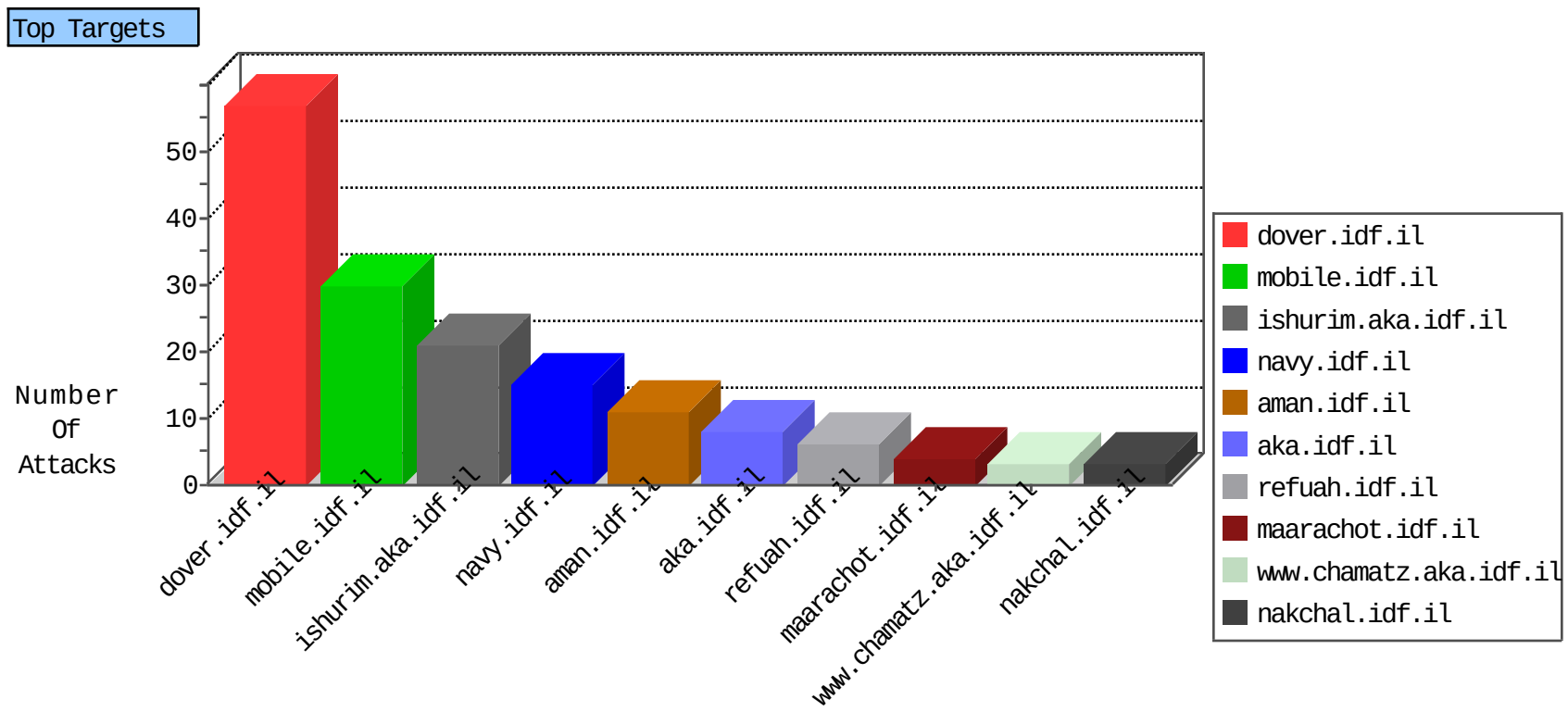
09-23-2016-06:04:05 to 09-23-2016-07:04:05

