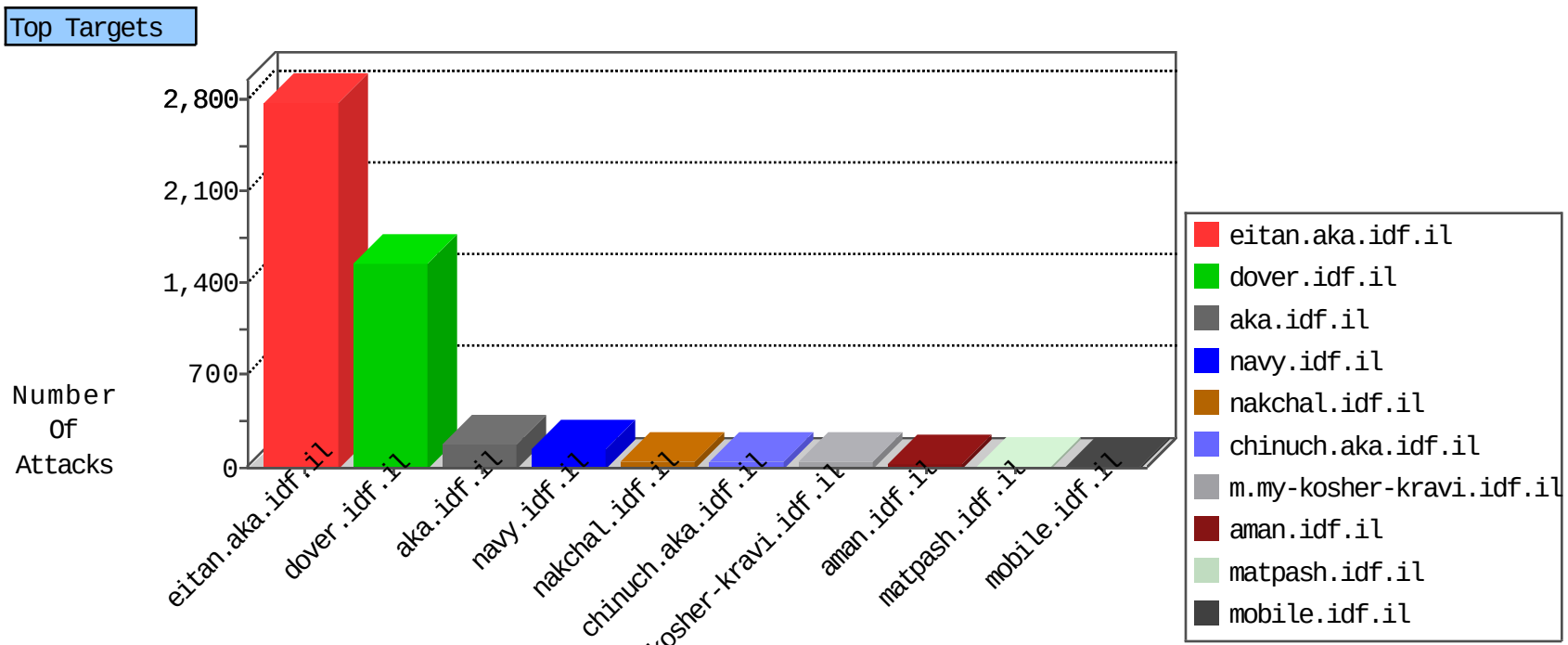
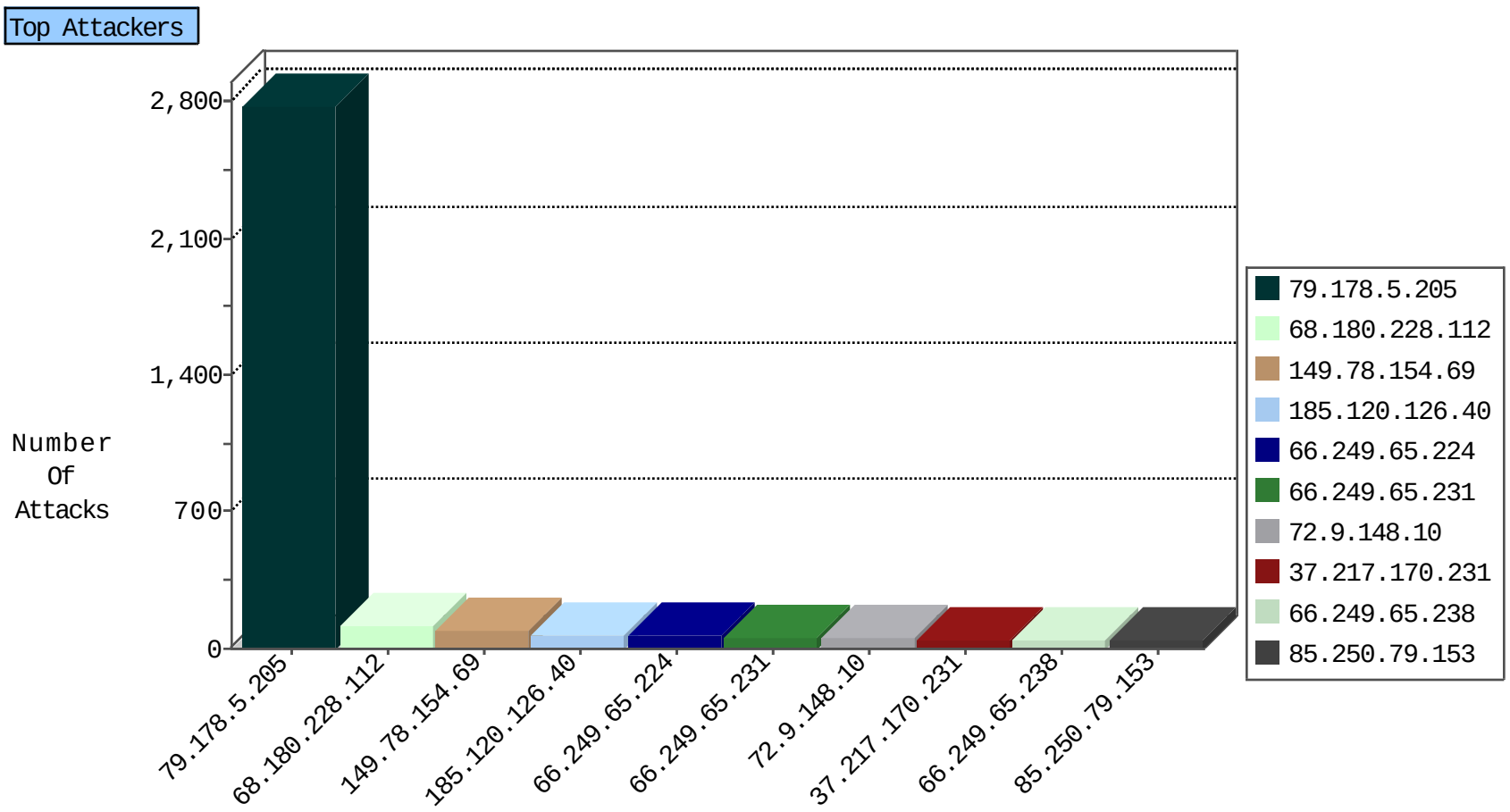
10-23-2015-23:04:04 to 10-24-2015-00:04:04

