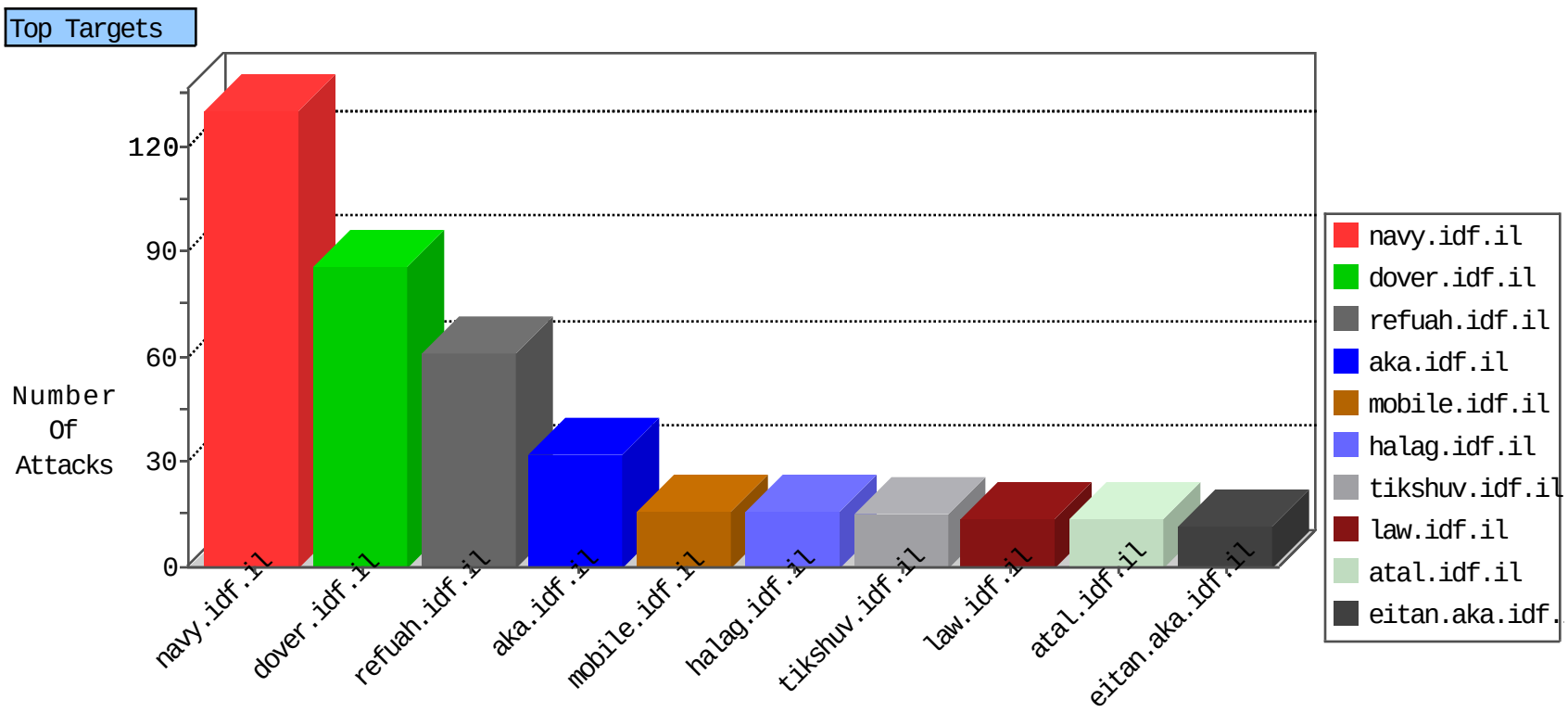
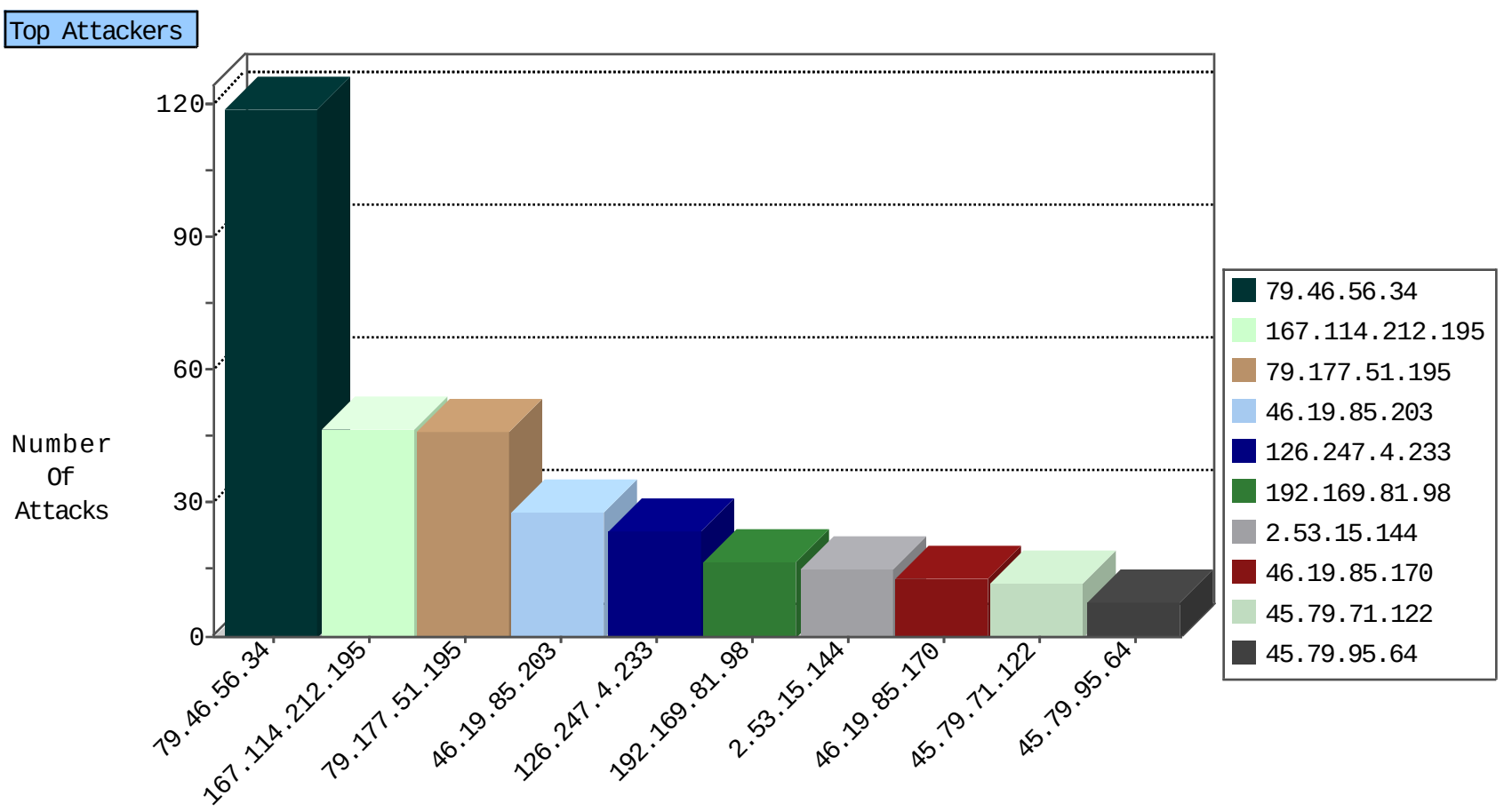
09-05-2016-01:08:04 to 09-05-2016-02:08:04

