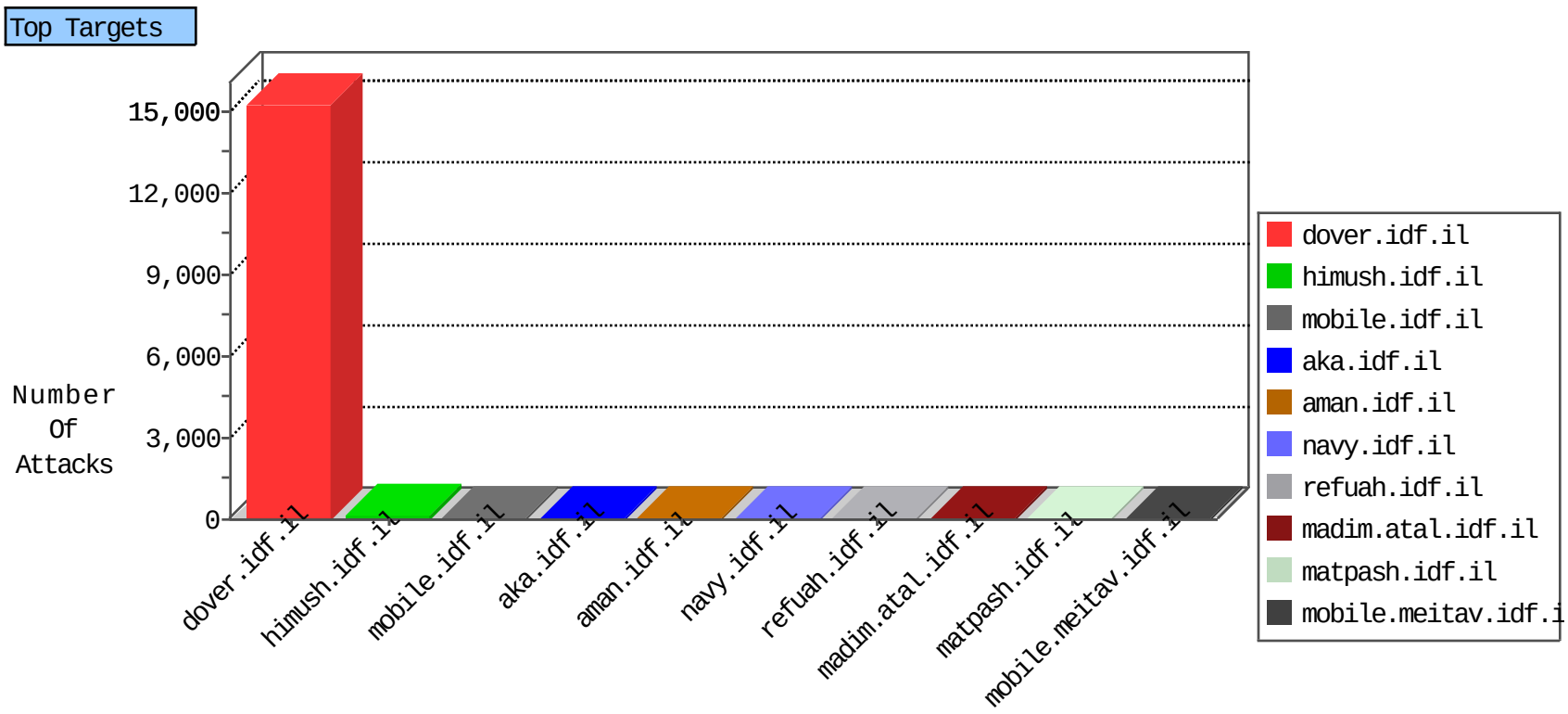
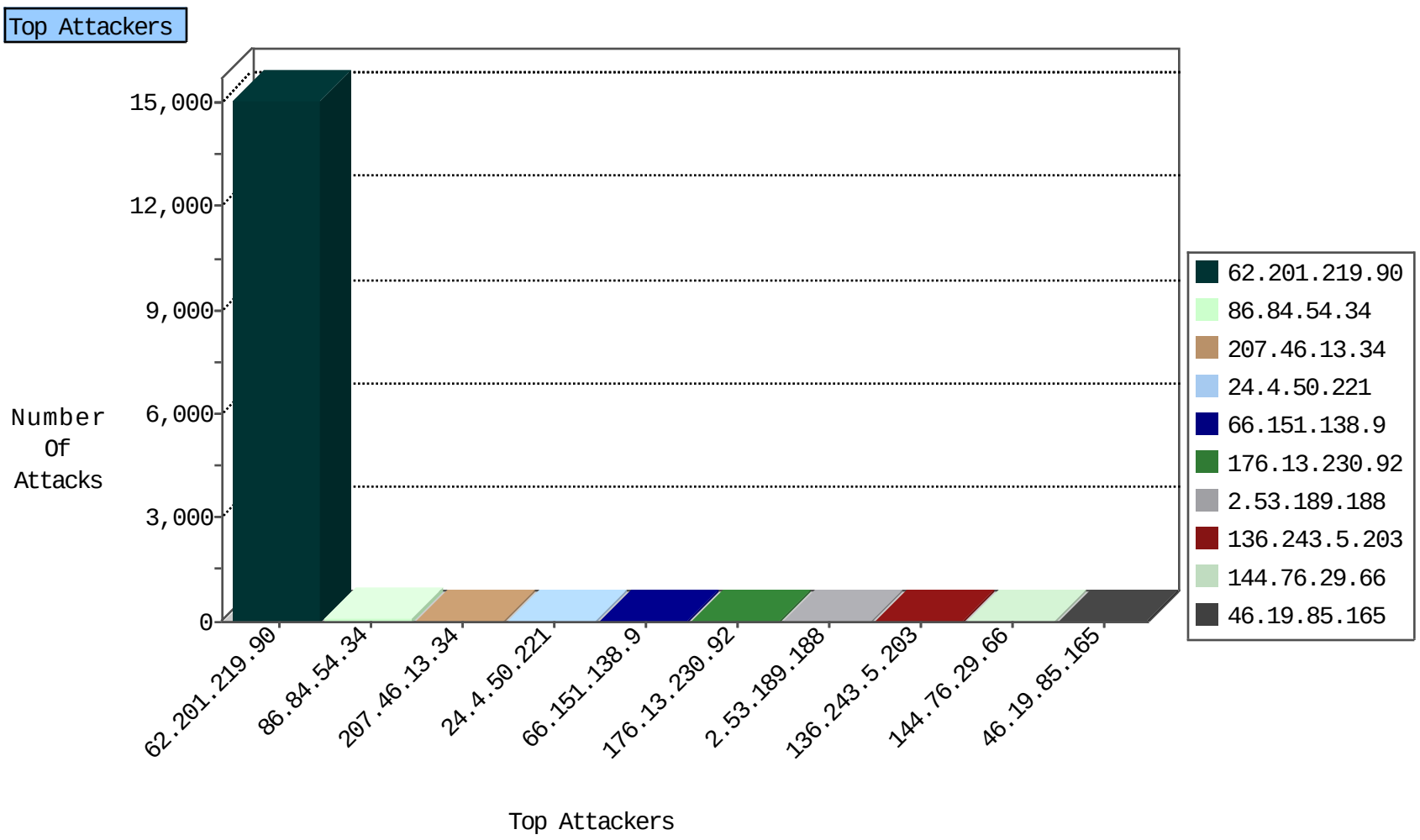
10-03-2016-00:04:01 to 10-03-2016-01:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-03-2016-00:04:01 to 10-03-2016-01:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.201.219.90	Iraq	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2985
62.201.219.90	Iraq	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	31
180.160.34.245	China	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	3
188.219.39.3	Italy	147.237.8.24	e.lifestyle.idf.il	L4 Source or Dest Port Zero	drop	1
94.102.49.190	Netherlands	147.237.76.196	e.sviva.idf.il	Black List	drop	1
58.218.200.137	China	147.237.76.177	ncore.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
141.226.161.165	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

