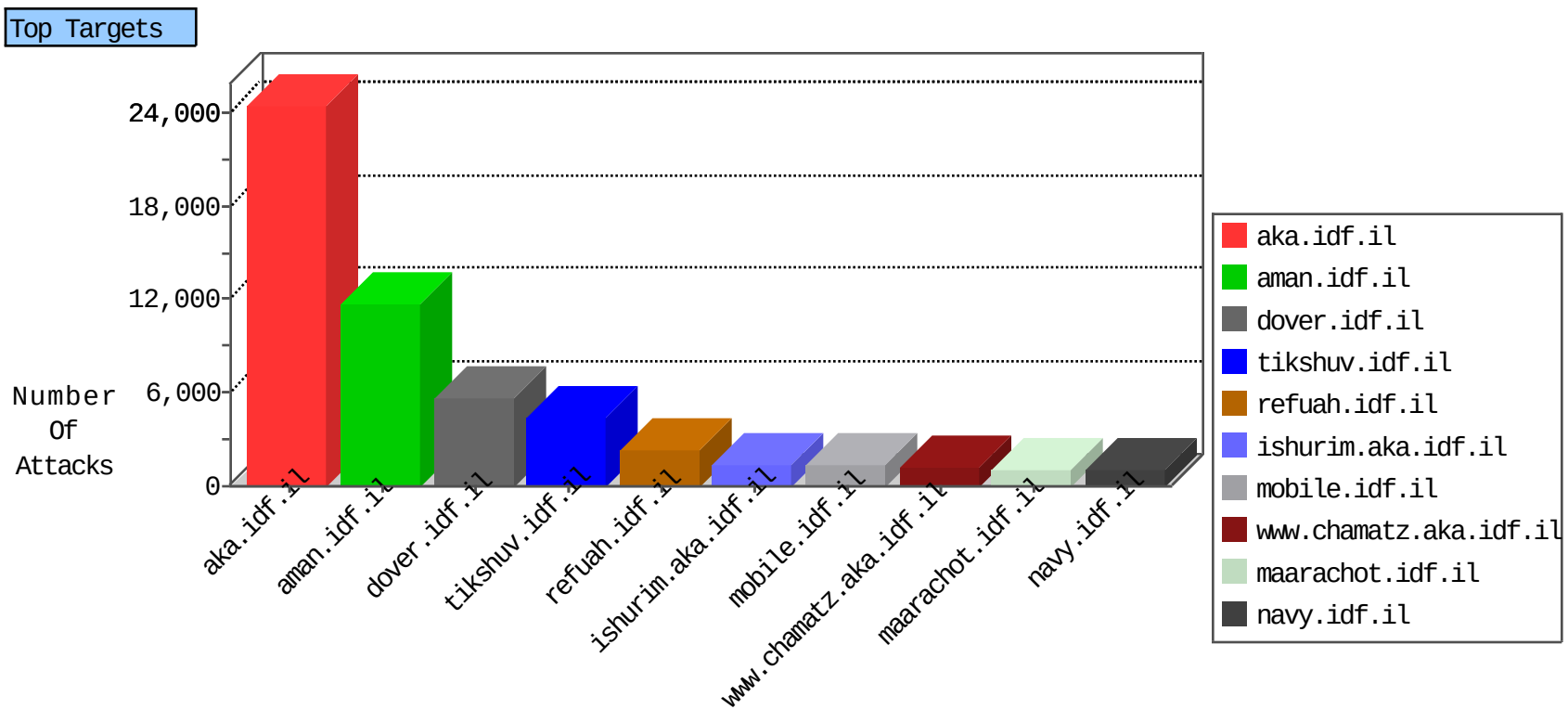
09-10-2016-19:04:04 to 09-10-2016-20:04:04

