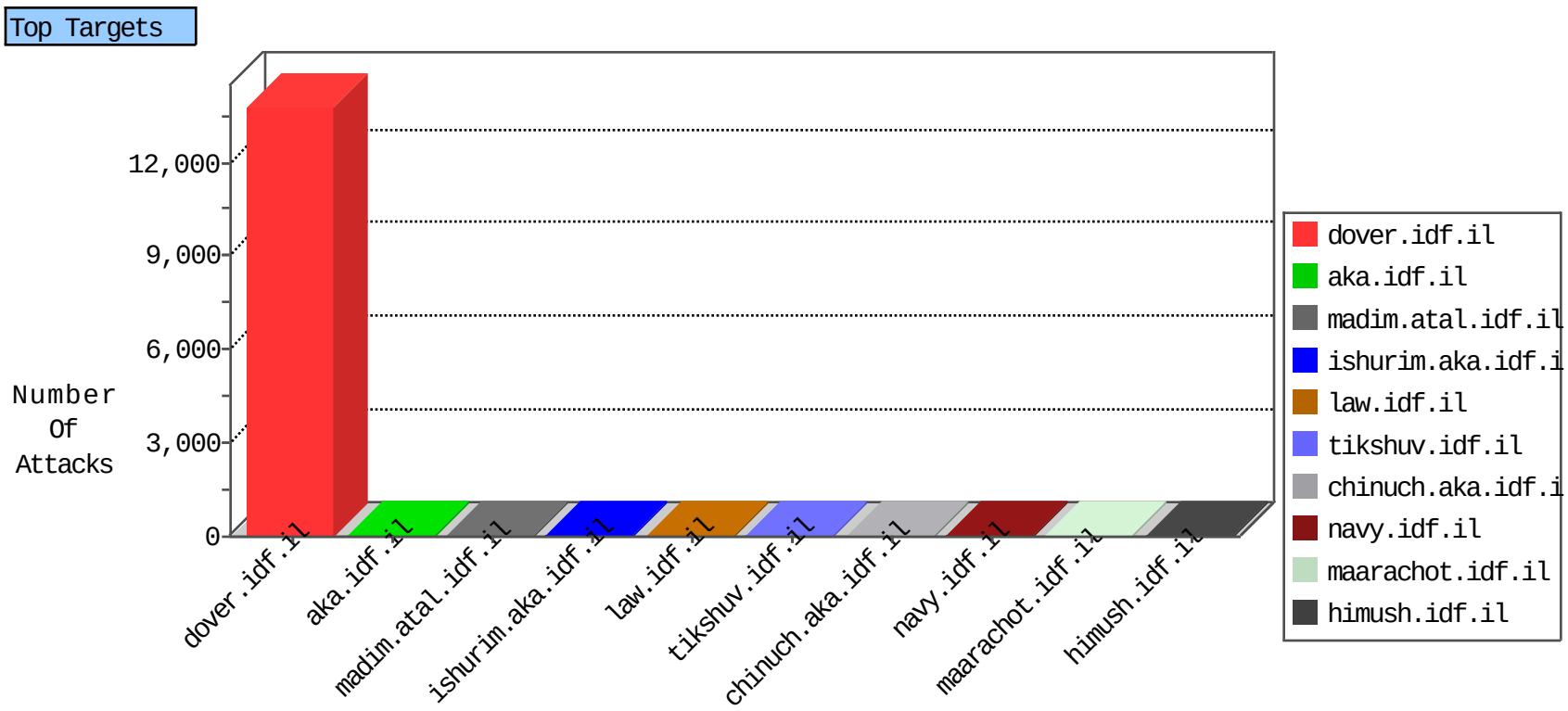
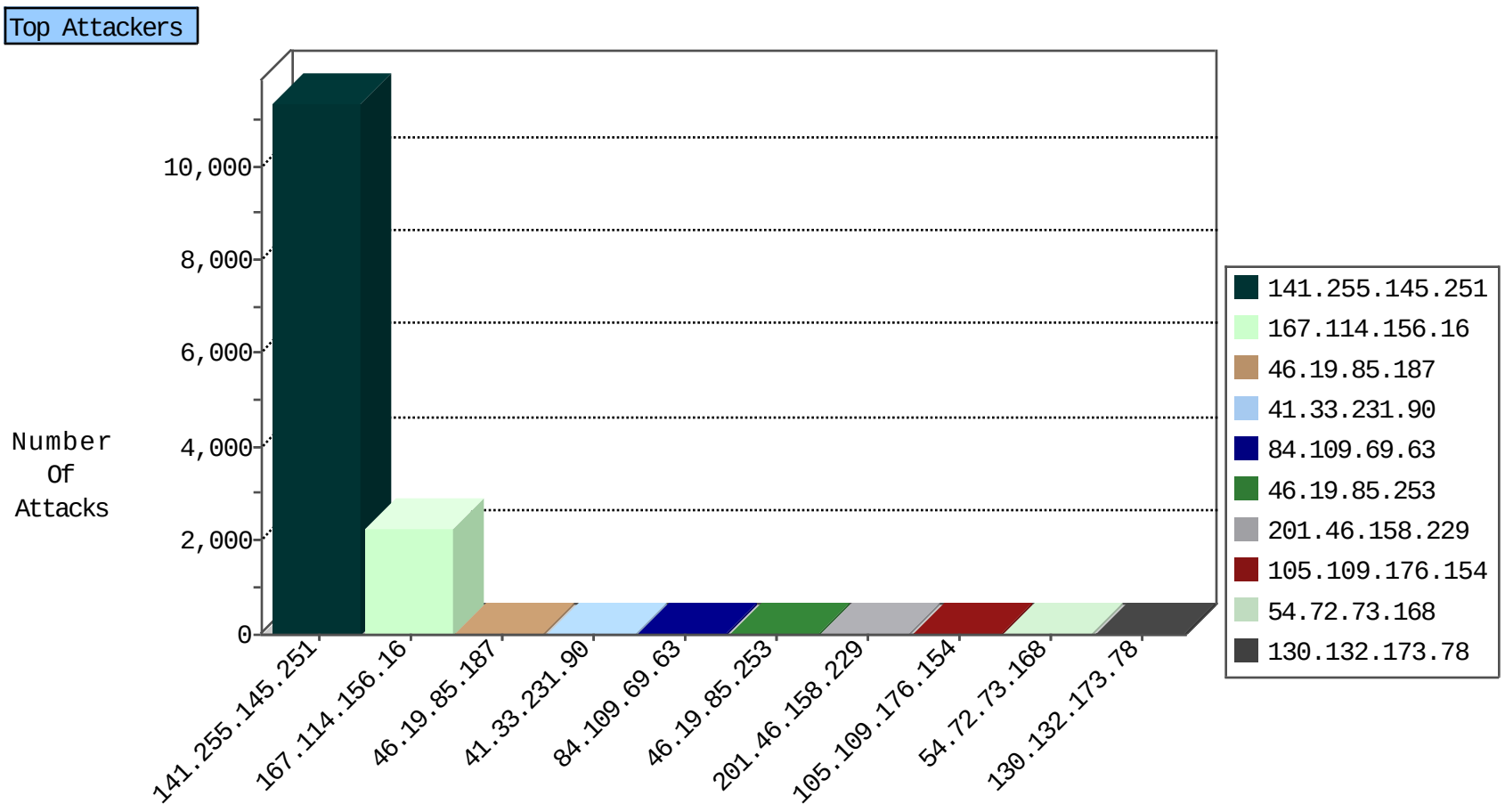
01-26-2016-05:04:04 to 01-26-2016-06:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-26-2016-05:04:04 to 01-26-2016-06:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
141.255.145.251	Netherlands	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	4018
141.255.145.251	Netherlands	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3768
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3046
141.255.145.251	Netherlands	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	1714
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	751
141.255.145.251	Netherlands	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	518
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	308
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	44
201.46.158.229	Brazil	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
66.249.78.166	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
66.249.78.173	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
96.245.39.39	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
115.239.228.10	China	147.237.0.15	kosher-kravi.idf.il	Frk_Under_Attack_Con_Http	drop	1
207.46.13.135	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
185.35.62.50	Switzerland	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1

