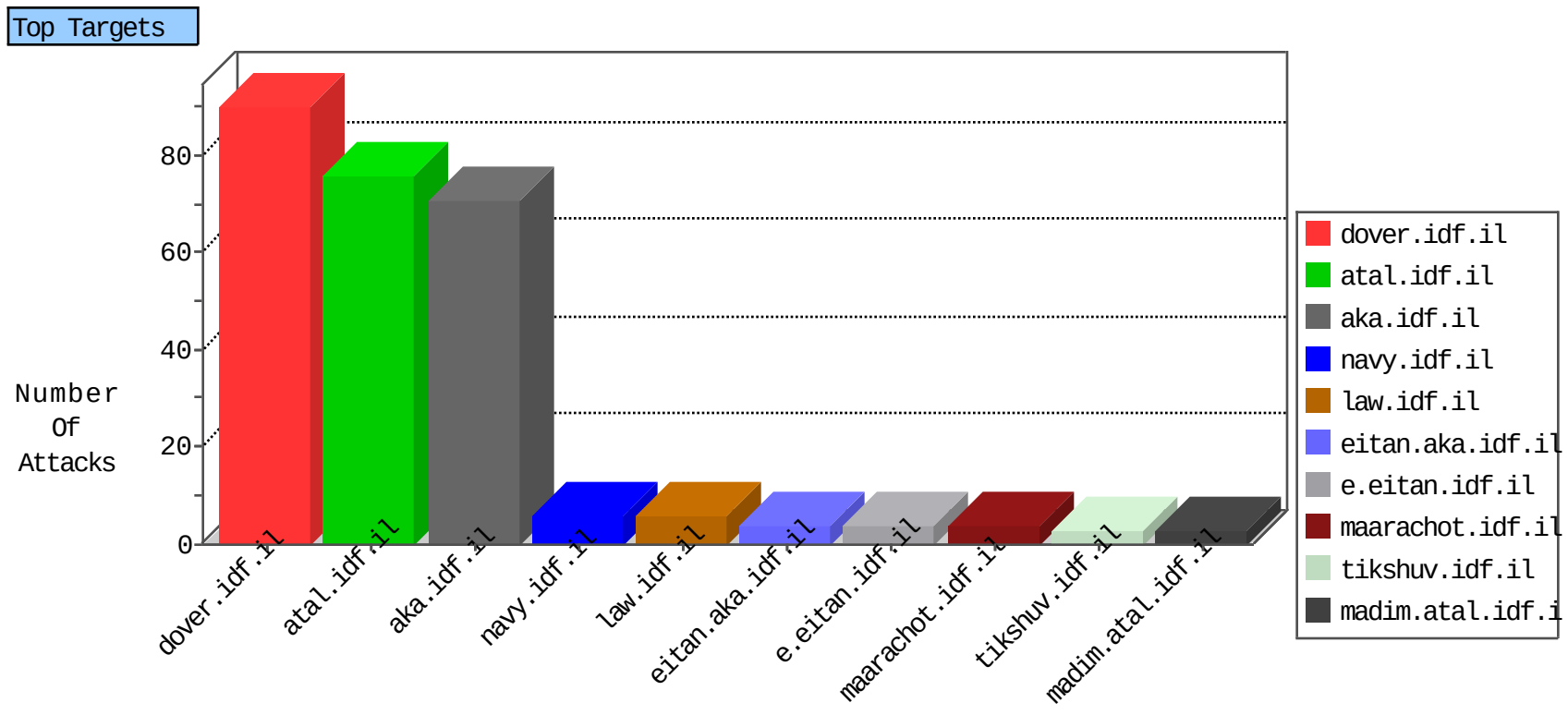
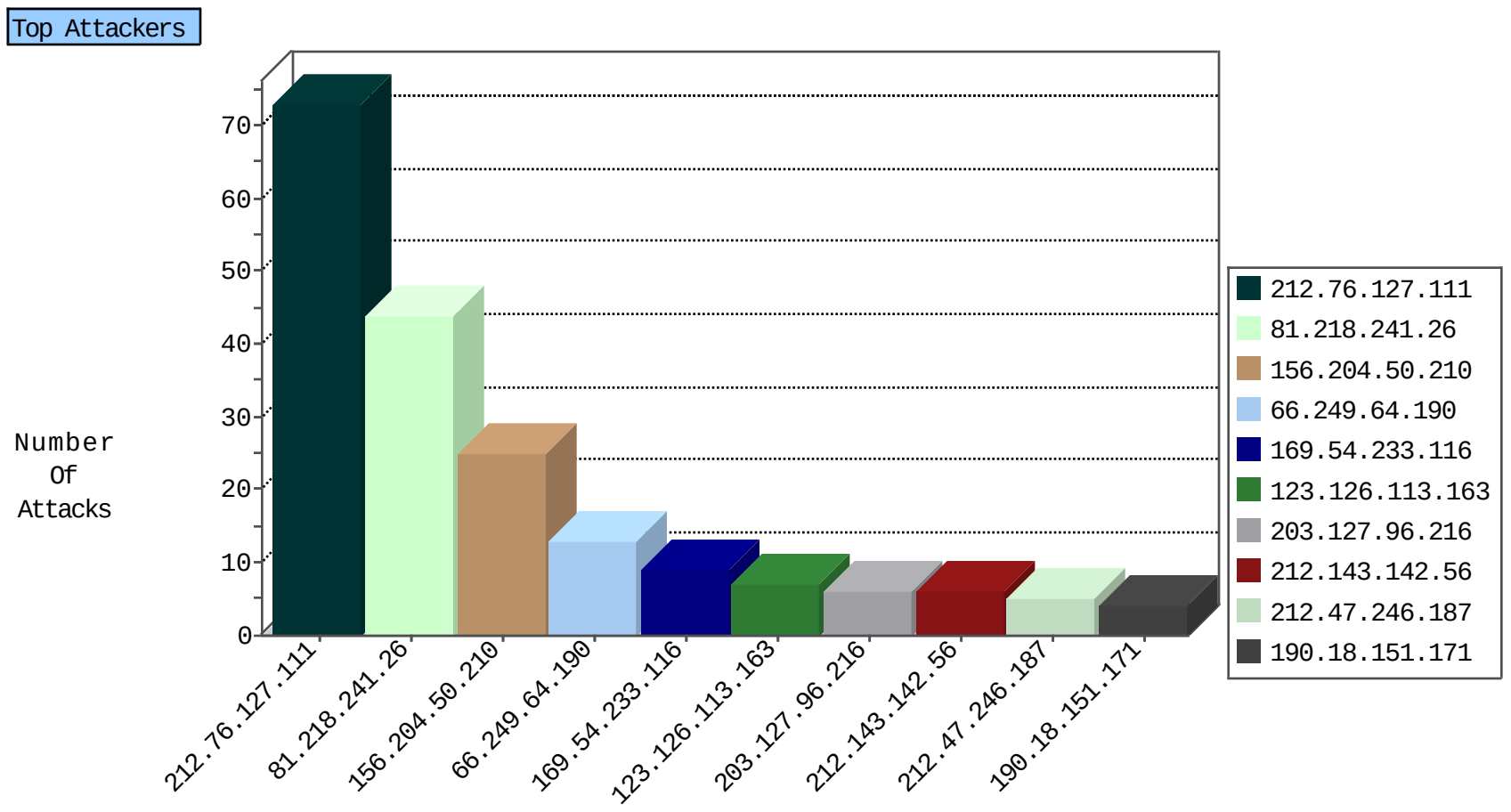
03-10-2016-02:04:01 to 03-10-2016-03:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-10-2016-02:04:01 to 03-10-2016-03:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	331
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
190.62.239.13	El Salvador	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
89.248.160.138	Netherlands	147.237.77.235	sviva.idf.il	Block_Ntp_All_Net	drop	1
178.162.198.132	Germany	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	1
89.248.160.138	Netherlands	147.237.77.243	mobile.idf.il	Block_Ntp_All_Net	drop	1
89.248.172.207	Netherlands	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
89.248.160.138	Netherlands	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
89.248.172.207	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	Block_Ntp_All_Net	drop	1

03-10-2016-02:04:01 to 03-10-2016-03:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.163	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
213.239.205.207	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
37.187.94.56	France	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
37.187.94.174	France	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
37.187.95.184	France	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
51.255.65.7	United Kingdom	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-10-2016-02:04:01 to 03-10-2016-03:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
37.187.152.205	147.237.77.74	France	law.idf.il	Tehila - Perl LWP with fake user agent	2
93.189.26.18	147.237.77.121	Austria	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
82.118.233.115	147.237.8.45	Bulgaria	e.eitan.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
54.179.151.204	147.237.8.14	Singapore	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
169.54.233.116	147.237.77.179	Netherlands	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
2.50.141.152	147.237.76.30	United Arab Emirates	himush.idf.il	ET SCAN NMAP -sS window 3072	1
169.54.233.116	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
169.54.233.116	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
169.54.233.116	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.193	147.237.77.179	Netherlands	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
93.189.26.18	147.237.77.226	Austria	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
93.189.26.18	147.237.8.45	Austria	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
