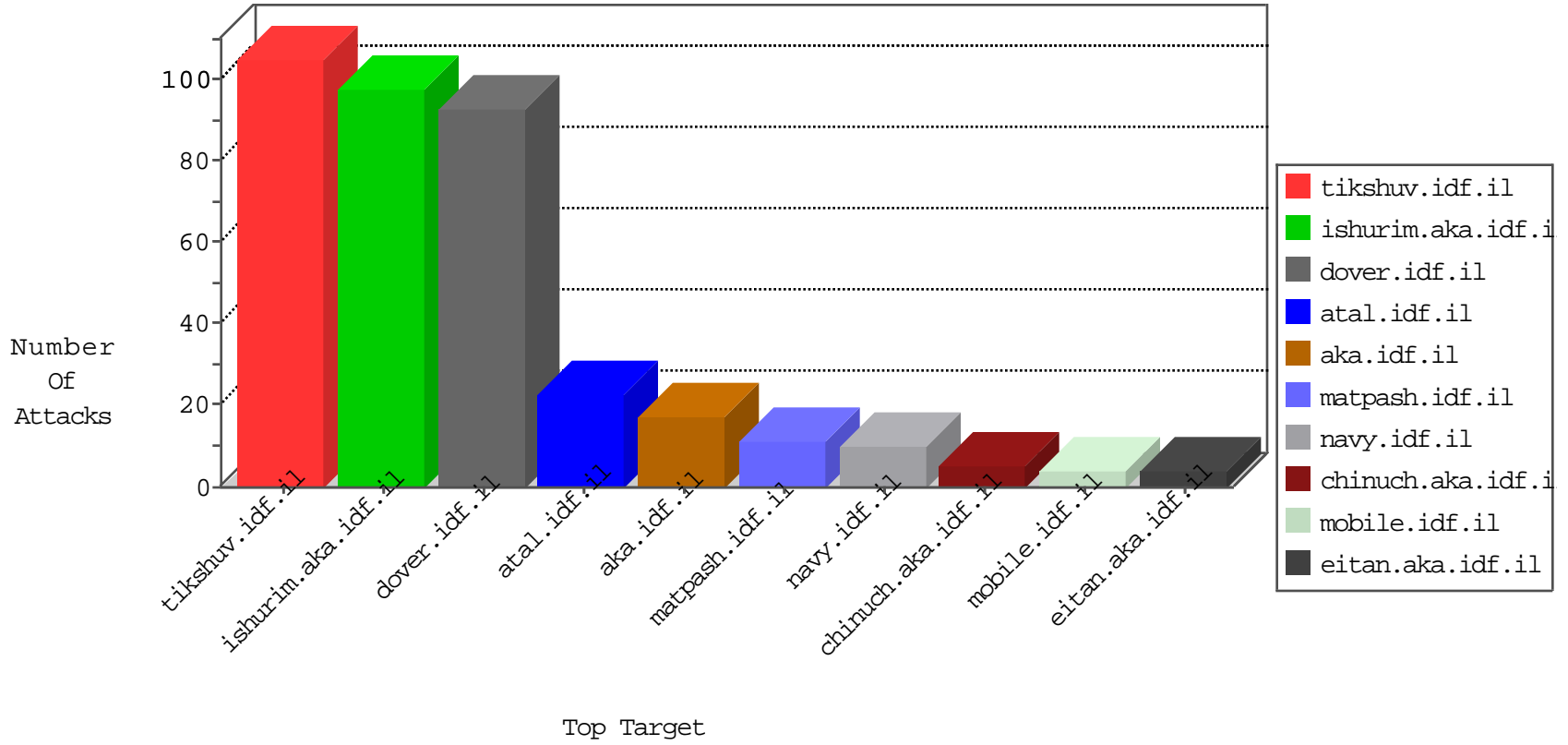


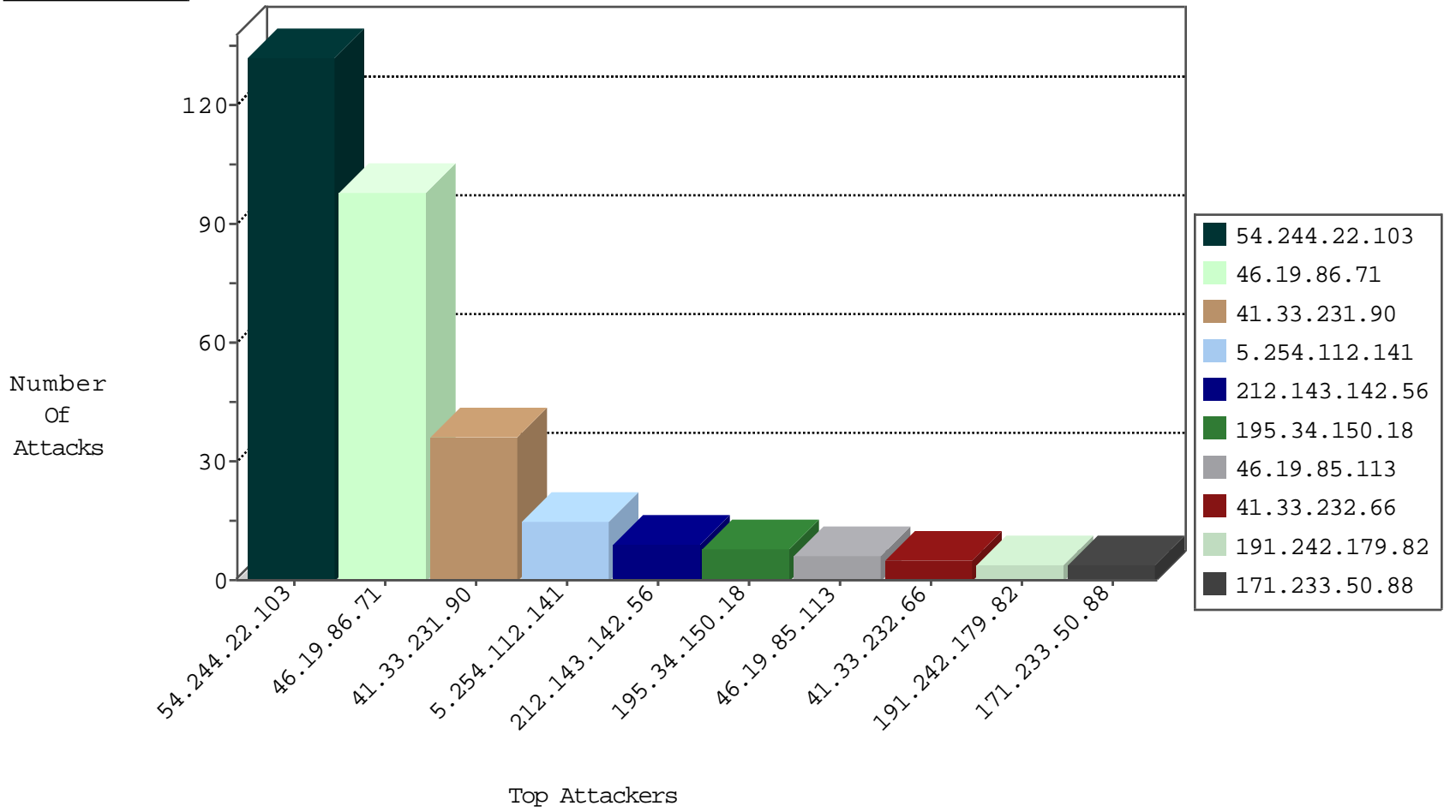
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
115.239.228.10	China	147.237.76.147	chinuch.aka.idf.il	JLM_Under_Attack_Con_Http	drop	2
71.6.135.131	United States	147.237.76.198	e.ychalan.idf.il	Block_Udp_All_Nets	drop	1
146.185.239.100	Russian Federation	147.237.76.200	eitan.aka.idf.il	block-sp-trafl	drop	1
104.207.128.23	United States	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
209.190.52.186	United States	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
104.207.128.23	United States	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.254.112.141	United Kingdom	147.237.76.86	navy.idf.il	0543: HTTP: php.cgi Access	Block	2
5.254.112.141	United Kingdom	147.237.77.216	dover.idf.il	0543: HTTP: php.cgi Access	Block	1
202.69.240.221	Hong Kong	147.237.77.226	www.chamatz.aka.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	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
93.104.213.84	147.237.0.15	Germany	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
190.124.35.115	147.237.77.216	Nicaragua	dover.idf.il	ET SCAN NMAP -sS window 2048	1
190.124.35.115	147.237.77.216	Nicaragua	dover.idf.il	ET SCAN NMAP -f -sS	1
183.60.48.25	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
113.130.201.211	147.237.0.35	Korea, Republic of	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
93.104.213.84	147.237.77.19	Germany	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
190.124.35.115	147.237.77.216	Nicaragua	dover.idf.il	ET SCAN NMAP -sS window 1024	1
187.244.119.116	147.237.72.14	Mexico	dover.idf.il(old)	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
183.60.48.25	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
177.230.131.251	147.237.0.34	Mexico	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
103.41.177.70	147.237.77.212		e.dover.idf.il	ET SCAN NMAP -sS window 3072	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	102
46.19.86.71	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	98
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	23
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.113	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
191.242.179.82	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
80.246.136.198	Israel	147.237.77.243	mobile.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
66.249.78.239	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
