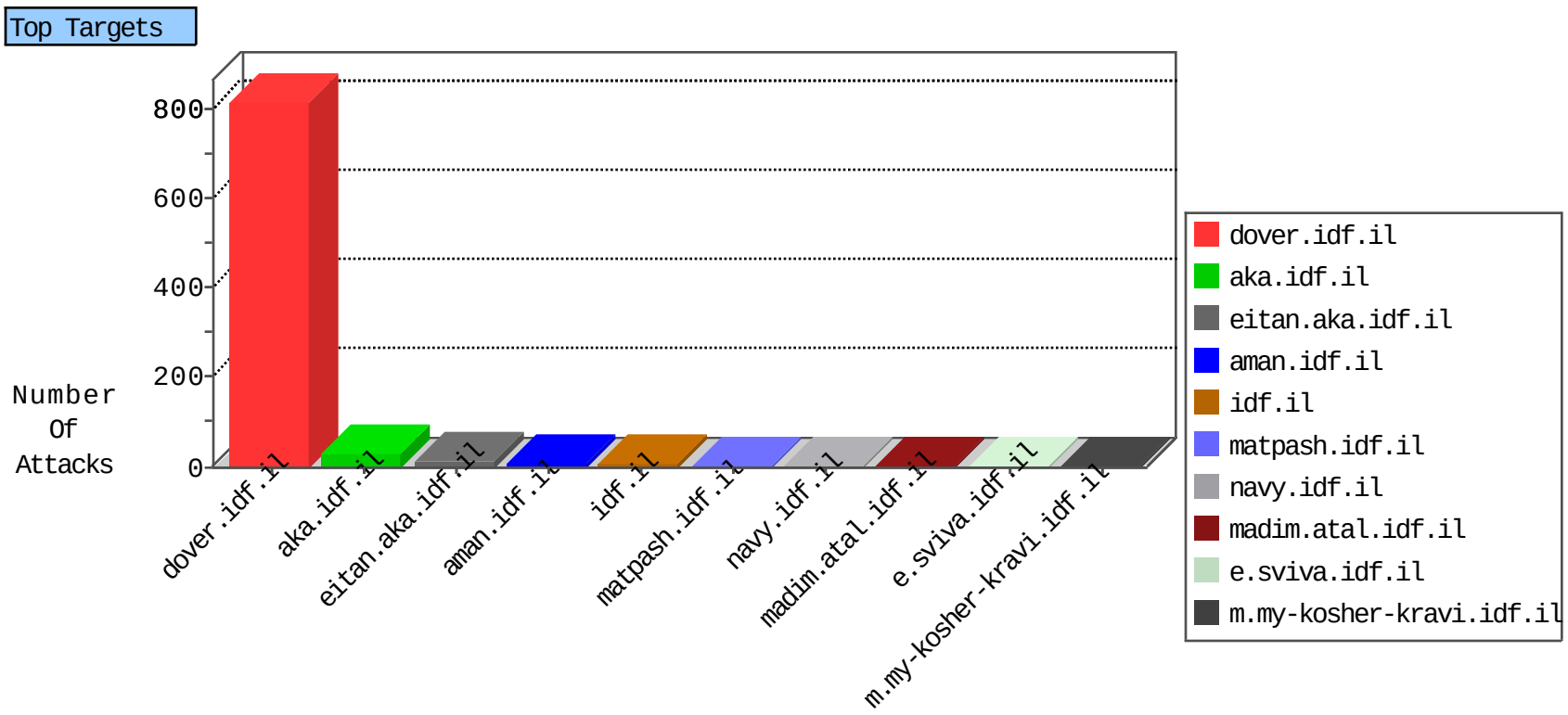
03-11-2016-05:04:07 to 03-11-2016-06:04:07

