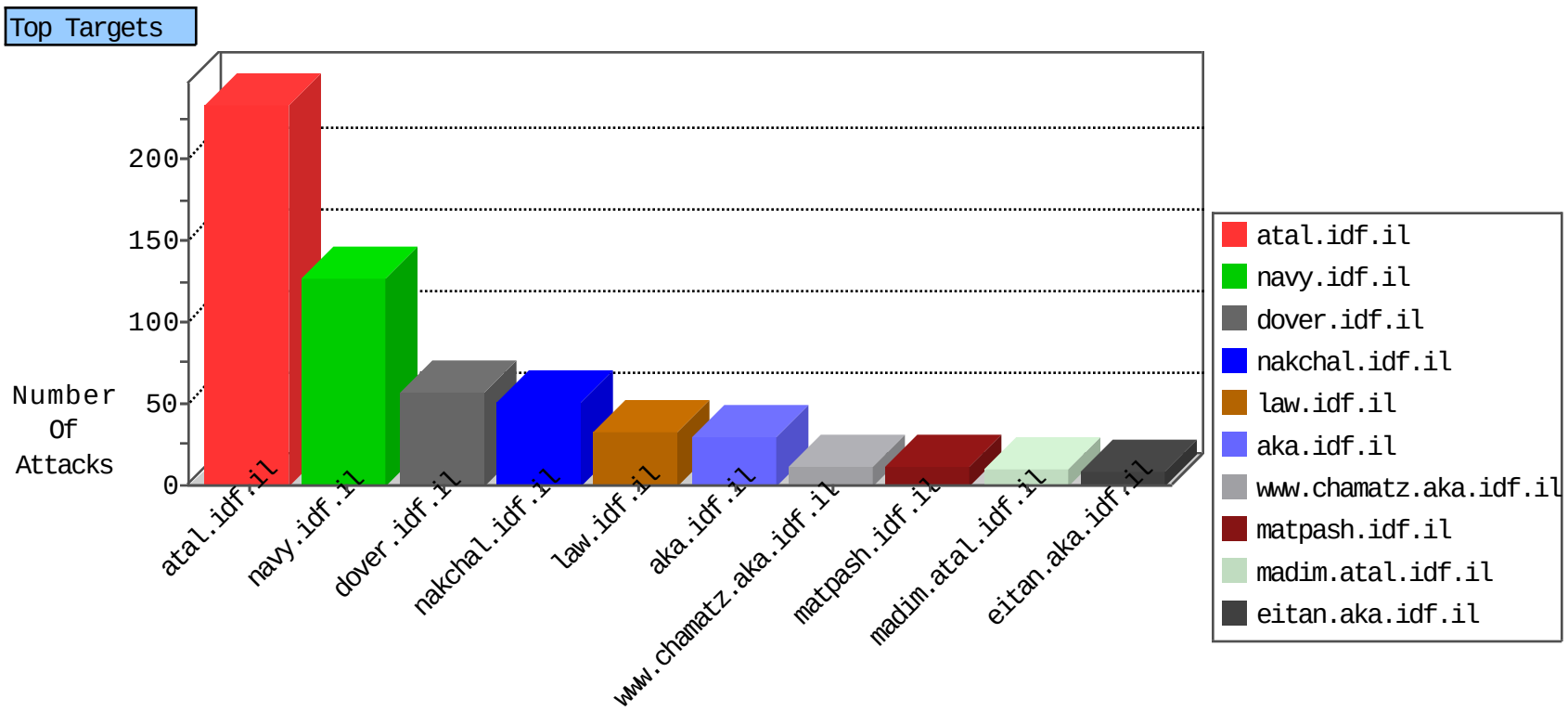
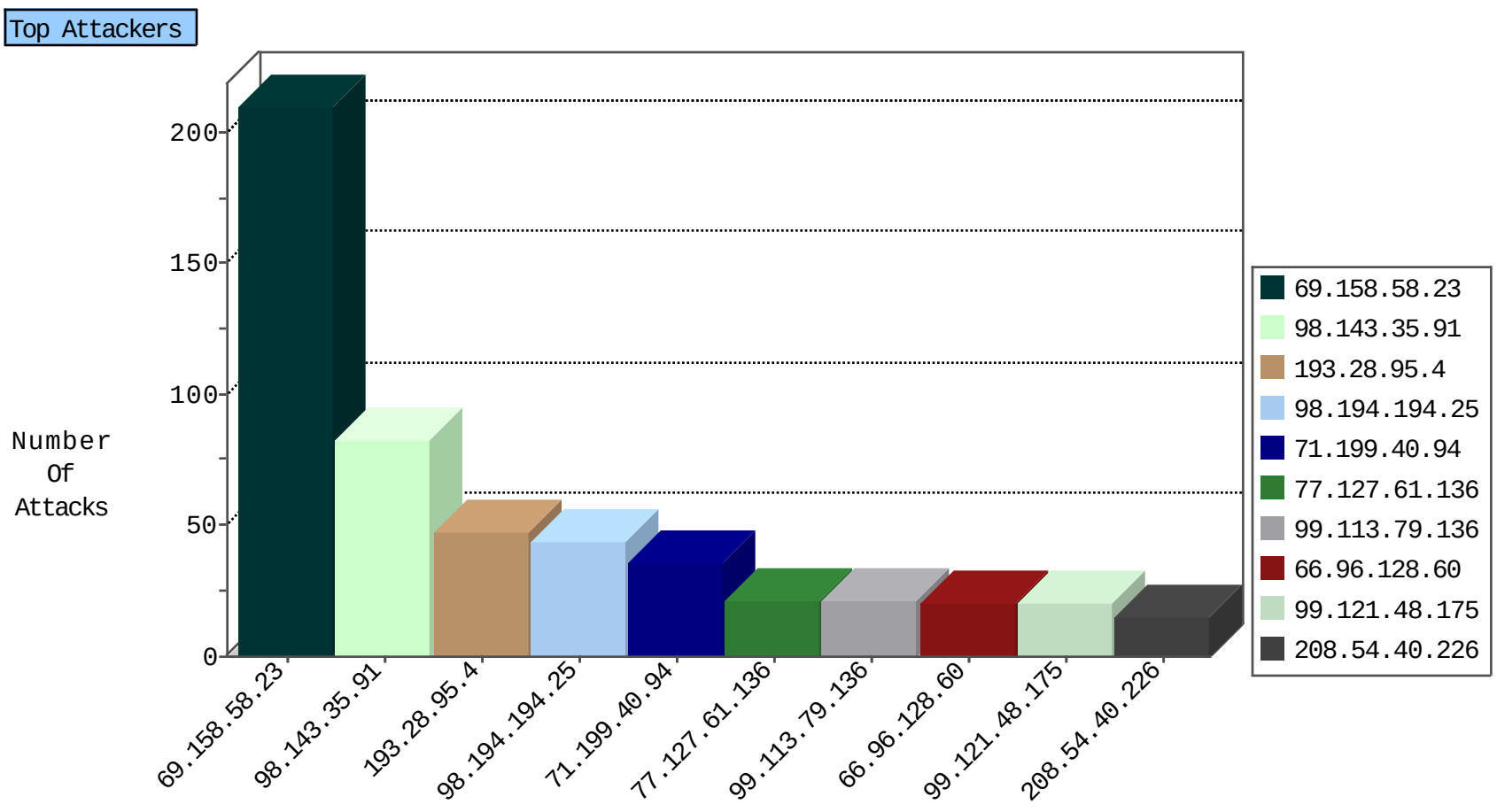
09-05-2016-05:04:03 to 09-05-2016-06:04:03

