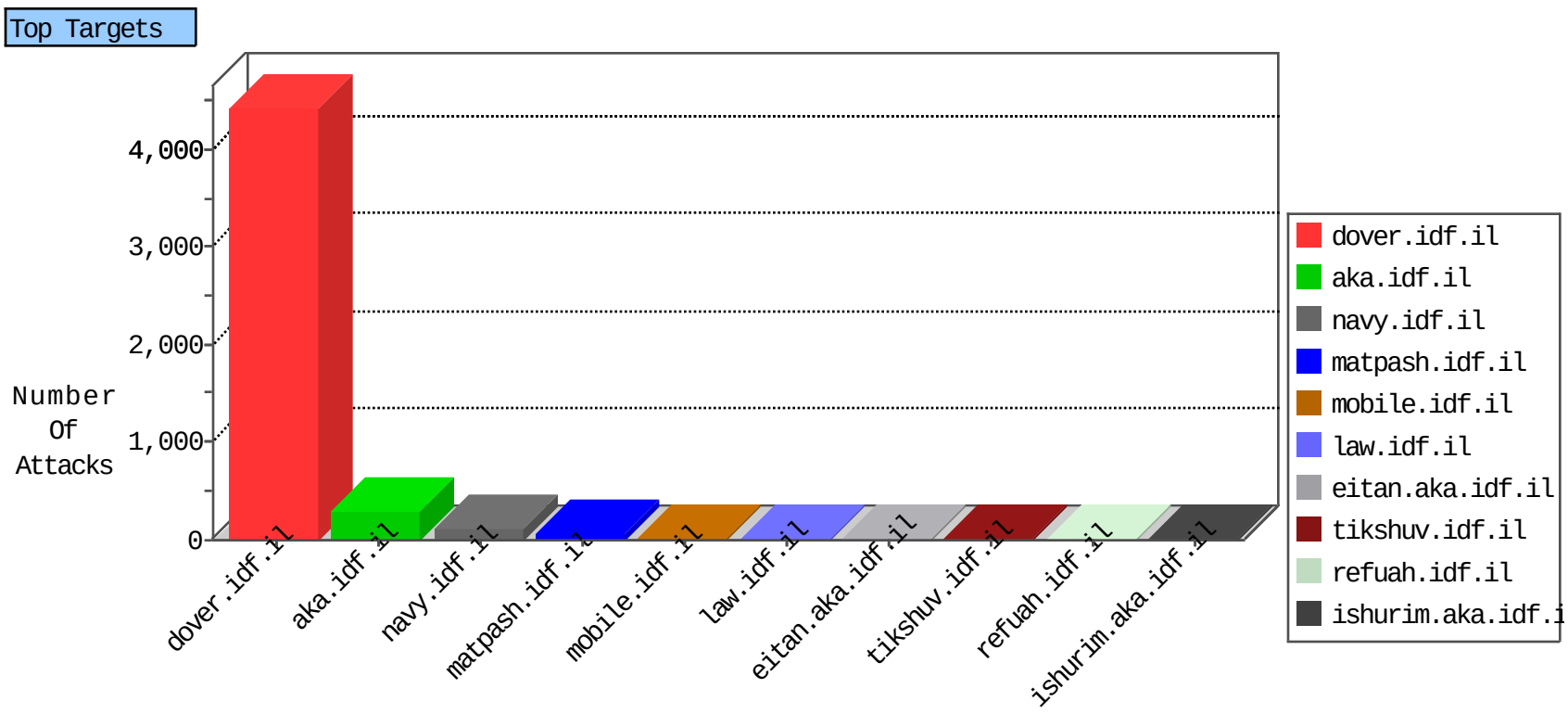
04-08-2016-23:04:00 to 04-09-2016-00:04:00

