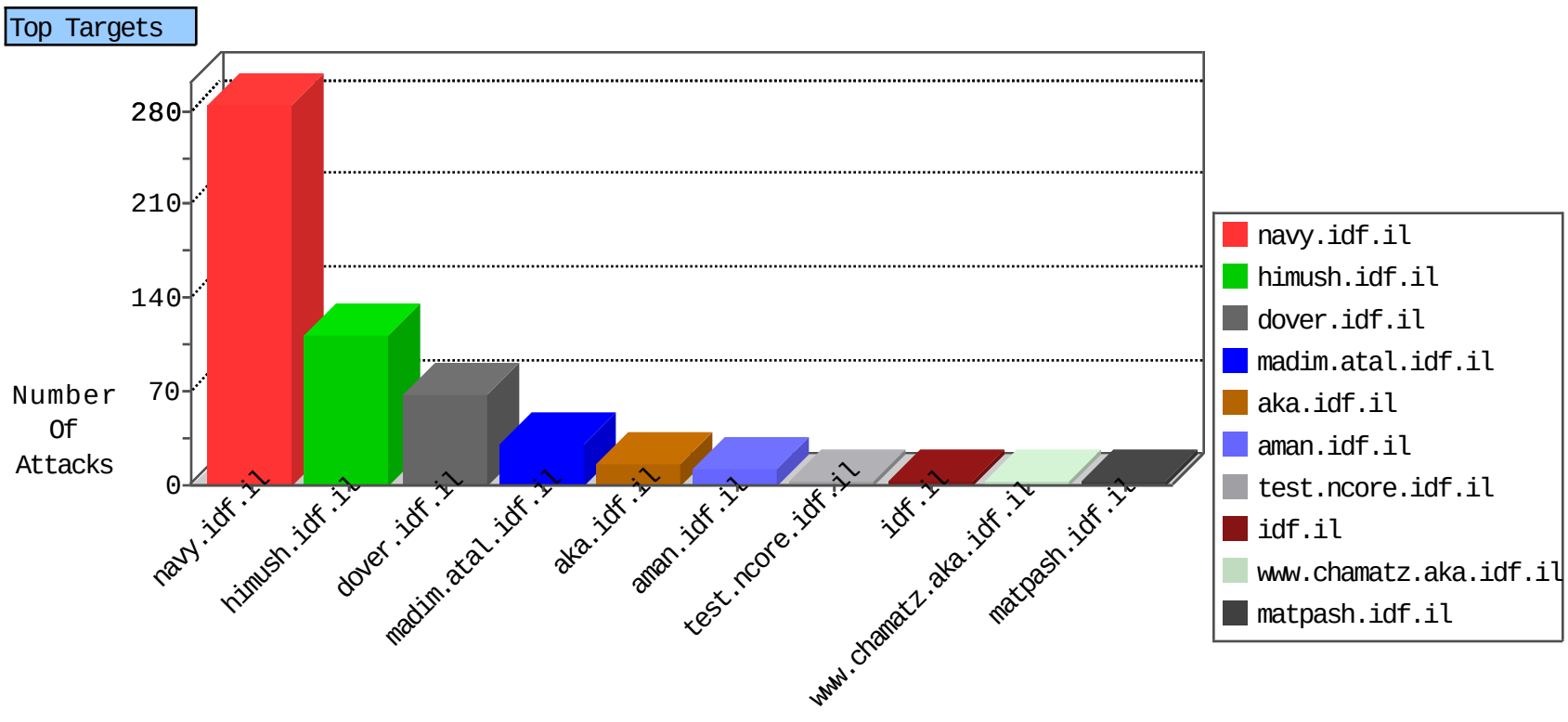
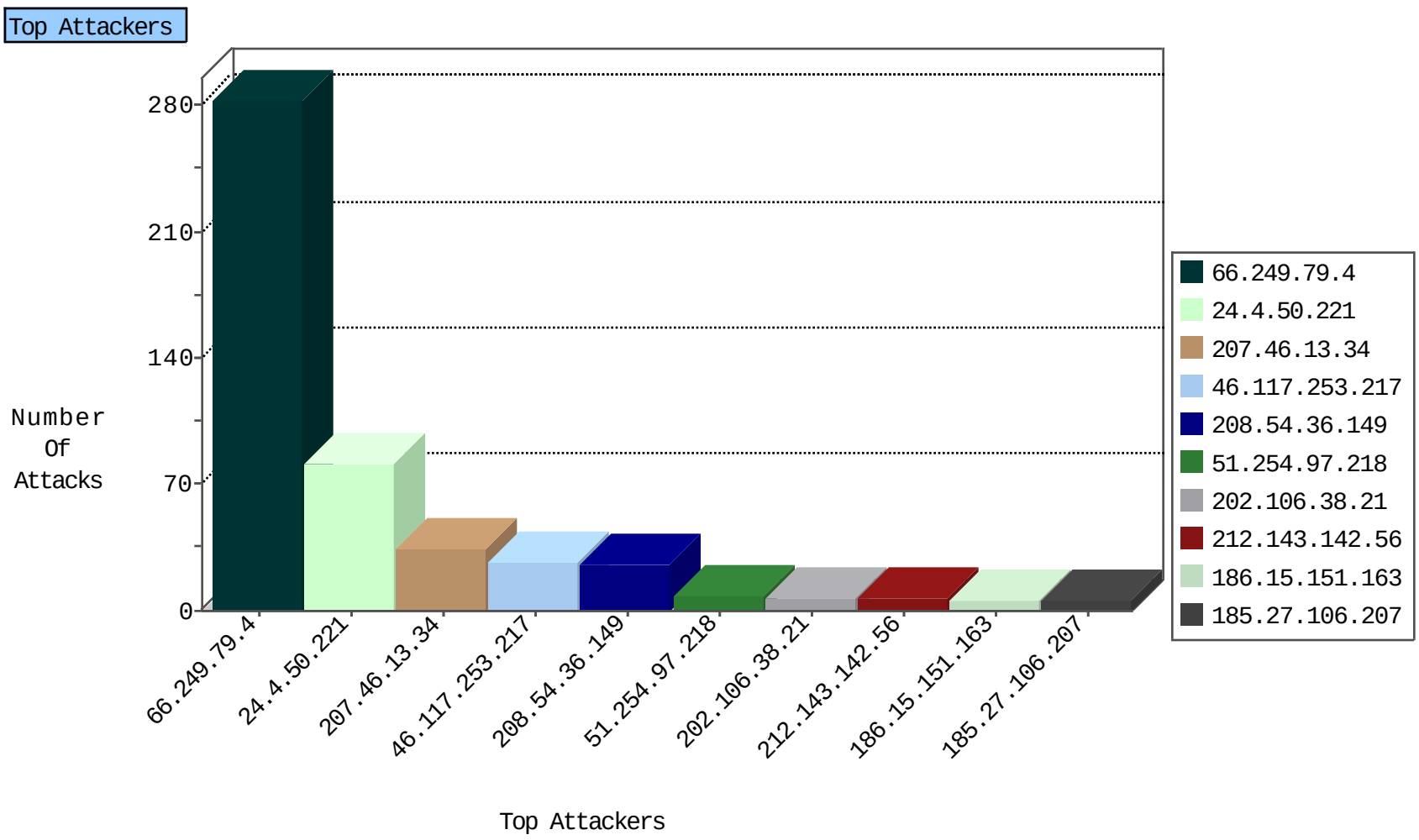
10-03-2016-03:04:08 to 10-03-2016-04:04:08

