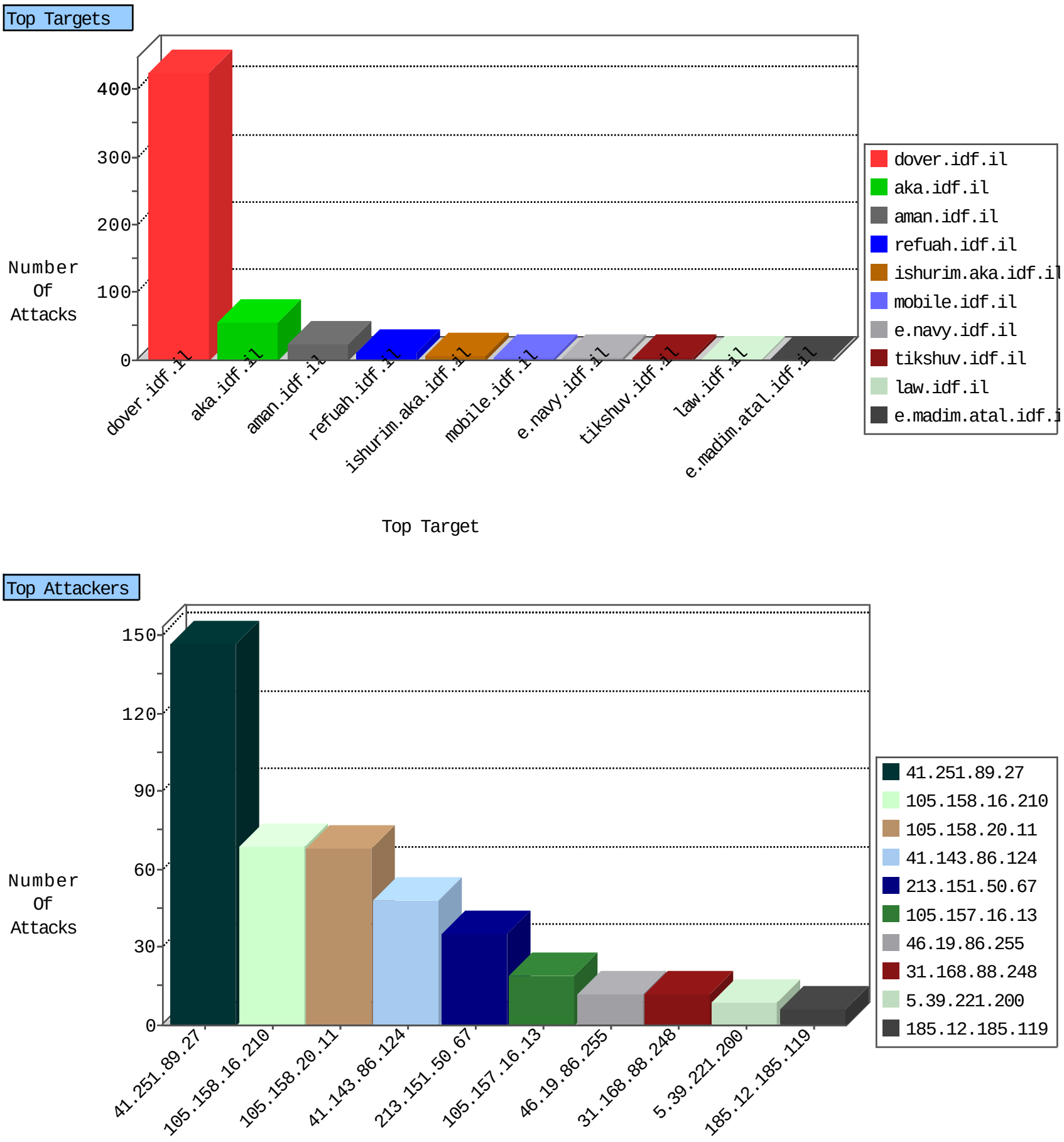
09-14-2016-03:04:00 to 09-14-2016-04:04:00

