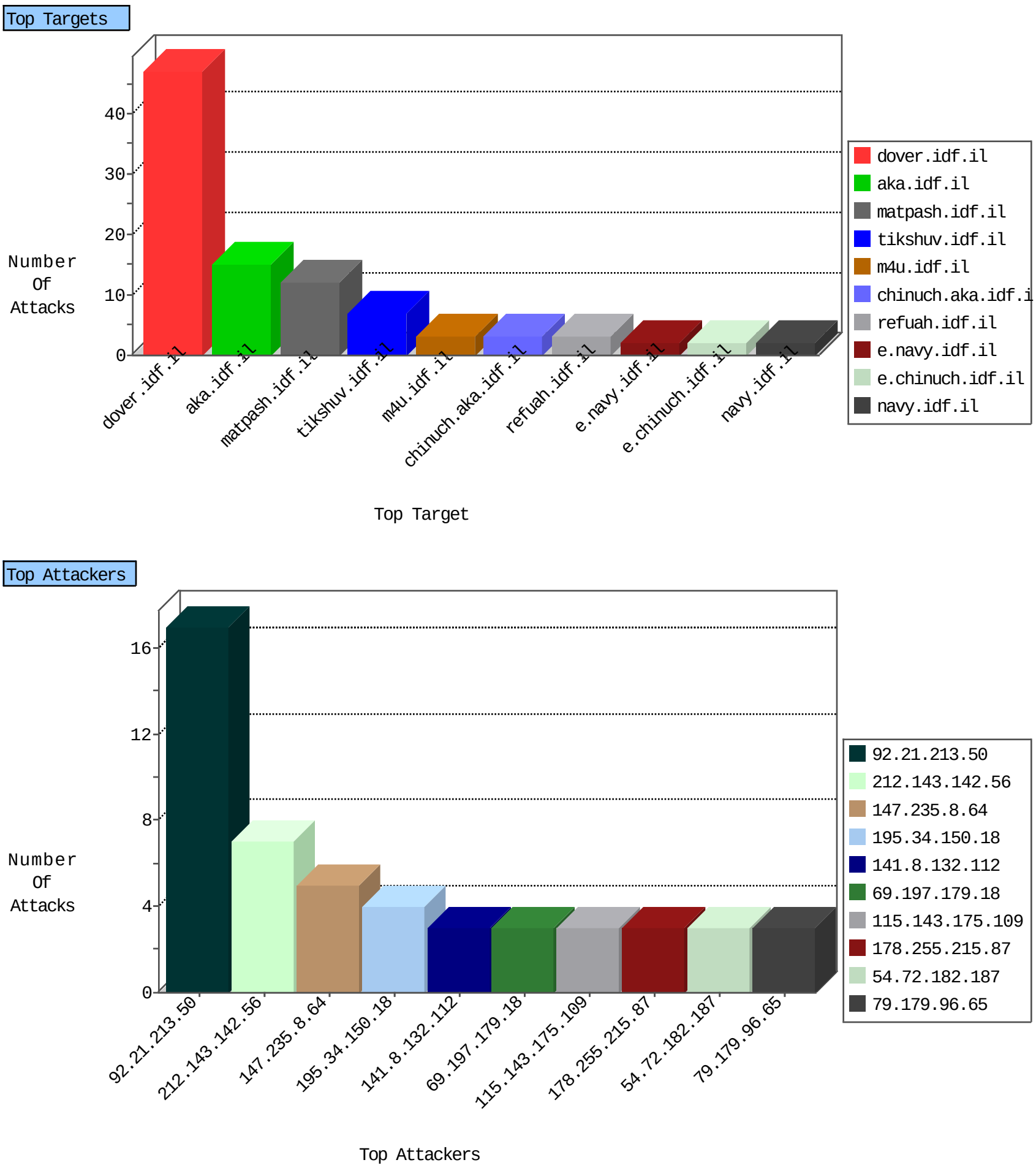
03-09-2016-03:04:05 to 03-09-2016-04:04:05

IDF Under Attack Daily Report



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

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
185.35.62.52	Switzerland	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
115.143.175.109	Korea, Republic of	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.228		147.237.8.46	e.chinuch.idf.il	Block_Udp_All_Nets	drop	1
104.156.246.165	United States	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
115.143.175.109	Korea, Republic of	147.237.0.35	akaws.idf.il	Block_Udp_All_Nets	drop	1
216.218.206.95	United States	147.237.77.179	e.mazi.idf.il	Block_Udp_All_Nets	drop	1
104.156.246.165	United States	147.237.77.205	prisha.idf.il	Block_Ntp_All_Net	drop	1
185.35.62.38	Switzerland	147.237.0.16	my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
115.143.175.109	Korea, Republic of	147.237.0.33	idf.il	Block_Udp_All_Nets	drop	1

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

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
61.135.189.69	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	2
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.66.184	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
188.166.239.76	Russian Federation	147.237.77.216	dover.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

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

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
218.246.0.97	147.237.76.202	China	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
208.67.1.194	147.237.0.200	United States	m4u.idf.il	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
208.67.1.194	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
93.189.26.18	147.237.72.14	Austria	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1

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

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
92.21.213.50	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
92.21.213.50	United Kingdom	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.96.65	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.255.215.87	France	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
130.193.37.16	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
147.235.8.64	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
77.237.138.202	Czech Republic	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
92.21.213.50	United Kingdom	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid sequence number	monitor	2
92.21.213.50	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
74.82.47.18	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
2.52.20.125	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
212.47.246.187	France	147.237.8.46	e.chinuch.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
87.70.24.213	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
69.197.179.18	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
147.235.8.64	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
94.230.93.4	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.42	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
2.52.20.125	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.208	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
69.197.179.18	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
94.230.93.33	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
31.39.188.171	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.96	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.209	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
69.197.179.18	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
159.226.95.66	China	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
123.125.71.18	China	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
37.130.227.133	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
147.235.8.64	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
70.193.56.117	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
80.178.98.54	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
61.135.189.69	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
147.235.8.64	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

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

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.224	Block	3
118.173.86.49	Thailand	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.17	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/dynamic_map/dynamic_map.aspx	Block	1
79.178.165.170	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$29 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
24.30.148.57	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
157.55.39.65	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/miluim/scriptresource.axd	Block	1
80.178.98.54	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
40.77.167.82	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
190.42.120.213	Peru	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.178.98.54	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.102.7.226	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
212.143.38.222	Israel	147.237.0.34	tikshuv.idf.il	PHP Attempt	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1381-he/dover.aspx	Block	1
92.21.213.50	United Kingdom	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.102.7.240	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
212.143.38.222	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/xmlrpc.php	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
24.30.148.57	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	1

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