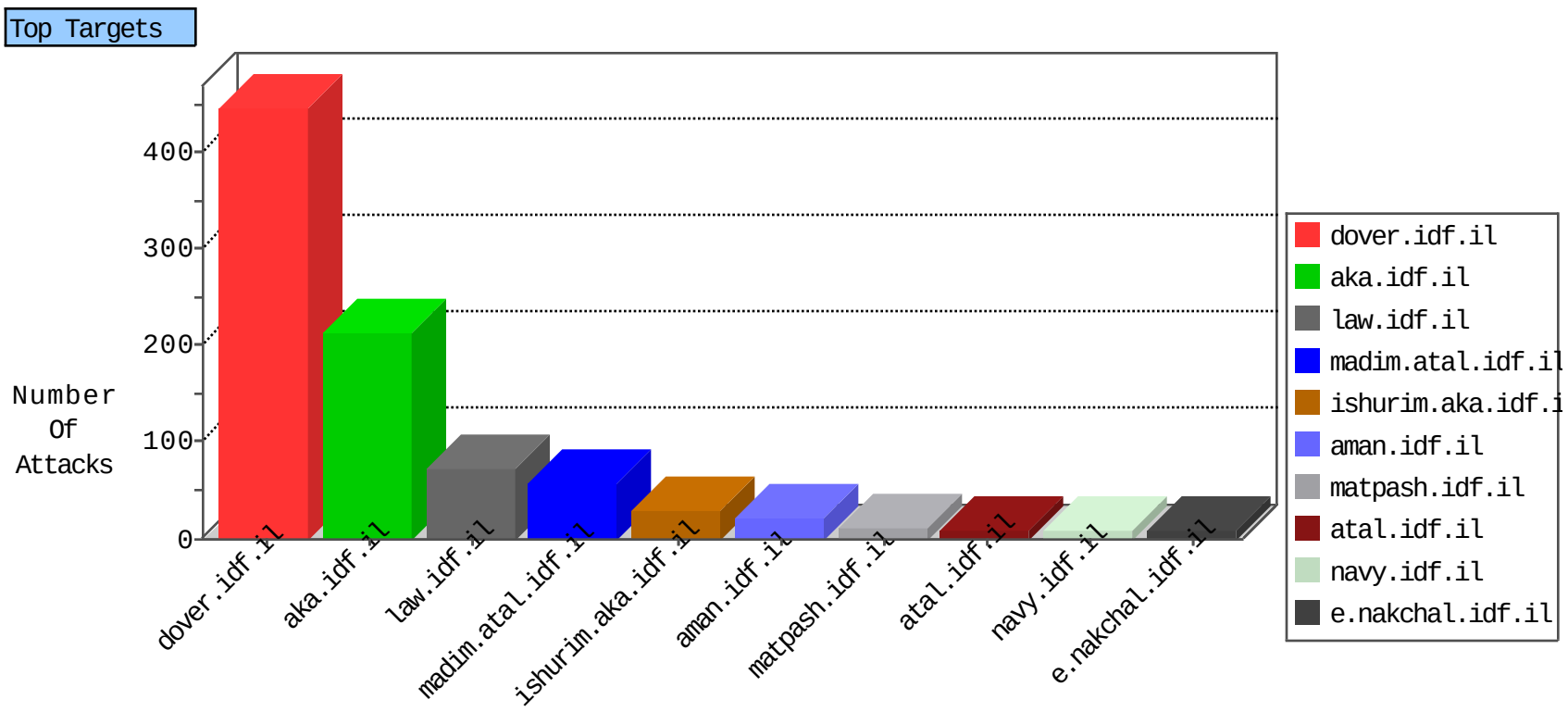
04-23-2016-19:04:09 to 04-23-2016-20:04:09

