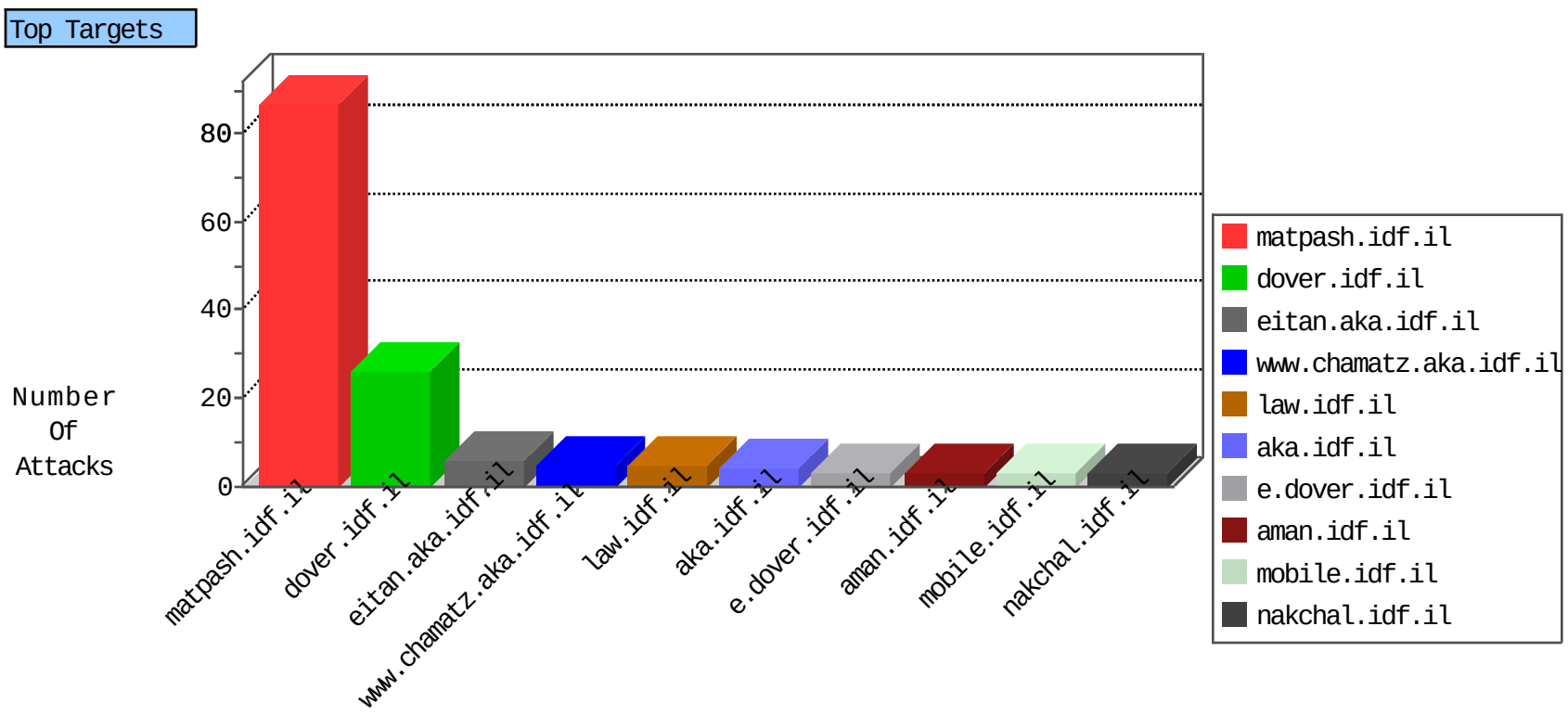
10-04-2016-05:04:02 to 10-04-2016-06:04:02

