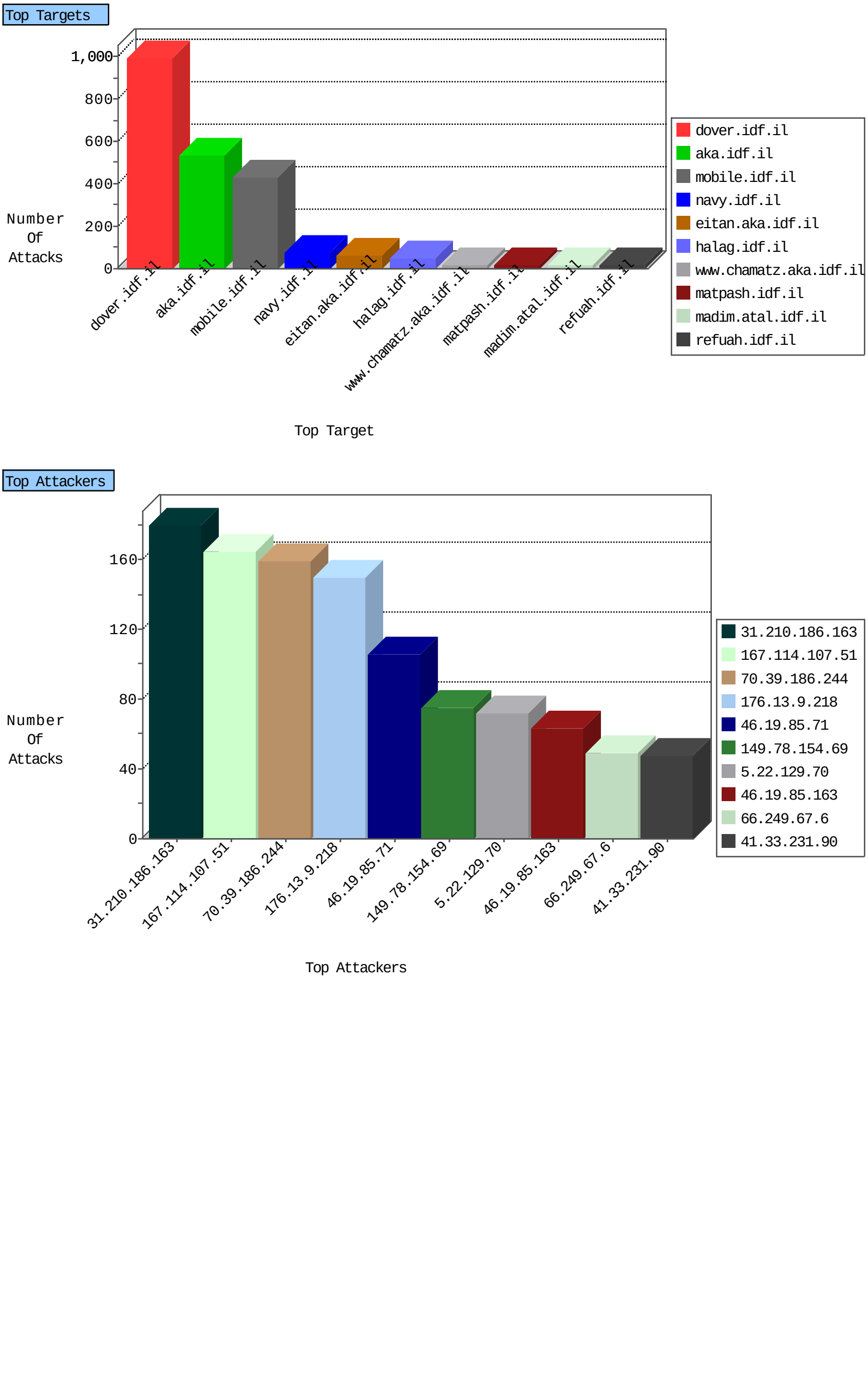
10-30-2015-02:04:03 to 10-30-2015-03:04:03

IDF Under Attack
Daily Report



10-30-2015-02:04:03 to 10-30-2015-03:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.78.166	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3528
95.86.86.118	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1045
66.249.69.92	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	548
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	444
96.54.248.209	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	411
66.249.78.134	United States	147.237.0.34	tikshuv.idf.il	TCP handshake violation, first packet not syn	drop	178
2.52.44.211	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	87
45.78.201.65		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	78
46.19.85.204	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
46.229.140.249	Russian Federation	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
37.76.217.18	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
66.249.67.20	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	4
104.32.178.58	United States	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	3
176.13.21.145	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
70.39.186.244	Satellite Provider	147.237.77.216	dover.idf.il	Frk_Purple_Con_Limit_Http	drop	3
70.39.186.244	Satellite Provider	147.237.77.216	dover.idf.il	Frk_Under_Attack_Con_Http	drop	2
222.186.56.115	China	147.237.76.148	gqcenter.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
66.249.75.60	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2
176.118.79.146	Russian Federation	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
157.55.39.183	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
66.249.69.50	United States	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	1
31.13.102.108	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
173.252.89.57	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
89.248.172.98	Netherlands	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
66.249.78.173	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
45.32.232.187		147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
149.78.154.69	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

