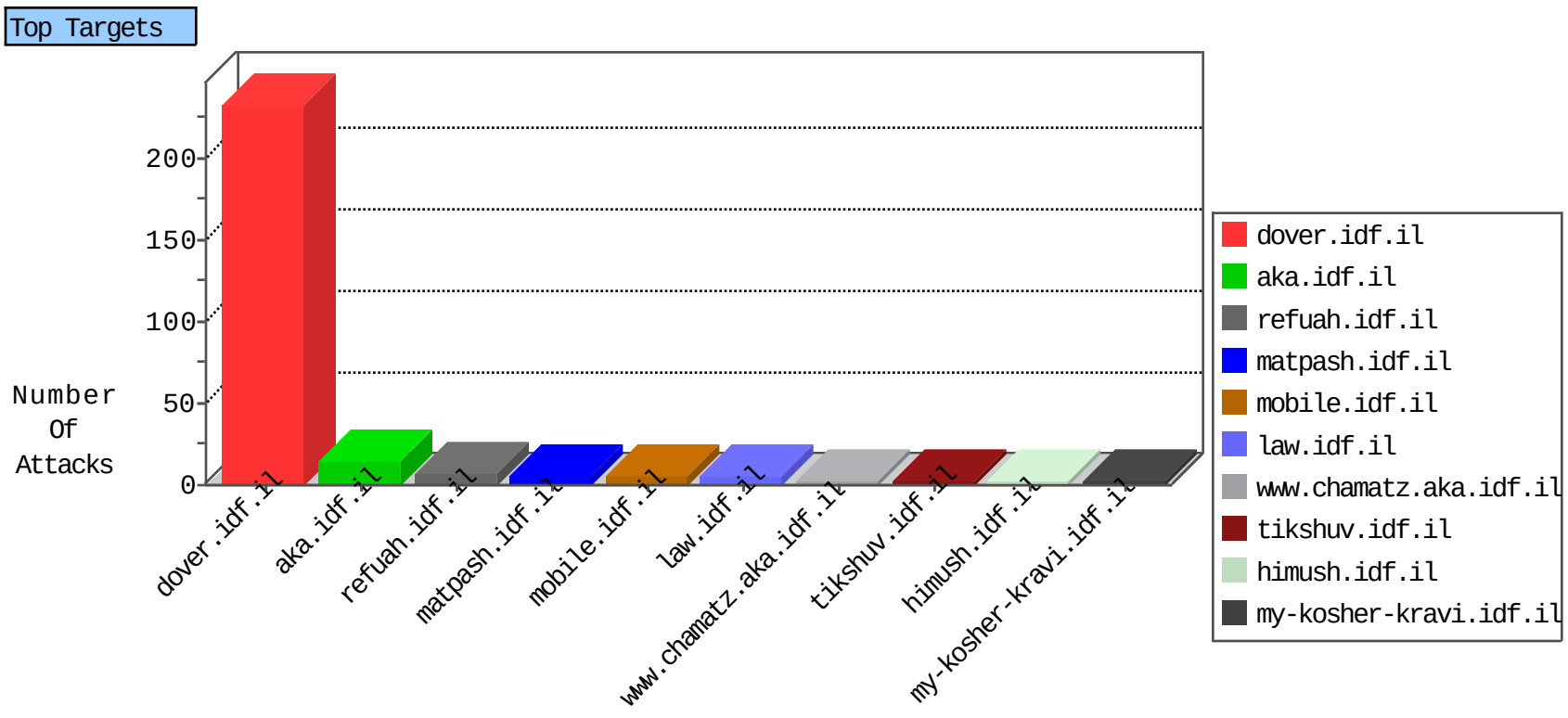
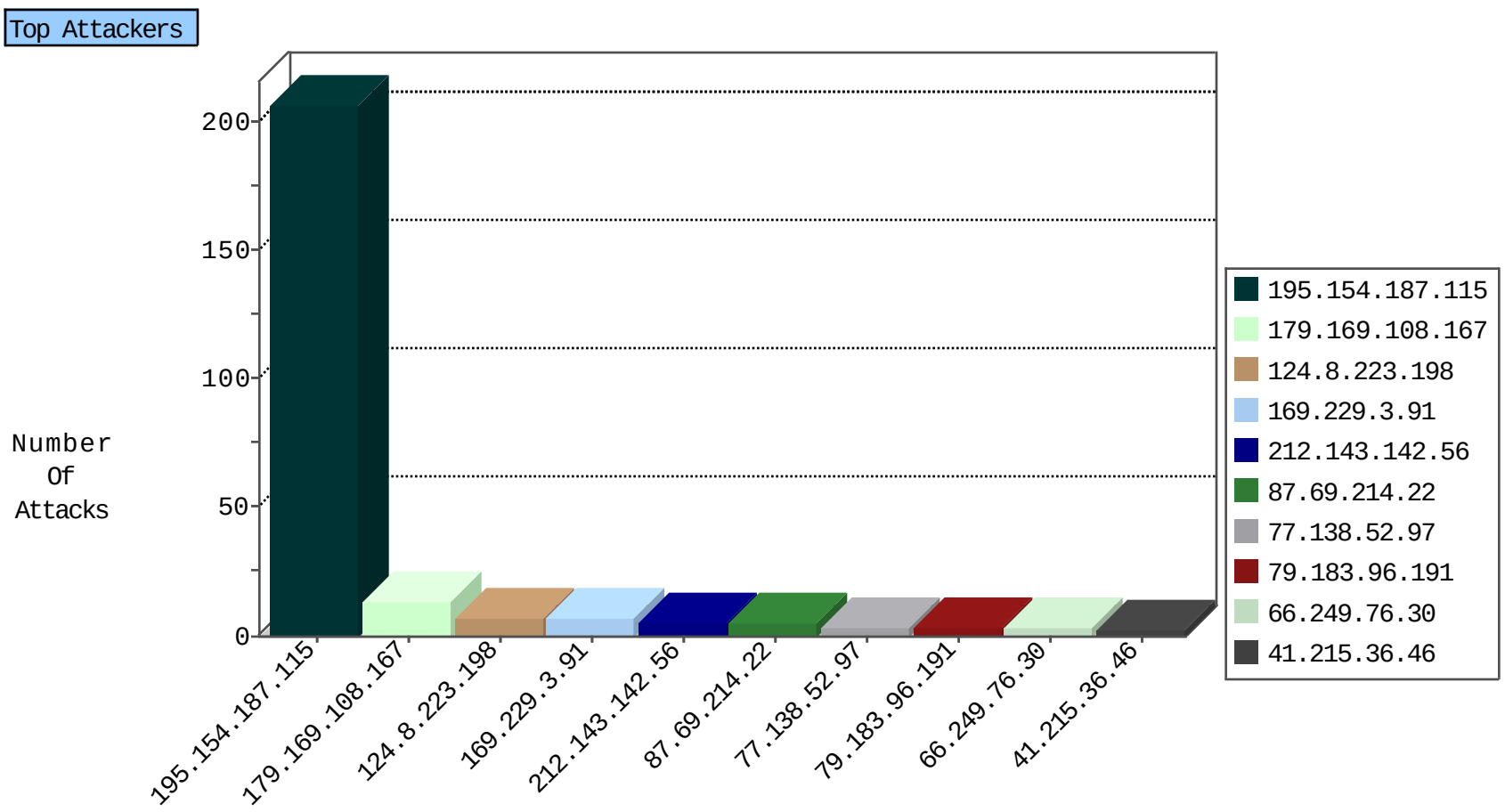
09-26-2016-03:04:01 to 09-26-2016-04:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-26-2016-03:04:01 to 09-26-2016-04:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
60.165.176.125	China	147.237.72.14	dover.idf.il(old)	Invalid TCP Flags	drop	2
37.186.206.220	Italy	147.237.77.212	e.dover.idf.il	L4 Source or Dest Port Zero	drop	1
185.94.111.1	Russian Federation	147.237.76.196	e.sviva.idf.il	Black List	drop	1
209.126.136.2	United States	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1

09-26-2016-03:04:01 to 09-26-2016-04:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
195.154.187.115	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	194
195.154.187.115	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	6
195.154.187.115	France	147.237.77.226	www.chamatz.aka.idf.il	C1000074: HTTP: majestic bot	Permit	3
195.154.187.115	France	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	2
195.154.187.115	France	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-26-2016-03:04:01 to 09-26-2016-04:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
103.207.37.81	147.237.72.167	Vietnam	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
78.129.171.173	147.237.77.19	United Kingdom	law-forum.idf.il	ET SCAN Potential SSH Scan	1
46.183.223.228	147.237.8.46	Latvia	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
195.80.140.250	147.237.77.74	Ukraine	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
41.215.36.46	147.237.77.179	Kenya	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.129.15	147.237.77.235	United Kingdom	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
124.8.223.198	147.237.76.199	Taiwan	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
124.8.223.198	147.237.76.44	Taiwan	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
124.8.223.198	147.237.0.35	Taiwan	akaws.idf.il	ET SCAN Potential SSH Scan	1
110.80.119.37	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
78.129.171.173	147.237.77.178	United Kingdom	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
41.215.36.46	147.237.77.205	Kenya	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
181.48.36.61	147.237.0.16	Colombia	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
