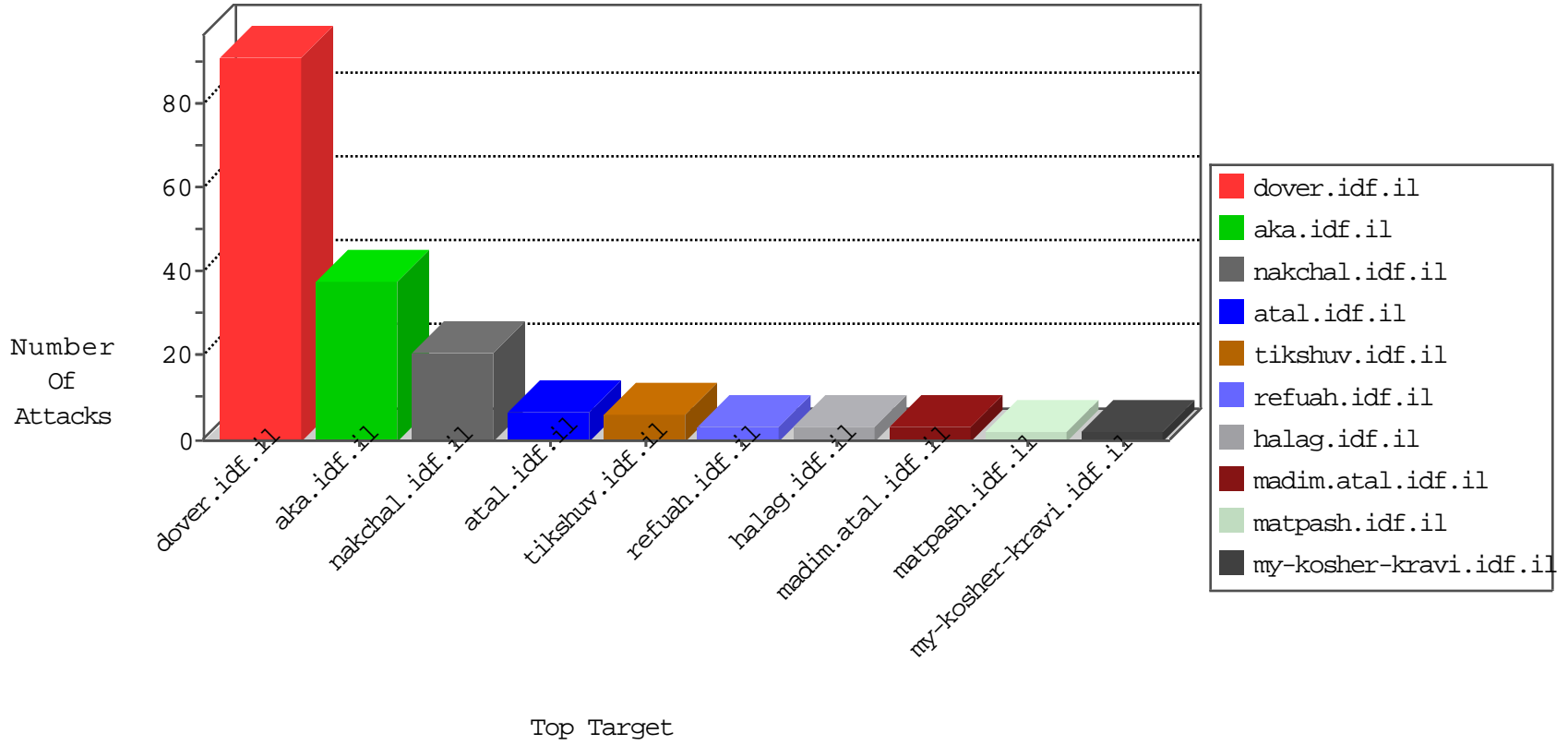


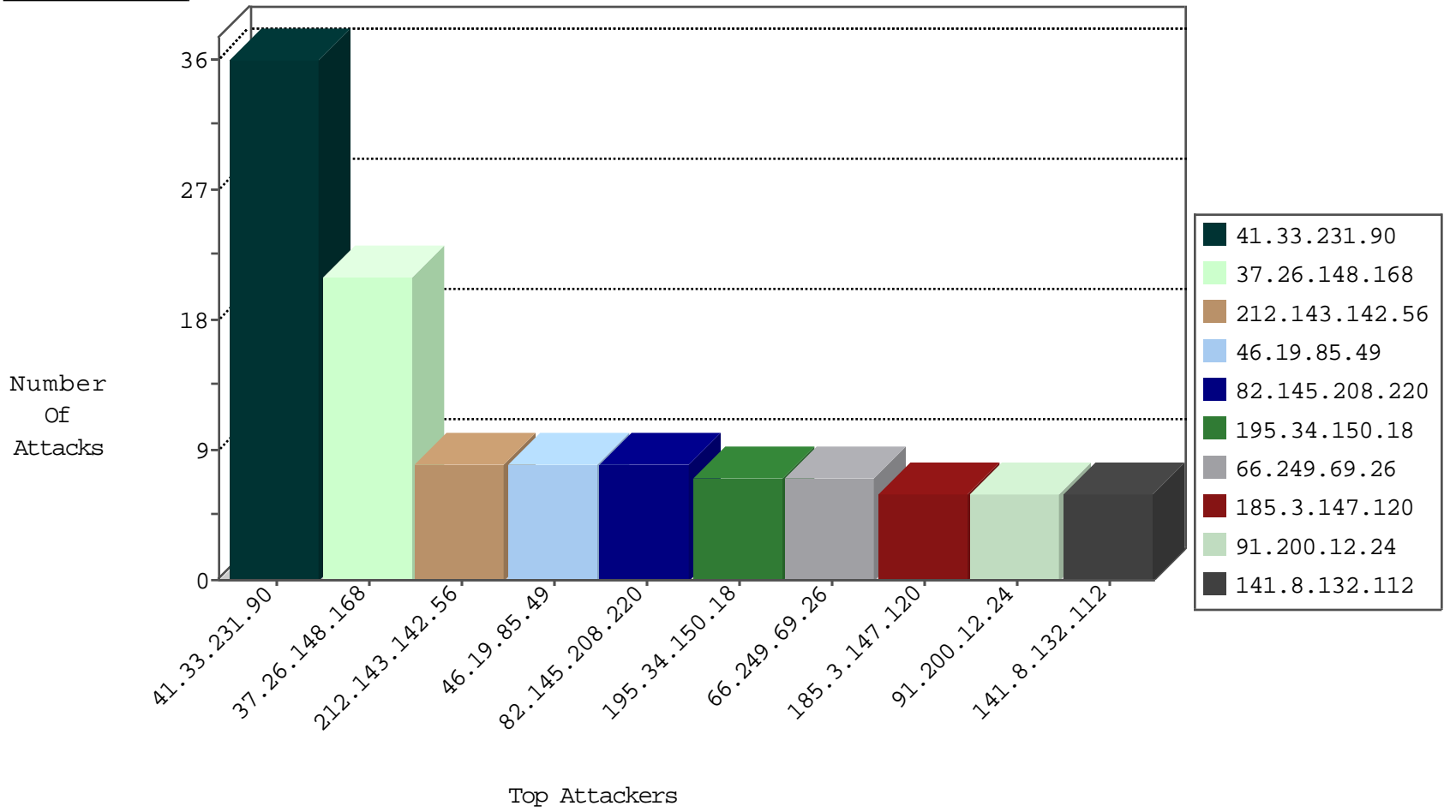
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

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	3
94.102.48.193	147.237.77.234	Netherlands	halag.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.114	147.237.0.19	Ukraine	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
69.197.145.242	147.237.77.179	United States	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
69.197.145.242	147.237.76.201	United States	e.atal.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.193	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.114	147.237.0.19	Ukraine	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
69.197.145.242	147.237.77.61	United States	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
69.197.145.242	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
37.26.148.168	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
82.145.208.220	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
185.3.147.120	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
91.200.12.24	Ukraine	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
46.19.85.49	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
82.145.218.133	Europe	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
46.19.86.70	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.49	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
79.180.26.109	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
5.22.130.96	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.172	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.26.148.254	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
137.116.71.170	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
37.26.148.254	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
104.45.18.178	United States	147.237.77.170	maarachot.idf.il	Instant Messengers	instant messenger pattern found, application: Skype	monitor	1
5.22.130.127	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
37.26.148.254	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
108.6.37.83	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
23.239.23.47	United States	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
157.55.39.161	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
89.138.81.253	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
195.62.53.168	Russian Federation	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
