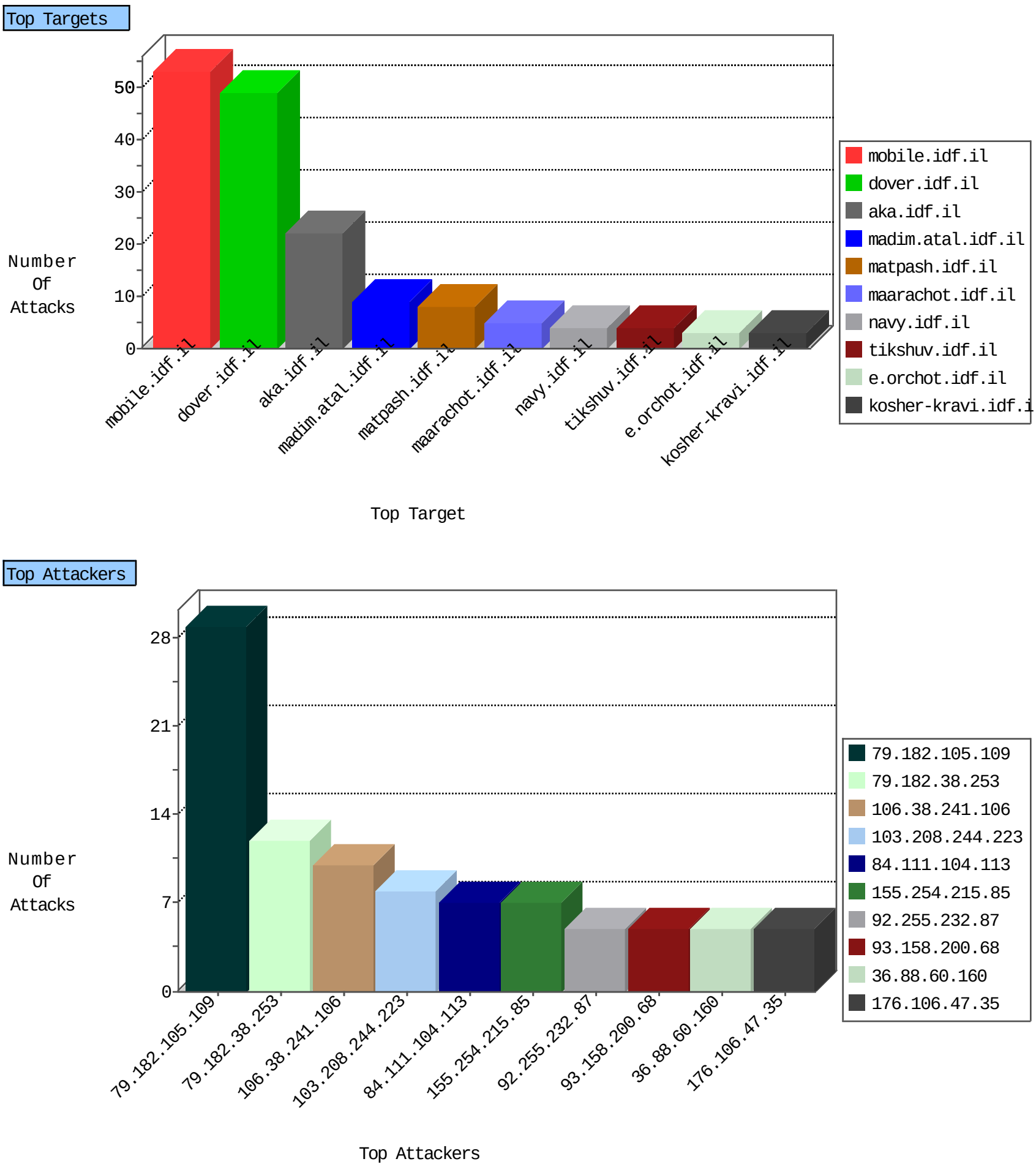
10-01-2016-07:04:01 to 10-01-2016-08:04:01

