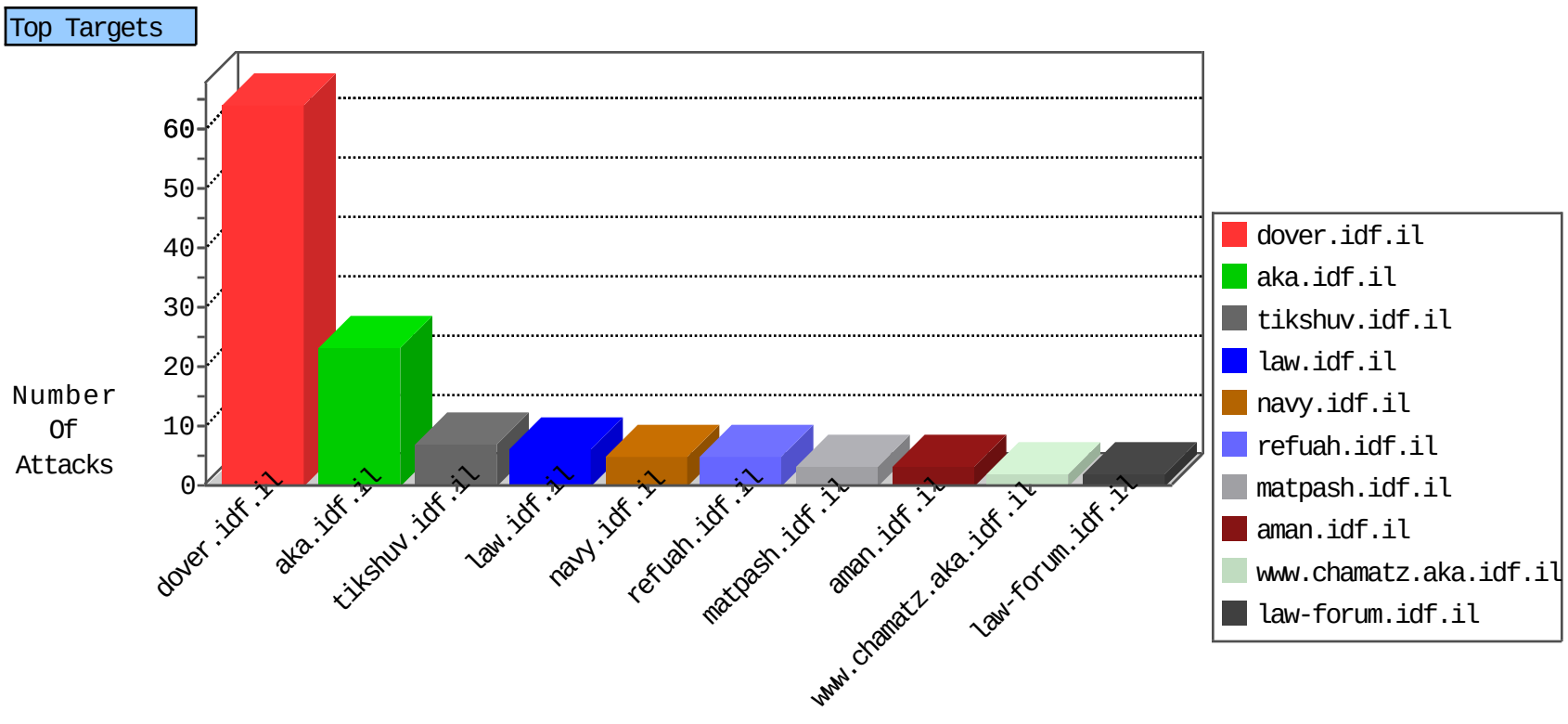
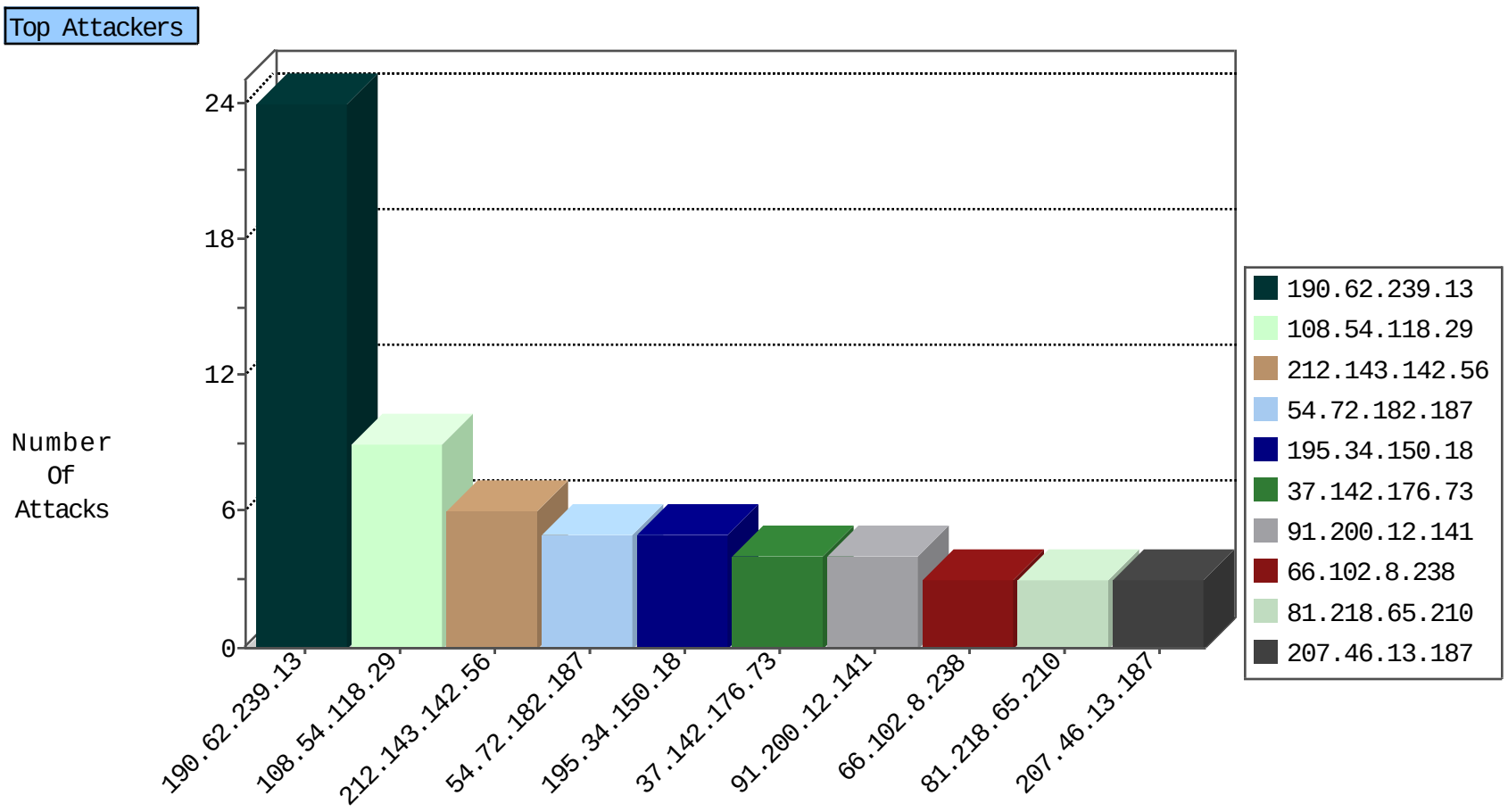
03-09-2016-05:04:09 to 03-09-2016-06:04:09

