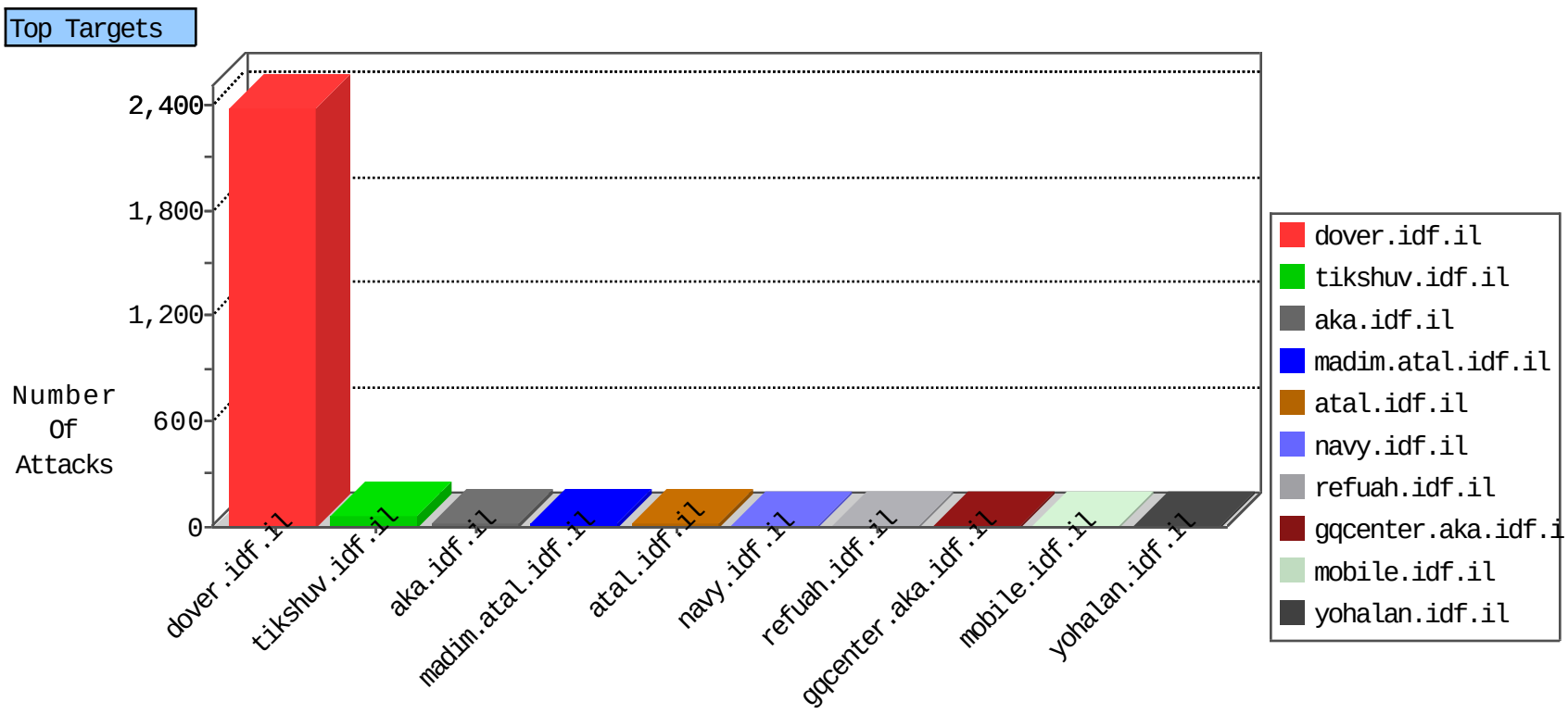
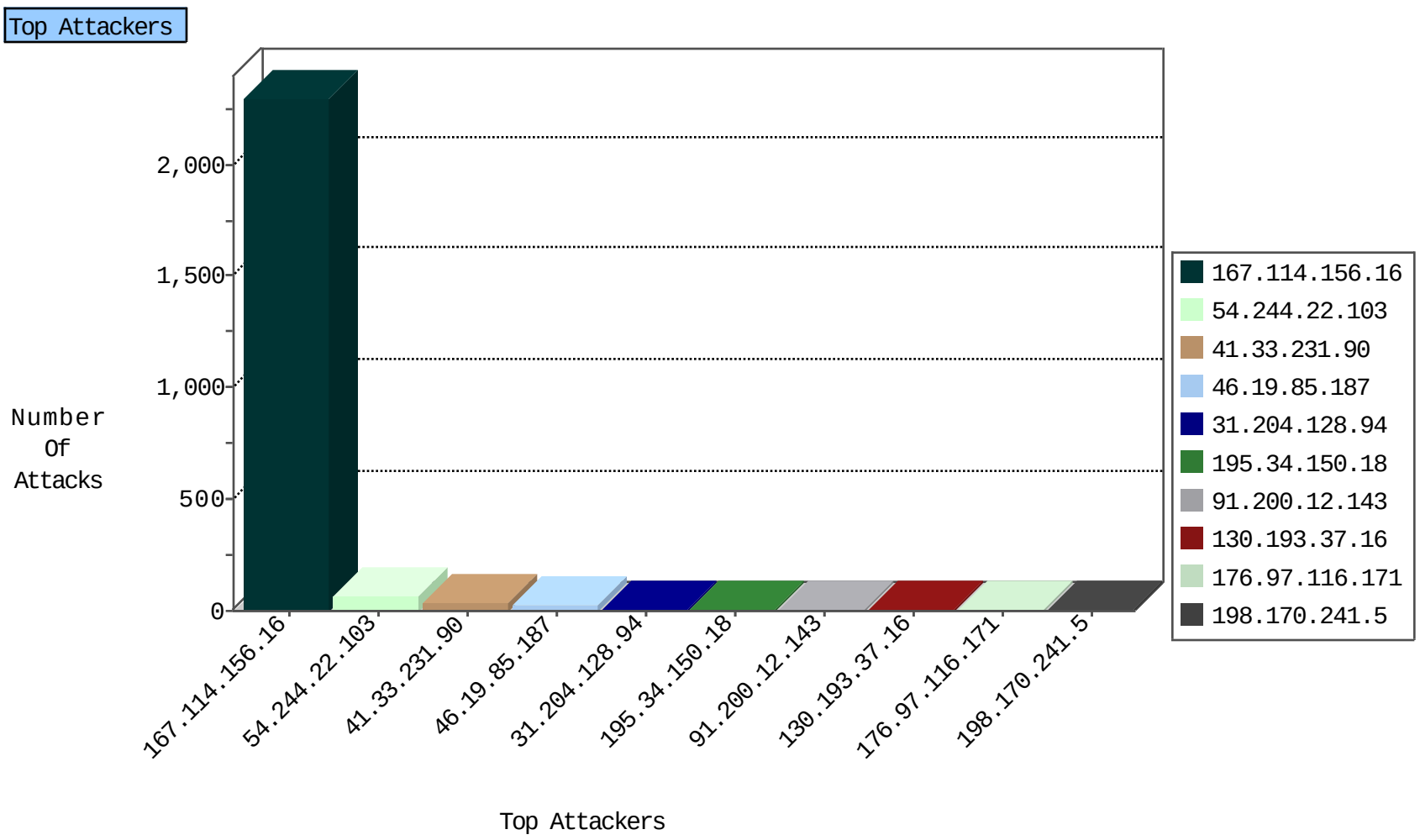
01-26-2016-04:04:07 to 01-26-2016-05:04:07

