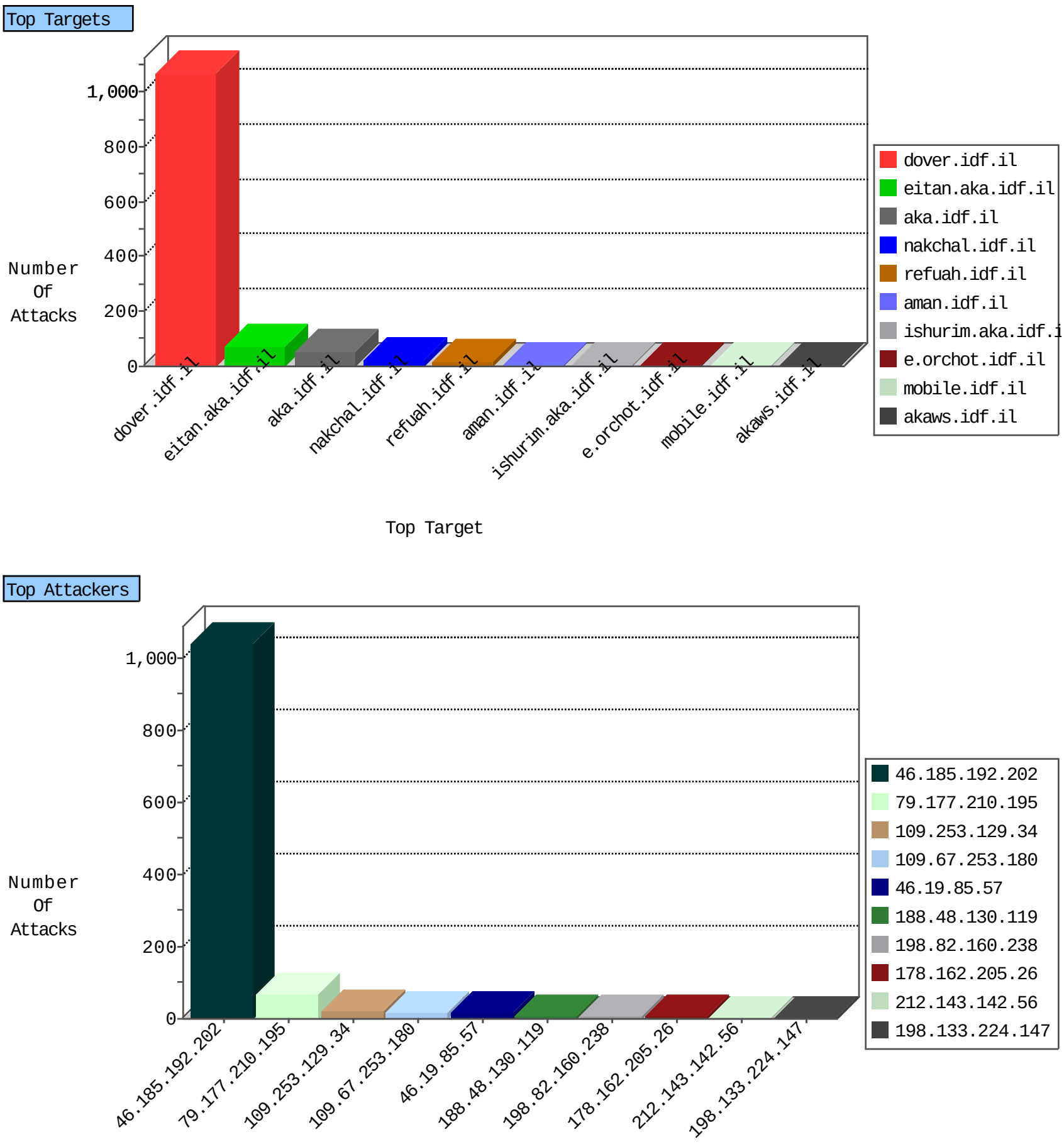
09-19-2016-02:04:05 to 09-19-2016-03:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers

