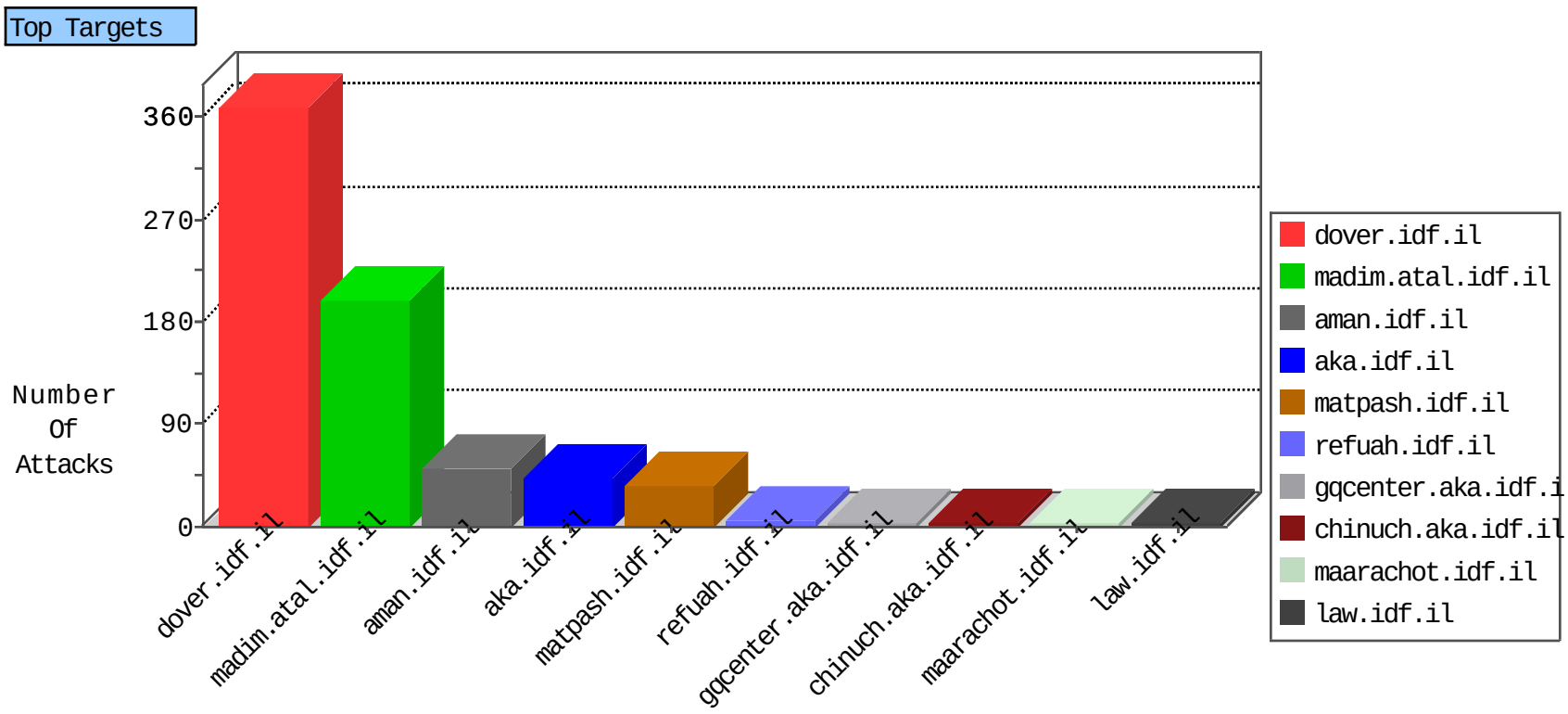
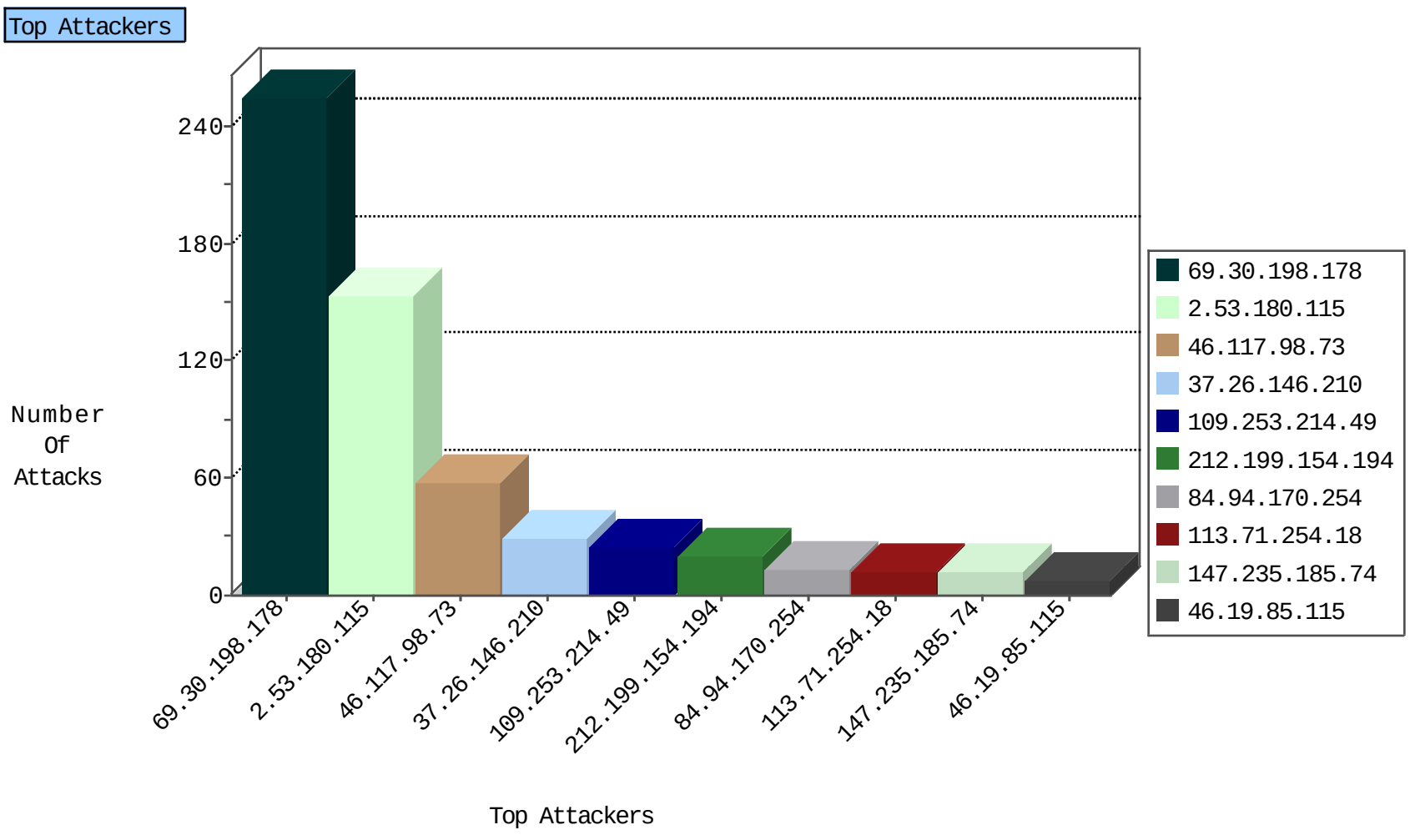
08-23-2016-10:04:06 to 08-23-2016-11:04:06

