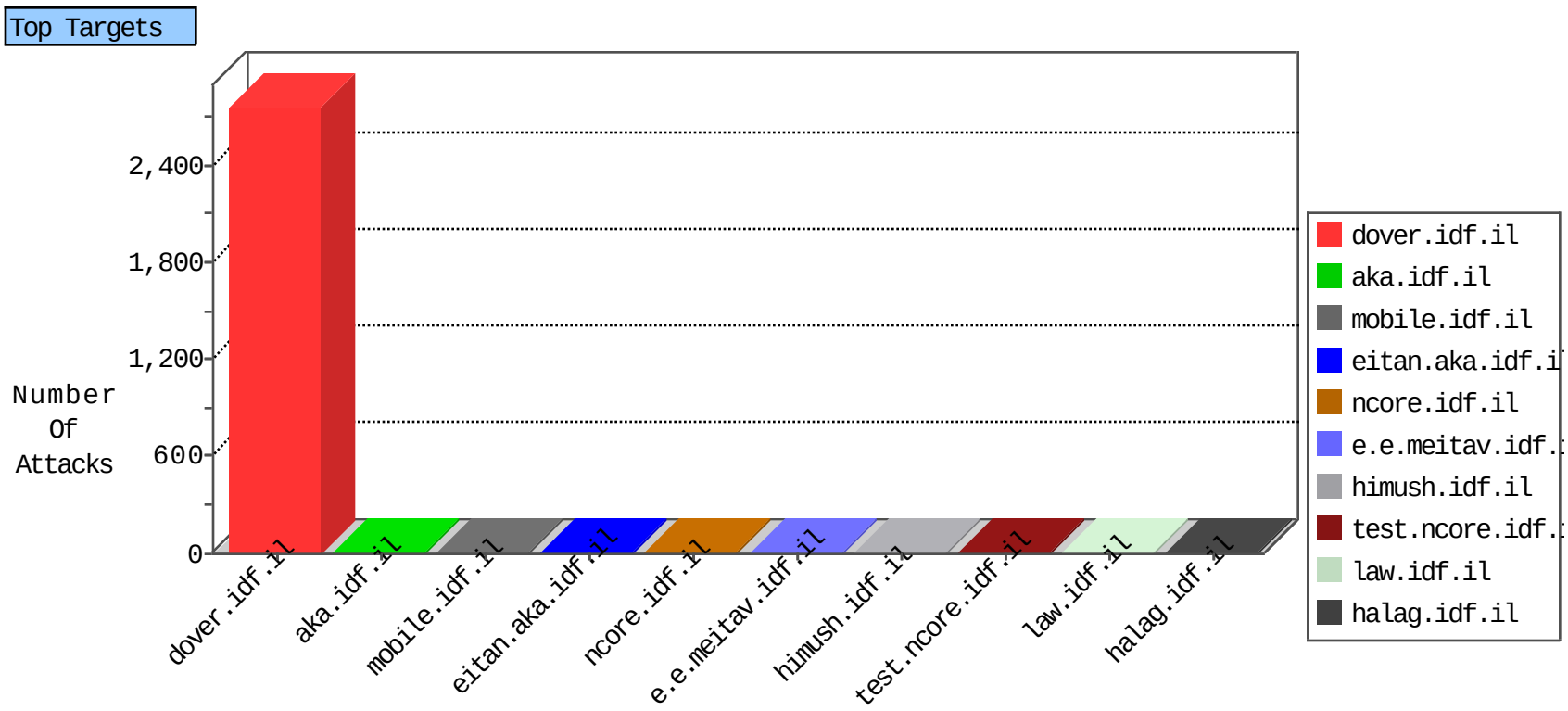
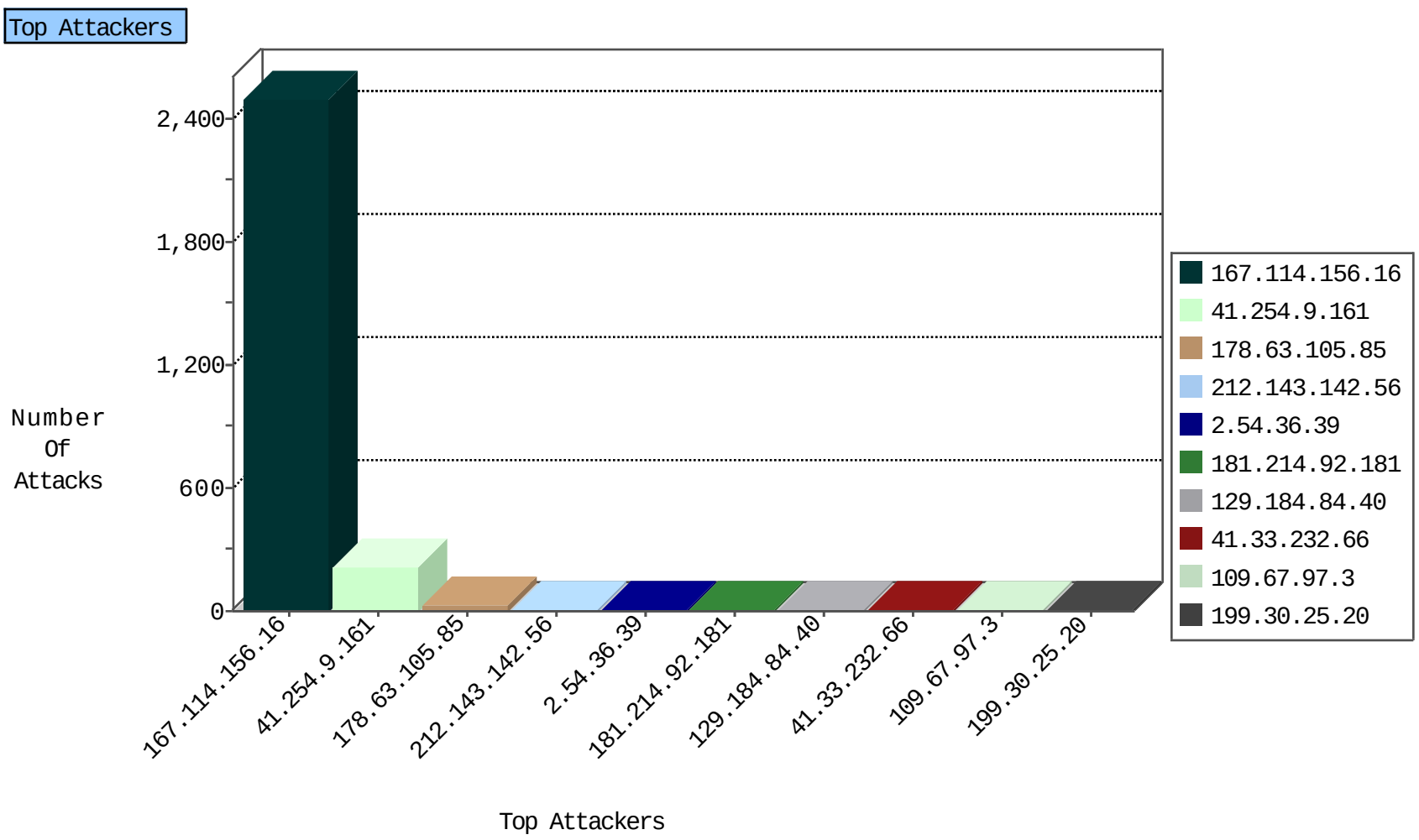
03-14-2016-04:04:07 to 03-14-2016-05:04:07

