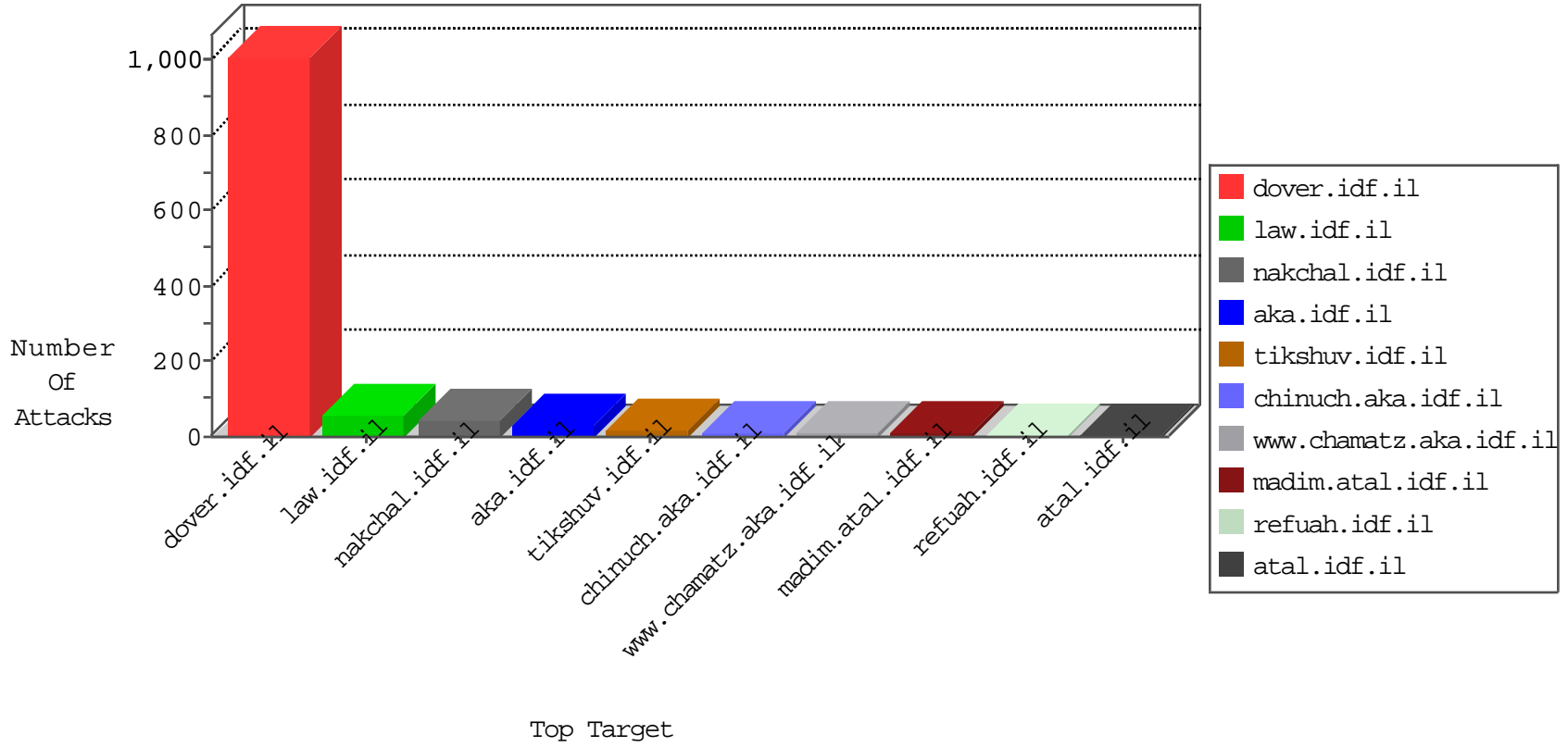


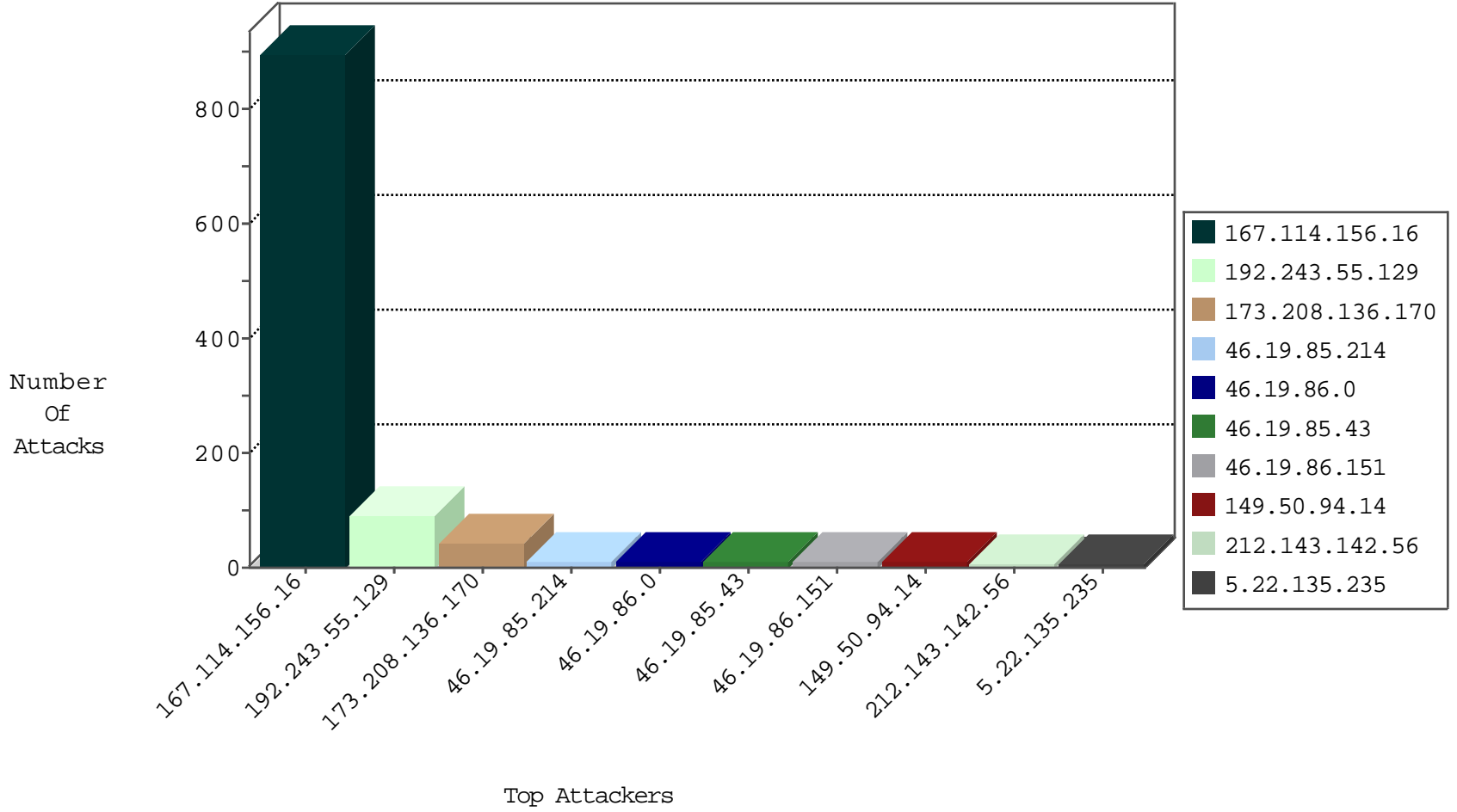
IDF Under Attack Daily Report



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	DOS-Tool-SwitchbladG	dest-reset	3997
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
184.105.139.67	United States	147.237.8.46	e.chinuch.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
89.163.216.214	Germany	147.237.8.46	e.chinuch.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.92	United States	147.237.77.205	prisha.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1		147.237.77.216	dover.idf.il	Block_Ntp_All_Net	drop	1
94.102.49.206	Netherlands	147.237.8.46	e.chinuch.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1		147.237.8.14	e.orchot.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.174		147.237.77.226	www.chamatz.aka.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.50.94.14	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
106.38.241.149	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
46.120.55.50	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
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
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

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
66.249.64.181	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
218.246.0.97	147.237.77.74	China	law.idf.il	ET SCAN NMAP -sS window 1024	1
93.189.26.18	147.237.76.38	Austria	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.98	147.237.76.202	United States	e.halag.idf.il	ET DROP Dshield Block Listed Source	1
179.43.141.234	147.237.0.16	Switzerland	ny-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
82.196.9.182	147.237.8.14	Netherlands	e.orchot.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
192.243.55.129	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
46.19.86.0	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
192.243.55.129	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
192.243.55.129	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
46.19.86.151	Israel	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	10
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
46.19.85.214	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
5.22.135.235	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.43	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.214	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.43	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.129	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.146.252	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
79.183.204.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.129	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	3
37.26.147.233	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.208	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.192	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
83.130.111.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.129	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	2
46.121.94.141	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
