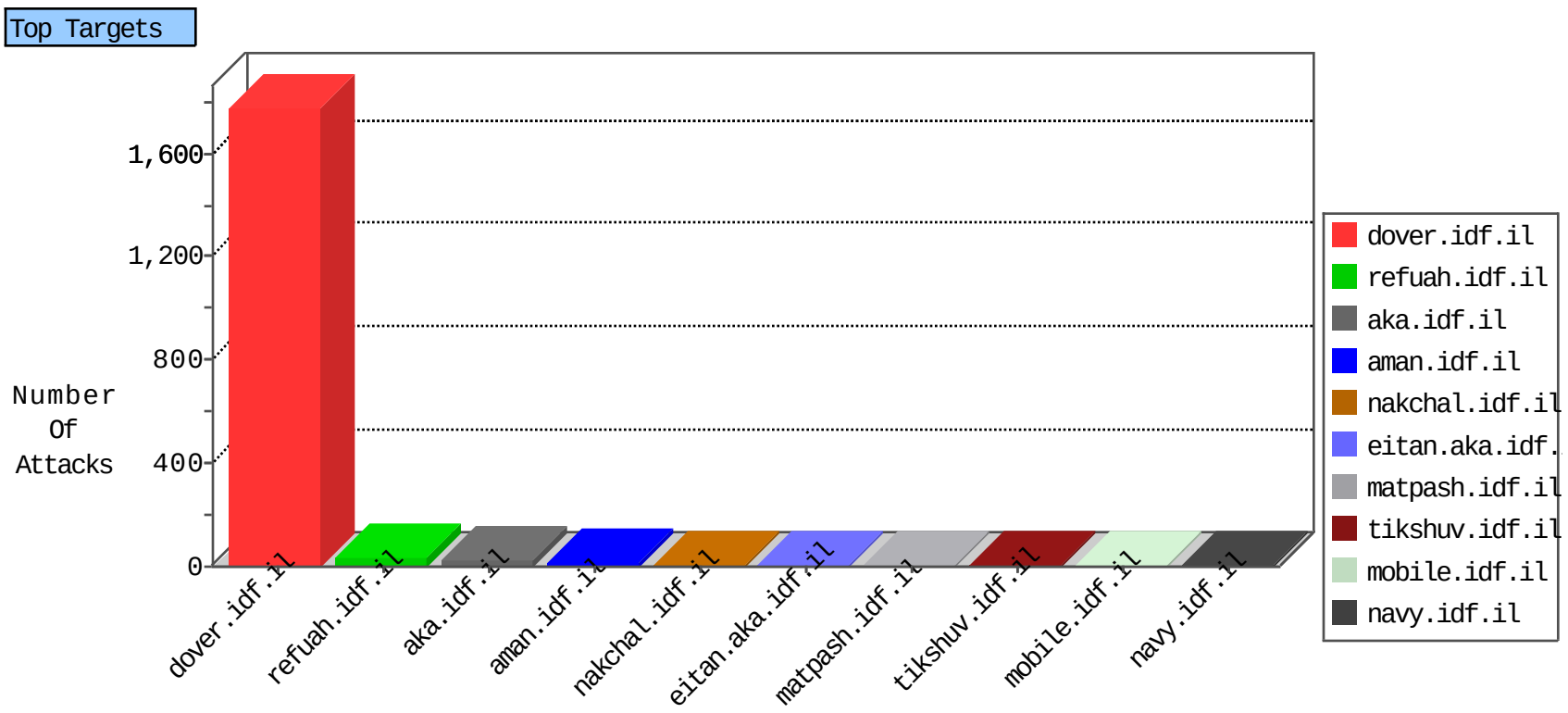
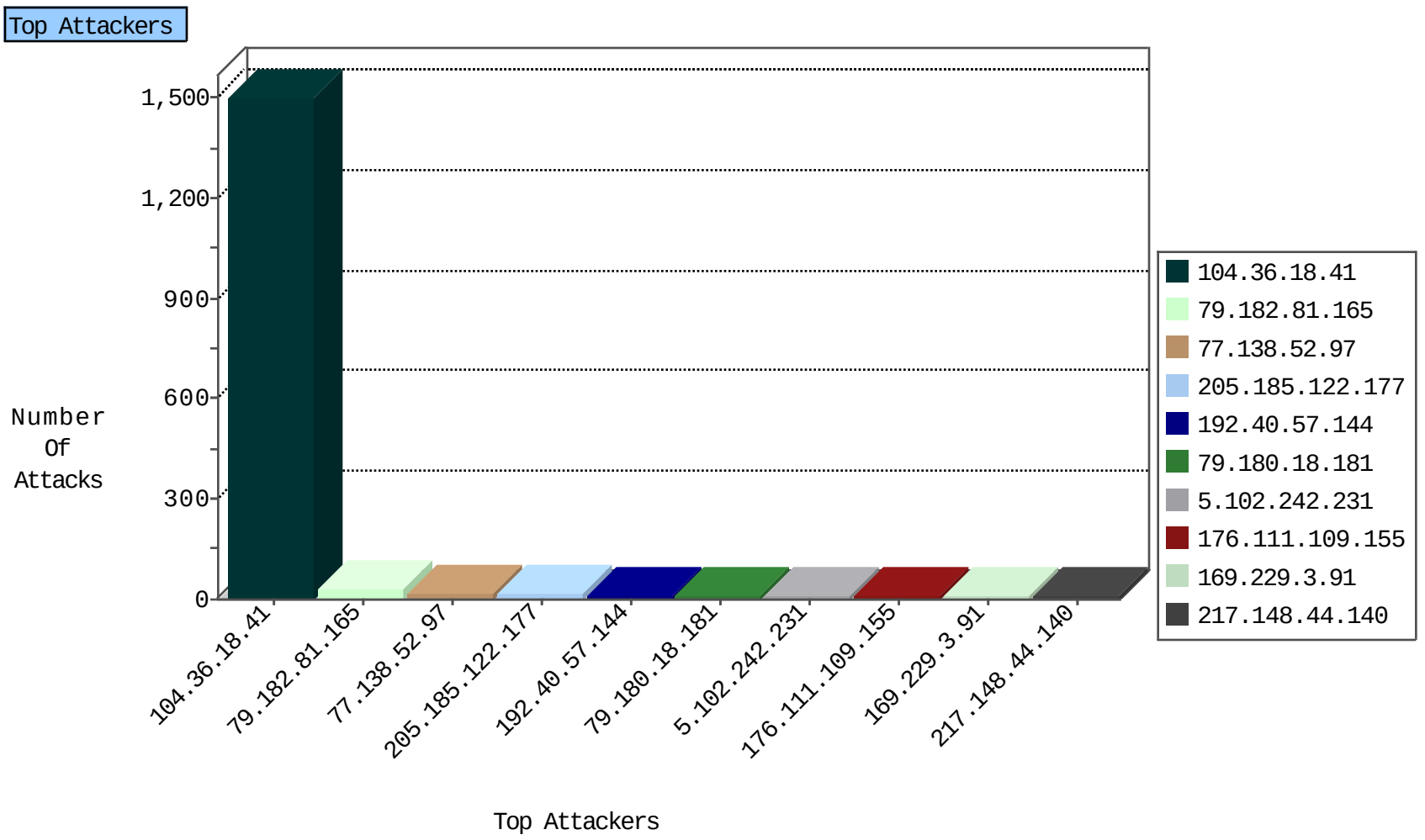
10-01-2016-02:04:06 to 10-01-2016-03:04:06