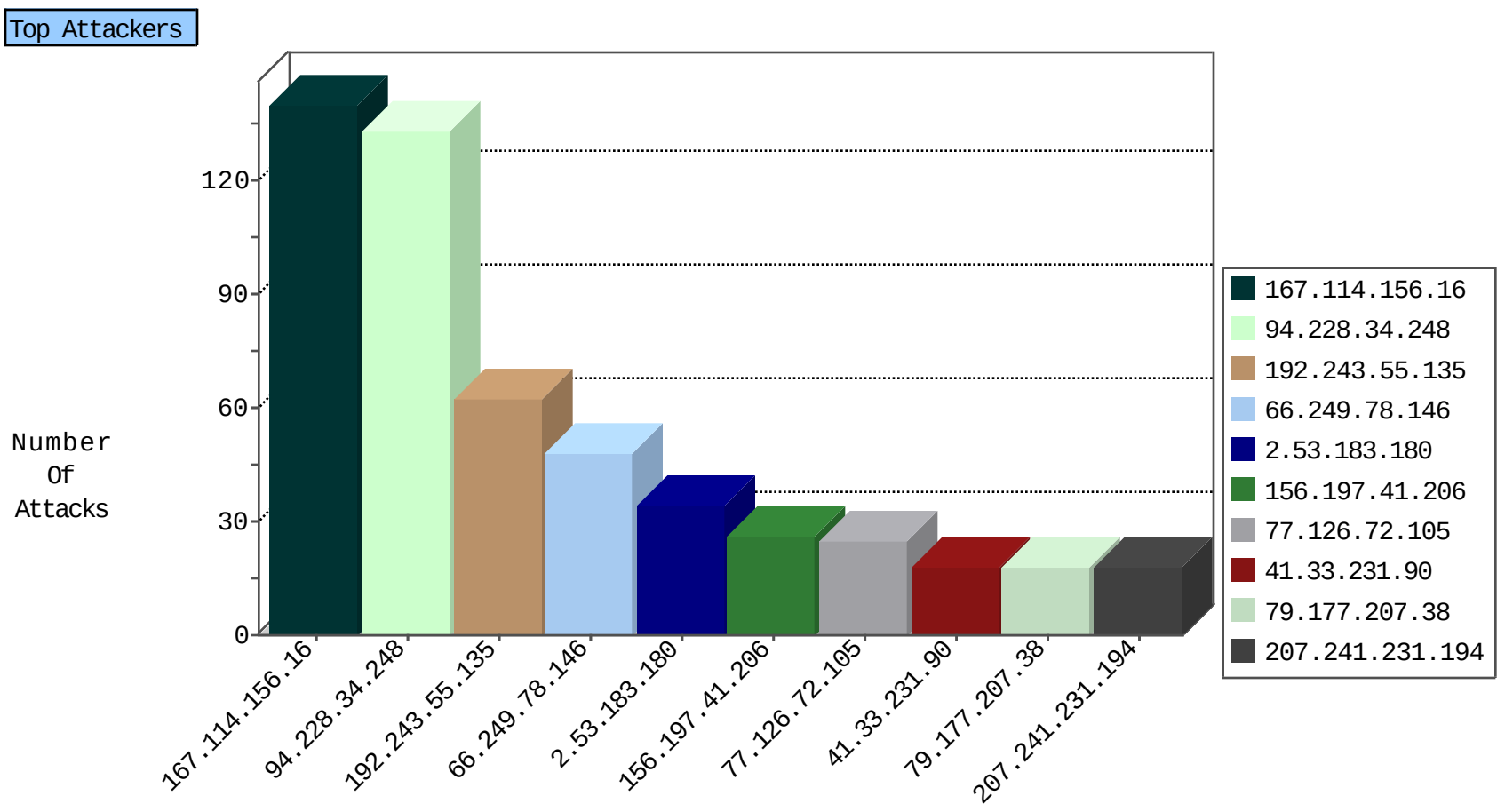
IDF Under Attack
Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

04-23-2016-19:04:09 to 04-23-2016-20:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	10321
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1195
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	282
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	4
134.147.203.115	Germany	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
134.147.203.115	Germany	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	2
89.46.100.170	Romania	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
69.30.198.150	United States	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1
185.130.5.99	Lithuania	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
104.238.135.152	United States	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	1
74.91.17.179	United States	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	1
69.30.198.146	United States	147.237.72.156	aman.idf.il	block-sp-traf1	drop	1
74.91.23.110	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	drop	1
69.30.198.150	United States	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	forward	1