185.5.223.11	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
93.172.183.61	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
185.5.223.11	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
2.52.157.232	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
80.246.130.32	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
185.5.223.11	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
74.82.47.51	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.32.179.29	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.90	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
106.120.173.159	China	147.237.77.233	atal.idf.il	drop	SAM rule	drop	1
82.196.9.182	Netherlands	147.237.76.31	nakchal.idf.il	Web Server Enforcement Violation	Masscan Port Scanner	reject	1
46.121.94.141	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
184.105.247.240	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
176.13.20.205	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
84.108.98.134	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.56	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.108	United States	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.102.254.136	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
82.196.9.182	Netherlands	147.237.76.34	yohalan.idf.il	drop		drop	1
176.13.22.3	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
184.105.247.200	United States	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
176.13.4.34	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	1

03-11-2016-07:04:03 to 03-11-2016-08:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
173.208.136.170	United States	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 173.208.136.170	Block	38
173.208.136.170	United States	147.237.76.31	nakchal.idf.il	Multiple Admin Blocking from 173.208.136.170	Block	6
185.120.125.88		147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
87.69.178.174	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.253.142.180	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.243.55.129	Block	1
79.183.204.236	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz/res#012ources/images/innerpage/goback.gif	Block	1
131.253.25.225	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.85.163	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
211.21.2.86	Taiwan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/).html(Block	1
79.183.204.236	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 79.183.204.236	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-he/dover.aspx	Block	1
5.18.229.133	Russian Federation	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/general.aspx	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9712-he/refuah.aspx	Block	1
109.253.133.33	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
38.111.147.84	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/bamachane	Block	1
79.183.26.14	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
40.77.167.82	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/watch	Block	1

03-11-2016-07:04:03 to 03-11-2016-08:04:03