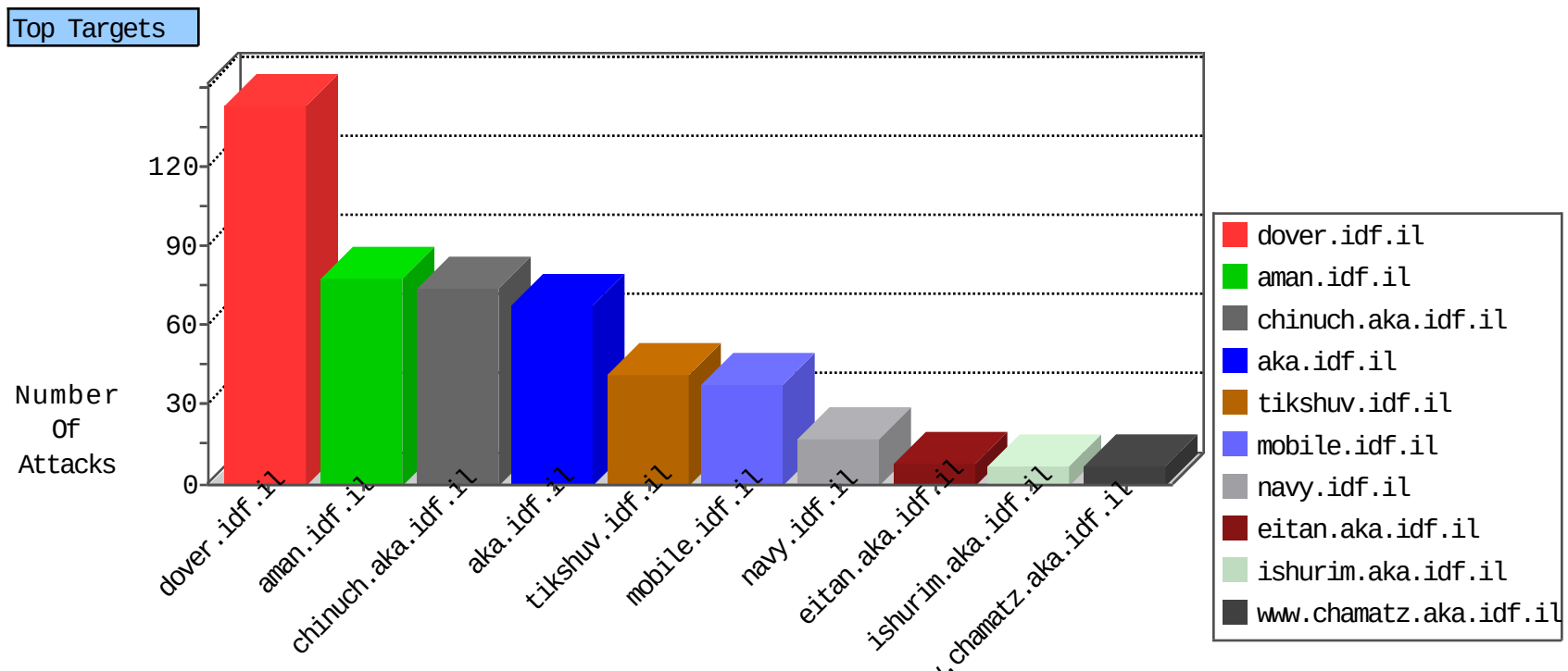
02-12-2016-01:06:11 to 02-12-2016-02:06:11

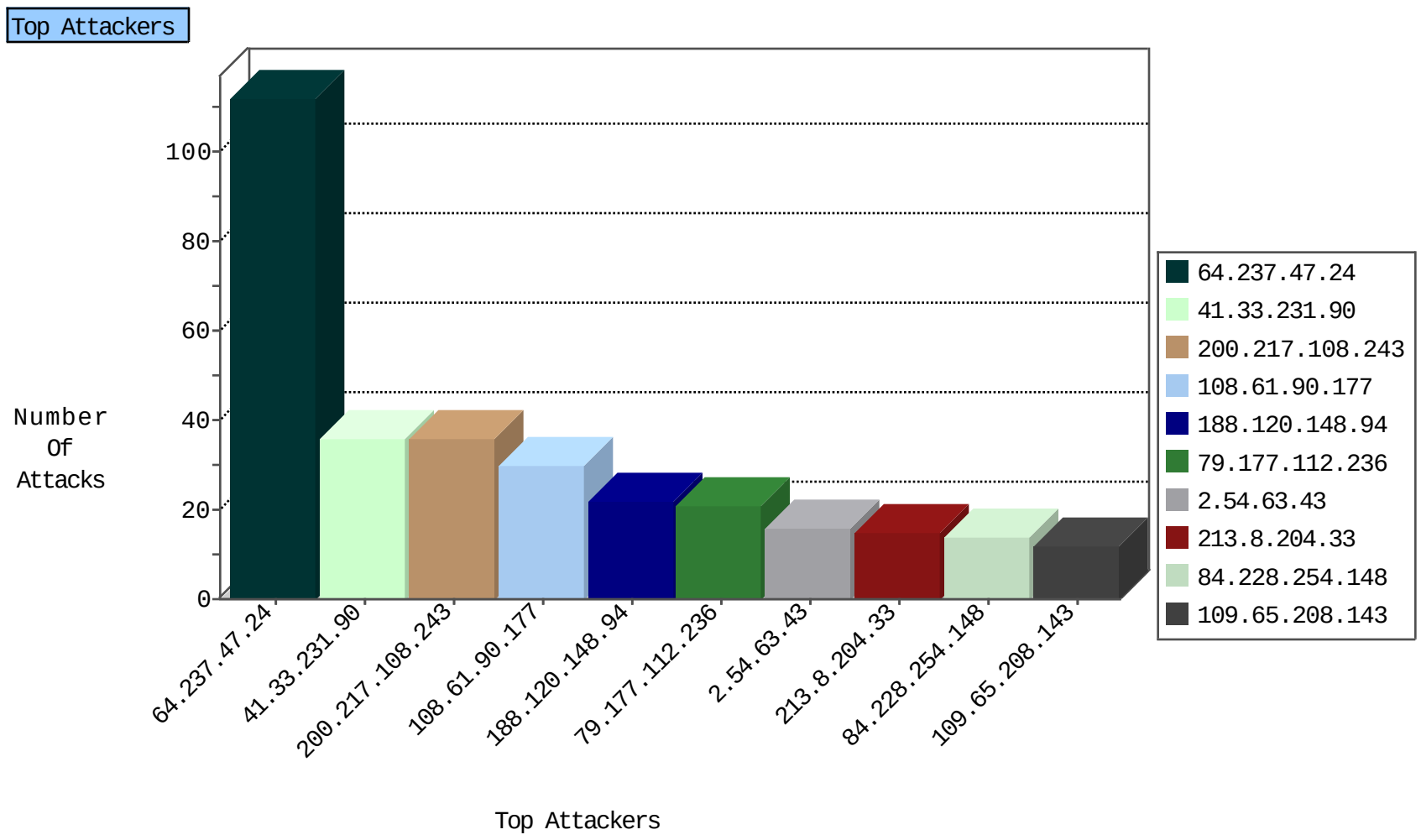
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