IDF Under Attack Daily Report



Top Target



Top Attackers

03-09-2016-05:04:09 to 03-09-2016-06:04:09

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	5
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
185.130.5.228		147.237.0.35	akaws.idf.il	Block_Udp_All_Nets	drop	1
104.156.246.165	United States	147.237.77.61	e.cogat.idf.il	Block_Ntp_All_Net	drop	1
23.228.107.104	United States	147.237.72.167	ishurim.aka.idf.il	Block_Ntp_All_Net	drop	1
71.6.216.40	United States	147.237.72.217	e.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.80	United States	147.237.77.176	matpash.idf.il	Block_Ntp_All_Net	drop	1
39.166.206.159	China	147.237.77.121	e.navy.idf.il	Block_Udp_All_Nets	drop	1
71.6.216.50	United States	147.237.77.179	e.mazi.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.88	United States	147.237.72.14	dover.idf.il(old)	Block_Ntp_All_Net	drop	1
49.80.195.83	China	147.237.77.121	e.navy.idf.il	Block_Udp_All_Nets	drop	1

03-09-2016-05:04:09 to 03-09-2016-06:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.4.32.75	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
66.249.66.184	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
37.142.176.73	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
173.208.136.170	United States	147.237.77.176	matpash.idf.il	C1000016: HTTP: administrator in URI	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-09-2016-05:04:09 to 03-09-2016-06:04:09

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	5
128.127.0.45	147.237.77.19	Italy	law-forum.idf.il	ET SCAN NMAP -sS window 4096	1
104.215.89.20	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 2048	1
98.119.105.221	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 2048	1
94.102.48.193	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
179.43.141.234	147.237.76.42	Switzerland	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
128.127.0.45	147.237.77.19	Italy	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
104.215.89.20	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -f -sS	1
98.119.105.221	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -f -sS	1
89.163.145.38	147.237.77.179	Germany	e.mazi.idf.il	ET SCAN NMAP -sS window 4096	1

03-09-2016-05:04:09 to 03-09-2016-06:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
190.62.239.13	El Salvador	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
190.62.239.13	El Salvador	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
108.54.118.29	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
108.54.118.29	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
87.71.43.83	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
190.62.239.13	El Salvador	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
79.177.48.4	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.142.176.73	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
91.200.12.141	Ukraine	147.237.77.74	law.idf.il	drop	SAM rule	drop	2
109.67.197.184	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
91.200.12.141	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
207.46.13.187	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
91.200.12.143	Ukraine	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	2
141.212.122.210	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
2.54.145.10	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
220.181.108.91	China	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.211	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.247.36.93	Netherlands	147.237.0.35	akaws.idf.il	drop		drop	1
198.20.69.98	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
79.178.223.148	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
8.37.227.69	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
184.105.139.110	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
45.35.64.142		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
131.253.26.244	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
84.110.184.33	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
8.37.227.70	Anonymous Proxy	147.237.72.166	aka.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
65.55.218.51	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
131.253.36.200	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
84.110.184.33	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
37.142.176.73	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
74.82.47.47	United States	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.108	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

03-09-2016-05:04:09 to 03-09-2016-06:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.102.8.238	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
66.102.8.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.102.8.243	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
207.46.13.187	United States	147.237.72.166	aka.idf.il	Unknown Parameter innercatid in aka.idf.il/giyus/qanda/	None	1
66.249.66.36	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
18.107.0.26	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
105.154.240.152	Morocco	147.237.77.74	law.idf.il	PHP Attempt	Block	1
66.249.64.51	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery/global.js	Block	1
66.249.66.187	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/contactus/contactus.aspx	Block	1
105.154.240.152	Morocco	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
66.249.64.137	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1153-he/dover.aspx	Block	1
185.112.248.32		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
66.249.64.143	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english	Block	1
194.72.238.241	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to /	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
74.82.47.3	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
66.249.64.3	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1

03-09-2016-05:04:09 to 03-09-2016-06:04:09