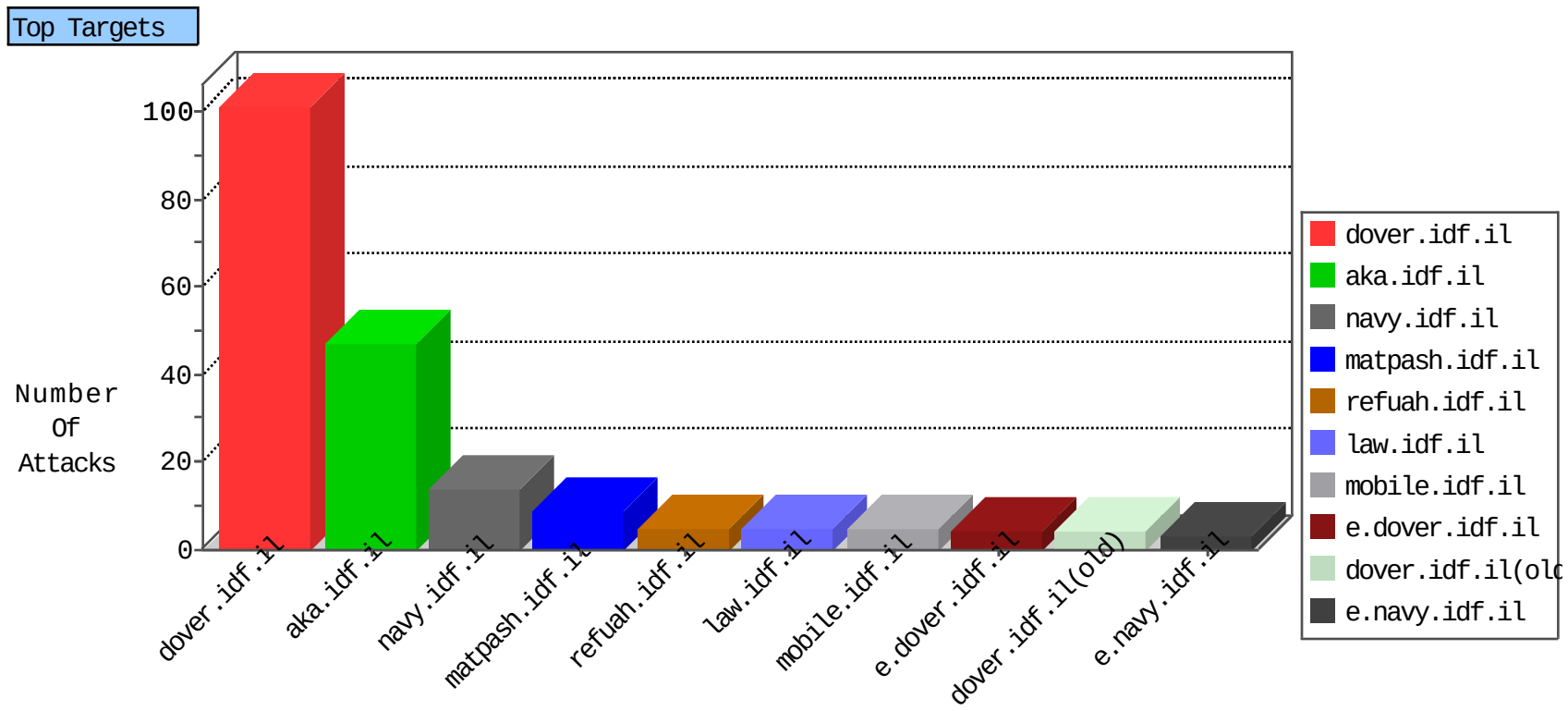
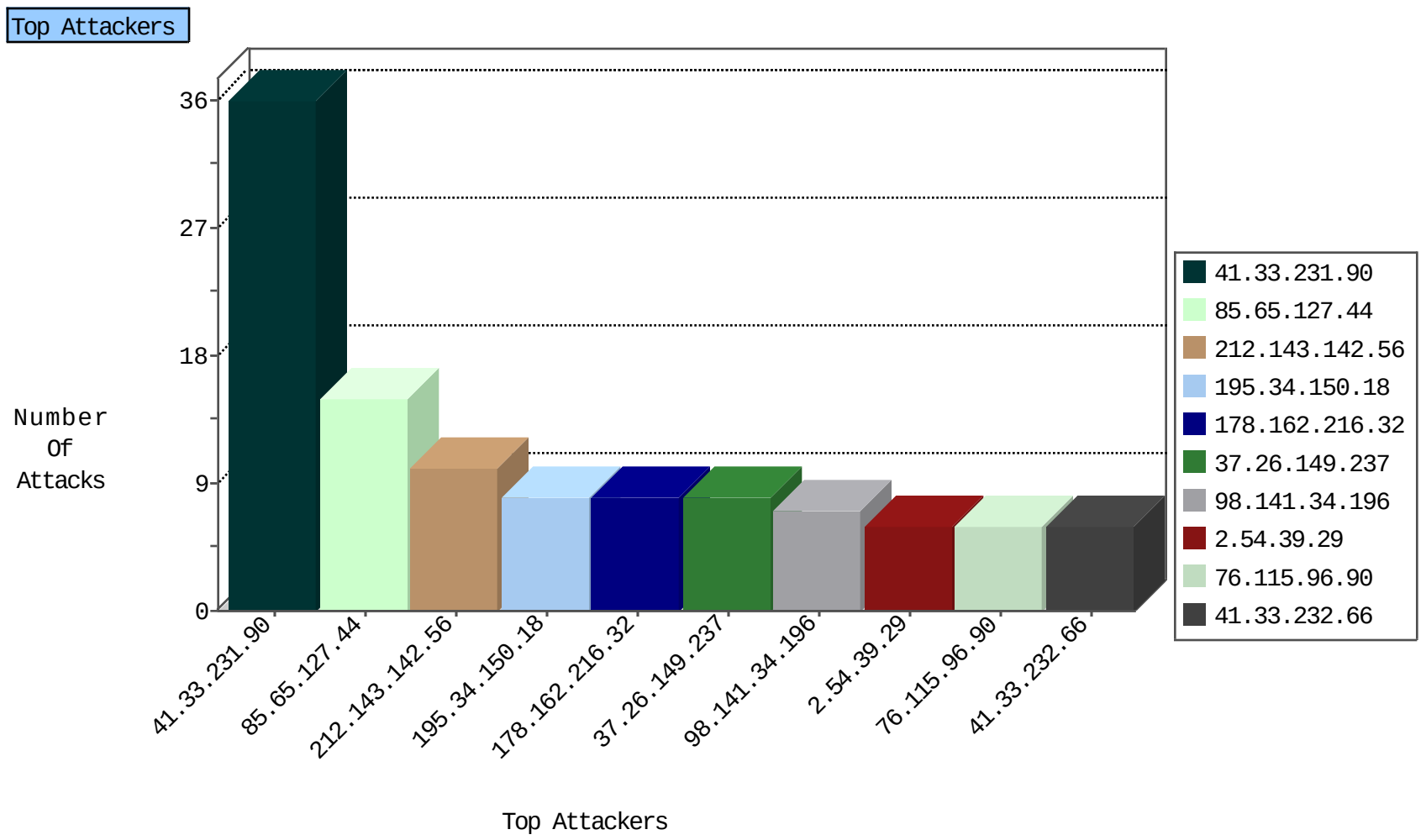
02-03-2016-02:04:02 to 02-03-2016-03:04:02

