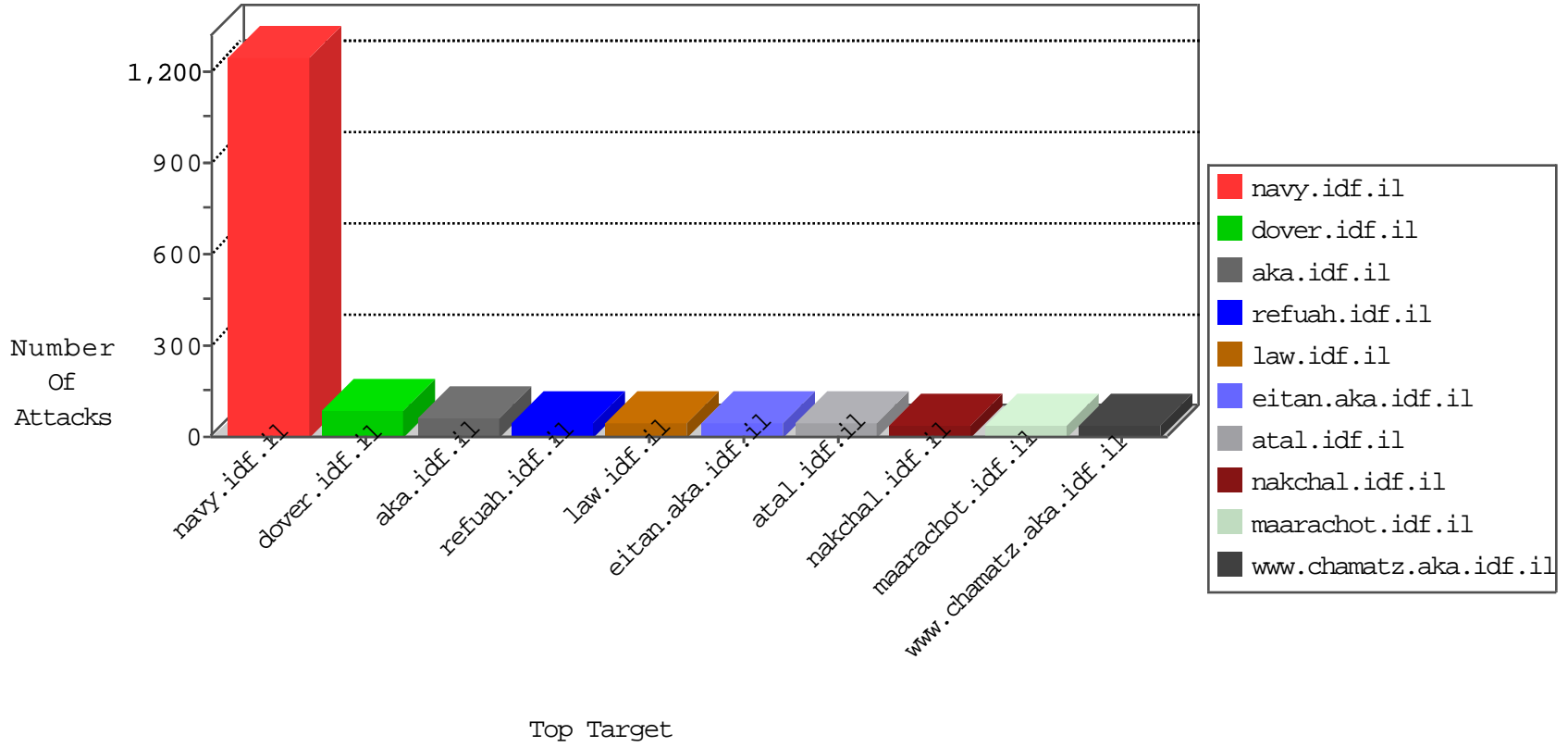


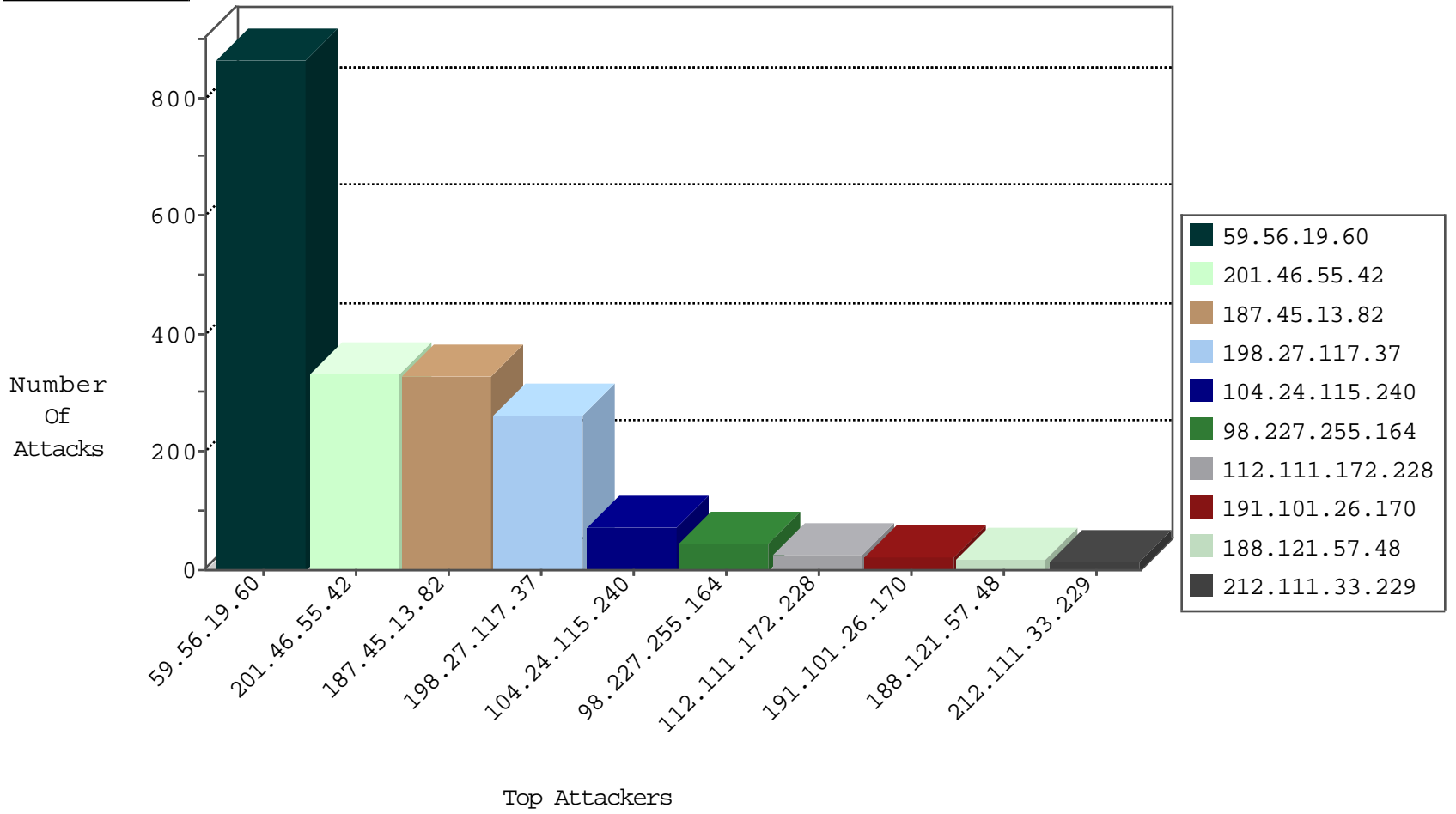
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.65.199.38	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	66
185.94.111.1	Russian Federation	147.237.76.199	e.nakchal.idf.il	Black List	drop	1
207.174.212.180	United States	147.237.0.16	my-kosher-kravi.idf.il	TCP handshake violation, first packet not syn	drop	1

09-10-2016-07:04:05 to 09-10-2016-08:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
1.179.134.194	Thailand	147.237.76.86	navy.idf.i	13076: HTTP: Apache Struts 2 OGNL Command Injection Vulnerability	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
91.201.236.158	147.237.77.205	Ukraine	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.66.102	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sA (2)	1
52.166.130.115	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
45.33.116.208	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
197.44.94.31	147.237.77.170	Egypt	maarachot.idf.il	ET SCAN NMAP -sS window 2048	1
195.88.208.193	147.237.77.205	Russian Federation	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
139.162.168.200	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
139.162.160.132	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.201.236.158	147.237.77.205	Ukraine	prisha.idf.il	ET SCAN NMAP -sS window 2048	1
91.201.236.158	147.237.77.205	Ukraine	prisha.idf.il	ET SCAN NMAP -f -sS	1
66.249.65.191	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	1
45.56.74.212	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
197.44.94.31	147.237.77.170	Egypt	maarachot.idf.il	ET SCAN NMAP -sS window 4096	1
197.44.94.31	147.237.77.170	Egypt	maarachot.idf.il	ET SCAN NMAP -f -sS	1
139.162.168.200	147.237.76.44	United States	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
139.162.168.200	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.158.203.149	147.237.72.166	Netherlands	aka.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
59.56.19.60	China	147.237.76.86	navy.idf.il	SYN Attack		monitor	492
59.56.19.60	China	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	271
198.27.117.37	Canada	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	134
