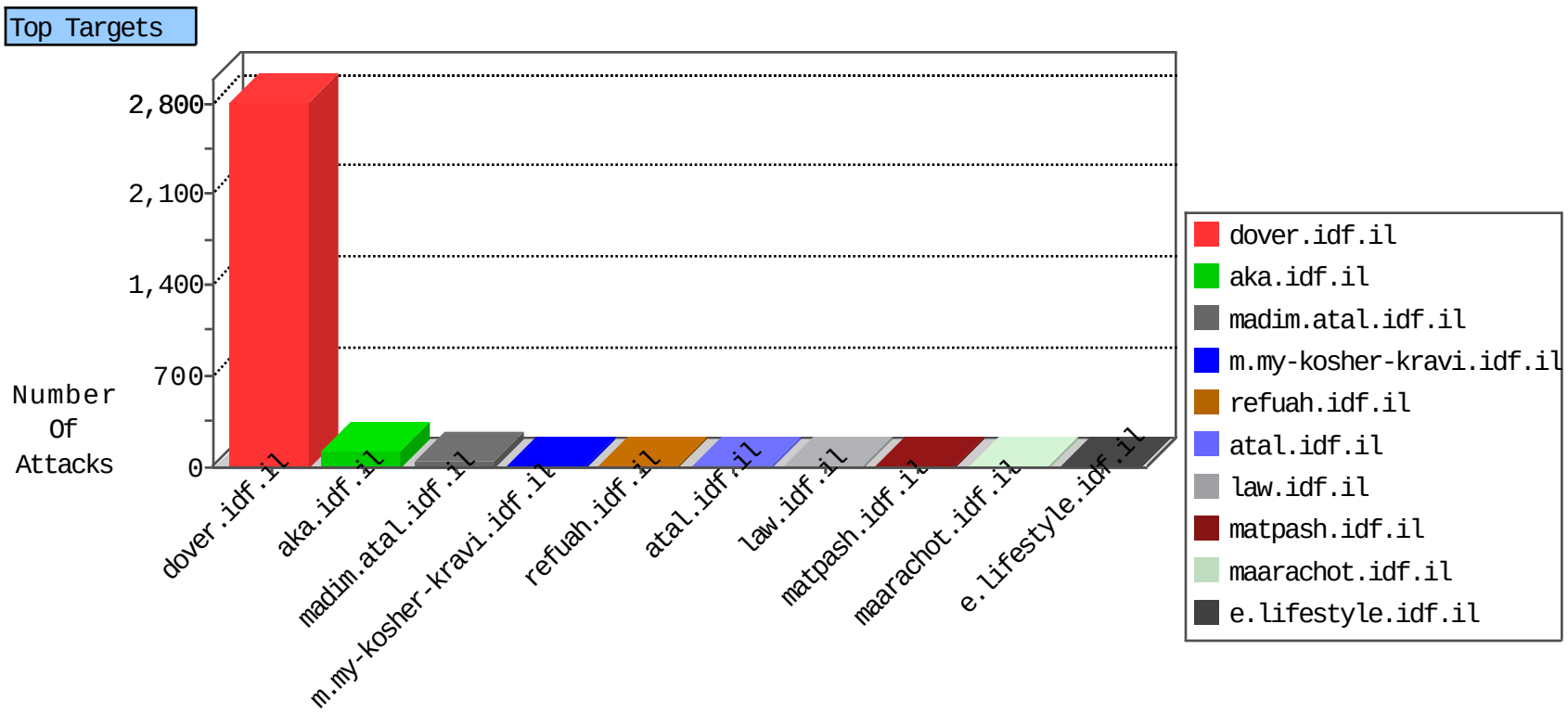
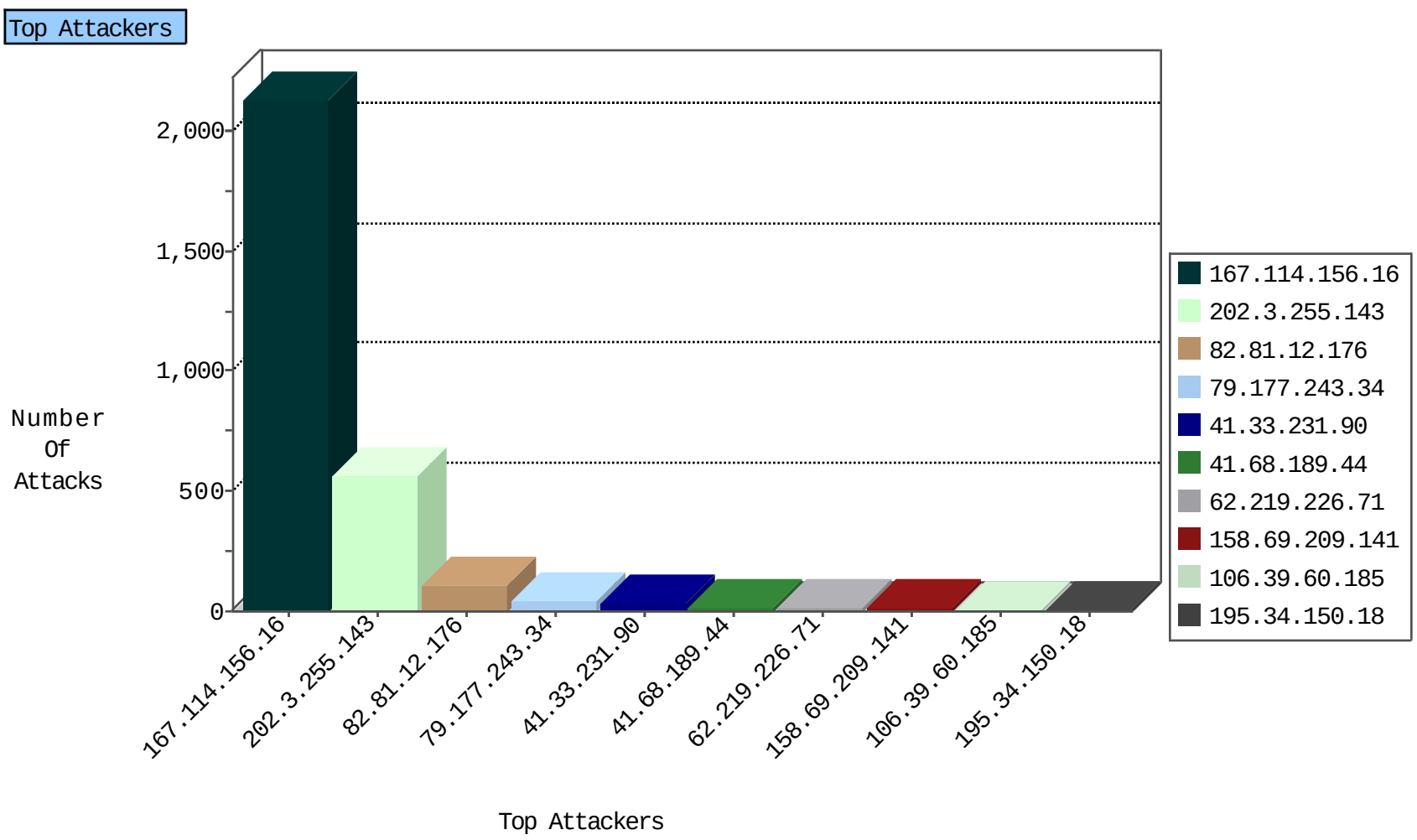
01-20-2016-04:04:08 to 01-20-2016-05:04:08