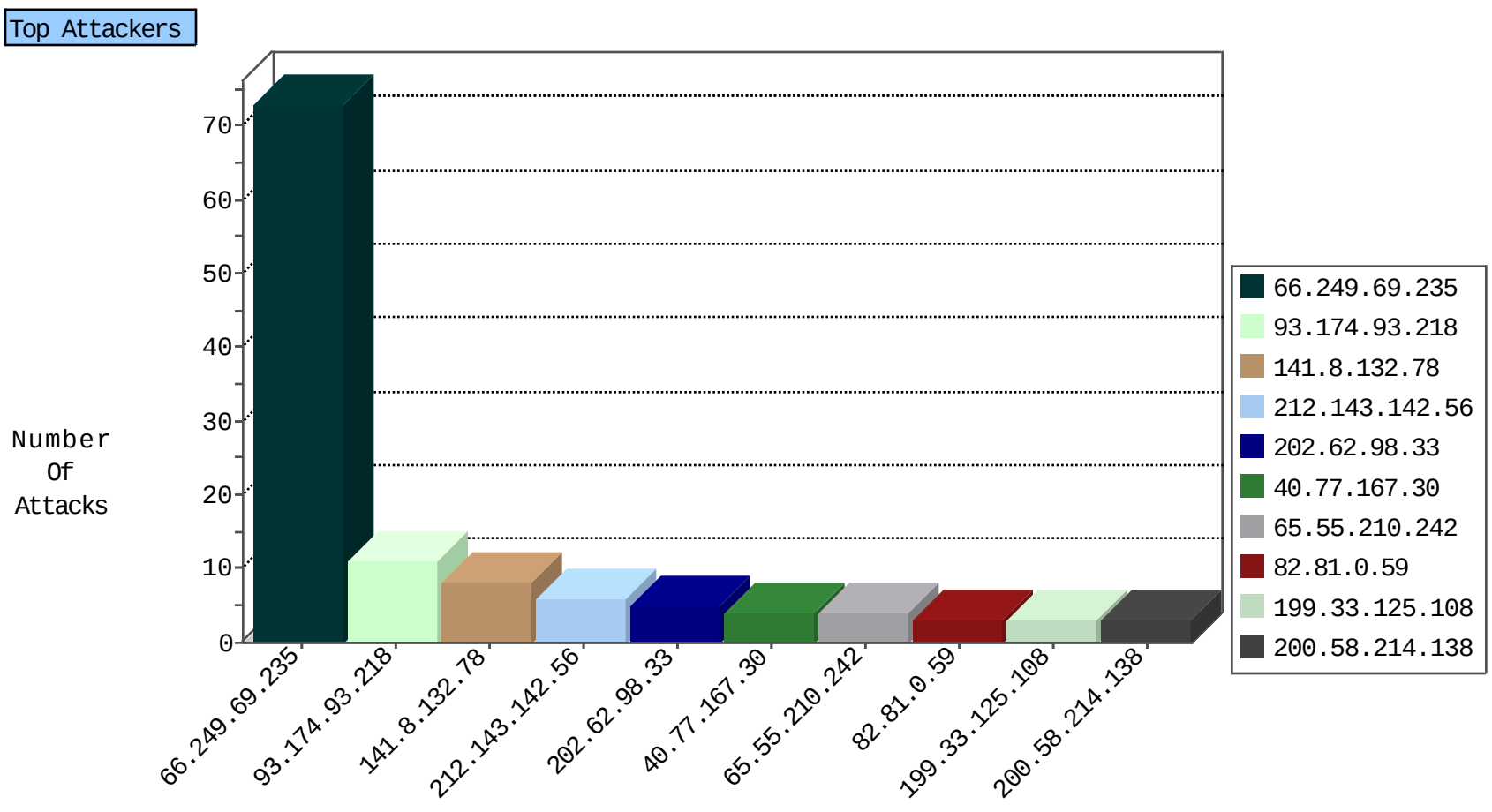
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

10-04-2016-05:04:02 to 10-04-2016-06:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.174.93.218	Netherlands	147.237.77.176	matpash.idf.il	block-sp-traf1	forward	2
93.174.94.235	Netherlands	147.237.76.34	yohalan.idf.il	Black List	drop	1
93.174.94.235	Netherlands	147.237.76.200	eitan.aka.idf.il	Black List	drop	1
199.33.125.108	United States	147.237.76.198	e.yohalan.idf.il	JLM_Purple_Con_Limit_Http	drop	1

