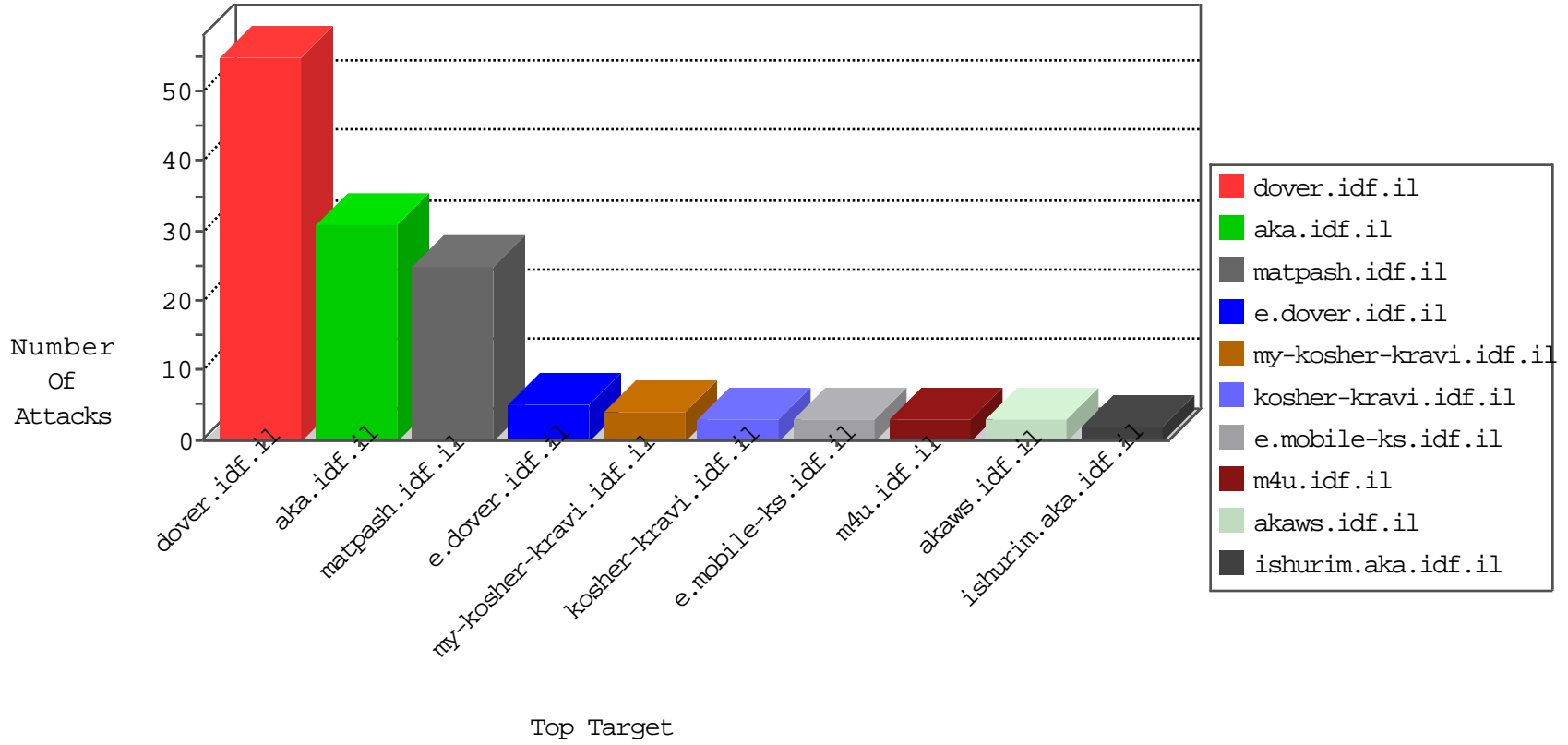


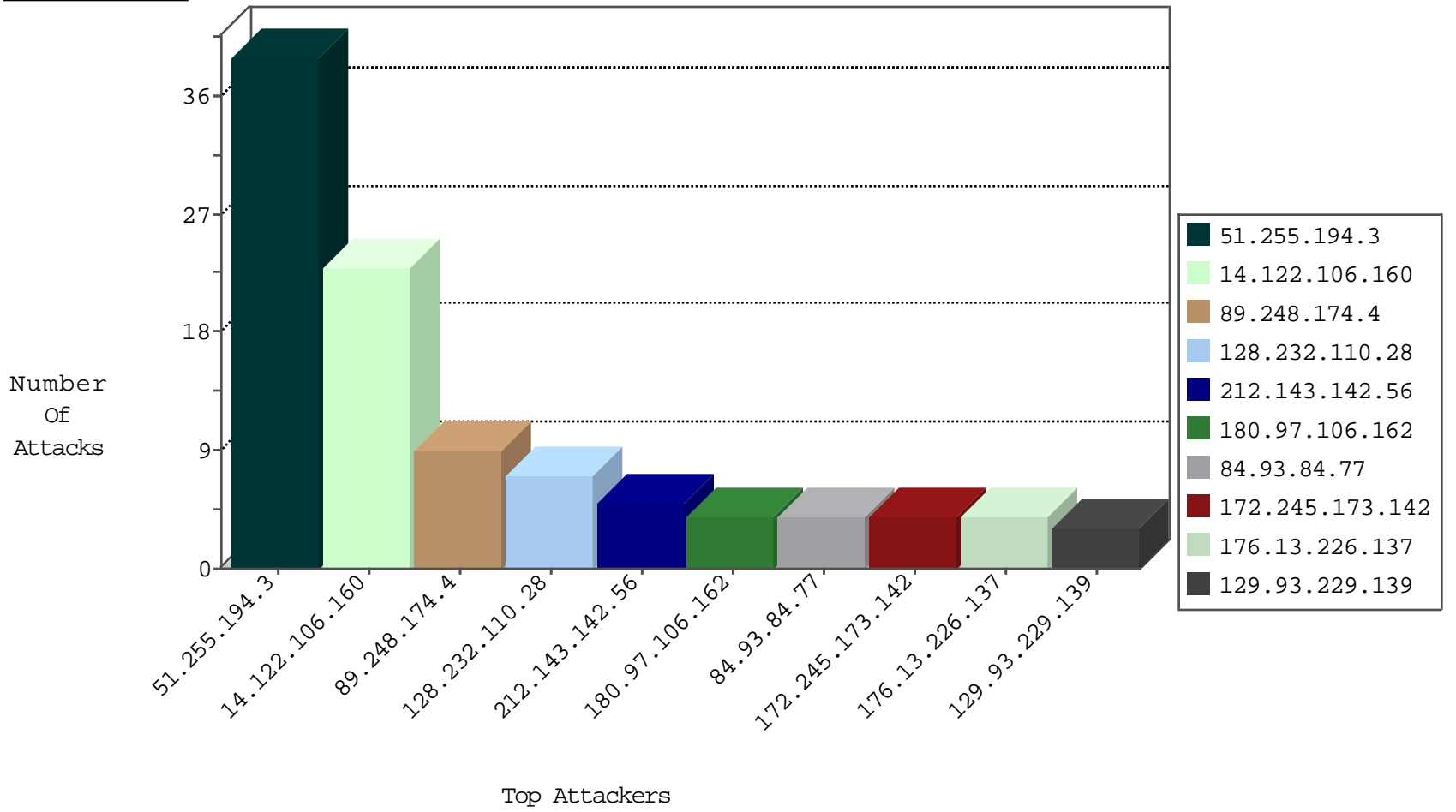
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
129.93.229.139	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.8.126.111	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.42.142.45	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
204.85.191.10	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
192.33.90.68	Switzerland	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
129.32.84.160	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
192.33.90.69	Switzerland	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
139.78.141.243	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.82	Czech Republic	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
164.107.127.12	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
51.255.194.3	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	37
51.255.194.3	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
94.102.49.193	Netherlands	147.237.0.16	my-kosher-kravi.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
106.120.188.145	China	147.237.77.74	law.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
84.93.84.77	147.237.77.216	United Kingdom	dover.idf.il	Tehila - Perl LWP with fake user agent	4
50.116.123.135	147.237.72.156	United States	aman.idf.il	ET SCAN Potential SSH Scan	1
217.165.65.195	147.237.77.216	United Arab Emirates	dover.idf.il	ET SCAN NMAP -sS window 1024	1
172.245.173.142	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
217.165.65.195	147.237.77.216	United Arab Emirates	dover.idf.il	ET SCAN NMAP -sS window 3072	1
179.43.141.198	147.237.72.14	Switzerland	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
163.172.129.15	147.237.76.200	United Kingdom	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
176.13.226.137	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
2.55.54.233	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
128.232.110.28	United Kingdom	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
128.232.110.28	United Kingdom	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
