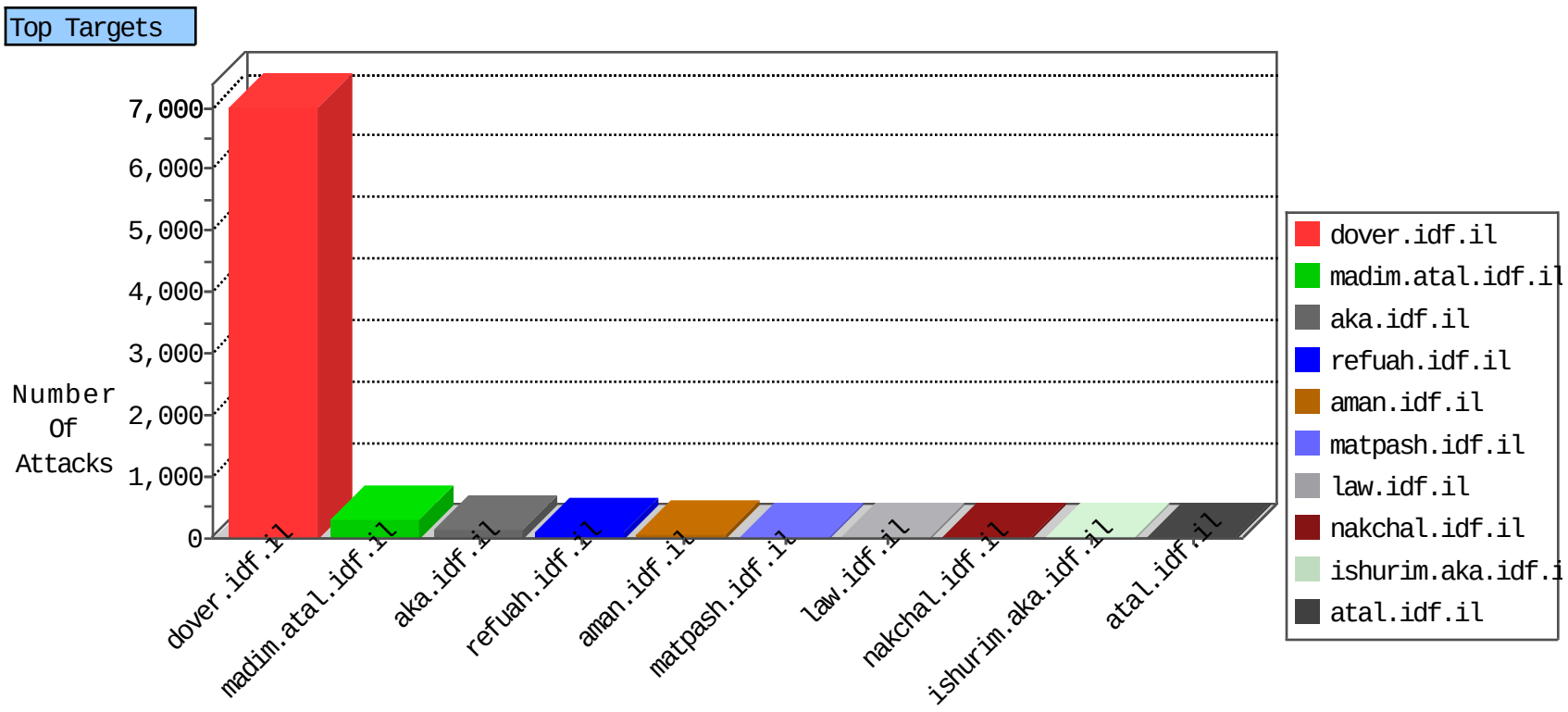
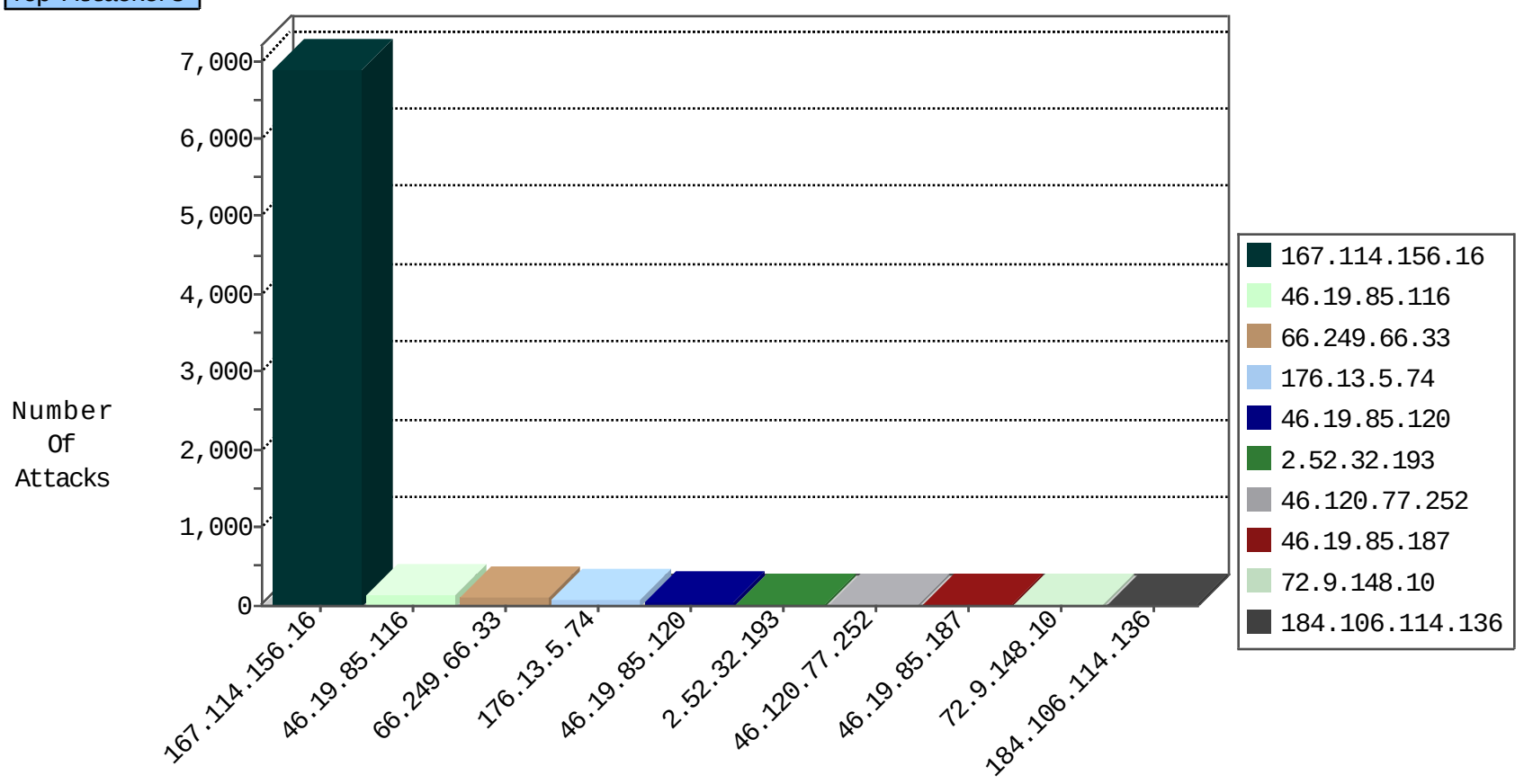
03-13-2016-07:04:00 to 03-13-2016-08:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-13-2016-07:04:00 to 03-13-2016-08:04:00

