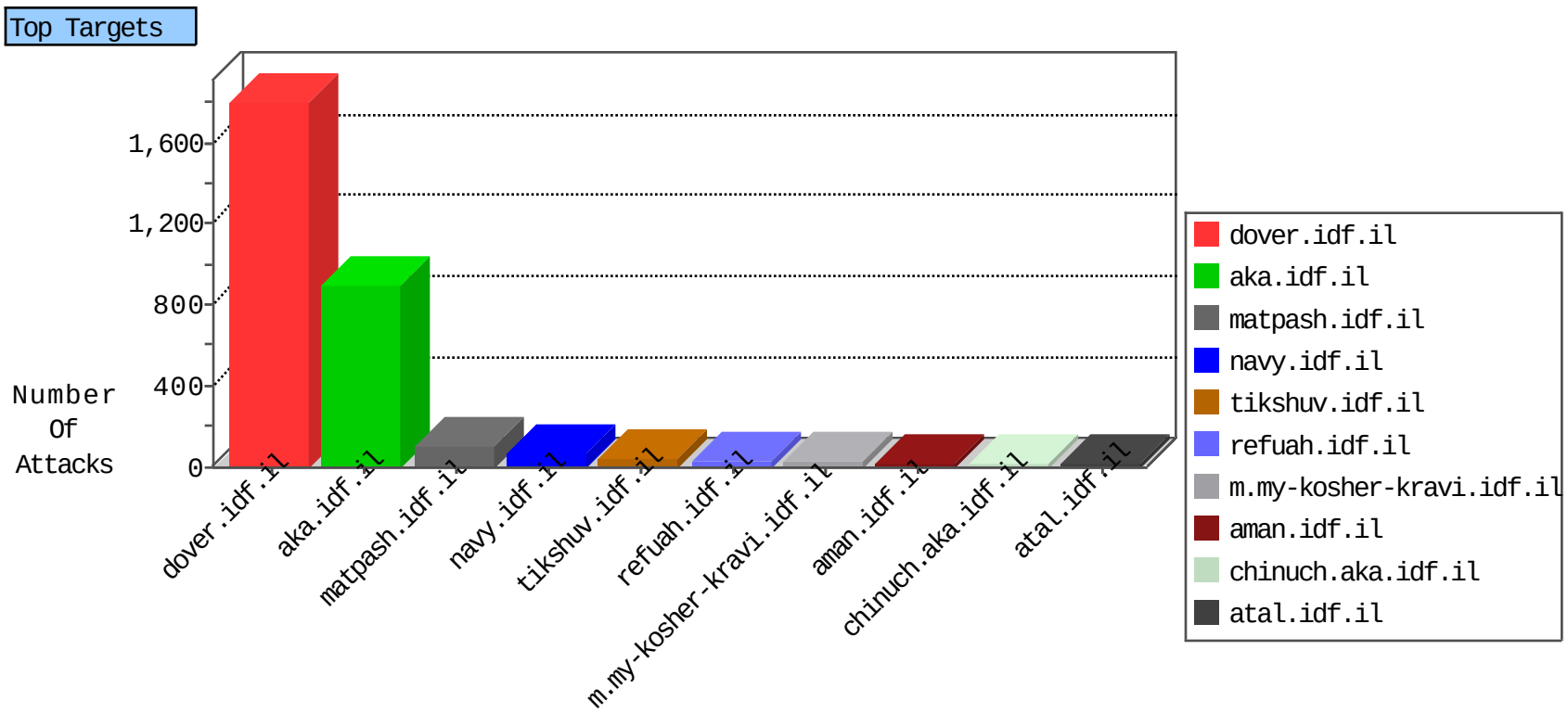
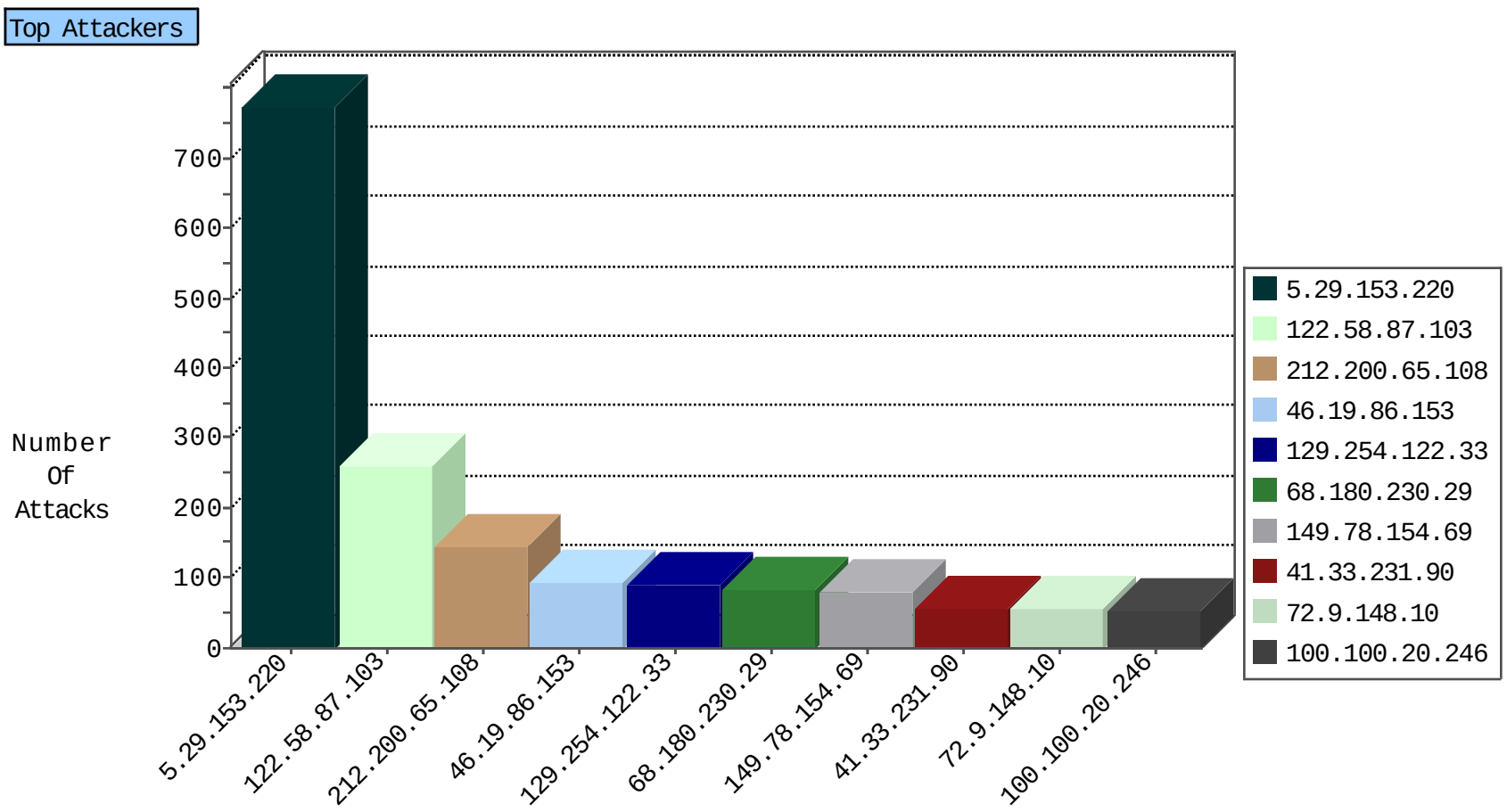
10-26-2015-06:04:05 to 10-26-2015-07:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-26-2015-06:04:05 to 10-26-2015-07:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.29.153.220	Israel	147.237.72.166	aka.idf.il	TCP Scan (vertical)	drop	3572
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	56
149.88.201.160	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	23
104.162.163.237	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	18
46.19.85.60	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	18
37.26.148.197	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	18
5.22.131.218	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
84.229.133.129	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
212.179.86.250	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
46.19.86.35	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
2.54.153.107	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
93.173.58.208	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
84.108.64.131	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
176.13.22.89	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.12.147.115	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.13.4.250	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
176.13.12.13	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
2.52.26.110	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
84.109.152.101	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
122.58.87.103	New Zealand	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
46.19.85.4	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
176.13.22.89	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
37.76.219.170	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
129.254.122.33	Korea, Republic of	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
212.199.57.198	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1

