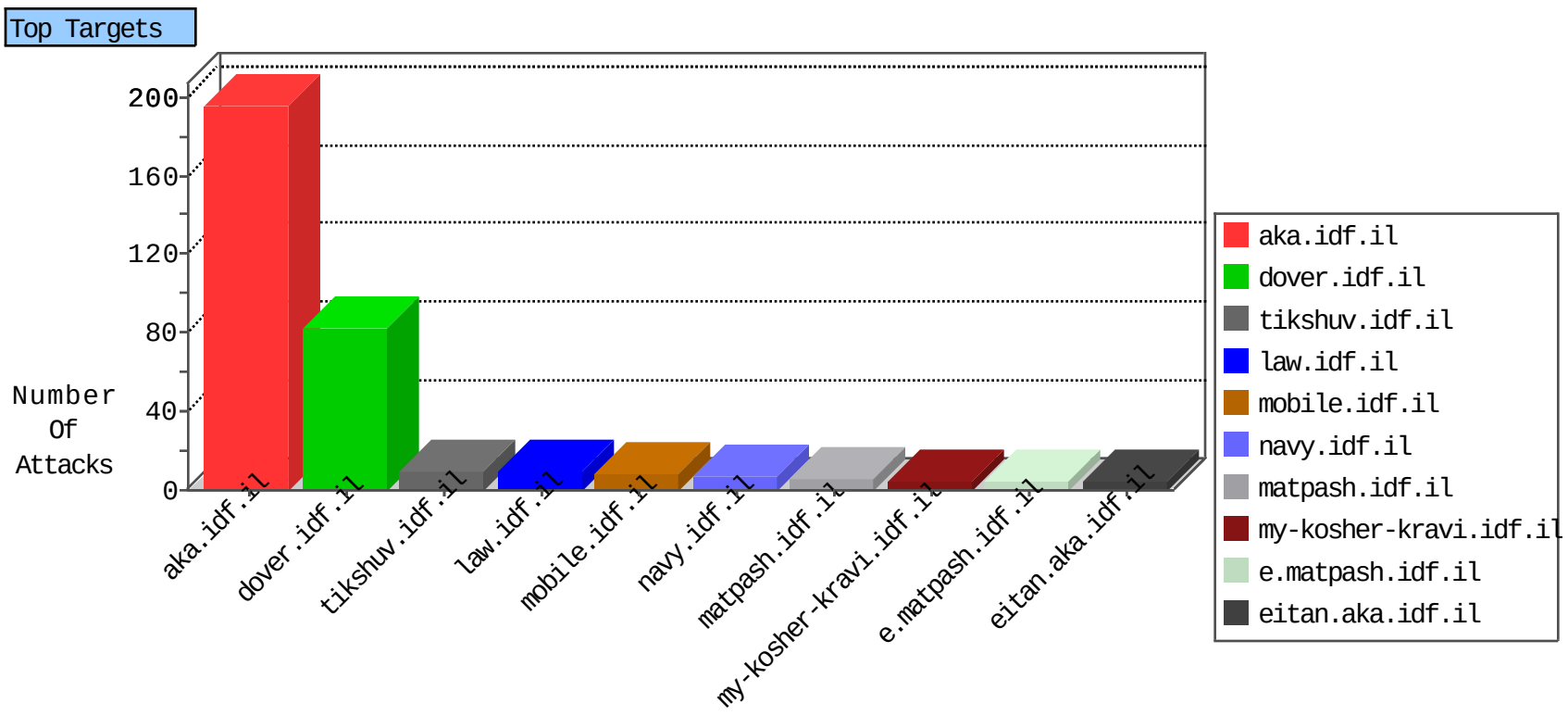
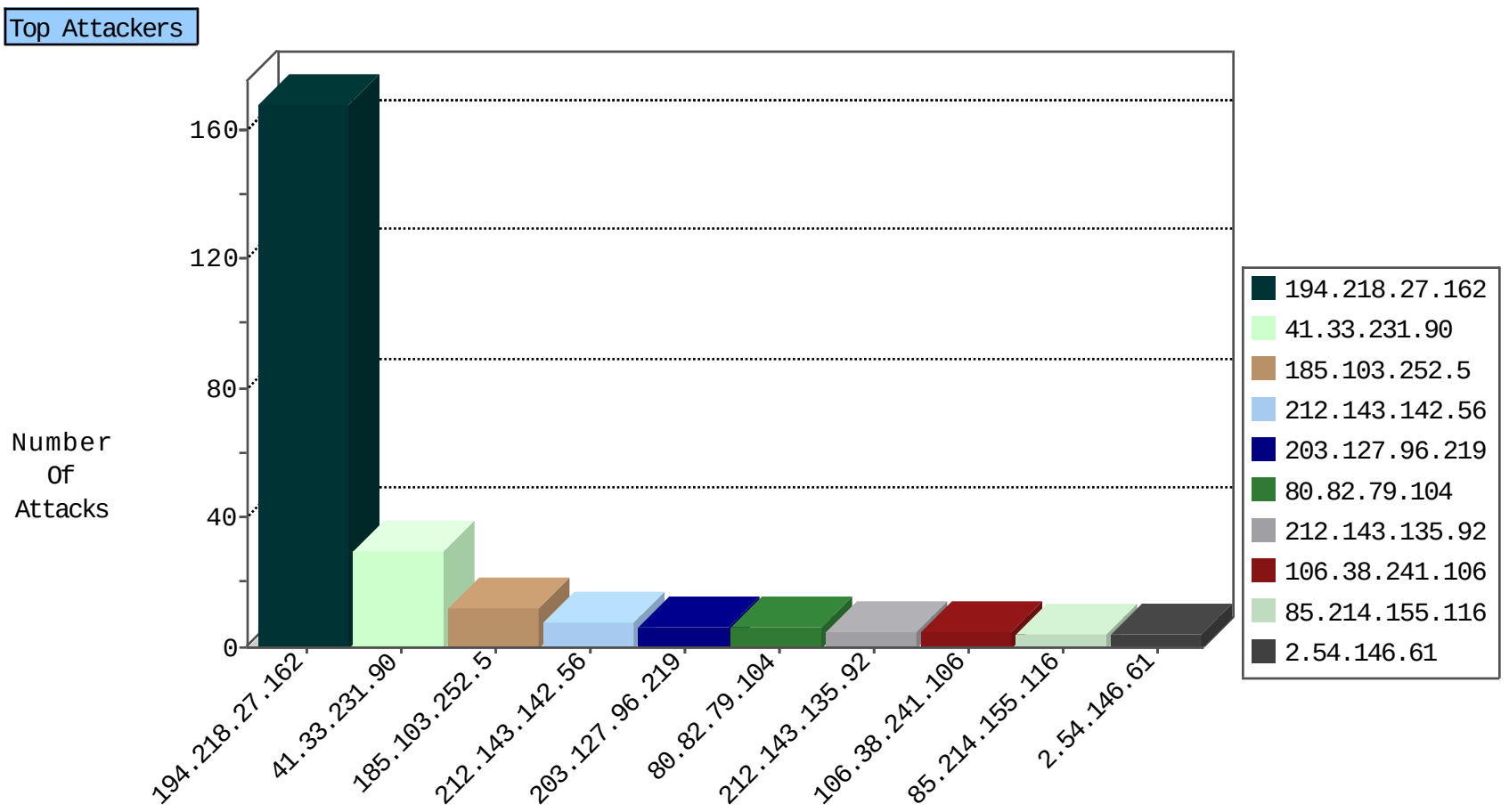
03-01-2016-02:04:07 to 03-01-2016-03:04:07

