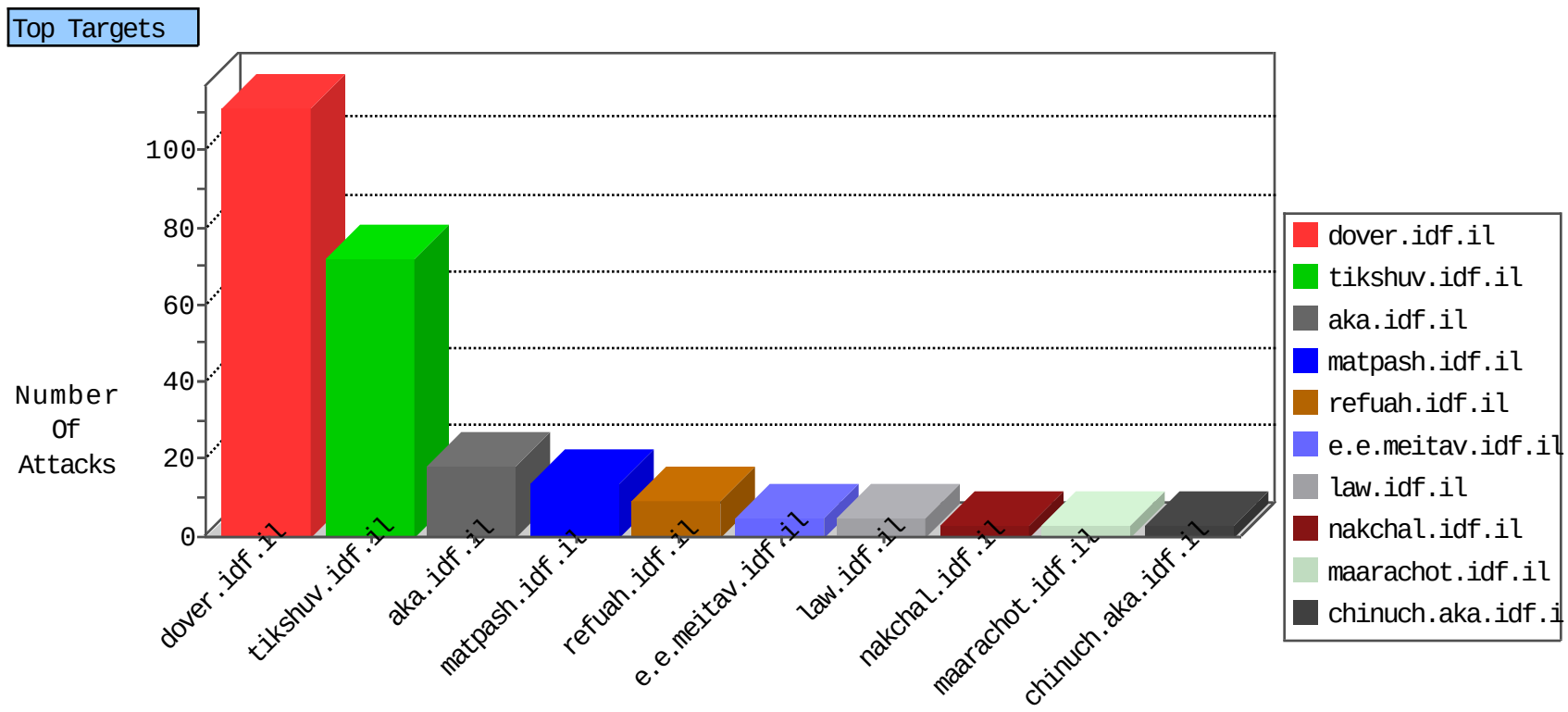
02-07-2016-05:04:00 to 02-07-2016-06:04:00

