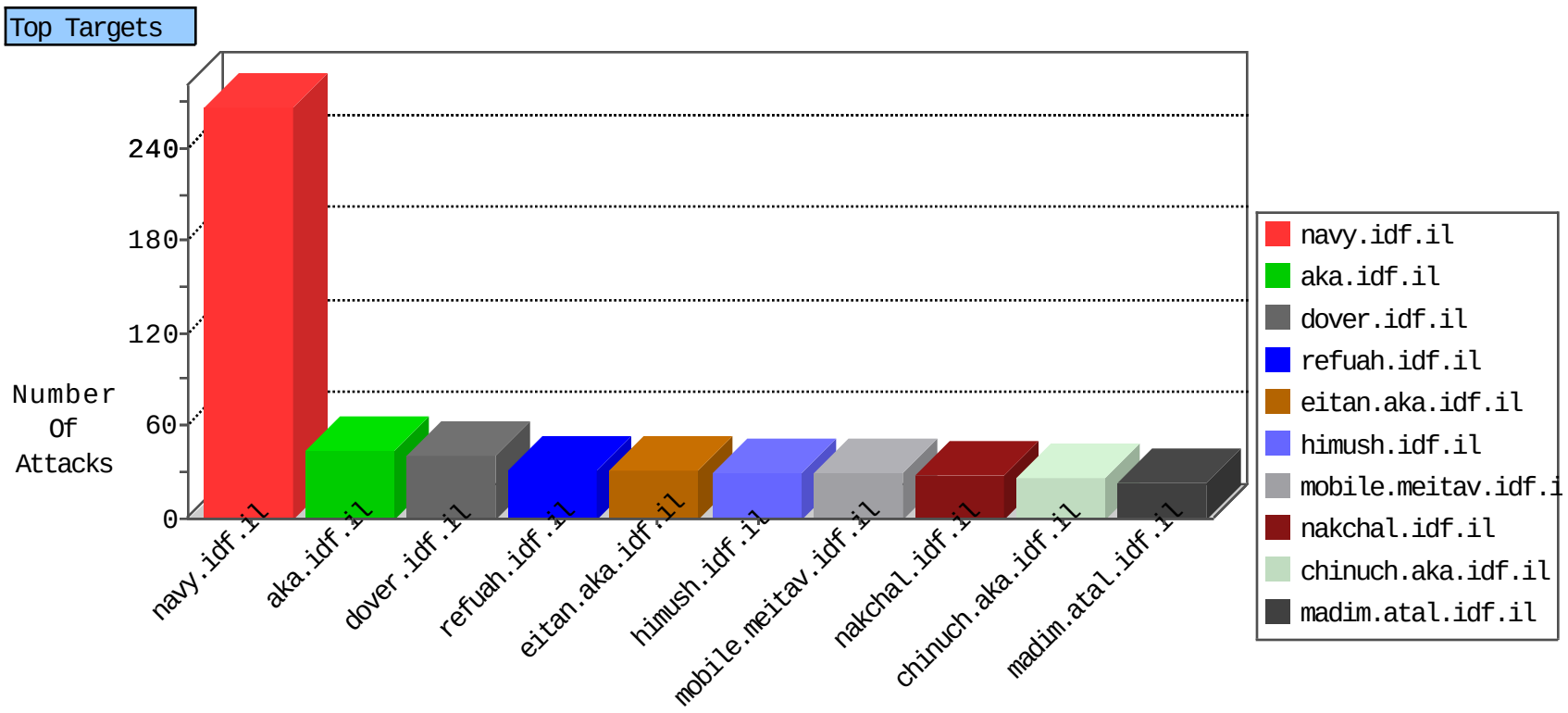
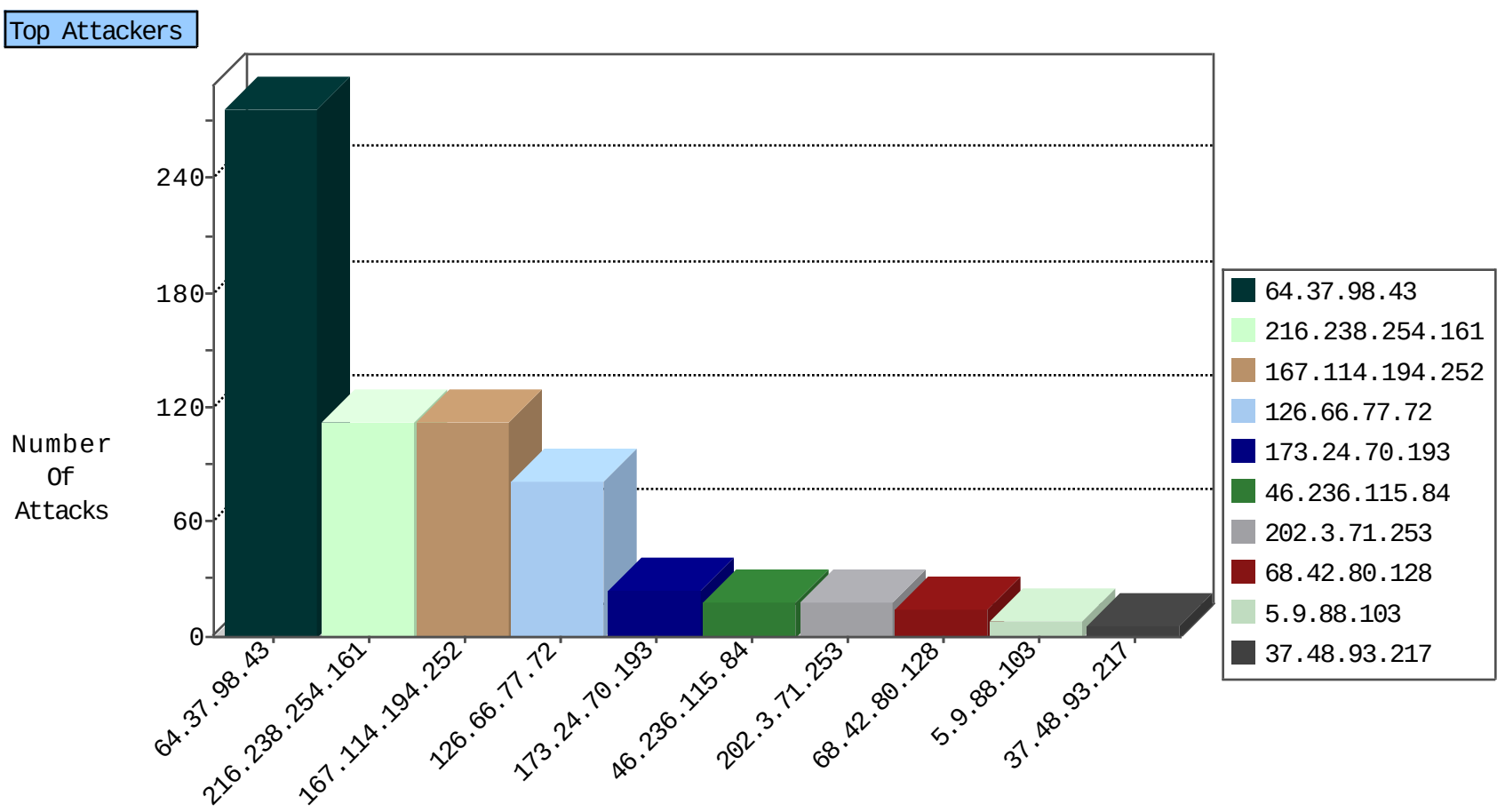
09-06-2016-05:04:07 to 09-06-2016-06:04:07