IDF Under Attack
Daily Report





10-03-2016-03:04:08 to 10-03-2016-04:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.184.40.86	United States	147.237.76.148	gqcenter.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
218.95.228.109	China	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

10-03-2016-03:04:08 to 10-03-2016-04:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
51.254.97.218	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	8
178.151.143.163	Ukraine	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
5.29.217.24	Israel	147.237.72.156	aman.idf.il	32390: HTTP: Suspicious User-Agent (Mozilla)	Block	2
69.30.213.202	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

10-03-2016-03:04:08 to 10-03-2016-04:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.79.4	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	283
46.120.122.219	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	2
27.72.57.38	147.237.77.216	Vietnam	dover.idf.il	Xenu Link Sleuth User Agent	2
120.33.120.83	147.237.77.74	China	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
66.249.66.103	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	1
46.172.91.21	147.237.76.199	Ukraine	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
2.50.129.147	147.237.76.147	United Arab Emirates	chinuch.aka.idf.il	ET SCAN NMAP -sS window 4096	1
185.40.4.208	147.237.76.30	Russian Federation	himush.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.64.99	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
46.172.91.21	147.237.76.176	Ukraine	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
208.100.26.228	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1

10-03-2016-03:04:08 to 10-03-2016-04:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
207.46.13.34	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
24.4.50.221	United States	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	17
24.4.50.221	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
24.4.50.221	United States	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	16
24.4.50.221	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	16
24.4.50.221	United States	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
208.54.36.149	United States	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	6
208.54.36.149	United States	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	5
208.54.36.149	United States	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
208.54.36.149	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
208.54.36.149	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
186.15.151.163	Costa Rica	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
202.106.38.21	China	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
185.27.106.207	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
202.106.38.21	China	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
92.98.103.150	United Arab Emirates	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
217.132.146.23	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
85.64.12.87	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
62.138.2.243	Germany	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
184.105.247.204	United States	147.237.0.33	idf.il	drop		drop	1
138.246.253.19	Germany	147.237.77.61	e.cogat.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
89.248.174.4	Netherlands	147.237.0.33	idf.il	drop		drop	1
188.32.132.38	Russian Federation	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
141.212.122.110	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
107.173.95.136	United States	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	1
216.218.206.114	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
66.191.166.230	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
202.226.145.18	Japan	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
184.105.247.232	United States	147.237.0.35	akaws.idf.il	drop		drop	1
141.212.122.21	United States	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
89.248.174.4	Netherlands	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
195.62.53.168	Russian Federation	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
141.212.122.111	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
107.173.95.136	United States	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	1
216.218.206.118	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
85.64.9.165	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.22	United States	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
37.26.149.181	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
195.62.53.168	Russian Federation	147.237.0.33	idf.il	drop		drop	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
109.67.104.115	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.105	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
107.173.95.136	United States	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.189	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
109.201.154.143	Netherlands	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
88.79.237.112	Germany	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
188.32.132.38	Russian Federation	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.106	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

10-03-2016-03:04:08 to 10-03-2016-04:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.117.253.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	27
185.27.106.207	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
203.66.168.203	Taiwan	147.237.76.31	nakchal.idf.il	PHP Attempt	Block	1
66.249.66.146	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/robots.txt	Block	1
40.77.167.46	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/robots.txt	Block	1
203.66.168.203	Taiwan	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/wp-login.php	Block	1
68.180.229.184	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/robots.txt	Block	1
186.15.151.163	Costa Rica	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 186.15.151.163 (Open Mode)	None	1
204.79.180.236	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/miluim/templates/inner.asp	Block	1
71.181.80.194	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	1
186.15.151.163	Costa Rica	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.102.6.4	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/sachar	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
190.51.24.142	Argentina	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
66.249.65.52	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1

10-03-2016-03:04:08 to 10-03-2016-04:04:08