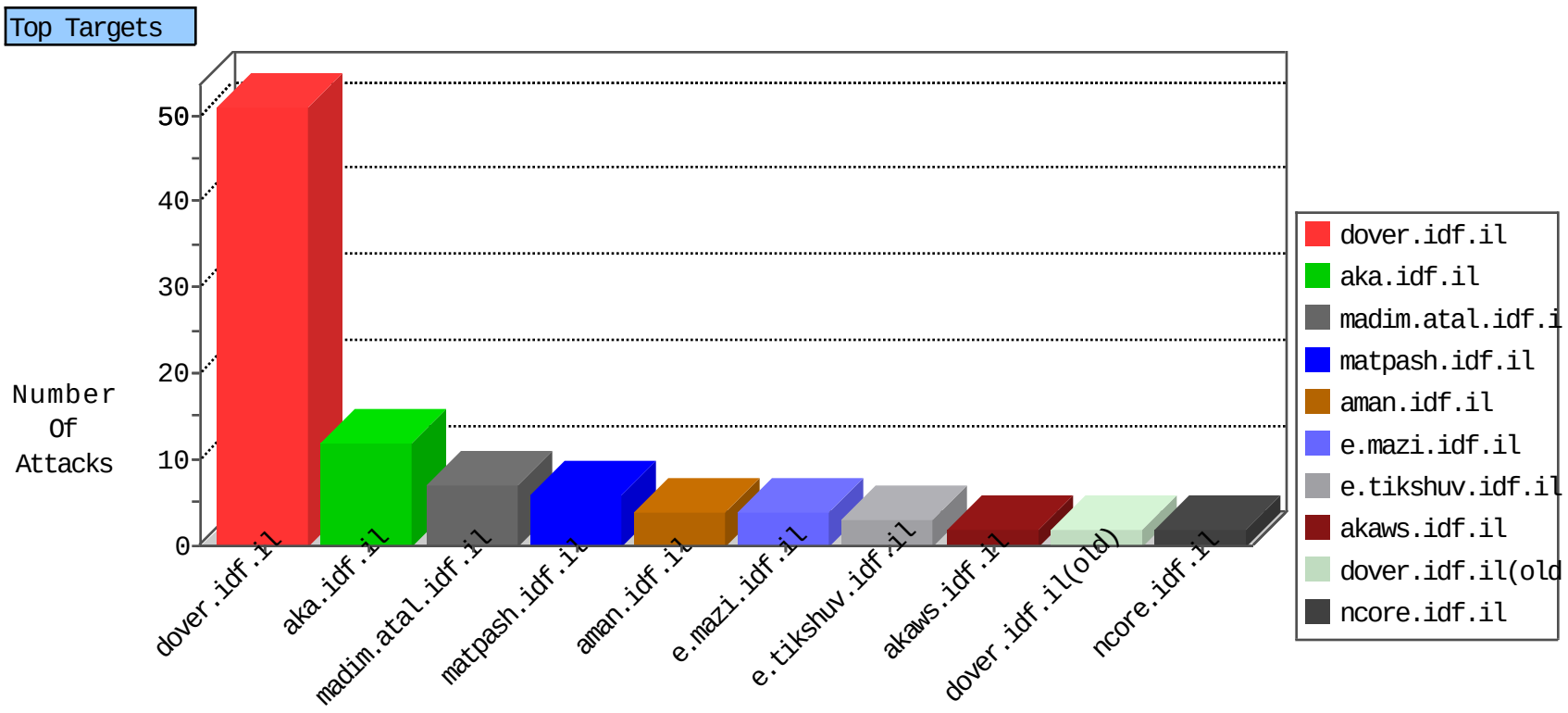
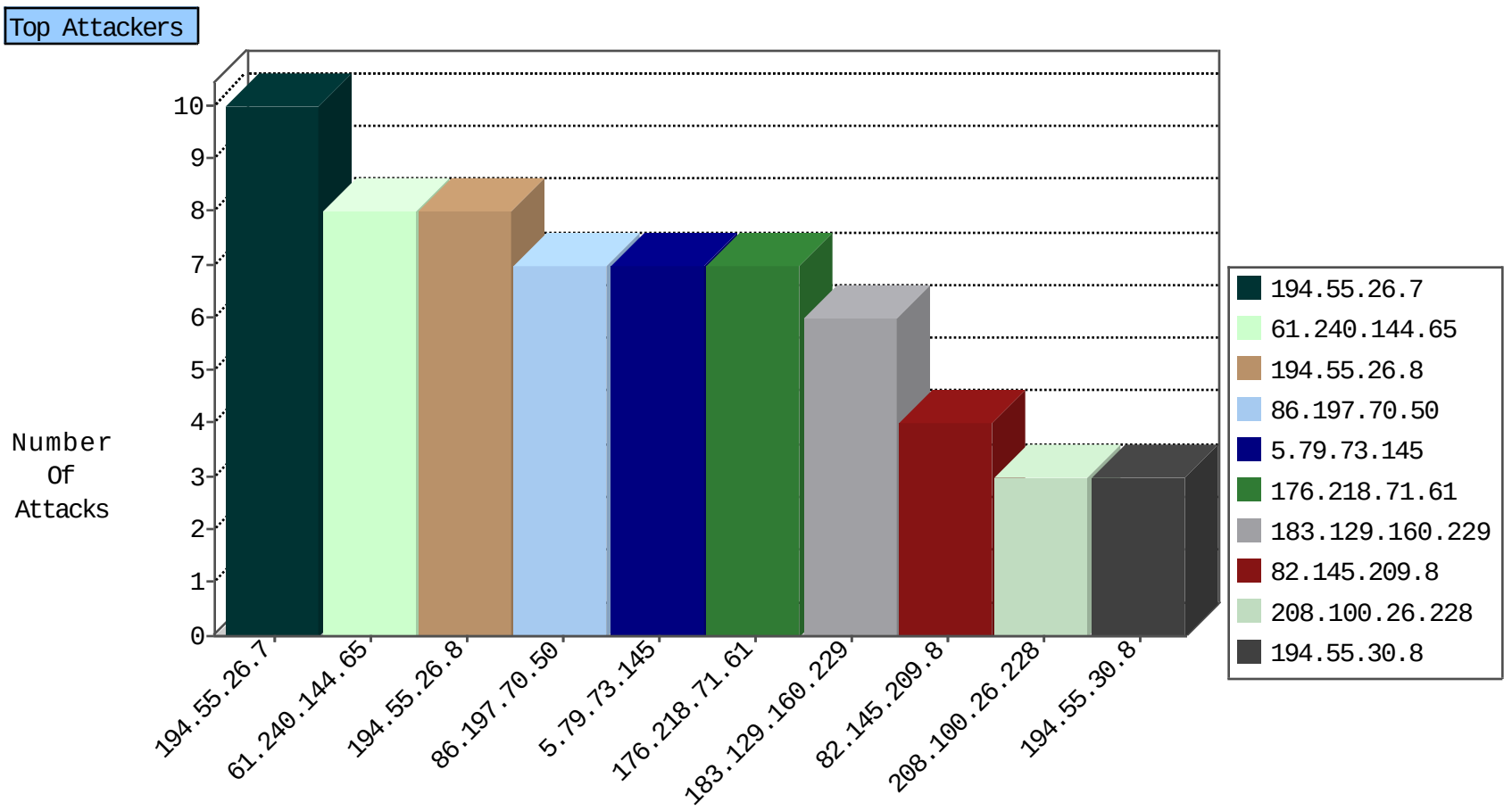
09-02-2016-22:04:06 to 09-02-2016-23:04:06