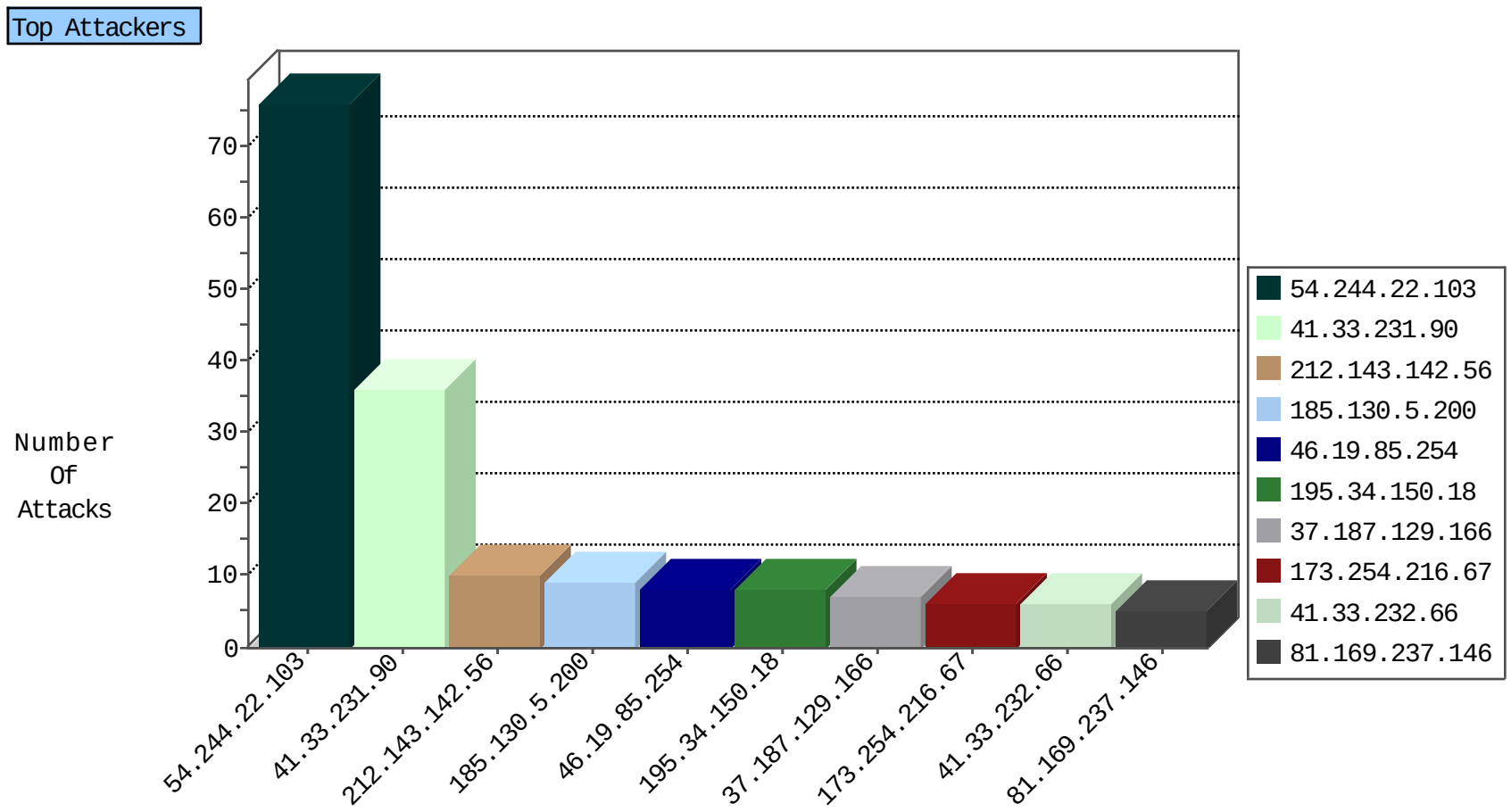
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

02-07-2016-05:04:00 to 02-07-2016-06:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
184.90.68.166	United States	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	2
115.230.124.164	China	147.237.76.38	e.e.meitav.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
45.32.229.187		147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
192.99.193.12	Canada	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
71.6.135.131	United States	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
192.99.193.12	Canada	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1

02-07-2016-05:04:00 to 02-07-2016-06:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
198.20.69.74	United States	147.237.76.197	e.himush.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

