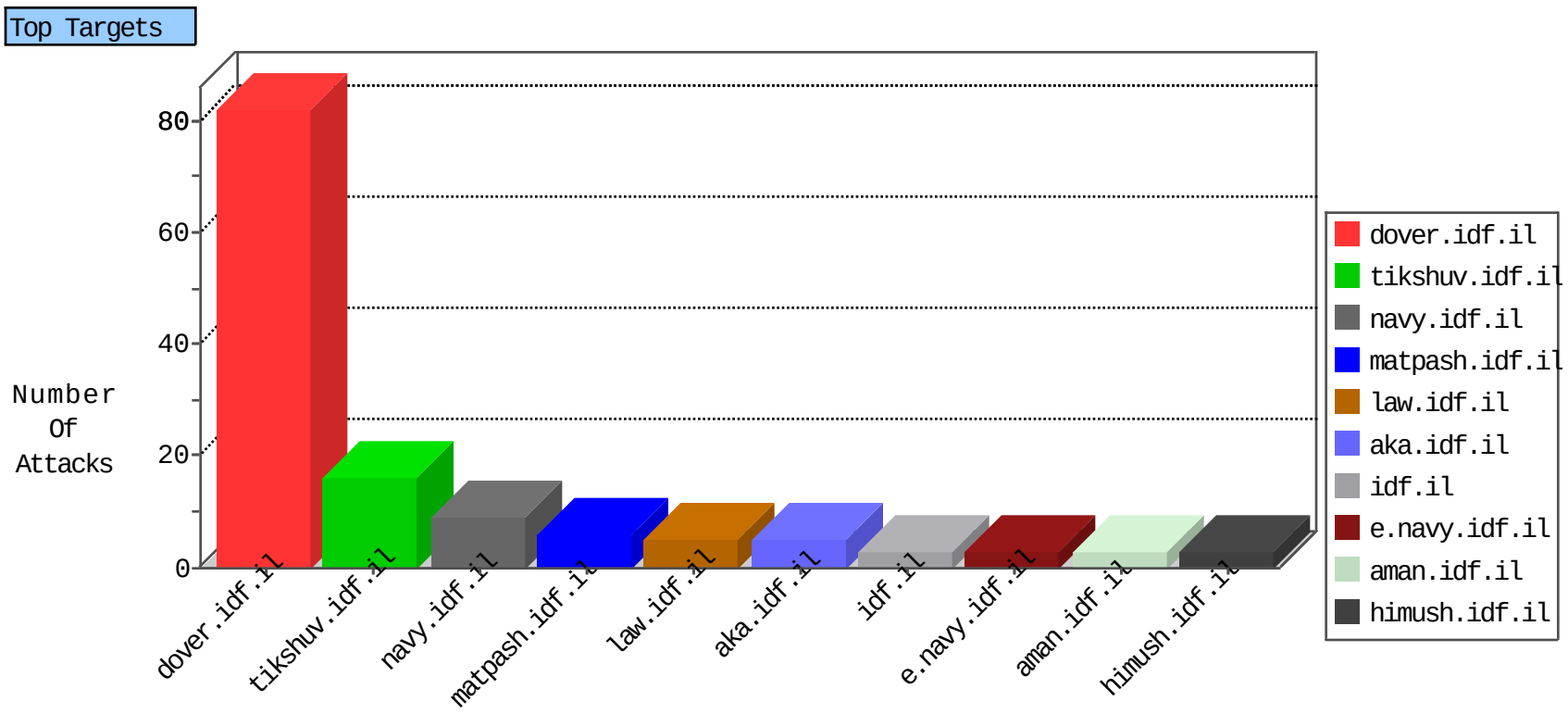
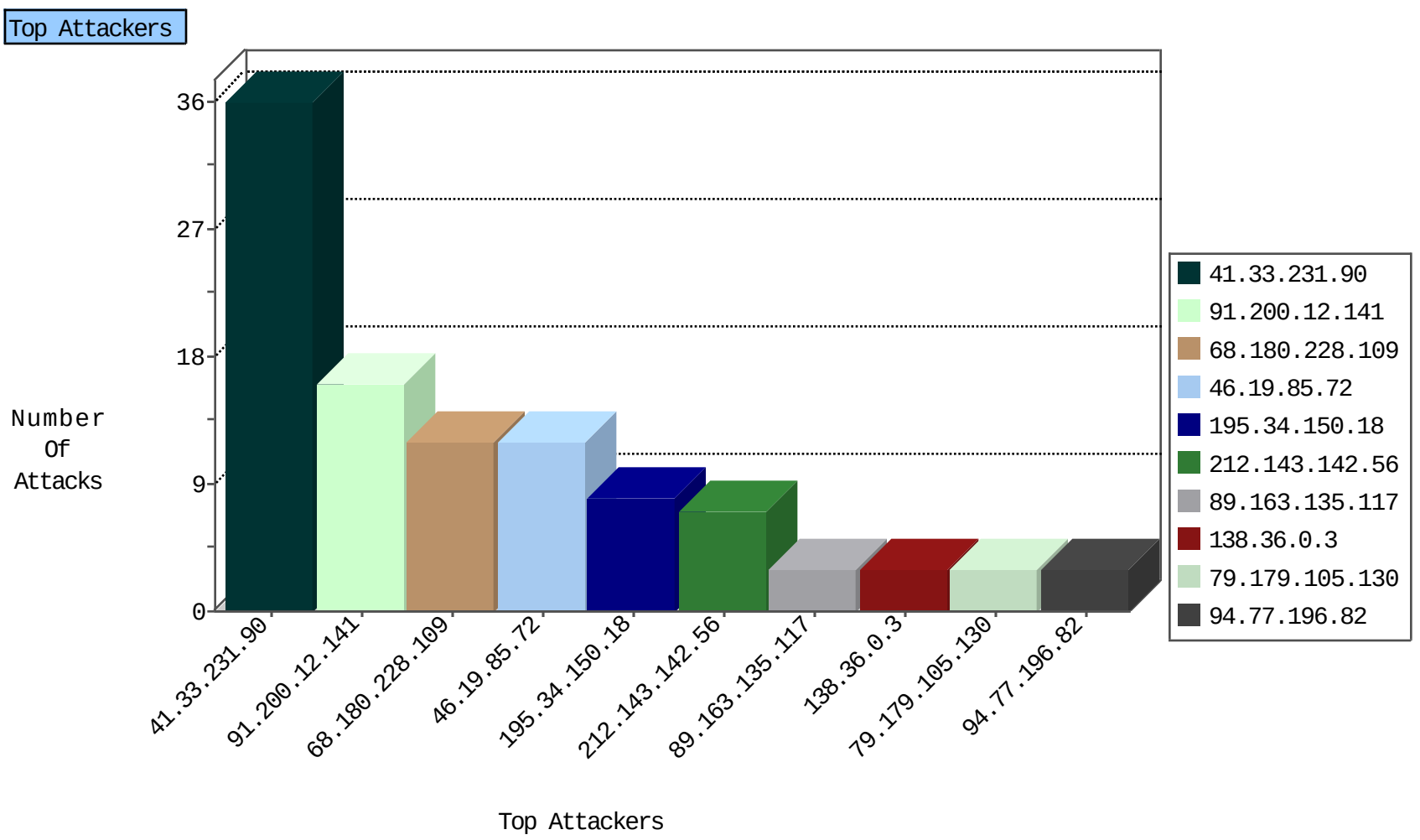
02-27-2016-04:04:03 to 02-27-2016-05:04:03

