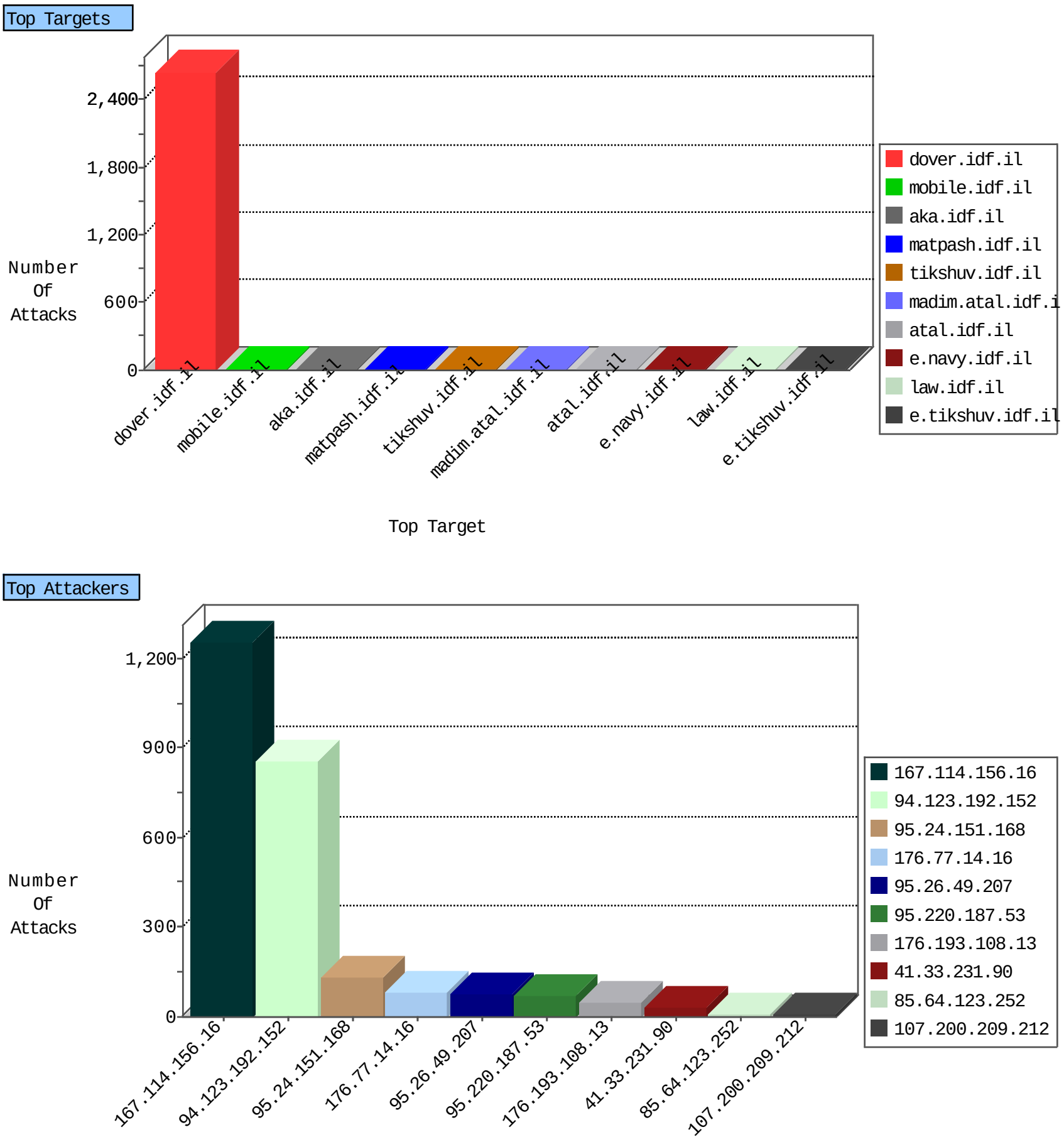
04-15-2016-06:04:06 to 04-15-2016-07:04:06