01-26-2016-05:04:04 to 01-26-2016-06:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
198.50.134.71	Canada	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1

01-26-2016-05:04:04 to 01-26-2016-06:04:04

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
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
113.171.23.126	147.237.76.30	Vietnam	himush.idf.il	ET SCAN Potential SSH Scan	1
107.2.79.150	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
94.76.0.204	147.237.76.196	Bahrain	e.sviva.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
5.22.250.202	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
172.98.200.237	147.237.77.170		maarachot.idf.il	ET SCAN NMAP -sS window 4096	1
172.98.200.237	147.237.77.170		maarachot.idf.il	ET SCAN NMAP -f -sS	1
113.171.23.126	147.237.76.201	Vietnam	e.atal.idf.il	ET SCAN Potential SSH Scan	1
107.2.79.150	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 4096	1
94.76.0.204	147.237.76.196	Bahrain	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
1.25.248.44	147.237.8.27	China	e.madim.atal.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
218.246.0.97	147.237.77.235	China	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
172.98.200.237	147.237.77.170		maarachot.idf.il	ET SCAN NMAP -sS window 2048	1
164.39.11.198	147.237.76.30	United Kingdom	himush.idf.il	ET SCAN NMAP -sS window 1024	1

01-26-2016-05:04:04 to 01-26-2016-06:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
141.255.145.251	Netherlands	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3421
141.255.145.251	Netherlands	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2920
141.255.145.251	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2270
141.255.145.251	Netherlands	147.237.77.216	dover.idf.il	drop		drop	739
141.255.145.251	Netherlands	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	165
141.255.145.251	Netherlands	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	134
141.255.145.251	Netherlands	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	35
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	28
141.255.145.251	Netherlands	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
105.109.176.154	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.253	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
130.132.173.78	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.253	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
84.109.69.63	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
84.109.69.63	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.182.15.245	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.109.69.63	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	6
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
201.46.158.229	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.253	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
84.109.69.63	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
130.193.37.16	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
89.138.97.105	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
65.34.85.169	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.127	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
89.138.97.105	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.109.69.63	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
46.19.85.208	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.9.122.203	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.255.215.87	France	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.78.144	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
24.218.80.94	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
52.16.5.197	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
2.52.1.155	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.34	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.255.145.251	Netherlands	147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	1
141.212.122.188	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
207.46.13.162	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
91.231.192.149	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.247.208	United States	147.237.0.33	idf.il	drop		drop	1

01-26-2016-05:04:04 to 01-26-2016-06:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.187	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	41
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
199.30.25.151	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1824-he/dover.aspx	Block	1
5.197.235.85	Azerbaijan	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
173.161.52.213	United States	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1415-10809-he/dover.aspx	Block	1
212.76.103.119	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/mas.aspx	Block	1
141.255.145.251	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
180.76.15.16	China	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
157.55.39.184	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/military-police/	Block	1
66.249.64.50	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;docid in www.aka.idf.il/main/giyus/general.aspx	None	1
198.20.69.74	United States	147.237.76.30	himush.idf.il	Unauthorized URL Access to 147.237.76.30/robots.txt	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
157.55.39.237	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/hinuch	Block	1
66.249.65.231	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aka	Block	1
199.30.25.151	United States	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 199.30.25.151 (sigalgs DoS Attack)	None	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/sachar/tfasim.aspx	Block	1
5.197.235.85	Azerbaijan	147.237.77.74	law.idf.il	PHP Attempt	Block	1
173.161.52.213	United States	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1
66.249.69.76	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1

01-26-2016-05:04:04 to 01-26-2016-06:04:04