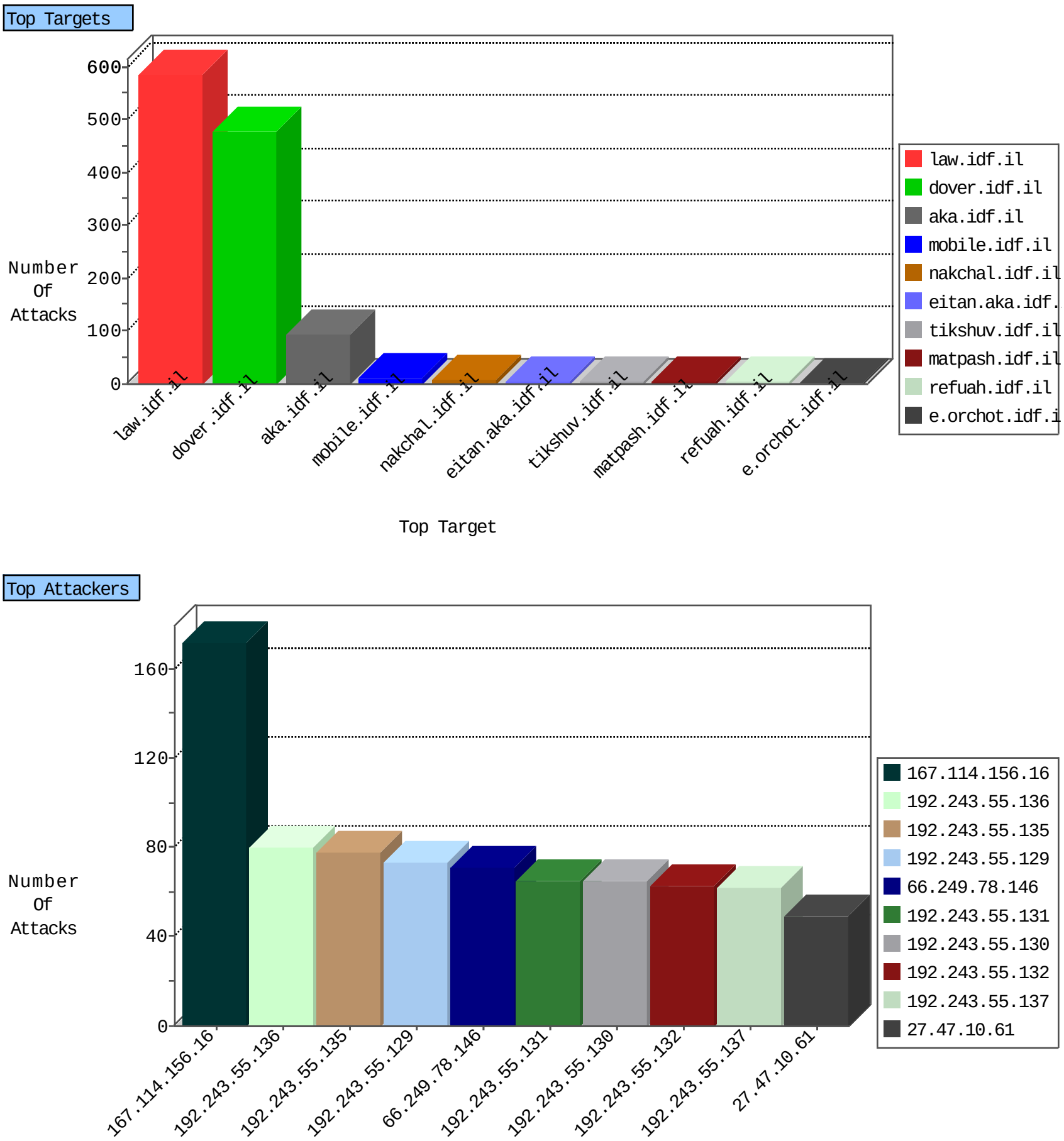
04-24-2016-04:04:03 to 04-24-2016-05:04:03

IDF Under Attack Daily Report



04-24-2016-04:04:03 to 04-24-2016-05:04:03

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	HTTP-POST-Segmented-DoS	dest-reset	17144
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	507
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	11
74.91.17.178	United States	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	2
74.91.17.180	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	2
173.208.197.254	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	2
192.243.55.136	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1
69.30.202.229	United States	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1
173.208.197.250	United States	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	drop	1

04-24-2016-04:04:03 to 04-24-2016-05:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-24-2016-04:04:03 to 04-24-2016-05:04:03

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	5
158.255.5.147	147.237.77.235	Russian Federation	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
202.29.86.129	147.237.76.201	Thailand	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
125.89.246.51	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
201.7.216.31	147.237.77.74	Brazil	law.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
13.82.25.17	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 4096	1
187.22.53.254	147.237.0.35	Brazil	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.130.5.99	147.237.76.31	Lithuania	nakchal.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.99	147.237.0.16	Lithuania	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
159.226.208.108	147.237.8.46	China	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
159.226.208.108	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
159.226.208.108	147.237.8.14	China	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
125.89.246.51	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
202.29.86.129	147.237.76.200	Thailand	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
81.218.188.199	147.237.0.15	Israel	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
2.178.160.57	147.237.8.14	Iran, Islamic Republic of	e.orchot.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.130.5.99	147.237.77.121	Lithuania	e.navy.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.99	147.237.0.33	Lithuania	idf.il	ET SCAN Potential SSH Scan	1
185.85.190.98	147.237.72.156	Turkey	aman.idf.il	ET SCAN Potential SSH Scan	1
159.226.208.108	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
159.226.208.108	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1

04-24-2016-04:04:03 to 04-24-2016-05:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	69
99.197.182.194	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
107.167.108.144	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	23
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	22
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	20
136.243.5.203	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	18
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	17
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16
192.243.55.136	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
192.243.55.129	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	16
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	15
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	15
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	15
27.47.10.61	China	147.237.77.216	dover.idf.il	drop		drop	15
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	15
192.243.55.135	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	13
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
192.243.55.135	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
27.47.10.61	China	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
27.47.10.61	China	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
192.243.55.131	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
192.243.55.130	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
192.243.55.137	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
192.243.55.136	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	11
192.243.55.129	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	10
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
192.243.55.130	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	10
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
192.243.55.137	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	10
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
192.243.55.132	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
109.253.224.203	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
192.243.55.132	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	9
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
192.243.55.134	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
192.243.55.131	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	8

04-24-2016-04:04:03 to 04-24-2016-05:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.102.6.131	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	3
109.253.224.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
208.115.111.73	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 208.115.111.73	Block	2
66.102.6.191	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
157.55.39.37	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.78.199	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/giyus/ge	Block	1
173.208.197.254	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.qeqe11.com/	Block	1
76.14.125.44	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
113.23.132.198	Malaysia	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/recruitlane.aspx	Block	1
66.102.6.188	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
198.58.102.156	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
76.14.125.44	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/index/	Block	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/main.asp	Block	1
113.80.208.142	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 113.80.208.142	Block	1
69.63.188.197	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
199.30.24.195	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
91.223.89.54	Ukraine	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;catId in www.aka.idf.il/lomdim/pniot/	None	1
113.80.208.142	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	1
74.82.47.3	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
66.249.64.70	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/news/{"key":"	Block	1
199.30.25.28	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
91.223.89.54	Ukraine	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
66.249.78.154	Israel	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
51.255.65.4	France	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
74.91.17.180	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.gege1.com/	Block	1
207.46.13.146	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1

04-24-2016-04:04:03 to 04-24-2016-05:04:03