IDF Under Attack Daily Report





09-05-2016-01:08:04 to 09-05-2016-02:08:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
141.212.122.103	United States	147.237.76.38	e.e.meitav.idf.il	Black List	drop	1
185.25.33.139	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
185.25.33.140	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

09-05-2016-01:08:04 to 09-05-2016-02:08:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-05-2016-01:08:04 to 09-05-2016-02:08:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
91.121.222.79	147.237.77.74	France	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	6
45.79.95.64	147.237.77.216	United States	dover.idf.il	WEB-MISC Chunked-Encoding transfer attempt	2
91.121.221.160	147.237.77.74	France	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
45.79.71.122	147.237.72.167	United States	ishurim.aka.idf.il	WEB-MISC Chunked-Encoding transfer attempt	2
91.201.236.155	147.237.8.24	Ukraine	e.lifestyle.idf.il	ET SCAN NMAP -sS window 3072	1
142.54.191.210	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 4096	1
45.79.71.122	147.237.72.166	United States	aka.idf.il	WEB-MISC Chunked-Encoding transfer attempt	1
94.156.128.25	147.237.77.233	Bulgaria	atal.idf.il	ET SCAN Potential SSH Scan	1
94.156.128.25	147.237.76.202	Bulgaria	e.halag.idf.il	ET SCAN Potential SSH Scan	1
94.156.128.25	147.237.76.30	Bulgaria	himush.idf.il	ET SCAN Potential SSH Scan	1
94.102.56.233	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.8.27	Netherlands	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.8.24	Ukraine	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
162.243.85.34	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
142.54.191.210	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
94.156.128.25	147.237.77.121	Bulgaria	e.navy.idf.il	ET SCAN Potential SSH Scan	1
94.156.128.25	147.237.76.147	Bulgaria	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
94.156.128.25	147.237.8.27	Bulgaria	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
94.102.56.233	147.237.76.197	Netherlands	e.himush.idf.il	ET SCAN Potential SSH Scan	1

