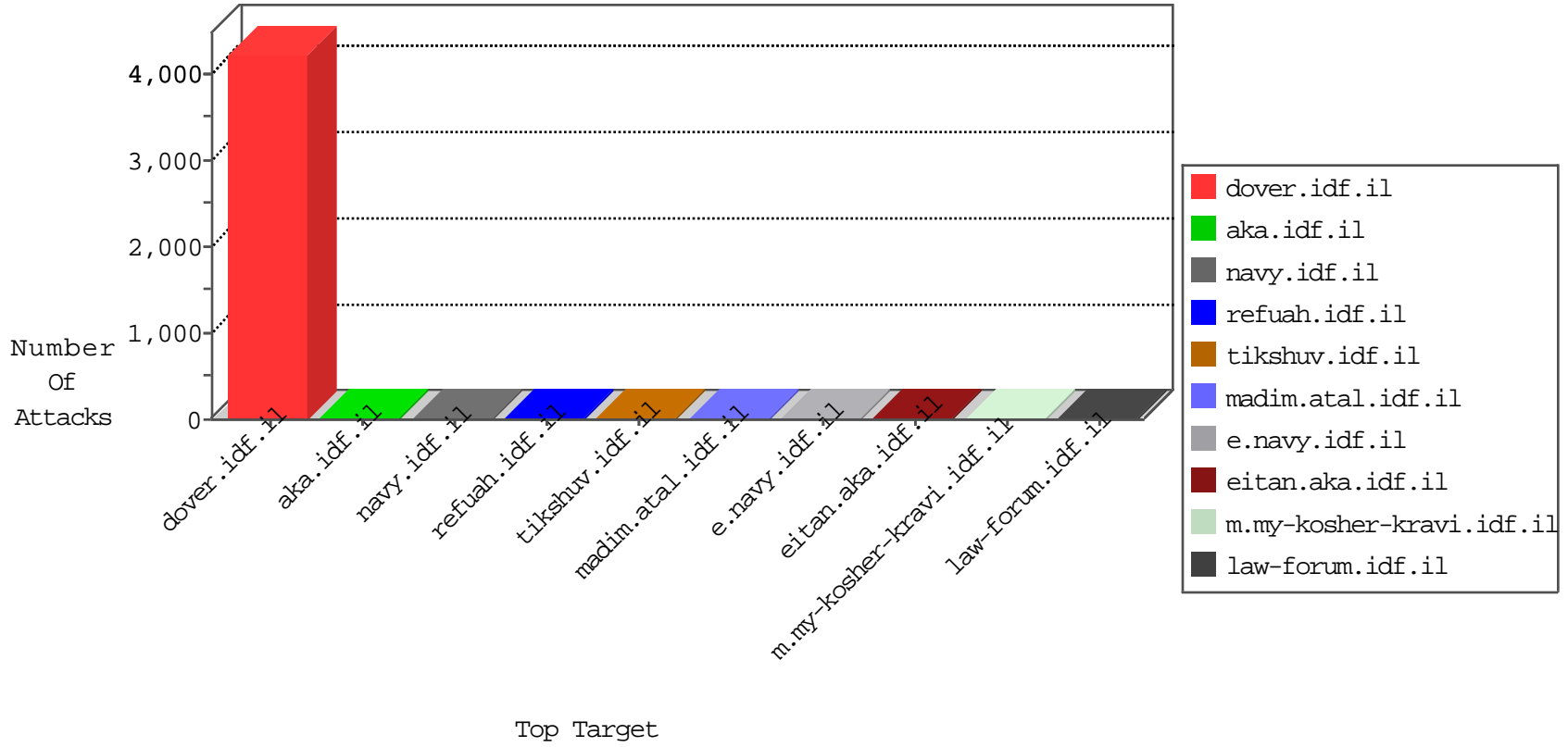




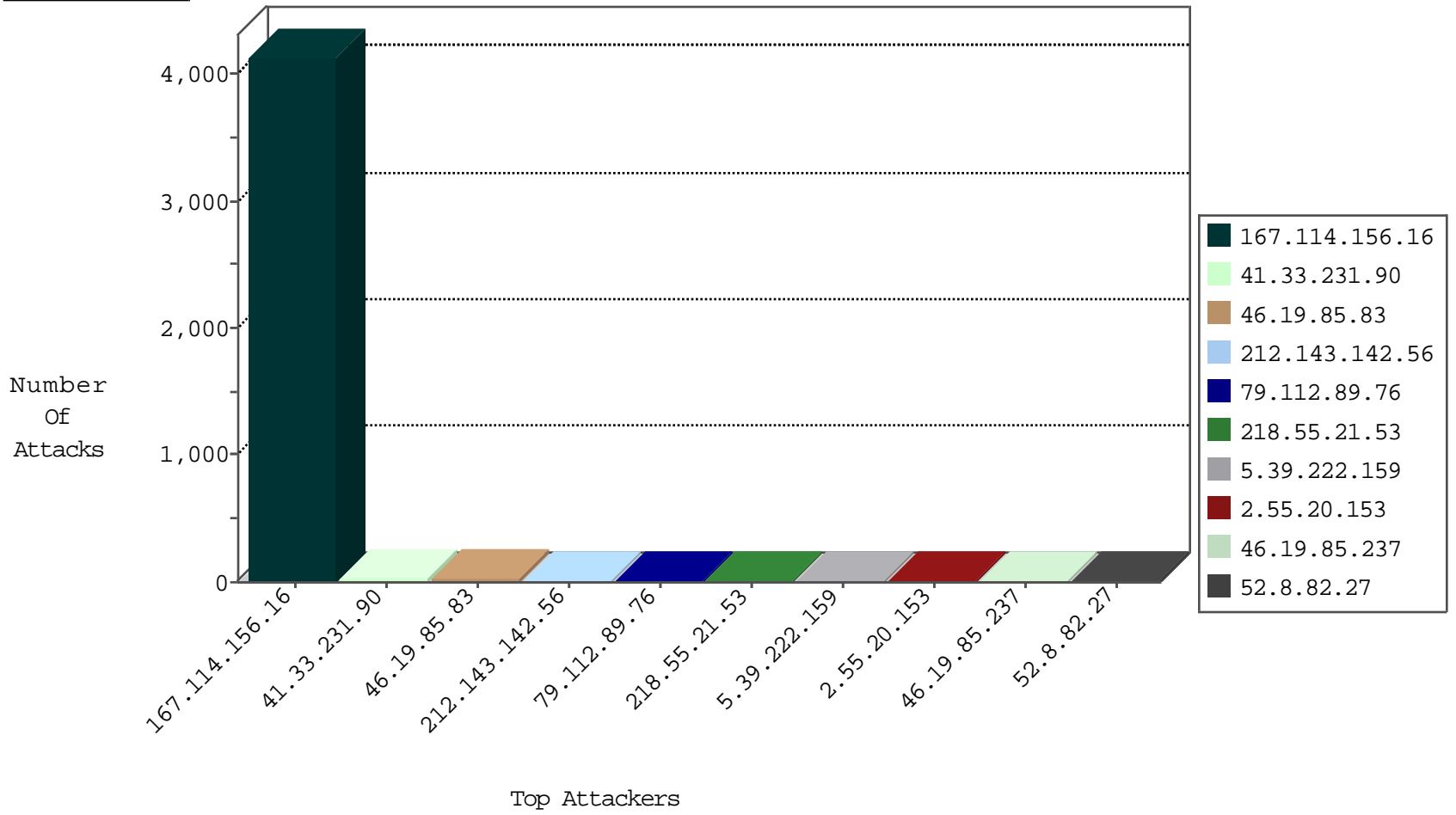
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4122
184.105.139.100	United States	147.237.8.45	e.eitan.idf.il	Block_Ntp_All_Net	drop	1
113.123.166.44	China	147.237.72.217	e.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.120	United States	147.237.77.74	law.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.96	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.104	United States	147.237.72.14	dover.idf.il(old)	Block_Ntp_All_Net	drop	1
184.105.139.124	United States	147.237.8.28	e.mobile-ks.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.96	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.108	United States	147.237.77.216	dover.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.68	United States	147.237.72.217	e.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.124	United States	147.237.77.179	e.mazi.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.100	United States	147.237.0.200	m4u.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.120	United States	147.237.0.34	tikshuv.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.68	United States	147.237.77.212	e.dover.idf.il	Block_Ntp_All_Net	drop	1

04-14-2016-06:04:01 to 04-14-2016-07:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
218.55.21.53	147.237.0.34	Korea, Republic of	tikshuv.idf.il	SERVER-APACHE Apache Tomcat Web Application Manager access	1
104.128.144.131	147.237.77.178	Canada	e.matpash.idf.il	ET SCAN NMAP -sS window 4096	1
80.82.78.38	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
46.4.79.76	147.237.0.34	Germany	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
218.55.21.53	147.237.0.19	Korea, Republic of	madim.atal.idf.il	SERVER-APACHE Apache Tomcat Web Application Manager access	1
106.39.38.20	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.114	147.237.8.45	Ukraine	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
46.4.79.76	147.237.0.16	Germany	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.19.85.83	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.83	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.83	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.83	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
52.8.82.27	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
79.181.245.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.135.65.145	France	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
66.249.66.64	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.49.41	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
46.120.2.214	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
2.55.20.153	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
2.55.20.153	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.237	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
46.19.85.237	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
5.22.135.179	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.201	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
106.186.113.132	Japan	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.120.2.214	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
218.55.21.53	Korea, Republic of	147.237.0.35	akaws.idf.il	drop		drop	1
37.26.148.217	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.99	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.194	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.51	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
