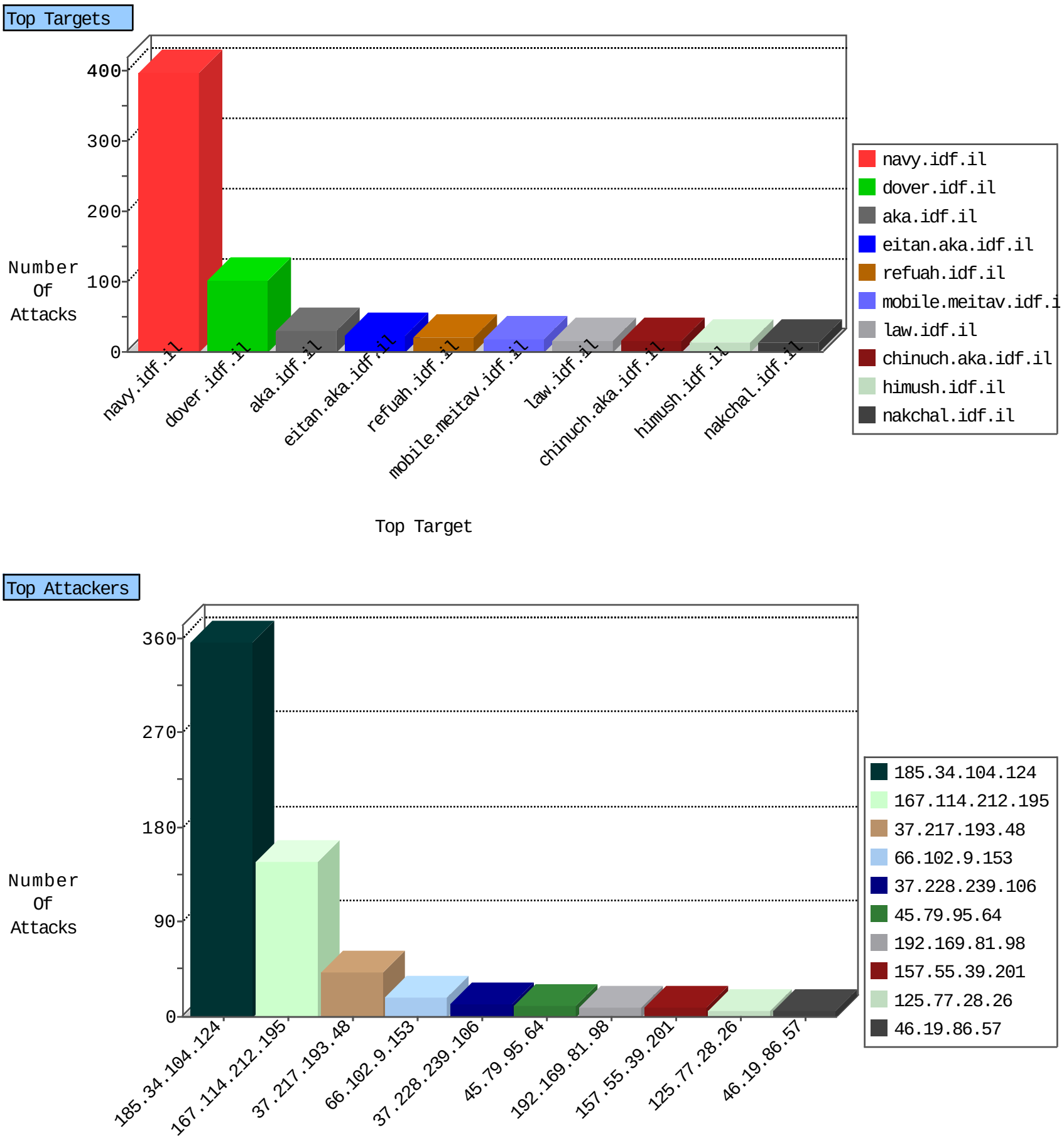
09-05-2016-02:04:05 to 09-05-2016-03:04:05

IDF Under Attack Daily Report



09-05-2016-02:04:05 to 09-05-2016-03:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.102.9.147	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9
139.162.13.205	Singapore	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	forward	2
109.236.84.10	Netherlands	147.237.76.200	eitan.aka.idf.il	Black List	drop	1