IDF Under Attack Daily Report



04-15-2016-06:04:06 to 04-15-2016-07:04:06

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	1257
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	6
2.53.55.193	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
204.42.253.2	United States	147.237.77.74	law.idf.il	Block_Ntp_All_Net	drop	2
184.105.139.112	United States	147.237.77.243	mobile.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.80	United States	147.237.8.28	e.mobile-ks.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.80	United States	147.237.77.74	law.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.72	United States	147.237.77.176	matpash.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.100	United States	147.237.0.200	m4u.idf.il	Block_Ntp_All_Net	drop	1
71.6.135.131	United States	147.237.72.217	e.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.72	United States	147.237.77.227	e.hamaz.idf.il	Block_Ntp_All_Net	drop	1

04-15-2016-06:04:06 to 04-15-2016-07:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.149	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
66.249.66.154	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
40.77.167.4	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-15-2016-06:04:06 to 04-15-2016-07:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
80.246.133.193	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
66.249.66.15	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
97.74.4.26	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
87.229.116.42	147.237.0.16	Hungary	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
64.20.48.41	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
13.92.100.128	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 4096	1
113.240.250.154	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
104.192.0.18	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
104.171.122.176	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
97.74.4.26	147.237.77.233	United States	atal.idf.il	ET SCAN Potential SSH Scan	1
87.229.116.42	147.237.0.34	Hungary	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
64.20.48.41	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
64.20.48.41	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -f -sS	1
122.3.37.100	147.237.0.35	Philippines	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.192.0.18	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
104.171.122.176	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 2048	1
104.171.122.176	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -f -sS	1

04-15-2016-06:04:06 to 04-15-2016-07:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
94.123.192.152	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	568
95.24.151.168	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	130
176.77.14.16	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	79
95.26.49.207	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	76
95.220.187.53	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	73
176.193.108.13	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	28
179.211.231.7	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
219.74.180.192	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
219.74.166.247	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
203.127.58.229	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
85.64.123.252	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
220.255.146.48	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
94.123.192.152	Turkey	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	4
107.200.209.212	United States	147.237.77.243	mobile.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
219.74.180.185	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.79.119	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.83.144	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
107.200.209.212	United States	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	3
130.193.37.16	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
203.127.58.228	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
203.127.96.232	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
203.127.96.249	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
119.73.253.5	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
203.127.96.234	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
203.127.58.233	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
203.127.96.237	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
203.127.96.221	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
157.55.39.4	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
203.127.96.245	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
80.246.133.193	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
203.127.96.229	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
68.180.230.155	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
219.74.166.227	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
203.127.96.246	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
80.82.70.198	Netherlands	147.237.0.33	idf.il	drop		drop	1
46.19.85.155	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.219	United States	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.87	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
80.246.133.193	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.11	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.208	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
80.82.70.198	Netherlands	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.220	United States	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.87	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

04-15-2016-06:04:06 to 04-15-2016-07:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
94.123.192.152	Turkey	147.237.77.216	dover.idf.il	Multiple Malformed URL from 94.123.192.152	Block	95
94.123.192.152	Turkey	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 94.123.192.152	Block	95
94.123.192.152	Turkey	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 94.123.192.152	Block	95
85.64.123.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
220.255.146.48	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
149.78.39.218	United States	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	1
69.171.228.120	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
184.105.247.194	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
149.78.254.45	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/tfasim.aspx/	Block	1
74.82.47.4	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
66.249.64.143	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/sachar/registrationwizard/register.aspx	Block	1
207.46.13.192	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
104.236.25.172	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter doc in www.aka.idf.il/kamlar/klali/default.asp	None	1
157.55.39.205	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.240	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/robots.txt	Block	1
216.218.206.68	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
107.200.209.212	United States	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
68.180.229.89	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/62312	Block	1
179.211.231.7	Brazil	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 179.211.231.7 (Open Mode)	None	1
66.249.69.125	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/templates/shared/usercontrols/navmenu/	Block	1
217.69.136.206	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/newsflash/newsflash.aspx/	Block	1
107.200.209.212	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/wp-login.php	Block	1
69.171.228.118	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
179.211.231.7	Brazil	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1

04-15-2016-06:04:06 to 04-15-2016-07:04:06