31.24.228.20	147.237.77.227	United Kingdom	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
124.8.223.198	147.237.76.202	Taiwan	e.halag.idf.il	ET SCAN Potential SSH Scan	1
124.8.223.198	147.237.76.177	Taiwan	ncore.idf.il	ET SCAN Potential SSH Scan	1
124.8.223.198	147.237.76.30	Taiwan	himush.idf.il	ET SCAN Potential SSH Scan	1
124.8.223.198	147.237.0.34	Taiwan	tikshuv.idf.il	ET SCAN Potential SSH Scan	1

09-26-2016-03:04:01 to 09-26-2016-04:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
179.169.108.167	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
66.249.76.30	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.183.96.191	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.69.214.22	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
95.25.94.51	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
68.180.228.99	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.85.147	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
109.63.129.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
87.69.214.22	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
109.173.32.191	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
23.248.234.11	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
169.229.3.91	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.50	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.199	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
115.75.2.254	Vietnam	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid sequence number	monitor	1
23.248.235.19	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
172.247.85.200	United States	147.237.0.33	idf.il	drop		drop	1
141.212.122.51	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
107.197.86.83	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
169.229.3.91	United States	147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
138.246.253.19	Germany	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
172.247.86.217	United States	147.237.0.200	m4u.idf.il	drop		drop	1
141.212.122.168	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.6	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
169.229.3.91	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
139.162.37.147	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
66.102.8.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.169	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
