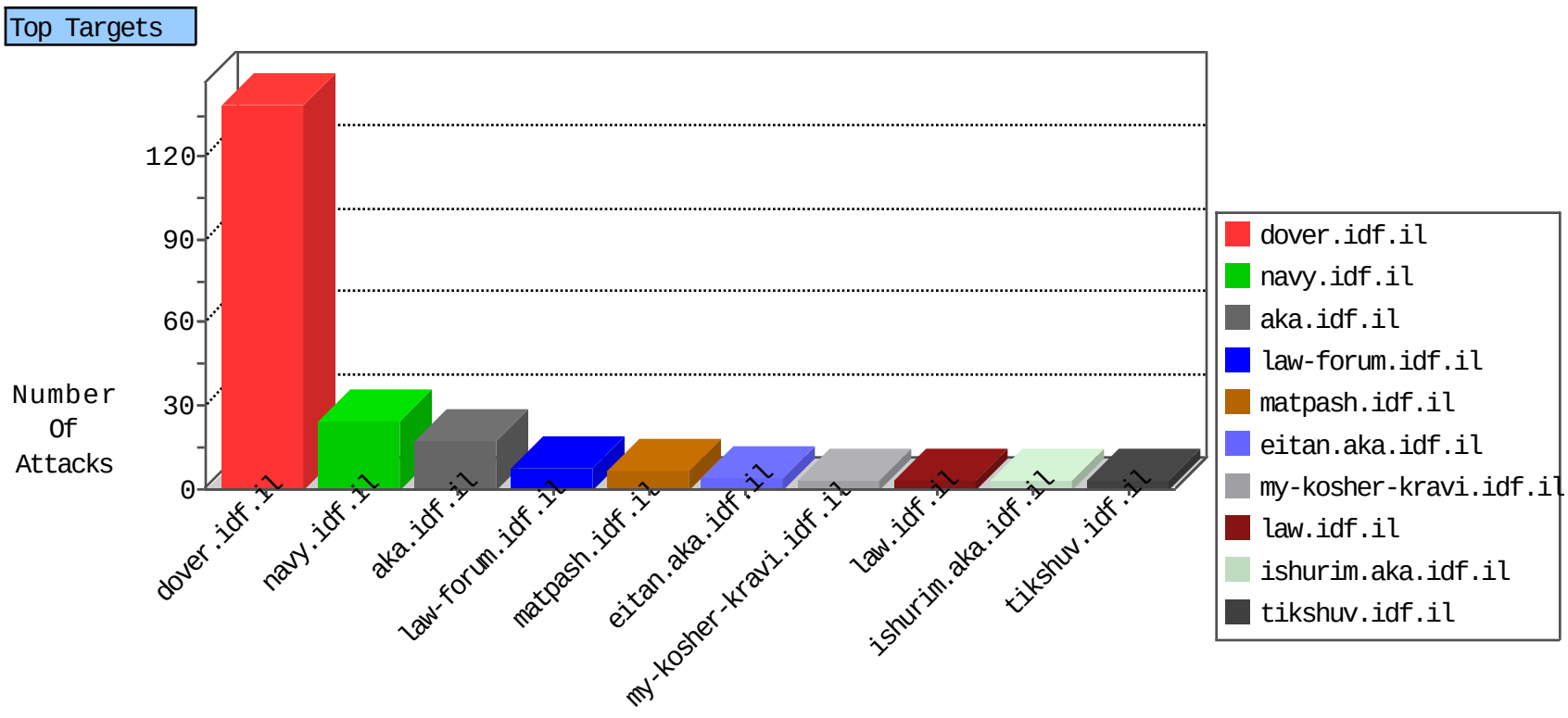
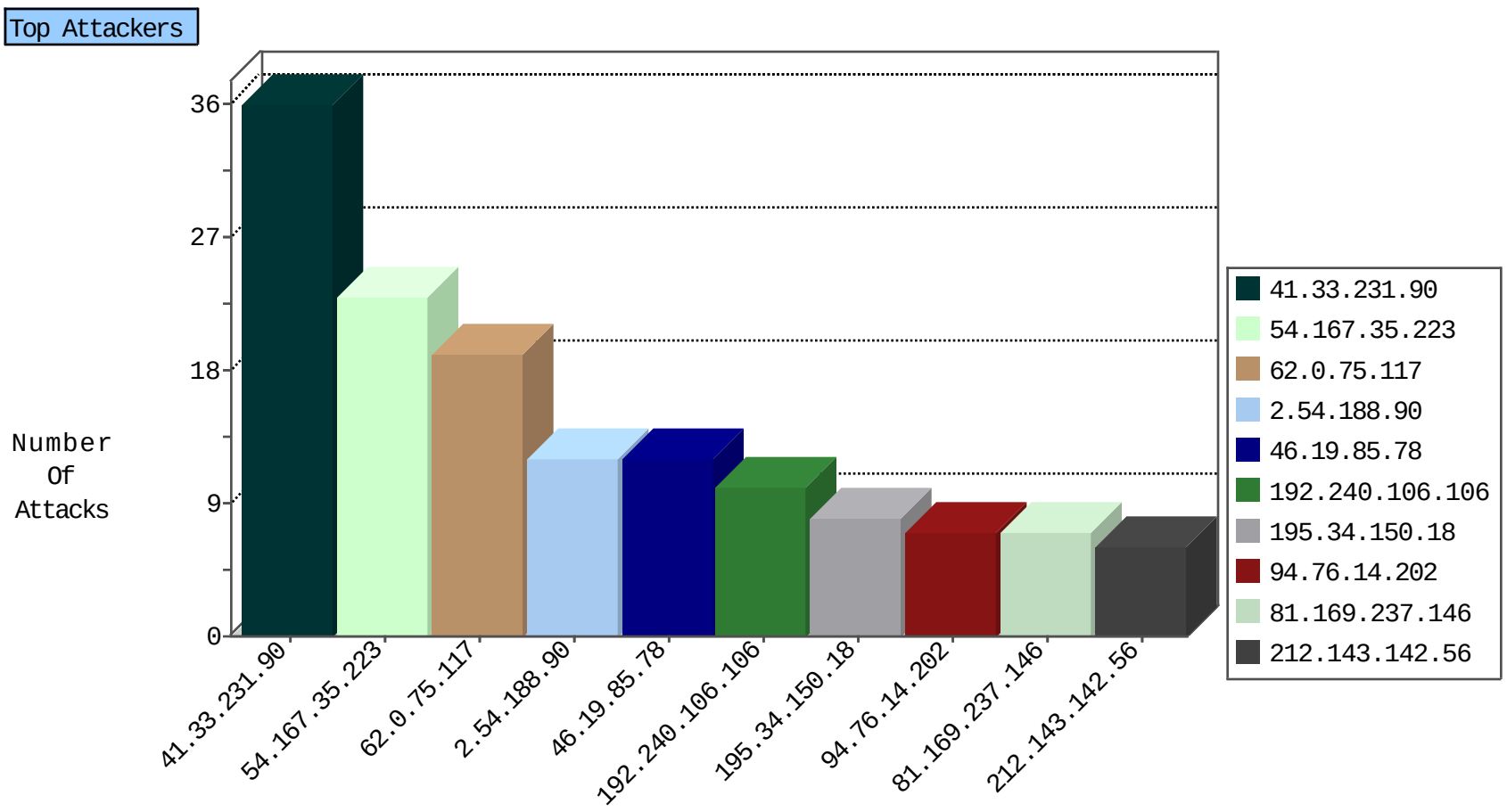
01-28-2016-04:04:01 to 01-28-2016-05:04:01