IDF Under Attack Daily Report





02-27-2016-04:04:03 to 02-27-2016-05:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
125.75.206.153	China	147.237.0.33	idf.il	Invalid TCP Flags	drop	2
89.163.135.117	Germany	147.237.0.15	kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
198.20.70.114	United States	147.237.77.179	e.mazi.idf.il	Block_Ntp_All_Net	drop	1
89.163.135.117	Germany	147.237.0.16	my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
89.163.135.117	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
71.6.165.200	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1

02-27-2016-04:04:03 to 02-27-2016-05:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-27-2016-04:04:03 to 02-27-2016-05:04:03

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
210.115.184.234	147.237.76.86	Korea, Republic of	navy.idf.il	ET SCAN NMAP -sA (2)	2
167.0.233.47	147.237.76.30	Colombia	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
146.185.250.2	147.237.76.30	Russian Federation	himush.idf.il	ET SCAN NMAP -sS window 1024	1
112.124.10.141	147.237.77.178	China	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.193	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
50.204.188.142	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
146.185.250.2	147.237.76.30	Russian Federation	himush.idf.il	ET SCAN Potential SSH Scan	1
118.70.80.152	147.237.0.15	Vietnam	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1
94.102.48.193	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
50.204.188.142	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 3072	1

02-27-2016-04:04:03 to 02-27-2016-05:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
68.180.228.109	United States	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	12
91.200.12.141	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
91.200.12.141	Ukraine	147.237.77.74	law.idf.il	drop	SAM rule	drop	4
46.19.85.72	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.72	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
91.200.12.141	Ukraine	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	4
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
79.179.105.130	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.72	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.72	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
74.82.47.11	United States	147.237.0.33	idf.il	drop		drop	1
216.218.206.112	United States	147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.124	United States	147.237.8.46	e.chinuch.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
114.112.90.54	China	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	1
88.200.214.8	Russian Federation	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
207.46.13.94	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.139.74	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.15	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.124	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.126	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
123.125.71.82	China	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1
88.200.214.8	Russian Federation	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.86	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.44	United States	147.237.8.27	e.madim.atal.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1
5.39.93.143	France	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
184.105.247.204	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
123.125.71.82	China	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
89.138.59.16	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
216.218.206.102	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.86	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
109.201.152.226	Netherlands	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
75.126.221.55	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
138.36.0.3		147.237.76.196	e.sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.112	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.111	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
114.112.90.54	China	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
195.62.53.168	Russian Federation	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
138.36.0.3		147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

02-27-2016-04:04:03 to 02-27-2016-05:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	2
41.47.17.249	Egypt	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	2
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1158-he/dover.aspx	Block	1
116.253.140.224	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/admin/login.asp	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/arabic/pages/default.aspx	Block	1
172.58.25.166	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
84.109.203.110	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	1
203.133.171.71	Korea, Republic of	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/modiin/default.aspx	Block	1
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	1
109.201.152.226	Netherlands	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
207.46.13.105	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
116.253.140.224	China	147.237.77.176	matpash.idf.il	Admin Blocking	Block	1

02-27-2016-04:04:03 to 02-27-2016-05:04:03