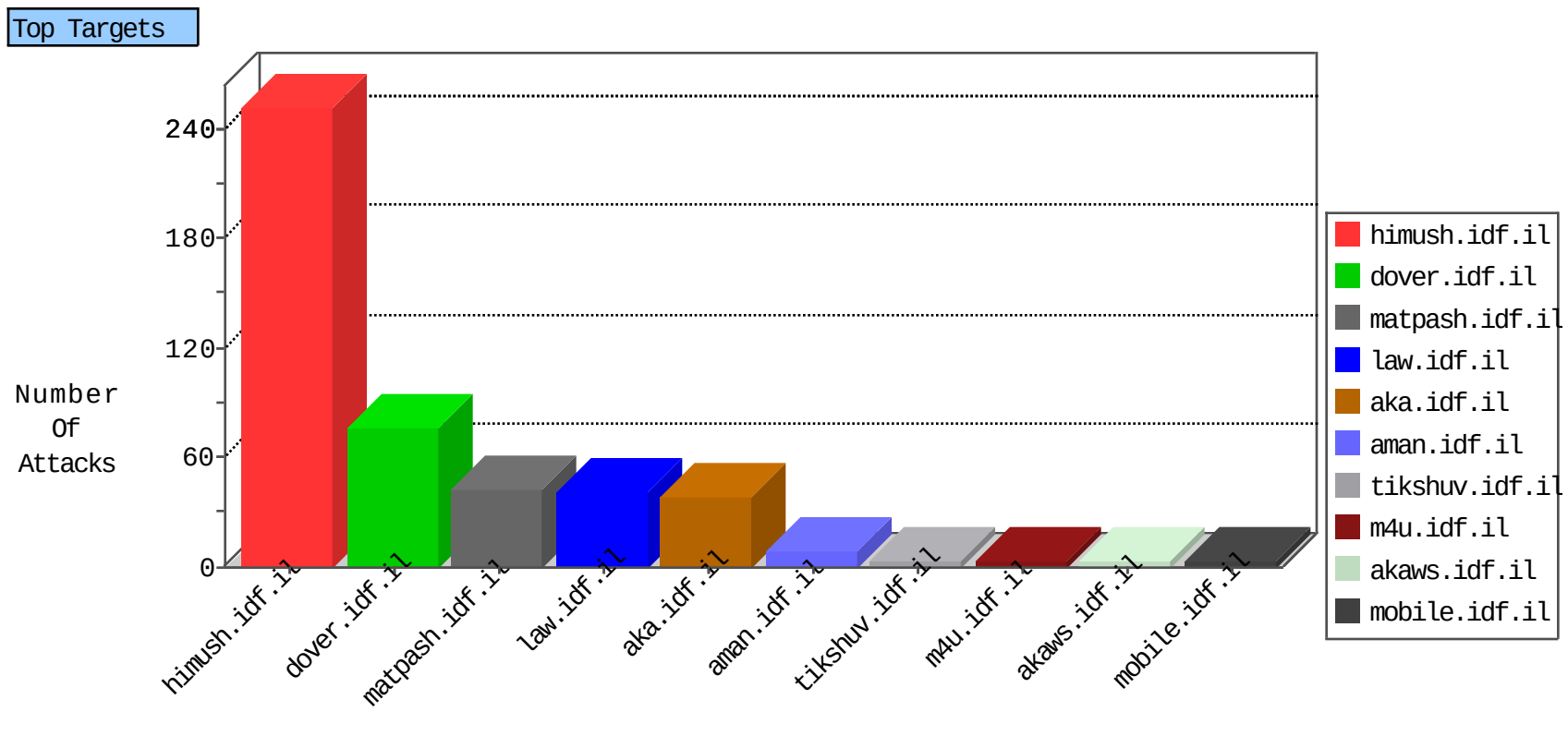
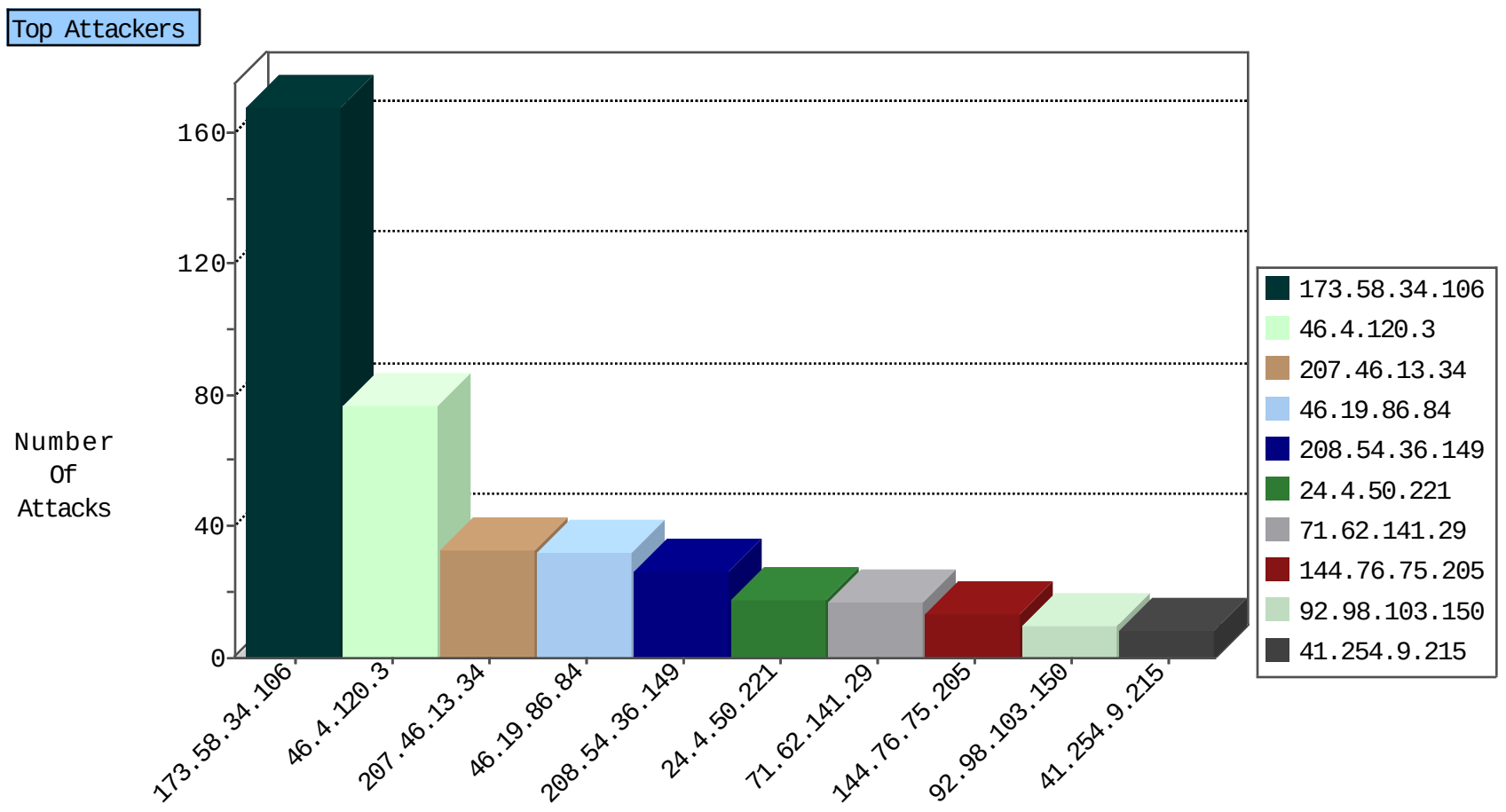
10-03-2016-02:04:05 to 10-03-2016-03:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-03-2016-02:04:05 to 10-03-2016-03:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.210.26.232	France	147.237.76.31	nakchal.idf.il	Black List	drop	1
94.177.164.99	Romania	147.237.76.44	e.refuah.idf.il	Black List	drop	1
173.208.203.10	United States	147.237.76.177	ncore.idf.il	Black List	drop	1
62.210.26.232	France	147.237.76.30	himush.idf.il	Black List	drop	1

10-03-2016-02:04:05 to 10-03-2016-03:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.4.120.3	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	38
46.4.120.3	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	24
46.4.120.3	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	13
46.4.120.3	Germany	147.237.77.234	halag.idf.il	C1000074: HTTP: majestic bot	Permit	2
151.80.41.169	France	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	1

10-03-2016-02:04:05 to 10-03-2016-03:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.254.9.215	147.237.77.216	Libyan Arab Jamahiriya	dover.idf.il	GPL WEB_SERVER /etc/passwd	4
41.254.9.215	147.237.77.216	Libyan Arab Jamahiriya	dover.idf.il	SQL Injection - Select From	4
91.121.142.227	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
172.242.41.105	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 4096	1
117.21.248.87	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
117.21.248.87	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
104.202.122.139	147.237.0.19	United States	madim.atal.idf.il	WEB-CGI redirect access	1
89.163.224.115	147.237.77.179	Germany	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
89.163.224.115	147.237.76.148	Germany	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
27.12.211.101	147.237.0.200	China	m4u.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
117.21.248.87	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
117.21.248.87	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
117.21.248.87	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
89.163.224.115	147.237.76.197	Germany	e.himush.idf.il	ET SCAN Potential SSH Scan	1
82.166.102.32	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

10-03-2016-02:04:05 to 10-03-2016-03:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
