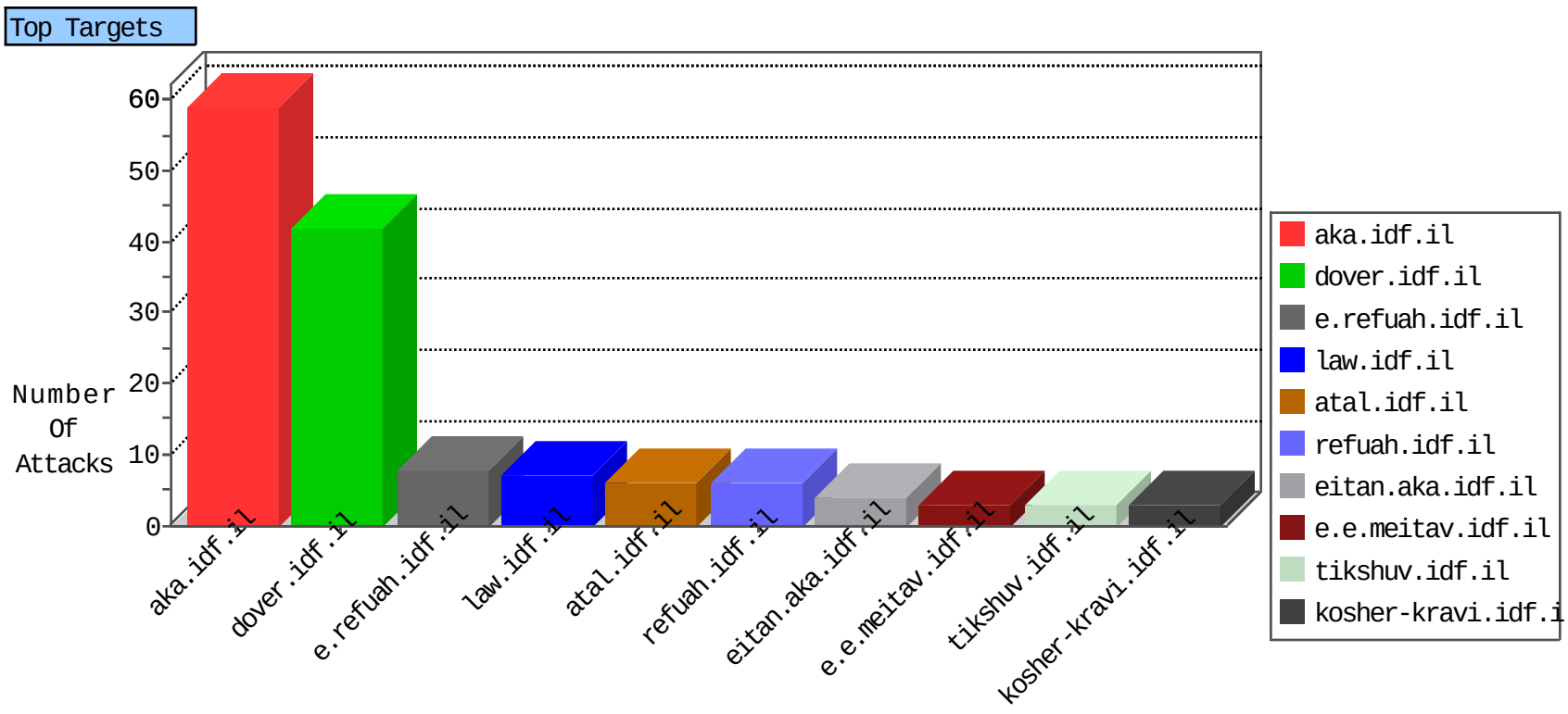
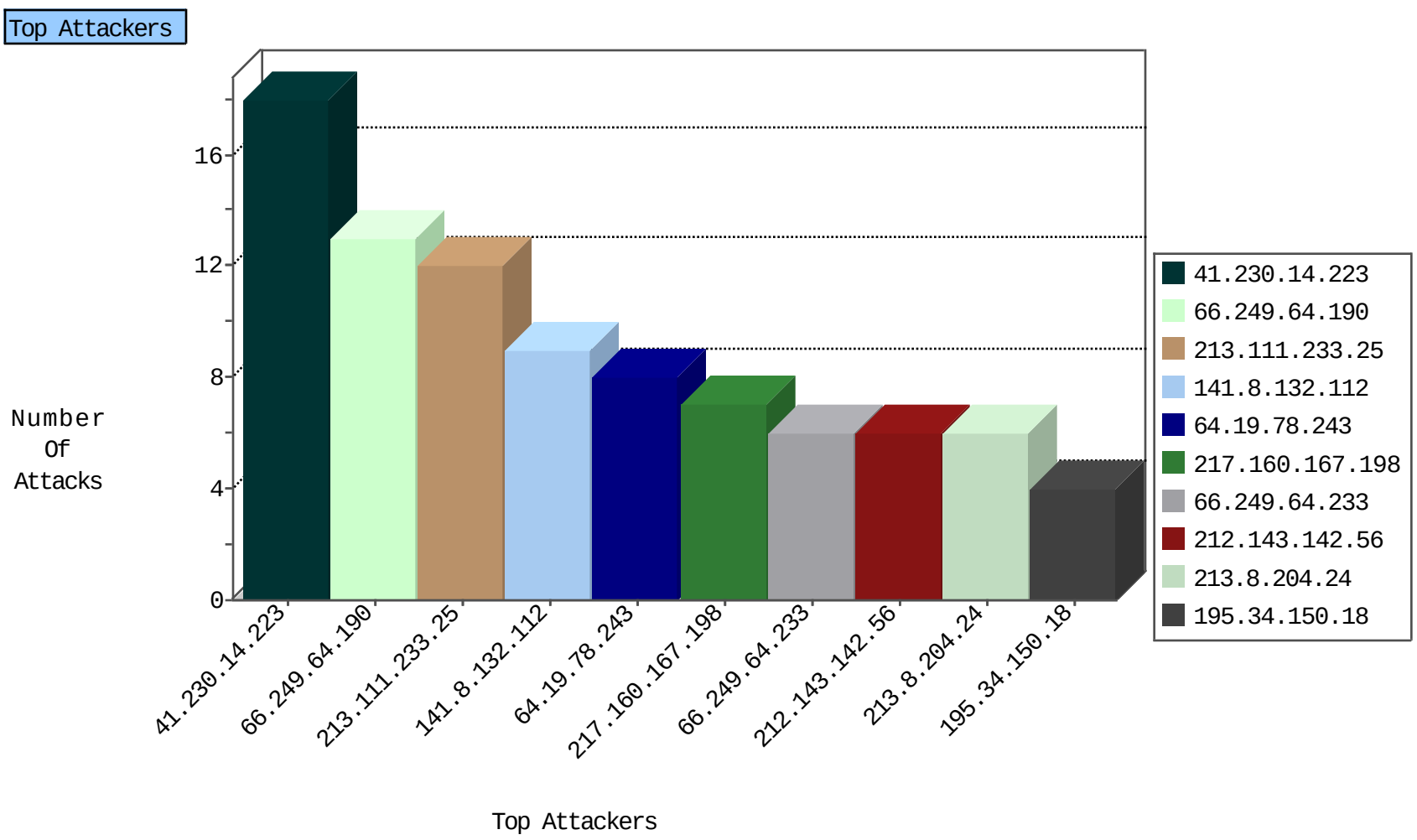
03-06-2016-04:04:06 to 03-06-2016-05:04:06