IDF Under Attack Daily Report



09-14-2016-03:04:00 to 09-14-2016-04:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.12.185.119	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-Url	dest-reset	5
198.133.224.147	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	5
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
200.19.159.35	Brazil	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	3
128.8.126.111	United States	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
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.10.120.193	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
141.22.213.34	Germany	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
131.247.2.241	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.208.4.197	United States	147.237.72.167	ishurim.aka.idf.i	network flood IPv4 ICMP	drop	1
202.4.4.147	Philippines	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
134.197.113.3	United States	147.237.72.166	aka.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
153.90.1.34	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
130.195.4.69	New Zealand	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
139.78.141.243	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.110.125.52	United States	147.237.72.167	ishurim.aka.idf.i	network flood IPv4 ICMP	drop	1
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.217.77.2	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.194.252.8	Australia	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.42.142.45	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
202.4.2.148	Philippines	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
164.107.127.12	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.93.229.139	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
41.251.89.27	Morocco	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
141.22.213.34	Germany	147.237.72.167	ishurim.aka.idf.i	network flood IPv4 ICMP	drop	1
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-14-2016-03:04:00 to 09-14-2016-04:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
78.160.93.53	Turkey	147.237.72.166	aka.idf.i	C1000018: HTTP: access to administrator/index.php -> Quarantine	Permit	1
78.160.93.53	Turkey	147.237.72.166	aka.idf.i	C1000016: HTTP: administrator in URI	Permit	1

09-14-2016-03:04:00 to 09-14-2016-04:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
84.93.84.77	147.237.77.216	United Kingdom	dover.idf.il	Tehila - Perl LWP with fake user agent	2
66.249.64.113	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
65.60.36.203	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.74	147.237.72.156	United States	aman.idf.il	ET DROP Dshield Block Listed Source	1
103.207.36.31	147.237.76.201	Vietnam	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.64.141	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
66.249.64.105	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
31.168.0.253	147.237.72.156	Israel	aman.idf.il	ET SCAN NMAP -sA (2)	1
193.201.225.149	147.237.77.19	Ukraine	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1

09-14-2016-03:04:00 to 09-14-2016-04:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
41.251.89.27	Morocco	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	85
41.251.89.27	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
105.158.20.11	Morocco	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	56
105.158.16.210	Morocco	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	42
213.151.50.67	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
41.143.86.124	Morocco	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	34
105.158.16.210	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
41.143.86.124	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
105.157.16.13	Morocco	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
31.168.88.248	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
105.158.20.11	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
5.39.221.200	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
105.157.16.13	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.255	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.255	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
85.250.125.172	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
176.13.244.61	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
192.114.91.214	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
71.6.216.53	United States	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
168.1.128.76	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
71.6.216.45	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
137.226.113.7	Germany	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
50.116.3.158	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
71.6.216.55	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.112	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
71.6.216.48	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
69.157.2.173	Canada	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
128.232.110.28	United Kingdom	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	1
71.6.216.60	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
180.97.106.161	China	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
71.6.216.54	United States	147.237.0.33	idf.il	drop		drop	1
172.56.15.146	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
71.6.216.45	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.97	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
187.6.78.186	Brazil	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
71.6.216.55	United States	147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
176.13.244.61	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
71.6.216.52	United States	147.237.8.27	e.madim.atal.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.113	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
128.232.110.28	United Kingdom	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
71.6.146.185	United States	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
79.181.120.230	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
180.97.106.161	China	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
71.6.216.54	United States	147.237.76.177	ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
172.56.38.173	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
71.6.216.46	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.98	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1

09-14-2016-03:04:00 to 09-14-2016-04:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
65.175.136.80	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
185.12.185.119	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	Unauthorized URL Access to www.idf.il/1038-ar/	Block	1
66.249.64.181	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
192.115.100.190	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/iturim/asp/wars.asp	Block	1
79.176.35.167	Israel	147.237.77.216	dover.idf.i	SSL Untraceable Connection - Open Mode	None	1
103.27.126.210	Hong Kong	147.237.77.216	dover.idf.i	PHP Attempt	Block	1
103.27.126.210	Hong Kong	147.237.77.216	dover.idf.i	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
66.249.64.113	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1

09-14-2016-03:04:00 to 09-14-2016-04:04:00