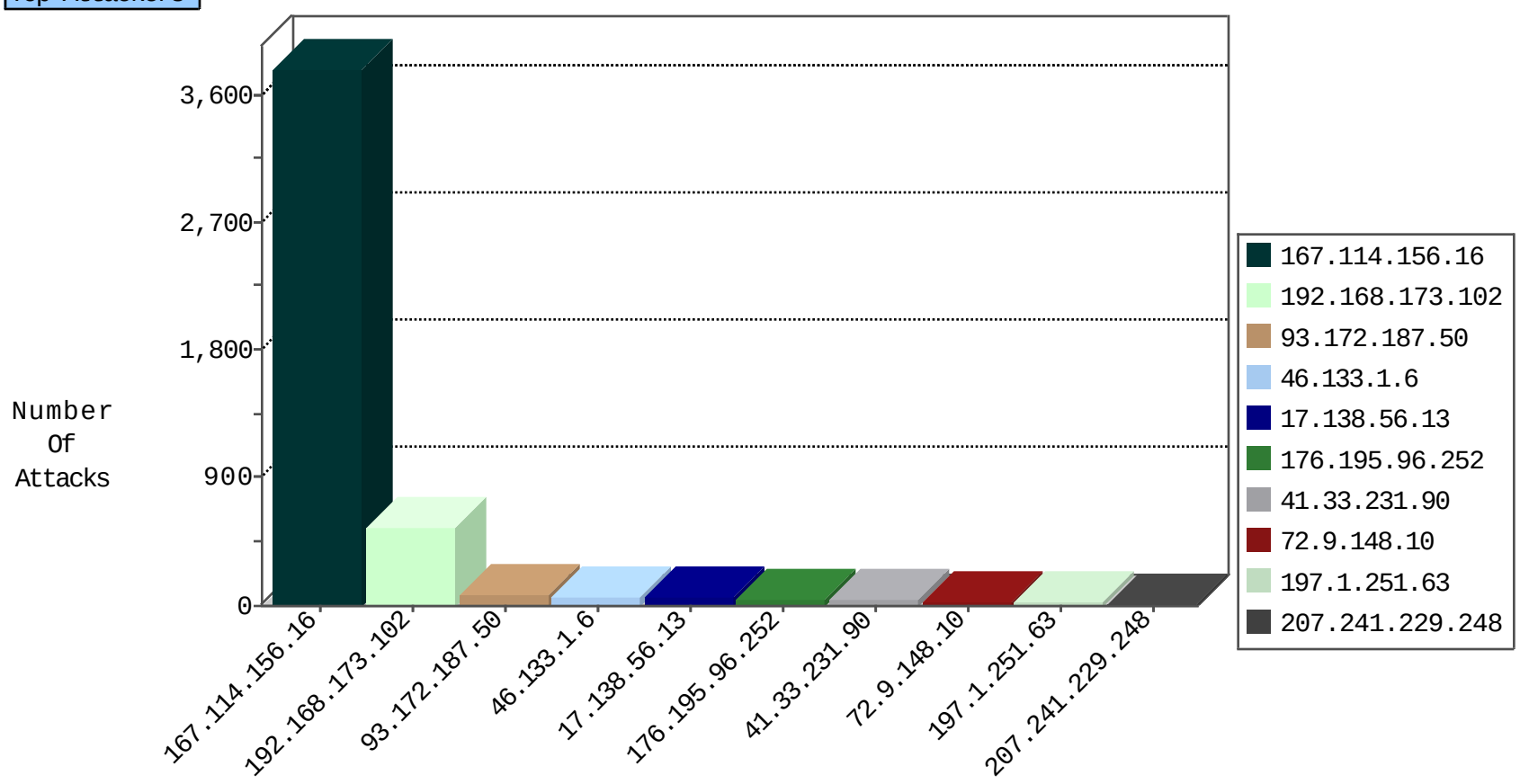
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

04-08-2016-23:04:00 to 04-09-2016-00:04:00

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	Block_Ip_Web_In	drop	3770
212.143.142.56	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	312
149.78.169.36	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	171
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
176.195.96.252	Russian Federation	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Http	drop	3
176.195.96.252	Russian Federation	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Http	drop	2
89.139.147.104	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
209.126.127.17	United States	147.237.8.27	e.madim.atal.idf.il	Block_Udp_All_Nets	drop	1
192.3.220.210	United States	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
151.82.188.168	Italy	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	1
209.126.127.17	United States	147.237.8.28	e.mobile-ks.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1	Russian Federation	147.237.8.28	e.mobile-ks.idf.il	Block_Ntp_All_Net	drop	1
192.206.214.254	United States	147.237.72.167	ishurim.aka.idf.il	TCP handshake violation, first packet not syn	drop	1
185.94.111.1	Russian Federation	147.237.72.156	aman.idf.il	Block_Ntp_All_Net	drop	1
209.126.127.17	United States	147.237.8.14	e.orchot.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1	Russian Federation	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1

