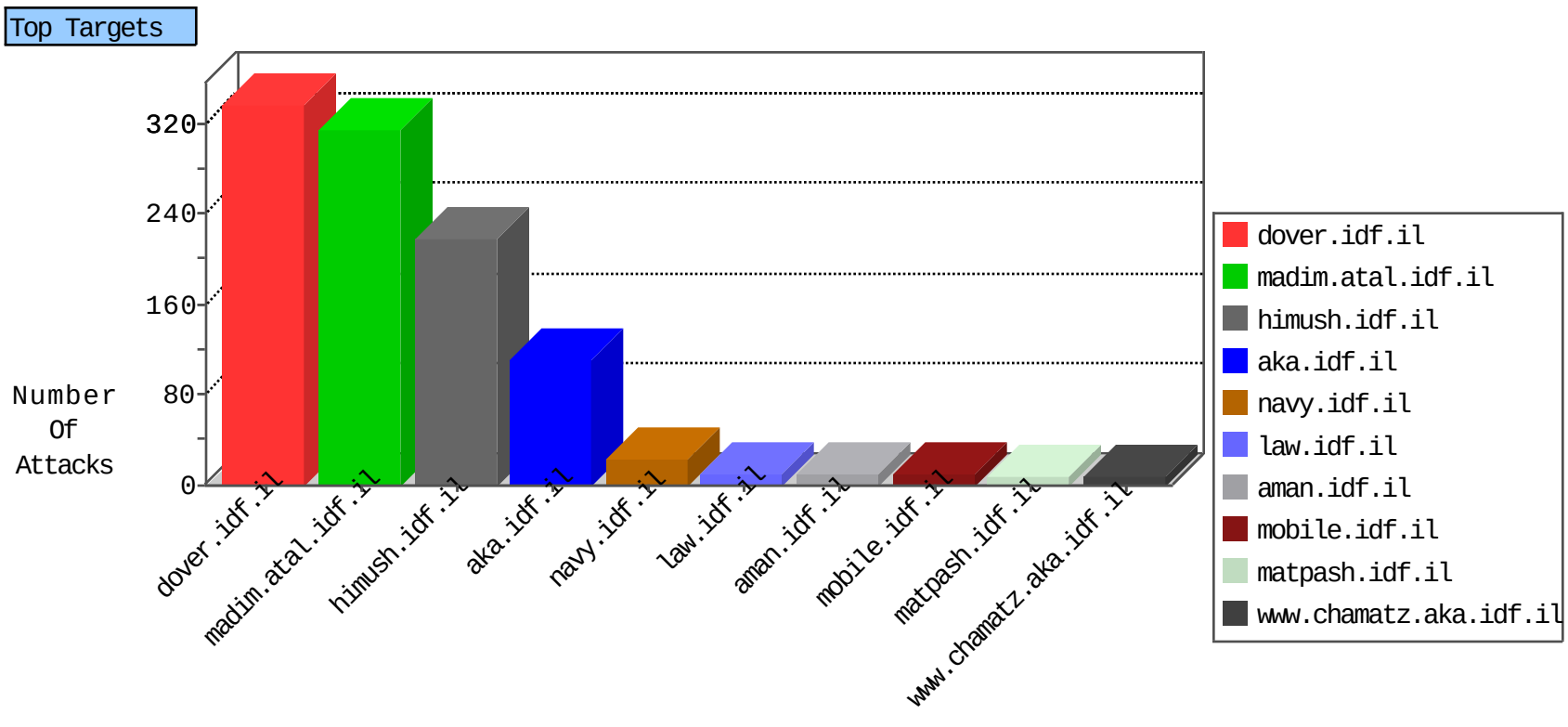
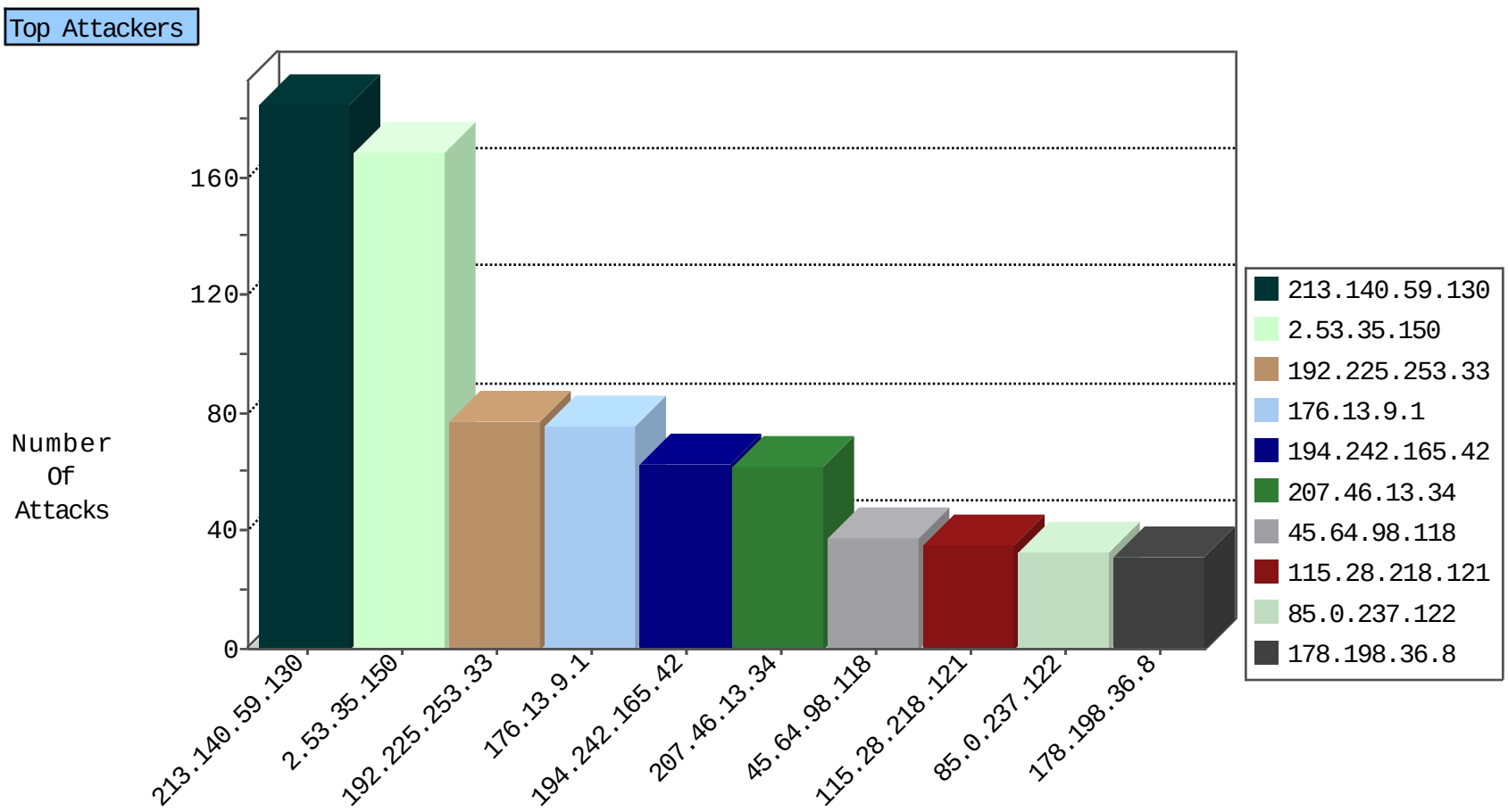
10-03-2016-12:04:00 to 10-03-2016-13:04:00