10-03-2016-00:04:01 to 10-03-2016-01:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
162.210.196.98	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
52.1.90.117	United States	147.237.72.156	aman.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

10-03-2016-00:04:01 to 10-03-2016-01:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
117.5.148.240	147.237.77.216	Vietnam	dover.idf.il	Xenu Link Sleuth User Agent	4
208.100.26.228	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
185.40.4.208	147.237.0.17	Russian Federation	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
106.75.9.82	147.237.0.33	China	idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.76.42	Ukraine	refuah.idf.il	ET SCAN NMAP -sS window 3072	1
66.249.65.51	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	1
5.255.90.133	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
208.100.26.228	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1
188.136.237.251	147.237.77.170	Iran, Islamic Republic of	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
176.20.227.98	147.237.77.234	Denmark	halag.idf.il	ET SCAN NMAP -sS window 1024	1
106.75.9.82	147.237.0.35	China	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
106.75.9.82	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.76.42	Ukraine	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
46.120.122.219	147.237.77.74	Israel	law.idf.il	Xenu Link Sleuth User Agent	1
222.181.100.241	147.237.77.61	China	e.cogat.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

10-03-2016-00:04:01 to 10-03-2016-01:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
62.201.219.90	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13934
86.84.54.34	Netherlands	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	82
62.201.219.90	Iraq	147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	66
207.46.13.34	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	46
62.201.219.90	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	38
62.201.219.90	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	36
2.53.189.188	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
176.13.230.92	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
66.151.138.9	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	29
136.243.5.203	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
24.4.50.221	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	11
24.4.50.221	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
24.4.50.221	United States	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	10
84.108.246.197	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
24.4.50.221	United States	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	8
45.59.183.222	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.151.138.9	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.85.165	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.165	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
144.76.29.66	Germany	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
64.229.233.235	Canada	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
77.139.109.97	France	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
62.201.219.90	Iraq	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
144.76.29.66	Germany	147.237.72.167	ishurim.aka.idf.il	drop	SAM rule	drop	4
77.139.109.97	France	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
92.213.30.40	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
71.62.141.29	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
109.253.145.40	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
24.4.50.221	United States	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
92.213.30.40	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
185.3.147.246	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
82.166.102.32	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
62.201.219.90	Iraq	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
144.76.29.66	Germany	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	2
5.22.134.238	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
109.253.133.251	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
187.61.127.153	Brazil	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
5.29.173.38	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
5.22.134.238	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
144.76.29.66	Germany	147.237.76.86	navy.idf.il	drop	SAM rule	drop	2
176.13.241.40	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.121.52.58	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
84.109.180.144	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
144.76.29.66	Germany	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
5.22.134.220	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
65.35.0.137	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1

10-03-2016-00:04:01 to 10-03-2016-01:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.201.219.90	Iraq	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 62.201.219.90	Block	303
62.201.219.90	Iraq	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 62.201.219.90	Block	303
62.201.219.90	Iraq	147.237.77.216	dover.idf.il	Multiple Malformed URL from 62.201.219.90	Block	303
62.201.219.90	Iraq	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Method from 62.201.219.90	Block	68
77.125.13.125	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 77.125.13.125	Block	4
5.22.134.225	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
77.125.13.125	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
77.125.13.125	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
136.243.35.38	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
66.102.9.8	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
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-ar/dover.aspx	Block	1
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/signals/atar/	Block	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	Multiple Untraceable SSL Sessions from 169.229.3.91 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
68.180.231.60	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2061-he/cogat.aspx	Block	1
85.64.9.165	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.65.60	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8941-he/refuah.aspx	Block	1
46.19.85.65	Israel	147.237.76.86	navy.idf.il	Malformed URL	Block	1
169.229.3.91	United States	147.237.76.39	mobile.meitav.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
68.180.231.60	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-he/cogat.aspx	Block	1
92.8.33.103	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133	Block	1
66.249.66.103	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on www.chamatz.aka.idf.il/404.aspx	Block	1
46.19.85.65	Israel	147.237.76.86	navy.idf.il	Unknown HTTP Request Method ok.katana in URL	Block	1

10-03-2016-00:04:01 to 10-03-2016-01:04:01