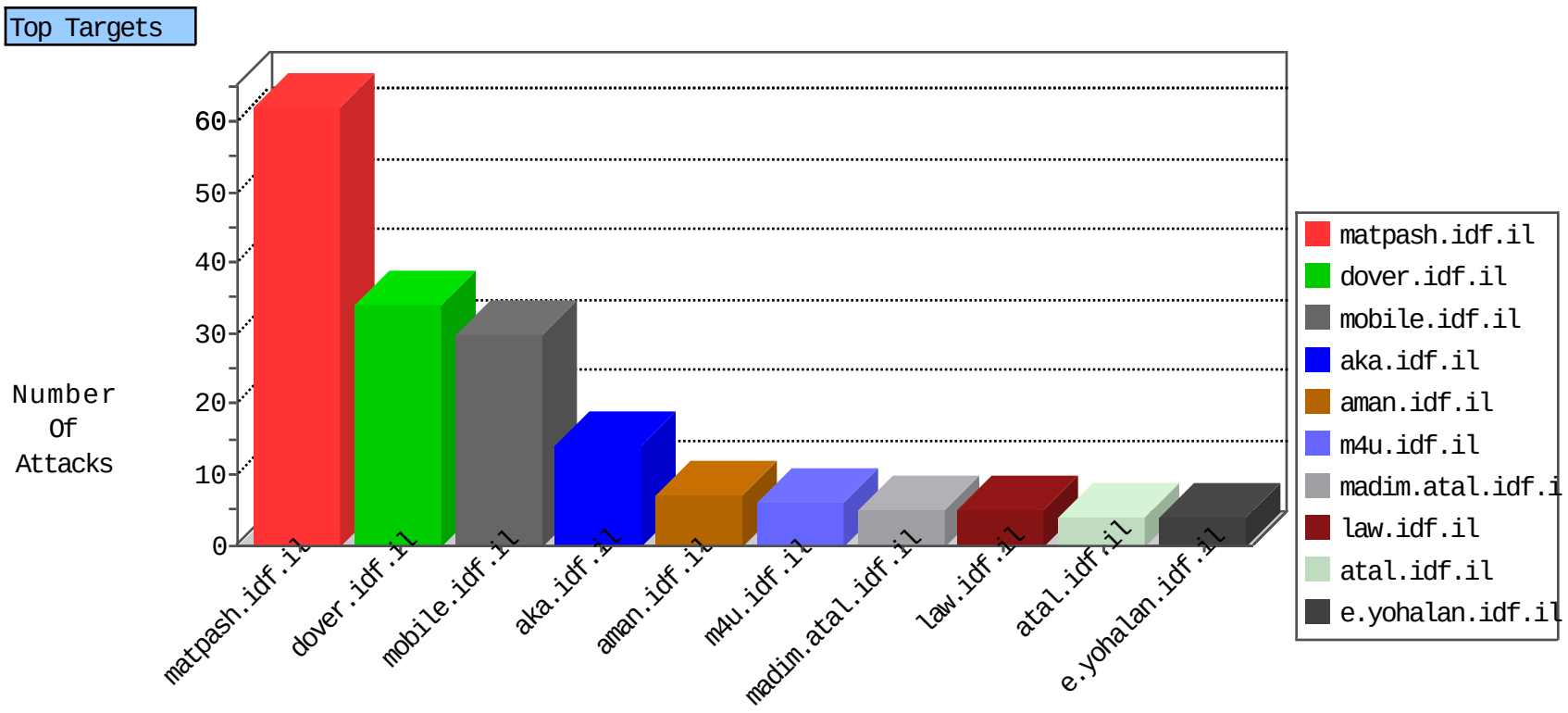
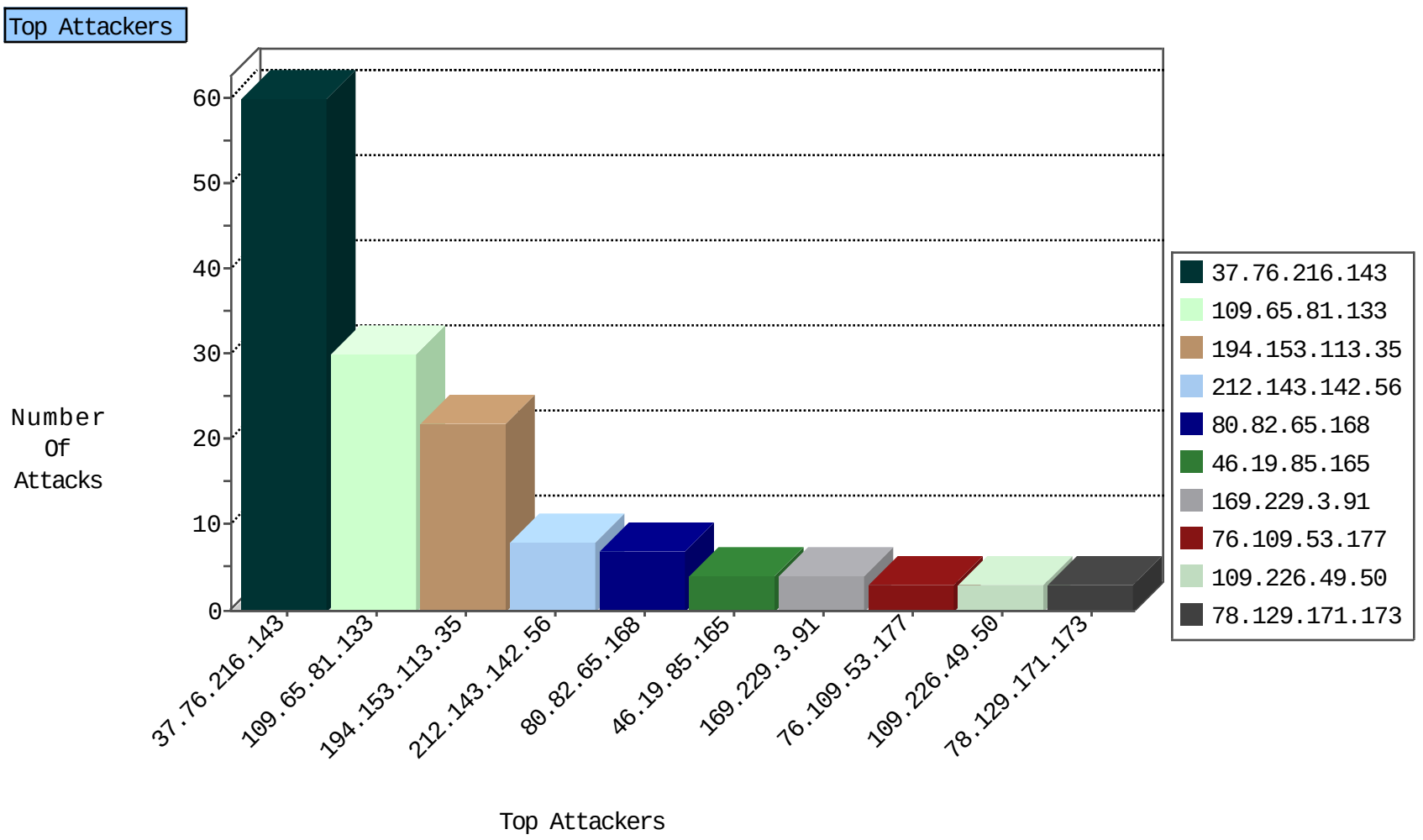
09-30-2016-03:04:04 to 09-30-2016-04:04:04