198.180.198.185	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
54.179.151.204	147.237.76.198	Singapore	e.yohalan.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
169.54.233.116	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN Potential SSH Scan	1
169.54.233.116	147.237.77.176	Netherlands	matpash.idf.il	ET SCAN Potential SSH Scan	1
2.50.141.152	147.237.76.30	United Arab Emirates	himush.idf.il	ET SCAN NMAP -sS window 1024	1
169.54.233.116	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN Potential SSH Scan	1
169.54.233.116	147.237.72.217	Netherlands	e.idf.il	ET SCAN Potential SSH Scan	1
169.54.233.116	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.193	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1

03-10-2016-02:04:01 to 03-10-2016-03:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
156.204.50.210		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
2.54.85.73	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	4
190.18.151.171	Argentina	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
199.30.16.167	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
109.67.35.186	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
130.193.37.16	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
203.127.96.216	Singapore	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
123.126.113.163	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
203.127.96.216	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
142.176.10.78	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
203.127.96.216	Singapore	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
142.176.10.78	Canada	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
212.47.246.187	France	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
103.16.228.98	Hong Kong	147.237.77.216	dover.idf.il	Header Rejection	header rejection pattern found in request	monitor	1
220.255.103.232	Singapore	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
203.127.96.218	Singapore	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.152	United States	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.102.195.72	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
212.47.246.187	France	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
203.127.96.217	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
159.226.95.66	China	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
203.127.96.218	Singapore	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
141.212.122.153	United States	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
31.44.134.248	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
212.47.246.187	France	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
203.127.96.217	Singapore	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
172.56.35.210	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
212.47.246.187	France	147.237.8.46	e.chinuch.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
203.127.96.217	Singapore	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
176.228.71.191	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
212.47.246.187	France	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
213.8.204.48	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
203.127.96.218	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.228.71.191	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.8.132.67	Russian Federation	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.76.127.111	Israel	147.237.77.233	atal.idf.il	Automated Vulnerability Scanning V1	Block	73
77.125.131.89	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
40.77.167.82	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
220.255.98.120	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
220.255.97.58	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
117.78.13.54	China	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/894-he	Block	1
203.127.58.236	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
68.180.228.112	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/'	Block	1
118.103.8.153	Japan	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
54.166.39.183	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
203.127.96.229	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
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	1
220.255.98.120	Singapore	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
156.199.25.11		147.237.77.170	maarachot.idf.il	PHP Attempt	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
220.255.103.232	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
156.199.25.11		147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/xmlrpc.php	Block	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/forms/downloadform.asp	Block	1
219.74.38.152	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1503-en/dover.aspx.	Block	1
31.44.134.248	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
220.255.145.186	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
203.127.58.235	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.83.155	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1