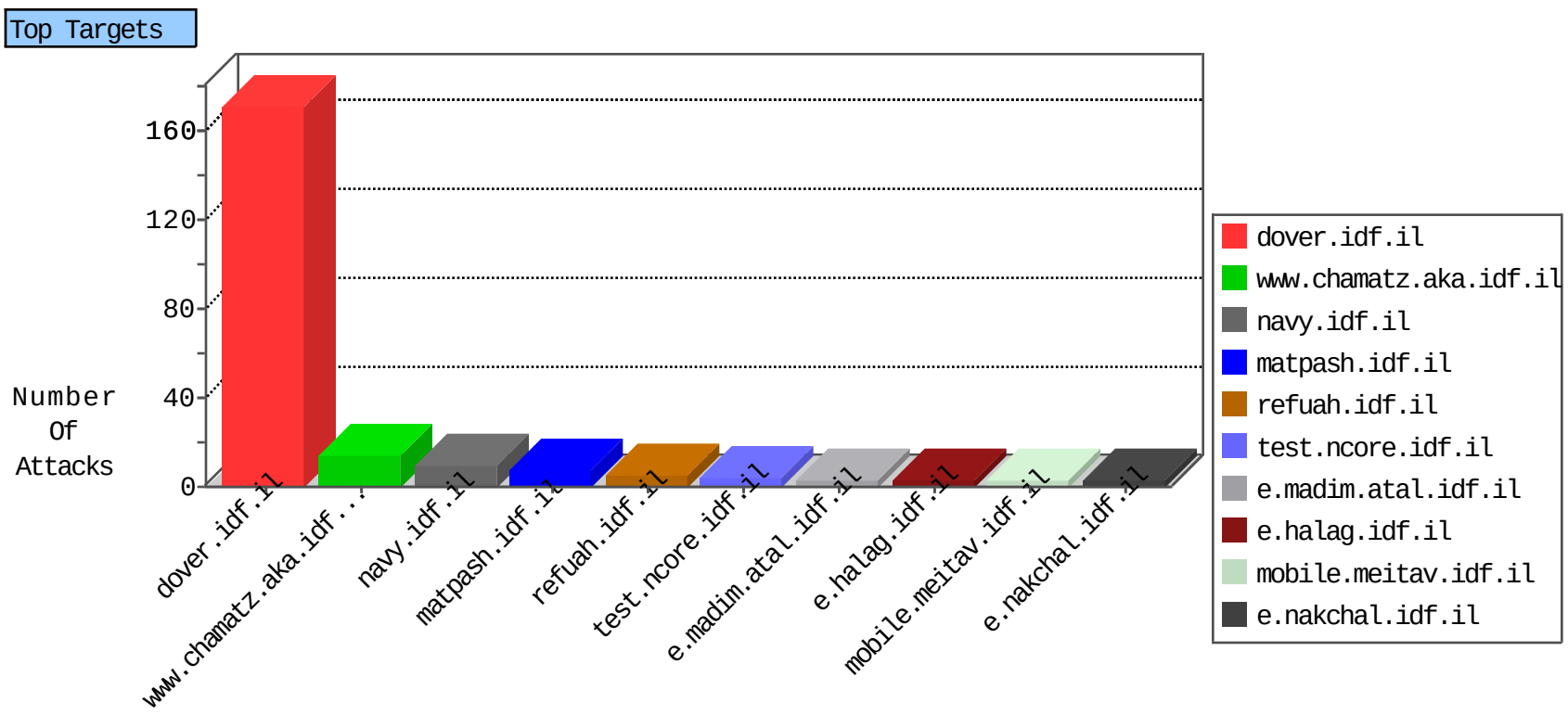
02-02-2016-04:04:08 to 02-02-2016-05:04:08

