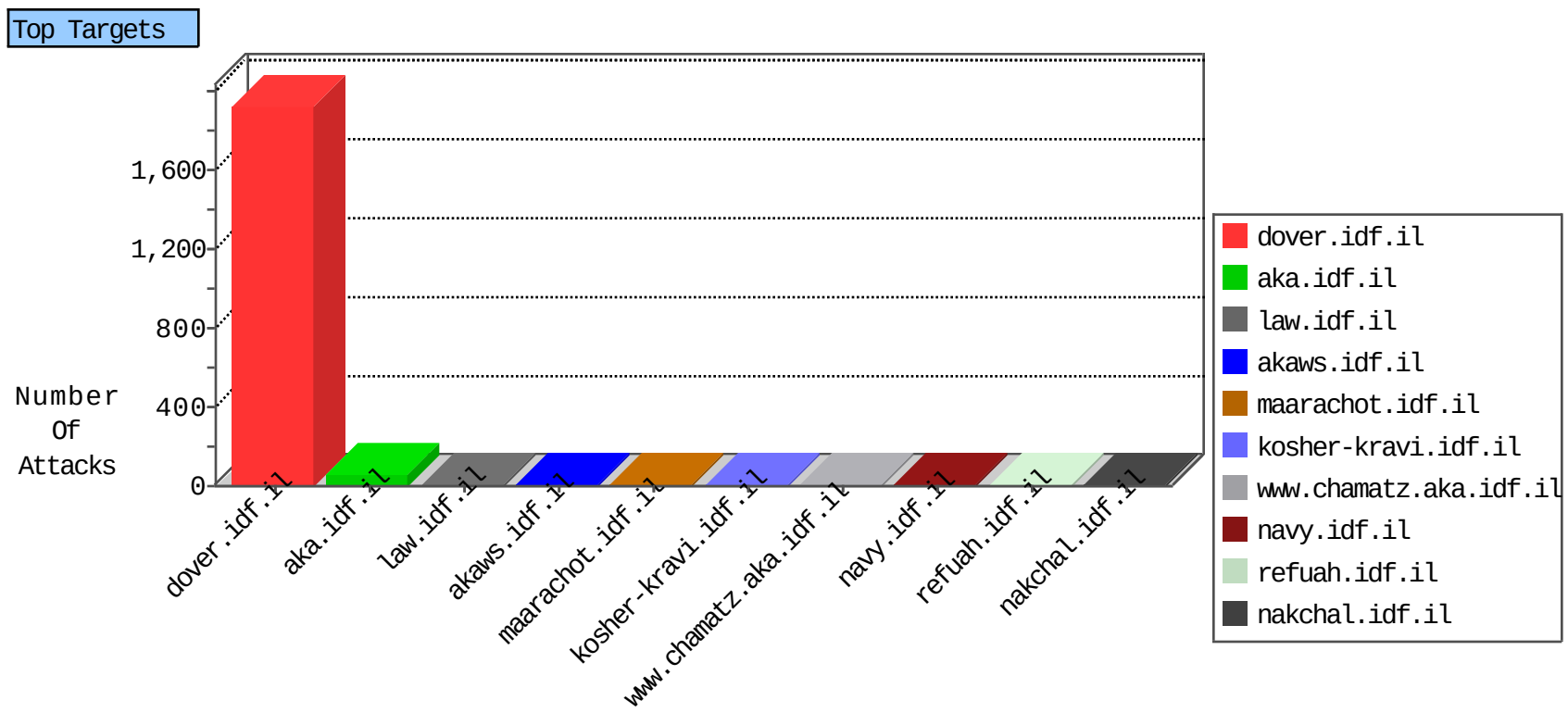
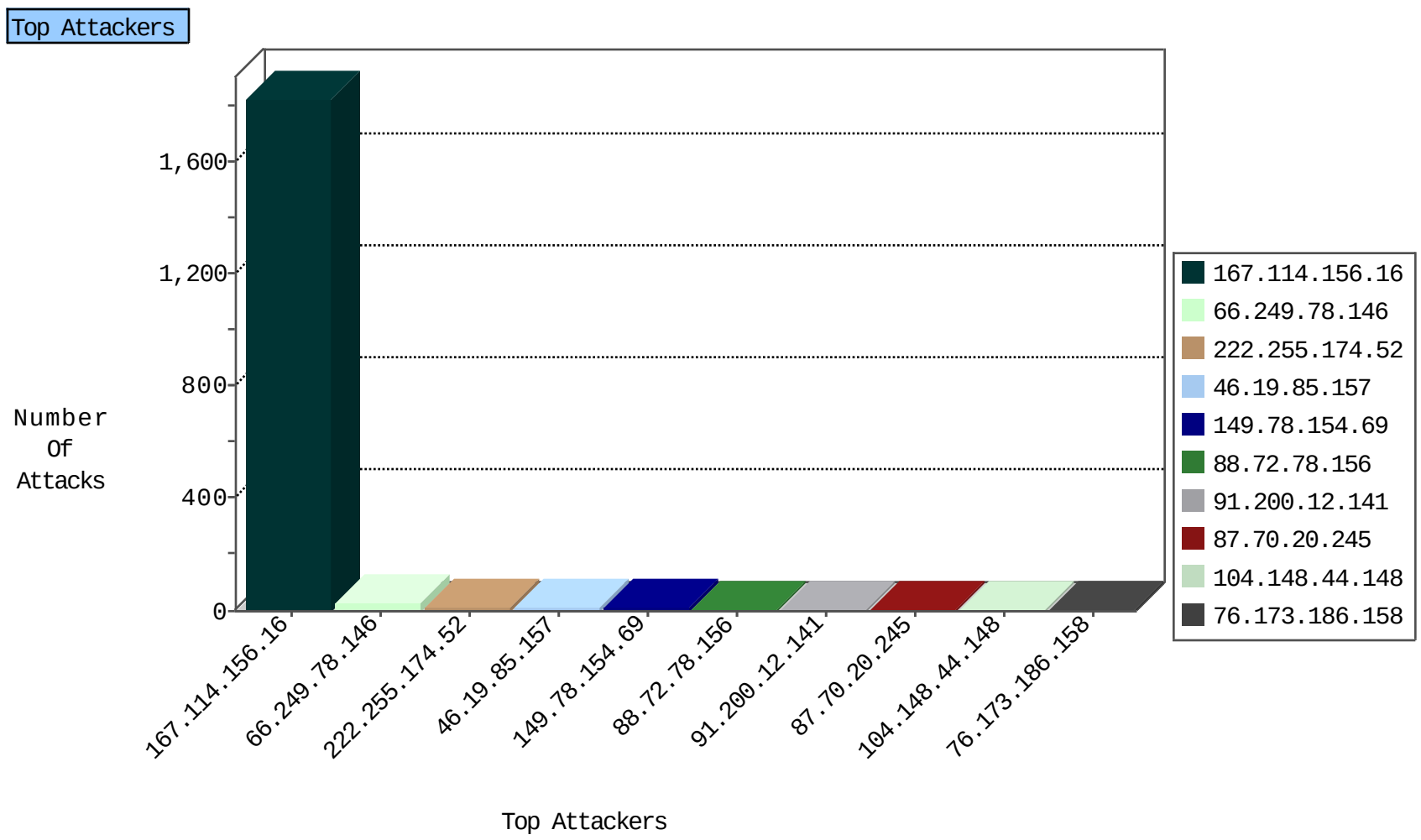
04-20-2016-03:04:02 to 04-20-2016-04:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-20-2016-03:04:02 to 04-20-2016-04:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2309
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	1641
167.114.156.16	Canada	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	7
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
14.3.253.52	Japan	147.237.8.27	e.madim.atal.idf.il	Block_Udp_All_Nets	drop	1
82.221.105.7	Iceland	147.237.8.46	e.chinuch.idf.il	Block_Udp_All_Nets	drop	1