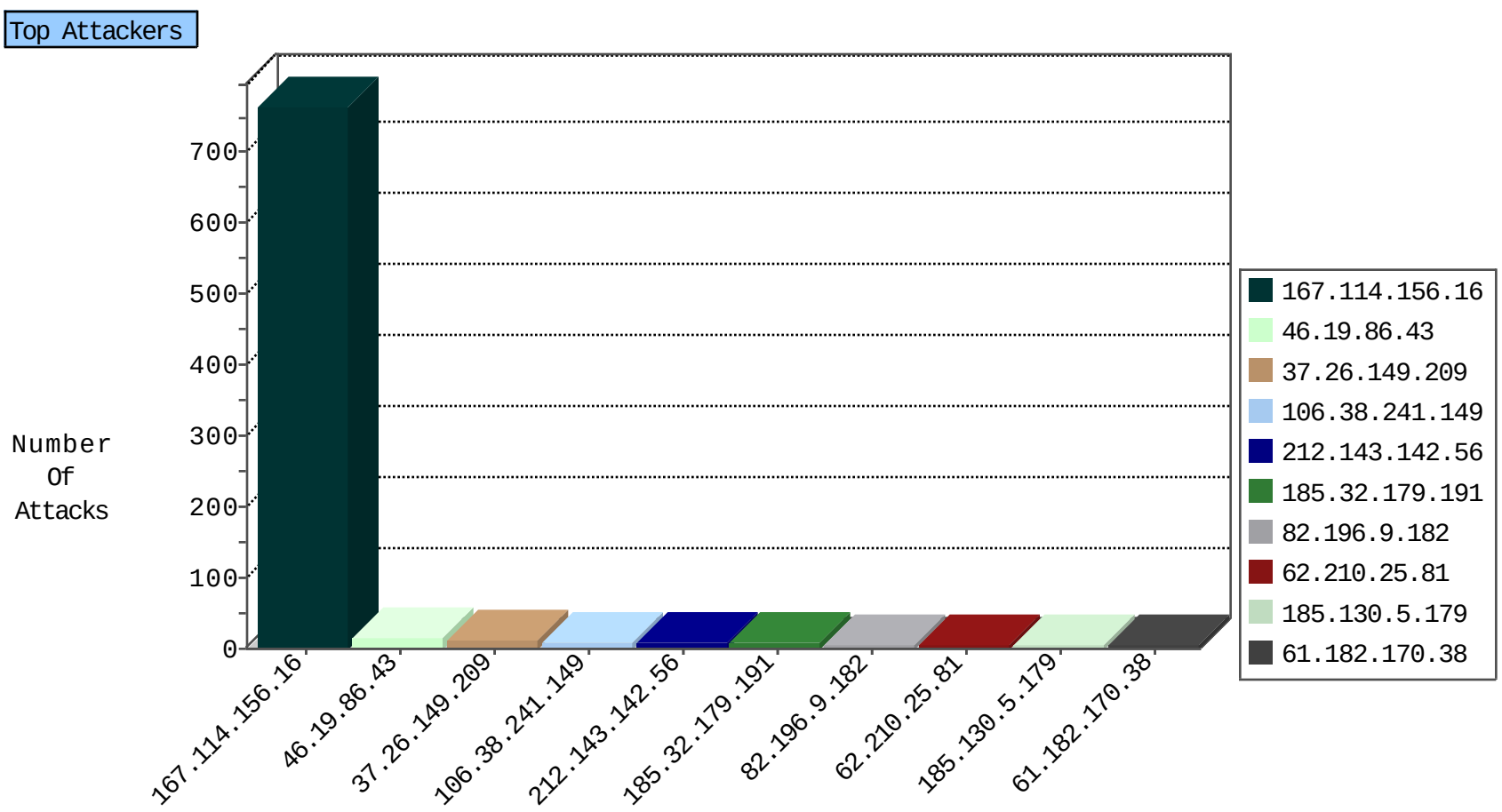
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

03-11-2016-05:04:07 to 03-11-2016-06:04:07

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	3419
46.19.86.43	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	88
204.42.253.2	United States	147.237.77.61	e.cogat.idf.il	Block_Ntp_All_Net	drop	2
184.105.139.80	United States	147.237.8.46	e.chinuch.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.72	United States	147.237.8.50	e.tikshuv.idf.il	Block_Ntp_All_Net	drop	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
184.105.139.72	United States	147.237.72.217	e.idf.il	Block_Ntp_All_Net	drop	1
141.212.122.198	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1

03-11-2016-05:04:07 to 03-11-2016-06:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.149	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	8
199.58.86.206	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
86.132.215.31	United Kingdom	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
108.59.8.70	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
69.116.219.171	United States	147.237.77.216	dover.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-11-2016-05:04:07 to 03-11-2016-06:04:07

