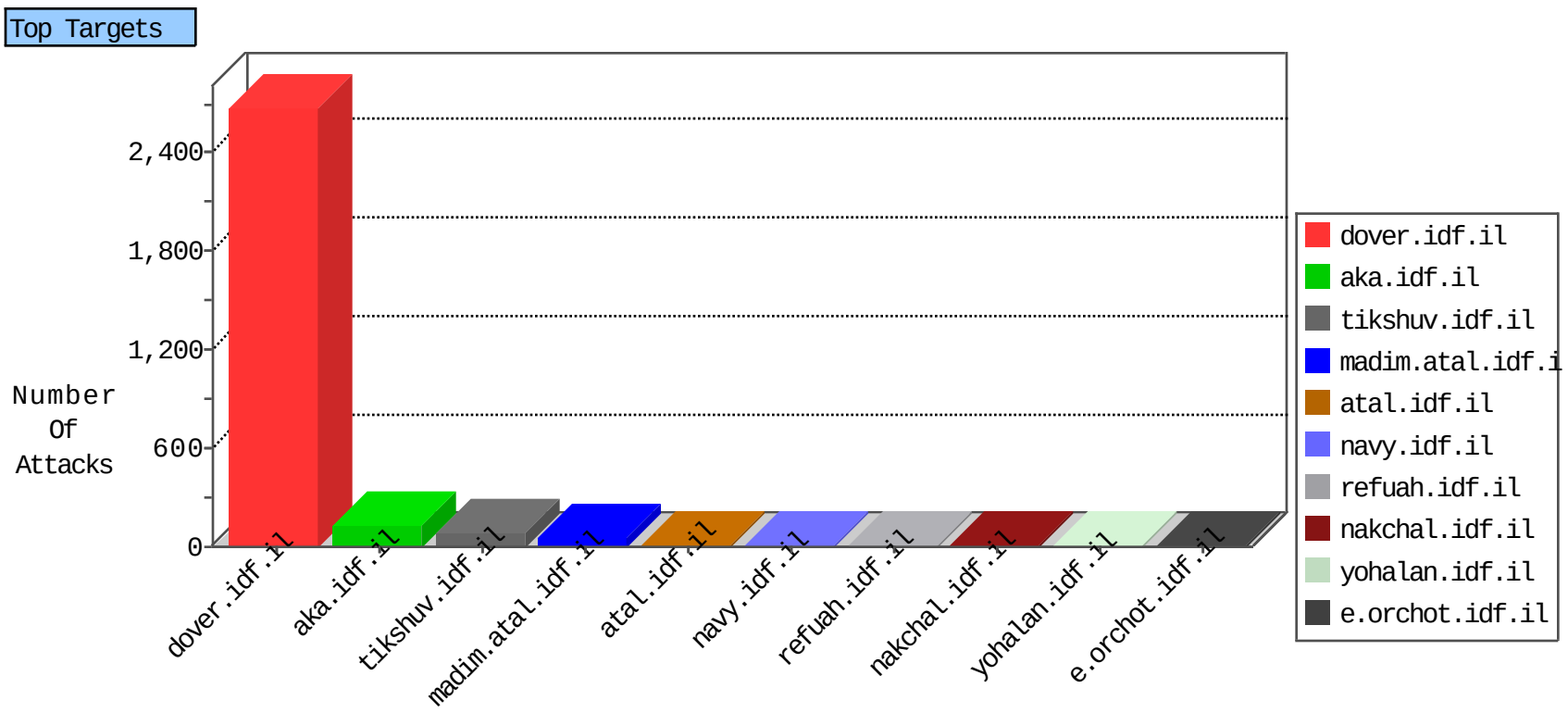
01-20-2016-02:04:00 to 01-20-2016-03:04:00

