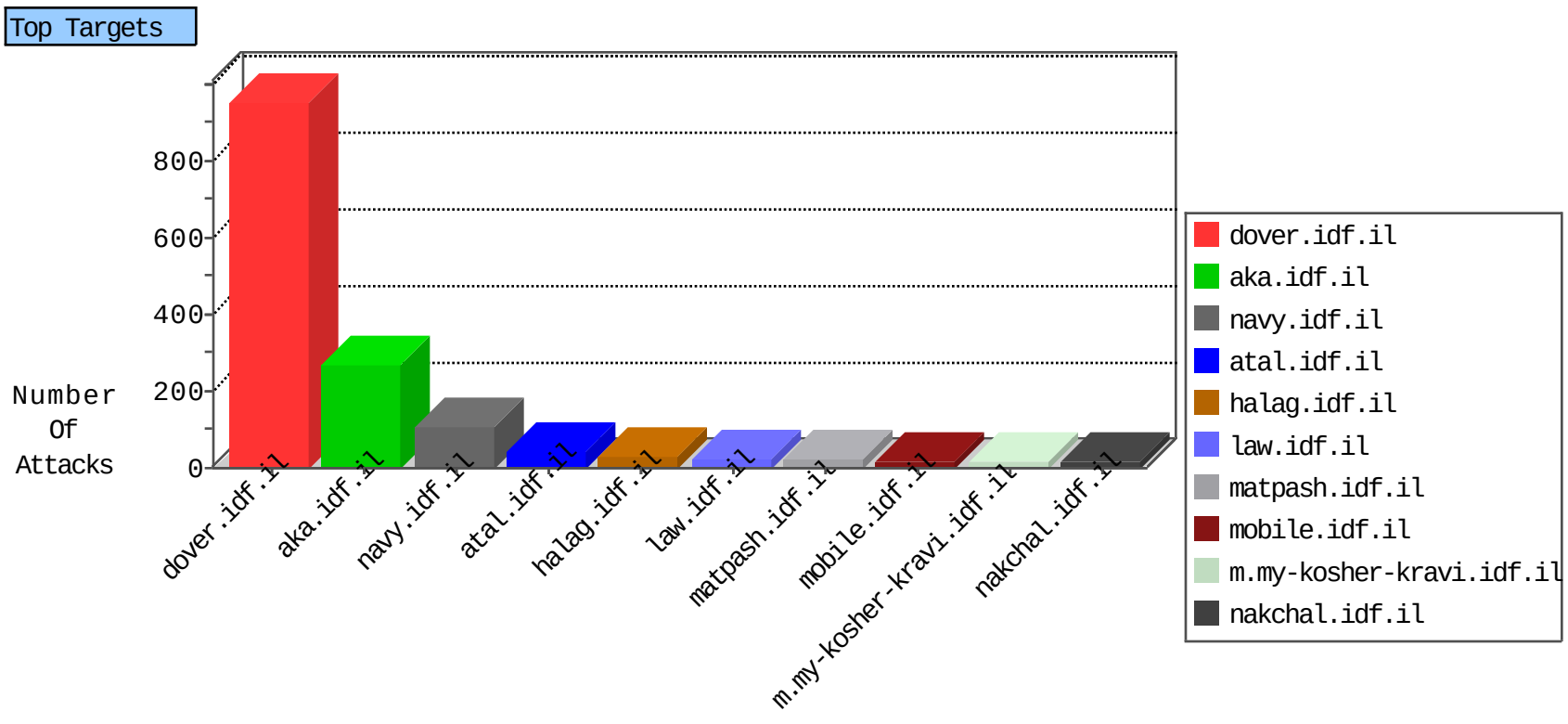
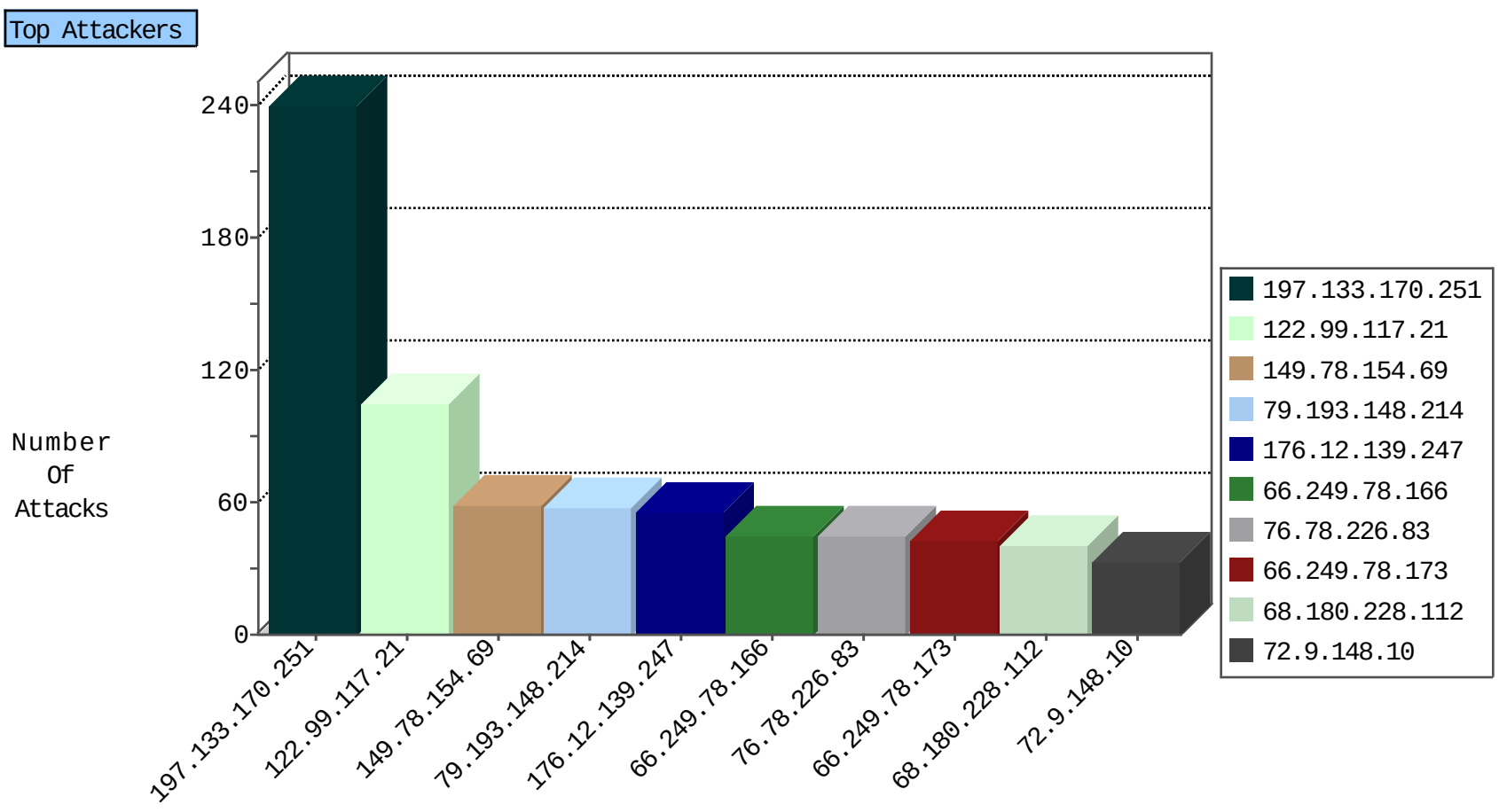
10-30-2015-03:04:07 to 10-30-2015-04:04:07