10-04-2016-05:04:02 to 10-04-2016-06:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	1090: HTTP: IIS .asp Source Code Read	Permit	8
151.80.31.181	France	147.237.77.216	dover.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

10-04-2016-05:04:02 to 10-04-2016-06:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.69.235	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	73
103.208.244.223	147.237.0.19		madim.atal.idf.il	ET SCAN Potential SSH Scan	1
58.177.250.130	147.237.8.14	Hong Kong	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
49.206.2.88	147.237.77.233	India	atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
204.83.37.63	147.237.76.202	Canada	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
200.58.214.138	147.237.72.166	Colombia	aka.idf.il	ET SCAN NMAP -sS window 4096	1
200.58.214.138	147.237.72.166	Colombia	aka.idf.il	ET SCAN NMAP -f -sS	1
113.108.195.106	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
103.208.244.223	147.237.76.30		himush.idf.il	ET SCAN Potential SSH Scan	1
54.82.56.247	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
46.172.91.21	147.237.76.31	Ukraine	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
201.114.60.162	147.237.76.39	Mexico	mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
200.58.214.138	147.237.72.166	Colombia	aka.idf.il	ET SCAN NMAP -sS window 2048	1
134.29.253.245	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
103.208.244.223	147.237.76.31		nakchal.idf.il	ET SCAN Potential SSH Scan	1

10-04-2016-05:04:02 to 10-04-2016-06:04:02

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	6
202.62.98.33	Lao People's Democratic Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
65.55.210.242	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
82.81.0.59	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.150	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
91.224.217.119	Poland	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
40.77.167.30	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
93.174.93.218	Netherlands	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Response out of state	monitor	2
69.30.213.202	United States	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	2
46.19.85.151	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
77.237.146.28	Czech Republic	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
23.248.234.30	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
183.129.160.229	China	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	1
141.212.122.109	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
40.77.167.30	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
199.33.125.108	United States	147.237.0.35	akaws.idf.il	drop		drop	1
23.224.123.42	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
172.247.83.204	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
138.246.253.19	Germany	147.237.76.177	ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.120.72.83	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
23.248.235.19	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
184.105.139.76	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
162.209.232.12	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
23.224.124.16	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
172.247.84.220	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
141.212.122.100	United States	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
23.248.235.27	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
184.105.247.208	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
162.209.232.14	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
40.77.167.30	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
202.62.98.33	Lao People's Democratic Republic	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
23.224.172.34	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
172.247.85.205	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
141.212.122.101	United States	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
23.248.237.22	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
184.105.247.232	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
162.209.233.38	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
94.102.49.193	Netherlands	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
23.248.234.25	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
172.247.85.206	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
141.212.122.108	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
23.248.237.29	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
189.149.160.9	Mexico	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
23.224.123.24	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
172.247.82.209	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
104.128.144.131	Canada	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1

10-04-2016-05:04:02 to 10-04-2016-06:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.174.93.218	Netherlands	147.237.77.176	matpash.idf.il	Multiple NULL Character in Method from 93.174.93.218	Block	3
93.174.93.218	Netherlands	147.237.77.176	matpash.idf.il	Multiple Illegal Byte Code Character in Method from 93.174.93.218	Block	2
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/sites/home/default.asp	Block	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-13885-en/dov.	Block	1
93.174.93.218	Netherlands	147.237.77.176	matpash.idf.il	NULL Character in Method	Block	1
66.249.76.74	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1
199.33.125.108	United States	147.237.77.216	dover.idf.il	Unauthorized Method HEAD for /	Block	1
93.174.93.218	Netherlands	147.237.77.176	matpash.idf.il	Illegal Byte Code Character in Method	Block	1
216.244.66.236	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in tikshuv.idf.il/site/general.aspx	Block	1
37.8.91.141	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1

10-04-2016-05:04:02 to 10-04-2016-06:04:02