04-23-2016-19:04:09 to 04-23-2016-20:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
69.30.223.170	United States	147.237.77.74	law.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1

04-23-2016-19:04:09 to 04-23-2016-20:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.78.199	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
104.171.122.176	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
104.171.122.176	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -f -sS	1
91.201.236.158	147.237.0.17	Ukraine	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
82.117.208.243	147.237.0.200		m4u.idf.il	ET SCAN NMAP -sS window 1024	1
61.182.170.38	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
61.182.170.38	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
196.203.149.99	147.237.76.198	Tunisia	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
174.37.194.144	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 4096	1
158.255.5.147	147.237.76.147	Russian Federation	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
104.171.122.176	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 2048	1
91.201.236.158	147.237.0.17	Ukraine	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
91.201.236.158	147.237.0.17	Ukraine	m.my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
61.182.170.38	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
196.203.149.99	147.237.76.198	Tunisia	e.yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
2.55.29.67	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
174.37.194.144	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 3072	1

04-23-2016-19:04:09 to 04-23-2016-20:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
94.228.34.248	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	132
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
156.197.41.206	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
77.126.72.105	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	25
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	22
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	18
207.241.231.194	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	18
37.26.148.155	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
192.243.55.135	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
77.126.82.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
79.177.207.38	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
79.177.207.38	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.135	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
109.64.86.82	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
84.108.28.243	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
46.19.85.116	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
84.108.28.243	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.116	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
77.126.92.31	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
40.77.167.15	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
84.108.28.243	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	4
76.111.6.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
92.222.23.240	France	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
197.27.74.35	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
197.27.74.35	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.55.154.86	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.109.234	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.86.82	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
93.119.76.186	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
66.249.93.182	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.179.37	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.13.63	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.71.53.91	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.204.34	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.249	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.215.145	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.160.112	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
157.55.39.37	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
37.27.187.73	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
66.249.64.80	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.55.7.177	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.159.147.242	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-23-2016-19:04:09 to 04-23-2016-20:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.183.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	34
37.46.38.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
195.200.205.72	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	8
195.200.205.72	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/9/	Block	5
2.53.50.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.119.127.129	Ukraine	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 46.119.127.129	Block	3
176.13.13.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.46.200	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
103.231.241.40	Philippines	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/wp-login.php	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1395-en/dover.aspx	Block	1
40.77.167.40	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
130.185.155.74	Sweden	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
83.34.235.1	Spain	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 83.34.235.1 (Open Mode)	None	1
66.249.78.147	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/chinuch/news/default.asp	Block	1
199.115.117.88	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/recordings/theme/iefixes.css	Block	1
107.150.32.61	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.yun.ph/	Block	1
69.30.198.150	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.gege1.com/	Block	1
46.19.86.71	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/smalim/html/2	Block	1
157.55.39.225	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
83.34.235.1	Spain	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
199.115.117.88	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/recordings/theme/iefixes.css	Block	1
109.64.86.82	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
74.91.20.195	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.yun.ph/	Block	1
83.247.85.194	Netherlands	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/	Block	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1927-he/cogat.aspx	Block	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/history/yoav.stm/	Block	1
128.238.182.61	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;catid in www.aka.idf.il/rights/asp/info.asp	None	1
74.91.20.197	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.yun.ph/	Block	1
46.119.127.129	Ukraine	147.237.77.74	law.idf.il	PHP Attempt	Block	1
103.231.241.40	Philippines	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1361-he/dover.aspx	Block	1
210.224.185.233	Japan	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/forms.aspx	Block	1
40.77.167.28	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/arabic/pages/default.aspx	Block	1
130.185.155.74	Sweden	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
82.205.55.247	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
46.119.127.129	Ukraine	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1

04-23-2016-19:04:09 to 04-23-2016-20:04:09