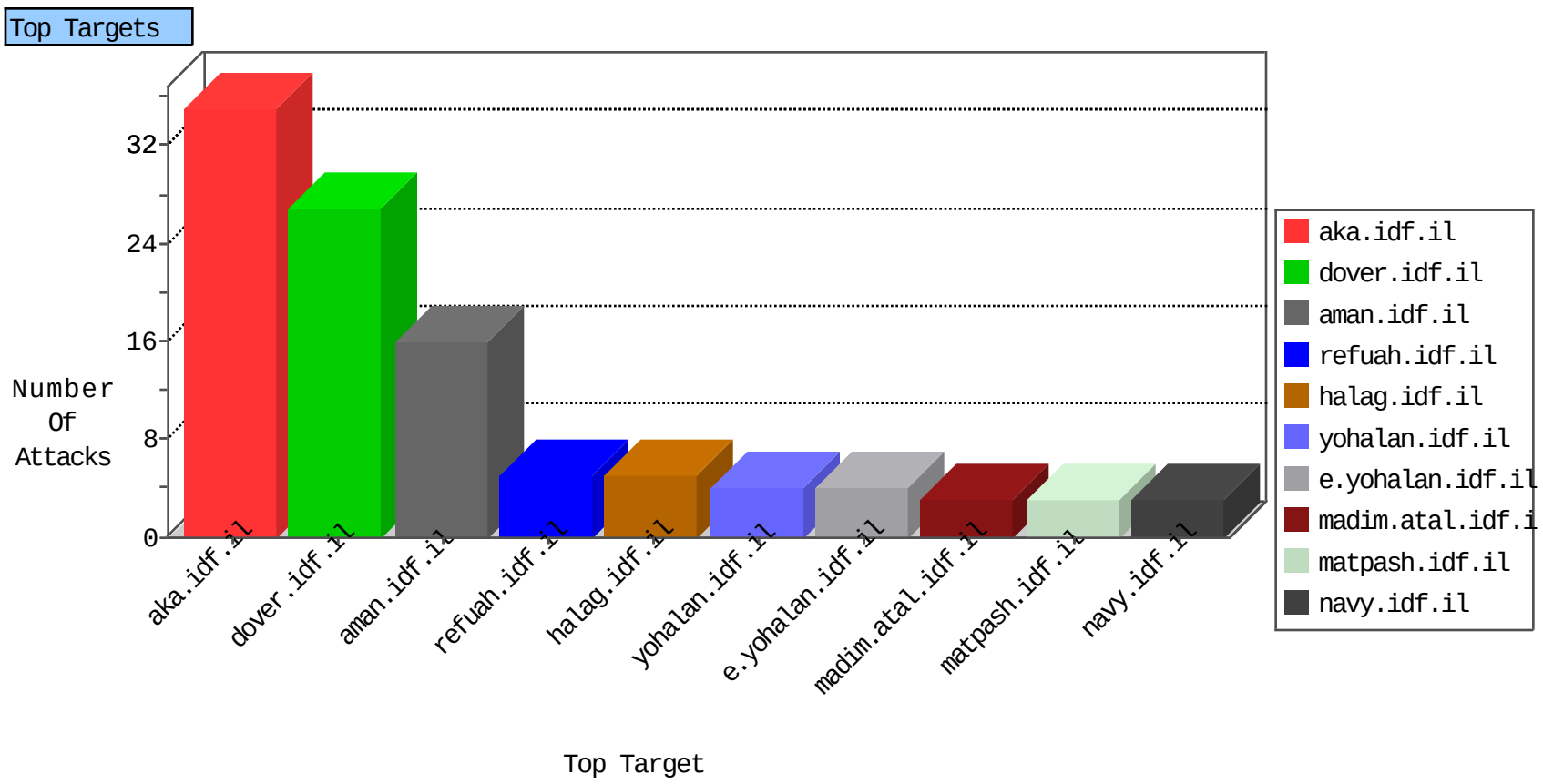
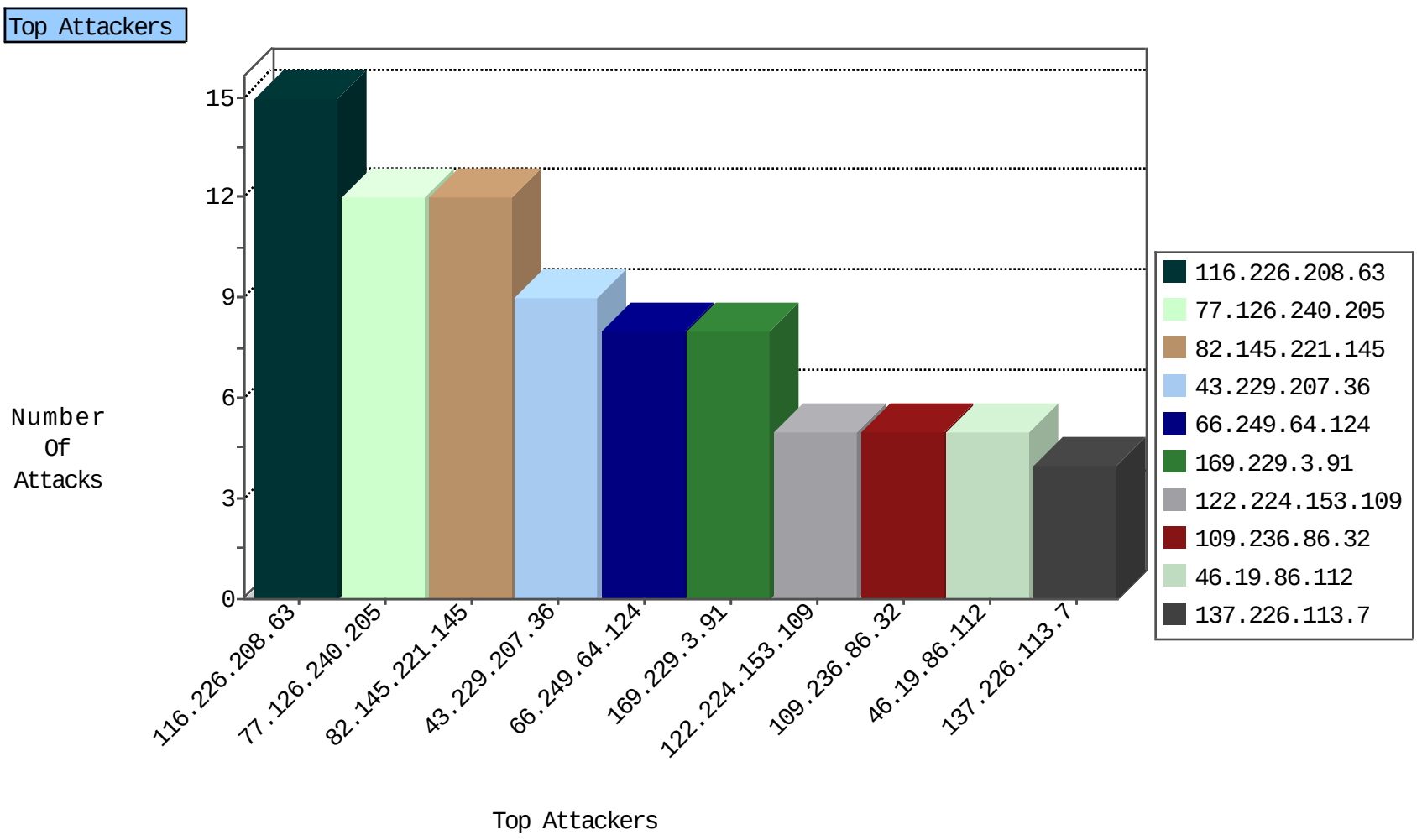
09-21-2016-02:04:01 to 09-21-2016-03:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-21-2016-02:04:01 to 09-21-2016-03:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
122.224.153.109	China	147.237.76.147	chinuch.aka.idf.il	JLM_Purple_Con_Limit_Http	drop	1
45.32.196.8	United States	147.237.76.198	e.yohalan.idf.il	Black List	drop	1
198.20.99.130	Netherlands	147.237.76.86	navy.idf.il	Black List	drop	1
71.6.146.185	United States	147.237.76.86	navy.idf.il	Black List	drop	1
94.102.49.193	Netherlands	147.237.76.198	e.yohalan.idf.il	Black List	drop	1

09-21-2016-02:04:01 to 09-21-2016-03:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-21-2016-02:04:01 to 09-21-2016-03:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
220.133.19.244	147.237.77.61	Taiwan	e.cogat.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
43.229.207.36	147.237.76.198	Indonesia	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
128.232.110.28	147.237.77.205	United Kingdom	prisha.idf.il	ET SCAN Potential SSH Scan	1
43.229.207.36	147.237.76.148	Indonesia	gqcenter.aka.idf.i	ET SCAN Potential SSH Scan	1
116.71.128.85	147.237.77.234	Pakistan	halag.idf.il	ET SCAN NMAP -sS window 1024	1
43.229.207.36	147.237.76.42	Indonesia	refuah.idf.il	ET SCAN Potential SSH Scan	1
116.71.128.85	147.237.77.205	Pakistan	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
43.229.207.36	147.237.76.30	Indonesia	himush.idf.il	ET SCAN Potential SSH Scan	1
109.236.86.32	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
109.236.86.32	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
94.102.49.92	147.237.0.33	Netherlands	idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.50	147.237.77.216	Ukraine	dover.idf.il	ET SCAN NMAP -f -sS	1
43.229.207.36	147.237.76.201	Indonesia	e.atal.idf.il	ET SCAN Potential SSH Scan	1
202.65.138.2	147.237.76.176	India	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
43.229.207.36	147.237.76.197	Indonesia	e.himush.idf.il	ET SCAN Potential SSH Scan	1
118.103.126.194	147.237.77.179	Japan	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
43.229.207.36	147.237.76.44	Indonesia	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
116.71.128.85	147.237.77.216	Pakistan	dover.idf.il	ET SCAN NMAP -sS window 1024	1
43.229.207.36	147.237.76.34	Indonesia	yohalan.idf.il	ET SCAN Potential SSH Scan	1
