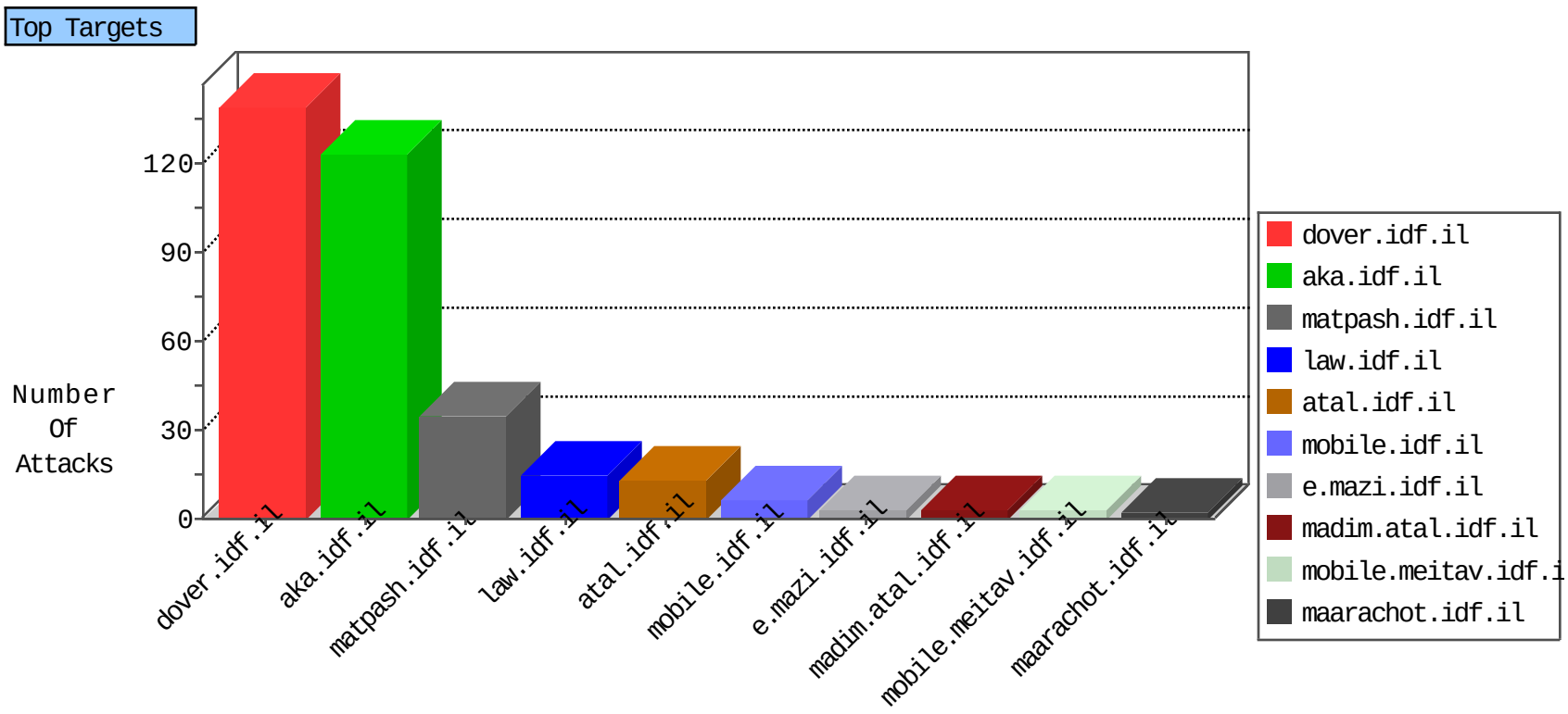
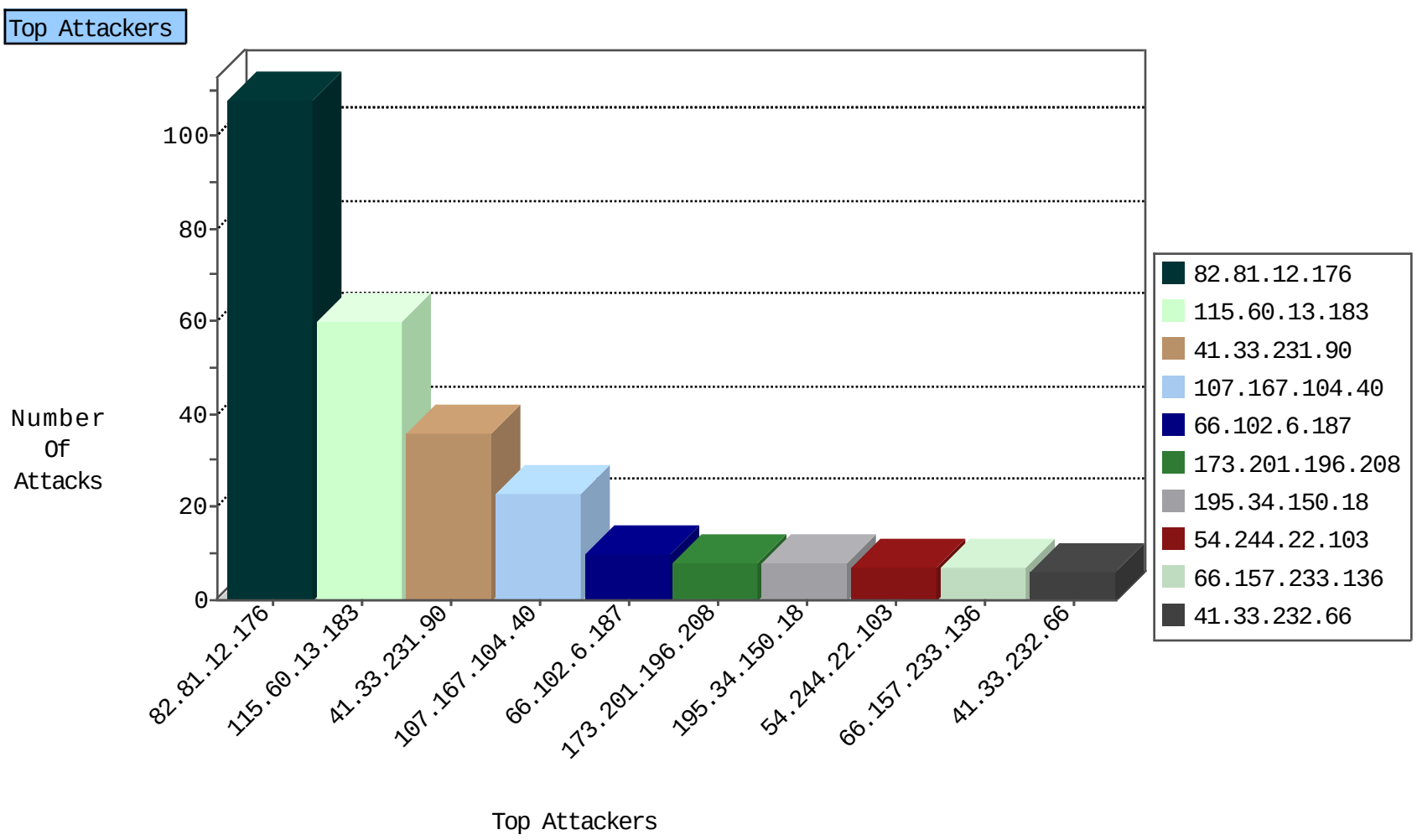
01-29-2016-04:04:04 to 01-29-2016-05:04:04

