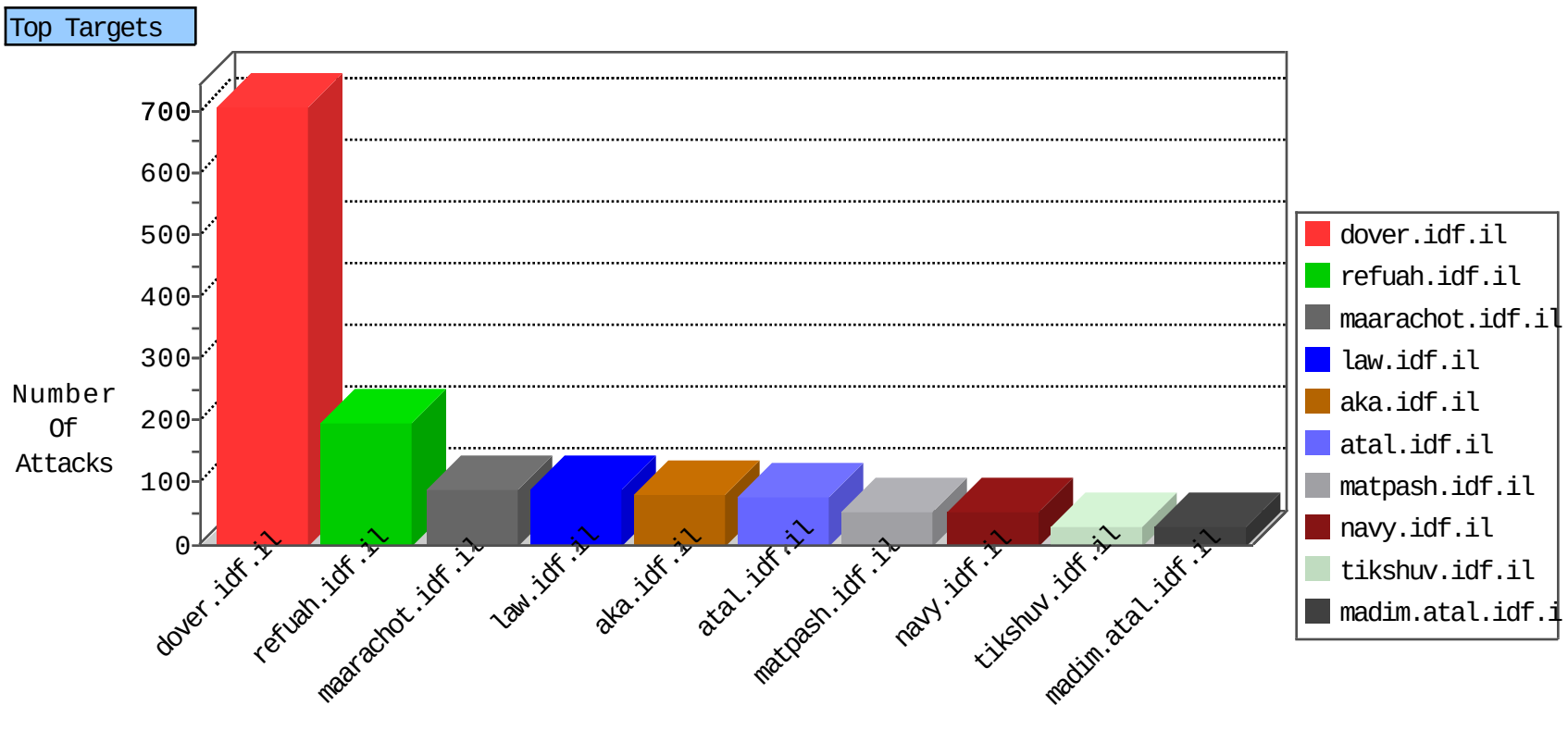
04-10-2015-05:03:01 to 04-10-2015-06:03:01

