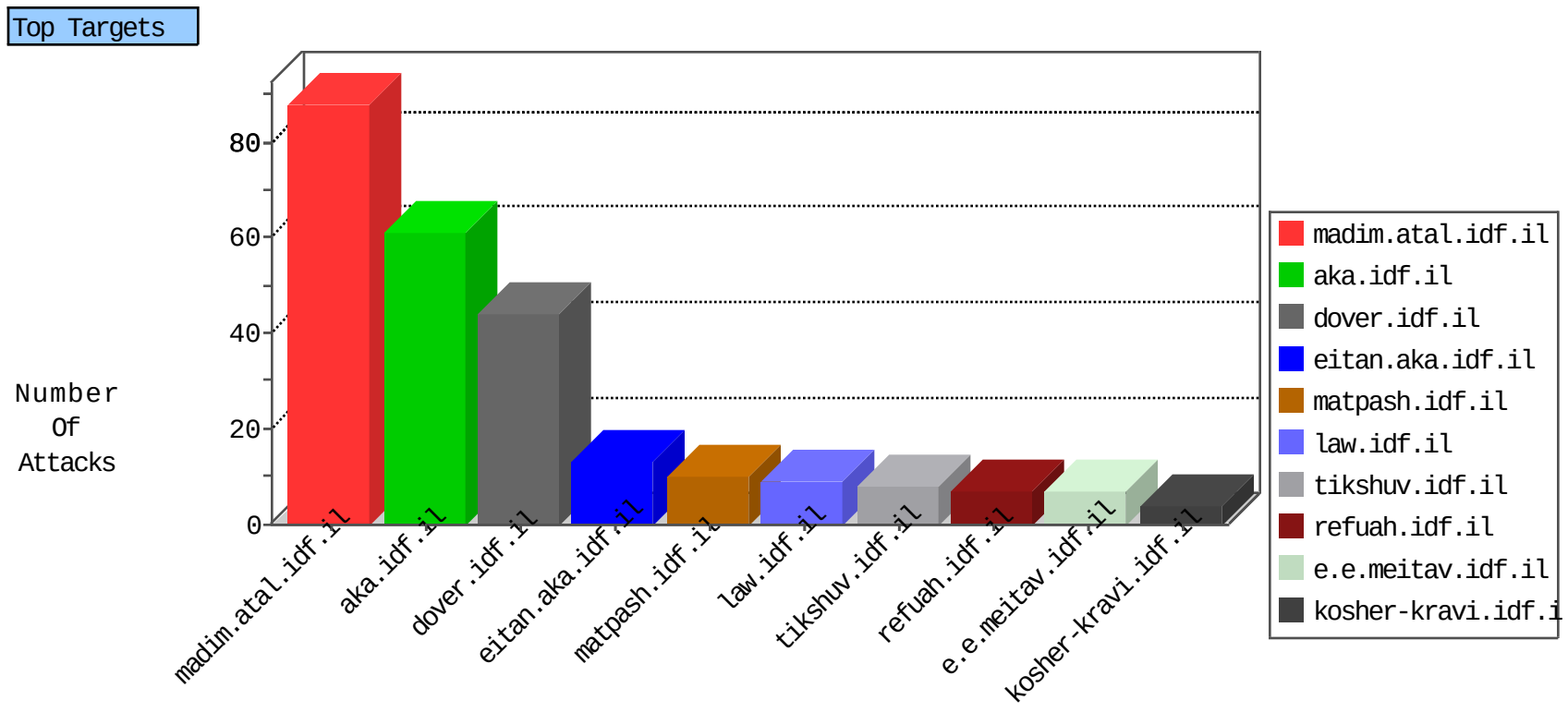
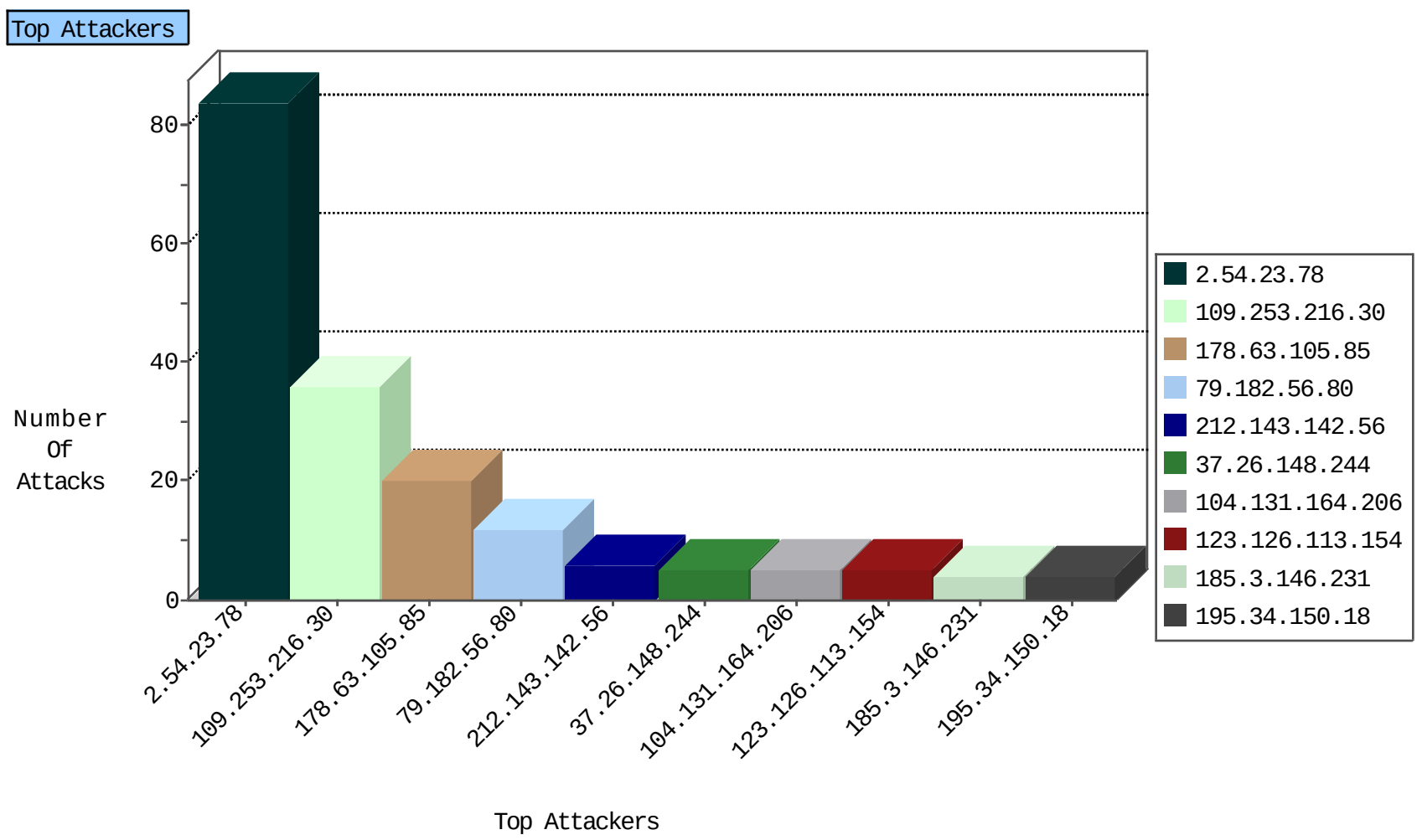
03-07-2016-06:04:04 to 03-07-2016-07:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-07-2016-06:04:04 to 03-07-2016-07:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.103.252.5		147.237.0.15	kosher-kravi.idf.il	Block_Udp_All_Nets	drop	4
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
184.105.139.72	United States	147.237.77.74	law.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1		147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.88	United States	147.237.0.200	m4u.idf.il	Block_Ntp_All_Net	drop	1
185.56.28.67	Netherlands	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
220.134.56.63	Taiwan	147.237.0.16	my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
104.245.97.224		147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
185.56.28.67	Netherlands	147.237.77.178	e.matpash.idf.il	Block_Ntp_All_Net	drop	1

