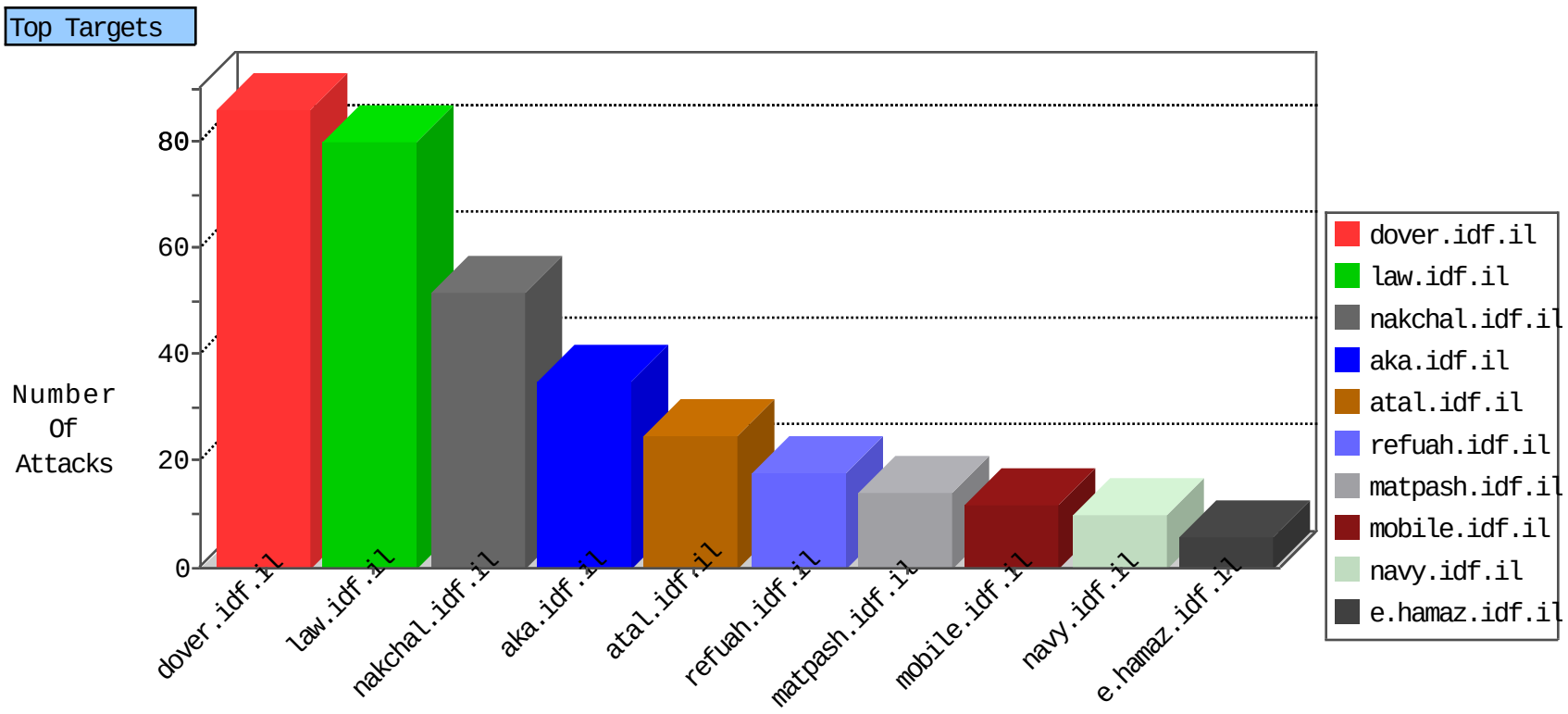
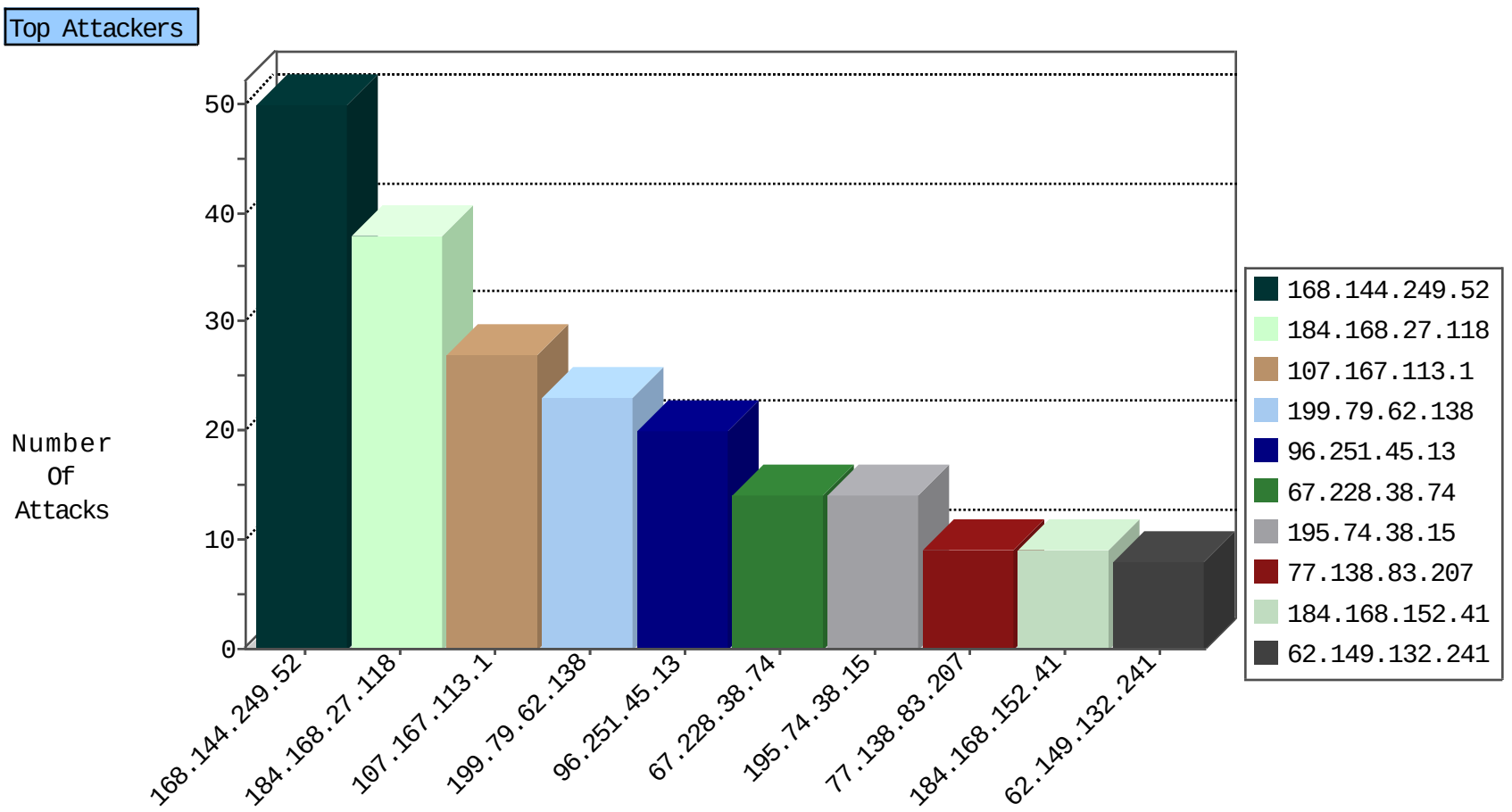
09-29-2016-05:04:08 to 09-29-2016-06:04:08

