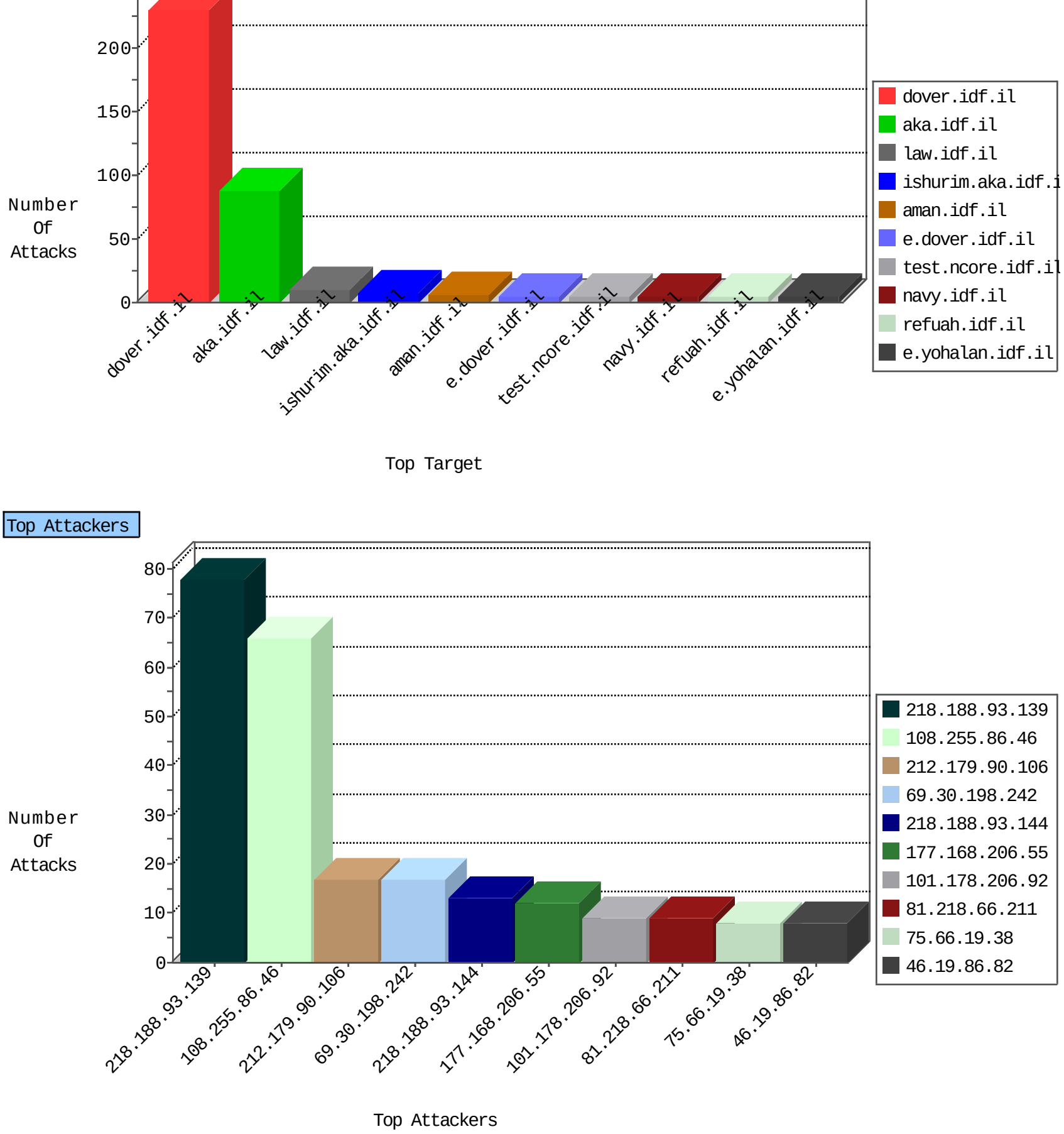
09-16-2016-03:04:03 to 09-16-2016-04:04:03

IDF Under Attack Daily Report



09-16-2016-03:04:03 to 09-16-2016-04:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	6
143.225.229.236	Italy	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	5
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	5
129.93.229.139	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	5
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
128.42.142.45	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
130.217.77.2	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
130.194.252.8	Australia	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	2
128.8.126.111	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
193.1.13.12	Ireland	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	2
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
153.90.1.35	United States	147.237.72.156	aman.idf.il	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
195.113.161.83	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
141.22.213.35	Germany	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
165.242.90.128	Japan	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
141.212.113.178	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
134.117.226.180	Canada	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1

