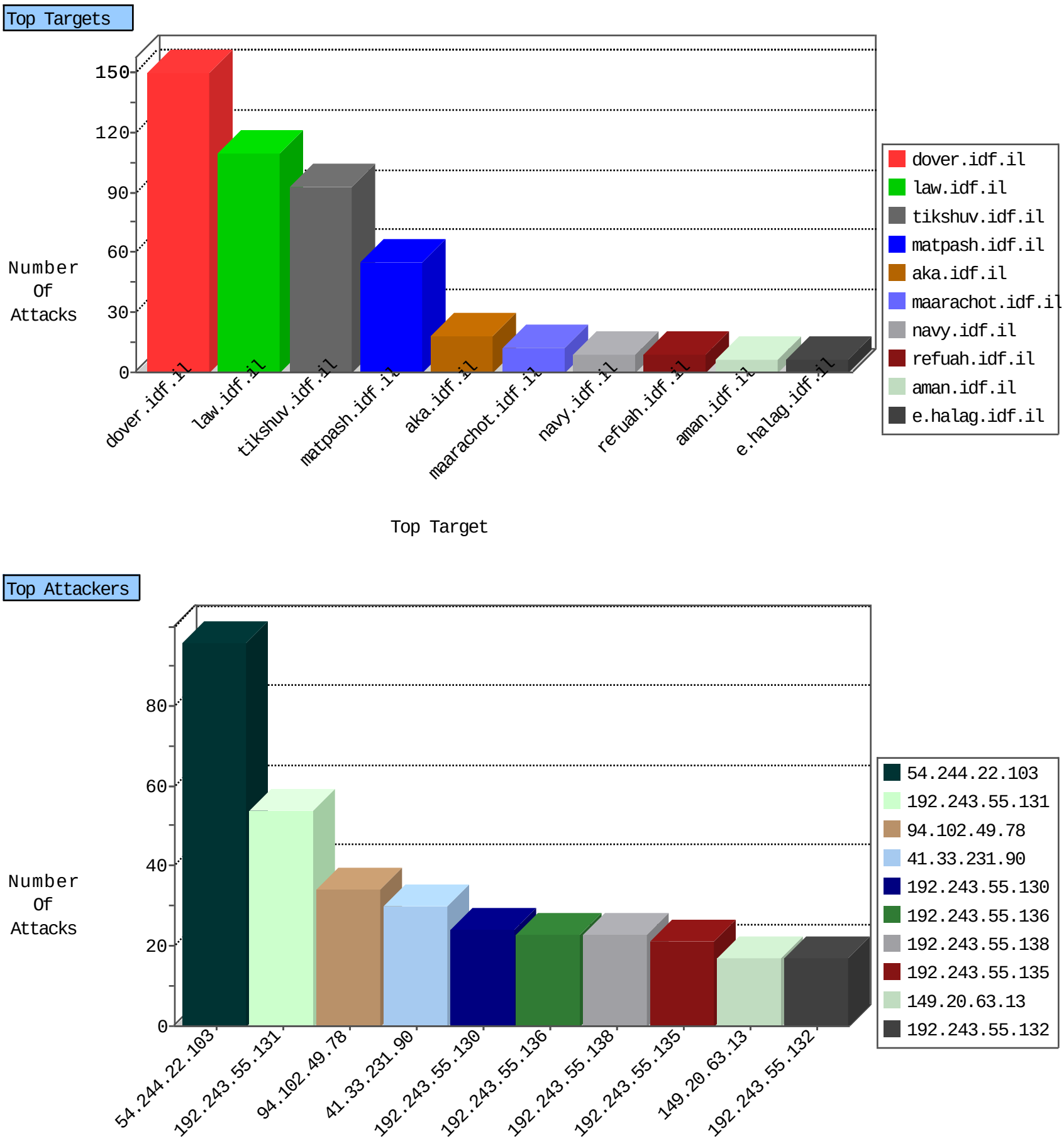
02-18-2016-04:04:09 to 02-18-2016-05:04:09

