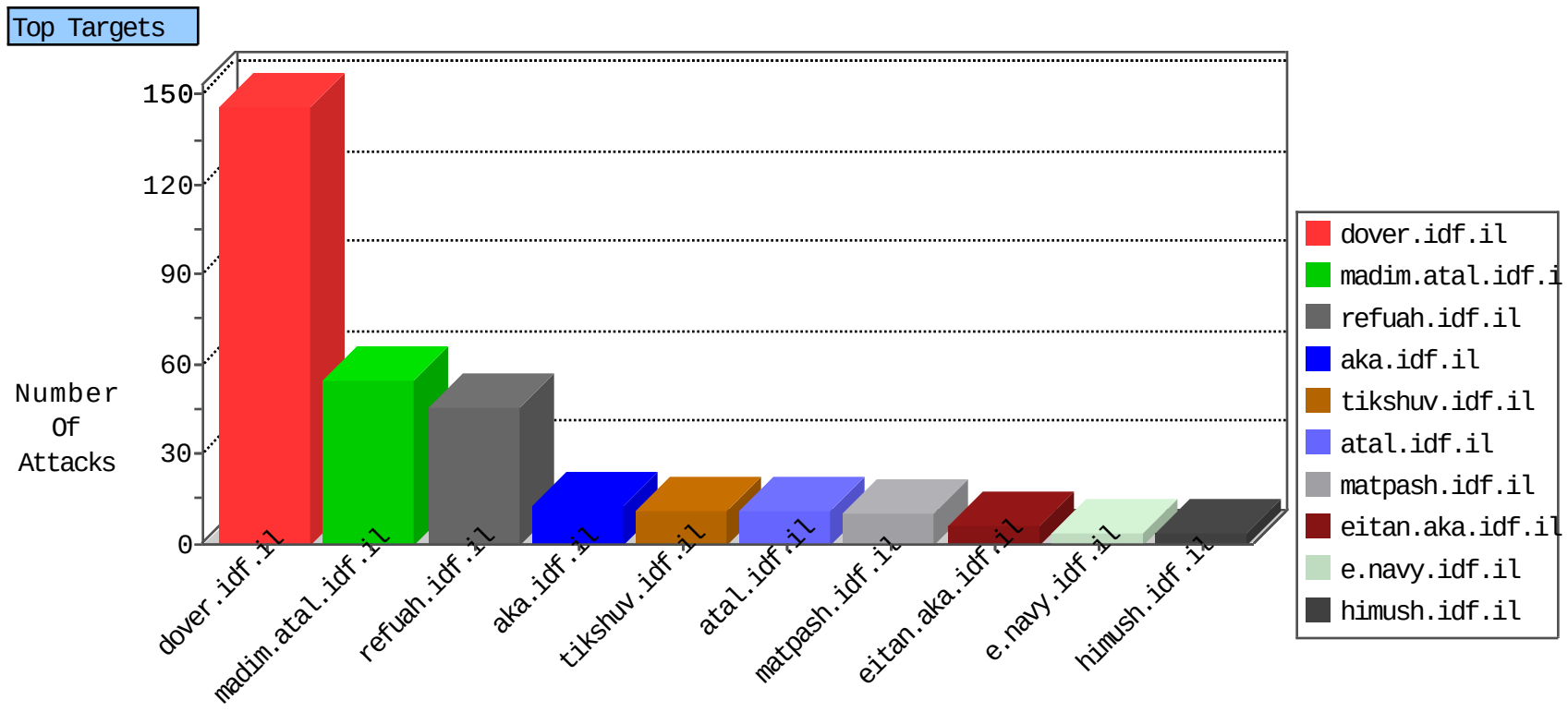
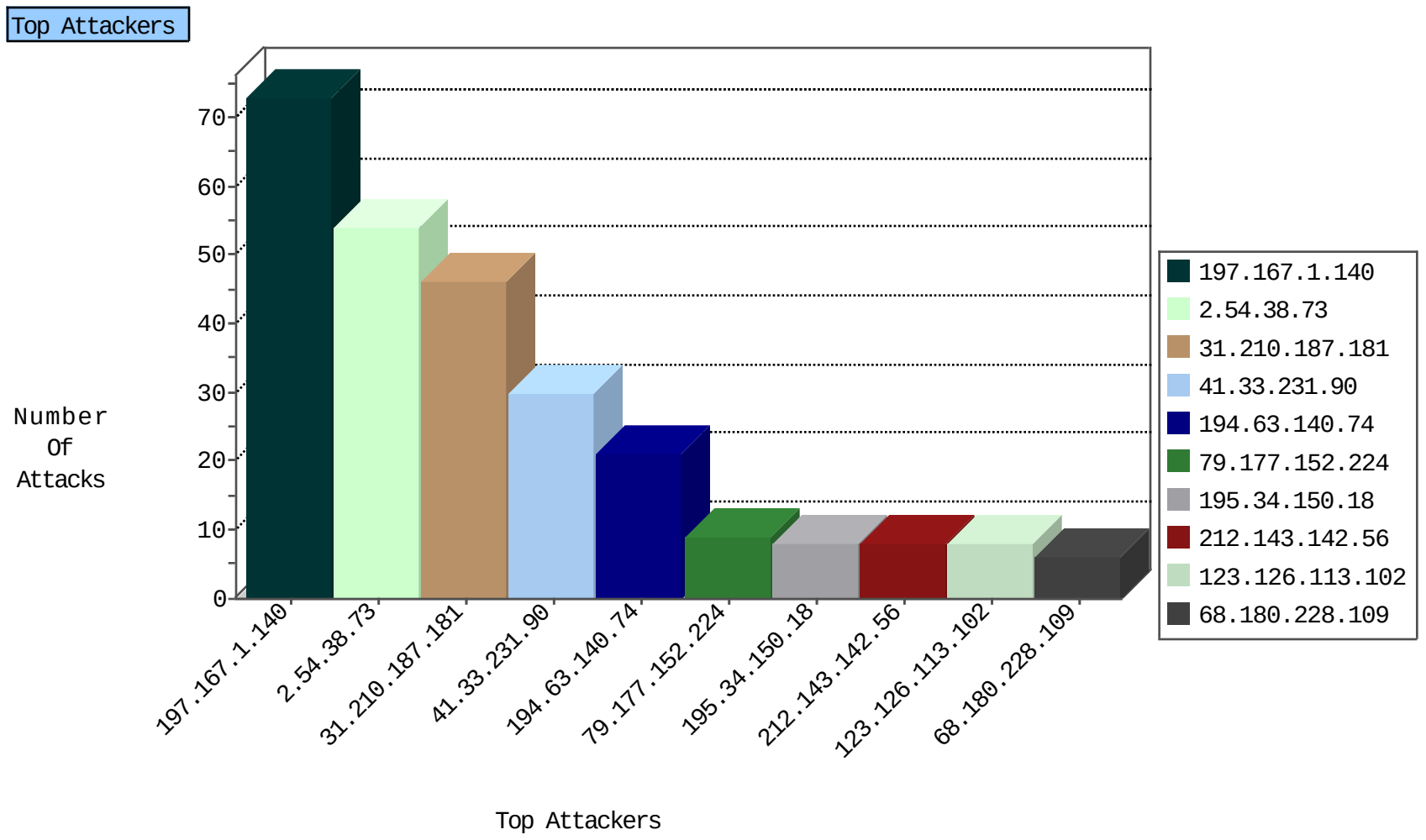
02-27-2016-02:04:00 to 02-27-2016-03:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-27-2016-02:04:00 to 02-27-2016-03:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
197.167.1.140	Egypt	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	28
197.167.1.140	Egypt	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	27
217.26.171.188	Moldova, Republic of	147.237.77.176	matpash.idf.il	L4 Source or Dest Port Zero	drop	3
134.147.203.115	Germany	147.237.77.121	e.navy.idf.il	Block_Ntp_All_Net	drop	2
185.94.111.1		147.237.0.19	madim.atal.idf.il	Block_Udp_All_Nets	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1