09-16-2016-03:04:03 to 09-16-2016-04:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
69.30.198.242	United States	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	10
69.30.198.242	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3
69.30.198.242	United States	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	2
69.30.198.242	United States	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	2
104.192.169.238	United States	147.237.72.166	aka.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1
125.208.24.2	China	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1

09-16-2016-03:04:03 to 09-16-2016-04:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
218.155.244.161	147.237.77.212	Korea, Republic of	e.dover.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	5
94.102.48.195	147.237.76.198	Netherlands	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.50	147.237.77.19	Ukraine	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.34.139	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
66.249.64.105	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
216.81.230.167	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sS window 1024	1
40.121.139.43	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
202.85.192.97	147.237.76.42	Hong Kong	refuah.idf.il	ET SCAN NMAP -sS window 4096	1
189.143.131.64	147.237.76.176	Mexico	test.ncore.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
151.11.201.3	147.237.77.226	Italy	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 3072	1
151.11.201.3	147.237.77.226	Italy	www.chamatz.aka.idf.il	ET SCAN NMAP -f -sS	1
103.207.37.81	147.237.76.39	Vietnam	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.50	147.237.77.19	Ukraine	law-forum.idf.il	ET SCAN NMAP -sS window 2048	1
91.201.236.50	147.237.77.19	Ukraine	law-forum.idf.il	ET SCAN NMAP -f -sS	1
64.137.168.128	147.237.76.30	Canada	himush.idf.il	ET SCAN Potential SSH Scan	1
202.155.58.28	147.237.77.178	Indonesia	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
192.81.216.190	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
179.43.141.198	147.237.76.197	Switzerland	e.himush.idf.il	ET SCAN Potential SSH Scan	1
151.11.201.3	147.237.77.226	Italy	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 2048	1
133.242.4.52	147.237.77.179	Japan	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1

09-16-2016-03:04:03 to 09-16-2016-04:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
218.188.93.139	Hong Kong	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	78
108.255.86.46	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	66
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
218.188.93.144	Hong Kong	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
75.66.19.38	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
46.19.86.82	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
207.46.13.91	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
84.94.160.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
177.168.206.55	Brazil	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
5.102.242.197	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.218.66.211	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
77.127.53.74	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
177.168.206.55	Brazil	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
177.168.206.55	Brazil	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
101.178.206.92	Australia	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
81.218.66.211	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
186.182.232.4	Argentina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
141.226.217.117	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
128.232.110.28	United Kingdom	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
82.81.55.162	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
101.178.206.92	Australia	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
177.168.206.55	Brazil	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
31.13.110.104	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.102	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
101.178.206.92	Australia	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
41.233.4.146	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
79.177.153.251	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
126.7.189.217	Japan	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
141.212.122.89	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
66.212.179.106	Canada	147.237.76.34	yohalan.idf.il	drop		drop	1
141.212.122.16	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
106.38.241.105	China	147.237.76.86	navy.idf.il	drop	SAM rule	drop	1
81.218.66.211	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
141.212.122.31	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.19.85.179	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
192.81.216.190	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
101.178.206.92	Australia	147.237.76.177	ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
177.168.206.55	Brazil	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.94	United States	147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
66.212.179.106	Canada	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.21	United States	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
212.179.20.4	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
23.101.61.176	Ireland	147.237.0.34	tikshuv.idf.il	Instant Messengers	instant messenger pattern found, application: Skype	monitor	1
186.182.232.4	Argentina	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
169.229.3.91	United States	147.237.76.148	gqcenter.aka.idf.i	drop	SAM rule	drop	1
141.212.122.88	United States	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
133.208.21.66	Japan	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
192.81.216.190	United States	147.237.77.227	e.hamaz.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1

09-16-2016-03:04:03 to 09-16-2016-04:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
104.128.144.131	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/redirect.php	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
147.236.238.20	Israel	147.237.76.31	nakchal.idf.i	Unauthorized HTTP Method	Block	1
40.77.167.21	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
85.64.135.77	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
217.132.135.142	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
93.172.122.219	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.64.43	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
104.128.144.131	Canada	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/redirect.php	Block	1
66.249.64.105	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.105	Block	1

09-16-2016-03:04:03 to 09-16-2016-04:04:03