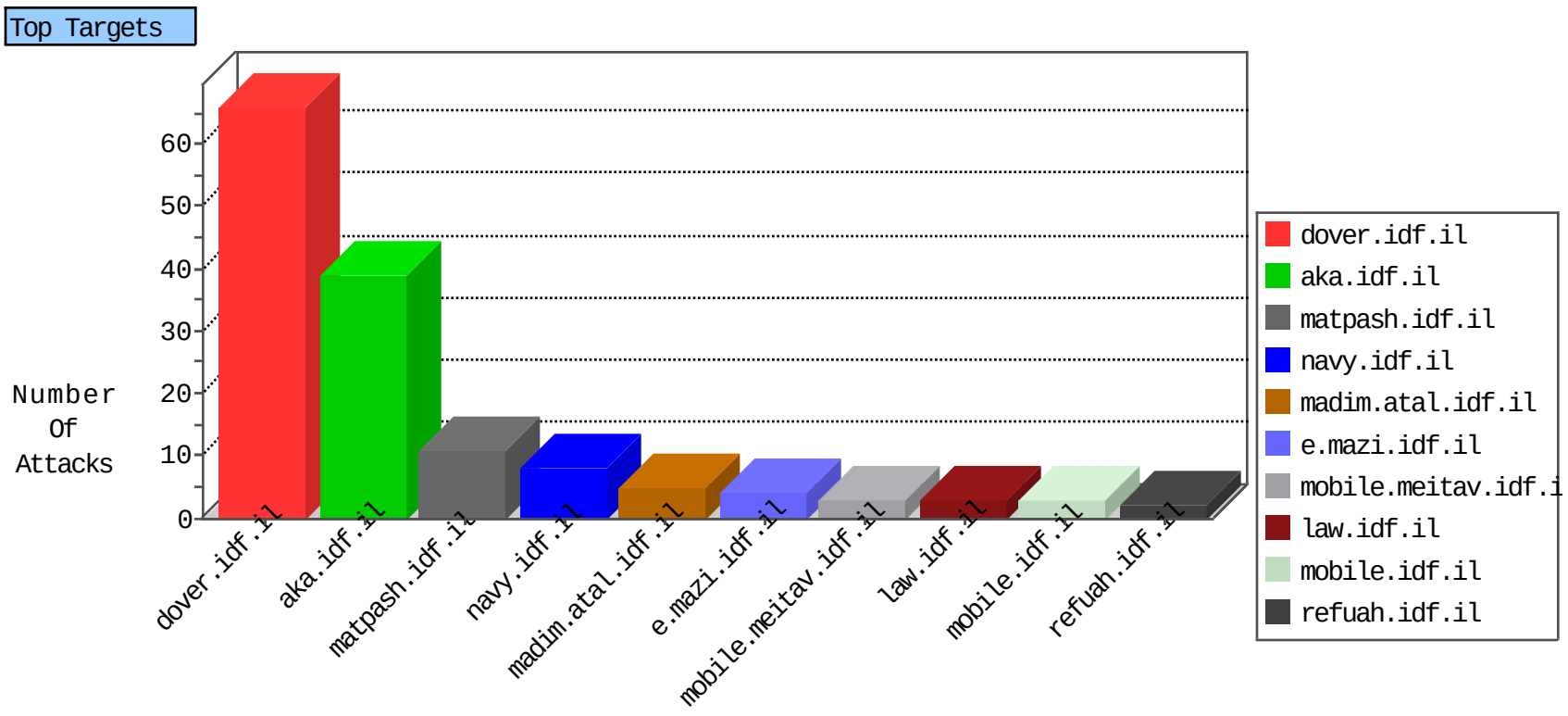
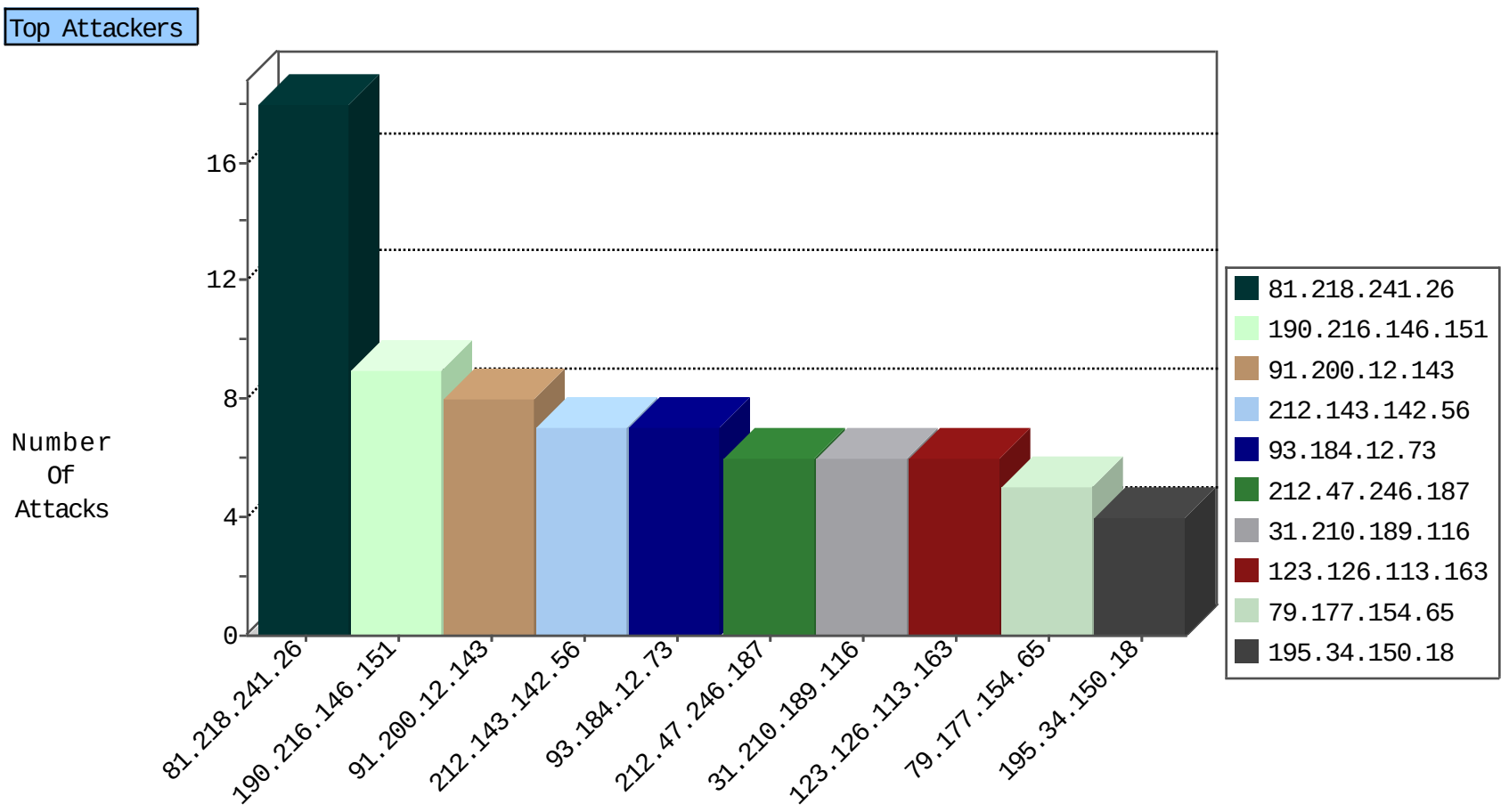
03-10-2016-03:04:04 to 03-10-2016-04:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-10-2016-03:04:04 to 03-10-2016-04:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
184.105.247.198	United States	147.237.8.28	e.mobile-ks.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
82.221.105.6	Iceland	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1