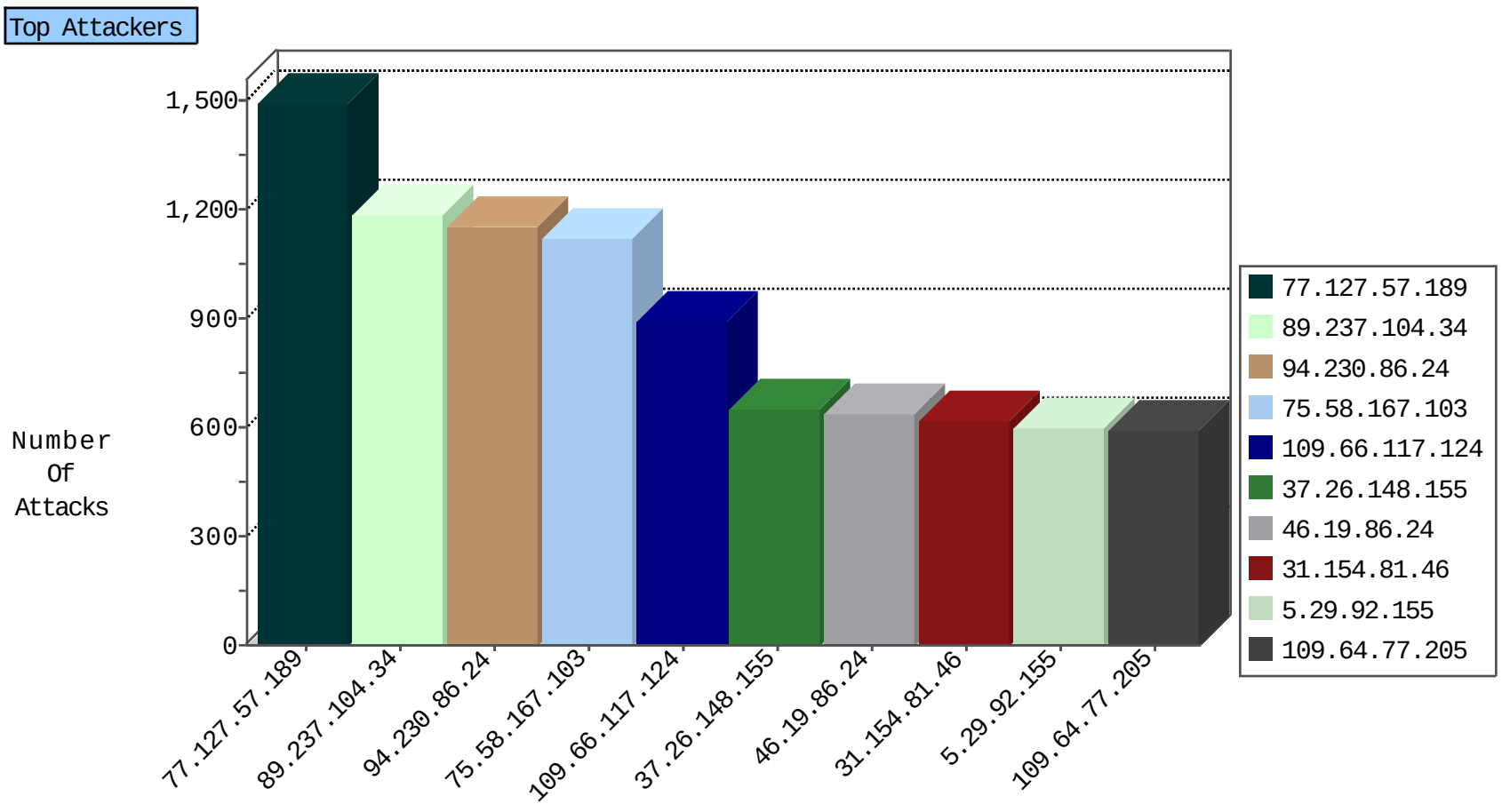
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

09-10-2016-19:04:04 to 09-10-2016-20:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.121.107.15	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4470
46.19.85.178	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1431
183.131.19.110	China	147.237.76.30	himush.idf.il	TCP Scan (vertical)	drop	137
79.181.106.173	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	117
46.116.125.115	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
77.125.9.174	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
42.112.10.66	Vietnam	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
42.112.10.80	Vietnam	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
212.143.142.56	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
42.112.10.70	Vietnam	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
79.182.3.3	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
42.112.10.83	Vietnam	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
42.112.10.74	Vietnam	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
79.182.60.248	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
42.112.10.93	Vietnam	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
42.112.10.75	Vietnam	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

09-10-2016-19:04:04 to 09-10-2016-20:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
179.43.141.208	Switzerland	147.237.76.31	nakchal.idf.il	34161: ICMP: Communication with Destination Host is Administratively Prohibited (Code 10)	Block	1
179.43.141.208	Switzerland	147.237.76.86	navy.idf.il	34161: ICMP: Communication with Destination Host is Administratively Prohibited (Code 10)	Block	1
179.43.141.208	Switzerland	147.237.76.200	eitan.aka.idf.i	34161: ICMP: Communication with Destination Host is Administratively Prohibited (Code 10)	Block	1

