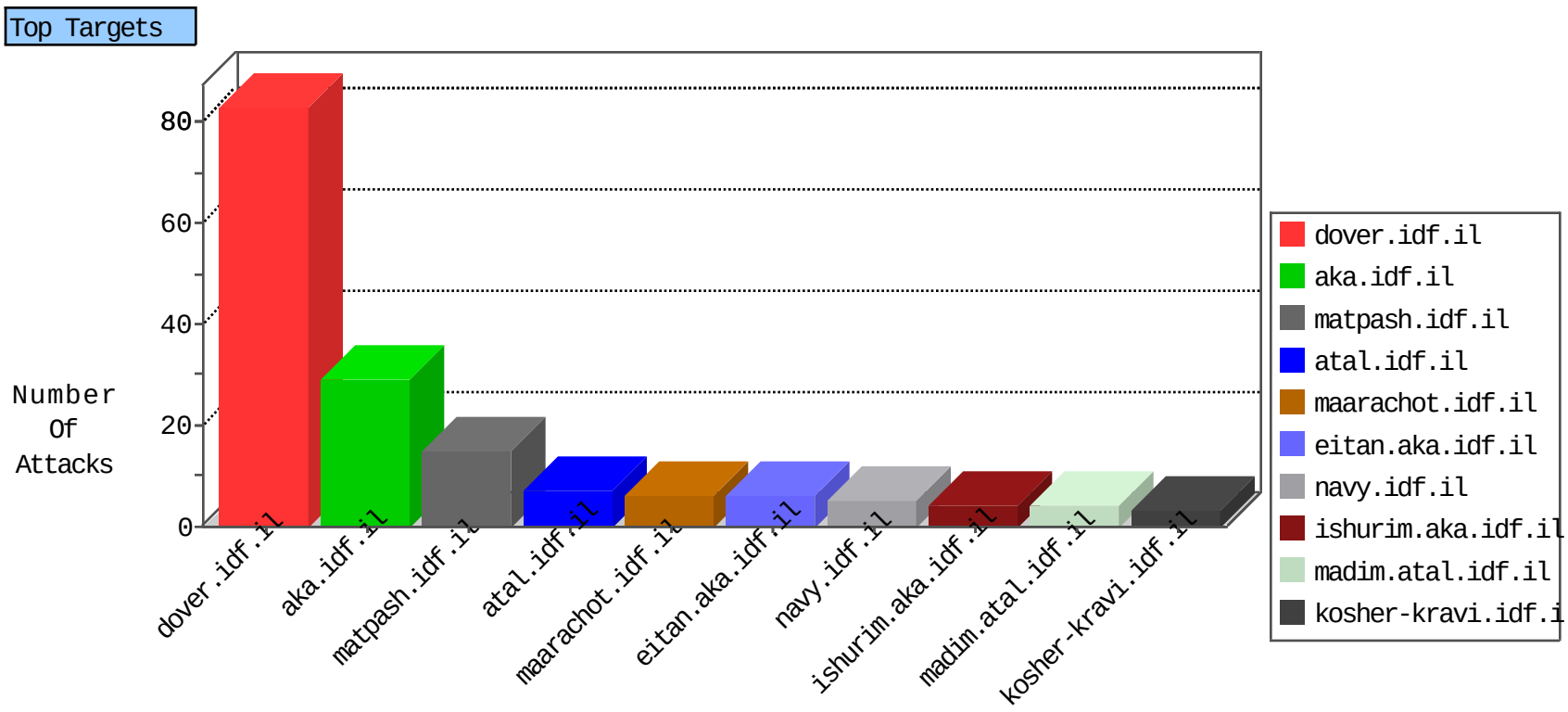
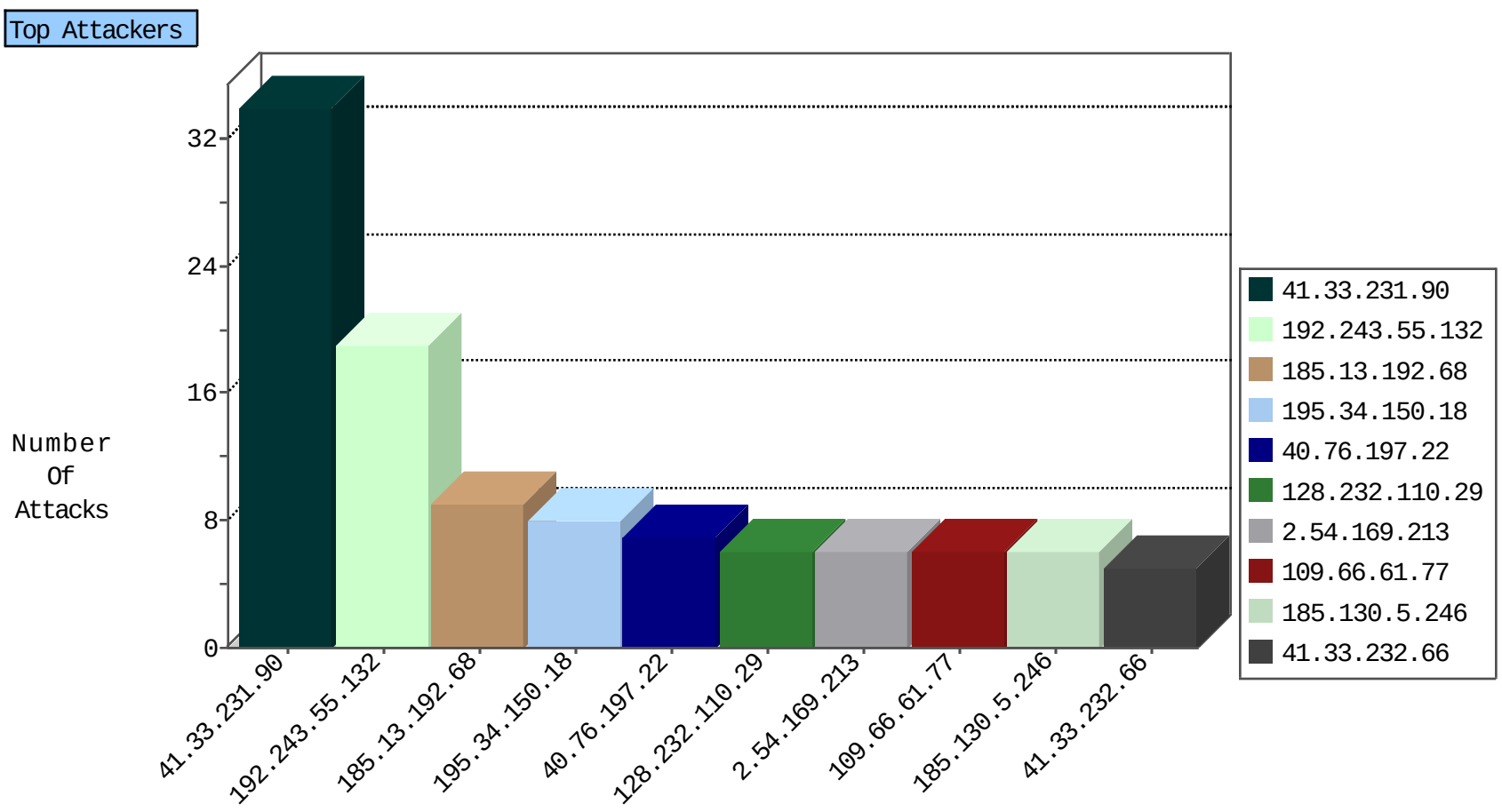
02-18-2016-02:04:05 to 02-18-2016-03:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-18-2016-02:04:05 to 02-18-2016-03:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
217.172.189.11	Germany	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	2
115.239.228.10	China	147.237.0.19	madim.atal.idf.il	Frk_Under_Attack_Con_Http	drop	2
123.151.42.61	China	147.237.76.86	navy.idf.il	Block_Udp_All_Nets_Con_Limit	drop	1
185.130.5.246		147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
146.185.239.100	Russian Federation	147.237.77.205	prisha.idf.il	block-sp-traf1	drop	1
185.130.5.246		147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
115.239.228.10	China	147.237.0.19	madim.atal.idf.il	Frk_Purple_Con_Limit_Http	drop	1
185.130.5.246		147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.246		147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.246		147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.246		147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1