10-30-2015-02:04:03 to 10-30-2015-03:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-30-2015-02:04:03 to 10-30-2015-03:04:03

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	4
66.249.75.2	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
80.82.50.142	147.237.8.28	Russian Federation	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
199.101.186.159	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 4096	1
61.182.170.38	147.237.76.39	China	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
199.101.186.159	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -f -sS	1
59.46.175.171	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
185.100.84.253	147.237.77.212		e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
46.183.219.66	147.237.0.19	Latvia	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
175.143.155.53	147.237.76.30	Malaysia	himush.idf.il	ET SCAN NMAP -sS window 2048	1
173.13.131.125	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 3072	1
116.58.240.201	147.237.72.166	Thailand	aka.idf.il	ET SCAN NMAP -sS window 1024	1
103.23.102.5	147.237.8.24	Indonesia	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
95.24.147.143	147.237.8.14	Russian Federation	e.orchot.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
199.101.186.159	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 2048	1
61.182.170.38	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
59.46.175.171	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
175.143.155.53	147.237.76.30	Malaysia	himush.idf.il	ET SCAN NMAP -sS window 4096	1
175.143.155.53	147.237.76.30	Malaysia	himush.idf.il	ET SCAN NMAP -f -sS	1
116.58.240.201	147.237.72.166	Thailand	aka.idf.il	ET SCAN NMAP -sS window 3072	1
103.23.102.5	147.237.8.27	Indonesia	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
103.23.102.5	147.237.8.14	Indonesia	e.orchot.idf.il	ET SCAN Potential SSH Scan	1

10-30-2015-02:04:03 to 10-30-2015-03:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
70.39.186.244	Satellite Provide	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	154
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	74
97.94.246.75	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
82.8.41.23	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
46.19.85.71	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
176.13.9.218	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	26
149.31.207.46	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
68.231.143.182	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
46.19.85.163	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
66.102.7.226	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
66.102.7.233	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
66.102.7.226	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
66.249.75.30	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
196.0.24.46	Uganda	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
5.22.129.70	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.229.140.249	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
54.72.73.168	Ireland	147.237.77.216	dover.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	9
151.80.31.112	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
66.249.75.46	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
103.18.137.21	New Zealand	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
199.30.24.137	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
173.252.89.52	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.249.75.38	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
31.168.72.175	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
31.168.72.175	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	7
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.67.65	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
96.54.248.209	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
31.154.91.159	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
77.125.136.65	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.154.167.159	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
92.247.181.31	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
157.55.39.183	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
157.55.39.3	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
202.171.186.156	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
157.55.12.69	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
198.58.96.215	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
100.100.67.69		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.67.6	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
31.13.102.125	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

10-30-2015-02:04:03 to 10-30-2015-03:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.9.218	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	120
167.114.107.51	Canada	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 167.114.107.51	Block	90
31.210.186.163	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/updatestatus.php	Block	90
31.210.186.163	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	88
46.19.85.71	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	75
167.114.107.51	Canada	147.237.72.166	aka.idf.il	Multiple Admin Blocking from 167.114.107.51	Block	60
5.22.129.70	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	60
46.19.85.163	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	45
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.67.13	Block	45
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	30
77.125.136.65	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	30
85.93.91.84	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training	Block	15
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-16648-en/dover.asp	Block	15
66.249.65.251	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/navy/terms.aspx	Block	15
167.114.107.51	Canada	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/home/main/home/default.aspx	Block	15
31.168.72.175	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	15
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/smalim/showbig.aspx	Block	15
141.212.122.64	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to /x	Block	15
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
31.168.150.126	Israel	147.237.76.200	eitan.aka.idf.il	PHP Attempt	Block	15
77.125.109.50	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	15
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/resources/images/pniot.jpg	Block	15
141.212.122.64	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to /x	Block	15
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.67.6	Block	15
176.118.79.146	Russian Federation	147.237.76.86	navy.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	15
31.168.150.126	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/xmlrpc.php	Block	15
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	15
46.19.85.204	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	15
66.249.78.204	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/	Block	15
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1146-he/chinuch.aspx	Block	15
188.165.15.66	France	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	15
77.126.22.61	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
66.249.69.42	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/1056-ar/hamaz.aspx	Block	15
66.249.65.115	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/size100x0/2978.jpg	Block	15
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/unitfs.asp	Block	15

10-30-2015-02:04:03 to 10-30-2015-03:04:03