IDF Under Attack
Daily Report





09-05-2016-05:04:03 to 09-05-2016-06:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
27.254.150.65	Thailand	147.237.76.201	e.atal.idf.il	JLM_Purple_Con_Limit_Tcp	drop	3
216.26.141.6	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
80.82.65.168	Netherlands	147.237.76.44	e.refuah.idf.il	Black List	drop	1
216.26.141.7	United States	147.237.77.74	law.idf.il	Invalid TCP Flags	drop	1
117.25.154.71	China	147.237.76.39	mobile.meitav.idf.il	JLM_Purple_Con_Limit_Http	drop	1
216.26.141.7	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
216.26.141.6	United States	147.237.77.74	law.idf.il	Invalid TCP Flags	drop	1

09-05-2016-05:04:03 to 09-05-2016-06:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
193.28.95.4	Italy	147.237.76.31	nakchal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
66.96.128.60	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
72.167.131.75	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
193.28.95.4	Italy	147.237.76.31	nakchal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
193.28.95.4	Italy	147.237.76.31	nakchal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
5.9.62.130	Germany	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-05-2016-05:04:03 to 09-05-2016-06:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
193.28.95.4	147.237.76.31	Italy	nakchal.idf.il	SQL Injection - Select From	23
72.167.131.75	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
66.96.128.60	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
84.93.84.77	147.237.77.176	United Kingdom	matpash.idf.il	Tehila - Perl LWP with fake user agent	2
45.79.95.64	147.237.77.216	United States	dover.idf.il	WEB-MISC Chunked-Encoding transfer attempt	2
5.135.165.89	147.237.77.74	France	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
91.201.236.158	147.237.77.205	Ukraine	prisha.idf.il	ET SCAN NMAP -f -sS	1
50.84.213.146	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.77.179	Ukraine	e.mazi.idf.il	ET SCAN NMAP -sS window 3072	1
5.255.90.133	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.77.179	Ukraine	e.mazi.idf.il	ET SCAN NMAP -f -sS	1
210.78.142.201	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.201.236.50	147.237.76.176	Ukraine	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
199.255.20.103	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
88.249.106.23	147.237.76.198	Turkey	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
162.243.85.34	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 1024	1
158.217.165.220	147.237.76.44	Japan	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
68.190.208.191	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
104.167.6.84	147.237.72.217	United States	e.idf.il	ET SCAN Potential SSH Scan	1
68.190.208.191	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
91.201.236.158	147.237.77.205	Ukraine	prisha.idf.il	ET SCAN NMAP -sS window 2048	1
50.84.213.146	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
91.201.236.158	147.237.77.205	Ukraine	prisha.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
91.201.236.155	147.237.77.179	Ukraine	e.mazi.idf.il	ET SCAN NMAP -sS window 2048	1
91.201.236.50	147.237.76.176	Ukraine	test.ncore.idf.il	ET SCAN NMAP -sS window 4096	1
199.255.20.103	147.237.0.33	United States	idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
91.201.236.50	147.237.76.176	Ukraine	test.ncore.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
87.236.194.161	147.237.72.167	Czech Republic	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
158.217.165.220	147.237.76.200	Japan	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
123.108.191.233	147.237.0.33	Korea, Republic of	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
68.190.208.191	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
104.167.6.84	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sS window 1024	1

09-05-2016-05:04:03 to 09-05-2016-06:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
69.158.58.23	Canada	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	204
77.127.61.136	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	12
98.194.194.25	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	9
98.194.194.25	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
77.127.61.136	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
98.194.194.25	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	9
98.194.194.25	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
71.199.40.94	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	8
71.199.40.94	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
98.194.194.25	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	8
71.199.40.94	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	7
71.199.40.94	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
208.54.40.226	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
66.96.128.60	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
98.143.35.91	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
71.199.40.94	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
66.249.76.67	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
50.63.197.204	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
98.143.35.91	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
98.143.35.91	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
98.143.35.91	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.86.91	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
98.143.35.91	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
99.113.79.136	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
98.143.35.91	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
99.113.79.136	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	4
98.143.35.91	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
99.121.48.175	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	4
71.178.175.11	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
98.143.35.91	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
99.113.79.136	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	4
98.143.35.91	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.19.86.91	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
99.121.48.175	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	4
99.113.79.136	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
98.143.35.91	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
98.143.35.91	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
99.121.48.175	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
99.113.79.136	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
99.121.48.175	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
98.143.35.91	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
5.102.253.82	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
99.121.48.175	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
98.143.35.91	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
208.54.40.226	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
98.143.35.91	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
98.143.35.91	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
98.143.35.91	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
98.143.35.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3

09-05-2016-05:04:03 to 09-05-2016-06:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
45.79.95.64	United States	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	2
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	2
45.79.95.64	United States	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	2
157.55.39.111	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
66.249.69.119	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/library/generaldoc.asp	Block	1
46.19.86.91	Israel	147.237.77.216	dover.idf.il	Malformed URL _pk_id.20.8afc=ecefefbf415afc36.1446217044.2.1473041329.1473041329.;	Block	1
77.237.146.28	Czech Republic	147.237.77.74	law.idf.il	Unauthorized URL Access to /	Block	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
45.79.95.64	United States	147.237.77.216	dover.idf.il	Malformed HTTP Header Line 3	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/	Block	1
46.19.86.91	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method %22%22%2C%22%22%2C1473041329%2C%22https%3A%2F%2Fwww.google.co.il%2F%22%5D; in URL _pk_id.20.8afc=ecefefbf415afc36.1446217044.2.1473041329.1473041329.	Block	1
104.222.140.64	Singapore	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
66.249.69.83	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/showforum.asp	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
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;docId in www.aka.idf.il/brothers/faq/default.asp	None	1
66.249.64.30	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
104.222.140.64	Singapore	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/wp-login.php	Block	1
66.249.69.97	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
46.19.86.91	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request request version	Block	1
66.249.79.44	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
66.249.64.33	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/robots.txt	Block	1
148.251.2.180	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
66.249.69.101	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/2/302.pdf	Block	1
46.19.86.91	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version _pk_ses.20.8afc=*	Block	1
69.158.58.23	Canada	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/favicon.ico	Block	1

09-05-2016-05:04:03 to 09-05-2016-06:04:03