09-10-2016-19:04:04 to 09-10-2016-20:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
84.93.84.77	147.237.77.176	United Kingdom	matpash.idf.il	Tehila - Perl LWP with fake user agent	2
163.172.129.15	147.237.0.35	United Kingdom	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
113.240.250.154	147.237.76.86	China	navy.idf.il	ET SCAN NMAP -sS window 1024	1
104.128.144.131	147.237.77.121	Canada	e.navy.idf.il	ET SCAN NMAP -sS window 3072	1
89.218.189.253	147.237.76.196	Kazakstan	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
69.24.208.162	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
54.205.154.137	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sS window 2048	1
50.87.144.145	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
179.43.141.198	147.237.76.198	Switzerland	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
23.92.20.154	147.237.76.176	United States	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
178.79.141.130	147.237.77.235	United Kingdom	sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
23.91.75.231	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
144.76.172.150	147.237.72.166	Germany	aka.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
106.186.20.183	147.237.76.199	Japan	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
89.218.189.253	147.237.77.176	Kazakstan	matpash.idf.il	ET SCAN Potential SSH Scan	1
54.205.154.137	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sS window 4096	1
54.205.154.137	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -f -sS	1
45.33.116.208	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
179.43.141.198	147.237.76.38	Switzerland	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
23.91.75.231	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1

09-10-2016-19:04:04 to 09-10-2016-20:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
77.127.57.189	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	1352
75.58.167.103	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	1124
94.230.86.24	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	1012
109.66.117.124	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	894
37.26.148.155	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	649
109.64.77.205	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	592
5.29.92.155	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	592
84.95.208.20	Israel	147.237.77.170	maarachot.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	590
89.237.104.34	France	147.237.77.234	halag.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	570
31.154.81.46	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	550
46.19.86.24	Israel	147.237.77.226	www.chamatz.aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	529
84.229.242.81	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	506
109.64.94.51	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	495
2.53.35.108	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	425
89.237.104.34	France	147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	423
79.182.48.122	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	420
84.94.180.179	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	414
79.180.193.150	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	412
96.246.166.92	United States	147.237.77.176	matpash.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	410
46.116.101.136	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	407
5.102.195.9	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	406
46.19.85.30	Israel	147.237.76.42	refuah.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	403
80.246.130.251	Israel	147.237.77.226	www.chamatz.aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	397
141.226.162.242	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	389
80.246.139.183	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	383
2.53.149.8	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	372
109.253.145.116	Israel	147.237.76.42	refuah.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	354
77.138.42.129	France	147.237.76.42	refuah.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	354
2.53.179.116	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	350
89.139.129.24	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	346
31.154.81.64	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	330
46.121.64.237	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	326
2.53.137.221	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	320
2.53.61.208	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	304
109.67.163.131	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	301
46.116.62.150	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	301
109.66.81.211	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	300

09-10-2016-19:04:04 to 09-10-2016-20:04:04

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
185.3.147.69	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	293
141.226.218.22	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	291
2.55.173.31	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	290
46.19.85.161	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	281
109.64.141.115	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	278
79.180.99.142	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	276
109.253.240.137	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	273
109.253.201.232	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	267
87.70.242.188	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	265
46.19.86.131	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	257
85.65.218.10	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	253
217.132.16.156	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	252
2.53.144.82	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	252

09-10-2016-19:04:04 to 09-10-2016-20:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.180.177.48	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	87
79.181.106.173	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	24
2.55.184.241	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	10
109.67.131.171	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/matash	Block	1
77.126.25.145	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/wp-login.php	Block	1
31.168.72.175	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/894-he/nakhal.aspx	Block	1
80.246.139.153	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
66.249.69.92	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1404-he/atal.aspx	Block	1
207.46.13.57	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
77.138.19.55	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
37.26.148.147	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.95.208.20	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1
66.249.69.96	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1403-he/atal.aspx	Block	1
212.129.62.79	France	147.237.76.42	refuah.idf.il	Unauthorized Method HEAD for 147.237.76.42/	Block	1
77.139.241.14	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
46.19.85.35	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
84.95.208.20	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/homepage/piwik.php	Block	1
71.230.147.105	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/yohalan/	Block	1
2.53.60.219	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.102.9.2	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
89.237.104.34	France	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
77.126.25.145	Israel	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
66.249.66.251	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/patzar	Block	1

09-10-2016-19:04:04 to 09-10-2016-20:04:04