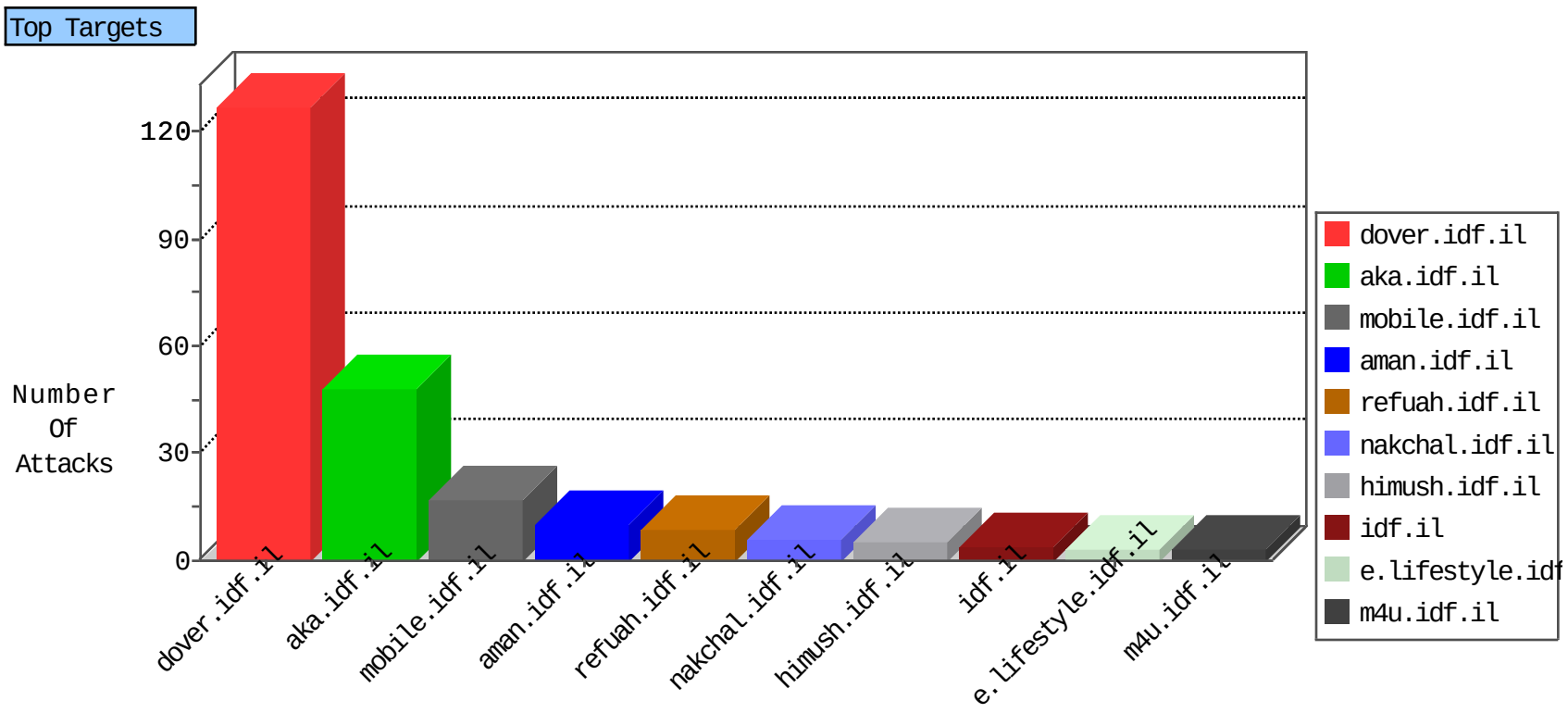
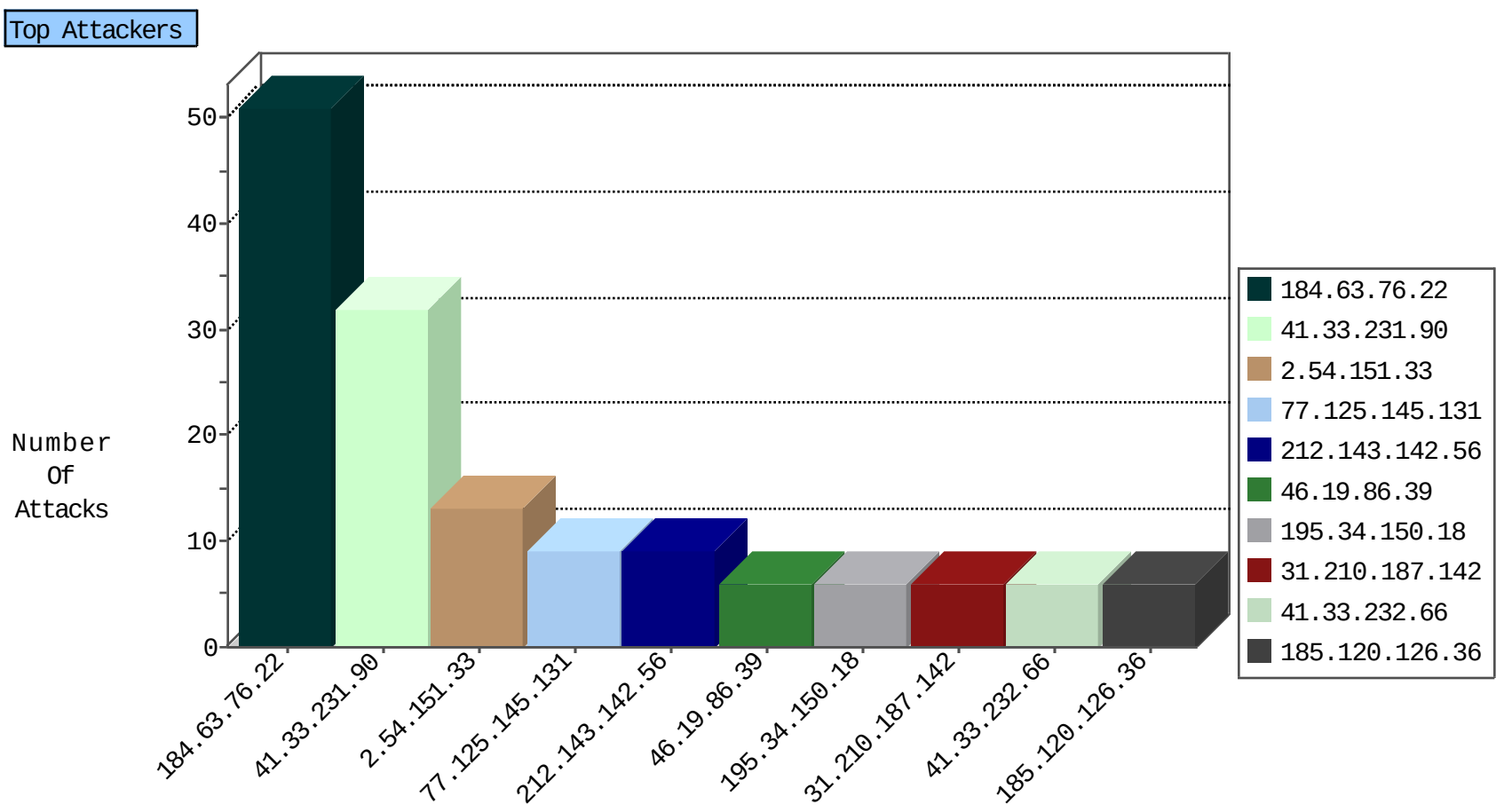
02-10-2016-06:04:02 to 02-10-2016-07:04:02