IDF Under Attack
Daily Report

Top Targets



Top Attackers



02-03-2016-02:04:02 to 02-03-2016-03:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	6
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	4
185.130.5.224		147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
74.91.28.59	United States	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	1

02-03-2016-02:04:02 to 02-03-2016-03:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-03-2016-02:04:02 to 02-03-2016-03:04:02

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
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
185.106.92.137	147.237.77.212		e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
185.106.92.137	147.237.76.148		gqcenter.aka.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
104.155.13.32	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
89.248.174.81	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.248.174.81	147.237.72.14	Netherlands	dover.idf.il(old)	ET SCAN Potential VNC Scan 5900-5920	1
218.246.0.97	147.237.0.34	China	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
50.204.188.142	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 1024	1
210.93.50.130	147.237.72.14	Korea, Republic of	dover.idf.il(old)	ET SCAN NMAP -sS window 2048	1
185.106.92.137	147.237.77.121		e.navy.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
145.255.2.133	147.237.0.16	Russian Federation	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
89.248.174.81	147.237.77.227	Netherlands	e.hamaz.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.248.174.81	147.237.72.156	Netherlands	aman.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
80.82.78.8	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
50.204.188.142	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 2048	1
210.93.50.130	147.237.72.14	Korea, Republic of	dover.idf.il(old)	ET SCAN NMAP -sS window 4096	1
50.204.188.142	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -f -sS	1
210.93.50.130	147.237.72.14	Korea, Republic of	dover.idf.il(old)	ET SCAN NMAP -f -sS	1

02-03-2016-02:04:02 to 02-03-2016-03:04:02

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
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
2.54.39.29	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	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
85.65.127.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
85.65.127.44	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
85.65.127.44	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
98.141.34.196	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
54.147.176.220	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.26.149.237	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
66.249.65.153	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
66.249.78.137	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	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
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
178.162.216.32	Germany	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	3
130.193.50.6	Russian Federation	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
76.115.96.90	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
79.178.5.78	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
42.62.74.78	China	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
91.200.12.106	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
75.149.194.90	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
37.26.149.237	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
37.26.149.237	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
178.162.216.32	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.196	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
37.142.64.38	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.179	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
98.141.34.196	United States	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
198.20.69.74	United States	147.237.76.44	e.refuah.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
79.181.53.254	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.191	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
85.130.235.1	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
178.162.216.32	Germany	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
68.180.231.40	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
149.88.81.165	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
37.245.163.41	United Arab Emirates	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.189	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
98.141.34.196	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
209.126.116.147	United States	147.237.0.33	idf.il	drop	SAM rule	drop	1
79.181.53.254	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
178.162.216.32	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.194	United States	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
137.116.71.170	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.3.147.249	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
149.88.81.165	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.189	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
107.203.254.103	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
209.126.116.147	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
178.162.216.32	Germany	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.195	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

02-03-2016-02:04:02 to 02-03-2016-03:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
76.115.96.90	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
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
104.131.245.20	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 104.131.245.20	Block	2
157.55.39.192	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/sachar	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-ar/dover.aspx	Block	1
8.37.70.126	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/&usg=alkjrhipim6mpmqfscwf3ppbfriubeanja	Block	1
110.77.204.89	Thailand	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.25	Block	1
8.37.71.56	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1393-en/dover.aspx&usg=alkjrhgzr4o3yugctdog1n3nt-xpy8oejq	Block	1
121.54.32.157	Philippines	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery.plugins/jquery.scrollfollow.js	Block	1
61.135.190.197	China	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
121.54.32.157	Philippines	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
66.249.78.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/ui/i18n/jquery-ui-i18n.js	Block	1
66.249.65.115	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/scroller/jquery.jcarousel.js	Block	1
157.55.39.57	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery.plugins/jquery.charts.js	Block	1
110.77.204.89	Thailand	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
66.249.65.118	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery/jquery-ui.js	Block	1

02-03-2016-02:04:02 to 02-03-2016-03:04:02