09-05-2016-02:04:05 to 09-05-2016-03:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-05-2016-02:04:05 to 09-05-2016-03:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.102.9.153	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	19
151.80.41.178	147.237.77.74	France	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
91.121.220.181	147.237.77.74	France	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
45.79.95.64	147.237.77.74	United States	law.idf.il	WEB-MISC Chunked-Encoding transfer attempt	2
151.80.41.177	147.237.77.74	France	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
104.197.206.193	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 2048	1
94.102.56.233	147.237.76.197	Netherlands	e.himush.idf.il	ET SCAN Potential SSH Scan	1
66.249.76.117	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
46.172.71.251	147.237.8.45	Ukraine	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
120.72.107.42	147.237.0.35	Vietnam	akaws.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
104.197.206.193	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 3072	1
104.197.206.193	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -f -sS	1
221.204.249.157	147.237.76.200	China	eitan.aka.idf.i	ET SCAN NMAP -sS window 1024	1
110.6.192.116	147.237.8.46	China	e.chinuch.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

09-05-2016-02:04:05 to 09-05-2016-03:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
185.34.104.124	Ireland	147.237.76.86	navy.idf.il	SYN Attack		monitor	221
185.34.104.124	Ireland	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	94
185.34.104.124	Ireland	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	42
37.217.193.48	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
167.114.212.195	Canada	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
167.114.212.195	Canada	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
167.114.212.195	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
167.114.212.195	Canada	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
167.114.212.195	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
167.114.212.195	Canada	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
167.114.212.195	Canada	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
167.114.212.195	Canada	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
157.55.39.201	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.228.239.106	Ireland	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
37.228.239.106	Ireland	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
167.114.212.195	Canada	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
167.114.212.195	Canada	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
131.253.25.143	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
167.114.212.195	Canada	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
66.102.9.149	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
87.69.255.212	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
66.249.76.2	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
167.114.212.195	Canada	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
167.114.212.195	Canada	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
167.114.212.195	Canada	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
157.55.39.150	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
167.114.212.195	Canada	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
167.114.212.195	Canada	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.86.57	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
167.114.212.195	Canada	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.86.57	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
223.62.16.178	Korea, Republic of	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
167.114.212.195	Canada	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
167.114.212.195	Canada	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
167.114.212.195	Canada	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
167.114.212.195	Canada	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
167.114.212.195	Canada	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
24.181.197.210	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
167.114.212.195	Canada	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
167.114.212.195	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
223.62.16.48	Korea, Republic of	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.102.9.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
167.114.212.195	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
167.114.212.195	Canada	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
167.114.212.195	Canada	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
84.236.167.27	Spain	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
109.66.139.232	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
24.59.63.96	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1

09-05-2016-02:04:05 to 09-05-2016-03:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
101.167.226.88	Australia	147.237.77.216	dover.idf.i	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
109.67.193.131	Israel	147.237.77.216	dover.idf.i	PHP Attempt	Block	1
66.249.69.83	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	Block	1
45.79.95.64	United States	147.237.77.74	law.idf.il	Multiple Malformed URL from 45.79.95.64	Block	1
77.138.11.23	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
45.79.95.64	United States	147.237.77.216	dover.idf.i	Multiple Malformed URL from 45.79.95.64	Block	1
109.67.193.131	Israel	147.237.77.216	dover.idf.i	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
66.249.76.47	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/iturim/asp/list.asp	Block	1
45.79.95.64	United States	147.237.77.74	law.idf.il	Multiple Unknown HTTP Request Method from 45.79.95.64	Block	1
95.84.159.144	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/kiosk/printablekiosk.aspx	Block	1
45.79.95.64	United States	147.237.77.216	dover.idf.i	Multiple Unknown HTTP Request Method from 45.79.95.64	Block	1
157.55.39.71	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	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
45.79.95.64	United States	147.237.77.216	dover.idf.i	Malformed HTTP Header Line 2	Block	1
101.167.226.86	Australia	147.237.77.216	dover.idf.i	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
45.79.95.64	United States	147.237.77.216	dover.idf.i	Unknown HTTP Request Method 1 in URL	Block	1
157.55.39.115	United States	147.237.77.216	dover.idf.i	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.76.116	Israel	147.237.77.216	dover.idf.i	Unauthorized URL Access to 147.237.77.216/1133-21969-he/idfgdover.aspx	Block	1
45.79.95.64	United States	147.237.77.216	dover.idf.i	Malformed URL	Block	1
66.249.66.177	Israel	147.237.77.216	dover.idf.i	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
45.79.95.64	United States	147.237.77.74	law.idf.il	Multiple Malformed HTTP Header Line from 45.79.95.64	Block	1
66.249.76.117	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
45.79.95.64	United States	147.237.77.216	dover.idf.i	Multiple Malformed HTTP Header Line from 45.79.95.64	Block	1

09-05-2016-02:04:05 to 09-05-2016-03:04:05