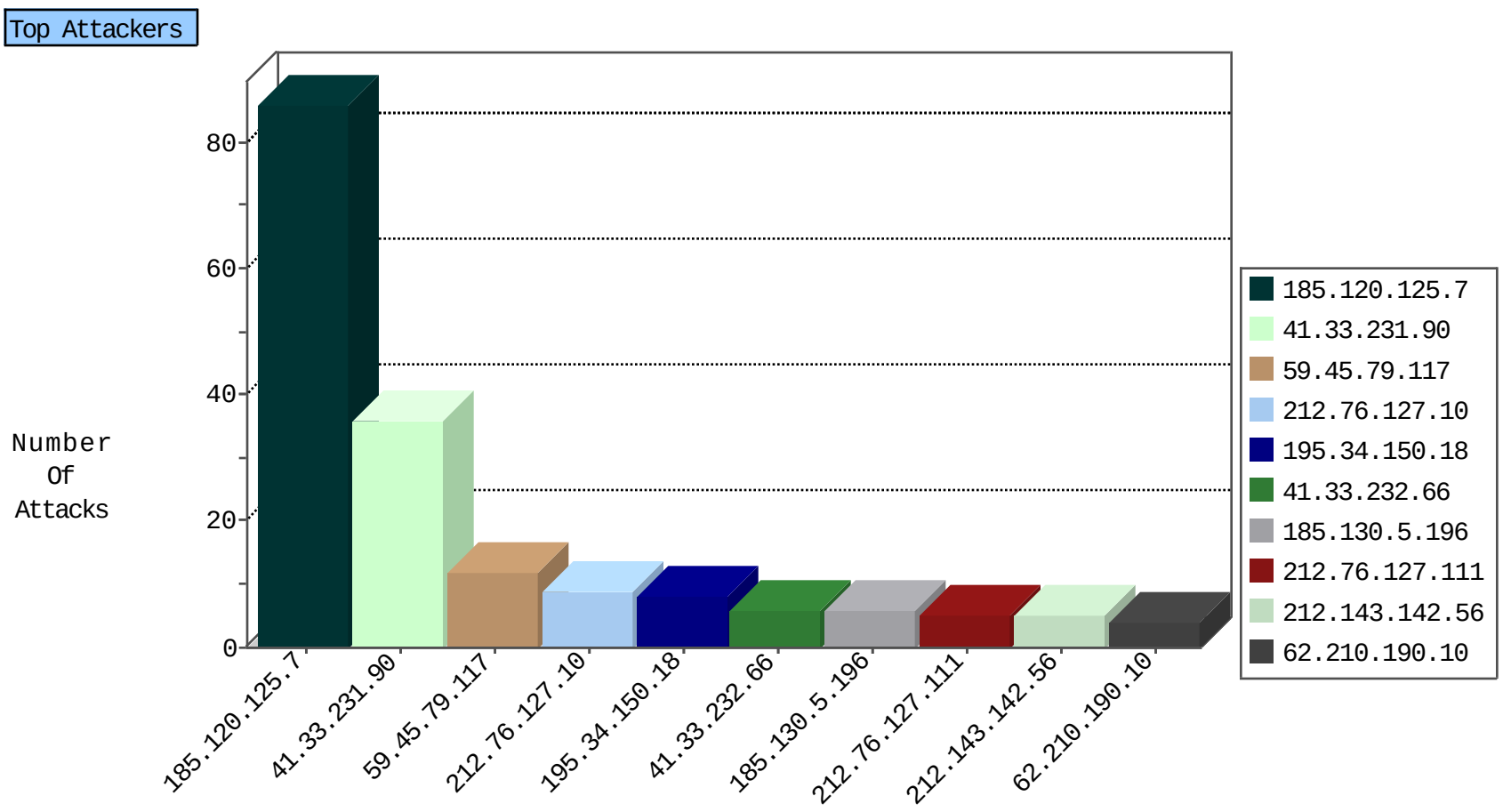
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

02-02-2016-04:04:08 to 02-02-2016-05:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	4
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
104.255.70.247		147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1

02-02-2016-04:04:08 to 02-02-2016-05:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.216.115.8		147.237.77.216	dover.idf.i	17272: HTTP: Suspicious User-Agent (WindowsNT) With No Separating Space	Block	2
51.255.162.163	United Kingdom	147.237.77.216	dover.idf.i	C106: HTTP: majestic bot	Block	1