IDF Under Attack Daily Report





10-01-2016-02:04:06 to 10-01-2016-03:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	4761
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	418
104.36.18.41	United States	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	55
5.102.242.231	Israel	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	10
79.180.18.181	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
205.185.122.177	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	6
104.36.18.41	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
176.111.109.155	Portugal	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
104.36.18.41	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	5
217.148.44.140	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
193.182.144.142	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
37.235.53.238	Spain	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
192.40.57.144	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
199.167.129.140	Canada	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
77.138.52.97	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
158.255.208.29	Hong Kong	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
46.117.235.185	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
192.71.249.215	Belgium	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
77.138.52.97	France	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	2
66.249.65.53	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
158.255.208.29	Hong Kong	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
85.250.214.228	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
207.46.13.161	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
85.250.214.228	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
207.46.13.161	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
85.250.214.228	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
109.226.40.40	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
207.46.13.161	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
192.40.57.144	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

10-01-2016-02:04:06 to 10-01-2016-03:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
162.210.196.98	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	4
46.118.155.156	Ukraine	147.237.77.216	dover.idf.il	15323: HTTP: User-Agent (MRSPUTNIK)	Block	3

10-01-2016-02:04:06 to 10-01-2016-03:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
222.186.34.141	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
222.186.34.141	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
222.186.34.141	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
183.129.160.229	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
146.200.148.0	147.237.77.216	United Kingdom	dover.idf.il	Tehila - Perl LWP with fake user agent	1
66.249.65.51	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	1
59.32.34.230	147.237.0.33	China	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.161.40.17	147.237.0.19	Russian Federation	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.34.141	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
222.186.34.141	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
222.186.34.141	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
210.30.128.25	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
176.20.227.98	147.237.77.176	Denmark	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
106.187.45.144	147.237.77.176	Japan	matpash.idf.il	ET SCAN Potential SSH Scan	1
64.233.172.139	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	1
46.172.91.21	147.237.0.35	Ukraine	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
222.253.214.215	147.237.76.196	Vietnam	e.sviva.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

10-01-2016-02:04:06 to 10-01-2016-03:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
104.36.18.41	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1223
104.36.18.41	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	215
79.182.81.165	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
79.182.81.165	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
45.59.183.115	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
207.46.13.161	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
50.79.101.141	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
79.182.81.165	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
2.53.142.151	Israel	147.237.76.200	eitan.aka.idf..	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.233	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
178.22.70.91	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
139.162.178.208	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.247.48.152	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
158.255.211.156	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
194.90.15.61	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
176.111.109.155	Portugal	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
5.34.183.55	Ukraine	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
91.224.13.64	Latvia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
5.45.183.194	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
94.75.199.193	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
178.17.170.69	Moldova, Republic of	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
205.185.122.177	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	Streaming Engine: TCP SYN Modified Retransmission	Data received before SYN was acknowledged. Stripping all packet data.	drop	3
79.181.99.166	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	3
77.138.52.97	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
192.40.57.144	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
217.148.44.140	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.79.4	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
199.167.129.140	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.233	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
158.255.208.29	Hong Kong	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.180.18.181	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
205.185.122.177	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
46.246.89.243	Sweden	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
2.55.174.253	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
85.250.214.228	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
79.182.81.165	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
79.180.18.181	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
192.40.57.144	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
5.102.253.62	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
94.230.86.138	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
79.181.99.166	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
77.138.52.97	France	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
180.183.158.64	Thailand	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.117.235.185	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
79.182.81.165	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2

10-01-2016-02:04:06 to 10-01-2016-03:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.65.12	Israel	147.237.77.243	mobile.idf.i	Unauthorized URL Access to mobile.idf.il/.well-known/assetlinks.json	Block	1
71.224.243.7	United States	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Parameter Name [[#1]]▫▫▫ [[#1]]@U[[#8]][[#2]]([[#19]]▫[[#1]]▫[[#14]]▫[[#1]]▫▫▫[[#1]]b<&[[#1]]▫▫▫ [[#1]]@▫▫▫ in www.idf.il/templates/social/▫ńw	Block	1
66.249.65.182	Israel	147.237.76.42	refuah.idf.i	Unauthorized URL Access to 147.237.76.42/994-8857-he/refuah.aspx	Block	1
71.224.243.7	United States	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Parameter Value at 1 for www.idf.il/templates/social/▫ńw	Block	1
66.249.65.185	Israel	147.237.76.42	refuah.idf.i	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/2418.jpg	Block	1
139.162.178.208	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/favicon.ico	Block	1
2.53.0.213	Israel	147.237.72.166	aka.idf.il	Unknown Parameter asm in www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	None	1
66.249.65.188	Israel	147.237.76.42	refuah.idf.i	Unauthorized URL Access to 147.237.76.42/994-8879-he/refuah.aspx	Block	1
178.255.87.242	United Kingdom	147.237.77.243	mobile.idf.i	Unauthorized URL Access to 147.237.77.243/robots.txt	Block	1
66.249.65.12	Israel	147.237.77.243	mobile.idf.i	Multiple Unauthorized URL Access from 66.249.65.12	Block	1
66.249.75.54	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/m/	Block	1

10-01-2016-02:04:06 to 10-01-2016-03:04:06