IDF Under Attack
Daily Report



10-01-2016-07:04:01 to 10-01-2016-08:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.111.104.113	Israel	147.237.72.166	aka.idf.il	Black List	drop	7
103.208.244.223		147.237.76.147	chinuch.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
155.94.224.164	United States	147.237.77.243	mobile.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1

10-01-2016-07:04:01 to 10-01-2016-08:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
151.80.31.160	France	147.237.0.34	tikshuv.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

10-01-2016-07:04:01 to 10-01-2016-08:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
40.84.189.118	147.237.76.201	United States	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
14.188.173.207	147.237.8.14	Vietnam	e.orchot.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
103.208.244.223	147.237.76.44		e.refuah.idf.il	ET SCAN Potential SSH Scan	1
103.208.244.223	147.237.76.31		nakchal.idf.il	ET SCAN Potential SSH Scan	1
103.208.244.223	147.237.0.19		madim.atal.idf.il	ET SCAN Potential SSH Scan	1
54.144.119.103	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
46.249.82.10	147.237.8.45	Bulgaria	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
31.211.102.129	147.237.77.74	Russian Federation	law.idf.il	ET SCAN NMAP -sS window 4096	1
14.152.59.11	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
124.232.156.78	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	1
103.208.244.223	147.237.76.38		e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
103.208.244.223	147.237.0.34		tikshuv.idf.il	ET SCAN Potential SSH Scan	1
103.208.244.223	147.237.0.16		my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
54.144.119.103	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1

10-01-2016-07:04:01 to 10-01-2016-08:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.182.105.109	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
79.182.38.253	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
155.254.215.85	Bahrain	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
106.38.241.106	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	7
185.110.108.165	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
66.102.9.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.102.9.149	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
31.13.113.87	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.180.210.188	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.13.113.80	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
157.55.39.196	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.104	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.183.76.4	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.106.47.35	Palestinian Territory Occupied	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
109.253.206.235	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.106.47.35	Palestinian Territory Occupied	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
31.13.113.77	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
69.170.45.138	United States	147.237.76.176	test.ncore.idf.il	drop	First packet isn't SYN	drop	2
141.226.217.65	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
141.0.12.47	Norway	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
31.13.113.84	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
89.204.137.4	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
216.218.206.116	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
77.37.221.60	Russian Federation	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
46.121.76.37	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
115.87.232.221	Thailand	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
93.158.200.68	Netherlands	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
79.182.105.109	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1
185.3.147.214	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
106.38.241.106	China	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	1
92.255.232.87	Russian Federation	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
218.22.211.69	China	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
77.37.221.60	Russian Federation	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
184.105.139.90	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
49.34.147.15	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
139.162.37.147	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
31.13.113.79	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
93.158.200.68	Netherlands	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
74.82.47.16	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.86.104	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
92.255.232.87	Russian Federation	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
184.105.139.116	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
54.144.119.103	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
93.158.200.68	Netherlands	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
79.182.105.109	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
195.62.53.168	Russian Federation	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
74.82.47.41	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
92.255.232.87	Russian Federation	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

10-01-2016-07:04:01 to 10-01-2016-08:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.245.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.182.38.253	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
36.88.60.160	Indonesia	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-en/dover.aspx	Block	3
36.88.60.160	Indonesia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	2
157.55.39.244	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/robots.txt	Block	1
66.249.65.52	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew	Block	1
79.177.220.49	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/about.aspx	Block	1
46.4.74.42	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
66.249.66.105	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
66.249.64.56	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
66.249.76.59	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/default.asp	Block	1
92.255.232.87	Russian Federation	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to /	Block	1
66.249.65.8	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchildsubcategories/1423	Block	1
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
92.255.232.87	Russian Federation	147.237.76.86	navy.idf.il	Unauthorized Method HEAD for /	Block	1
66.249.65.52	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.52	Block	1
68.180.231.60	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1956-he/cogat.aspx	Block	1

10-01-2016-07:04:01 to 10-01-2016-08:04:01