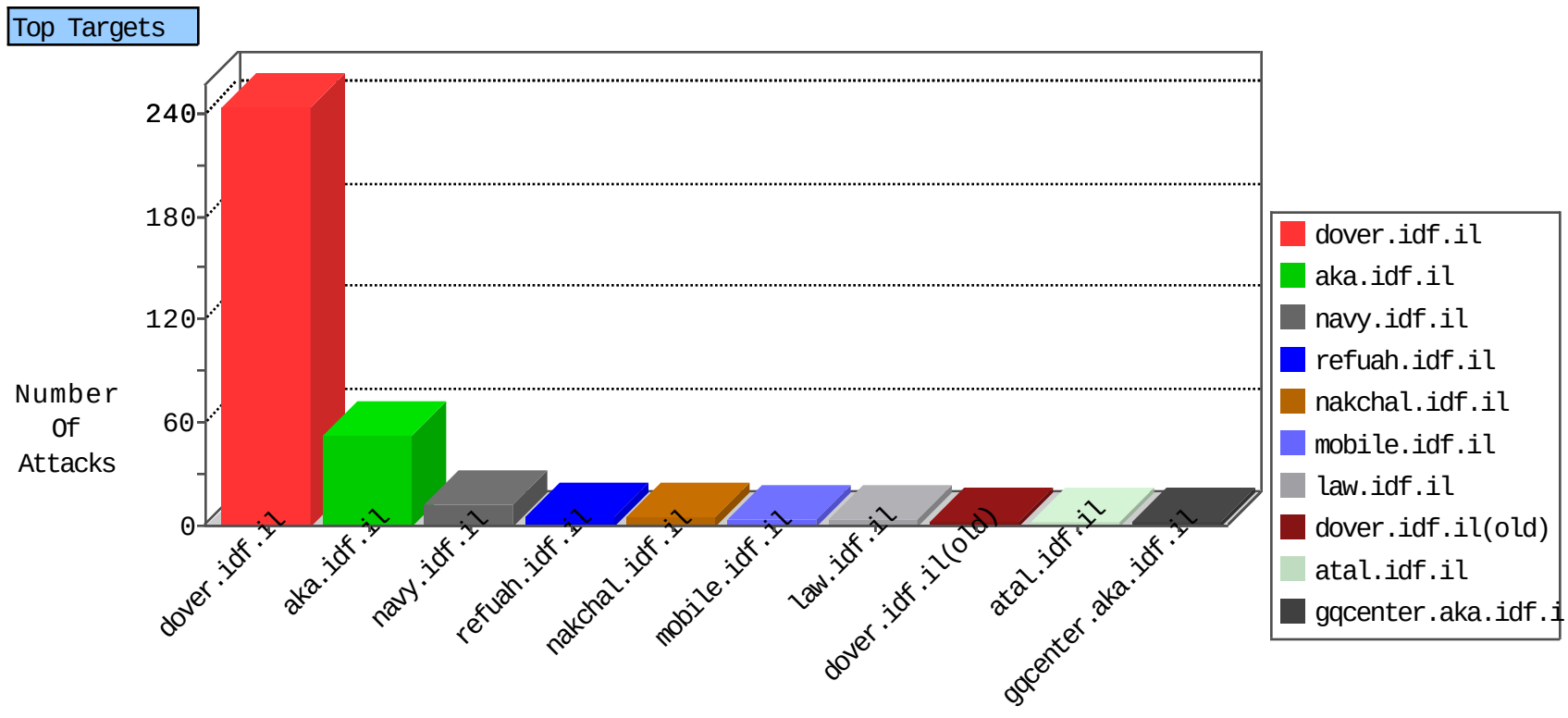
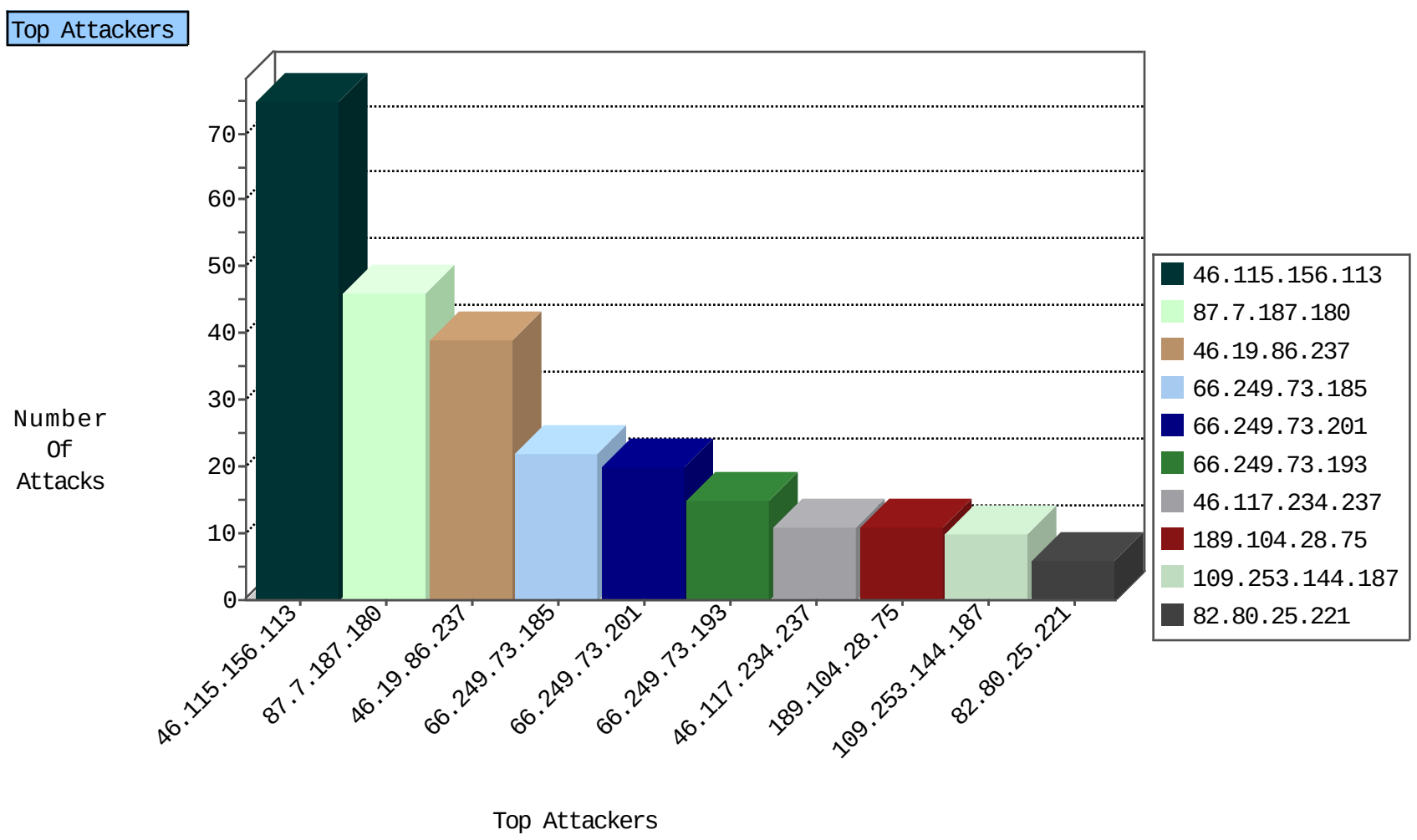
03-28-2015-02:03:00 to 03-28-2015-03:03:00

