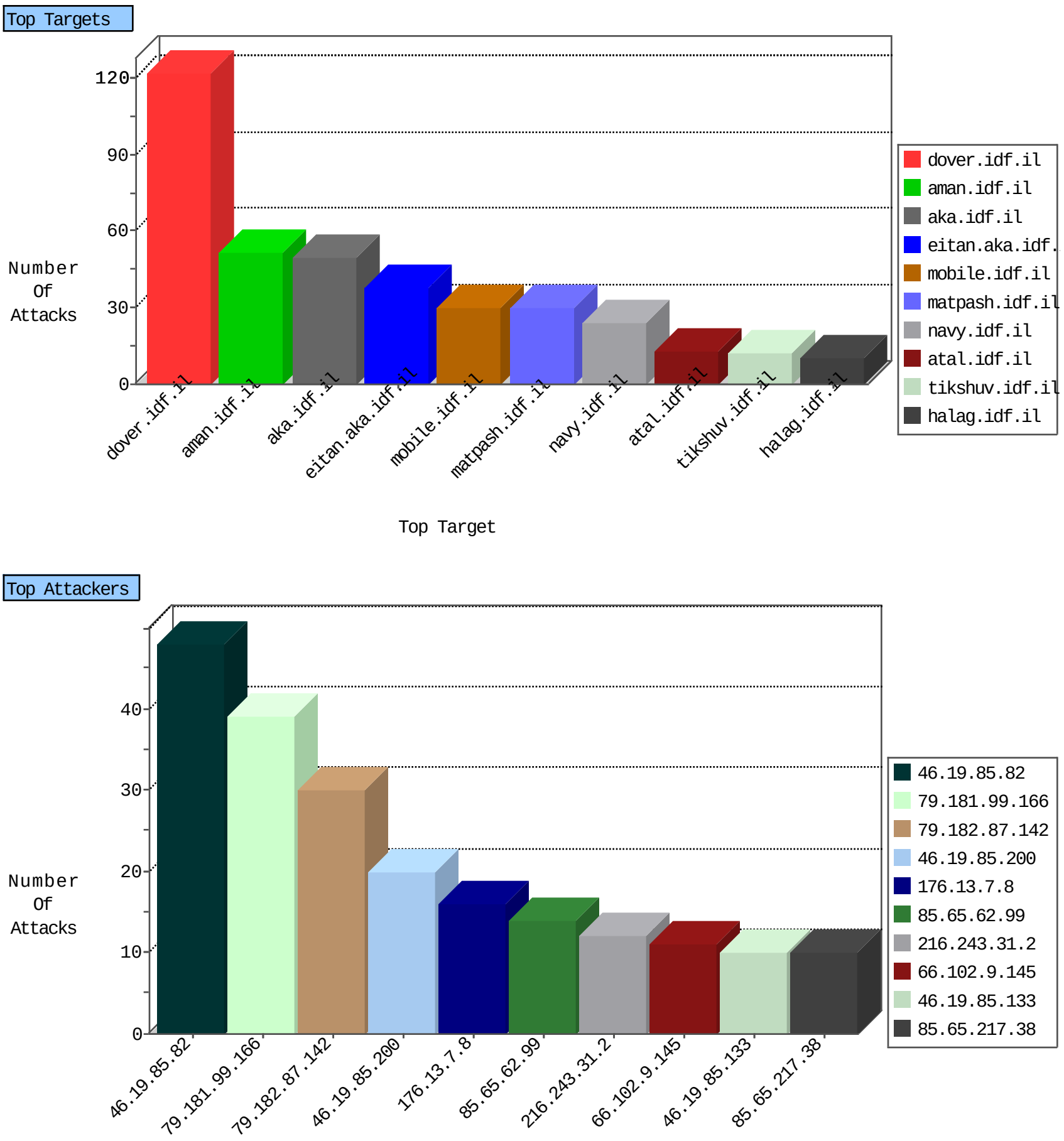
09-30-2016-23:04:04 to 10-01-2016-00:04:04

