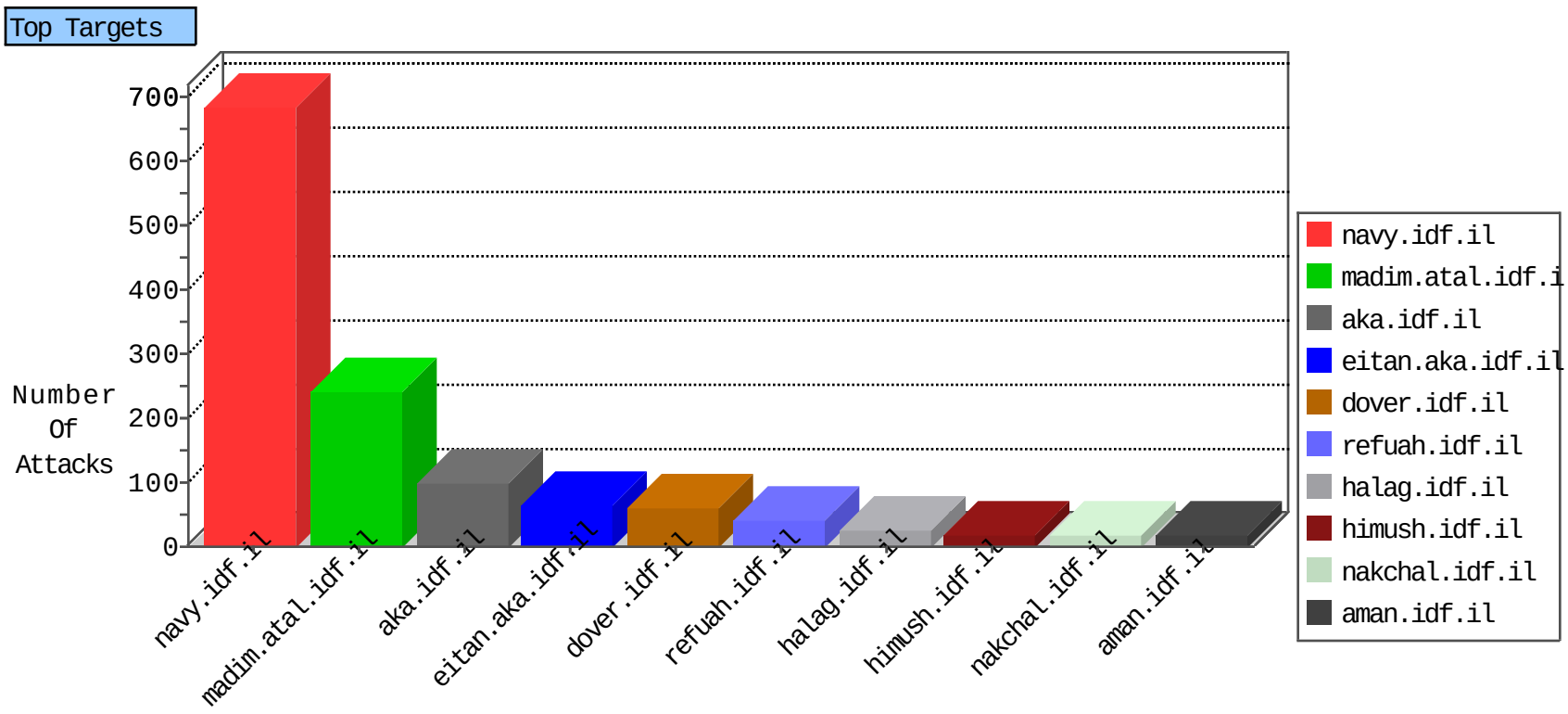
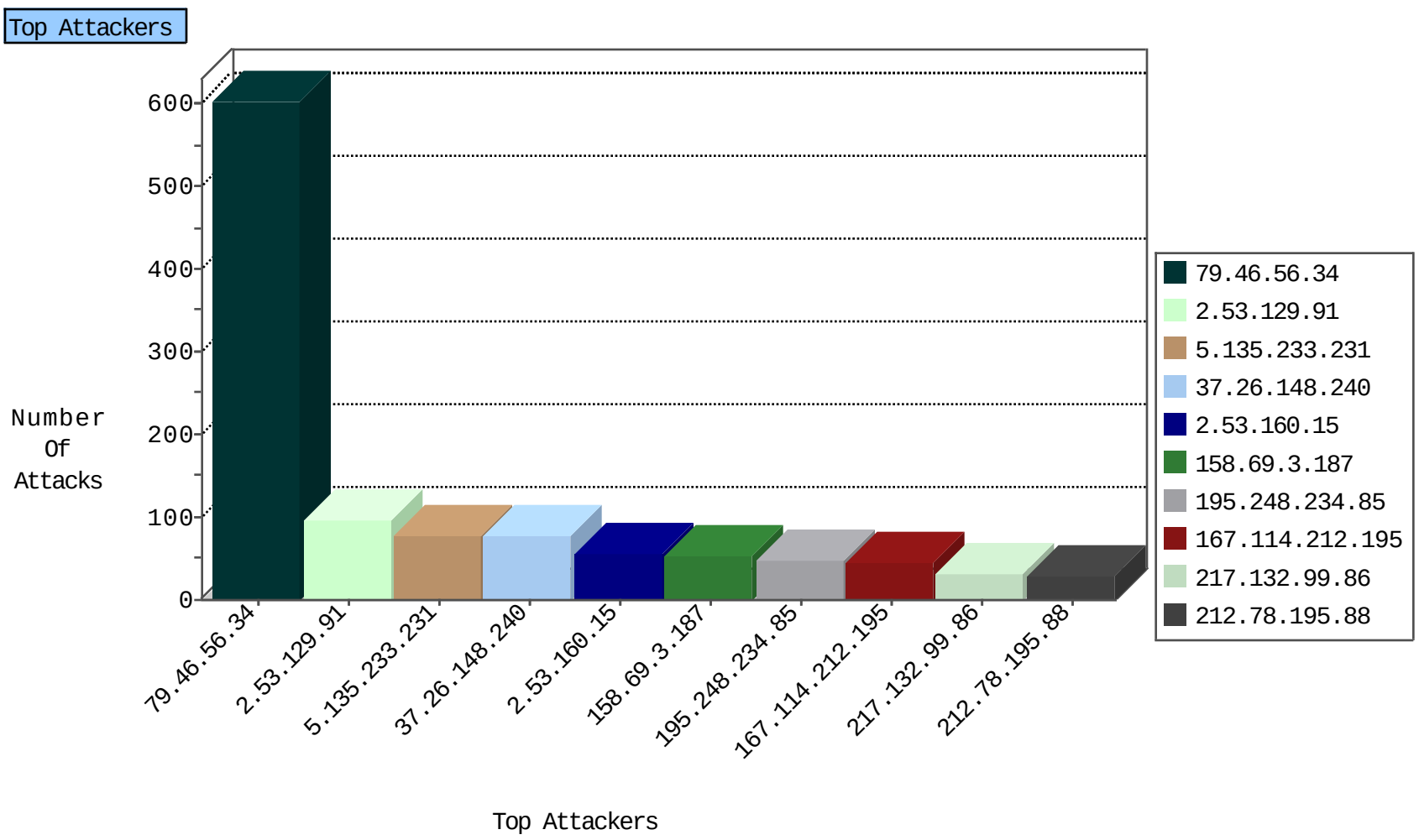
09-05-2016-00:04:06 to 09-05-2016-01:04:06