109.236.86.32	147.237.76.198	Netherlands	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
109.236.86.32	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
109.236.86.32	147.237.8.28	Netherlands	e.mobile-ks.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.201.236.50	147.237.77.216	Ukraine	dover.idf.il	ET SCAN NMAP -sS window 2048	1
43.229.207.36	147.237.77.216	Indonesia	dover.idf.il	ET SCAN Potential SSH Scan	1
216.81.230.167	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1

09-21-2016-02:04:01 to 09-21-2016-03:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
82.145.221.145	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	12
116.226.208.63	China	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
66.249.64.124	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
116.226.208.63	China	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.86.112	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
77.126.240.205	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	4
2.53.181.177	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
116.226.208.63	China	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
62.212.73.211	Netherlands	147.237.77.234	halag.idf.il	drop	SAM rule	drop	2
187.61.109.18	Brazil	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
77.126.240.205	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
188.120.154.204	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
77.126.240.205	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
122.224.153.109	China	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
84.109.113.237	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
180.97.106.161	China	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
125.209.235.180	Korea, Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
109.253.205.77	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
180.97.106.162	China	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
169.229.3.91	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
2.53.181.177	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
137.226.113.7	Germany	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
122.224.153.109	China	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
84.111.39.155	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
180.97.106.161	China	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
169.229.3.91	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
137.116.71.170	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
180.97.106.37	China	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.164	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
122.224.153.109	China	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
93.104.215.125	Germany	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
180.97.106.161	China	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
169.229.3.91	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
137.226.113.7	Germany	147.237.0.35	akaws.idf.il	drop		drop	1
180.97.106.37	China	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.19.86.1	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.165	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
122.224.153.109	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
104.246.16.27	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
180.97.106.161	China	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
169.229.3.91	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
137.226.113.7	Germany	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
198.20.87.98	United States	147.237.0.200	m4u.idf.il	drop		drop	1
84.109.113.237	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
180.97.106.37	China	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.19.86.6	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1

09-21-2016-02:04:01 to 09-21-2016-03:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.64.108	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.64.108	Block	2
66.249.64.124	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.124	Block	2
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.106	Block	2
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Unknown Parameter doc in www.aka.idf.il/kamlar/klali/default.asp	None	1
157.55.39.242	United States	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/robots.txt	Block	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english	Block	1
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.i	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
68.180.231.60	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-he/cogat.aspx	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
80.246.137.63	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	1
93.173.37.19	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1

09-21-2016-02:04:01 to 09-21-2016-03:04:01