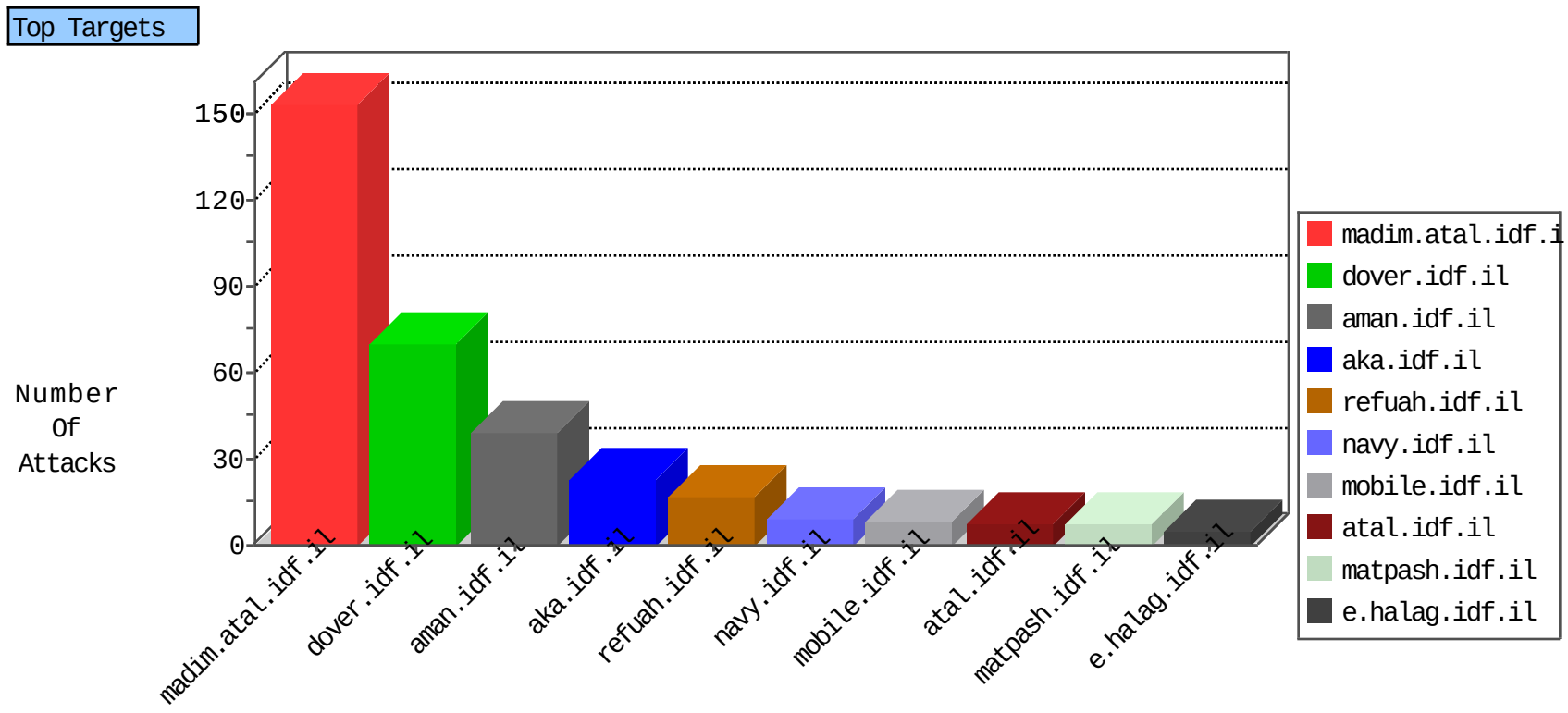
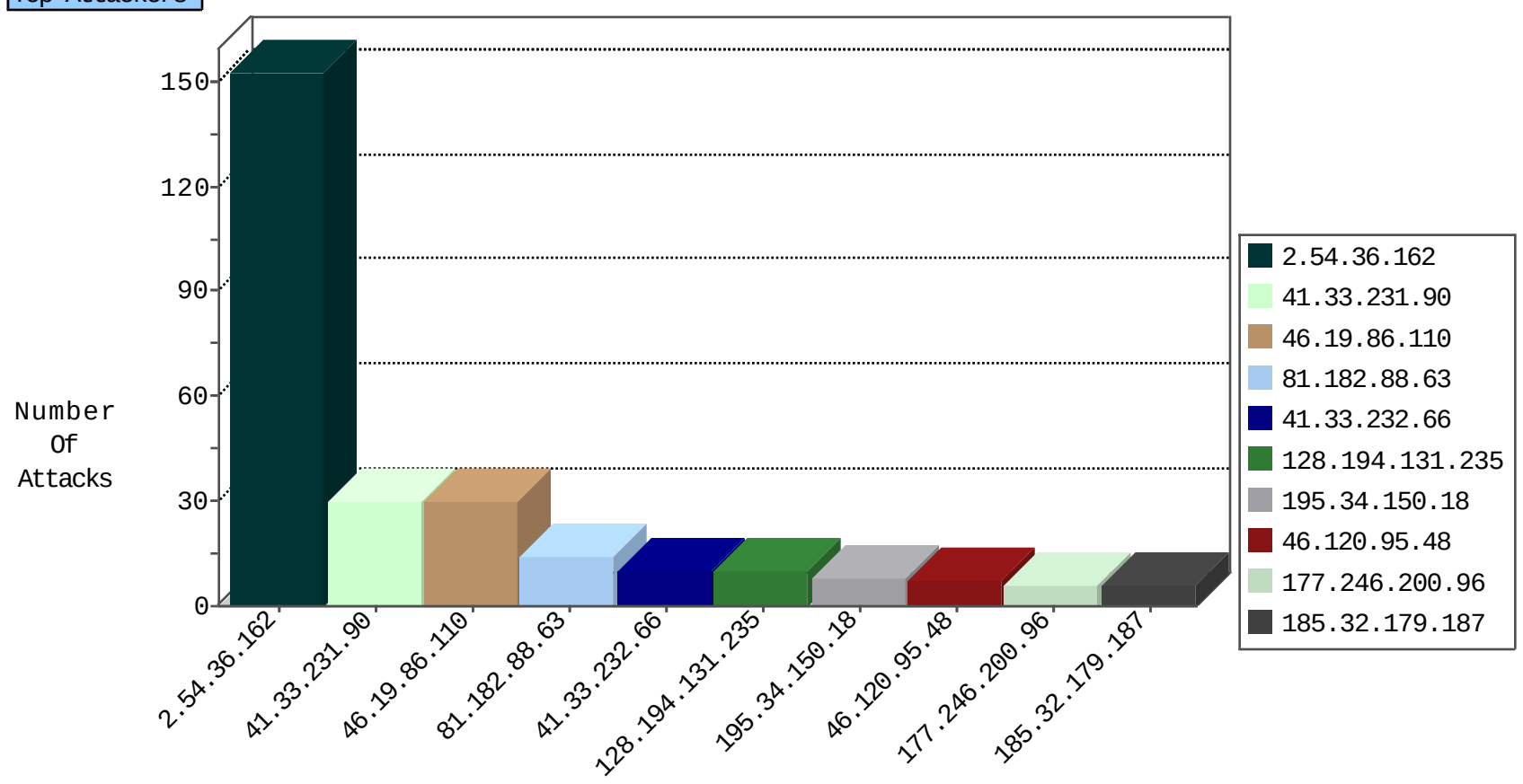
02-09-2016-03:04:07 to 02-09-2016-04:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-09-2016-03:04:07 to 02-09-2016-04:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
204.42.253.130	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	2
203.171.173.96	Korea, Republic of	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
142.54.160.214	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	drop	1
159.122.252.41	Netherlands	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1