IDF Under Attack Daily Report





09-06-2016-05:04:07 to 09-06-2016-06:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.106.92.139	Germany	147.237.0.200	m4u.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1

09-06-2016-05:04:07 to 09-06-2016-06:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-06-2016-05:04:07 to 09-06-2016-06:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
91.121.221.160	147.237.77.74	France	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
203.128.177.68	147.237.77.170	Korea, Republic of	maarachot.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
139.162.13.205	147.237.77.226	Singapore	www.chamatz.aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
104.197.206.193	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 4096	1
104.197.206.193	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -f -sS	1
37.48.93.217	147.237.76.198	Netherlands	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
222.186.58.176	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
37.48.93.217	147.237.72.167	Netherlands	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
222.186.58.176	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
37.48.93.217	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
222.186.58.176	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
195.88.154.2	147.237.8.46	Russian Federation	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
106.186.20.183	147.237.76.38	Japan	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
104.197.206.193	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 2048	1
103.207.36.31	147.237.0.200	Vietnam	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
37.48.93.217	147.237.77.216	Netherlands	dover.idf.il	ET SCAN Potential SSH Scan	1
222.186.58.176	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
37.48.93.217	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.58.176	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
37.48.93.217	147.237.8.28	Netherlands	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
222.186.58.176	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1

09-06-2016-05:04:07 to 09-06-2016-06:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
216.238.254.161	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	113
126.66.77.72	Japan	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	81
173.24.70.193	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	24
46.236.115.84	Sweden	147.237.72.166	aka.idf.il	drop	SAM rule	drop	18
167.114.194.252	Canada	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
167.114.194.252	Canada	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
167.114.194.252	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
167.114.194.252	Canada	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
167.114.194.252	Canada	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
68.42.80.128	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
167.114.194.252	Canada	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
167.114.194.252	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
167.114.194.252	Canada	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
64.37.98.43	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
64.37.98.43	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
64.37.98.43	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
64.37.98.43	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
64.37.98.43	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
64.37.98.43	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
64.37.98.43	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
64.37.98.43	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
64.37.98.43	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
64.37.98.43	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
64.37.98.43	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
64.37.98.43	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
64.37.98.43	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
64.37.98.43	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
64.37.98.43	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
64.37.98.43	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
64.37.98.43	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
64.37.98.43	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
64.37.98.43	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
64.37.98.43	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
64.37.98.43	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
64.37.98.43	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
67.253.251.158	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
5.9.88.103	Germany	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
64.231.75.63	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
5.9.88.103	Germany	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	2
207.46.13.32	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
202.3.71.253	Thailand	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
5.9.88.103	Germany	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	2
202.3.71.253	Thailand	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
202.3.71.253	Thailand	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
5.9.88.103	Germany	147.237.77.233	atal.idf.il	drop	SAM rule	drop	2
202.3.71.253	Thailand	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
46.19.86.40	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP anomaly detected	Non-compliant TCP packets coming from multiple external sources were detected. This may result from potential network configuration problem.	drop	1
128.232.110.28	United Kingdom	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	1
202.3.71.253	Thailand	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1

09-06-2016-05:04:07 to 09-06-2016-06:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.2.169	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
109.253.206.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.69.97	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/2/242.doc	Block	1
207.182.140.210	United States	147.237.76.42	refuah.idf.il	Unauthorized Method POST for 147.237.76.42/	Block	1
76.185.108.254	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/ishurim/main/	Block	1
139.162.13.205	Singapore	147.237.77.226	www.chamatz.aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.69.101	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/365-he/patzar.aspx	Block	1
213.57.98.207	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
77.125.67.242	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
144.76.96.81	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
40.77.167.52	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/logi	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/library/generaldoc.asp	Block	1
139.162.13.205	Singapore	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.102.8.217	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
204.79.180.16	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	1
71.196.2.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.idf.il/1038-en/dover.aspx	Block	1
139.162.13.205	Singapore	147.237.77.226	www.chamatz.aka.idf.il	Multiple Untraceable SSL Sessions from 139.162.13.205 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1

09-06-2016-05:04:07 to 09-06-2016-06:04:07