02-07-2016-05:04:00 to 02-07-2016-06:04:00

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
66.249.78.191	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sA (2)	2
185.130.5.200	147.237.8.50		e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.200	147.237.0.35		akaws.idf.il	ET SCAN Potential SSH Scan	1
120.198.126.84	147.237.0.33	China	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
114.112.90.54	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
93.189.26.18	147.237.77.226	Austria	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
82.117.208.243	147.237.77.170		maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.200	147.237.77.74		law.idf.il	ET SCAN Potential SSH Scan	1
46.151.52.161	147.237.76.39	Ukraine	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.200	147.237.76.39		mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.200	147.237.72.166		aka.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.200	147.237.8.46		e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
180.156.115.130	147.237.76.31	China	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
114.112.90.54	147.237.76.42	China	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
93.189.26.18	147.237.77.243	Austria	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
93.189.26.18	147.237.77.170	Austria	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.200	147.237.77.205		prisha.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.200	147.237.76.202		e.halag.idf.il	ET SCAN Potential SSH Scan	1
40.115.57.147	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.200	147.237.72.217		e.idf.il	ET SCAN Potential SSH Scan	1

02-07-2016-05:04:00 to 02-07-2016-06:04:00

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	70
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
89.204.137.40	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.85.254	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
47.17.214.150	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.254	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
77.126.94.49	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.49.14	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.169.237.146	Germany	147.237.77.61	e.cogat.idf.il	drop	SAM rule	drop	2
46.19.86.173	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
86.176.146.147	United Kingdom	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
130.193.50.33	Russian Federation	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
81.169.237.146	Germany	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	2
52.33.66.29	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	2
157.55.39.79	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
74.82.47.50	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.95.47.166	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
8.37.228.77	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
115.230.124.164	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
184.105.139.86	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.112	United States	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
87.69.124.174	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
74.82.47.39	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
130.193.51.66	Russian Federation	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.247.215	United States	147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
87.69.124.174	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.42	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
81.169.237.146	Germany	147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	1
184.105.247.227	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.65.28.77	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/homepage/www.youtube.com/v/3g51ei5nuhg	Block	5
37.187.129.166	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
173.254.216.67	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
171.25.193.131	Sweden	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-he	Block	3
77.247.181.163	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-he	Block	2
37.187.129.166	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-he	Block	2
173.254.216.67	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-he	Block	2
94.242.250.117	Luxembourg	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-he	Block	2
192.243.55.133	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.133	Block	2
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/3394.jpg	Block	1
94.242.250.117	Luxembourg	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1934-he/cogat.aspx	Block	1
201.103.142.239	Mexico	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.66.115	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding j.e[8l2tEjLR>S>2vSL;*$zzuM(&4WRz in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
157.55.39.251	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
77.247.181.163	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.78.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/3384.jpg	Block	1
101.99.65.48	Malaysia	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
69.194.230.99	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
207.46.13.142	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
66.249.66.117	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	1
91.226.212.54	Ukraine	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-ar/dover.aspx	Block	1
37.187.129.166	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19405-he/dover.aspx)	Block	1
184.95.47.166	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/4f23fe5992ad007acd6ceab7b35c8576	Block	1
146.185.234.48	Russian Federation	147.237.77.176	matpash.idf.il	Parameter Type Violation fromDate in www.cogat.idf.il/901-en/cogat.aspx	Block	1
71.43.100.242	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/).html(	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter hc_location in www.aka.idf.il/main/haredim/general.aspx	None	1
173.236.176.119	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
93.158.152.49	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1379-he/dover.aspx	Block	1
188.143.232.10	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1283-en/dover.aspx	Block	1
64.90.48.202	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
146.185.234.48	Russian Federation	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
74.208.16.113	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/blog/wp-admin/	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1779-he/dover.aspx	Block	1
66.249.65.112	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/2418.jpg	Block	1
157.55.39.80	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/61998	Block	1

02-07-2016-05:04:00 to 02-07-2016-06:04:00