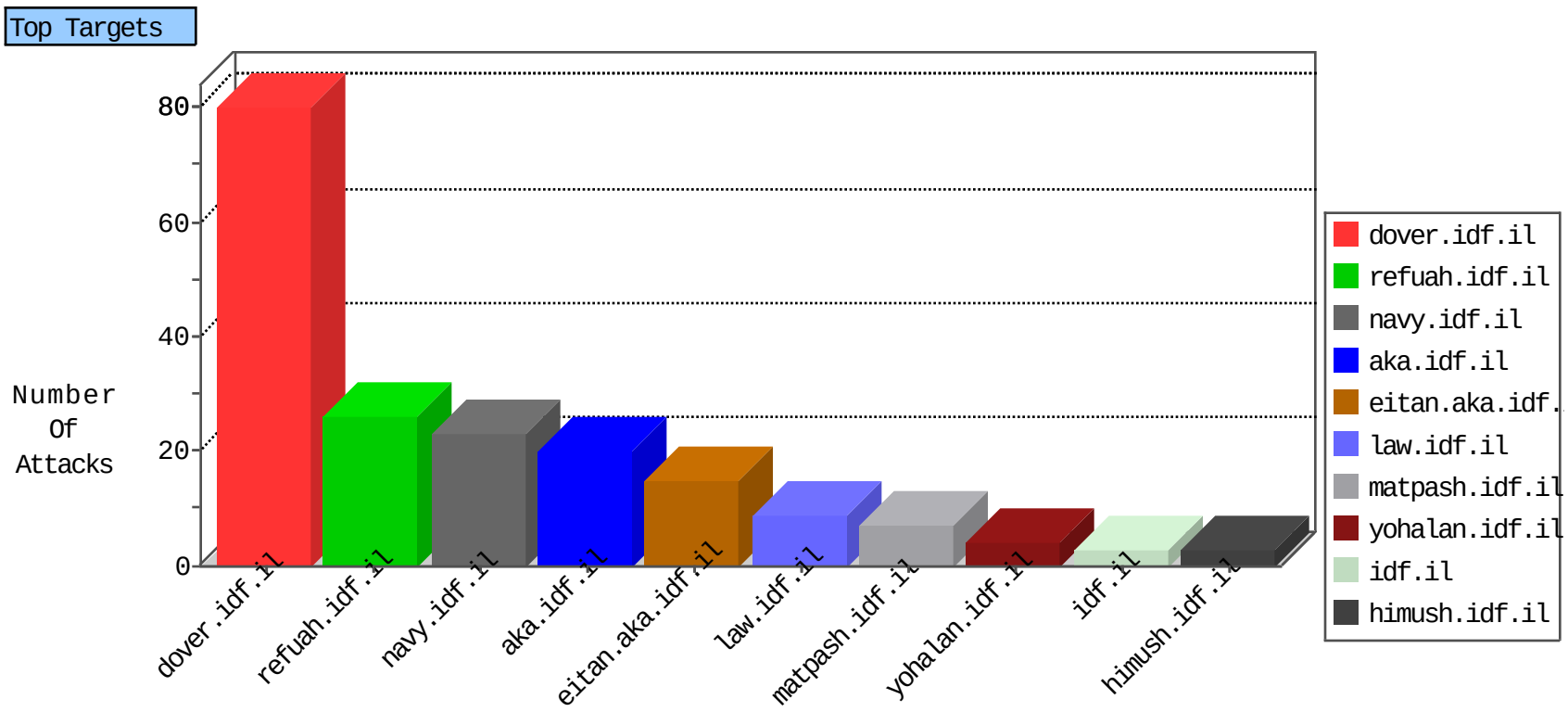
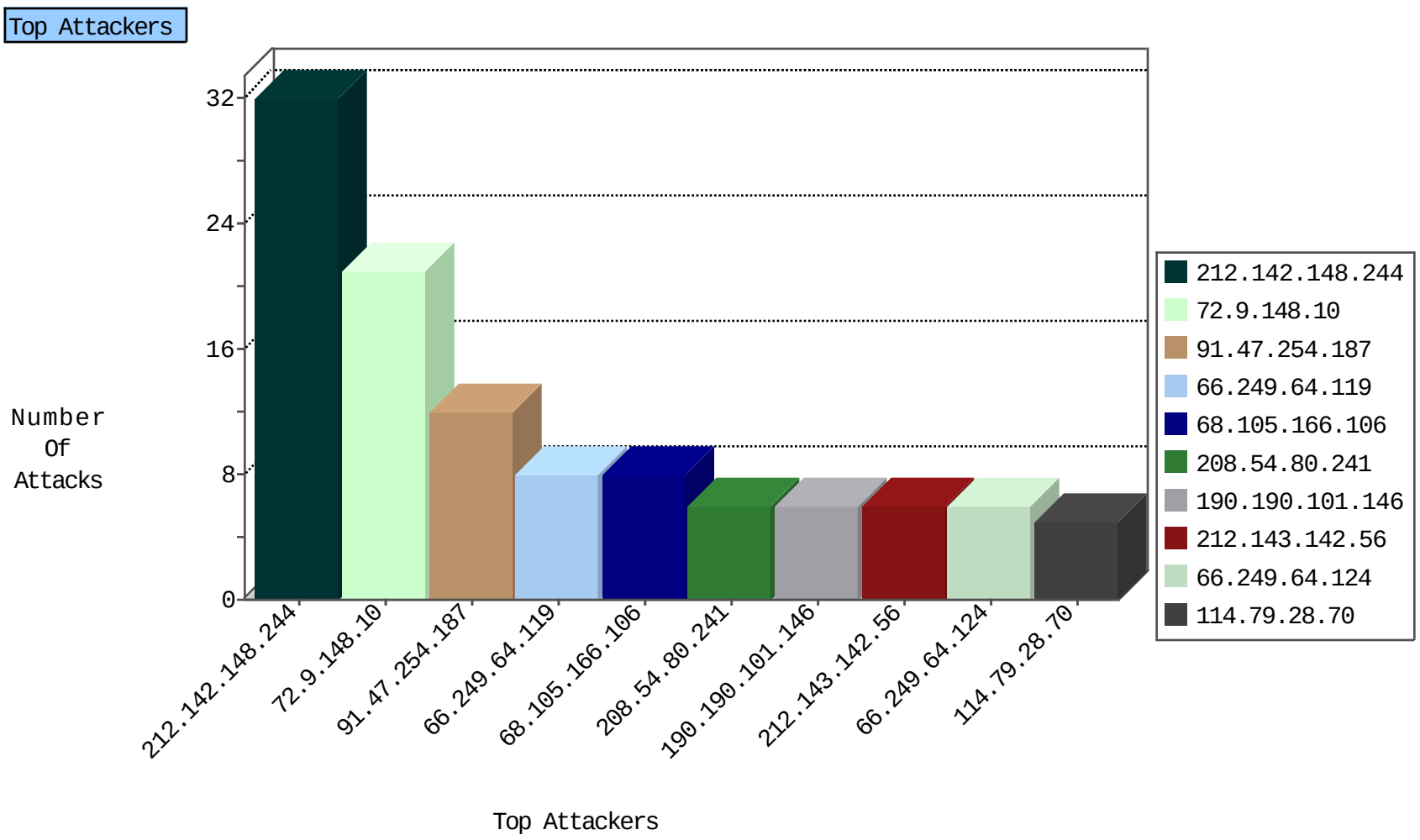
03-08-2016-03:04:04 to 03-08-2016-04:04:04