09-05-2016-01:08:04 to 09-05-2016-02:08:04

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	119
79.177.51.195	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	38
126.247.4.233	Japan	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
2.53.15.144	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.85.203	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
46.19.85.203	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
87.68.16.197	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.203	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.203	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
141.226.217.96	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.177.51.195	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
46.19.85.170	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
167.114.212.195	Canada	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
167.114.212.195	Canada	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
167.114.212.195	Canada	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
62.16.65.157	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.170	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
167.114.212.195	Canada	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
141.226.217.96	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
167.114.212.195	Canada	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
46.19.86.57	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
167.114.212.195	Canada	147.237.77.216	dover.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	alert	2
176.24.9.113	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.85.22	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
109.65.55.126	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
46.147.208.177	Russian Federation	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.22	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.188.58.116	Russian Federation	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.170	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
5.164.79.92	Russian Federation	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	2
167.114.212.195	Canada	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
188.32.20.207	Russian Federation	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.170	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
167.114.212.195	Canada	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
77.139.68.213	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
192.169.81.98	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
46.19.86.133	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
167.114.212.195	Canada	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
188.44.55.20	Russian Federation	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	1
125.77.28.26	China	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
167.114.212.195	Canada	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
167.114.212.195	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
192.169.81.98	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
46.121.153.250	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
167.114.212.195	Canada	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
192.169.81.98	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
141.212.122.86	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
167.114.212.195	Canada	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1

09-05-2016-01:08:04 to 09-05-2016-02:08:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.76.83	Block	3
84.229.78.129	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/	Block	2
45.79.71.122	United States	147.237.72.167	ishurim.aka.idf.i	Multiple Malformed HTTP Header Line from 45.79.71.122	Block	2
105.131.211.108	Morocco	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 105.131.211.108	Block	2
45.79.71.122	United States	147.237.72.167	ishurim.aka.idf.i	Multiple Malformed URL from 45.79.71.122	Block	2
45.79.71.122	United States	147.237.72.167	ishurim.aka.idf.i	Multiple Unknown HTTP Request Method from 45.79.71.122	Block	2
66.249.76.70	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1
192.169.7.223	United States	147.237.72.156	aman.idf.il	Unauthorized Method HEAD for 147.237.72.156/	Block	1
45.79.95.64	United States	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 45.79.95.64	Block	1
45.79.71.122	United States	147.237.72.166	aka.idf.il	Malformed URL	Block	1
105.131.211.108	Morocco	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
76.121.232.137	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
46.19.86.63	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
157.55.39.115	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
45.79.95.64	United States	147.237.77.216	dover.idf.il	Malformed HTTP Header Line 2	Block	1
84.229.78.129	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 84.229.78.129	Block	1
5.228.99.191	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/iturim/asp/	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/7/70607.pdf	Block	1
45.79.95.64	United States	147.237.77.216	dover.idf.il	Unknown HTTP Request Method 1 in URL	Block	1
45.79.71.122	United States	147.237.72.166	aka.idf.il	Unknown HTTP Request Method 1 in URL	Block	1
105.131.211.108	Morocco	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 105.131.211.108	Block	1
77.138.237.170	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
46.188.32.37	Russian Federation	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/rabanut/general.aspx	Block	1
176.193.23.38	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/contactus.aspx	Block	1
45.79.95.64	United States	147.237.77.216	dover.idf.il	Malformed URL	Block	1
31.173.85.233	Russian Federation	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
46.19.85.22	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
79.177.51.195	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
66.249.64.230	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/9/108889.pdf	Block	1
176.193.98.211	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/haredim/general.aspx	Block	1
45.79.95.64	United States	147.237.77.216	dover.idf.il	Multiple Malformed HTTP Header Line from 45.79.95.64	Block	1
37.112.227.244	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/66846.ppt	Block	1
93.80.63.183	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
46.19.85.170	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
105.131.211.108	Morocco	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ardmin	Block	1
79.177.51.195	Israel	147.237.77.233	atal.idf.il	Suspicious Response Code	Block	1
66.249.66.162	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/.well-known/apple-app-site-association	Block	1
176.193.248.84	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/edim/library/generaldoc.asp	Block	1
45.79.95.64	United States	147.237.77.216	dover.idf.il	Multiple Malformed URL from 45.79.95.64	Block	1
45.79.71.122	United States	147.237.72.166	aka.idf.il	Malformed HTTP Header Line 2	Block	1
95.28.56.93	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/iturim/asp/displayonesoldier.asp	Block	1
68.180.228.231	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-ar/cogat.aspx	Block	1
46.19.85.187	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
109.65.172.104	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
79.177.51.195	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1

09-05-2016-01:08:04 to 09-05-2016-02:08:04