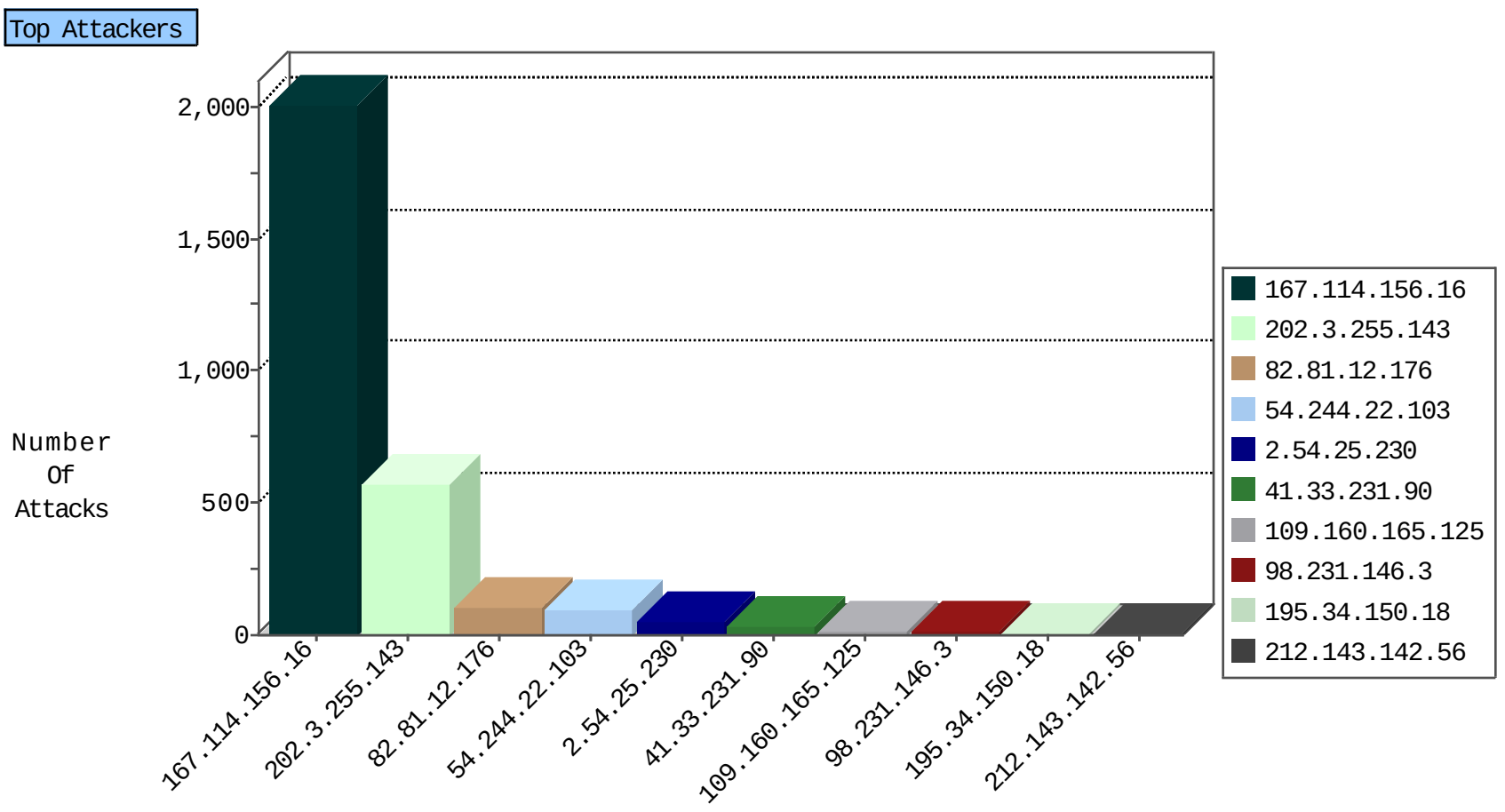
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

01-20-2016-02:04:00 to 01-20-2016-03:04:00

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
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	107
117.90.150.146	China	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
185.81.158.41		147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
117.90.150.146	China	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
204.42.253.2	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
82.221.105.7	Iceland	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
117.90.150.146	China	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
117.90.150.146	China	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1

01-20-2016-02:04:00 to 01-20-2016-03:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.76.42	refuah.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

01-20-2016-02:04:00 to 01-20-2016-03:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
202.3.255.143	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	528
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
61.149.161.186	147.237.8.14	China	e.orchot.idf.il	GPL SCAN nmap TCP	2
185.66.250.189	147.237.8.14	Netherlands	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
110.125.47.90	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
82.117.208.243	147.237.77.74		law.idf.il	ET SCAN NMAP -sS window 1024	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	1
193.201.227.7	147.237.76.34	Ukraine	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
110.125.47.90	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
110.125.47.90	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1

01-20-2016-02:04:00 to 01-20-2016-03:04:00

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	85
202.3.255.143	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	10
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
98.231.146.3	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
98.231.146.3	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
79.177.1.37	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.160.165.125	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
79.177.240.116	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.160.165.125	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
207.237.82.50	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
109.160.165.125	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
5.22.135.142	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.249.64.163	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
45.56.71.97		147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
64.110.145.90	Satellite Provider	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.141	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.243	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
94.230.86.36	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
64.125.239.160	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
173.161.52.213	United States	147.237.77.216	dover.idf.il	Header Rejection	header rejection pattern found in request	monitor	1
108.168.185.133	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
2.54.174.12	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.121.192	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
98.231.146.3	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
64.125.239.244	United States	147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.185	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
79.182.169.119	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
23.101.61.176	Ireland	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	1
141.212.122.186	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
75.131.215.197	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
93.115.82.54	Anonymous Proxy	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
64.125.239.16	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
31.210.188.26	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
104.209.188.207	United States	147.237.76.31	nakchal.idf.il	Instant Messengers	instant messenger pattern found, application: Skype	monitor	1
75.131.215.197	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.121.192	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

01-20-2016-02:04:00 to 01-20-2016-03:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.25.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	50
69.163.144.121	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 69.163.144.121	Block	2
173.161.52.213	United States	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	1
208.113.160.6	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
173.161.52.213	United States	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/watch	Block	1
69.163.144.121	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
46.19.85.180	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/sendtofriend/kkkkkkk=34d19df9kkkkkkk_34d19df9	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
69.194.230.99	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
64.71.32.30	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
188.55.75.239	Saudi Arabia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.png	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
80.82.65.74	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
66.249.69.2	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
195.62.53.168	Russian Federation	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to /admin/login	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-he/dover.aspx	Block	1

01-20-2016-02:04:00 to 01-20-2016-03:04:00