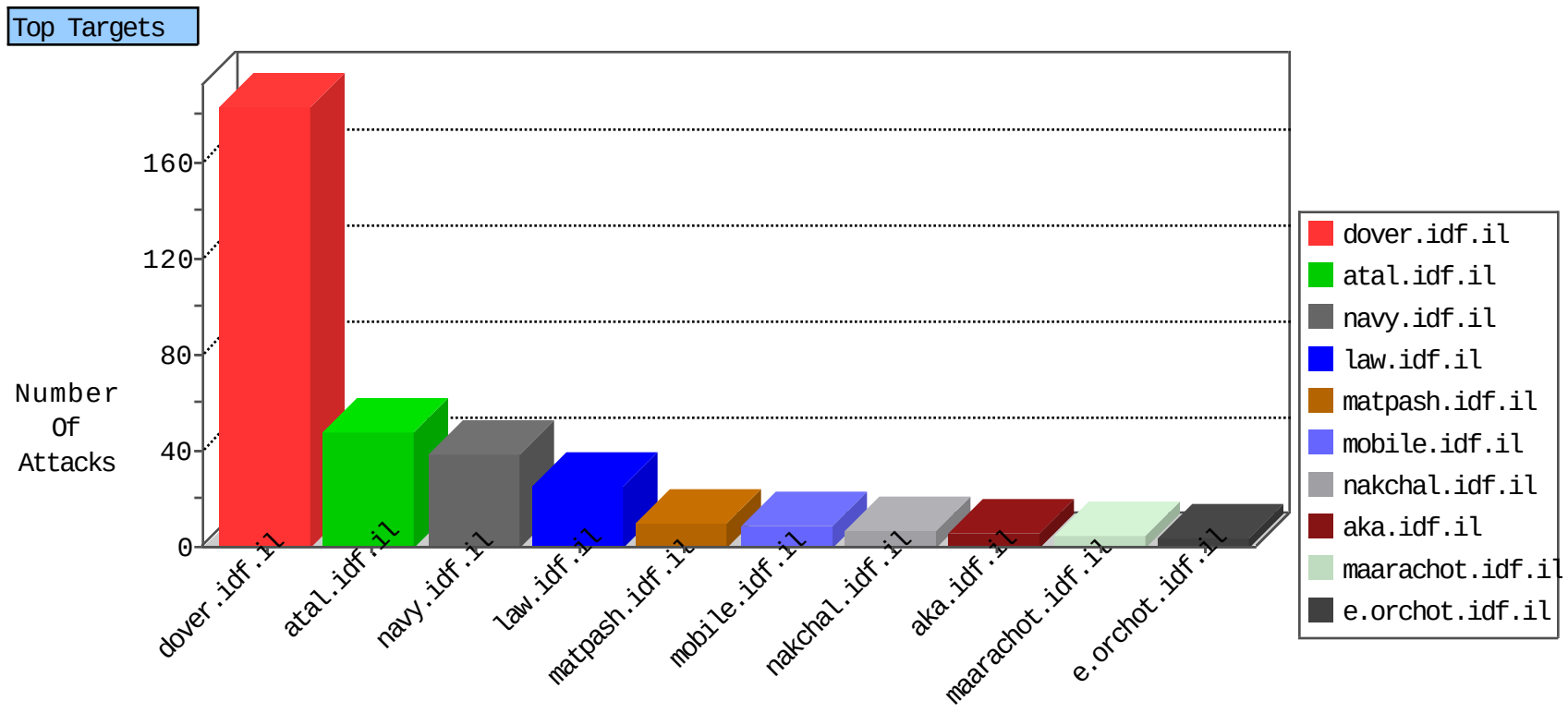
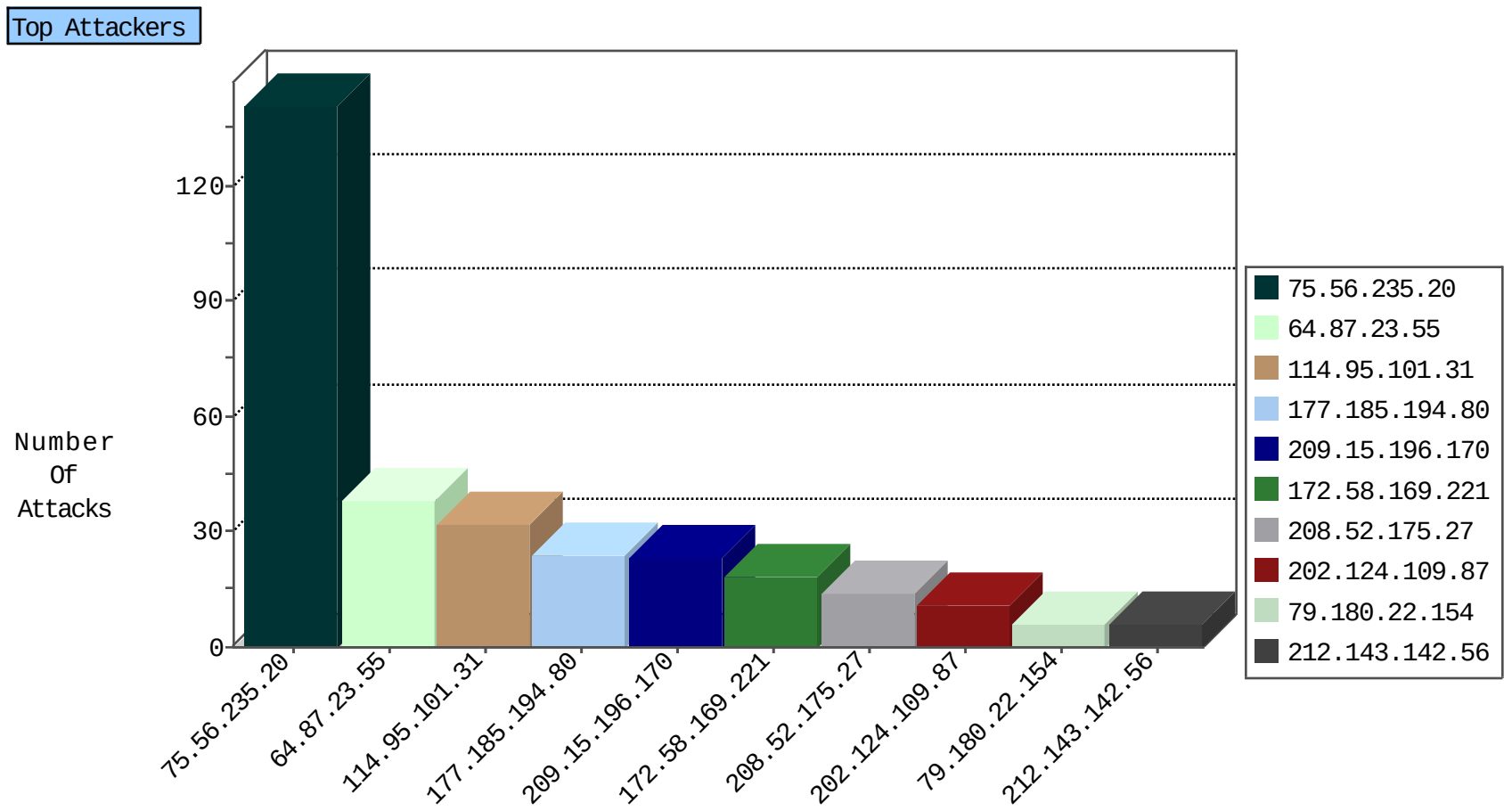
09-23-2016-03:04:06 to 09-23-2016-04:04:06