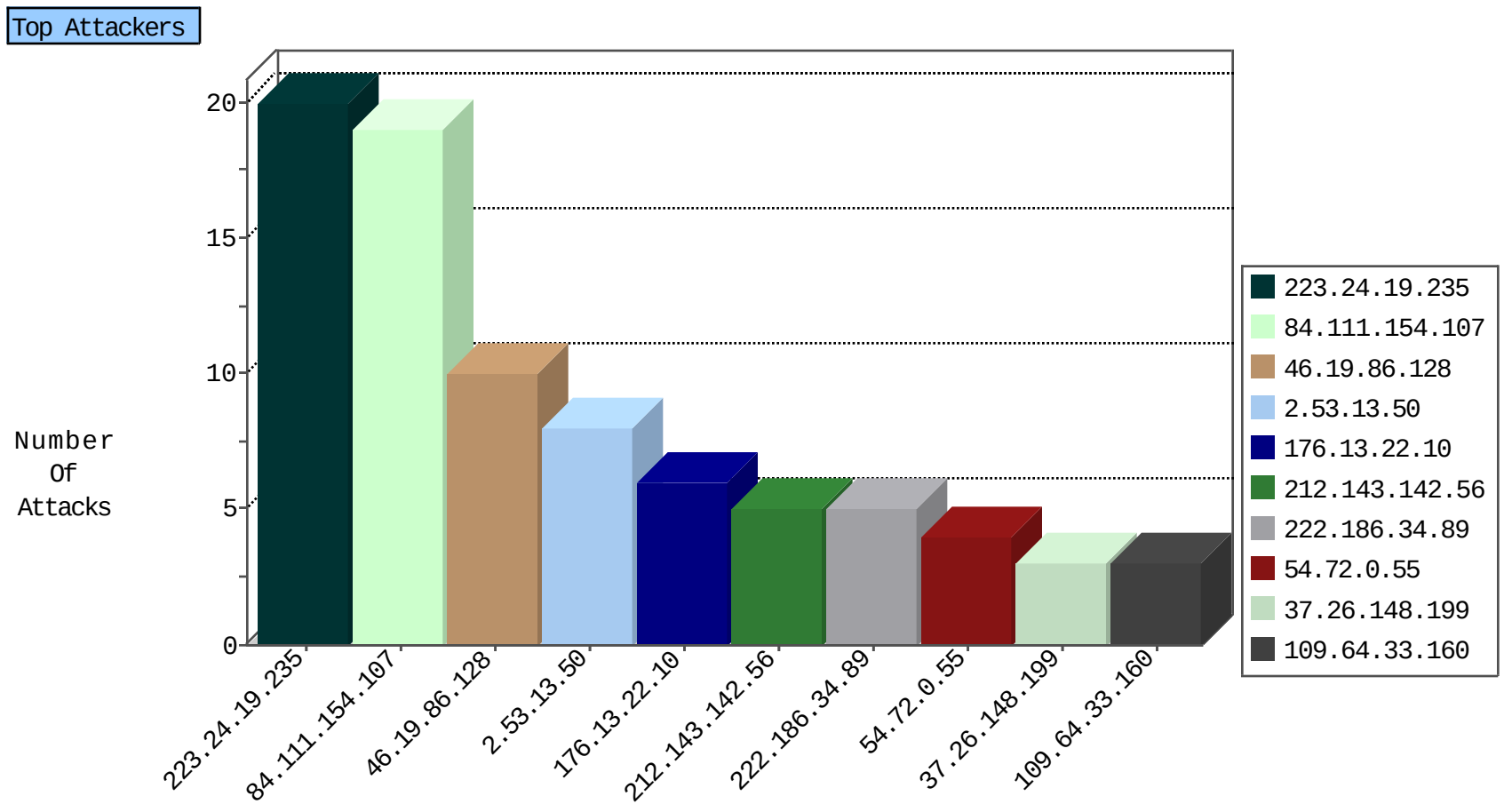
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

09-23-2016-06:04:05 to 09-23-2016-07:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
80.246.133.230	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
179.99.200.39	Brazil	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	forward	1
66.240.236.119	United States	147.237.76.196	e.sviva.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.42	refuah.idf.il	Black List	drop	1
212.143.142.56	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
168.235.207.204	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	1
66.240.192.138	United States	147.237.76.198	e.yohalan.idf.il	Black List	drop	1

09-23-2016-06:04:05 to 09-23-2016-07:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
69.30.213.82	United States	147.237.76.42	refuah.idf.il	C1000074: HTTP: majestic bot	Permit	2
199.58.86.206	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
46.165.197.141	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

09-23-2016-06:04:05 to 09-23-2016-07:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
222.186.34.89	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
222.186.34.89	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
222.186.34.89	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
211.149.231.57	147.237.0.15	China	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1
139.162.187.89	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
100.13.130.4	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
46.161.40.17	147.237.0.35	Russian Federation	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
223.245.239.8	147.237.77.216	China	dover.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
222.186.34.89	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
222.186.34.89	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
211.149.240.243	147.237.76.31	China	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
211.149.197.148	147.237.77.121	China	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
128.232.110.28	147.237.77.243	United Kingdom	mobile.idf.il	ET SCAN Potential SSH Scan	1
66.249.76.83	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	1

09-23-2016-06:04:05 to 09-23-2016-07:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
223.24.19.235	Thailand	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
46.19.86.128	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	10
84.111.154.107	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence		monitor	7
176.13.22.10	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.13.50	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
84.111.154.107	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
37.26.148.199	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
84.111.154.107	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	3
84.111.154.107	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
2.53.13.50	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.165	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
84.111.154.107	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.60	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
106.186.113.132	Japan	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
81.199.120.32	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
71.127.37.44	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
5.29.29.22	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
184.105.247.235	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
123.125.67.148	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
184.105.139.75	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
100.13.130.4	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
188.120.154.174	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.135	United States	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.120.69.225	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
216.218.206.103	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.112	United States	147.237.0.33	idf.il	drop		drop	1
100.13.130.4	United States	147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
79.176.88.83	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
193.15.16.4	Sweden	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
141.212.122.136	United States	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.120.152.132	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.247.203	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
79.176.88.83	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
198.96.155.3	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
66.249.66.153	Israel	147.237.0.33	idf.il	drop		drop	1
184.105.247.214	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
109.226.57.50	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	1
46.19.85.251	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
212.106.67.181	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
177.154.145.101	Brazil	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1

09-23-2016-06:04:05 to 09-23-2016-07:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.64.33.160	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/he/navy.aspx	Block	3
176.228.151.248	Israel	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/he/navy.aspx	Block	2
66.249.76.31	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1751	Block	1
66.249.66.185	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/3/3493.jpg	Block	1
88.190.87.46	France	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 88.190.87.46 (Unsupported Cipher)	None	1
66.249.66.188	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/2271.jpg	Block	1
66.249.64.156	Israel	147.237.0.34	tikshuv.idf.i	Unauthorized URL Access to www.tikshuv.idf.il/shared/usercontrols/headerupper/	Block	1
66.249.76.2	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1752	Block	1
157.55.39.1	United States	147.237.76.31	nakchal.idf.i	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
66.249.64.159	Israel	147.237.0.34	tikshuv.idf.i	Unauthorized URL Access to www.tikshuv.idf.il/modules/forums.frm/frmprintmessage.aspx	Block	1
66.249.76.31	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.76.31	Block	1
157.55.39.155	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list20041220a.htm	Block	1
66.249.66.182	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/scriptresource.axd	Block	1

09-23-2016-06:04:05 to 09-23-2016-07:04:05