IDF Under Attack
Daily Report





08-23-2016-10:04:06 to 08-23-2016-11:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.180.139.4	Israel	147.237.72.166	aka.idf.il	Black List	drop	1

08-23-2016-10:04:06 to 08-23-2016-11:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
69.30.198.178	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	224
69.30.198.178	United States	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	13
69.30.198.178	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	13
69.30.198.178	United States	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	3
51.254.131.245	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	3
69.30.198.178	United States	147.237.76.42	refuah.idf.il	C1000074: HTTP: majestic bot	Permit	2
178.239.167.15	United Kingdom	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1

08-23-2016-10:04:06 to 08-23-2016-11:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
162.213.1.246	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	5
109.253.140.3	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
62.219.209.237	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.201	147.237.72.14	Ukraine	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
46.19.86.5	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
45.79.156.96	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
132.68.5.103	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
41.33.231.86	147.237.77.216	Egypt	dover.idf.il	portscan: TCP Distributed Portscan	1
212.150.97.225	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.29.238.117	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.97.13.120	147.237.72.166	Kyrgyzstan	aka.idf.il	portscan: TCP Distributed Portscan	1
109.67.158.68	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
202.83.21.48	147.237.76.147	India	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
84.108.89.147	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.88.208.193	147.237.77.227	Russian Federation	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
79.183.1.28	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.201	147.237.77.212	Ukraine	e.dover.idf.il	ET SCAN Potential SSH Scan	1
77.124.12.104	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.201	147.237.76.44	Ukraine	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
62.0.76.227	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.201	147.237.0.16	Ukraine	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.115	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
132.74.7.90	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
45.79.156.96	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
212.179.90.106	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
128.199.33.160	147.237.77.176	Netherlands	matpash.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
5.39.222.253	147.237.8.14	Netherlands	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
212.143.166.124	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.160.213.235	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.29.212.82	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.139.177.193	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.88.208.193	147.237.77.233	Russian Federation	atal.idf.il	ET SCAN NMAP -sS window 1024	1
84.94.170.254	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.114.105.246	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.181.52.112	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.201	147.237.77.170	Ukraine	maarachot.idf.il	ET SCAN Potential SSH Scan	1

08-23-2016-10:04:06 to 08-23-2016-11:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.117.98.73	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
109.253.214.49	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	25
212.199.154.194	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	20
84.94.170.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
147.235.185.74	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
62.0.197.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
165.51.166.129	Tunisia	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
188.161.105.210	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
176.13.231.94	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	3
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
192.117.170.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
193.188.73.1	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
74.91.23.166	United States	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	2
95.86.121.24	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.77	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
123.59.59.68	China	147.237.76.148	gqcenter.aka.idf.i	drop		drop	1
141.212.122.97	United States	147.237.76.148	gqcenter.aka.idf.i	drop		drop	1
128.232.110.28	United Kingdom	147.237.76.148	gqcenter.aka.idf.i	drop		drop	1
82.213.15.214	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.110	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
109.253.198.178	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
137.116.71.170	United States	147.237.0.200	m4u.idf.il	drop		drop	1
84.56.62.188	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.111	United States	147.237.0.35	akaws.idf.il	drop		drop	1
66.249.64.164	Israel	147.237.0.19	madim.atal.idf.il	drop	First packet isn't SYN	drop	1
176.13.247.161	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.96	United States	147.237.0.35	akaws.idf.il	drop		drop	1
141.212.122.111	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
109.253.217.58	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.96	United States	147.237.76.148	gqcenter.aka.idf.i	drop		drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.180.115	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	153
37.26.146.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
113.71.254.18	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 113.71.254.18	Block	8
46.19.85.115	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
77.124.16.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
37.8.11.201	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/homepage/www.youtube.com/v/3g51ei5nuhg	Block	3
194.114.146.227	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 194.114.146.227	Block	3
66.249.79.37	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.37	Block	3
2.53.143.109	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.244.148	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	3
113.71.254.18	China	147.237.77.176	matpash.idf.il	PHP Attempt	Block	3
84.109.116.254	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
80.246.130.46	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
176.13.1.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
192.116.60.166	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/4/109644.pdf	Block	2
176.13.238.90	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
82.81.136.58	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	2
79.180.34.148	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
31.154.49.113	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
212.179.28.215	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
192.115.67.2	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl09 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.66.6	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/	Block	1
192.243.55.138	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=62117&docid=76428	Block	1
113.71.254.18	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/index.asp	Block	1
212.179.42.241	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
192.116.60.166	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 192.116.60.166	Block	1
109.65.181.209	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
66.249.66.188	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
2.53.61.192	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
81.218.56.171	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/sip_storage/files/7	Block	1
213.57.159.165	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
109.253.230.72	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
194.114.146.227	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/4/	Block	1
82.81.83.130	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 82.81.83.130	Block	1
192.243.55.131	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/templates/shared/usercontrols/headeruppe r/	Block	1
199.30.24.21	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.85.170	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
192.243.55.135	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/tizmoret/gallery	Block	1