109.63.145.60	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
74.82.47.37	United States	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
169.229.3.91	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	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
66.102.8.156	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
184.105.139.76	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
169.229.3.91	United States	147.237.0.35	akaws.idf.il	drop		drop	1
74.82.47.38	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1

09-26-2016-03:04:01 to 09-26-2016-04:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.224	Block	2
96.242.35.164	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/tizmoret/	Block	2
185.13.193.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl83 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
84.108.87.238	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1
46.4.74.42	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
157.55.39.28	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
66.249.69.229	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/.well-known/assetlinks.json	Block	1
207.46.13.3	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/robots.txt	Block	1
84.108.87.238	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/wp-login.php	Block	1
60.240.90.32	Australia	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
157.55.39.133	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/robots.txt	Block	1
66.249.76.85	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
207.46.13.24	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/kamlar/klali/default.asp	None	1
84.109.3.215	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
65.208.151.116	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/sip_storage/files/0/	Block	1
157.55.39.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/article/watch	Block	1
66.249.76.87	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9031-he/refuah.aspx	Block	1
207.46.13.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/article/watch	Block	1
90.31.89.227	Guadeloupe	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/en	Block	1
40.77.167.53	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1
66.249.69.228	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1

09-26-2016-03:04:01 to 09-26-2016-04:04:01