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
61.182.170.38	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.179	147.237.77.61		e.cogat.idf.il	ET SCAN Potential SSH Scan	1
42.247.4.164	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.179	147.237.76.176		test.ncore.idf.il	ET SCAN Potential SSH Scan	1
23.96.109.87	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
185.130.5.179	147.237.72.166		aka.idf.il	ET SCAN Potential SSH Scan	1
173.224.117.146	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
66.249.64.253	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
62.210.25.81	147.237.0.33	France	idf.il	ET SCAN NMAP -sS window 1024	1
61.182.170.38	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
61.182.170.38	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
189.254.90.133	147.237.76.196	Mexico	e.sviva.idf.il	ET SCAN NMAP -f -sS	1
42.247.4.164	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.179	147.237.76.196		e.sviva.idf.il	ET SCAN Potential SSH Scan	1
23.96.109.87	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
185.130.5.179	147.237.72.167		ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
178.63.11.208	147.237.77.227	Germany	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
82.117.208.243	147.237.77.74		law.idf.il	ET SCAN NMAP -sS window 1024	1
62.210.25.81	147.237.0.33	France	idf.il	ET SCAN NMAP -sS window 2048	1
62.210.25.81	147.237.0.33	France	idf.il	ET SCAN NMAP -f -sS	1
61.182.170.38	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
189.254.90.133	147.237.76.196	Mexico	e.sviva.idf.il	ET SCAN NMAP -sS window 2048	1

03-11-2016-05:04:07 to 03-11-2016-06:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.26.149.209	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
185.32.179.191	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
109.253.143.203	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.14.172	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.114.107.70	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
31.154.19.209	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
5.22.135.235	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
144.76.93.46	Germany	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
46.120.100.173	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
62.210.25.81	France	147.237.0.33	idf.il	drop		drop	2
82.196.9.182	Netherlands	147.237.0.34	tikshuv.idf.il	Web Server Enforcement Violation	Masscan Port Scanner	reject	1
216.218.206.78	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
5.28.135.37	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.247.223	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.219	United States	147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.7	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
184.105.139.74	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.142	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
82.196.9.182	Netherlands	147.237.72.156	aman.idf.il	Web Server Enforcement Violation	Masscan Port Scanner	reject	1
216.218.206.78	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.231	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.220	United States	147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
96.246.211.180	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.15	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
192.241.202.144	United States	147.237.0.35	akaws.idf.il	drop		drop	1
184.105.139.111	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.143	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
82.196.9.182	Netherlands	147.237.72.166	aka.idf.il	Web Server Enforcement Violation	Masscan Port Scanner	reject	1
220.181.108.186	China	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.32.179.191	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
106.120.173.159	China	147.237.77.233	atal.idf.il	drop	SAM rule	drop	1
82.196.9.182	Netherlands	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
195.62.53.168	Russian Federation	147.237.8.27	e.madim.atal.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1
5.22.135.235	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.112	United States	147.237.0.33	idf.il	drop		drop	1
141.212.122.208	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
82.196.9.182	Netherlands	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
185.32.179.191	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid sequence number	alert	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
82.196.9.182	Netherlands	147.237.0.33	idf.il	drop		drop	1
5.28.135.37	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
184.105.139.112	United States	147.237.8.27	e.madim.atal.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.209	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
85.114.107.70	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
185.32.179.191	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid sequence number	monitor	1
123.125.71.15	China	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

03-11-2016-05:04:07 to 03-11-2016-06:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.64.22.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
121.169.10.226	Korea, Republic of	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	2
121.169.10.226	Korea, Republic of	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
72.74.162.73	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.253	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
92.98.236.92	United Arab Emirates	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
37.142.68.1	Israel	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
131.253.25.230	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.66.22	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/templates/news/news.aspx	Block	1
92.98.236.92	United Arab Emirates	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	1
37.142.68.1	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
167.114.172.229	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	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
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
180.76.15.7	China	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/1105-en/contactus.aspx	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/main.asp	Block	1
66.249.64.186	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
195.138.85.250	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/sendtofriend/sendtofriend.aspx?&amp	Block	1

03-11-2016-05:04:07 to 03-11-2016-06:04:07