10-26-2015-06:04:05 to 10-26-2015-07:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.210.113.143	France	147.237.72.166	aka.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	13
93.173.15.230	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
188.138.17.205	France	147.237.76.202	e.halag.idf.i	13840: TLS: OpenSSL Heartbeat Packet	Block	1

10-26-2015-06:04:05 to 10-26-2015-07:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
5.29.153.220	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sS window 1024	60
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	7
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
213.225.220.68	147.237.77.74	Italy	law.idf.il	Tehila - Perl LWP with fake user agent	2
189.138.62.17	147.237.0.35	Mexico	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
94.102.48.194	147.237.72.167	Netherlands	ishurim.aka.idf.i	ET SCAN NMAP -sS window 1024	1
93.174.93.194	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
46.162.116.221	147.237.76.31	Sweden	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
201.232.25.160	147.237.8.14	Colombia	e.orchot.idf.il	ET SCAN NMAP -sS window 4096	1
190.124.35.115	147.237.76.198	Nicaragua	e.yohalan.idf.il	ET SCAN NMAP -f -sS	1
114.35.103.120	147.237.0.34	Taiwan	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
94.102.48.194	147.237.72.166	Netherlands	aka.idf.il	ET SCAN NMAP -sS window 1024	1
64.233.172.171	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	1
5.8.66.90	147.237.8.45	Russian Federation	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
199.168.136.173	147.237.77.121	United States	e.navy.idf.il	ET SCAN Potential SSH Scan	1
190.124.35.115	147.237.76.198	Nicaragua	e.yohalan.idf.il	ET SCAN NMAP -sS window 2048	1

10-26-2015-06:04:05 to 10-26-2015-07:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
122.58.87.103	New Zealand	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	257
212.200.65.108		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	145
46.19.86.153	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	93
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	80
129.254.122.33	Korea, Republic of	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	74
100.100.20.246		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	53
176.12.138.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
212.116.177.130	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
37.26.148.197	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
85.65.43.153	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
71.48.222.41	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
200.105.190.47	Bolivia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	20
149.88.201.160	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
95.35.166.41	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
5.22.131.218	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
2.54.57.255	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
93.173.233.91	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
46.19.86.39	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
46.19.85.60	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
96.29.170.195	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
2.52.26.110	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
100.100.89.19		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
31.168.2.130	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.134	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
5.102.254.93	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
176.12.140.76	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.10	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.67.192.243	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
209.133.111.211	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
37.76.219.170	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
208.69.40.101	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
65.19.138.33	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
176.13.9.145	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.29.162.165	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
65.19.138.34	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.183.32.151	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.0.101.59	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
199.16.156.125	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
68.173.158.46	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5

10-26-2015-06:04:05 to 10-26-2015-07:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1966-he/cogat.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
146.185.234.48	Russian Federation	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 146.185.234.48	Block	28
138.134.192.10	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	14
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	14
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mmmmmmm=d507fb8emmmmmmm_d507fb8e	Block	14
37.26.149.222	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	14
213.57.49.3	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	14
188.165.15.162	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9692-he/refuah.aspx	Block	14
74.82.47.2	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/	Block	14
66.249.64.239	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	14
146.185.234.48	Russian Federation	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/templates/news/news.in.aspx/templates/sendtofriend/sendtofriend.aspx	Block	14
66.249.67.227	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/23012011yezu.aspx	Block	14
199.59.148.209	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/9/size220x0/17429.jpg	Block	14
80.246.139.144	Israel	147.237.72.166	aka.idf.il	Double URL Encoding - parameter: search in www.aka.idf.il/main/giyus/pniothandler1.asmx/search	Block	14
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	14
176.13.0.28	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	14
66.249.69.35	Israel	147.237.76.147	chinuch.aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	14
199.59.148.211	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/sip_storage/files/9/size220x0/17429.jpg	Block	14
129.254.122.33	Korea, Republic of	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/en	Block	14
176.13.0.28	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Parameter Type Violation __EVENTVALIDATION in m.my-kosher-kravi.idf.il/templates/training/training.aspx	Block	14
37.26.149.219	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	14
207.46.13.46	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/cometous/	Block	14
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.59	Block	10

10-26-2015-06:04:05 to 10-26-2015-07:04:05