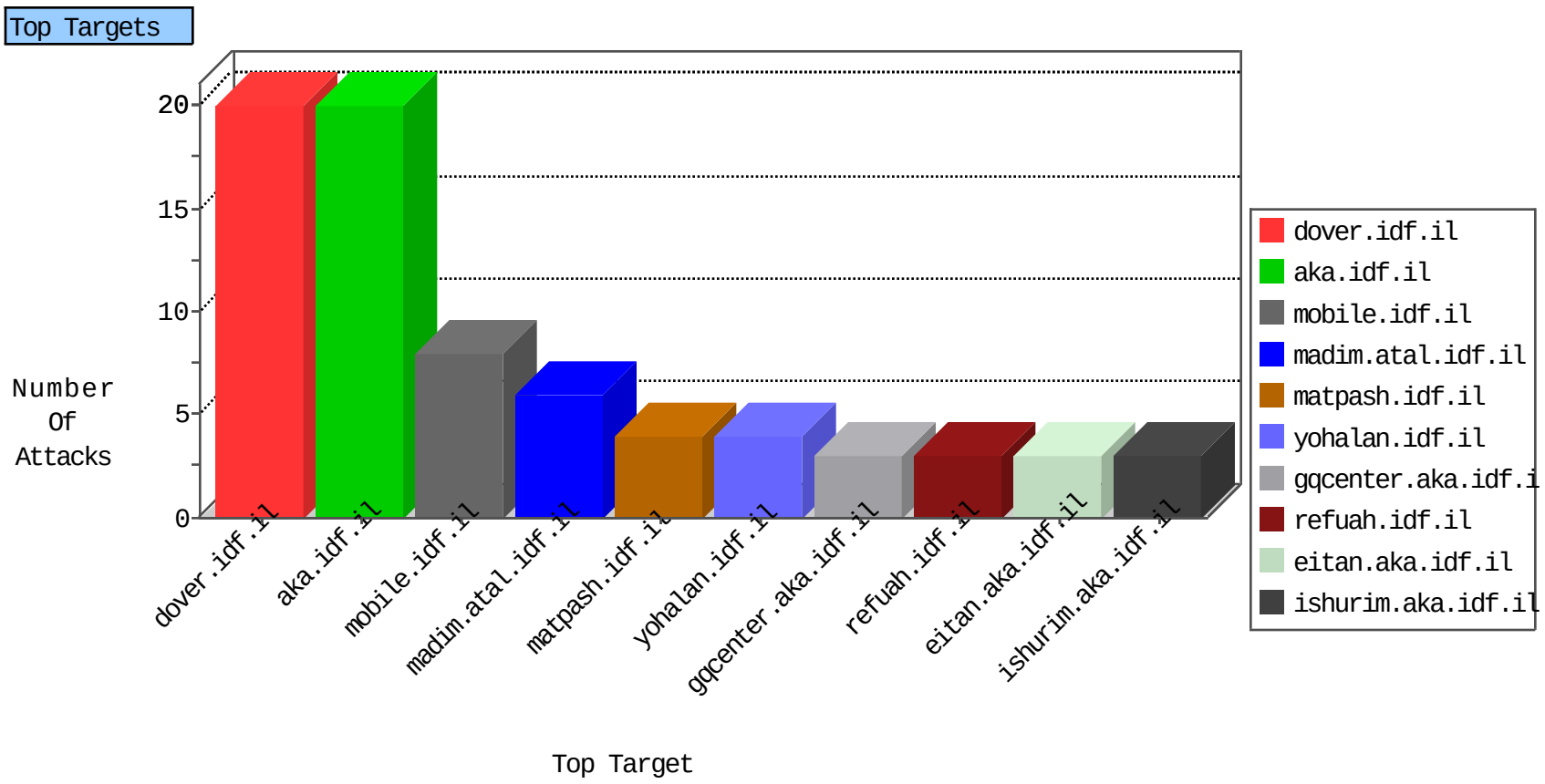
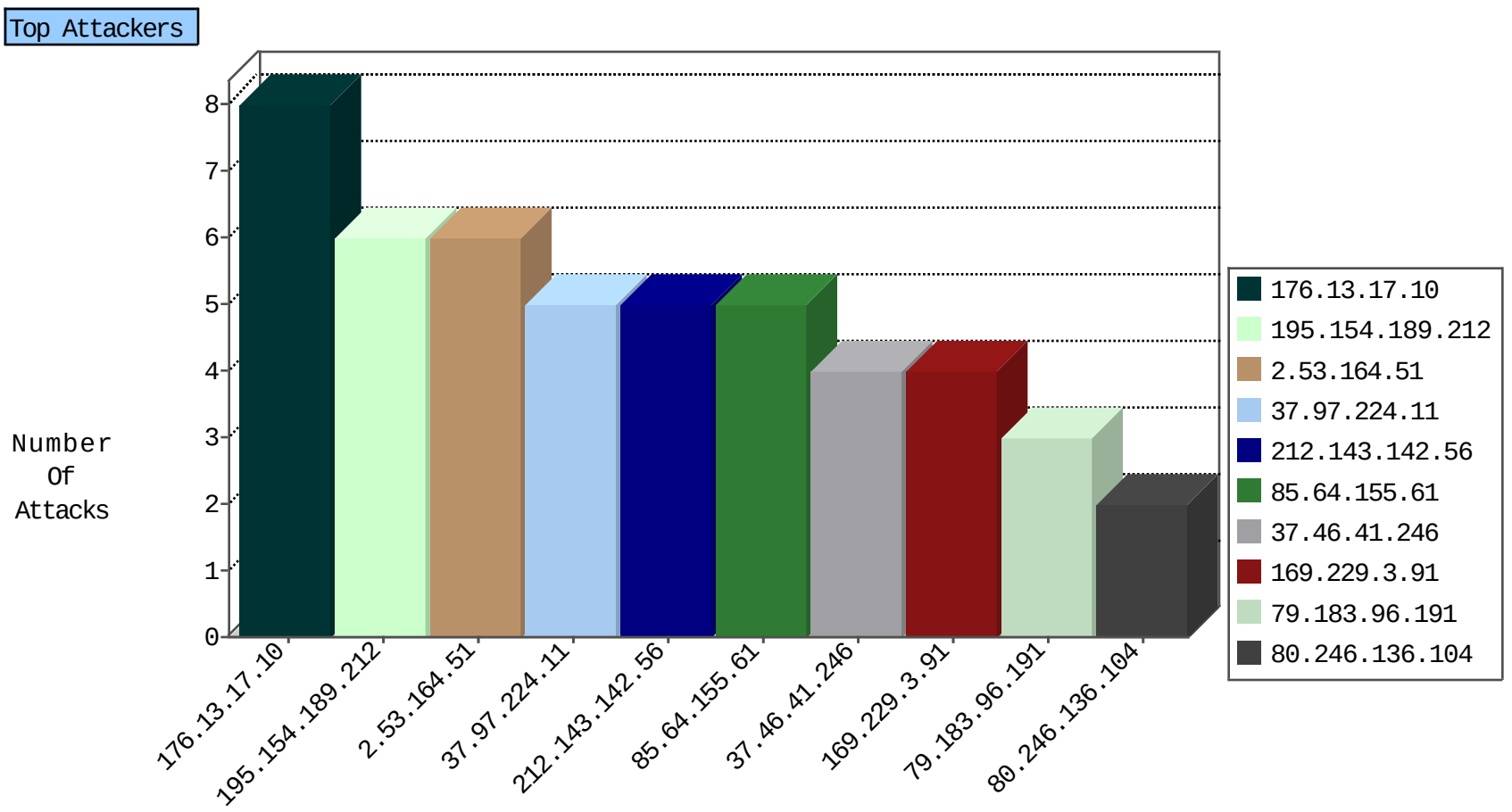
09-26-2016-02:04:07 to 09-26-2016-03:04:07