5.39.222.159	Netherlands	147.237.0.35	akaws.idf.il	drop		drop	1
141.212.122.202	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
106.186.113.132	Japan	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
37.187.114.171	France	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.99	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.195	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.70	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
5.39.222.159	Netherlands	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.202	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
106.186.113.132	Japan	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.116	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.199	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
97.88.213.192	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
216.218.206.78	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.39.222.159	Netherlands	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.203	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
123.126.113.154	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
62.138.3.98	Germany	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.223	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.22.131.26	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.200	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
97.88.213.192	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
218.55.21.53	Korea, Republic of	147.237.0.33	idf.il	drop		drop	1
184.105.139.75	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
123.126.113.154	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.112.89.76	Romania	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 79.112.89.76	Block	5
5.39.222.159	Netherlands	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
137.186.92.195	Canada	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/wp-login.php	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/gyus/forum/asp/showforum.asp	Block	1
218.55.21.53	Korea, Republic of	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/manager/html	Block	1
98.214.123.91	United States	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
37.187.114.171	France	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to /irj/portal	Block	1
157.55.39.234	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/brothers/skira/default.asp	None	1
68.180.230.45	United States	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 68.180.230.45	Block	1
218.55.21.53	Korea, Republic of	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/manager/html	Block	1
98.214.123.91	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/wp-login.php	Block	1
40.77.167.20	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
184.105.247.195	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dover/site/homepage/asp	Block	1
109.253.132.207	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/newsarchive.aspx	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/gyus/general.aspx	Block	1
207.46.13.72	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
137.186.92.195	Canada	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/gyus/forum/asp/showforum.asp	Block	1
207.241.237.222	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/imagevideogallerylobby/imagevideogallerylobby.aspx	Block	1
79.112.89.76	Romania	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1