IDF Under Attack
03-28-2015-02:03:00

Top Targets



Top Attackers



03-28-2015-02:03:00 to 03-28-2015-03:03:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count

03-28-2015-02:03:00 to 03-28-2015-03:03:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
189.104.28.75	Brazil	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
77.127.132.2	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
206.207.225.86	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.43.94	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
85.250.189.52	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
46.19.85.36	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
46.117.69.46	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
200.98.146.202	Brazil	147.237.77.216	dover.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1

03-28-2015-02:03:00 to 03-28-2015-03:03:00

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
193.107.17.72	Russian Federation	147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 1024	1
183.136.216.7	China	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
115.231.218.147	China	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
5.150.198.62	Sweden	147.237.0.19	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
196.47.173.21	Cote D'Ivoire	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 2048	1
183.136.216.7	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
183.136.216.7	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
115.231.218.147	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
81.214.124.139	Turkey	147.237.77.233	atal.idf.il	ET DOS SSL Bomb DoS Attempt	1
5.196.248.85	Germany	147.237.76.148	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.77.178	e.matpash.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
196.47.173.21	Cote D'Ivoire	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -f -sS	1

03-28-2015-02:03:00 to 03-28-2015-03:03:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
46.115.156.113	Germany	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	75
87.7.187.180	Italy	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	46
66.249.73.201	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
66.249.73.185	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
66.249.73.193	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
109.253.144.187	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
199.30.24.136	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
46.117.234.237	Israel	147.237.76.86	navy.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
46.117.234.237	Israel	147.237.76.86	navy.idf.il	Invalid ACK number	Bad TCP sequence	alert	5
46.19.85.148	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
5.102.254.212	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
189.104.28.75	Brazil	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
171.4.247.4	Thailand	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	3
189.104.28.75	Brazil	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
109.253.129.240	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
38.106.31.85	United States	147.237.77.74	law.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	1
141.212.122.88	United States	147.237.76.200	eitan.aka.idf.il		drop	drop	1
128.103.64.114	United States	147.237.77.216	dover.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	1
141.212.122.179	United States	147.237.8.27	e.madim.atal.idf.i	Geo-location inbound enforcement	Geo-location enforcement	drop	1
46.19.86.85	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
141.212.122.46	United States	147.237.76.34	yohalan.idf.il		drop	drop	1
109.64.105.247	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.19.86.237	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
141.212.122.82	United States	147.237.77.178	e.matpash.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
5.196.248.85	Germany	147.237.76.148	gqcenter.aka.idf.i		drop	drop	1
46.19.86.237	Israel	147.237.72.166	aka.idf.il	illegal header format detected: Malformed HTTP protocol name in response	Block HTTP Non Compliant	monitor	1
141.212.122.83	United States	147.237.0.35	akaws.idf.il		drop	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.86.237	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	37
79.180.144.62	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 79.180.144.62	Block	3
107.170.42.23	United States	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 107.170.42.23	Block	2
79.177.63.68	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	2
82.102.251.11	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 82.102.251.11	Block	2
207.46.13.79	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 207.46.13.79	Block	2
188.165.15.196	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.196	Block	1
66.249.79.41	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
217.69.133.220	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/zahar	Block	1
128.103.64.114	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arafat/terrorism/english/main_index.stm	Block	1
81.163.101.20	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
66.249.73.193	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.193	Block	1
200.98.146.202	Brazil	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
107.170.42.23	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.65.188	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.188	Block	1
157.55.39.137	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.75.50	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/general/general.aspx	Block	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	1
207.46.13.30	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on navy.idf.il//captcha.ashx	Block	1
112.111.191.19	China	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/564-en/patzar.aspx/trackback/	Block	1
79.177.109.2	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.65.188	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1283-10669-en/dover.aspx	Block	1
171.4.247.4	Thailand	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
85.65.116.79	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/iturim/iturim.aspx	None	1
66.249.75.54	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
37.105.7.151	Saudi Arabia	147.237.77.216	dover.idf.il	Unknown HTTP Request Method COOK in URL www.idf.il/1558-en/dover.aspx	Block	1
123.125.80.244	China	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
66.249.73.185	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.185	Block	1
180.76.4.32	China	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
107.23.45.196	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/modiin/default.aspx	Block	1
66.249.75.117	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
38.106.31.85	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
207.46.13.79	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/kamlar/eurl.axd/73879113e5ed344fa80d3b2b3f38c361/	Block	1
128.103.64.114	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 128.103.64.114	Block	1
79.180.144.62	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
66.249.73.185	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1