02-12-2016-01:06:11 to 02-12-2016-02:06:11

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.145.220.44	Europe	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	5
79.180.22.229	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
159.203.15.149	United States	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
159.203.71.54	United States	147.237.76.39	mobile.meitav.idf.il	Invalid TCP Flags	drop	1
115.230.124.164	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1
185.130.5.179		147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
142.54.160.212	United States	147.237.72.156	aman.idf.il	block-sp-traf1	drop	1

02-12-2016-01:06:11 to 02-12-2016-02:06:11

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.165.15.211	France	147.237.72.167	ishurim.aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1
198.50.134.71	Canada	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1

02-12-2016-01:06:11 to 02-12-2016-02:06:11

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	2
66.249.64.133	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
51.254.23.230	147.237.8.28	United Kingdom	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
193.105.134.220	147.237.77.233	Sweden	atal.idf.il	ET SCAN NMAP -sS window 1024	1

02-12-2016-01:06:11 to 02-12-2016-02:06:11

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
64.237.47.24	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	56
64.237.47.24	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	56
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
79.177.112.236	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
200.217.108.243	Brazil	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	19
200.217.108.243	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	17
108.61.90.177	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	15
108.61.90.177	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	15
109.65.208.143	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
188.120.148.94	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
84.228.254.148	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	7
84.228.254.148	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
2.54.185.136	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	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
46.19.85.213	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
66.249.65.18	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.254	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
50.118.197.42	United States	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.254	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
188.120.148.94	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
71.118.241.94	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
188.120.148.94	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
213.8.204.33	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
213.8.204.33	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
213.8.204.33	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
108.61.2.225	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
108.61.2.225	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
169.237.145.68	United States	147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
149.78.22.73	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.154.147.166	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.102.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
172.56.41.40	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
79.183.112.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
188.120.148.94	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
177.17.33.160	Brazil	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
208.115.111.73	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
94.230.86.52	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
62.210.206.180	France	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
77.163.84.205	Netherlands	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
81.169.237.146	Germany	147.237.77.61	e.cogat.idf.il	drop	SAM rule	drop	1
141.212.122.76	United States	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
77.163.84.205	Netherlands	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
159.121.166.99	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.153	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
213.8.204.33	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
37.46.38.23	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

02-12-2016-01:06:11 to 02-12-2016-02:06:11

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.63.43	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.63.43	Block	15
84.108.106.108	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	4
109.253.215.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.63.43	Israel	147.237.0.34	tikshuv.idf.il	Too Many 404: Response Code per Session	Block	1
185.120.126.201		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
157.55.39.39	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/left.asp	Block	1
66.249.66.131	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/3480.jpg	Block	1
207.46.13.58	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/navmenu/mazi.idf.il	Block	1
46.60.83.119	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
185.120.126.201		147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1
54.183.1.75	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/wp-login.php	Block	1
185.120.126.201		147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 185.120.126.201	Block	1
157.55.39.209	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.209	Block	1
66.249.66.136	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/5/2975.jpg	Block	1
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
185.120.126.201		147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 185.120.126.201	Block	1
66.249.64.229	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1396-he/atal.aspx	Block	1
40.77.167.32	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/smalim/html/1.asp	Block	1
185.120.126.201		147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	1
157.55.39.233	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
66.249.66.191	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/6/2726.jpg	Block	1
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
185.120.126.201		147.237.76.86	navy.idf.il	PHP Attempt	Block	1
141.165.60.183	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.65.18	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
186.193.132.145	Brazil	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
41.44.4.237	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
185.32.179.254	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
79.182.123.50	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 79.182.123.50 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	1
185.120.126.201		147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
157.55.39.39	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.39	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-23131-he/	Block	1
186.193.132.145	Brazil	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
41.44.4.237	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
185.120.126.201		147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
79.182.123.50	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
54.183.1.75	United States	147.237.77.74	law.idf.il	PHP Attempt	Block	1

02-12-2016-01:06:11 to 02-12-2016-02:06:11