IDF Under Attack Daily Report





Top Attackers

01-20-2016-04:04:08 to 01-20-2016-05:04:08

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	3060
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	107
185.130.5.224		147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1

01-20-2016-04:04:08 to 01-20-2016-05:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
158.69.209.141	United States	147.237.76.31	nakchal.idf.il	C106: HTTP: majestic bot	Block	2
158.69.209.141	United States	147.237.76.86	navy.idf.il	C106: HTTP: majestic bot	Block	2
158.69.209.141	United States	147.237.77.74	law.idf.il	C106: HTTP: majestic bot	Block	2
158.69.209.141	United States	147.237.77.170	maarachot.idf.il	C106: HTTP: majestic bot	Block	2
158.69.209.141	United States	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	2
188.165.15.231	France	147.237.72.156	aman.idf.il	C228: HTTP: AhrefBot crawler	Block	1
106.38.241.106	China	147.237.76.42	refuah.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
106.39.60.178	China	147.237.8.45	e.eitan.idf.il	13891: TLS: OpenSSL Encrypted/Unencrypted Heartbeat Packet	Permit	1
106.39.60.178	China	147.237.8.46	e.chinuch.idf.il	13891: TLS: OpenSSL Encrypted/Unencrypted Heartbeat Packet	Permit	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