89.248.174.4	Netherlands	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	1
180.97.106.37	China	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.109	United States	147.237.0.35	akaws.idf.il	drop		drop	1
137.116.71.170	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
89.248.174.4	Netherlands	147.237.77.235	sviva.idf.il	drop	SAM rule	drop	1
180.97.106.162	China	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.60	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
172.245.173.142	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.102	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
128.232.110.28	United Kingdom	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
89.248.174.4	Netherlands	147.237.76.200	eitan.aka.idf.il	drop	SAM rule	drop	1
180.97.106.161	China	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.109	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
139.162.37.147	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
94.102.49.193	Netherlands	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
180.97.106.162	China	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
89.248.174.4	Netherlands	147.237.0.15	kosher-kravi.idf.il	drop	SAM rule	drop	1
172.245.173.142	United States	147.237.77.212	e.dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.105	United States	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
128.232.110.28	United Kingdom	147.237.76.148	ggcenter.aka.idf.il	drop		drop	1
216.218.206.106	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
89.248.174.4	Netherlands	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	1
180.97.106.161	China	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
71.6.216.51	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
141.212.122.110	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.97	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
104.209.188.207	United States	147.237.77.216	dover.idf.il	Instant Messengers	instant messenger pattern found, application: Skype	monitor	1
184.105.139.95	United States	147.237.0.35	akaws.idf.il	drop		drop	1
