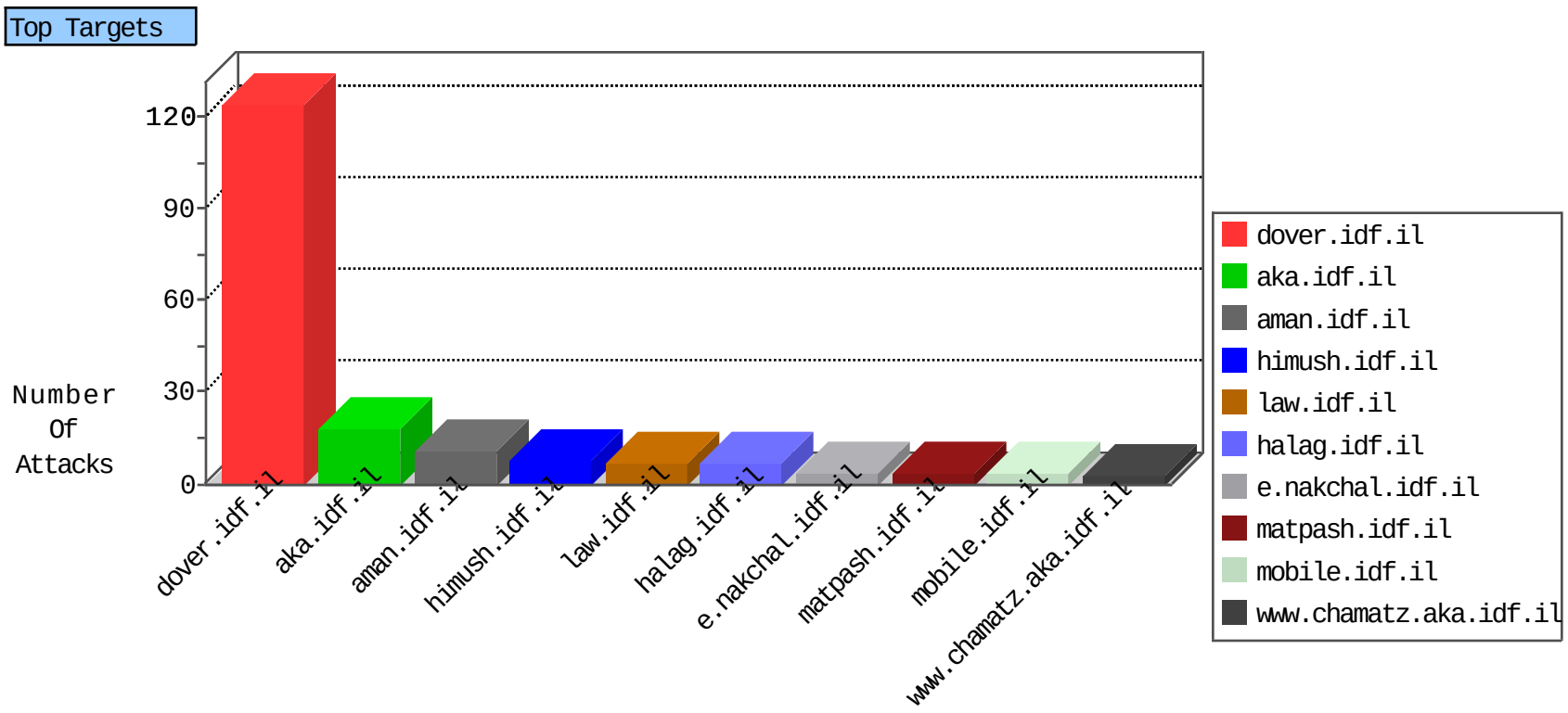
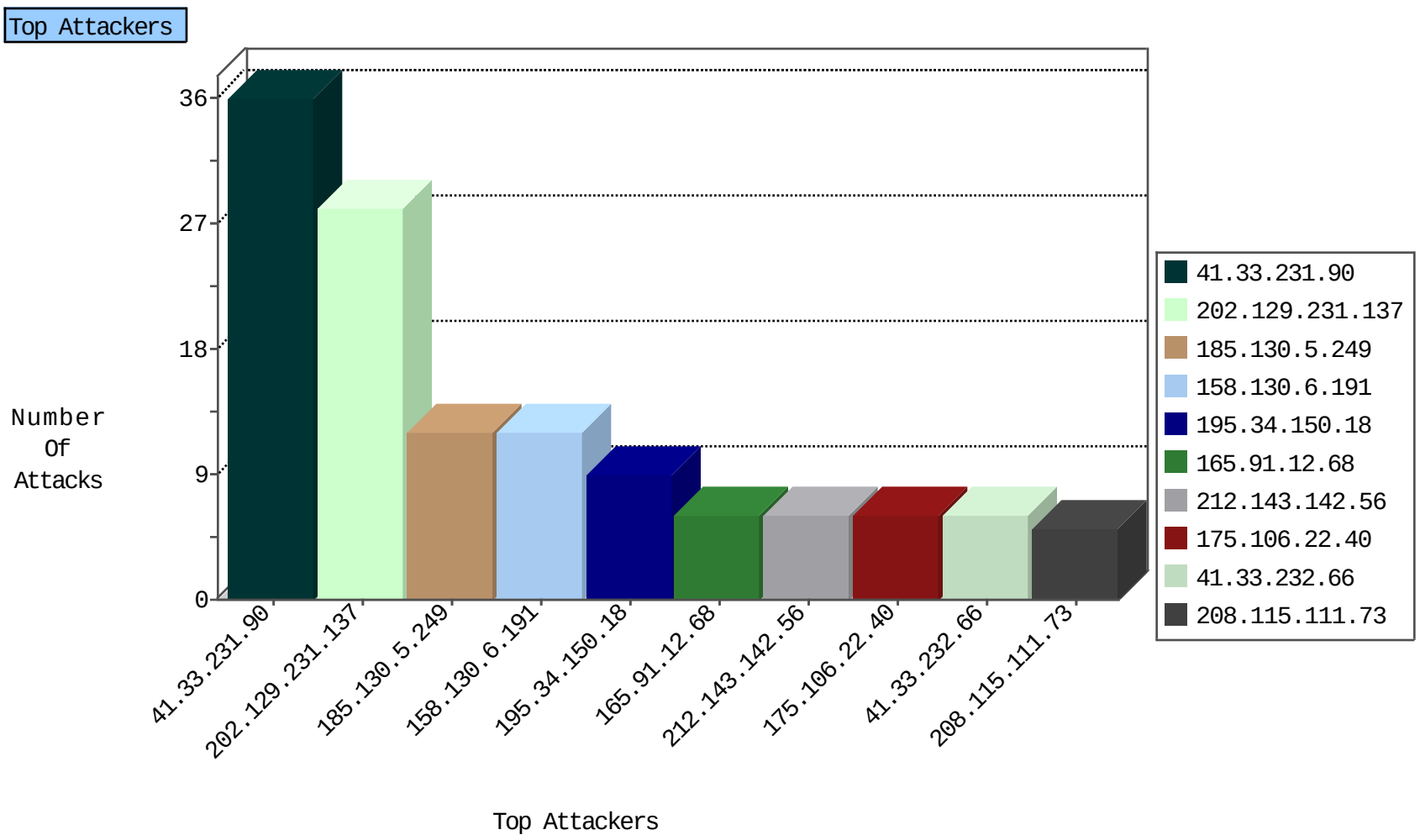
02-11-2016-04:04:02 to 02-11-2016-05:04:02