IDF Under Attack Daily Report



Top Target



Top Attackers

03-01-2016-02:04:07 to 03-01-2016-03:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.103.252.5		147.237.8.50	e.tikshuv.idf.il	Block_Udp_All_Nets	drop	4
185.103.252.5		147.237.77.178	e.matpash.idf.il	Block_Udp_All_Nets	drop	4
185.103.252.5		147.237.0.16	my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	4
185.130.5.246		147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.246		147.237.77.170	maarachot.idf.il	Block_Ntp_All_Net	drop	1
52.53.222.9	United States	147.237.77.176	matpash.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.246		147.237.0.35	akaws.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.246		147.237.8.28	e.mobile-ks.idf.il	Block_Ntp_All_Net	drop	1

03-01-2016-02:04:07 to 03-01-2016-03:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
61.135.189.110	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
109.66.183.210	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
199.30.24.212	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
40.77.167.88	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

03-01-2016-02:04:07 to 03-01-2016-03:04:07

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
66.249.66.107	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
113.59.33.61	147.237.72.14	China	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
107.2.79.150	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 3072	1
107.2.79.150	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN NMAP -f -sS	1
222.186.56.27	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
82.222.137.109	147.237.72.156	Turkey	aman.idf.il	ET SCAN NMAP -sS window 2048	1
201.173.93.184	147.237.76.176	Mexico	test.ncore.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
82.222.137.109	147.237.72.156	Turkey	aman.idf.il	ET SCAN NMAP -f -sS	1
198.72.107.101	147.237.77.74	Canada	law.idf.il	ET SCAN NMAP -sS window 2048	1
63.221.141.195	147.237.0.200	Hong Kong	m4u.idf.il	ET SCAN Potential SSH Scan	1
198.72.107.101	147.237.77.74	Canada	law.idf.il	ET SCAN NMAP -f -sS	1
120.72.118.152	147.237.76.200	Vietnam	eitan.aka.idf.il	ET SCAN NMAP -sS window 4096	1
113.59.33.61	147.237.72.14	China	dover.idf.il(old)	ET SCAN NMAP -sS window 2048	1
113.59.33.61	147.237.72.14	China	dover.idf.il(old)	ET SCAN NMAP -f -sS	1
107.2.79.150	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 2048	1
222.186.56.27	147.237.0.33	China	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
94.142.141.48	147.237.76.42	Russian Federation	refuah.idf.il	ET SCAN NMAP -sS window 3072	1
201.173.93.184	147.237.76.196	Mexico	e.sviva.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
82.222.137.109	147.237.72.156	Turkey	aman.idf.il	ET SCAN NMAP -sS window 1024	1
201.173.93.184	147.237.76.34	Mexico	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
198.72.107.101	147.237.77.74	Canada	law.idf.il	ET SCAN NMAP -sS window 1024	1
120.72.118.152	147.237.76.200	Vietnam	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1

03-01-2016-02:04:07 to 03-01-2016-03:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	112
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	56
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
2.54.146.61	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
85.214.155.116	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
79.180.209.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
129.98.33.244	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.78.223	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.132.32	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.52	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.250.171	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.143.135.92	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
5.102.195.133	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
106.38.241.106	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
40.77.167.98	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
203.127.96.219	Singapore	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
203.127.96.219	Singapore	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
80.100.6.253	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
212.143.135.92	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
203.127.96.219	Singapore	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
199.30.25.160	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
159.226.95.66	China	147.237.76.34	yohalan.idf.il	drop		drop	1
114.112.90.54	China	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
80.82.79.104	Netherlands	147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
203.127.96.221	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
46.121.122.48	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
192.0.100.154	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.146	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
201.103.232.23	Mexico	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
165.120.30.248	United Kingdom	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
80.82.79.104	Netherlands	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
203.127.96.221	Singapore	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.150	United States	147.237.0.33	idf.il	drop		drop	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
219.74.35.13	Singapore	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
80.82.79.104	Netherlands	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
173.208.213.114	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
80.82.79.104	Netherlands	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
203.127.96.221	Singapore	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
73.188.9.111	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.151	United States	147.237.0.33	idf.il	drop		drop	1
106.38.241.106	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
221.199.217.173	Australia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
80.82.79.104	Netherlands	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
178.214.79.207	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
75.68.51.127	United States	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
195.62.53.168	Russian Federation	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.22.131.120	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

03-01-2016-02:04:07 to 03-01-2016-03:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
208.113.248.206	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 208.113.248.206	Block	3
66.249.66.184	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 66.249.66.184	Block	2
108.7.216.104	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mai/giyus/general.aspx	Block	1
66.102.8.243	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
220.255.103.5	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
157.55.39.152	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/shared/usercontrols/headerupper/	Block	1
207.46.13.107	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
108.7.216.104	United States	147.237.72.166	aka.idf.il	Unknown Parameter catld in www.aka.idf.il/main/giyus/general.aspx	None	1
66.249.66.65	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/mobile/templates/getfile/getfile.aspx	Block	1
189.217.128.170	Mexico	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.69.26	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	1
24.70.166.62	Canada	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
108.7.216.104	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.66.126	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/5/110895.pdf	Block	1
189.217.128.170	Mexico	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/dover.aspx/	Block	1
40.77.167.45	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1360-he/atal.aspx	Block	1
212.140.142.99	United Kingdom	147.237.77.243	mobile.idf.il	Untraceable SSL Sessions: Open Mode	None	1
114.112.90.54	China	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/	Block	1
66.249.66.176	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/9/1449.doc	Block	1
192.157.245.129	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/pricing	Block	1
69.58.178.56	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/shared/usercontrols/headerupper/	Block	1
66.102.8.238	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
216.196.226.99	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.png	Block	1
131.253.25.246	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.66.179	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/8/1258.doc	Block	1
203.127.96.201	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1

03-01-2016-02:04:07 to 03-01-2016-03:04:07