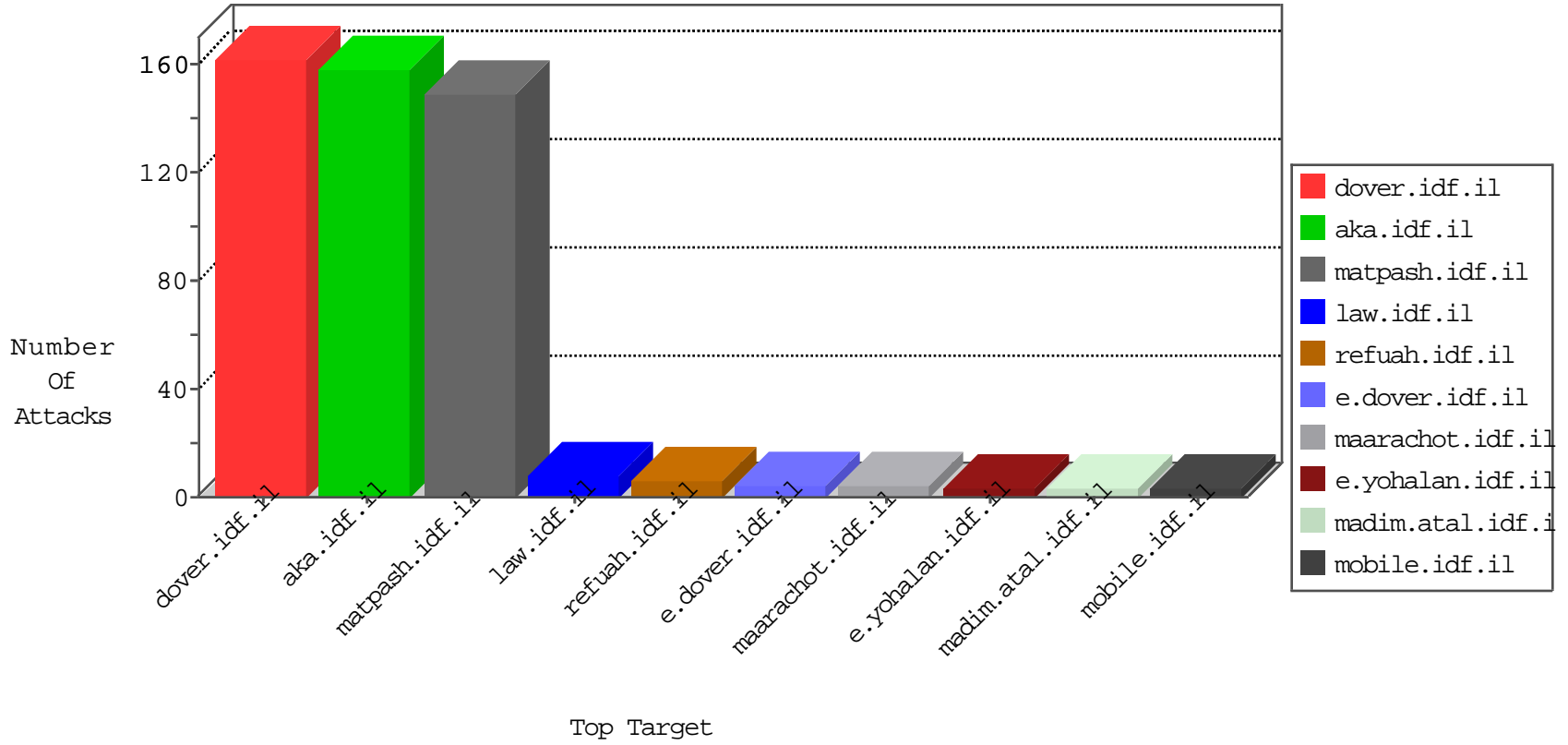


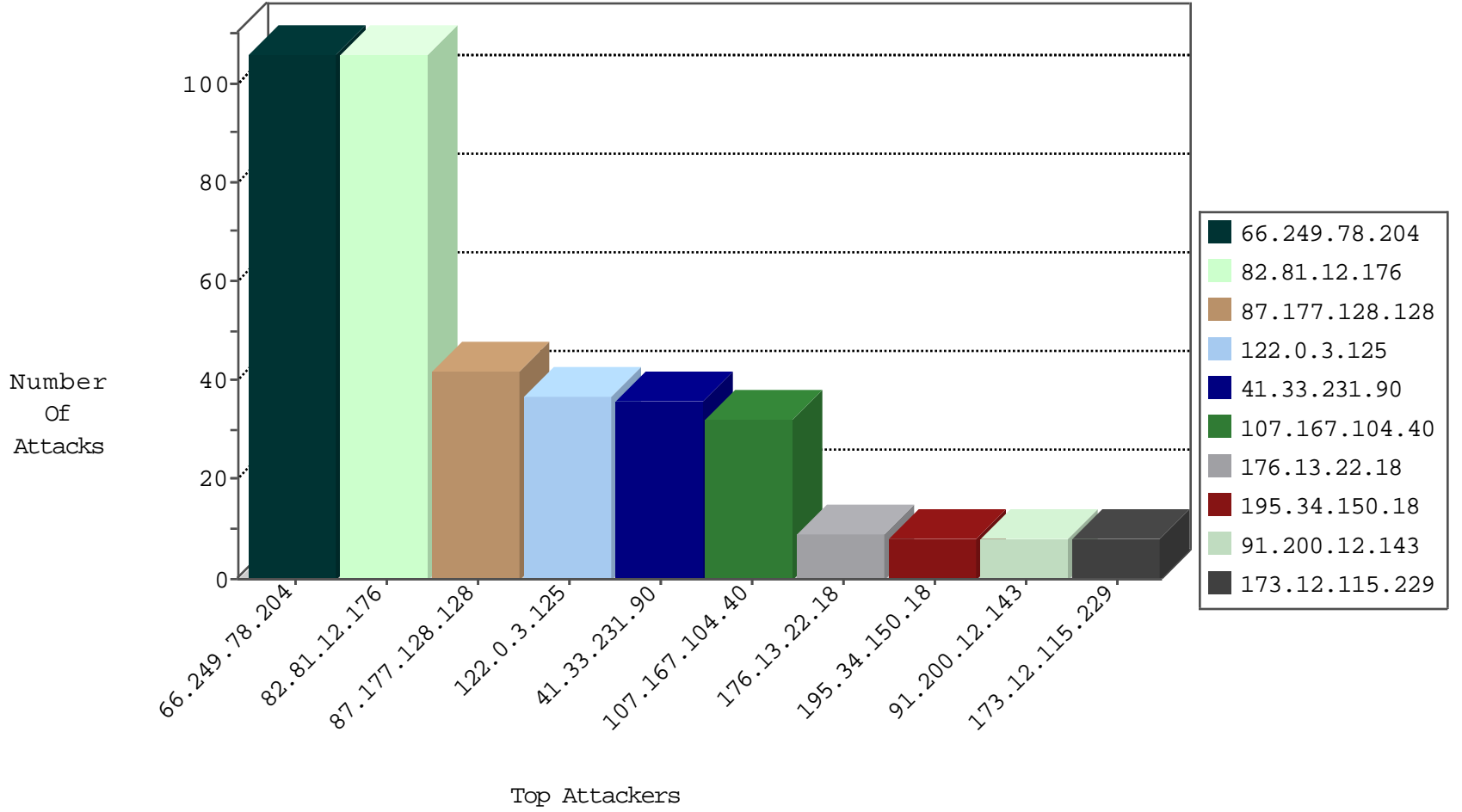
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.78.146	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1278
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	106

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.78.204	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	106
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
94.76.11.255	147.237.72.14	Bahrain	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	2
94.76.11.255	147.237.72.156	Bahrain	aman.idf.il	ET SCAN NMAP -sS window 1024	2
218.246.0.97	147.237.77.233	China	atal.idf.il	ET SCAN NMAP -sS window 1024	1
210.93.50.130	147.237.76.198	Korea, Republic of	e.yohalan.idf.il	ET SCAN NMAP -f -sS	1
188.0.236.123	147.237.76.42	Moldova, Republic of	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
173.12.115.229	147.237.0.34	United States	tikshuv.idf.il	SERVER-APACHE Apache Tomcat Web Application Manager access	1
173.12.115.229	147.237.0.15	United States	kosher-kravi.idf.il	SERVER-APACHE Apache Tomcat Web Application Manager access	1
94.76.11.255	147.237.72.167	Bahrain	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
210.93.50.130	147.237.76.198	Korea, Republic of	e.yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
173.55.32.113	147.237.76.39	United States	mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
173.12.115.229	147.237.0.19	United States	madim.atal.idf.il	SERVER-APACHE Apache Tomcat Web Application Manager access	1
168.62.238.153	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
87.177.128.128	Germany	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	40
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
122.0.3.125	Thailand	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
107.167.104.40	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	32
176.13.22.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
91.200.12.143	Ukraine	147.237.77.74	law.idf.il	drop	SAM rule	drop	4
91.200.12.143	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
37.247.36.72	Netherlands	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
109.65.6.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.117.59	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
207.46.13.49	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.12.155.133	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
157.55.39.214	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.188.32	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.64.180.244	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
91.200.12.136	Ukraine	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	2
176.12.155.133	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
87.177.128.128	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
54.152.28.97	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
91.200.12.7	Ukraine	147.237.77.74	law.idf.il	drop	SAM rule	drop	2
5.22.130.88	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
91.200.12.7	Ukraine	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	2
46.120.29.189	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
123.181.96.99	China	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
91.200.12.7	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
46.19.85.195	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
123.181.96.99	China	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
74.82.47.38	United States	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.121.61.195	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
216.218.206.120	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.16	United States	147.237.0.33	idf.il	drop		drop	1
184.105.139.78	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.253	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
132.68.10.118	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
2.36.176.147	Italy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.122	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.16	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.115	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.85.253	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
83.250.199.52	Sweden	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
60.225.115.91	Australia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.19.85.116	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
122.0.3.125	Thailand	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
217.132.111.248	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	1
74.82.47.19	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.247	United States	147.237.0.35	akaws.idf.il	drop		drop	1