IDF Under Attack Daily Report



02-18-2016-04:04:09 to 02-18-2016-05:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
115.239.228.10	China	147.237.76.200	eitan.aka.idf.il	JLM_Under_Attack_Con_Http	drop	2
185.130.5.179		147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.246		147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
46.218.35.219	France	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.246		147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
85.107.113.242	Turkey	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.246		147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.246		147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1

02-18-2016-04:04:09 to 02-18-2016-05:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	2
40.77.167.14	United States	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	1
157.55.39.87	United States	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	1

02-18-2016-04:04:09 to 02-18-2016-05:04:09

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
41.140.253.9	147.237.77.243	Morocco	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
41.140.253.9	147.237.77.243	Morocco	mobile.idf.il	ET SCAN NMAP -sS window 3072	1
188.64.169.106	147.237.0.19	Russian Federation	madim.atal.idf.il	ET SCAN Potential SSH Scan	1

02-18-2016-04:04:09 to 02-18-2016-05:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	91
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
149.20.63.13	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	17
46.19.85.42	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.52.83.133	Saudi Arabia	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.131	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
192.243.55.131	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
46.52.83.133	Saudi Arabia	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
82.145.220.122	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.130	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.216	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	5
192.243.55.136	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
94.102.153.58	United Kingdom	147.237.77.74	law.idf.il	drop	SAM rule	drop	4
192.243.55.132	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.130	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
94.102.49.78	Netherlands	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
190.9.203.24	Colombia	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.216	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
94.102.49.78	Netherlands	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
94.102.49.78	Netherlands	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
192.243.55.131	Dominica	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
2.54.12.201	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
221.139.14.120	Korea, Republic of	147.237.72.166	aka.idf.il	drop	SAM rule	drop	3
94.102.49.78	Netherlands	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
177.185.194.45	Brazil	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
192.243.55.131	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
192.243.55.130	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
94.102.49.78	Netherlands	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
94.102.49.78	Netherlands	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
192.243.55.130	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
192.243.55.136	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
192.243.55.132	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
94.102.49.78	Netherlands	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
69.157.13.103	Canada	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
94.102.49.78	Netherlands	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
94.102.49.78	Netherlands	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3

02-18-2016-04:04:09 to 02-18-2016-05:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
87.255.95.145	Moldova, Republic of	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	1
192.243.55.130	Dominica	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/getfile.aspx?filename=xgf5b3nolwrvy3ncdghpa2fcdhphdmltxdewmtguzg9j&infocenteritem=true	Block	1
107.168.32.37	United States	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1
2.52.144.238	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
177.185.194.45	Brazil	147.237.72.156	aman.idf.il	MSSQL Data Retrieval with Implicit Conversion Errors	None	1
94.102.49.78	Netherlands	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to savash.org/	Block	1
208.115.113.89	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/tizmoret/sitemap/	Block	1
107.168.32.37	United States	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
37.142.195.151	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$23 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
177.185.194.45	Brazil	147.237.72.156	aman.idf.il	Multiple signatures from 177.185.194.45	Block	1
94.102.49.78	Netherlands	147.237.77.74	law.idf.il	Unauthorized URL Access to savash.org/	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/9/59829.pdf	Block	1
65.55.210.226	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
184.105.247.196	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
107.168.32.37	United States	147.237.72.166	aka.idf.il	E-mail collector robots 14	Block	1
172.94.14.47		147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1395-en/dover.aspx	Block	1
188.138.1.218	Germany	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
107.168.32.37	United States	147.237.72.166	aka.idf.il	eMail Hoarding	Block	1
172.94.14.47		147.237.77.216	dover.idf.il	Parameter Type Violation lang in www.idf.il/1395-en/dover.aspx	Block	1

02-18-2016-04:04:09 to 02-18-2016-05:04:09