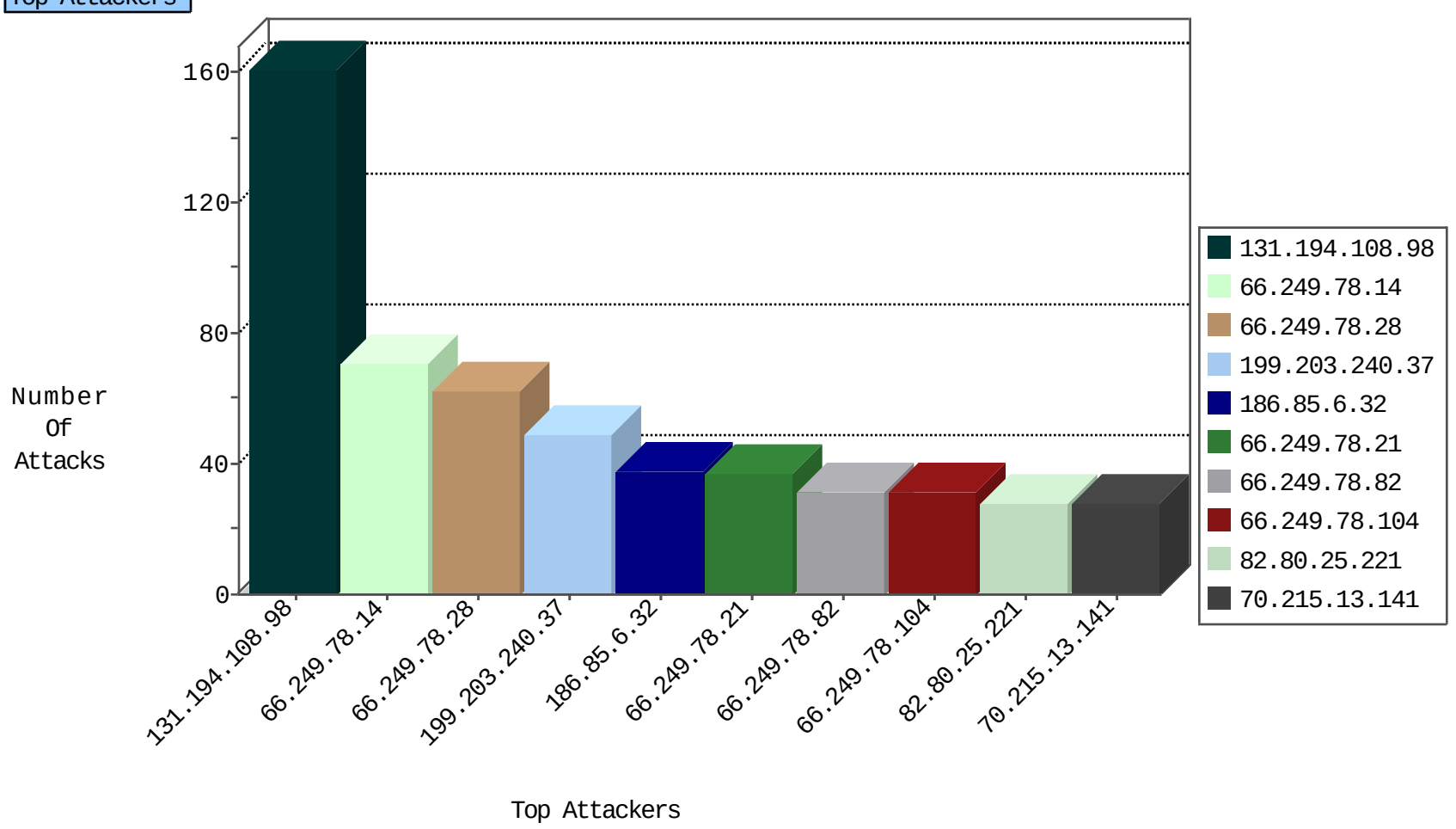
IDF Under Attack
04-10-2015-05:03:01

Top Targets



Top Target

Top Attackers



Top Attackers

04-10-2015-05:03:01 to 04-10-2015-06:03:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.14	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	71
66.249.78.28	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	62
66.249.78.21	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	35
66.249.78.82	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	31
66.249.78.104	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	30
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	27
66.249.78.111	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	24
66.249.78.97	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	24
66.249.78.96	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	23
66.249.78.86	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	23
66.249.67.22	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	20
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	19
66.249.78.79	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	18
66.249.65.132	United States	147.237.0.19	madim.atal.idf.il	Block_Ip_Web_In	drop	17
66.249.78.190	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	17
66.249.67.30	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	17
66.249.78.204	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	17
66.249.78.134	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	16
66.249.67.14	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	14
66.249.78.93	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	14
66.249.78.197	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	14
66.249.65.200	United States	147.237.0.19	madim.atal.idf.il	Block_Ip_Web_In	drop	13
66.249.78.38	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	13
66.249.69.109	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	12
66.249.78.89	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	12
66.249.69.101	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	12
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	12
66.249.78.120	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	12
66.249.69.42	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	11
66.249.69.93	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	9
66.249.65.147	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	9
66.249.64.125	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	8
66.249.69.16	United States	147.237.77.234	halag.idf.il	Block_Ip_Web_In	drop	8
66.249.69.34	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	7
66.249.64.121	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	7
66.249.80.67	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	7
66.249.78.60	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	7
66.249.69.8	United States	147.237.77.234	halag.idf.il	Block_Ip_Web_In	drop	7
66.249.78.22	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	7
66.249.89.103	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	7
66.249.78.15	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	6
66.249.78.74	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	5
66.249.64.129	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	5
66.249.89.101	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	5
66.249.69.50	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	5
66.249.64.10	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	5
66.249.64.146	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4
66.249.69.128	United States	147.237.77.234	halag.idf.il	Block_Ip_Web_In	drop	4
66.249.64.45	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	4
66.249.64.55	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	4

04-10-2015-05:03:01 to 04-10-2015-06:03:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	10
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	10

04-10-2015-05:03:01 to 04-10-2015-06:03:01

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	28
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
183.136.216.7	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.213	China	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
119.235.30.50	Indonesia	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.213	China	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	1
99.244.135.30	Canada	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 4096	1
221.235.188.213	China	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
88.249.106.23	Turkey	147.237.8.27	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.213	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.76.198	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.213	China	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