02-09-2016-03:04:07 to 02-09-2016-04:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
95.211.213.213	Netherlands	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
172.246.104.194	United States	147.237.77.233	atal.idf.il	0543: HTTP: php.cgi Access	Block	1

02-09-2016-03:04:07 to 02-09-2016-04:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
218.246.0.97	147.237.76.86	China	navy.idf.il	ET SCAN NMAP -sS window 1024	1
218.108.132.58	147.237.76.34	China	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.171.131	147.237.77.216	Netherlands	dover.idf.il	ET SCAN NMAP -sS window 1024	1
81.182.88.63	147.237.76.199	Hungary	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
46.45.137.67	147.237.76.196	Turkey	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
218.108.132.58	147.237.76.42	China	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.171.131	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
46.45.137.67	147.237.76.202	Turkey	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1

02-09-2016-03:04:07 to 02-09-2016-04:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.86.110	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
46.120.95.48	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
81.182.88.63	Hungary	147.237.76.42	refuah.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	6
185.32.179.187	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
128.194.131.235	United States	147.237.72.166	aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
177.246.200.96	Mexico	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
128.194.131.235	United States	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
46.19.85.122	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	3
66.249.78.216	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.136.123	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.182.88.63	Hungary	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
217.69.133.68	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
45.63.97.227		147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
46.19.85.130	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.121.38	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
155.94.254.143	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
73.134.180.83	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.121.39	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
45.63.97.227		147.237.77.74	law.idf.il	drop	SAM rule	drop	1
137.116.71.170	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.15	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	1
141.212.121.44	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
81.182.88.63	Hungary	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
45.63.97.227		147.237.77.233	atal.idf.il	drop	SAM rule	drop	1
178.33.126.108	France	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
137.116.71.170	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.45.137.67	Turkey	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.82	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.121.46	United States	147.237.76.177	ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
128.194.131.235	United States	147.237.72.156	aman.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
68.81.38.133	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.81	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
81.182.88.63	Hungary	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
46.45.137.67	Turkey	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.82	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
45.63.97.227		147.237.72.156	aman.idf.il	drop	SAM rule	drop	1
141.212.121.47	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
73.134.180.83	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1

02-09-2016-03:04:07 to 02-09-2016-04:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.36.162	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.36.162	Block	113
2.54.36.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
172.246.104.194	United States	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 172.246.104.194	Block	3
80.246.136.123	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
188.143.232.11	Russian Federation	147.237.77.176	matpash.idf.il	Parameter Type Violation fromDate in www.cogat.idf.il/901-en/cogat.aspx	Block	2
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-he/cogat.aspx	Block	1
45.64.133.78	Bangladesh	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
188.143.232.11	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1283-en/dover.aspx	Block	1
81.182.88.63	Hungary	147.237.76.42	refuah.idf.il	Malformed URL towards	Block	1
66.249.66.26	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
172.246.104.194	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/cgi-bin/php	Block	1
74.82.47.3	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
45.64.133.78	Bangladesh	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
96.36.149.75	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.idf.il/1038-en/dover.aspx	Block	1
66.249.79.105	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
177.246.200.96	Mexico	147.237.72.156	aman.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
47.32.117.21	Canada	147.237.77.216	dover.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 47.32.117.21	Block	1
207.46.13.142	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
128.194.131.235	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
66.249.79.218	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
177.246.200.96	Mexico	147.237.72.166	aka.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
81.182.88.63	Hungary	147.237.76.42	refuah.idf.il	Abnormally Long Request request version	Block	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx	Block	1
212.106.77.59	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
166.170.5.107	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/en	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1815-he/dover.aspx	Block	1
8.37.70.72	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he/dover.aspx&usg=alkjrhgrl3l5pe0mum8-e-y8r0wqik3lug	Block	1
81.182.88.63	Hungary	147.237.76.42	refuah.idf.il	Illegal HTTP Version the green fields outside. Watch the goats chewing the grass. What is the meaning of life? Life isn't about getting to the end. Goats know this. You should know too. Goats are wise. Goats are cute. Listen to them! This is the message. Love goats, love the Internet! ðŸ?? Kecske. HTTP/1.0	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/http:/www.idf.il/english/	Block	1

02-09-2016-03:04:07 to 02-09-2016-04:04:07