IDF Under Attack Daily Report





03-08-2016-03:04:04 to 03-08-2016-04:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.145.210.238	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	5
114.79.28.7	Indonesia	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	3
114.79.28.70	Indonesia	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	3
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
114.79.28.134	Indonesia	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	3
114.79.28.198	Indonesia	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	2
114.79.28.198	Indonesia	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	2
114.79.28.70	Indonesia	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	2
185.94.111.1		147.237.8.27	e.madim.atal.idf.il	Block_Udp_All_Nets	drop	1
216.218.206.123	United States	147.237.0.200	m4u.idf.il	Block_Udp_All_Nets	drop	1
71.6.216.38	United States	147.237.0.200	m4u.idf.il	Block_Udp_All_Nets	drop	1
210.6.215.37	Hong Kong	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
210.6.215.37	Hong Kong	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
184.105.247.234	United States	147.237.8.45	e.eitan.idf.il	Block_Udp_All_Nets	drop	1
210.6.215.37	Hong Kong	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1

03-08-2016-03:04:04 to 03-08-2016-04:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-08-2016-03:04:04 to 03-08-2016-04:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
212.142.148.244	147.237.76.42	Spain	refuah.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	18
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
132.252.173.4	147.237.77.216	Germany	dover.idf.il	GPL SCAN nmap TCP	2
104.197.254.53	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 4096	1
72.252.24.133	147.237.72.217	Jamaica	e.idf.il	ET SCAN NMAP -f -sS	1
212.142.148.244	147.237.76.42	Spain	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
40.76.95.41	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 4096	1
212.142.148.244	147.237.76.39	Spain	mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
40.76.95.41	147.237.0.33	United States	idf.il	ET SCAN NMAP -f -sS	1
212.142.148.244	147.237.76.38	Spain	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
212.142.148.244	147.237.76.34	Spain	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
212.142.148.244	147.237.76.30	Spain	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
209.126.116.147	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.72.166	China	aka.idf.il	ET SCAN NMAP -sS window 1024	1
72.252.24.133	147.237.72.217	Jamaica	e.idf.il	ET SCAN NMAP -sS window 2048	1
212.142.148.244	147.237.76.42	Spain	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.244.49.137	147.237.8.14	Hong Kong	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
212.142.148.244	147.237.76.39	Spain	mobile.meitav.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
40.76.95.41	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 2048	1
212.142.148.244	147.237.76.38	Spain	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
212.142.148.244	147.237.76.34	Spain	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
212.142.148.244	147.237.76.31	Spain	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
209.126.116.147	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 1024	1

03-08-2016-03:04:04 to 03-08-2016-04:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	15
91.47.254.187	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
68.105.166.106	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
66.249.64.119	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.64.124	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
190.190.101.146	Argentina	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
66.249.66.129	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
66.249.64.3	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
93.158.152.83	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.106.12	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
130.193.51.69	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
208.54.80.241	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
38.111.147.86	United States	147.237.77.216	dover.idf.il	drop		drop	2
68.180.228.112	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
72.9.148.10	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	2
66.249.66.133	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
212.142.148.244	Spain	147.237.76.34	yohalan.idf.il	drop		drop	2
132.252.173.4	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.155	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
212.142.148.244	Spain	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
195.62.53.168	Russian Federation	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
132.252.173.4	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.208.155.105	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
208.54.80.241	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
159.226.95.66	China	147.237.8.27	e.madim.atal.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1
51.254.44.137	United Kingdom	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
208.54.80.241	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.144	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
209.126.116.147	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
159.226.95.66	China	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
123.126.113.80	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
217.78.141.141	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
62.72.70.2	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
208.54.80.241	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.145	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.111.52.202	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
209.126.116.147	United States	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	1
184.56.214.197	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
208.54.80.241	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	1
141.212.122.154	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.111.52.202	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

03-08-2016-03:04:04 to 03-08-2016-04:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.64.119	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/shared/ajax/setivgallerycontrol.aspx	Block	2
185.82.200.91		147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to 147.237.76.200/	Block	1
70.197.72.64	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
66.249.64.53	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/2/112222.pdf	Block	1
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
37.142.68.133	Israel	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
185.112.248.32		147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
94.10.27.96	United Kingdom	147.237.77.74	law.idf.il	PHP Attempt	Block	1
134.191.232.72	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.69.3	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
37.142.68.133	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
212.142.148.244	Spain	147.237.76.42	refuah.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
94.10.27.96	United Kingdom	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
66.249.64.131	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/4/70284.pdf	Block	1
157.55.2.146	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
67.68.240.127	Canada	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
40.77.167.10	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
134.191.232.69	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.137	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
172.56.37.229	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1927-he/cogat.aspx	Block	1
51.254.44.137	United Kingdom	147.237.77.74	law.idf.il	Unauthorized URL Access to /	Block	1
134.191.232.70	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.165	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/faq/faq.aspx	Block	1

03-08-2016-03:04:04 to 03-08-2016-04:04:04