03-10-2016-03:04:04 to 03-10-2016-04:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.163	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
46.4.32.75	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
69.30.198.186	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
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
66.249.66.184	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-10-2016-03:04:04 to 03-10-2016-04:04:04

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
94.102.48.193	147.237.77.216	Netherlands	dover.idf.il	ET SCAN NMAP -sS window 1024	1
190.216.146.151	147.237.76.86	Chile	navy.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.114	147.237.0.200	Ukraine	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
190.216.146.151	147.237.0.33	Chile	idf.il	ET SCAN Potential SSH Scan	1
23.96.109.87	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sS window 4096	1
190.216.146.151	147.237.0.17	Chile	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
23.96.109.87	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -f -sS	1
151.11.201.3	147.237.77.216	Italy	dover.idf.il	ET SCAN NMAP -sS window 3072	1
151.11.201.3	147.237.77.216	Italy	dover.idf.il	ET SCAN NMAP -f -sS	1
218.246.0.97	147.237.76.176	China	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
119.10.114.32	147.237.0.19	China	madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
104.207.135.64	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 3072	1
190.216.146.151	147.237.76.177	Chile	ncore.idf.il	ET SCAN Potential SSH Scan	1
104.207.135.64	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -f -sS	1
190.216.146.151	147.237.76.147	Chile	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
93.189.26.18	147.237.8.45	Austria	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
190.216.146.151	147.237.0.35	Chile	akaws.idf.il	ET SCAN Potential SSH Scan	1
82.117.208.243	147.237.76.147		chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
190.216.146.151	147.237.0.19	Chile	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
23.96.109.87	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sS window 2048	1
182.162.20.47	147.237.77.216	Korea, Republic of	dover.idf.il	ET SCAN NMAP -sS window 1024	1
151.11.201.3	147.237.77.216	Italy	dover.idf.il	ET SCAN NMAP -sS window 2048	1
119.10.114.32	147.237.0.19	China	madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
209.126.116.147	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
119.10.114.32	147.237.0.19	China	madim.atal.idf.il	ET SCAN NMAP -f -sS	1
190.216.146.151	147.237.76.199	Chile	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
104.207.135.64	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 2048	1
190.216.146.151	147.237.76.148	Chile	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1

03-10-2016-03:04:04 to 03-10-2016-04:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
93.184.12.73	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
31.210.189.116	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
91.200.12.143	Ukraine	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
91.200.12.143	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
2.54.85.73	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	4
79.181.150.82	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
24.207.218.19	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
204.79.180.102	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.154.65	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
123.126.113.163	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
84.227.99.213	Switzerland	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
5.22.135.235	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
212.47.246.187	France	147.237.77.61	e.cogat.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.99	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
212.47.246.187	France	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
109.65.56.72	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
212.47.246.187	France	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.119.167.19		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
74.82.47.20	United States	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
212.47.246.187	France	147.237.8.24	e.lifestyle.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.119.167.19		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
79.177.154.65	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
212.47.246.187	France	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.8.132.67	Russian Federation	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
213.8.204.48	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
195.62.53.168	Russian Federation	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
94.230.86.86	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
79.177.154.65	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
212.47.246.187	France	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
85.64.229.229	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
221.199.217.173	Australia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
96.244.197.50	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

03-10-2016-03:04:04 to 03-10-2016-04:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
131.253.25.173	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
66.102.7.226	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
199.30.24.192	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
207.241.229.225	United States	147.237.76.200	eitan.aka.idf.i	Unauthorized URL Access to www.eitan.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
156.199.3.206		147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/main.asp	Block	1
156.199.93.207		147.237.77.233	atal.idf.il	PHP Attempt	Block	1
94.230.93.106	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
156.199.3.206		147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/xmlrpc.php	Block	1
84.109.202.86	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
17.142.156.109	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1
156.199.93.207		147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/xmlrpc.php	Block	1
94.230.93.122	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
156.199.22.162		147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
94.230.93.13	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
40.77.167.33	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
157.55.12.65	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.66.176	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/0/880.pdf	Block	1
156.199.22.162		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
94.230.93.26	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
141.8.132.95	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx	Block	1
156.199.25.11		147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/xmlrpc.php	Block	1
94.230.93.96	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.102.7.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1

03-10-2016-03:04:04 to 03-10-2016-04:04:04