52.33.66.29	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	2
167.114.159.9	Canada	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
141.212.122.123	United States	147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.114	United States	147.237.8.46	e.chinuch.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
213.57.181.132	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
79.180.138.78	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.247.215	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.155	United States	147.237.76.148	ggcenter.aka.idf.il	drop		drop	1
141.212.122.118	United States	147.237.0.33	idf.il	drop		drop	1
141.212.122.73	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
194.72.238.241	United Kingdom	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
74.82.47.16	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
54.251.144.191	Singapore	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.126	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.115	United States	147.237.8.46	e.chinuch.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.114	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
184.105.247.251	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
69.137.61.138	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
141.212.122.156	United States	147.237.76.148	ggcenter.aka.idf.il	drop		drop	1
54.244.22.103	United States	147.237.0.15	kosher-kravi.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.120	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.74	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
195.28.180.101	Israel	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
74.82.47.22	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
54.251.144.191	Singapore	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.127	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.116	United States	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
83.166.234.5	Russian Federation	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
71.183.222.63	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.157	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.121	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.74	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.26	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.108	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
54.251.144.191	Singapore	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.153	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.117	United States	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.254.112.141	United Kingdom	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 5.254.112.141	Block	7
5.254.112.141	United Kingdom	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.254.112.141	Block	3
192.243.55.138	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.138	Block	2
192.243.55.131	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.131	Block	2
192.243.55.135	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.135	Block	2
192.243.55.137	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.137	Block	2
37.142.68.7	Israel	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
192.243.55.132	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/gyus/general.aspx?catid=59329&docid=64979	Block	1
74.82.47.2	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
192.243.55.130	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/gyus/general.aspx?catid=58564&docid=35722	Block	1
37.142.68.7	Israel	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	1
192.243.55.134	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.134	Block	1
157.55.39.138	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/main/sachar/klali.aspx	None	1
5.254.112.141	United Kingdom	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/cgi-bin/php	Block	1
194.72.238.241	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to /	Block	1
66.249.64.198	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1769	Block	1
185.25.151.159	Poland	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to testp3.pospr.waw.pl/testproxy.php	Block	1
192.243.55.131	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gyus/kadatz	Block	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1414-10828-he/dover.aspx	Block	1
192.243.55.136	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.136	Block	1
188.143.232.70	Russian Federation	147.237.77.176	matpash.idf.il	Parameter Type Violation fromDate in www.cogat.idf.il/901-en/cogat.aspx	Block	1
5.254.112.141	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to ww.idf.il/cgi-bin/php	Block	1
192.243.55.132	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.132	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to ww.idf.il/atall/izkor/view_img.asp	Block	1
192.243.55.129	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/gyus/general.aspx?catid=59268&docid=65384	Block	1