IDF Under Attack Daily Report



Top Target



Top Attackers

10-30-2015-03:04:07 to 10-30-2015-04:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.69.76	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	4845
66.249.75.60	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	632
66.249.69.84	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	153
62.219.254.22	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
88.250.180.58	Turkey	147.237.72.156	aman.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
141.212.122.160	United States	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
89.248.172.98	Netherlands	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1

10-30-2015-03:04:07 to 10-30-2015-04:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-30-2015-03:04:07 to 10-30-2015-04:04:07

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
66.249.78.190	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.34	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
66.249.69.84	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.65.37	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	2
169.57.5.20	147.237.76.197	Netherlands	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
162.248.242.88	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
14.169.116.235	147.237.8.28	Vietnam	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
210.61.150.154	147.237.76.177	Taiwan	ncore.idf.il	ET SCAN NMAP -sS window 4096	1
177.40.31.114	147.237.77.212	Brazil	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
162.248.242.88	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 3072	1
101.17.245.173	147.237.76.148	China	gqcenter.aka.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
210.61.150.154	147.237.76.177	Taiwan	ncore.idf.il	ET SCAN NMAP -sS window 3072	1
177.40.31.114	147.237.77.235	Brazil	sviva.idf.il	ET SCAN NMAP -sS window 1024	1

10-30-2015-03:04:07 to 10-30-2015-04:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
197.133.170.251	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	240
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
79.193.148.214	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
176.12.139.247	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	44
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	40
46.19.86.85	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
76.78.226.83	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
24.182.106.14	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
46.19.86.191	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
66.249.64.250	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
74.14.50.145	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
72.73.89.211	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
107.77.72.35	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
66.249.64.139	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
70.27.111.214	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
41.130.1.232	Egypt	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	10
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
190.154.50.69	Ecuador	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
73.172.68.191	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
40.77.167.33	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
142.134.92.112	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
82.80.25.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.140.188.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.196	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.196	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
77.126.238.53	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
100.100.85.239		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
66.249.67.65	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
199.30.24.117	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
54.66.144.179	Australia	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	3
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
130.193.48.16	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
199.16.156.125	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	3
66.249.75.30	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
81.218.235.10	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
157.55.39.183	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.249.78.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2

10-30-2015-03:04:07 to 10-30-2015-04:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
122.99.117.21	Australia	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	45
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	30
122.99.117.21	Australia	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/index.php	Block	30
66.249.69.97	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	15
66.249.65.251	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/navy/links.aspx	Block	15
157.55.39.173	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1116-he/Ã‚Â¦Ã‚â€?	Block	15
68.180.228.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.112	Block	15
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
66.249.73.210	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/eitan/listpage/	Block	15
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.67.6	Block	15
188.138.17.205	France	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	15
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1068-he/chinuch.aspx/1239-he/chinuch.aspx	Block	15
37.140.188.112	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/reserve	Block	15
122.99.117.21	Australia	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 122.99.117.21	Block	15
66.249.75.70	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/8/888.pdf	Block	15
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam/main/procedure.asp	Block	15
188.165.15.37	France	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1462-he/atal.aspx	Block	15
76.78.226.83	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation SearchText in www.cogat.idf.il/938-en/cogat.aspx	Block	15
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
41.130.1.232	Egypt	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	15
66.249.79.121	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1775	Block	15
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.67.13	Block	15
207.46.13.66	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/894-he/nakhal.aspx)	Block	15
85.250.79.1	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	15
66.249.69.81	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1352-he/atal.aspx	Block	15
66.249.65.132	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/default.aspx×¦×•	Block	15
141.212.122.64	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to /x	Block	15
68.180.228.112	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/shared/usercontrols/headerupper/	Block	15
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	15
207.46.13.142	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/main/haredim/general.aspx	None	15
122.99.117.21	Australia	147.237.72.166	aka.idf.il	Distributed Admin Blocking	Block	15

10-30-2015-03:04:07 to 10-30-2015-04:04:07