09-19-2016-02:04:05 to 09-19-2016-03:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.185.192.202	Jordan	147.237.77.216	dover.idf.il	network flood IPv4 ICMP	drop	15662
46.185.192.202	Jordan	147.237.77.216	dover.idf.il	ICMP-fragmented	drop	23
46.19.85.57	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	12
188.48.130.119	Saudi Arabia	147.237.77.216	dover.idf.il	network flood IPv4 ICMP	drop	7
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	5
0.0.0.0		147.237.77.216	dover.idf.il	network flood IPv4 ICMP	drop	4
198.133.224.147	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
129.10.120.193	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
130.194.252.8	Australia	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
192.33.90.68	Switzerland	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
131.247.2.241	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
160.80.221.37	Italy	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
129.97.74.14	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
194.29.178.14	Poland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
134.197.113.3	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
129.93.229.138	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
139.78.141.243	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
129.93.229.139	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
192.33.90.68	Switzerland	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
130.217.77.4	New Zealand	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.113	United States	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.83	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
156.56.250.227	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
111.73.45.159	China	147.237.0.15	kosher-kravi.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1

09-19-2016-02:04:05 to 09-19-2016-03:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
125.208.24.2	China	147.237.76.200	eitan.aka.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1

09-19-2016-02:04:05 to 09-19-2016-03:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.64.160	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	3
5.255.90.133	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
183.19.190.239	147.237.77.178	China	e.matpash.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
178.162.205.26	147.237.72.166	Germany	aka.idf.il	ET SCAN Potential SSH Scan	1
178.162.205.26	147.237.8.14	Germany	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
103.207.36.31	147.237.72.14	Vietnam	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
50.84.213.146	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -f -sS	1
5.255.90.133	147.237.8.28	Netherlands	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
178.162.205.26	147.237.76.196	Germany	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
178.162.205.26	147.237.8.24	Germany	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
178.162.205.26	147.237.0.19	Germany	madim.atal.idf.il	ET SCAN Potential SSH Scan	1

09-19-2016-02:04:05 to 09-19-2016-03:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
79.177.210.195	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	68
109.253.129.34	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
109.67.253.180	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.67.253.180	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.85.57	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.57	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.67.253.180	Israel	147.237.72.166	aka.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	4
176.13.244.191	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
84.111.13.61	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
196.217.31.132	Morocco	147.237.77.216	dover.idf.il	drop		drop	2
46.19.85.7	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.105	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
138.255.72.254	Brazil	147.237.0.35	akaws.idf.il	drop		drop	1
72.197.8.34	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
174.200.13.178	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.97	United States	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.19.85.7	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.105	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.64	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.98	United States	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.107	United States	147.237.0.33	idf.il	drop		drop	1
141.212.122.65	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
176.21.88.145	Denmark	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.104	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.108	United States	147.237.0.33	idf.il	drop		drop	1
141.212.122.68	United States	147.237.0.35	akaws.idf.il	drop		drop	1
106.38.241.105	China	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	1
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
141.212.122.104	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
115.31.175.92	Thailand	147.237.77.216	dover.idf.il	Header Rejection	header rejection pattern found in request	monitor	1
46.19.85.240	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
173.57.166.111	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
141.212.122.69	United States	147.237.0.35	akaws.idf.il	drop		drop	1

09-19-2016-02:04:05 to 09-19-2016-03:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.249.234	Israel	147.237.77.243	mobile.idf.i	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	3
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/1/69041.pdf	Block	1
185.86.77.38	Ukraine	147.237.77.233	atal.idf.il	Parameter Type Violation searchText in www.atal.idf.il/1402-he/atal.aspx	Block	1
84.111.13.61	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
193.252.118.176	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
148.251.13.51	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
66.249.64.180	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1237-he/atal.aspx	Block	1
157.55.39.12	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/994-9065-he/navy.aspx	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/qanda/default.asp	Block	1

09-19-2016-02:04:05 to 09-19-2016-03:04:05