IDF Under Attack Daily Report





09-30-2016-03:04:04 to 09-30-2016-04:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.82.65.168	Netherlands	147.237.0.200	m4u.idf.il	Frk_Under_Attack_Con_Http	drop	2
180.153.91.178	China	147.237.76.30	himush.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.42	refuah.idf.il	Black List	drop	1
80.82.65.168	Netherlands	147.237.0.200	m4u.idf.il	Frk_Purple_Con_Limit_Http	drop	1

09-30-2016-03:04:04 to 09-30-2016-04:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.120.188.139	China	147.237.77.74	law.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1
151.80.31.163	France	147.237.76.86	navy.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

09-30-2016-03:04:04 to 09-30-2016-04:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.154.184.122	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
195.143.227.35	147.237.76.196	United Kingdom	e.sviva.idf.il	ET SCAN NMAP -sS window 4096	1
188.136.237.251	147.237.76.34	Iran, Islamic Republic of	yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
91.201.236.50	147.237.77.178	Ukraine	e.matpash.idf.il	ET SCAN NMAP -sS window 4096	1
91.201.236.50	147.237.77.178	Ukraine	e.matpash.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
78.129.171.173	147.237.76.198	United Kingdom	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
78.129.171.173	147.237.0.200	United Kingdom	m4u.idf.il	ET SCAN Potential SSH Scan	1
66.55.141.76	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
46.161.40.17	147.237.76.30	Russian Federation	himush.idf.il	ET SCAN NMAP -sS window 1024	1
195.143.227.35	147.237.76.196	United Kingdom	e.sviva.idf.il	ET SCAN NMAP -sS window 3072	1
188.136.237.251	147.237.76.34	Iran, Islamic Republic of	yohalan.idf.il	ET SCAN NMAP -f -sS	1
91.201.236.50	147.237.77.178	Ukraine	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
85.120.95.250	147.237.77.178	Romania	e.matpash.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
78.129.171.173	147.237.76.44	United Kingdom	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
66.249.66.12	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
46.161.40.17	147.237.76.38	Russian Federation	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.74	147.237.77.179	United States	e.mazi.idf.il	ET DROP Dshield Block Listed Source	1

09-30-2016-03:04:04 to 09-30-2016-04:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
37.76.216.143	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	60
109.65.81.133	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
194.153.113.35	Germany	147.237.77.74	law.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
46.19.85.165	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
109.226.49.50	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
194.153.113.35	Germany	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
194.153.113.35	Germany	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
194.153.113.35	Germany	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
79.177.89.177	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
194.153.113.35	Germany	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
185.120.125.67	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
194.153.113.35	Germany	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
149.202.173.163	France	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
194.153.113.35	Germany	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
46.19.86.146	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
192.118.60.69	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.117	United States	147.237.77.61	e.cogat.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
76.109.53.177	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
37.49.226.132	Netherlands	147.237.77.216	dover.idf.il	Header Rejection	header rejection pattern found in request	monitor	1
169.229.3.91	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.95	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
80.82.65.168	Netherlands	147.237.0.33	idf.il	drop		drop	1
213.57.231.114	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
46.19.86.146	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.125	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
131.253.36.196	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
169.229.3.91	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.112	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
80.82.65.168	Netherlands	147.237.0.35	akaws.idf.il	drop		drop	1
216.218.206.116	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.60	United States	147.237.77.61	e.cogat.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.126	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.90	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
79.182.123.3	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
194.153.113.35	Germany	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	1
41.239.61.195	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
141.212.122.113	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
94.102.49.193	Netherlands	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
76.109.53.177	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
31.13.113.88	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.91	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
80.82.65.168	Netherlands	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
192.118.60.69	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.116	United States	147.237.77.61	e.cogat.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
76.109.53.177	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
31.13.113.92	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.94	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
80.82.65.168	Netherlands	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1

09-30-2016-03:04:04 to 09-30-2016-04:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.220.90	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.86.81	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
50.186.152.66	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
192.243.55.130	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/asp/giyus.asp	Block	1
81.104.113.8	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/pniotanswer.aspx	Block	1
136.160.90.33	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.64.183	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-21810-he/idfgdover.aspx	Block	1
194.153.113.35	Germany	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
148.251.192.100	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/home/default.aspx	Block	1
66.249.75.8	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9023-he/refuah.aspx	Block	1
194.153.113.35	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/robots.txt	Block	1
110.136.51.124	Indonesia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
5.29.4.211	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
169.229.3.91	United States	147.237.76.200	eitan.aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.75.12	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
194.153.113.35	Germany	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
118.201.50.146	Singapore	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
185.32.179.88	Israel	147.237.72.166	aka.idf.il	Unknown Parameter asm in www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	None	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
204.79.180.179	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/miluim/templates/inner.asp	Block	1
136.160.90.33	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 136.160.90.33	Block	1

09-30-2016-03:04:04 to 09-30-2016-04:04:04