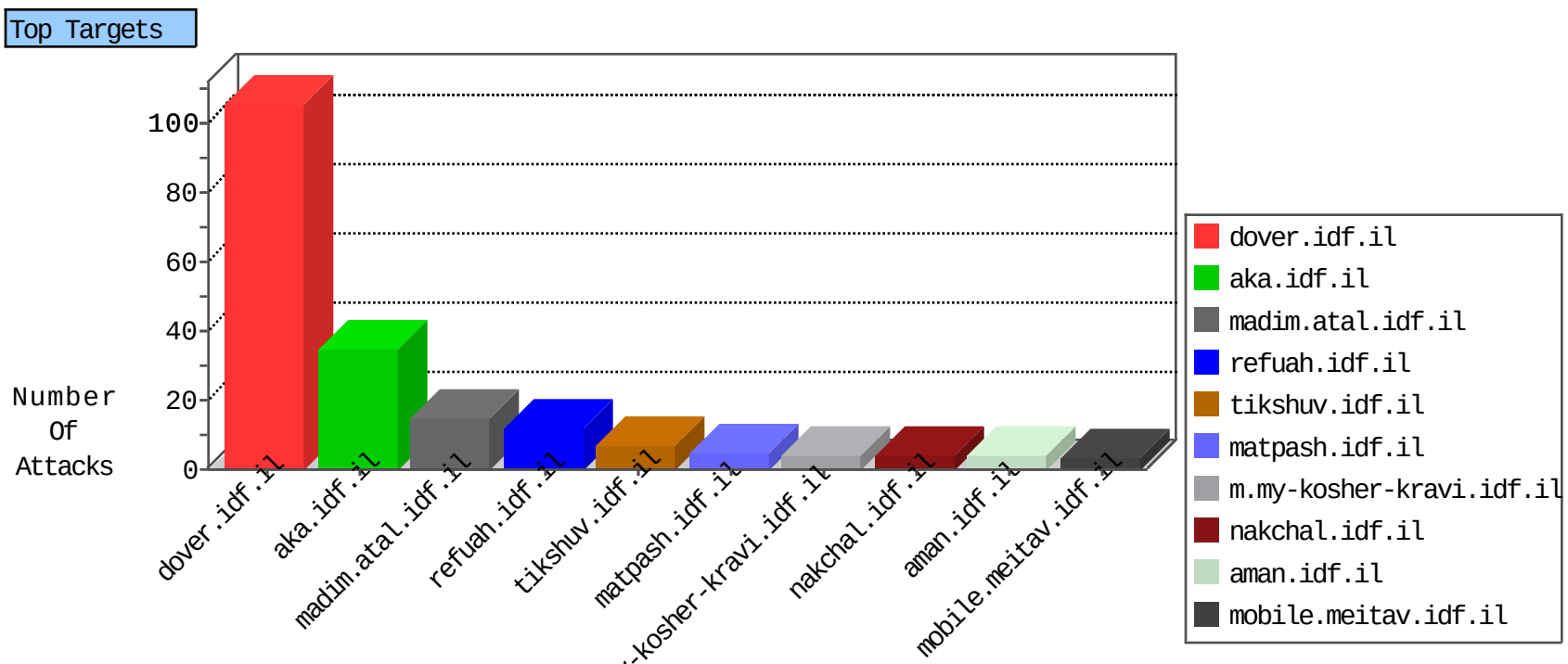
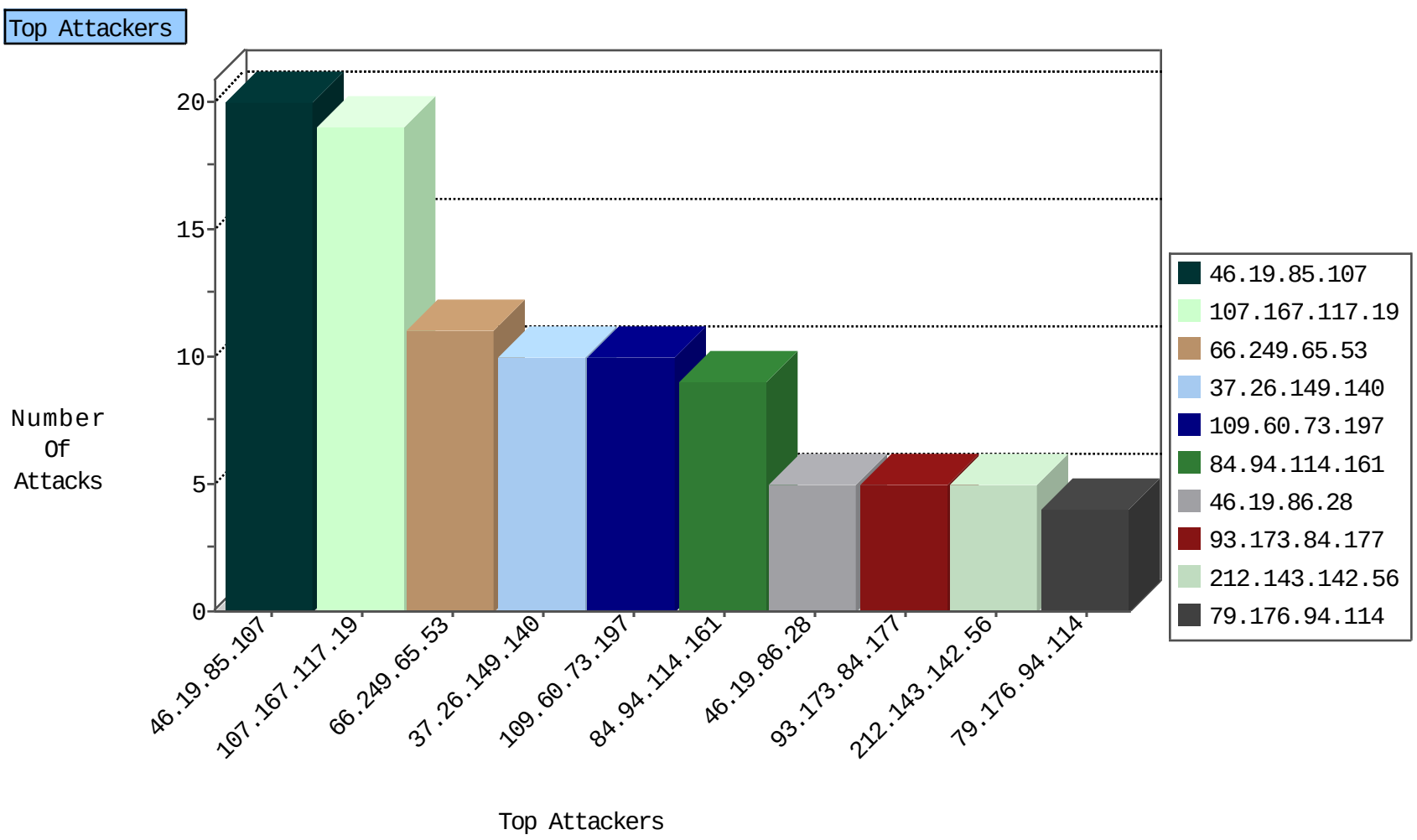
10-04-2016-00:04:07 to 10-04-2016-01:04:07