IDF Under Attack Daily Report





02-10-2016-06:04:02 to 02-10-2016-07:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
204.42.253.2	United States	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
71.6.216.58	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
184.63.76.22	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	1

02-10-2016-06:04:02 to 02-10-2016-07:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.130.5.207		147.237.76.30	himush.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1

02-10-2016-06:04:02 to 02-10-2016-07:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
77.85.35.211	147.237.77.235	Bulgaria	sviva.idf.il	ET SCAN NMAP -sS window 3072	1
218.246.0.97	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
50.204.188.142	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 3072	1
185.130.5.207	147.237.76.30		himush.idf.il	SERVER-WEBAPP Setup.php access	1
50.204.188.142	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -f -sS	1
125.212.232.146	147.237.72.14	Vietnam	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
37.123.100.26	147.237.77.216	Turkey	dover.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
125.88.182.238	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
37.123.100.26	147.237.0.33	Turkey	idf.il	ET SCAN Potential VNC Scan 5800-5820	1
104.128.144.131	147.237.77.227	Canada	e.hamaz.idf.il	ET SCAN NMAP -sS window 2048	1
98.119.105.221	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 2048	1
98.119.105.221	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -f -sS	1
220.231.195.122	147.237.0.33	China	idf.il	ET SCAN NMAP -sS window 2048	1
80.82.78.67	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
220.231.195.122	147.237.0.33	China	idf.il	ET SCAN NMAP -f -sS	1
77.85.35.211	147.237.77.235	Bulgaria	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
50.204.188.142	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 2048	1
185.130.5.207	147.237.76.30		himush.idf.il	ET WEB_SERVER Muieblackcat scanner	1
125.88.182.238	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
37.123.100.26	147.237.0.200	Turkey	m4u.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
125.88.182.238	147.237.0.200	China	m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.128.144.131	147.237.77.227	Canada	e.hamaz.idf.il	ET SCAN NMAP -f -sS	1
98.119.105.221	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.67	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN Potential SSH Scan	1
220.231.195.122	147.237.0.33	China	idf.il	ET SCAN NMAP -sS window 1024	1

02-10-2016-06:04:02 to 02-10-2016-07:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
184.63.76.22	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	50
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
2.54.151.33	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
77.125.145.131	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
46.19.86.39	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.120.126.36		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.235.64.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.0.80.128	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
87.69.195.133	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.68	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
128.194.131.235	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
82.166.239.53	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.57.215.42	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
2.52.129.48	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.14.40	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.0.81.57	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
31.210.187.142	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
31.210.187.142	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
94.230.86.212	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
54.241.198.78	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
31.210.187.142	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	2
184.105.247.247	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.84	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.186	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.111	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
111.206.36.4	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
192.0.100.166	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
184.105.247.212	United States	147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
165.91.12.152	United States	147.237.72.166	aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
141.212.122.183	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.251	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.111	United States	147.237.0.35	akaws.idf.il	drop		drop	1
141.212.122.188	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
128.194.131.235	United States	147.237.72.156	aman.idf.il	drop	SAM rule	drop	1
79.177.202.180	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	1
184.105.247.215	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.184	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.78	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
93.186.182.35	Netherlands	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
184.105.139.114	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.189	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
208.54.37.144	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.224	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.67	United States	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	1
141.212.122.184	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.99	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

02-10-2016-06:04:02 to 02-10-2016-07:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
141.212.122.177	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/	Block	1
46.105.98.166	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
186.202.150.213	Brazil	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/blog/wp-admin/	Block	1
69.194.230.99	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
157.7.105.198	Japan	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
66.249.78.177	Israel	147.237.76.200	eitan.aka.idf.i	Unknown Parameter tab in www.eitan.aka.idf.il/938-he/eitan.aspx	None	1
207.46.13.192	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
79.176.126.176	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$74 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
2.54.151.33	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.39	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1787-he/dover/aspx	Block	1
66.249.79.75	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training/catalog.asp	Block	1
91.121.93.7	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
37.26.149.249	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
157.55.39.184	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/robots.txt	Block	1
66.249.79.123	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx	Block	1
141.212.122.177	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
46.105.98.166	France	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 46.105.98.166	Block	1
185.130.5.207		147.237.76.30	himush.idf.il	Unauthorized URL Access to 147.237.76.30/scripts/setup.php	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/signals/atar/	Block	1

02-10-2016-06:04:02 to 02-10-2016-07:04:02