IDF Under Attack
Daily Report

Top Targets



Top Attackers



09-05-2016-00:04:06 to 09-05-2016-01:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.133.207	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
109.236.84.10	Netherlands	147.237.76.201	e.atal.idf.i	Black List	drop	1
179.99.200.39	Brazil	147.237.72.166	aka.idf.il	block-sp-traf1	forward	1

09-05-2016-00:04:06 to 09-05-2016-01:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
64.34.186.9	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
198.20.69.74	United States	147.237.72.156	aman.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

09-05-2016-00:04:06 to 09-05-2016-01:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
64.34.186.9	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	8
45.79.71.122	147.237.77.74	United States	law.idf.il	WEB-MISC Chunked-Encoding transfer attempt	2
79.180.82.190	147.237.0.34	Israel	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
61.178.42.242	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
221.204.249.157	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
50.116.123.135	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.225.138	147.237.0.15	Ukraine	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
94.156.128.25	147.237.76.196	Bulgaria	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
94.102.52.71	147.237.77.179	Netherlands	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.76.30	Netherlands	himush.idf.il	ET SCAN Potential SSH Scan	1
61.178.42.242	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
61.178.42.242	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
50.116.123.135	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.225.138	147.237.0.17	Ukraine	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
46.227.67.172	147.237.76.200	Sweden	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
104.167.6.84	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
5.255.90.133	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
94.156.128.25	147.237.72.14	Bulgaria	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.76.30	Netherlands	himush.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
61.178.42.242	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1

09-05-2016-00:04:06 to 09-05-2016-01:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
79.46.56.34	Italy	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	598
195.248.234.85	Ukraine	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	47
217.132.99.86	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	32
212.78.195.88	Netherlands	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	28
5.22.134.166	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
87.71.7.52	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
5.135.233.231	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
5.135.233.231	France	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
5.135.233.231	France	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
5.135.233.231	France	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
5.135.233.231	France	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
5.135.233.231	France	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
5.135.233.231	France	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
5.135.233.231	France	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
37.26.148.240	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
66.249.76.106	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.148.240	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
185.32.179.249	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.8.204.38	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
5.40.138.109	Spain	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
158.69.3.187	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
188.172.244.59	Austria	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
188.172.244.59	Austria	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
188.172.244.59	Austria	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
87.71.6.11	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	3
213.57.70.7	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.86.173	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.8	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
46.19.86.8	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
167.114.212.195	Canada	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.86.173	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
188.172.244.59	Austria	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
167.114.212.195	Canada	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
158.69.3.187	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
167.114.212.195	Canada	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.86.8	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
141.226.217.158	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
158.69.3.187	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.173	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
24.127.38.78	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
167.114.212.195	Canada	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
188.172.244.59	Austria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.86.173	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
167.114.212.195	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
167.114.212.195	Canada	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
156.204.13.8	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
167.114.212.195	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
167.114.212.195	Canada	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
188.172.244.59	Austria	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2

09-05-2016-00:04:06 to 09-05-2016-01:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.129.91	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	96
37.26.148.240	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	57
2.53.160.15	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	56
176.13.23.58	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
81.0.251.10	Czech Republic	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	4
185.32.179.249	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
66.249.83.219	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.83.220	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
87.71.7.135	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
45.79.71.122	United States	147.237.77.74	law.idf.il	Unknown HTTP Request Method 1 in URL	Block	1
77.125.7.174	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
46.19.86.173	Israel	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method c4aba000 in URL	Block	1
45.79.71.122	United States	147.237.77.74	law.idf.il	Malformed URL	Block	1
109.64.118.132	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.85.36	Israel	147.237.76.42	refuah.idf.il	Distributed Malformed URL	Block	1
178.137.4.87	Ukraine	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
2.53.169.29	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/nav.css	Block	1
77.138.240.236	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
45.79.71.122	United States	147.237.77.74	law.idf.il	Multiple Malformed HTTP Header Line from 45.79.71.122	Block	1
109.67.161.123	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	1
46.19.85.36	Israel	147.237.76.42	refuah.idf.il	Distributed Unknown HTTP Request Method	Block	1
5.22.134.166	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
79.180.241.149	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
45.79.71.122	United States	147.237.77.74	law.idf.il	Multiple Malformed URL from 45.79.71.122	Block	1
109.253.193.213	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.85.36	Israel	147.237.76.42	refuah.idf.il	Illegal HTTP Version	Block	1
207.46.13.76	United States	147.237.72.166	aka.idf.il	Unknown Parameter 136cd360 in www.aka.idf.il/main/home/default.aspx	None	1
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Unknown Parameter list in www.aka.idf.il/megurim/news/	None	1
45.79.71.122	United States	147.237.77.74	law.idf.il	Multiple Unknown HTTP Request Method from 45.79.71.122	Block	1
157.55.39.246	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
66.249.83.221	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.86.173	Israel	147.237.76.42	refuah.idf.il	Malformed URL	Block	1
45.79.71.122	United States	147.237.77.74	law.idf.il	Malformed HTTP Header Line 4	Block	1
66.249.76.117	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1362-14724-he/dover.aspx	Block	1

09-05-2016-00:04:06 to 09-05-2016-01:04:06