IDF Under Attack
Daily Report

Top Targets



Top Attackers



10-04-2016-00:04:07 to 10-04-2016-01:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.60.73.197	Croatia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	18
195.62.53.168	Russian Federation	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	2
208.100.32.119	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
208.100.32.116	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
208.100.32.121	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
208.100.32.117	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
128.242.249.12	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
208.100.32.118	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

10-04-2016-00:04:07 to 10-04-2016-01:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-04-2016-00:04:07 to 10-04-2016-01:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	2
54.90.189.128	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
213.42.28.185	147.237.77.212	United Arab Emirates	e.dover.idf.il	ET SCAN NMAP -sS window 2048	1
18.85.22.237	147.237.77.74	United States	law.idf.il	Tehila - Perl LWP with fake user agent	1
180.213.5.205	147.237.76.200	China	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
109.236.86.32	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.158	147.237.76.31	Ukraine	nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
91.201.236.158	147.237.76.31	Ukraine	nakchal.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
89.163.224.115	147.237.76.38	Germany	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
89.163.224.115	147.237.72.156	Germany	aman.idf.il	ET SCAN Potential SSH Scan	1
222.114.255.132	147.237.77.216	Korea, Republic of	dover.idf.il	portscan: TCP Distributed Portscan	1
62.219.128.187	147.237.76.42	Israel	refuah.idf.il	ET SCAN NMAP -sA (2)	1
213.42.28.185	147.237.77.212	United Arab Emirates	e.dover.idf.il	ET SCAN NMAP -sS window 4096	1
213.42.28.185	147.237.77.212	United Arab Emirates	e.dover.idf.il	ET SCAN NMAP -f -sS	1
121.223.248.67	147.237.0.34	Australia	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.158	147.237.76.31	Ukraine	nakchal.idf.il	ET SCAN NMAP -sS window 3072	1
91.201.236.158	147.237.76.31	Ukraine	nakchal.idf.il	ET SCAN NMAP -f -sS	1
89.163.224.115	147.237.76.196	Germany	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
89.163.224.115	147.237.76.34	Germany	yohalan.idf.il	ET SCAN Potential SSH Scan	1
69.129.141.35	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
216.81.230.167	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1

10-04-2016-00:04:07 to 10-04-2016-01:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
107.167.117.19	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	19
66.249.65.53	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	11
46.19.85.107	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.19.85.107	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
84.94.114.161	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
46.19.86.28	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
109.60.73.197	Croatia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
93.173.84.177	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
207.46.13.58	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
185.6.19.55	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
79.176.94.114	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
188.120.154.41	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.253.208.255	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
84.94.114.161	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
92.2.50.155	United Kingdom	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.133	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.85.110	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
92.2.50.155	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
157.55.39.41	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
24.222.178.200	Canada	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.86.22	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
157.55.39.49	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
83.216.94.137	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
77.138.234.231	France	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
89.197.128.154	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
176.13.231.91	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
31.210.187.150	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
77.138.234.231	France	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
109.253.215.43	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
2.53.154.26	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
79.180.131.114	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
185.3.147.87	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
37.133.249.120	Spain	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
79.176.85.76	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.226.162.125	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
23.101.61.176	Ireland	147.237.72.156	aman.idf.il	drop	SAM rule	drop	1
79.181.6.82	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.120.122.219	Israel	147.237.77.74	law.idf.il	Command Injection	command injection detected in URL: 'label'	monitor	1
185.3.147.163	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.68	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
109.60.73.197	Croatia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
89.139.105.22	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
79.176.85.76	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
46.19.85.139	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
93.172.107.154	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
79.181.6.82	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
185.6.19.55	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
46.19.85.88	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
109.60.73.197	Croatia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

10-04-2016-00:04:07 to 10-04-2016-01:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.149.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
37.26.146.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.138.157.248	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/booklets.aspx	Block	3
51.171.108.65	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/	Block	2
66.249.76.54	Israel	147.237.0.17	m.my-kosher-kravi .idf.il	Distributed Illegal Parameter Encoding	None	2
195.62.53.168	Russian Federation	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to gmail.com/engine/log.txt	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
46.120.122.219	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/726-en/patzar.aspx200oktext/html34445 idf law review 3200:00.359utf-8	Block	1
91.77.231.156	Russian Federation	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
66.249.65.52	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1
207.46.13.46	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/robots.txt	Block	1
68.180.231.60	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2110-he/cogat.aspx	Block	1
156.202.29.57	Egypt	147.237.77.216	dover.idf.il	Multiple NULL Character in Url from 156.202.29.57	Block	1
66.249.65.54	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/.well-known/apple-app-site-association	Block	1
66.102.9.26	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
156.202.29.57	Egypt	147.237.77.216	dover.idf.il	NULL Character in URL /1133-#[[إنترنيـــت،]]0#[[]]0]]	Block	1
37.133.249.120	Spain	147.237.76.42	refuah.idf.il	Unauthorized HTTP Method	Block	1
77.139.252.122	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/rights/asp/info.asp	Block	1
66.249.64.134	Israel	147.237.0.17	m.my-kosher-kravi .idf.il	Distributed Illegal Parameter Encoding	None	1
185.97.132.8	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
66.249.76.54	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
37.133.249.120	Spain	147.237.76.42	refuah.idf.il	Unauthorized Method OPTIONS for /	Block	1
79.253.3.246	Germany	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/iturim/asp/displayallsoldiers.asp	Block	1
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1

10-04-2016-00:04:07 to 10-04-2016-01:04:07