04-08-2016-23:04:00 to 04-09-2016-00:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.64.223.223	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
2.53.10.238	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-08-2016-23:04:00 to 04-09-2016-00:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
93.172.187.50	147.237.76.86	Israel	navy.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	66
93.172.187.50	147.237.77.216	Israel	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	14
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.69.34	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
80.82.79.104	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
199.101.186.221	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
65.98.40.74	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
176.223.1.38	147.237.72.166	Romania	aka.idf.il	ET SCAN NMAP -sS window 1024	1
104.128.144.131	147.237.77.176	Canada	matpash.idf.il	ET SCAN NMAP -sS window 4096	1
91.201.236.114	147.237.76.39	Ukraine	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.114	147.237.72.217	Ukraine	e.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
66.249.69.124	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
199.101.186.221	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 2048	1
66.240.213.93	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
199.101.186.221	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -f -sS	1
180.76.170.207	147.237.77.19	China	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
118.173.135.57	147.237.76.38	Thailand	e.e.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
94.255.224.2	147.237.77.226	Sweden	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.114	147.237.72.217	Ukraine	e.idf.il	ET SCAN NMAP -sS window 1024	1

04-08-2016-23:04:00 to 04-09-2016-00:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	344
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	203
17.138.56.13	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	57
176.195.96.252	Russian Federation	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	42
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
46.133.1.6	Ukraine	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	30
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
207.241.229.248	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	15
132.74.145.160	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.133.1.6	Ukraine	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
84.109.94.243	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
185.3.144.101	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
177.16.130.140	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
197.3.217.110	Tunisia	147.237.77.216	dover.idf.il	drop	SAM rule	drop	7
79.179.197.237	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
154.70.157.1	Uganda	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
208.115.111.68	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	6
31.210.189.19	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
134.196.234.127	Thailand	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.67.59.26	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.16.68.22	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
46.133.1.6	Ukraine	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.133.1.6	Ukraine	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
123.126.113.109	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	5
185.3.144.34	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
130.203.136.75	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	4
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
65.55.210.105	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.187.200.36	France	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
5.102.195.106	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
62.16.68.22	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
185.3.147.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.39.76	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.255.212	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
185.120.126.201	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.172.158	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.160.167.253	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.195.100	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
149.50.44.92	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
37.218.214.61	Palestinian Territory, Occupied	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	2
197.1.251.63	Tunisia	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	2
5.102.255.212	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
5.22.131.9	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.133.1.6	Ukraine	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	2
87.71.83.177	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	2
197.1.251.63	Tunisia	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
79.179.123.246	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
197.1.251.63	Tunisia	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
5.102.255.212	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2

04-08-2016-23:04:00 to 04-09-2016-00:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
151.147.196.20	United States	147.237.76.42	refuah.idf.il	Unauthorized HTTP Method	Block	4
151.147.196.20	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/sip_storage/files/1/	Block	3
37.26.146.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.178.218.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
8.30.87.101	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.idf.il/1038-en/dover.aspx	Block	3
157.55.39.205	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
62.210.148.91	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
66.249.69.2	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/7/71477.pdf	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
66.249.65.191	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1
5.22.135.245	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
66.249.69.34	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/שקופ 5 ית'	Block	1
40.77.167.31	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.224	Block	1
188.244.47.215	Russian Federation	147.237.76.86	navy.idf.il	Cookie Tampering on cookie sssssss: Expected a1f76f86sssssss_a1f76f86, Observed 8daa1a5asssssss_8daa1a5a	None	1
66.249.69.124	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
50.116.28.209	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
151.147.196.20	United States	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 151.147.196.20	Block	1
66.249.65.237	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-9241-he/dover.aspx	Block	1
12.37.9.42	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ID in www.idf.il/1294-en/dover.aspx	Block	1
66.249.75.44	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	Block	1
62.210.148.91	France	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
66.249.66.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/size100x0/2801.jpg	Block	1
31.210.189.19	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.75.60	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1

04-08-2016-23:04:00 to 04-09-2016-00:04:00