IDF Under Attack Daily Report





09-29-2016-05:04:08 to 09-29-2016-06:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.178.93.250	Israel	147.237.77.216	dover.idf.il	Black List	drop	2

09-29-2016-05:04:08 to 09-29-2016-06:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
168.144.249.52	Canada	147.237.76.31	nakchal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
184.168.27.118	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
184.168.27.118	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
168.144.249.52	Canada	147.237.76.31	nakchal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
67.228.38.74	United States	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
168.144.249.52	Canada	147.237.76.31	nakchal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
96.251.45.13	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
88.198.16.12	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3
199.79.62.138	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	3
46.4.123.172	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
199.58.86.206	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
125.208.24.2	China	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1

09-29-2016-05:04:08 to 09-29-2016-06:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
168.144.249.52	147.237.76.31	Canada	nakchal.idf.il	SQL Injection - Select From	26
184.168.27.118	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	20
96.251.45.13	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	16
195.74.38.15	147.237.77.216	Sweden	dover.idf.il	SQL Injection - Select From	14
199.79.62.138	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	9
184.168.152.41	147.237.77.176	United States	matpash.idf.il	SQL Injection - Select From	9
67.228.38.74	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	8
62.149.132.241	147.237.77.74	Italy	law.idf.il	SQL Injection - Select From	8
220.70.219.86	147.237.76.44	Korea, Republic of	e.refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
123.232.26.132	147.237.76.39	China	mobile.meitav.idf.i	ET SCAN NMAP -f -sS	1
221.229.172.116	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
58.56.98.132	147.237.76.39	China	mobile.meitav.idf.i	ET SCAN NMAP -f -sS	1
40.121.139.43	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
123.232.26.132	147.237.76.39	China	mobile.meitav.idf.i	ET SCAN NMAP -sS window 2048	1
115.79.215.249	147.237.72.167	Vietnam	ishurim.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
89.248.174.30	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
66.249.66.234	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
221.229.172.116	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
58.56.98.132	147.237.76.39	China	mobile.meitav.idf.i	ET SCAN NMAP -sS window 2048	1
50.116.123.33	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.169.150	147.237.76.31	United Kingdom	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1

09-29-2016-05:04:08 to 09-29-2016-06:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
107.167.113.1	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	27
77.138.83.207	France	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
64.50.250.94	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	6
199.79.62.138	United States	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
199.79.62.138	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
176.13.247.202	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
2.55.149.33	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
109.253.195.125	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.163.96	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
207.46.13.142	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.6.227.162	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
37.142.193.233	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
151.235.150.146	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
207.41.191.18	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
188.120.154.35	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
151.235.150.146	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
151.235.150.146	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.166.188.220	Netherlands	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
77.139.140.166	France	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
213.57.135.172	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
62.210.243.100	France	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
180.97.106.162	China	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
139.162.37.147	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
87.71.23.247	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
66.87.130.162	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
46.166.188.220	Netherlands	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
2.55.149.33	Israel	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	1
109.253.204.190	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	1
77.139.140.166	France	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
62.210.243.100	France	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
184.105.247.235	United States	147.237.0.35	akaws.idf.il	drop		drop	1
66.87.130.162	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
180.97.106.37	China	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
49.228.97.28	Thailand	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
5.22.134.72	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
109.253.209.74	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
79.176.19.12	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
62.210.243.100	France	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
37.142.193.233	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
2.55.149.33	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.14	United States	147.237.0.33	idf.il	drop		drop	1
61.136.195.22	China	147.237.0.33	idf.il	drop		drop	1
180.97.106.37	China	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
5.102.195.42	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
114.112.90.54	China	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
87.69.137.150	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
62.210.243.100	France	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
199.79.62.138	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
46.19.85.162	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

09-29-2016-05:04:08 to 09-29-2016-06:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.234.169	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	4
109.253.218.201	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.253.218.201	Block	3
84.95.208.20	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	3
112.198.77.58	Philippines	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	3
84.95.208.20	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
180.97.106.162	China	147.237.77.235	sviva.idf.il	Multiple Illegal Byte Code Character in Method from 180.97.106.162	Block	1
109.253.195.125	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/	Block	1
66.249.66.26	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
180.97.106.37	China	147.237.77.170	maarachot.idf.il	Illegal Byte Code Character in Method	Block	1
77.138.240.165	France	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
180.97.106.162	China	147.237.77.235	sviva.idf.il	Multiple NULL Character in Method from 180.97.106.162	Block	1
66.249.66.180	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/oref/	Block	1
180.97.106.37	China	147.237.77.170	maarachot.idf.il	NULL Character in Method	Block	1
66.249.64.11	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/modules/forums.frm/frmsendmessage.aspx	Block	1
199.30.25.63	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/scripts.asmx/getjs	Block	1
109.253.218.201	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/apple-touch-icon.png	Block	1
66.249.75.4	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9186-he/refuah.aspx	Block	1
180.97.106.162	China	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
66.249.64.64	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/asp/giyus.asp	Block	1
207.46.13.187	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
66.249.75.12	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8857-he/refuah.aspx	Block	1
180.97.106.162	China	147.237.77.216	dover.idf.il	Distributed NULL Character in Method	Block	1
84.95.208.20	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/general/piwik.php	Block	1
66.249.66.23	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1407-he/atal.aspx	Block	1
77.124.37.26	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/sachar/	Block	1

09-29-2016-05:04:08 to 09-29-2016-06:04:08