198.27.117.37	Canada	147.237.76.86	navy.idf.il	SYN Attack		monitor	117
59.56.19.60	China	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	64
187.45.13.82	Brazil	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	18
187.45.13.82	Brazil	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
187.45.13.82	Brazil	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
187.45.13.82	Brazil	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
187.45.13.82	Brazil	147.237.76.147	chimuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
201.46.55.42	Brazil	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
187.45.13.82	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
187.45.13.82	Brazil	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
201.46.55.42	Brazil	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
187.45.13.82	Brazil	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
201.46.55.42	Brazil	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
201.46.55.42	Brazil	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
201.46.55.42	Brazil	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
201.46.55.42	Brazil	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
201.46.55.42	Brazil	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
201.46.55.42	Brazil	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
201.46.55.42	Brazil	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
201.46.55.42	Brazil	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
201.46.55.42	Brazil	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
201.46.55.42	Brazil	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
201.46.55.42	Brazil	147.237.76.147	chimuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
201.46.55.42	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
201.46.55.42	Brazil	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
201.46.55.42	Brazil	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
201.46.55.42	Brazil	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
201.46.55.42	Brazil	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
201.46.55.42	Brazil	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
187.45.13.82	Brazil	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
201.46.55.42	Brazil	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
187.45.13.82	Brazil	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
187.45.13.82	Brazil	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
187.45.13.82	Brazil	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
187.45.13.82	Brazil	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
187.45.13.82	Brazil	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
187.45.13.82	Brazil	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
187.45.13.82	Brazil	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
187.45.13.82	Brazil	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
187.45.13.82	Brazil	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
187.45.13.82	Brazil	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
201.46.55.42	Brazil	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
187.45.13.82	Brazil	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
187.45.13.82	Brazil	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
201.46.55.42	Brazil	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
106.38.241.105	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	12
187.45.13.82	Brazil	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12

09-10-2016-07:04:05 to 09-10-2016-08:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
112.111.172.228	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 112.111.172.228	Block	17
112.111.172.228	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	6
109.64.134.122	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012ources/images/innerpage/goback.gif	Block	1
66.249.66.174	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
109.64.134.122	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 109.64.134.122	Block	1
66.249.66.176	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
77.139.89.13	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
109.64.51.153	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
112.111.172.228	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.asp	Block	1

09-10-2016-07:04:05 to 09-10-2016-08:04:05