02-02-2016-04:04:08 to 02-02-2016-05:04:08

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
66.249.75.130	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	2
59.45.79.117	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.196	147.237.77.61		e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
158.130.6.191	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN Rapid POP3 Connections - Possible Brute Force Attack	1
59.45.79.117	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
146.0.75.114	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
50.204.188.142	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 4096	1
98.119.105.221	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 3072	1
46.166.129.183	147.237.72.156	Netherlands	aman.idf.il	ET SCAN NMAP -sS window 2048	1
46.45.137.67	147.237.72.217	Turkey	e.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
173.55.32.113	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.8.46	China	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
146.0.75.114	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
146.0.75.114	147.237.76.86	Netherlands	navy.idf.il	ET SCAN NMAP -sS window 1024	1
50.204.188.142	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 3072	1
82.117.208.243	147.237.76.201		e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
46.166.129.183	147.237.72.156	Netherlands	aman.idf.il	ET SCAN NMAP -f -sS	1
59.45.79.117	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1

02-02-2016-04:04:08 to 02-02-2016-05:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
185.120.125.7		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	58
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
185.120.125.7		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	28
212.76.127.10	Israel	147.237.77.226	www.chamatz.aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
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	5
212.76.127.111	Israel	147.237.77.226	www.chamatz.aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
66.249.78.161	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
67.198.134.186	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
141.212.122.150	United States	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.58	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.130.5.196		147.237.76.148	gqcenter.aka.idf.il	drop	SAM rule	drop	1
141.212.122.156	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
137.116.71.170	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.102	United States	147.237.0.35	akaws.idf.il	drop		drop	1
141.212.122.150	United States	147.237.76.177	ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
83.31.40.221	Poland	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
216.218.206.92	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
47.18.211.68	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
185.130.5.196		147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	1
141.212.122.156	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.144	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.19	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
195.154.146.225	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
141.212.122.151	United States	147.237.76.177	ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
85.10.210.199	Germany	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
216.218.206.118	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
47.18.211.68	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.130.5.196		147.237.76.200	eitan.aka.idf.il	drop	SAM rule	drop	1
141.212.122.157	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.145	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.48	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
8.37.227.68	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
141.212.122.153	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
94.230.86.168	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
54.152.28.97	United States	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
185.130.5.196		147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
141.212.122.157	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.149	United States	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.55	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.130.5.196		147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	1
141.212.122.154	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
114.112.90.54	China	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
192.185.4.15	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
157.55.39.69	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

02-02-2016-04:04:08 to 02-02-2016-05:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
17.138.60.89	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	2
62.210.190.10	France	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
66.249.78.10	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding VsWyqxZX0UY!9:nRmp:CUt%YC4)S2Z9KLNT*N:B_dHSsf{j41sveTwA(zl;70(vz?)k in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
52.23.181.90	United States	147.237.76.86	navy.idf.il	Directory Traversal (In URL)	Block	1
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/2271.jpg	Block	1
62.210.190.10	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/license.php	Block	1
41.237.123.131	Egypt	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
195.154.226.90	France	147.237.77.216	dover.idf.il	Illegal HTTP Version HTTP/	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/main/rabanut/general.aspx	None	1
52.23.181.90	United States	147.237.76.86	navy.idf.il	Directory Traversal - 16	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unknown Parameter hc_location in www.aka.idf.il/main/giyus/general.aspx	None	1
66.249.64.42	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
41.237.123.131	Egypt	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/xmlrpc.php	Block	1
195.154.226.90	France	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 195.154.226.90	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
54.152.28.97	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il./images/shared/home.png	Block	1
84.108.208.214	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1412-he/atal.aspx	Block	1
66.249.69.24	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/sidebar/sidebar.js	Block	1
41.237.123.131	Egypt	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
66.249.78.177	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/news/{"key":"	Block	1
41.36.182.92	Egypt	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
157.55.39.6	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/resources/content/images/insignia/54dotgif	Block	1
41.237.123.131	Egypt	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/xmlrpc.php	Block	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
62.210.190.10	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 62.210.190.10	Block	1
41.36.182.92	Egypt	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	1
188.143.232.35	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1

02-02-2016-04:04:08 to 02-02-2016-05:04:08