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	DOS-Tool-SwitchbladG	dest-reset	9072
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
196.45.48.28	Nigeria	147.237.76.86	navy.idf.il	Invalid L4 Header Length	drop	1

03-13-2016-07:04:00 to 03-13-2016-08:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.206.169	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
184.106.114.136	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	8
106.38.241.149	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
144.76.8.132	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
80.246.133.235	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
144.76.8.132	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
188.165.15.108	France	147.237.72.156	aman.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

03-13-2016-07:04:00 to 03-13-2016-08:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.66.33	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	101
184.106.114.136	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	10
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
165.255.73.89	147.237.0.16		my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
119.139.65.64	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
119.139.65.64	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
199.101.186.245	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 3072	1
119.139.65.64	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
193.105.134.220	147.237.8.24	Sweden	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
119.139.65.64	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
185.106.92.65	147.237.72.167		ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
106.38.241.149	147.237.77.216	China	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.93.103	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
165.255.73.89	147.237.8.45		e.eitan.idf.il	ET SCAN Potential SSH Scan	1
165.255.73.89	147.237.0.35		akaws.idf.il	ET SCAN Potential SSH Scan	1
119.139.65.64	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	1
119.139.65.64	147.237.77.176	China	matpash.idf.il	ET SCAN Potential SSH Scan	1
212.129.8.145	147.237.8.27	France	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
119.139.65.64	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
119.139.65.64	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
187.188.111.60	147.237.76.147	Mexico	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
109.253.203.186	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.106.92.65	147.237.8.27		e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
104.238.98.124	147.237.72.166		aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
165.255.73.89	147.237.8.24		e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1

03-13-2016-07:04:00 to 03-13-2016-08:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3004
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	149
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack		reject	44
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
46.19.85.24	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
5.102.254.144	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
62.219.155.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.24.93	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
5.22.130.237	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.120	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.120	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.22.130.237	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.120	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
2.52.177.88	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.120	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
212.34.20.5	Jordan	147.237.77.176	matpash.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.120	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.187	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.120	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.13.3.9	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
178.63.105.85	Germany	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	5
46.19.85.187	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
94.230.86.141	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.187	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.46.41.183	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
85.64.86.162	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
199.30.24.55	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
176.13.3.9	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
37.26.147.175	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.63.105.85	Germany	147.237.77.61	e.cogat.idf.il	drop	SAM rule	drop	3
82.80.97.80	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.122	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
121.54.54.49	Philippines	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
176.13.3.101	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.80.179.250	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.170.171	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.187	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
79.182.107.66	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
121.54.54.49	Philippines	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.85.71	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.2.131	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	3
176.13.15.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.139.138	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.148.14	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.111.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.98.181	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3

03-13-2016-07:04:00 to 03-13-2016-08:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.116	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	137
176.13.5.74	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	84
2.52.32.193	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	26
46.120.77.252	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	24
46.19.86.73	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
2.54.169.112	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
46.19.85.25	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
104.238.98.124		147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	3
199.30.24.7	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
65.55.210.206	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
80.246.139.216	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.54.1.187	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
46.19.85.71	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
157.55.39.193	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
70.195.198.244	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
46.19.85.187	Israel	147.237.76.31	nakchal.idf.il	Distributed Malformed URL	Block	1
212.34.20.5	Jordan	147.237.77.176	matpash.idf.il	Abnormally Long Request method	Block	1
174.129.237.157	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.66.172	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
212.34.20.5	Jordan	147.237.77.176	matpash.idf.il	Multiple Abnormally Long Request from 212.34.20.5	Block	1
207.46.13.134	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 207.46.13.134	Block	1
46.19.85.187	Israel	147.237.76.31	nakchal.idf.il	Distributed Unknown HTTP Request Method	Block	1
212.34.20.5	Jordan	147.237.77.176	matpash.idf.il	Illegal Byte Code Character in Header Name torage/FILES/3/size220X0/4303.jpg HTTP/1.1	Block	1
66.249.69.2	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
212.34.20.5	Jordan	147.237.77.176	matpash.idf.il	Multiple Illegal HTTP Version from 212.34.20.5	Block	1
207.46.13.134	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
212.34.20.5	Jordan	147.237.77.176	matpash.idf.il	Illegal HTTP Version	Block	1
198.20.69.74	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.69.30	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1878	Block	1
212.34.20.5	Jordan	147.237.77.176	matpash.idf.il	Redundant HTTP Headers Referer	Block	1
46.19.85.100	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
207.241.237.166	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
157.55.39.189	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
212.34.20.5	Jordan	147.237.77.176	matpash.idf.il	Malformed HTTP Header Line 2	Block	1
5.102.254.144	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
68.180.228.151	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1398-en/dover.aspx	Block	1
212.34.20.5	Jordan	147.237.77.176	matpash.idf.il	Unknown HTTP Request Method pts/Scroller/jquery.jcarousel.js in URL www.cogat.idf.ilhttp/1.1	Block	1
207.241.237.166	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
212.34.20.5	Jordan	147.237.77.176	matpash.idf.il	Malformed URL http/1.1	Block	1
37.26.146.200	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
199.30.25.90	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1

03-13-2016-07:04:00 to 03-13-2016-08:04:00