IDF Under Attack Daily Report



Top Target



Top Attackers

10-03-2016-12:04:00 to 10-03-2016-13:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
209.126.136.2	United States	147.237.76.199	e.nakchal.idf.il	Black List	drop	1
89.248.174.4	Netherlands	147.237.76.201	e.atal.idf.il	Black List	drop	1
94.177.164.99	Romania	147.237.76.176	test.ncore.idf.il	Black List	drop	1

10-03-2016-12:04:00 to 10-03-2016-13:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
199.58.86.211	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3
144.76.4.148	Germany	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	2

10-03-2016-12:04:00 to 10-03-2016-13:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
91.121.184.8	147.237.72.166	France	aka.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	4
220.121.93.217	147.237.76.177	Korea, Republic of	ncore.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
24.37.68.226	147.237.77.227	Canada	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
14.152.59.11	147.237.76.199	China	e.nakchal.idf.i	ET SCAN NMAP -sS window 1024	1
212.34.20.97	147.237.77.216	Jordan	dover.idf.il	portscan: TCP Distributed Portscan	1
99.196.46.95	147.237.8.14	United States	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
24.37.68.226	147.237.77.179	Canada	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
106.187.45.144	147.237.8.14	Japan	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.194	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1

10-03-2016-12:04:00 to 10-03-2016-13:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
213.140.59.130	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	81
192.225.253.33	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	77
207.46.13.34	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	62
213.140.59.130	Algeria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	47
213.140.59.130	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
213.140.59.130	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	19
213.140.59.130	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	19
79.178.129.68	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
45.64.98.118	Indonesia	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
115.28.218.121	China	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
66.249.93.83	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
45.64.98.118	Indonesia	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	9
176.13.228.61	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
115.28.218.121	China	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	9
115.28.218.121	China	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	8
45.64.98.118	Indonesia	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	8
85.0.237.122	Switzerland	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
85.0.237.122	Switzerland	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	7
178.198.36.8	Switzerland	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
85.0.237.122	Switzerland	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	7
141.226.162.119	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
178.198.36.8	Switzerland	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	6
45.64.98.118	Indonesia	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.85.136	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.179.128.184	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
79.178.129.68	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.85.136	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
178.198.36.8	Switzerland	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
85.0.237.122	Switzerland	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	6
79.178.129.68	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
178.198.36.8	Switzerland	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	5
85.0.237.122	Switzerland	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
178.198.36.8	Switzerland	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
115.28.218.121	China	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
106.51.117.216	India	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.231	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
185.110.108.165	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.55	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.55	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
45.64.98.118	Indonesia	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
2.53.63.228	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.86.146	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
66.249.65.12	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.106.21	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
115.28.218.121	China	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
109.253.192.111	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.123	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.176.12.26	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.94	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

10-03-2016-12:04:00 to 10-03-2016-13:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.35.150	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	169
194.242.165.42	France	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	63
176.13.9.1	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	45
46.117.128.137	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.117.128.137	Block	24
46.117.30.117	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 46.117.30.117	Block	4
46.117.30.117	Israel	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	3
37.46.41.131	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 37.46.41.131	Block	2
77.138.126.252	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	2
37.142.71.189	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
84.111.171.47	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
66.249.73.133	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
37.46.41.131	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
79.178.22.235	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
84.111.171.47	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-login.php	Block	1
77.138.89.114	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	Block	1
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
46.117.128.137	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
2.53.130.46	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
110.78.146.118	Thailand	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
84.108.214.219	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 84.108.214.219	Block	1
46.120.5.130	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mofet	Block	1
31.28.244.146	Ukraine	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
157.55.39.195	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/...	Block	1
77.139.93.177	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
84.108.214.219	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/giyus/main/	Block	1
66.249.66.146	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	1
37.26.147.166	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
157.55.39.196	United States	147.237.72.166	aka.idf.il	Unknown Parameter KEY in aka.idf.il/ishurim/cityofficers/	None	1
79.178.13.18	Israel	147.237.77.234	halag.idf.il	Parameter Type Violation SearchText in www.logistics.atal.idf.il/938-he/halag.aspx	Block	1

10-03-2016-12:04:00 to 10-03-2016-13:04:00