IDF Under Attack
Daily Report

Top Targets



Top Attackers



09-02-2016-22:04:06 to 09-02-2016-23:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
86.197.70.50	France	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-Url	dest-reset	4
176.218.71.61	Turkey	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
185.128.40.162	Switzerland	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1
217.23.9.123	Netherlands	147.237.76.86	navy.idf.il	Black List	drop	1
109.236.84.10	Netherlands	147.237.76.176	test.ncore.idf.il	Black List	drop	1

09-02-2016-22:04:06 to 09-02-2016-23:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-02-2016-22:04:06 to 09-02-2016-23:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
5.79.73.145	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.50	147.237.77.216	Ukraine	dover.idf.il	ET SCAN NMAP -sS window 3072	1
211.23.156.152	147.237.76.199	Taiwan	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
208.100.26.228	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential VNC Scan 5800-5820	1
198.211.122.147	147.237.72.156	Netherlands	aman.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	147.237.0.33	China	idf.il	ET SCAN Potential VNC Scan 5800-5820	1
163.172.238.37	147.237.76.147	United Kingdom	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
50.84.213.146	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
122.72.53.188	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
5.79.73.145	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN Potential SSH Scan	1
104.167.6.84	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 1024	1
5.79.73.145	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.155	147.237.77.179	Ukraine	e.mazi.idf.il	ET SCAN NMAP -sS window 3072	1
5.79.73.145	147.237.8.24	Netherlands	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.155	147.237.77.179	Ukraine	e.mazi.idf.il	ET SCAN NMAP -f -sS	1
86.197.70.50	147.237.77.216	France	dover.idf.il	SERVER-WEBAPP client negative Content-Length attempt	1
208.100.26.228	147.237.76.196	United States	e.sviva.idf.il	ET SCAN Rapid POP3S Connections - Possible Brute Force Attack	1
61.240.144.65	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
208.100.26.228	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
61.240.144.65	147.237.8.14	China	e.orchot.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
187.40.190.88	147.237.8.24	Brazil	e.lifestyle.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
50.84.213.146	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 3072	1
128.199.49.205	147.237.76.42	Netherlands	refuah.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
5.79.73.145	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN Potential SSH Scan	1
106.186.20.183	147.237.8.45	Japan	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
5.79.73.145	147.237.76.198	Netherlands	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
103.207.37.81	147.237.77.234	Vietnam	halag.idf.il	ET SCAN NMAP -sS window 1024	1
5.79.73.145	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.155	147.237.77.179	Ukraine	e.mazi.idf.il	ET SCAN NMAP -sS window 2048	1

09-02-2016-22:04:06 to 09-02-2016-23:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.218.71.61	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
82.145.209.8	Europe	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
194.55.26.7	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
183.129.160.229	China	147.237.8.27	e.madim.atal.idf.il	drop	SAM rule	drop	2
194.55.26.8	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
194.55.30.7	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
183.129.160.229	China	147.237.8.50	e.tikshuv.idf.il	drop	SAM rule	drop	2
194.55.30.8	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
141.212.122.17	United States	147.237.0.35	akaws.idf.il	drop		drop	1
183.129.160.229	China	147.237.72.14	dover.idf.il(old)	drop	SAM rule	drop	1
202.3.76.56		147.237.76.34	yohalan.idf.il	drop		drop	1
31.154.49.113	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
109.253.128.237	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
61.240.144.65	China	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	1
109.253.218.191	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
183.129.160.229	China	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	1
61.240.144.65	China	147.237.77.178	e.matpash.idf.il	drop	SAM rule	drop	1
141.212.122.16	United States	147.237.0.35	akaws.idf.il	drop		drop	1
61.240.144.65	China	147.237.77.235	sviva.idf.il	drop	SAM rule	drop	1

09-02-2016-22:04:06 to 09-02-2016-23:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
194.55.26.7	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	8
194.55.26.8	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
176.13.229.150	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.251.134	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
188.167.70.160	Slovakia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	3
77.138.193.70	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/rights/asp/info.asp	Block	2
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/tizmoret/gallery/showpicture.asp	Block	1
213.57.147.240	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	1
66.102.9.2	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
194.55.30.7	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
86.135.150.254	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.png	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/7/71477.pdf	Block	1
213.57.147.240	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/&gws_rd=cr&ei=strjv5f3ejc6usl2stgc	Block	1
77.139.125.132	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
194.55.30.8	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
87.69.90.34	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/matash	Block	1
66.249.76.115	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1129-he/dover.aspx	Block	1
79.180.187.238	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.69.72	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/938-he/refuah.aspx	Block	1
204.79.180.227	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/miluim/templates/inner.asp	Block	1
157.55.39.254	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_text.asp	Block	1
68.180.230.47	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/iraq/english/default.asp	Block	1
85.64.68.213	Israel	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
66.249.76.46	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/default.asp	Block	1
207.46.13.107	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
173.208.157.186	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman--><אירתוו	Block	1
71.6.165.200	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/robots.txt	Block	1
85.64.68.213	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/wp-login.php	Block	1

09-02-2016-22:04:06 to 09-02-2016-23:04:06