IDF Under Attack Daily Report





01-26-2016-04:04:07 to 01-26-2016-05:04:07

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	3006
212.179.54.237	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
42.2.134.26	Hong Kong	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	2

01-26-2016-04:04:07 to 01-26-2016-05:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
42.101.154.233	China	147.237.77.216	dover.idf.il	13764: HTTP: China Chopper Malware Communication Attempt	Block	1
69.30.214.46	United States	147.237.72.166	aka.idf.il	C106: HTTP: majestic bot	Block	1
188.165.15.177	France	147.237.77.170	maarachot.idf.il	C228: HTTP: AhrefBot crawler	Block	1

01-26-2016-04:04:07 to 01-26-2016-05:04:07

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
66.249.78.79	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
183.3.202.115	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
89.163.148.90	147.237.76.86	Germany	navy.idf.il	ET SCAN Potential SSH Scan	1
66.240.213.93	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 1024	1
66.240.192.138	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
195.216.176.244	147.237.77.243	Latvia	mobile.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potentia Scan or Infection	1
185.130.5.235	147.237.76.34		yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.235	147.237.0.33		idf.il	ET SCAN NMAP -sS window 1024	1
183.3.202.115	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
183.3.202.115	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
183.3.202.115	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
66.240.192.138	147.237.76.31	United States	nakchal.idf.il	ET SCAN Potential SSH Scan	1
212.179.227.181	147.237.76.148	Israel	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 3072	1
23.125.172.41	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.235	147.237.8.28		e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
183.179.89.114	147.237.72.166	Hong Kong	aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
183.3.202.115	147.237.76.39	China	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1

01-26-2016-04:04:07 to 01-26-2016-05:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	51
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	9
31.204.128.94	Netherlands	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
130.193.37.16	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
201.187.80.43	Chile	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
91.200.12.143	Ukraine	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
91.200.12.143	Ukraine	147.237.77.233	atal.idf.il	drop	SAM rule	drop	4
91.200.12.139	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
40.77.167.86	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	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
141.8.142.1	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
37.26.148.152	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
91.200.12.136	Ukraine	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	2
91.200.12.136	Ukraine	147.237.77.233	atal.idf.il	drop	SAM rule	drop	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
5.255.253.46	Russian Federation	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.180	United States	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.15	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.76	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
174.118.251.160	Canada	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
79.180.131.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
184.105.247.252	United States	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
8.37.227.68	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
141.212.122.181	United States	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.42	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.86	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
176.97.116.171	Ukraine	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
79.180.131.99	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
24.181.122.68	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.187	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
74.82.47.44	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.243	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
141.212.122.179	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
69.116.86.148	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.188	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
104.130.78.65	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
74.82.47.56	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
50.201.97.226	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.247.244	United States	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.180	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
69.116.86.148	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.59	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
54.244.22.103	United States	147.237.0.15	kosher-kravi.idf.il	drop	First packet isn't SYN	drop	1
184.105.247.252	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

01-26-2016-04:04:07 to 01-26-2016-05:04:07

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.il	Suspicious Response Code	Block	18
198.170.241.5	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 198.170.241.5	Block	5
98.244.112.96	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	2
176.97.116.171	Ukraine	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
157.55.39.179	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-13807-he/dov	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
31.204.128.94	Netherlands	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/shared/usercontrols/headerupper/	Block	1
184.105.247.196	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
84.111.187.38	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.185	United States	147.237.72.166	aka.idf.il	Unknown Parameter tm in www.aka.idf.il/main/giyus/	None	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18551-he/dover.aspx	Block	1
41.213.166.75	Reunion	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
54.83.90.73	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx	Block	1
41.213.166.75	Reunion	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
65.208.151.112	United States	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 65.208.151.112	Block	1
176.97.116.171	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 176.97.116.171	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
42.101.154.233	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22638-he/dover.aspx.	Block	1
65.208.151.117	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/shared/clientscripts/{1}	Block	1
31.204.128.94	Netherlands	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 31.204.128.94	Block	1
176.97.116.171	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	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
42.101.154.233	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dxyylc/md5.php	Block	1

01-26-2016-04:04:07 to 01-26-2016-05:04:07