IDF Under Attack Daily Report





01-29-2016-04:04:04 to 01-29-2016-05:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	108
204.42.253.2	United States	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
52.53.222.9	United States	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1

01-29-2016-04:04:04 to 01-29-2016-05:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.165.15.205	France	147.237.72.166	aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1

01-29-2016-04:04:04 to 01-29-2016-05:04:04

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
66.249.78.9	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
118.173.138.55	147.237.76.30	Thailand	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
109.235.254.181	147.237.77.179	Turkey	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
94.76.11.255	147.237.72.217	Bahrain	e.idf.il	ET SCAN NMAP -sS window 1024	1
46.45.137.67	147.237.77.234	Turkey	halag.idf.il	ET SCAN NMAP -sS window 1024	1
46.45.137.67	147.237.77.74	Turkey	law.idf.il	ET SCAN NMAP -sS window 1024	1
109.235.254.181	147.237.77.179	Turkey	e.mazi.idf.il	ET SCAN NMAP -sS window 2048	1
109.235.254.181	147.237.77.179	Turkey	e.mazi.idf.il	ET SCAN NMAP -f -sS	1
46.45.137.67	147.237.77.212	Turkey	e.dover.idf.i	ET SCAN NMAP -sS window 1024	1

01-29-2016-04:04:04 to 01-29-2016-05:04:04

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
107.167.104.40	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	23
66.102.6.187	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	10
173.201.196.208	United States	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
190.113.147.22	Argentina	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
54.244.22.103	United States	147.237.77.176	matpash.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
5.102.216.11	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.68.62.247	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	3
46.121.123.18	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
157.55.39.214	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
91.200.12.7	Ukraine	147.237.77.74	law.idf.il	drop	SAM rule	drop	2
52.33.66.29	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	2
91.200.12.7	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
207.46.13.49	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
66.157.233.136	United States	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
66.157.233.136	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
37.142.138.16	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.219	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
108.61.166.139	United States	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
66.157.233.136	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
198.20.69.74	United States	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
60.225.115.91	Australia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
216.218.206.80	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.236	United States	147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
115.230.124.164	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
66.157.233.136	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
207.46.13.24	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
216.218.206.106	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.100.85.191		147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
130.193.50.33	Russian Federation	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
66.157.233.136	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
54.193.212.129	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
184.105.139.104	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	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
46.19.85.116	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.8.183.20	Russian Federation	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
74.82.47.52	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
207.46.13.49	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
31.210.188.10	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.247.216	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.86.188	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

01-29-2016-04:04:04 to 01-29-2016-05:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
115.60.13.183	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 115.60.13.183	Block	25
115.60.13.183	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 115.60.13.183	Block	24
115.60.13.183	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	5
115.60.13.183	China	147.237.77.176	matpash.idf.il	PHP Attempt	Block	5
77.125.123.77	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
83.250.199.52	Sweden	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/english/pages/default.aspx	Block	1
207.46.13.10	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training/course_photos.asp	Block	1
108.61.166.139	United States	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
115.60.13.183	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-19117-en/contact.php	Block	1
94.159.209.178	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 94.159.209.178 (sigalgs DoS Attack)	None	1
207.46.13.68	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17607-en/dover.aspx-title=over	Block	1
66.249.69.92	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	1
94.159.209.178	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.78.96	Israel	147.237.77.74	law.idf.il	Multiple Illegal Parameter Encoding from 66.249.78.96	None	1
198.20.69.74	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22638-he/dover.aspx.	Block	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
107.178.194.87	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22461-he/dover.aspx.	Block	1

01-29-2016-04:04:04 to 01-29-2016-05:04:04