IDF Under Attack Daily Report





09-26-2016-02:04:07 to 09-26-2016-03:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
78.129.171.175	United Kingdom	147.237.76.44	e.refuah.idf.il	Black List	drop	1
93.174.94.235	Netherlands	147.237.76.177	ncore.idf.il	Black List	drop	1
195.154.189.212	France	147.237.0.200	m4u.idf.il	JLM_Purple_Con_Limit_Http	drop	1

09-26-2016-02:04:07 to 09-26-2016-03:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-26-2016-02:04:07 to 09-26-2016-03:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
37.97.224.11	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
37.97.224.11	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
37.97.224.11	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
13.90.253.185	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
211.149.244.79	147.237.77.227	China	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.169.150	147.237.72.167	United Kingdom	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
109.75.44.26	147.237.76.31	Armenia	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
82.79.75.5	147.237.77.170	Romania	maarachot.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
69.129.141.35	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 3072	1
37.97.224.11	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
37.97.224.11	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
31.24.228.20	147.237.0.15	United Kingdom	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
210.212.207.80	147.237.8.50	India	e.tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
125.107.121.5	147.237.77.74	China	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
103.207.36.31	147.237.76.176	Vietnam	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
69.129.141.35	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 4096	1

09-26-2016-02:04:07 to 09-26-2016-03:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.13.17.10	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
85.64.155.61	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
79.183.96.191	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.46.41.246	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.53.164.51	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.139.72.137	France	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
80.246.136.104	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
207.46.13.24	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
23.248.235.20	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
195.154.189.212	France	147.237.76.34	yohalan.idf.il	drop		drop	1
169.229.3.91	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.173	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
5.22.134.98	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
162.209.180.150	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
105.155.158.216	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
23.248.236.4	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
195.154.189.212	France	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
172.247.82.216	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
141.212.122.174	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
5.29.29.22	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
190.106.245.213	Bolivia	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
122.103.208.34	Japan	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
195.154.189.212	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
172.247.83.197	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
141.212.122.175	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
23.248.234.19	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
195.154.189.212	France	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
169.229.3.91	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
122.103.208.34	Japan	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
37.46.41.246	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
172.247.83.219	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
156.204.211.110	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
23.248.234.27	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
195.154.189.212	France	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
169.229.3.91	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
141.212.122.172	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
71.6.165.200	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
2.55.173.7	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
172.247.85.198	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
162.205.68.202	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
85.65.71.112	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1

09-26-2016-02:04:07 to 09-26-2016-03:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.164.51	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
157.55.39.155	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/watch	Block	1
66.249.66.176	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/5/1635.pdf	Block	1
173.58.246.46	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
180.76.15.14	China	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il/robots.txt	Block	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1815-he/dover.aspx	Block	1
204.79.180.204	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/templates/inner.asp	Block	1
2.55.129.131	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	1
81.223.254.34	Austria	147.237.77.74	law.idf.il	Unauthorized URL Access to /robots.txt	Block	1

09-26-2016-02:04:07 to 09-26-2016-03:04:07