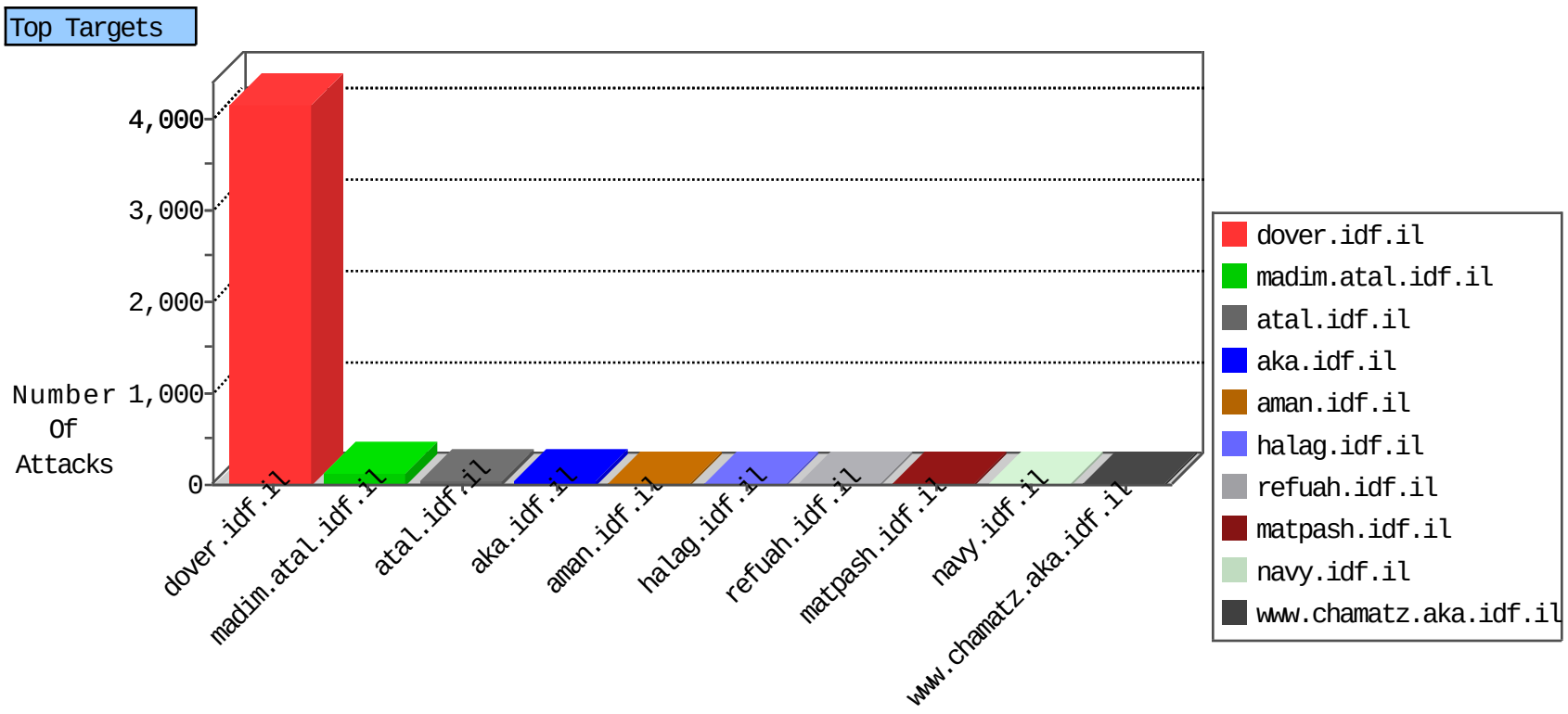
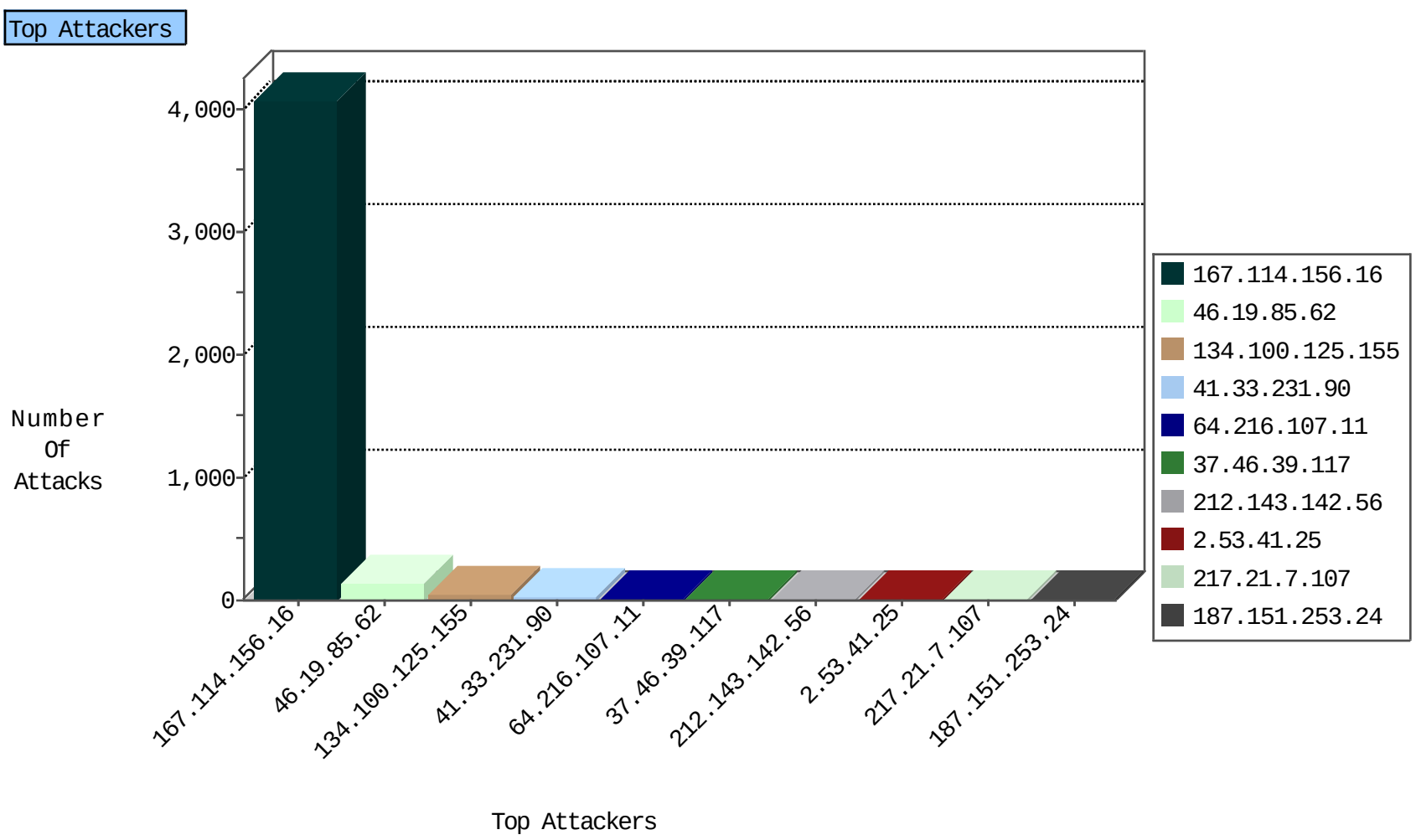
04-18-2016-01:10:03 to 04-18-2016-02:10:03