IDF Under Attack Daily Report



09-30-2016-23:04:04 to 10-01-2016-00:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.128.43.99	Switzerland	147.237.76.177	ncore.idf.il	Black List	drop	1
185.128.43.99	Switzerland	147.237.76.197	e.himush.idf.il	Black List	drop	1
52.198.29.244	Japan	147.237.76.198	e.yohalan.idf.il	Black List	drop	1
185.128.43.99	Switzerland	147.237.76.202	e.halag.idf.il	Black List	drop	1
185.128.43.99	Switzerland	147.237.76.38	e.e.meitav.idf.il	Black List	drop	1

09-30-2016-23:04:04 to 10-01-2016-00:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-30-2016-23:04:04 to 10-01-2016-00:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
109.67.239.218	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	3
109.67.239.218	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	2
91.121.142.199	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
202.65.138.2	147.237.77.176	India	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
194.224.101.170	147.237.77.226	Spain	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
2.50.168.178	147.237.76.42	United Arab Emirates	refuah.idf.il	ET SCAN NMAP -sS window 3072	1
218.72.209.112	147.237.77.121	China	e.navy.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
194.224.101.170	147.237.77.243	Spain	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
124.197.116.5	147.237.8.45	Singapore	e.eitan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
69.129.141.35	147.237.76.201	United States	e.atal.idf.il	ET SCAN NMAP -sS window 4096	1

09-30-2016-23:04:04 to 10-01-2016-00:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.182.87.142	Israel	147.237.76.200	eitan.aka.idf..	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
46.19.85.82	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
46.19.85.82	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
79.181.99.166	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	12
46.19.85.200	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
66.102.9.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
85.65.62.99	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
85.65.217.38	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.200	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
91.133.95.150	Austria	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
79.181.99.166	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
79.181.99.166	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.82	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.181.99.166	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.82	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
218.161.1.157	Taiwan	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	6
87.197.164.92	Slovakia	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
79.181.99.166	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.133	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
176.13.7.8	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
172.56.19.200	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.86.117	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.86.117	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
85.65.52.197	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
176.13.7.8	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
77.138.247.182	France	147.237.76.200	eitan.aka.idf..	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
85.65.62.99	Israel	147.237.76.200	eitan.aka.idf..	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.133	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
80.246.137.157	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
79.177.56.173	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.203	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
130.193.50.14	Russian Federation	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.198.53	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
5.102.242.49	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.102.9.149	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
106.38.241.106	China	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	3
37.26.148.203	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
2.53.179.193	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
109.253.198.53	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
66.249.65.12	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
106.38.241.106	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	3
46.19.86.175	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.53.164.180	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
66.102.9.145	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
83.22.252.113	Poland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
88.135.174.250	Poland	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
176.13.7.8	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
77.127.83.137	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
176.13.7.8	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2

09-30-2016-23:04:04 to 10-01-2016-00:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.7.1	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.149.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
36.88.60.160	Indonesia	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/1065-en/dover.aspx parameter SearchText	Block	2
36.88.60.160	Indonesia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	2
85.65.217.38	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
77.138.244.176	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/sachar	Block	2
31.154.45.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.49	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	2
109.67.239.218	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/elram	Block	1
66.249.65.58	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 66.249.65.58	Block	1
208.51.63.37	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/upfilees.php.suspected_	Block	1
85.65.62.99	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
63.96.14.2	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-en/dover.aspx	Block	1
148.251.192.100	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/giyus/	Block	1
66.249.65.182	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9186-he/refuah.aspx	Block	1
213.8.204.22	Israel	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1
66.102.8.213	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
188.194.219.176	Germany	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
66.249.66.101	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on www.chamatz.aka.idf.il/404.aspx	Block	1
213.8.204.22	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on www.refua.atal.idf.il/xmlrpc.php	Block	1
109.67.239.218	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.67.239.218	Block	1
66.249.65.10	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
5.35.39.154	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
204.79.180.132	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/templates/home.asp	Block	1
46.19.85.133	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
213.8.204.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/main/	Block	1
109.67.239.218	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 109.67.239.218	Block	1
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.51	Block	1
207.46.13.98	United States	147.237.72.166	aka.idf.il	Unknown Parameter pageNum in aka.idf.il/patzar/klali/default.asp	None	1
84.94.52.110	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl25 in www.aka.idf.il/main/sachar/payslips.aspx	None	1

09-30-2016-23:04:04 to 10-01-2016-00:04:04