108.6.37.83	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.105.88.65	France	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
178.33.83.219	France	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
128.194.131.235	United States	147.237.72.166	aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
184.105.139.108	United States	147.237.77.216	dover.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
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	7
89.138.81.253	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 89.138.81.253	Block	4
178.137.93.235	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi/	Block	3
98.139.204.18	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 98.139.204.18	Block	3
184.105.139.68	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
98.139.204.18	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
66.249.66.39	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
123.125.71.69	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/3/3203.pdf	Block	1
89.138.81.253	Israel	147.237.0.34	tikshuv.idf.il	Too Many 404: Response Code per Session	Block	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/./shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
98.139.204.33	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wordpress/wp-admin/	Block	1
66.249.66.75	Israel	147.237.77.176	matpash.idf.il	Suspicious Response Code	Block	1
157.55.39.77	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
208.115.111.73	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
104.236.50.16		147.237.0.16	my-kosher-kravi.idf.il	SSL Untraceable Connection - Unsupported Cipher	None	1
165.138.36.2	United States	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/	Block	1
91.200.12.24	Ukraine	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/fckeditor/_whatsnew.html	Block	1
109.232.226.5	Netherlands	147.237.76.42	refuah.idf.il	Distributed Parameter Type Violation on www.refua.atal.idf.il/templates/sendtofriend/sendtofriend.aspx parameter &l	Block	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-7909-he/dover.aspx	Block	1
8.37.70.92	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/1326-he/refuah.aspx&usg=alkjrhg7qazpruckvpljcph7guacuooqlg	Block	1
109.232.226.5	Netherlands	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/templates/sendtofriend/sendtofriend.aspx parameter &l	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1781-he/dover.aspx	Block	1