IDF Under Attack Daily Report



Top Target



Top Attackers

02-11-2016-04:04:02 to 02-11-2016-05:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
36.81.31.130	Indonesia	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	3
116.192.8.111	China	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	2
115.239.228.10	China	147.237.76.34	yohalan.idf.il	JLM_Under_Attack_Con_Http	drop	2
206.196.184.99	United States	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	2
185.62.188.131	Netherlands	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
66.240.192.138	United States	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.228		147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1

02-11-2016-04:04:02 to 02-11-2016-05:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-11-2016-04:04:02 to 02-11-2016-05:04:02

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
46.45.137.67	147.237.76.30	Turkey	himush.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.21.73	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.249	147.237.77.234		halag.idf.il	ET SCAN NMAP -sS window 1024	1
183.61.109.189	147.237.77.234	China	halag.idf.il	ET SCAN NMAP -sS window 1024	1
175.99.87.209	147.237.8.27	Taiwan	e.madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
82.117.208.243	147.237.8.14		e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
60.169.78.38	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
60.169.78.38	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
222.186.21.73	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
46.45.137.67	147.237.76.38	Turkey	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.21.73	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
183.61.109.189	147.237.77.234	China	halag.idf.il	ET SCAN NMAP -sS window 4096	1
175.99.87.209	147.237.8.27	Taiwan	e.madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1
175.99.87.209	147.237.8.27	Taiwan	e.madim.atal.idf.il	ET SCAN NMAP -f -sS	1
60.169.78.38	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
60.169.78.38	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
60.169.78.38	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
222.186.21.73	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1

02-11-2016-04:04:02 to 02-11-2016-05:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
202.129.231.137	Australia	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
202.129.231.137	Australia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
175.106.22.40	Indonesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	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	5
141.0.14.243	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
79.179.0.220	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
109.66.179.24	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.111.105.19	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
66.249.78.216	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
24.246.35.189	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
79.177.173.4	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
91.200.12.7	Ukraine	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
208.115.111.73	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
130.193.50.33	Russian Federation	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
91.200.12.7	Ukraine	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	2
158.130.6.191	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
208.115.111.73	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
158.130.6.191	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.130.5.249		147.237.77.234	halag.idf.il	drop	SAM rule	drop	1
184.105.247.244	United States	147.237.77.212	e.dover.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
165.91.12.68	United States	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	1
216.218.206.124	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
158.130.6.191	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.202	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.130.5.249		147.237.77.121	e.navy.idf.il	drop	SAM rule	drop	1
184.105.139.122	United States	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
165.91.4.53	United States	147.237.72.156	aman.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
8.37.227.70	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
158.130.6.191	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.130.5.249		147.237.77.235	sviva.idf.il	drop	SAM rule	drop	1
141.212.122.198	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.130.5.249		147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
165.91.12.68	United States	147.237.72.166	aka.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
221.199.217.173	Australia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
158.130.6.191	United States	147.237.76.177	ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.202	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.130.5.249		147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
115.230.124.164	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
184.105.139.122	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
80.82.64.68	Netherlands	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
165.91.4.53	United States	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	1
208.115.113.88	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
8.37.227.81	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
158.130.6.191	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.130.5.249		147.237.77.243	mobile.idf.il	drop	SAM rule	drop	1

02-11-2016-04:04:02 to 02-11-2016-05:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	1
165.91.12.68	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il/robots.txt	Block	1
79.180.117.161	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
40.77.167.40	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/kamlar/news/×¢×œ ×?×£ ×©×?×™ × ×• × ×—×©×‘ ×¡×˜×“×˜× ×˜ ×¢×•×œ× ×¤×•×¤×•×œ×¨×™×•×ª ×?×©×¨×™×?×” ×œ×©×©×?×” ×¢×©×¨×•×ª, ×¨×©×?×™ ×œ×”×¤×¢×™×œ ×‘×©×©×” ×•×œ×¢×ª×?	Block	1
207.46.13.31	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.31	Block	1
145.255.2.4	Russian Federation	147.237.77.74	law.idf.il	Parameter Type Violation InfoCenterItem in www.law.idf.il/templates/getfile/getfile.aspx	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
165.91.12.68	United States	147.237.72.166	aka.idf.il	Multiple NULL Character in Method from 165.91.12.68	Block	1
106.51.22.253	India	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
66.249.64.181	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/321-en/patzar.aspxthe	Block	1
207.46.13.31	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
157.55.39.113	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.112	Block	1
165.91.12.68	United States	147.237.72.166	aka.idf.il	NULL Character in Method	Block	1
106.51.22.253	India	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
66.249.64.229	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
207.46.13.88	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
157.55.39.209	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/toolfs.asp	Block	1
68.180.229.121	United States	147.237.76.200	eitan.aka.idf.i	Unauthorized URL Access to www.eitan.aka.idf.il/shared/usercontrols/headerupper/	Block	1
201.24.171.147	Brazil	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
123.125.71.89	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/3192.pdf	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush	Block	1
165.91.4.53	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
79.177.167.103	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/requestpayslipexplanation.aspx	None	1
201.24.171.147	Brazil	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
145.255.2.4	Russian Federation	147.237.77.74	law.idf.il	Parameter Type Violation FileName in www.law.idf.il/templates/getfile/getfile.aspx	Block	1

02-11-2016-04:04:02 to 02-11-2016-05:04:02