03-07-2016-06:04:04 to 03-07-2016-07:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.154	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
46.19.86.196	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-07-2016-06:04:04 to 03-07-2016-07:04:04

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
64.233.172.169	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
218.246.0.97	147.237.76.200	China	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
123.203.22.142	147.237.8.28	Hong Kong	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
115.85.192.40	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.76.196	China	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
120.26.115.52	147.237.76.177	China	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
115.85.192.40	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
61.163.231.229	147.237.77.61	China	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1

03-07-2016-06:04:04 to 03-07-2016-07:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.253.216.30	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
79.182.56.80	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
178.63.105.85	Germany	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	5
185.3.146.231	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
178.63.105.85	Germany	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	3
2.54.21.171	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.63.105.85	Germany	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	3
109.65.33.137	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.75	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.63.105.85	Germany	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	3
178.63.105.85	Germany	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	2
46.19.85.254	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
46.31.103.31	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.26.148.244	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
46.19.85.254	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
208.115.113.89	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
84.108.61.45	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
178.63.105.85	Germany	147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	2
37.26.148.244	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
74.82.47.48	United States	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.215	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
208.115.113.88	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.26.148.244	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
84.110.145.71	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.7	United States	147.237.0.33	idf.il	drop		drop	1
216.218.206.88	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.56	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
84.229.243.115	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
74.82.47.24	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.96	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
5.144.131.170	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
123.126.113.80	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
46.120.248.201	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
37.26.149.223	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
74.82.47.40	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.106	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.43	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
195.62.53.168	Russian Federation	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	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
178.63.105.85	Germany	147.237.0.16	my-kosher-kravi.idf.il	drop	SAM rule	drop	1
46.120.248.201	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
37.26.149.223	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
109.186.162.201	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
74.82.47.44	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.86.157	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
198.20.69.74	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
178.63.105.85	Germany	147.237.0.19	madim.atal.idf.il	drop	SAM rule	drop	1

03-07-2016-06:04:04 to 03-07-2016-07:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.23.78	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	84
17.138.56.26	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.138.56.26	Block	4
104.131.164.206	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 104.131.164.206	Block	4
2.52.52.183	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
107.197.57.146	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	2
107.197.57.146	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	2
104.131.164.206	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22927-ar/idfgdover.aspx	Block	1
66.249.69.85	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/dynamic_map/dynamic_map.aspx	Block	1
187.181.215.250	Brazil	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
77.119.129.31	Austria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
46.19.86.229	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
196.221.237.247	Egypt	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on www.refua.atal.idf.il/xmlrpc.php	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-he/dover.aspx	Block	1
187.181.215.250	Brazil	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	1
94.230.93.56	Israel	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
66.249.64.124	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
196.221.237.247	Egypt	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
68.180.228.175	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/228-he/faq.aspx	Block	1
188.120.148.64	Israel	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
94.230.93.56	Israel	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	1
66.249.64.233	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	1
196.221.237.247	Egypt	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
146.199.3.182	United Kingdom	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1934-he/cogat.aspx	Block	1
41.237.51.59	Egypt	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
188.120.148.64	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1
66.249.66.33	United States	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
199.30.24.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
146.199.3.182	United Kingdom	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	1
77.119.129.31	Austria	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
41.237.51.59	Egypt	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	1
196.221.237.247	Egypt	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1

03-07-2016-06:04:04 to 03-07-2016-07:04:04