IDF Under Attack Daily Report





04-18-2016-01:10:03 to 04-18-2016-02:10:03

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	Block_Ip_Web_In	drop	4063
120.132.50.135	China	147.237.77.216	dover.idf.il	block-sp-traf1	forward	4
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
185.103.252.96	Russian Federation	147.237.77.74	law.idf.il	Block_Udp_All_Nets	drop	1
159.122.220.135	United States	147.237.8.27	e.madim.atal.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.209	Lithuania	147.237.77.74	law.idf.il	Block_Udp_All_Nets	drop	1
159.122.220.135	United States	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
59.127.241.196	Taiwan	147.237.0.33	idf.il	Block_Udp_All_Nets	drop	1

04-18-2016-01:10:03 to 04-18-2016-02:10:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.120.173.103	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
198.20.69.74	United States	147.237.76.201	e.atal.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
66.249.66.190	Israel	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

04-18-2016-01:10:03 to 04-18-2016-02:10:03

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	4
106.186.113.67	147.237.72.166	Japan	aka.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
13.94.233.163	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 3072	1
204.152.218.49	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
185.103.252.8	147.237.76.34	Russian Federation	yohalan.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.155	147.237.8.50	Ukraine	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
13.94.233.163	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 4096	1

04-18-2016-01:10:03 to 04-18-2016-02:10:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
134.100.125.155	Germany	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	34
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
64.216.107.11	United States	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
134.100.125.155	Germany	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
37.46.39.117	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.117.182.13	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	5
217.21.7.107	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
79.182.13.223	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.254.140	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
178.255.215.87	France	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.41.25	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
157.55.39.163	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
105.155.145.91	Morocco	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
79.181.111.121	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	1
185.103.252.5	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.121	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.204	United States	147.237.76.177	ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.29.215.95	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.84	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
89.138.83.152	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
70.214.70.29	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.46.39.193	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.199	United States	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
105.155.145.91	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
194.187.168.212	France	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
46.19.86.121	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.204	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.102.215.166	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
141.212.122.85	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
90.148.237.201	Saudi Arabia	147.237.77.216	dover.idf.il	Command Injection	command injection detected in URL: 'cat'	monitor	1
71.6.146.185	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
159.226.95.66	China	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.46.39.193	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.199	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
1.127.49.19	Australia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
120.132.67.209	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.111.70.124	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
194.187.168.232	France	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
141.212.122.205	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.196	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
105.155.145.91	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
71.6.165.200	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
40.78.146.128	United States	147.237.77.216	dover.idf.il	Instant Messengers	instant messenger pattern found, application: Skype	monitor	1
141.212.122.200	United States	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.213.34.5	Norway	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.205	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
23.101.61.176	Ireland	147.237.77.216	dover.idf.il	Instant Messengers	instant messenger pattern found, application: Skype	monitor	1
141.212.122.197	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
105.155.145.91	Morocco	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1

04-18-2016-01:10:03 to 04-18-2016-02:10:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	131
2.53.41.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
188.163.78.47	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 188.163.78.47	Block	3
188.163.78.47	Ukraine	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
157.55.39.83	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8870-he/refuah.aspx	Block	1
187.151.253.24	Mexico	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in URL	Block	1
85.93.91.84	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
27.159.234.88	China	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	1
188.163.78.47	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/xmlrpc.php	Block	1
173.79.166.38	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 173.79.166.38	Block	1
66.249.79.105	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
187.151.253.24	Mexico	147.237.76.42	refuah.idf.il	NULL Character in Method ¬[[#0]][[#0]][[#0]]p;[[#23]]Ü‘0W'[[#31]]D¹°úêmCvðžFš¸AµŸÿê²…/äšr_i¡[[#2]]bR˜Iåü[[#30]]›Khv×¥Ó[[#6]]•°÷}[[#11]]ð×ÄÐ±	Block	1
90.148.237.201	Saudi Arabia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/?cat=1'	Block	1
198.58.103.28	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
173.79.166.38	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/ military service	Block	1
68.180.229.226	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
5.153.234.154	Sweden	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
187.151.253.24	Mexico	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method ¬[[#0]][[#0]][[#0]]p;[[#23]]Ü‘0W'[[#31]]D¹°úêmCvðžFš¸AµŸÿê²…/äšr_i¡[[#2]]bR˜Iåü[[#30]]›Khv×¥Ó[[#6]]•°÷}[[#11]]ð×ÄÐ±	Block	1
120.132.50.135	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.ctrip.com/894-he/dover.aspx	Block	1
64.216.107.11	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list20050529.htm	Block	1
207.46.13.93	United States	147.237.72.166	aka.idf.il	Unknown Parameter profid in aka.idf.il/main/giyus/tafkidsearchformanilot.aspx	None	1
187.151.253.24	Mexico	147.237.76.42	refuah.idf.il	Abnormally Long Request method	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1806-he/dover.aspx	Block	1
5.153.234.154	Sweden	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
134.100.125.155	Germany	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
187.151.253.24	Mexico	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in Method ¬[[#0]][[#0]][[#0]]p;[[#23]]Ü‘0W'[[#31]]D¹°úêmCvðžFš¸AµŸÿê²…/äšr_i¡[[#2]]bR˜Iåü[[#30]]›Khv×¥Ó[[#6]]•°÷}[[#11]]ð×ÄÐ±	Block	1
79.180.13.245	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
23.114.212.179	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/general/mobile	Block	1

04-18-2016-01:10:03 to 04-18-2016-02:10:03