IDF Under Attack
Daily Report

Top Targets



Top Attackers



03-14-2016-04:04:07 to 03-14-2016-05:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.254.9.161	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	4322
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3380
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
184.105.139.92	United States	147.237.0.200	m4u.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.124	United States	147.237.77.233	atal.idf.il	Block_Ntp_All_Net	drop	1

03-14-2016-04:04:07 to 03-14-2016-05:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.64.185	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
24.235.56.194	Canada	147.237.77.74	law.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1

03-14-2016-04:04:07 to 03-14-2016-05:04:07

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	3
23.96.109.87	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 4096	1
181.214.92.181	147.237.76.197	Chile	e.himush.idf.il	ET SCAN Potential SSH Scan	1
181.214.92.181	147.237.0.17	Chile	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
104.44.133.108	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 2048	1
104.41.144.192	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 4096	1
61.220.102.6	147.237.76.42	Taiwan	refuah.idf.il	ET SCAN NMAP -sS window 2048	1
61.220.102.6	147.237.76.42	Taiwan	refuah.idf.il	ET SCAN NMAP -f -sS	1
203.115.196.137	147.237.77.234	Malaysia	halag.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1
23.125.172.41	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 4096	1
181.214.92.181	147.237.76.198	Chile	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
181.214.92.181	147.237.76.30	Chile	himush.idf.il	ET SCAN Potential SSH Scan	1
104.44.133.108	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 4096	1
104.44.133.108	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -f -sS	1
80.82.64.117	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
61.220.102.6	147.237.76.42	Taiwan	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
203.115.196.137	147.237.77.234	Malaysia	halag.idf.il	ET SCAN NMAP -sS window 3072	1
59.45.79.117	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.98	147.237.77.176	United States	matpash.idf.il	ET DROP Dshield Block Listed Source	1
59.45.79.117	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
181.214.92.181	147.237.76.201	Chile	e.atal.idf.il	ET SCAN Potential SSH Scan	1

03-14-2016-04:04:07 to 03-14-2016-05:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	15
178.63.105.85	Germany	147.237.76.177	ncore.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	7
2.54.36.39	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
178.63.105.85	Germany	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	5
199.30.25.125	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
199.30.25.20	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
176.13.3.84	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.63.105.85	Germany	147.237.76.176	test.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	3
109.67.97.3	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.196.242	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
217.69.133.246	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
178.63.105.85	Germany	147.237.77.61	e.cogat.idf.il	drop	SAM rule	drop	2
37.46.38.108	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
141.212.122.167	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
64.46.23.242	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
184.105.247.220	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
157.55.39.193	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.73	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
2.52.13.39	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.115	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.169	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
220.181.108.147	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.42	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.232	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.73	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
207.46.13.87	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.247.207	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
178.63.105.85	Germany	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	1
141.212.122.170	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
195.62.53.168	Russian Federation	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.74	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.207	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
178.63.105.85	Germany	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
141.212.122.170	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
184.105.139.80	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.166	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
216.218.206.106	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.212	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.171	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.72	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.99	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

03-14-2016-04:04:07 to 03-14-2016-05:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
129.184.84.40	France	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx	Block	4
157.55.39.193	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-he	Block	1
66.249.64.137	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
207.46.13.160	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
36.84.0.88	Indonesia	147.237.77.216	dover.idf.il	Parameter Type Violation &l in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
157.55.39.193	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.198	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1879	Block	1
129.184.84.40	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
37.26.147.231	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
183.206.175.39	China	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/editorold/editor/	Block	1
66.249.75.218	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
141.212.122.64	United States	147.237.76.30	himush.idf.il	Unauthorized URL Access to /x	Block	1
45.216.203.36	Uruguay	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
183.206.175.39	China	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 183.206.175.39	Block	1
73.172.146.3	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
157.55.39.70	United States	147.237.72.166	aka.idf.il	Unknown Parameter 136cd360 in www.aka.idf.il/main/home/default.aspx	None	1
45.216.203.36	Uruguay	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
197.231.221.211	Liberia	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
109.67.97.3	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/igyus	Block	1

03-14-2016-04:04:07 to 03-14-2016-05:04:07