IDF Under Attack
Daily Report





01-28-2016-04:04:01 to 01-28-2016-05:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
120.25.86.171	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1
23.239.64.15	United States	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
167.114.92.57	Canada	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
71.6.167.142	United States	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
115.230.124.164	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1

01-28-2016-04:04:01 to 01-28-2016-05:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
94.76.10.91	Bahrain	147.237.77.19	law-forum.idf.il	C107: DDOS-Spoofed HTTP Packets	Block	1
192.240.106.106	United States	147.237.76.86	navy.idf.il	0543: HTTP: php.cgi Access	Block	1
192.240.106.106	United States	147.237.77.216	dover.idf.il	0543: HTTP: php.cgi Access	Block	1

01-28-2016-04:04:01 to 01-28-2016-05:04:01

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
66.249.78.97	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.2	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
218.246.0.97	147.237.72.166	China	aka.idf.il	ET SCAN NMAP -sS window 1024	1
185.56.82.22	147.237.77.216	Netherlands	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
185.56.82.22	147.237.0.33	Netherlands	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
168.62.238.153	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
95.183.51.251	147.237.0.15	Switzerland	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
94.76.11.132	147.237.77.74	Bahrain	law.idf.il	ET SCAN NMAP -sS window 1024	1
185.56.82.22	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.61.109.189	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
113.118.112.211	147.237.76.30	China	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
94.76.11.132	147.237.77.121	Bahrain	e.navy.idf.il	ET SCAN Potential SSH Scan	1
94.76.10.91	147.237.76.86	Bahrain	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

01-28-2016-04:04:01 to 01-28-2016-05:04:01

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
54.167.35.223	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	23
62.0.75.117	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
94.76.14.202	Bahrain	147.237.77.19	law-forum.idf.il	drop	SAM rule	drop	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.78	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
171.161.160.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.78	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
54.241.198.78	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
75.181.170.42	United States	147.237.77.216	dover.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
2.54.188.90	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
81.169.237.146	Germany	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	3
130.193.51.2	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.169.237.146	Germany	147.237.77.61	e.cogat.idf.il	drop	SAM rule	drop	2
2.54.188.90	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
2.54.188.90	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
85.93.91.84	Germany	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
66.249.78.239	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
198.1.101.123	United States	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
2.54.188.90	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	2
41.202.84.86	Cote D'Ivoire	147.237.77.216	dover.idf.il	Header Rejection	header rejection pattern found in request	monitor	2
147.235.8.62	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
147.235.8.62	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
208.115.111.73	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
5.144.131.170	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.95	United States	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
104.130.78.65	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
186.247.213.165	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
149.210.158.71	Netherlands	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
208.115.111.73	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
184.105.139.100	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
115.230.124.164	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
77.77.76.3	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
216.218.206.82	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
157.55.39.43	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
184.105.139.110	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
81.169.237.146	Germany	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	1
52.49.79.6	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
74.82.47.7	United States	147.237.0.33	idf.il	drop		drop	1
212.76.127.44	Israel	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
184.105.247.216	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
81.169.237.146	Germany	147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	1
201.8.232.32	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.126.252.12	Romania	147.237.0.33	idf.il	drop		drop	1
99.238.52.167	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
74.82.47.39	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

01-28-2016-04:04:01 to 01-28-2016-05:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.240.106.106	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.240.106.106	Block	3
192.240.106.106	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 192.240.106.106	Block	3
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
106.51.185.146	India	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.png	Block	2
107.178.194.79	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22461-he/dover.aspx.	Block	1
2.54.188.90	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 2.54.188.90 (Open Mode)	None	1
204.13.201.138	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
187.189.195.40	Mexico	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/a2billing/customer/iridium_threed.php	Block	1
192.240.106.106	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/cgi-bin/php	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
2.54.188.90	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
187.189.195.40	Mexico	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/a2billing/customer/iridium_threed.php	Block	1
66.249.78.201	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
193.109.199.36	United Kingdom	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
178.255.215.87	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
41.202.84.86	Cote D'Ivoire	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1
68.180.229.239	United States	147.237.72.166	aka.idf.il	Unknown Parameter siteid in www.aka.idf.il/sites/home/default.asp	None	1
193.109.199.36	United Kingdom	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
184.105.139.67	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
41.202.84.86	Cote D'Ivoire	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
192.240.106.106	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/cgi-bin/php	Block	1
204.13.201.137	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
184.105.139.70	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
66.249.78.82	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1

01-28-2016-04:04:01 to 01-28-2016-05:04:01