01-20-2016-04:04:08 to 01-20-2016-05:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
202.3.255.143	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	527
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
37.187.24.36	147.237.77.216	France	dover.idf.il	Tehila - Perl LWP with fake user agent	3
143.208.27.192	147.237.0.34		tikshuv.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.28	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	2
212.7.211.7	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
143.208.27.192	147.237.8.14		e.orchot.idf.il	ET SCAN Potential SSH Scan	1
85.93.5.65	147.237.77.235	Germany	sviva.idf.il	ET SCAN Potential SSH Scan	1
46.161.40.120	147.237.0.17	Russian Federation	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.72.166	China	aka.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.227.7	147.237.0.15	Ukraine	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
143.208.27.192	147.237.0.35		akaws.idf.il	ET SCAN Potential SSH Scan	1
143.208.27.192	147.237.0.33		idf.il	ET SCAN Potential SSH Scan	1

01-20-2016-04:04:08 to 01-20-2016-05:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
202.3.255.143	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
41.68.189.44	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
212.143.142.56	Israel	147.237.77.216	dover.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
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
66.183.199.239	Canada	147.237.77.216	dover.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
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
106.39.60.185	China	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
41.68.189.44	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
195.154.56.44	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
212.76.127.10	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
157.55.39.60	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.76.127.111	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
157.55.39.131	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
66.249.78.160	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
106.39.60.185	China	147.237.8.27	e.madim.atal.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	2
208.120.46.224	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
106.39.60.185	China	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
84.228.127.115	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	2
40.77.167.105	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
106.39.60.185	China	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
5.102.254.132	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
64.125.239.113	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.146	United States	147.237.0.35	akaws.idf.il	drop		drop	1
108.168.185.133	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.227	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
142.59.115.168	Canada	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
37.48.101.193	Netherlands	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
141.212.121.192	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
64.125.239.180	United States	147.237.76.148	gqcenter.aka.idf.i	drop		drop	1
141.212.122.146	United States	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
207.46.13.5	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
74.82.47.26	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.228	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.85.239	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
142.59.115.168	Canada	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
37.142.68.25	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.145	United States	147.237.0.35	akaws.idf.il	drop		drop	1
217.91.39.121	Germany	147.237.72.166	aka.idf.il	Header Rejection	header rejection pattern found in request	monitor	1
195.154.56.44	France	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
64.125.239.232	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.139.75	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.146	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
130.193.50.33	Russian Federation	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
74.82.47.26	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.232	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

01-20-2016-04:04:08 to 01-20-2016-05:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.177.243.34	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	42
62.219.226.71	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 62.219.226.71	None	13
107.170.129.218	United States	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 107.170.129.218	Block	3
37.187.24.36	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 37.187.24.36	Block	2
37.187.24.36	France	147.237.77.216	dover.idf.il	PHP Attempt	Block	2
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20315-he/dover.aspx	Block	1
216.218.206.68	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
68.180.230.167	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in nakhal.idf.il/1117-he/nakhal.aspx	Block	1
107.170.129.218	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/shared/usercontrols/headerupper/	Block	1
66.249.69.48	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
217.91.39.121	Germany	147.237.72.166	aka.idf.il	E-mail collector robots 14	Block	1
111.217.132.24	Japan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/kapatz/default.aspx 	Block	1
217.91.39.121	Germany	147.237.72.166	aka.idf.il	eMail Hoarding	Block	1
91.200.12.138	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1086-17714-en/dover.aspx/trackback/	Block	1
62.219.226.71	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
157.55.39.193	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	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
91.207.60.64	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
216.218.206.66	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/igf	Block	1
37.48.101.193	Netherlands	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1

01-20-2016-04:04:08 to 01-20-2016-05:04:08