217.91.181.112	Germany	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 4096	1
203.151.27.95	Thailand	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
183.136.216.7	China	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
173.170.182.212	United States	147.237.77.205	prisha.idf.il	SERVER-WEBAPP bad HTTP/1.1 request, Potentially worm attack	1
221.235.188.213	China	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1
119.235.30.50	Indonesia	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.213	China	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	1
99.244.135.30	Canada	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.213	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.213	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.213	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
209.126.230.72	United States	147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1

04-10-2015-05:03:01 to 04-10-2015-06:03:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
131.194.108.98	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	159
199.203.240.37	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	49
186.85.6.32	Colombia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	38
185.11.8.185	Yemen	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
70.215.13.141	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
109.253.131.171	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
89.139.185.104	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
109.253.141.214	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
76.26.162.97	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
46.19.86.168	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	9
108.208.206.40	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
157.55.39.6	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
99.237.141.86	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
109.65.74.105	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
46.19.85.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
157.55.39.42	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
157.55.39.114	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
8.37.227.70	Anonymous Proxy	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	5
109.253.142.97	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
173.170.182.212	United States	147.237.77.227	e.hamaz.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	4
31.13.102.121	Ireland	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
173.170.182.212	United States	147.237.77.61	e.cogat.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	4
31.13.102.116	Ireland	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
173.170.182.212	United States	147.237.77.121	e.navy.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	4
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
188.165.15.196	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
173.170.182.212	United States	147.237.77.178	e.matpash.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	4
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
173.170.182.212	United States	147.237.77.212	e.dover.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	4
31.13.102.120	Ireland	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
104.128.23.155		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
157.55.39.6	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
109.120.157.179	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
89.216.115.8		147.237.77.216	dover.idf.il	SAM rule	drop	drop	3
104.140.80.213		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
204.237.22.235	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
8.37.228.81	Anonymous Proxy	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
196.45.48.254	Nigeria	147.237.76.196	e.sviva.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	3
8.37.228.81	Anonymous Proxy	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	3
24.15.83.48	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
198.58.103.158	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2

04-10-2015-05:03:01 to 04-10-2015-06:03:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
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	2
173.170.182.212	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
209.126.230.72	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_SERVER_HELLO)	None	1
173.170.182.212	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
173.170.182.212	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
157.55.39.114	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/french/nahal.stm.	Block	1
173.170.182.212	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
207.46.13.2	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1

04-10-2015-05:03:01 to 04-10-2015-06:03:01