IDF Under Attack
Daily Report

Top Targets



Top Attackers



09-23-2016-03:04:06 to 09-23-2016-04:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
60.191.221.150	China	147.237.76.31	nakchal.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
185.94.111.1	Russian Federation	147.237.76.86	navy.idf.il	Black List	drop	1

09-23-2016-03:04:06 to 09-23-2016-04:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
75.56.235.20	United States	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	24
209.15.196.170	Canada	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
75.56.235.20	United States	147.237.77.216	dover.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
64.87.23.55	United States	147.237.76.86	navy.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
208.52.175.27	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
64.87.23.55	United States	147.237.76.86	navy.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
64.87.23.55	United States	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
177.185.194.80	Brazil	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
202.124.109.87	New Zealand	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
209.15.196.170	Canada	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	5
162.210.196.100	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
151.80.31.108	France	147.237.72.156	aman.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
190.44.30.152	Chile	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1

09-23-2016-03:04:06 to 09-23-2016-04:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
75.56.235.20	147.237.77.216	United States	dover.idf.il	SQL Injection - Select From	105
64.87.23.55	147.237.76.86	United States	navy.idf.il	SQL Injection - Select From	20
177.185.194.80	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	18
208.52.175.27	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
209.15.196.170	147.237.77.233	Canada	atal.idf.il	SQL Injection - Select From	6
202.124.109.87	147.237.77.233	New Zealand	atal.idf.il	SQL Injection - Select From	5
114.95.101.31	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	3
114.95.101.31	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	3
114.95.101.31	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
114.95.101.31	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	2
114.95.101.31	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	2
114.95.101.31	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
114.95.101.31	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
114.95.101.31	147.237.77.176	China	matpash.idf.il	ET SCAN Potential SSH Scan	1
114.95.101.31	147.237.77.74	China	law.idf.il	ET SCAN Potential SSH Scan	1
104.167.6.84	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
114.95.101.31	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
114.95.101.31	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
163.172.129.15	147.237.8.28	United Kingdom	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
114.95.101.31	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
125.213.243.10	147.237.76.198	Thailand	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
114.95.101.31	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
114.95.101.31	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	1
114.95.101.31	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
114.95.101.31	147.237.8.14	China	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
114.95.101.31	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
114.95.101.31	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
114.95.101.31	147.237.77.170	China	maarachot.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
163.172.129.15	147.237.8.46	United Kingdom	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
114.95.101.31	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
128.232.110.28	147.237.77.235	United Kingdom	sviva.idf.il	ET SCAN Potential SSH Scan	1
114.95.101.31	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
114.95.101.31	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1
114.95.101.31	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
114.95.101.31	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
114.95.101.31	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1

09-23-2016-03:04:06 to 09-23-2016-04:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
172.58.169.221	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	18
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
100.92.4.17		147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
93.238.200.226	Germany	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.146.229	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.22.154	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
73.232.243.122	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
83.130.64.6	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
83.130.64.6	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
46.19.86.56	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
141.212.122.60	United States	147.237.77.179	e.mazi.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
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
68.184.119.61	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
141.212.122.87	United States	147.237.0.33	idf.il	drop		drop	1
141.212.122.55	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
100.13.130.4	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.72	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
77.92.76.248	United Kingdom	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.88	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
46.19.86.56	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.60	United States	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.50	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
68.184.119.61	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
141.212.122.87	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.56	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
100.13.130.4	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.89	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.19.86.56	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.61	United States	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.51	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
100.13.130.4	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.88	United States	147.237.0.33	idf.il	drop		drop	1
141.212.122.57	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
80.246.136.79	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.89	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.86.56	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.61	United States	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.51	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
100.13.130.4	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.95	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.36	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.88	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.58	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.49	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.89	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
141.212.122.86	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.52	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
100.13.130.4	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

09-23-2016-03:04:06 to 09-23-2016-04:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.180.22.154	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	2
66.249.64.181	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
66.249.66.188	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/6/2726.jpg	Block	1
130.113.69.42	Canada	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.asp	Block	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
2.53.29.77	Israel	147.237.76.31	nakchal.idf.il	Parameter Type Violation search in www.nakhal.idf.il/1119-he/nakhal.aspx	Block	1
79.180.22.154	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	1

09-23-2016-03:04:06 to 09-23-2016-04:04:06