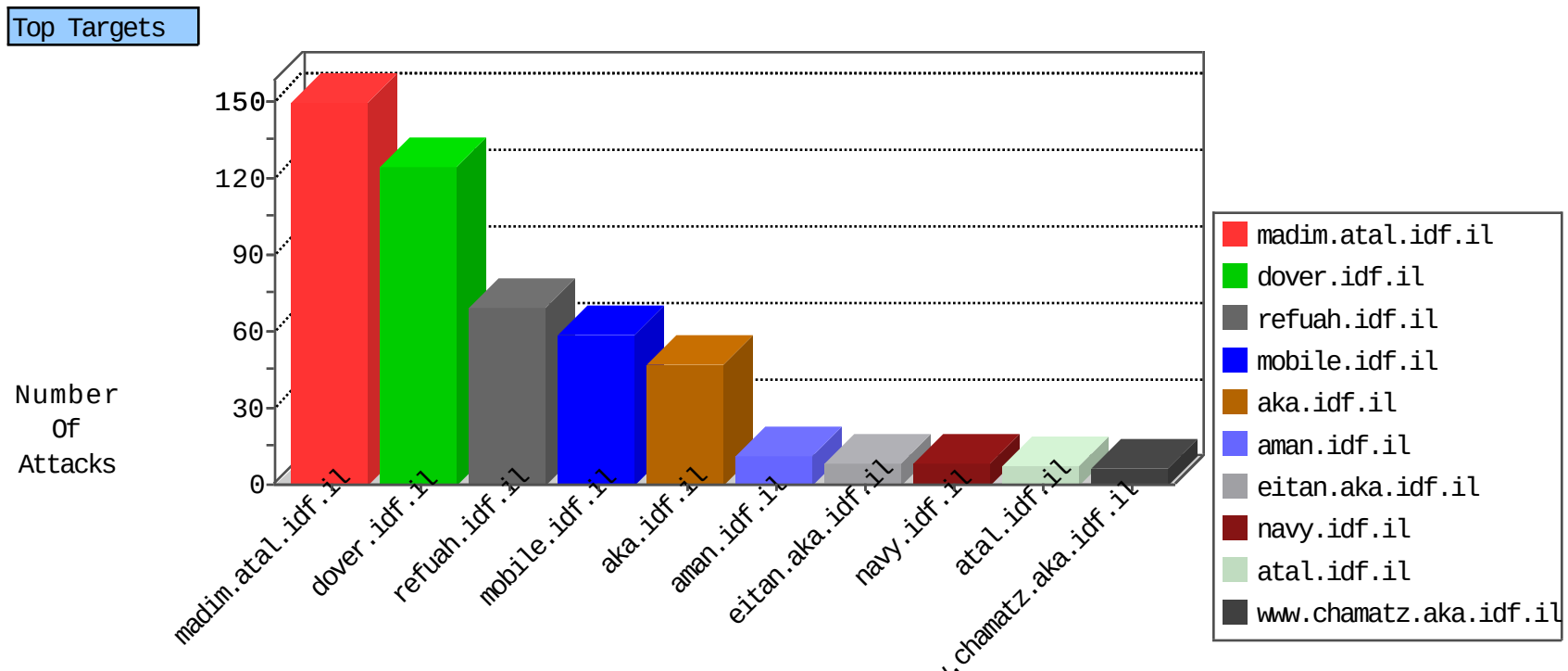
10-02-2016-03:04:09 to 10-02-2016-04:04:09

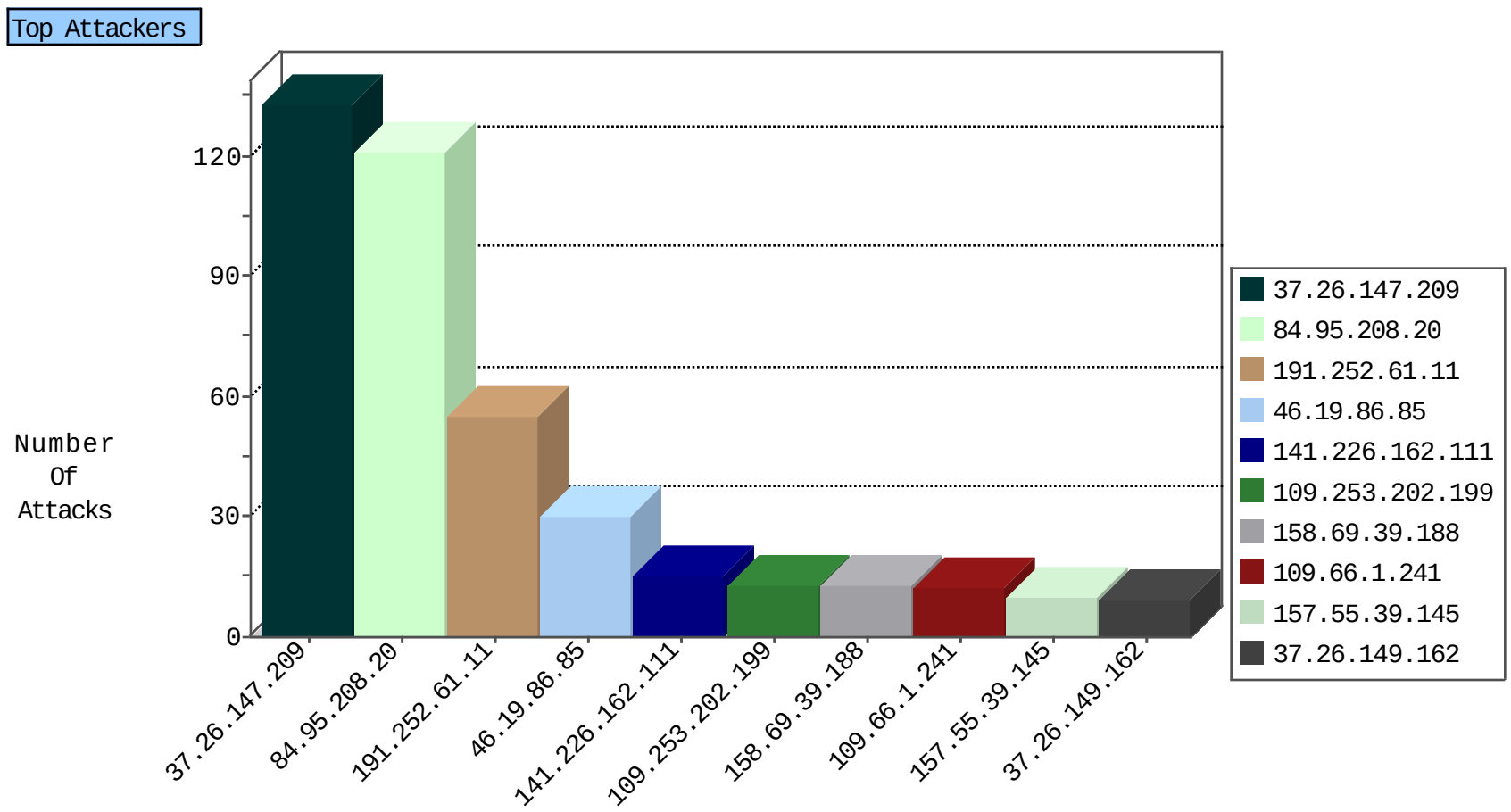
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