IDF Under Attack
Daily Report

Top Targets



Top Attackers



10-23-2015-23:04:04 to 10-24-2015-00:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	33
85.250.239.57	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
185.32.179.83	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	16
100.100.7.6		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
41.226.106.165	Tunisia	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
5.29.243.70	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
213.57.205.84	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
5.29.206.197	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
109.67.6.98	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
188.222.45.52	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
5.29.251.55	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
176.13.19.118	Israel	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	2
66.36.159.171	Canada	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
71.6.167.142	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
176.13.19.118	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
46.19.85.104	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
50.201.129.218	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
5.102.116.26	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
5.29.228.207	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1

10-23-2015-23:04:04 to 10-24-2015-00:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-23-2015-23:04:04 to 10-24-2015-00:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
46.151.55.40	147.237.0.15	Ukraine	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
177.107.111.200	147.237.0.34	Brazil	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
37.143.82.50	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
160.92.181.236	147.237.0.16	France	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
119.90.139.50	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
59.45.79.117	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1
177.107.111.200	147.237.77.243	Brazil	mobile.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
177.107.111.200	147.237.76.147	Brazil	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
177.107.111.200	147.237.8.45	Brazil	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
177.107.111.200	147.237.0.16	Brazil	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
119.90.139.50	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
119.90.139.50	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN NMAP -f -sS	1
59.45.79.117	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.45	China	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
177.107.111.200	147.237.77.74	Brazil	law.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
177.107.111.200	147.237.76.44	Brazil	e.refuah.idf.il	ET SCAN Potential SSH Scan	1

10-23-2015-23:04:04 to 10-24-2015-00:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.178.5.205	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	750
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	92
185.120.126.40		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	69
37.217.170.231	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
85.250.79.153	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
109.67.146.232	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
66.249.65.231	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	38
37.140.188.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
75.127.60.26	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
66.249.65.224	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	32
79.179.36.42	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
89.168.7.169	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
79.200.252.214	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
173.54.15.189	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
100.100.104.13		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
66.249.65.238	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
5.102.116.26	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
100.100.7.6		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
100.100.72.222		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
2.54.57.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	17
176.13.19.118	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
183.79.222.44	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
37.142.149.170	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
72.192.201.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
41.226.106.165	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
66.102.8.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.102.8.168	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
100.100.5.4		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
100.100.7.6		147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	10
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
70.196.77.137	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.116.169.4	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
84.228.150.201	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.34.113	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
198.58.96.215	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
50.201.129.218	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.136	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
109.65.168.248	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
185.32.179.83	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
79.180.185.191	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
37.142.185.179	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8

10-23-2015-23:04:04 to 10-24-2015-00:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.178.5.205	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 79.178.5.205	Block	1975
68.180.228.112	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	84
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	56
79.178.5.205	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/shared/ajax/lightboxmediagallery.aspx	Block	42
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	28
168.235.194.60	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shavascript	Block	14
66.249.65.231	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	14
93.158.178.208	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
46.19.85.148	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/2/1682.doc	Block	14
176.13.7.61	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	14
95.108.158.172	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
68.197.228.235	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
46.120.46.55	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	14
207.46.13.129	United States	147.237.72.166	aka.idf.il	Unknown Parameter 136cd360 in www.aka.idf.il/main/home/default.aspx	None	14
84.228.207.30	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtAreaRemarks in m.my-kosher-kravi.idf.il/templates/training/training.aspx	Block	14
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	14
141.212.122.160	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	14
46.163.68.111	Germany	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/qiyus/qeneral/default.a	Block	14
207.46.13.129	United States	147.237.72.166	aka.idf.il	Unknown Parameter KEY in aka.idf.il/ishurim/cityofficers/	None	14
84.228.207.30	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtWeight in m.my-kosher-kravi.idf.il/templates/training/training.aspx	Block	14
66.249.67.235	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/news/pages/shommronim20042011.aspx	Block	14
168.235.194.60	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 168.235.194.60	Block	14
79.178.5.205	Israel	147.237.76.200	eitan.aka.idf.il	Too Many 404: Response Code per Session	Block	14
87.250.241.67	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
67.19.79.218	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to /robots.txt	Block	14
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.238	Block	10

10-23-2015-23:04:04 to 10-24-2015-00:04:04