02-18-2016-02:04:05 to 02-18-2016-03:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	4
158.69.214.109	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	2
136.243.103.92	Germany	147.237.72.156	aman.idf.il	C1000106: HTTP: majestic bot	Block	1

02-18-2016-02:04:05 to 02-18-2016-03:04:05

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
190.216.146.151	147.237.0.15	Chile	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
188.64.169.106	147.237.0.35	Russian Federation	akaws.idf.il	ET SCAN Potential SSH Scan	1
188.64.169.106	147.237.0.16	Russian Federation	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
40.76.197.22	147.237.76.201	United States	e.atal.idf.il	ET SCAN Potential SSH Scan	1
40.76.197.22	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
40.76.197.22	147.237.72.14	United States	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
40.76.197.22	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
190.0.226.242	147.237.0.19	Costa Rica	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
188.64.169.106	147.237.0.17	Russian Federation	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
46.151.52.161	147.237.76.39	Ukraine	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
40.76.197.22	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
40.76.197.22	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
40.76.197.22	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
222.186.21.181	147.237.77.216	China	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

02-18-2016-02:04:05 to 02-18-2016-03:04:05

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	34
2.54.169.213	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
109.66.61.77	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.13.192.68	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
192.243.55.132	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
199.30.16.185	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
192.243.55.132	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	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
185.13.192.68	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.126.35		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
138.44.64.30	Australia	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
192.243.55.133	Dominica	147.237.77.170	maarachot.idf.il	Bad TCP sequence		monitor	2
192.243.55.132	Dominica	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
192.243.55.132	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
108.54.167.76	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
192.243.55.132	Dominica	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
50.63.197.108	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
192.243.55.132	Dominica	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
128.232.110.29	United Kingdom	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
87.69.238.94	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
197.38.197.170	Egypt	147.237.77.233	atal.idf.il	drop	SAM rule	drop	1
146.185.239.102	Russian Federation	147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
128.232.110.29	United Kingdom	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
203.127.96.220	Singapore	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
65.55.218.54	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
192.243.55.133	Dominica	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
128.232.110.29	United Kingdom	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
198.20.69.74	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.46.41.208	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
128.232.110.29	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
203.127.96.220	Singapore	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
68.174.243.158	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
131.253.24.153	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
94.230.86.215	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
198.20.69.74	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
128.232.110.29	United Kingdom	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
203.127.96.220	Singapore	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
85.65.106.128	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
195.62.53.168	Russian Federation	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
131.253.36.204	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
128.232.110.29	United Kingdom	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
85.65.106.128	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
195.154.146.225	France	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
203.127.96.220	Singapore	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

02-18-2016-02:04:05 to 02-18-2016-03:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
92.53.112.156	Russian Federation	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 92.53.112.156	Block	3
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.118.155.237	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi/	Block	2
40.77.167.84	United States	147.237.77.243	mobile.idf.il	Suspicious Response Code	Block	1
176.116.188.83	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi'a=0	Block	1
195.154.146.225	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-trackback.php	Block	1
68.180.230.226	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/robots.txt	Block	1
185.13.192.68	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.69.33	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/5/111255.pdf	Block	1
199.30.24.27	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.102.8.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
189.167.94.122	Mexico	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	1
66.249.69.41	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/4/112454.pdf	Block	1
131.253.25.210	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.102.8.238	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
195.154.146.225	France	147.237.77.216	dover.idf.il	Illegal HTTP Version HTTP/	Block	1
66.249.79.28	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
157.55.39.226	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/www.rabanut-downloads.webs.com	Block	1
66.249.66.75	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
195.154.146.225	France	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
66.249.79.31	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1

02-18-2016-02:04:05 to 02-18-2016-03:04:05