04-20-2016-03:04:02 to 04-20-2016-04:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.113.202.68	Sweden	147.237.77.216	dover.idf.il	5141: HTTP: Sqlmap HTTP Request	Block	1

04-20-2016-03:04:02 to 04-20-2016-04:04:02

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
66.249.78.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
188.214.249.152	147.237.77.216	Romania	dover.idf.il	Xenu Link Sleuth User Agent	2
66.249.64.50	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
222.255.174.52	147.237.76.198	Vietnam	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
222.255.174.52	147.237.76.148	Vietnam	gqcenter.aka.idf.i	ET SCAN Potential SSH Scan	1
222.255.174.52	147.237.72.14	Vietnam	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
222.255.174.52	147.237.0.15	Vietnam	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
149.78.154.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.158	147.237.72.166	Ukraine	aka.idf.il	ET SCAN NMAP -sS window 1024	1
222.255.174.52	147.237.77.243	Vietnam	mobile.idf.il	ET SCAN Potential SSH Scan	1
222.255.174.52	147.237.77.74	Vietnam	law.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.185	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
222.255.174.52	147.237.76.177	Vietnam	ncore.idf.il	ET SCAN Potential SSH Scan	1
222.255.174.52	147.237.76.38	Vietnam	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
222.255.174.52	147.237.0.35	Vietnam	akaws.idf.il	ET SCAN Potential SSH Scan	1
201.17.138.59	147.237.0.34	Brazil	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.201.236.158	147.237.72.166	Ukraine	aka.idf.il	ET SCAN NMAP -sS window 4096	1
80.82.78.38	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
222.255.174.52	147.237.77.121	Vietnam	e.navy.idf.il	ET SCAN Potential SSH Scan	1

04-20-2016-03:04:02 to 04-20-2016-04:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
88.72.78.156	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
87.70.20.245	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
91.200.12.141	Ukraine	147.237.77.74	law.idf.il	drop	SAM rule	drop	4
76.173.186.158	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
66.249.93.184	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.255.215.87	France	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
104.148.2.169	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
91.200.12.141	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
46.19.85.157	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
49.229.172.140	Thailand	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
46.19.85.26	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
95.90.209.170	Germany	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
162.243.97.21	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
157.55.2.144	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.157	Israel	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	illegal header format detected: Illega start line in request	monitor	1
141.212.122.197	United States	147.237.0.35	akaws.idf.il	drop		drop	1
104.148.44.148	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
162.238.199.28	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.203	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.26	Israel	147.237.77.226	www.chamatz.aka.idf .il	Bad TCP sequence	Invalid ACK number	alert	1
108.46.39.202	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
70.95.64.64	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
157.55.2.144	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
46.120.21.184	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.198	United States	147.237.0.35	akaws.idf.il	drop		drop	1
104.148.44.148	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
213.57.135.55	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
162.238.199.28	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.206	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.26	Israel	147.237.77.226	www.chamatz.aka.idf .il	Bad TCP sequence	Invalid ACK number	monitor	1
137.116.71.170	United States	147.237.0.33	idf.il	drop		drop	1
104.148.44.148	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
169.229.3.91	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.50	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
157.55.2.144	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.120.21.184	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.200	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
106.184.3.122	Japan	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
162.243.97.21	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	1
141.212.122.207	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.157	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.193	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

04-20-2016-03:04:02 to 04-20-2016-04:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
131.253.25.143	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
66.102.6.191	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
199.30.25.95	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
208.109.207.221	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 208.109.207.221	Block	2
157.55.39.223	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.75.118	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.75.118	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-12321-en	Block	1
46.19.85.157	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
77.237.138.202	Czech Republic	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to /	Block	1
46.161.9.8	Russian Federation	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/xmlrpc.php	Block	1
203.127.96.245	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1
46.19.85.157	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1
66.102.6.188	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1930-he/cogat.aspx	Block	1
46.19.85.157	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
157.55.39.213	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/page.asp	Block	1
40.77.167.5	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to chinuch.aka.idf.il/404.htm	Block	1
208.109.207.221	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
68.180.230.45	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9066-he/refuah.aspx	Block	1
46.19.85.157	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method e;q=0.8,en-US;q=0.6,en;q=0.4 in URL	Block	1
40.77.167.16	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
220.255.146.215	Singapore	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1115-ar/dover.aspx	Block	1
46.161.9.8	Russian Federation	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1

04-20-2016-03:04:02 to 04-20-2016-04:04:02