02-27-2016-02:04:00 to 02-27-2016-03:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.102	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
84.228.197.36	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
157.55.39.92	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

02-27-2016-02:04:00 to 02-27-2016-03:04:00

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
194.63.140.74	147.237.0.35	Russian Federation	akaws.idf.il	ET SCAN Potential SSH Scan	2
194.63.140.74	147.237.76.196	Russian Federation	e.sviva.idf.il	ET SCAN Potential SSH Scan	2
37.26.149.185	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
194.63.140.74	147.237.72.166	Russian Federation	aka.idf.il	ET SCAN Potential SSH Scan	2
194.63.140.74	147.237.76.197	Russian Federation	e.himush.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.193	147.237.8.14	Netherlands	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
194.63.140.74	147.237.76.177	Russian Federation	ncore.idf.il	ET SCAN Potential SSH Scan	1
62.210.69.71	147.237.77.19	France	law-forum.idf.il	ET SCAN Potential SSH Scan	1
194.63.140.74	147.237.76.86	Russian Federation	navy.idf.il	ET SCAN Potential SSH Scan	1
194.63.140.74	147.237.76.30	Russian Federation	himush.idf.il	ET SCAN Potential SSH Scan	1
194.63.140.74	147.237.72.167	Russian Federation	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
194.63.140.74	147.237.72.14	Russian Federation	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
194.63.140.74	147.237.77.61	Russian Federation	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
179.211.41.208	147.237.76.30	Brazil	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
194.63.140.74	147.237.76.199	Russian Federation	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
104.255.65.207	147.237.77.233		atal.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.114	147.237.0.34	Ukraine	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
194.63.140.74	147.237.76.147	Russian Federation	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
194.63.140.74	147.237.76.38	Russian Federation	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
194.63.140.74	147.237.72.217	Russian Federation	e.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.76.44	China	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
194.63.140.74	147.237.8.45	Russian Federation	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
194.63.140.74	147.237.77.121	Russian Federation	e.navy.idf.il	ET SCAN Potential SSH Scan	1
194.63.140.74	147.237.0.33	Russian Federation	idf.il	ET SCAN Potential SSH Scan	1
194.63.140.74	147.237.76.201	Russian Federation	e.atal.idf.il	ET SCAN Potential SSH Scan	1
144.76.224.3	147.237.8.28	Germany	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1

02-27-2016-02:04:00 to 02-27-2016-03:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
31.210.187.181	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	44
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
79.177.152.224	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
197.167.1.140	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
109.253.138.114	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
68.180.228.109	United States	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	6
58.10.175.60	Thailand	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
197.167.1.140	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
197.167.1.140	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
77.127.165.114	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
123.126.113.102	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
197.167.1.140	Egypt	147.237.77.216	dover.idf.il	SYN Attack		reject	2
195.62.53.168	Russian Federation	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
31.210.187.181	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.82.200.91		147.237.0.200	m4u.idf.il	drop		drop	1
195.62.53.168	Russian Federation	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
112.134.33.255	Sri Lanka	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
203.127.96.218	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
185.82.200.91		147.237.76.39	mobile.meitav.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
50.28.99.117	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
203.127.96.218	Singapore	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
188.138.1.218	Germany	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
87.69.112.80	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
182.50.130.133	Singapore	147.237.77.216	dover.idf.il	drop	SAM rule	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
185.3.146.198	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

02-27-2016-02:04:00 to 02-27-2016-03:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.38.73	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	54
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	3
73.22.155.10	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/	Block	2
157.55.39.37	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
50.62.161.156	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/test/wp-admin/	Block	1
75.119.220.105	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/wordpress/wp-admin/	Block	1
38.111.147.88	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
176.9.61.55	Germany	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/old/wp-admin/	Block	1
62.210.131.104	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
79.177.152.224	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
179.7.69.67	Peru	147.237.72.167	ishurim.aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
64.13.232.32	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/wp/wp-admin/	Block	1
109.186.27.25	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
185.82.200.91		147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1043-ar/cogat.aspx	Block	1
119.81.196.37	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/wp-admin/	Block	1
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
195.154.108.146	France	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/blog/wp-admin/	Block	1
31.210.187.181	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery/jquery.nyromodal-1.6.2.js	Block	1

02-27-2016-02:04:00 to 02-27-2016-03:04:00