IDF Under Attack Daily Report





03-06-2016-04:04:06 to 03-06-2016-05:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
134.147.203.115	Germany	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	2
134.147.203.115	Germany	147.237.77.205	prisha.idf.il	Block_Ntp_All_Net	drop	2
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1

03-06-2016-04:04:06 to 03-06-2016-05:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.12.55	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
207.46.13.70	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
66.249.66.187	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-06-2016-04:04:06 to 03-06-2016-05:04:06

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	4
66.249.64.34	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	2
196.47.173.21	147.237.76.38	Cote D'Ivoire	e.e.meitav.idf.il	ET SCAN NMAP -sS window 2048	1
177.158.21.202	147.237.0.33	Brazil	idf.il	ET SCAN NMAP -sS window 2048	1
106.240.247.42	147.237.76.86	Korea, Republic of	navy.idf.il	ET SCAN Potential SSH Scan	1
85.93.5.65	147.237.77.233	Germany	atal.idf.il	ET SCAN Potential SSH Scan	1
52.87.243.150	147.237.76.148	United States	gqcenter.aka.idf.i	ET SCAN NMAP -sS window 1024	1
196.47.173.21	147.237.76.38	Cote D'Ivoire	e.e.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
196.47.173.21	147.237.76.38	Cote D'Ivoire	e.e.meitav.idf.il	ET SCAN NMAP -f -sS	1
191.109.40.47	147.237.76.30	Colombia	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
177.158.21.202	147.237.0.33	Brazil	idf.il	ET SCAN NMAP -f -sS	1
104.128.144.131	147.237.8.24	Canada	e.lifestyle.idf.il	ET SCAN NMAP -sS window 3072	1
218.246.0.97	147.237.77.235	China	sviva.idf.il	ET SCAN NMAP -sS window 1024	1

03-06-2016-04:04:06 to 03-06-2016-05:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
64.19.78.243	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	8
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
41.230.14.223	Tunisia	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
217.160.167.198	Germany	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
199.30.25.139	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
80.179.9.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
46.19.85.102	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
208.115.113.89	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.100	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
74.82.47.56	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.244	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.244	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
94.102.48.193	Netherlands	147.237.0.35	akaws.idf.il	drop	SAM rule	drop	1
184.105.139.102	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
184.105.247.251	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.250	United States	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
106.38.241.106	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
216.218.206.96	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.111	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.94.32.197	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
37.26.148.224	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
195.62.53.168	Russian Federation	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
146.185.239.102	Russian Federation	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
184.105.139.124	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.232	United States	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.94.32.197	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
37.46.41.103	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.100	United States	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
106.38.241.106	China	147.237.77.233	atal.idf.il	drop	SAM rule	drop	1
74.82.47.26	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.239	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.235	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
94.102.48.193	Netherlands	147.237.0.15	kosher-kravi.idf.il	drop	SAM rule	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.230.14.223	Tunisia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	7
213.111.233.25	Ukraine	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	6
66.249.64.233	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	6
213.111.233.25	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 213.111.233.25	Block	5
66.249.64.190	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.190	Block	3
41.230.14.223	Tunisia	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/https:/www.facebook.com/meitavidf&width=338&height=315&show_faces=false&colorscheme=light&stream=true&show_border=false&header=false	Block	3
73.22.155.10	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/	Block	2
41.230.14.223	Tunisia	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 41.230.14.223	Block	2
185.24.76.136	Israel	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
92.37.203.100	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation f in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
213.8.204.24	Israel	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	1
184.105.139.68	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/paratroopers	Block	1
203.133.170.162	Korea, Republic of	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
92.37.203.100	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation l in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
66.249.64.190	United States	147.237.72.166	aka.idf.il	Unknown Parameter Do in www.aka.idf.il/giyus/general/default.asp	None	1
213.8.204.24	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/xmlrpc.php	Block	1
185.24.76.136	Israel	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
213.111.233.25	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/index.php	Block	1
207.46.13.5	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
92.99.14.14	United Arab Emirates	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
213.8.204.24	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
185.24.76.136	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1
89.138.106.196	Israel	147.237.77.233	atal.idf.il	Distributed PHP Attempt	Block	1
217.160.167.198	Germany	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 217.160.167.198 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
213.8.204.24	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
92.99.14.14	United Arab Emirates	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
66.249.64.239	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to chinuch.aka.idf.il/404.htm	Block	1
213.8.204.24	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
185.24.76.136	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
89.138.106.196	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/xmlrpc.php	Block	1
213.8.204.24	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 213.8.204.24	Block	1
149.88.71.234	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
66.249.66.65	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/164-3952	Block	1