173.58.34.106	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	167
207.46.13.34	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	33
46.19.86.84	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
46.19.86.84	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
92.98.103.150	United Arab Emirates	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	10
84.108.201.51	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.86.84	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
208.54.36.149	United States	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	6
208.54.36.149	United States	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
66.102.9.149	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
24.4.50.221	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
208.54.36.149	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
208.54.36.149	United States	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	5
71.62.141.29	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
71.62.141.29	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
24.4.50.221	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
208.54.36.149	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
198.50.16.254	Argentina	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
71.62.141.29	United States	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	4
66.191.166.230	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
24.4.50.221	United States	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	4
24.4.50.221	United States	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
71.62.141.29	United States	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	3
144.76.75.205	Germany	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	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
144.76.75.205	Germany	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
144.76.75.205	Germany	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
31.13.100.114	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
144.76.75.205	Germany	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	2
109.253.213.202	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
144.76.75.205	Germany	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
89.138.110.206	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
46.19.85.189	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
89.139.171.215	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
31.13.100.112	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
79.180.14.91	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.86.40	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
109.253.201.46	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
89.248.174.4	Netherlands	147.237.0.35	akaws.idf.il	drop		drop	1
195.62.53.168	Russian Federation	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
169.229.3.91	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
52.198.122.46	Japan	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.105	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
89.248.174.4	Netherlands	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
169.229.3.91	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
109.253.202.120	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
89.248.174.4	Netherlands	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
169.229.3.91	United States	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
52.198.122.46	Japan	147.237.0.35	akaws.idf.il	drop		drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.139.171.215	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 89.139.171.215 (Open Mode)	None	1
173.231.185.150	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/admin/i18n/readme.txt	Block	1
66.249.64.103	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/	Block	1
89.139.171.215	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
207.46.13.42	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.66.196	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
104.236.122.34	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1
66.249.76.63	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/6/שקופית8	Block	1
148.251.192.100	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/ishurim/	Block	1
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/miluim/templates/inner.asp	Block	1
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/null	Block	1
173.231.185.150	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/admin/i18n/readme.txt	Block	1
66.102.6.3	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/sachar	Block	1