89.248.174.4	Netherlands	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
172.245.173.142	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.106	United States	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
89.248.174.4	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	1
180.97.106.162	China	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
71.6.216.51	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.118	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.98	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.104	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
89.248.174.4	Netherlands	147.237.72.167	ishurim.aka.idf.il	drop	SAM rule	drop	1
141.212.122.108	United States	147.237.0.35	akaws.idf.il	drop		drop	1
137.116.71.170	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
89.248.174.4	Netherlands	147.237.77.233	atal.idf.il	drop	SAM rule	drop	1
180.97.106.162	China	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
71.6.216.58	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.119	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.101	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

09-14-2016-04:04:08 to 09-14-2016-05:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
14.122.106.160	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 14.122.106.160	Block	16
14.122.106.160	China	147.237.77.176	matpash.idf.il	PHP Attempt	Block	6
68.180.228.171	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2110-he/cogat.aspx	Block	1
5.148.73.101	United Kingdom	147.237.77.216	dover.idf.il	Illegal Byte Code Character in URL /english/#012	Block	1
68.180.229.223	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1393-en/dover.aspx	Block	1
109.65.30.44	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
144.76.16.162	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
14.122.106.160	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/index.asp	Block	1
200.111.107.58	Chile	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/index.php	Block	1

09-14-2016-04:04:08 to 09-14-2016-05:04:08