10-02-2016-03:04:09 to 10-02-2016-04:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
124.173.113.45	China	147.237.77.212	e.dover.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1

10-02-2016-03:04:09 to 10-02-2016-04:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-02-2016-03:04:09 to 10-02-2016-04:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
5.255.90.133	147.237.72.167	Netherlands	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
208.100.26.228	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.194	147.237.72.167	Netherlands	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.72.156	Ukraine	aman.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.72.156	Ukraine	aman.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
50.116.123.33	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
14.219.67.91	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
180.213.5.205	147.237.72.166	China	aka.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.72.156	Ukraine	aman.idf.il	ET SCAN NMAP -sS window 2048	1
91.201.236.155	147.237.72.156	Ukraine	aman.idf.il	ET SCAN NMAP -f -sS	1
52.6.235.156	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
50.116.123.33	147.237.72.156	United States	aman.idf.il	ET SCAN NMAP -sS window 1024	1

10-02-2016-03:04:09 to 10-02-2016-04:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.86.85	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
157.55.39.145	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
141.226.162.111	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
191.252.61.11	Brazil	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	9
191.252.61.11	Brazil	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.255	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
191.252.61.11	Brazil	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	7
191.252.61.11	Brazil	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
207.46.13.98	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
141.226.162.111	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.53.28.20	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
191.252.61.11	Brazil	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
109.66.1.241	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
109.253.202.199	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
109.66.1.241	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
109.253.202.199	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
191.252.61.11	Brazil	147.237.76.42	refuah.idf.il	Bad TCP sequence		monitor	4
191.252.61.11	Brazil	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	4
109.66.1.241	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
109.253.202.199	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
191.252.61.11	Brazil	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
191.252.61.11	Brazil	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
46.133.75.102	Ukraine	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
158.69.39.188	United States	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	3
2.53.15.110	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
191.252.61.11	Brazil	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid sequence number	alert	3
158.69.39.188	United States	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
151.15.23.72	Italy	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
158.69.39.188	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
151.15.23.72	Italy	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
158.69.39.188	United States	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	2
216.145.11.94	United States	147.237.0.15	kosher-kravi.idf.i	Header Rejection	header rejection pattern found in request	monitor	2
141.226.217.223	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
158.69.39.188	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
46.19.86.167	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
191.252.61.11	Brazil	147.237.76.42	refuah.idf.il	SYN Attack		monitor	2
2.55.14.166	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.120.122.219	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
192.154.111.98	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
74.82.47.23	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
163.172.220.201	United Kingdom	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	SQL Injection	SQL injection detected in URL: 'concat'	monitor	1
169.229.3.91	United States	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
195.62.53.168	Russian Federation	147.237.0.35	akaws.idf.il	drop		drop	1
74.82.47.23	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
163.172.220.201	United Kingdom	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.86.33	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Command Injection	command injection detected in URL: 'replace'	monitor	1

10-02-2016-03:04:09 to 10-02-2016-04:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.147.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	133
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	81
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	11
37.26.149.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	5
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	5
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	4
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
176.13.9.1	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.27.106.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
82.145.211.186	Europe	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/	Block	2
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.51	Block	2
66.249.65.185	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8803-he/refuah.aspx	Block	1
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	1
79.178.59.75	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.66.201	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list2005b.htm	Block	1
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/div.item	Block	1
66.249.66.206	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
40.77.169.100	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-16898-he/dover.aspx idf spokesperson	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/piwik.php	Block	1
68.180.229.62	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	1
68.180.230.181	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/templates/shared/usercontrols/headerupper/	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1

10-02-2016-03:04:09 to 10-02-2016-04:04:09