39.16	Block	2
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/8/69058.pdf	Block	1
85.64.144.11	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
82.81.251.28	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	None	1
79.36.199.120	Italy	147.237.77.216	dover.idf.il	Multiple Redundant HTTP Headers in header Referer	Block	1
66.249.69.20	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/398-	Block	1
46.117.112.148	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in atal.idf.il/1440-he/atal.aspx	Block	1
80.246.137.149	Israel	147.237.72.166	aka.idf.il	Abnormally Long Request method	Block	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1393-en/dover.aspx	Block	1
66.249.64.43	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/2/71762.pdf	Block	1
89.237.64.126	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
46.19.86.67	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
79.36.199.120	Italy	147.237.77.216	dover.idf.il	Redundant HTTP Headers Referer	Block	1
66.249.73.133	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/894-he/dover.aspx	Block	1
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/patzar/klali/default.asp	Block	1
80.246.137.149	Israel	147.237.72.166	aka.idf.il	Malformed URL	Block	1
68.180.231.60	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-he/cogat.aspx	Block	1
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/watch	Block	1
109.66.60.102	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$emailUpdate$rptEmailSubjectsLi in www.aka.idf.il/main/giyus/userdetails/updateuserdetails.aspx	None	1
46.19.86.151	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	1
79.36.199.120	Italy	147.237.77.216	dover.idf.il	Redundant HTTP Headers from 79.36.199.120	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/0/69400.jpg	Block	1
54.82.56.247	United States	147.237.76.39	mobile.meitav.idf.il	Distributed Malformed URL	Block	1
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	1
80.246.137.149	Israel	147.237.72.166	aka.idf.il	Unknown HTTP Request Method .1 in URL www.aka.idf.il	Block	1
68.180.231.60	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1927-he/cogat.aspx	Block	1
109.66.60.102	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.66.103	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
46.19.86.151	Israel	147.237.77.216	dover.idf.il	Malformed URL he-il,he;q=0.8,en-us;q=0.6,en;q=0.4	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/3/71763.pdf	Block	1
54.82.56.247	United States	147.237.76.39	mobile.meitav.idf.il	NULL Character in Method	Block	1
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/templates/homepage/piwik.php	Block	1
80.246.139.9	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.53.179.222	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giy	Block	1
77.138.155.132	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
204.79.180.180	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	1
66.249.69.20	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 66.249.69.20	Block	1
46.19.86.151	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method pt-Language: in URL he-il,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/general.aspx	Block	1
66.249.76.108	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/sites/skira/default.asp	None	1

10-03-2016-20:04:06 to 10-03-2016-21:04:06