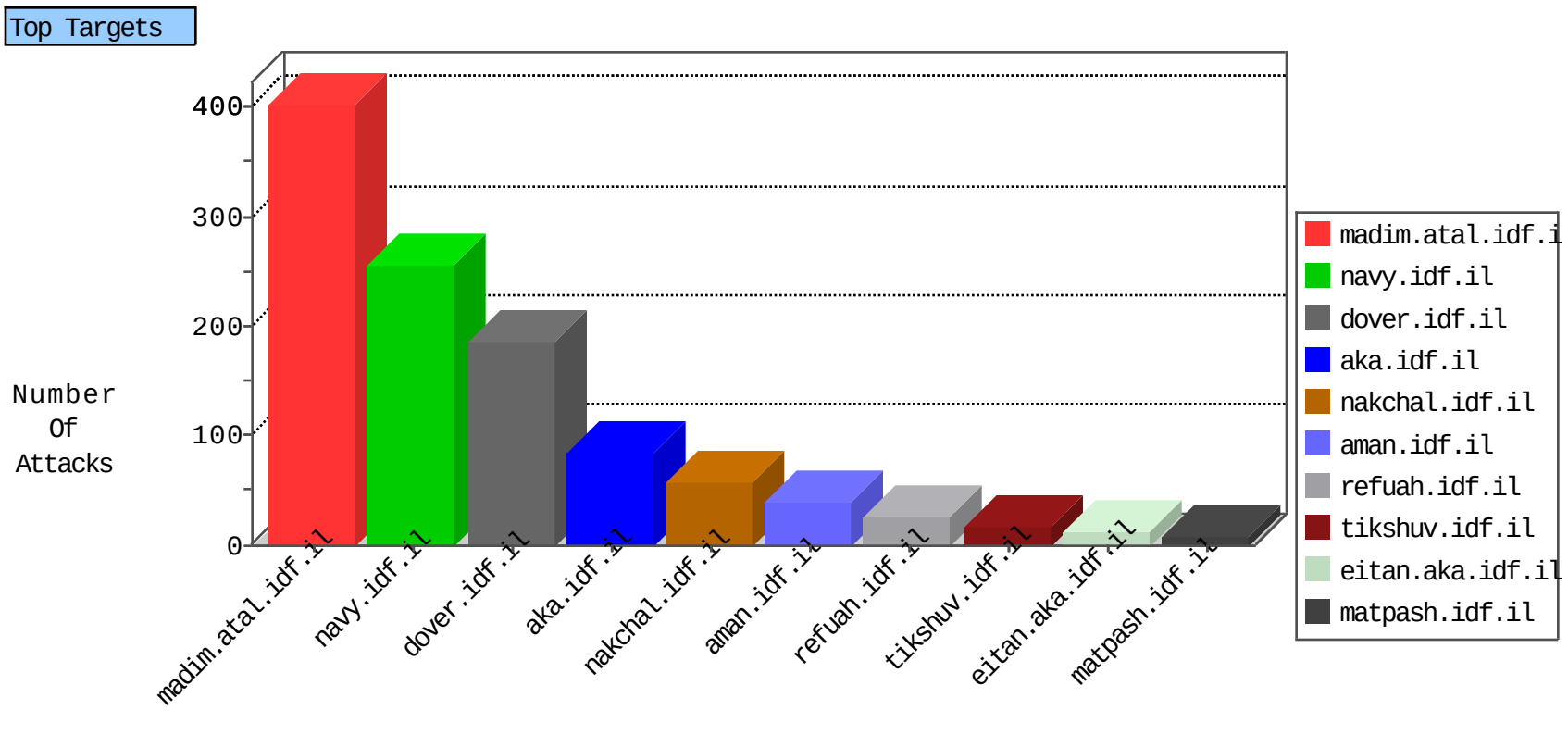
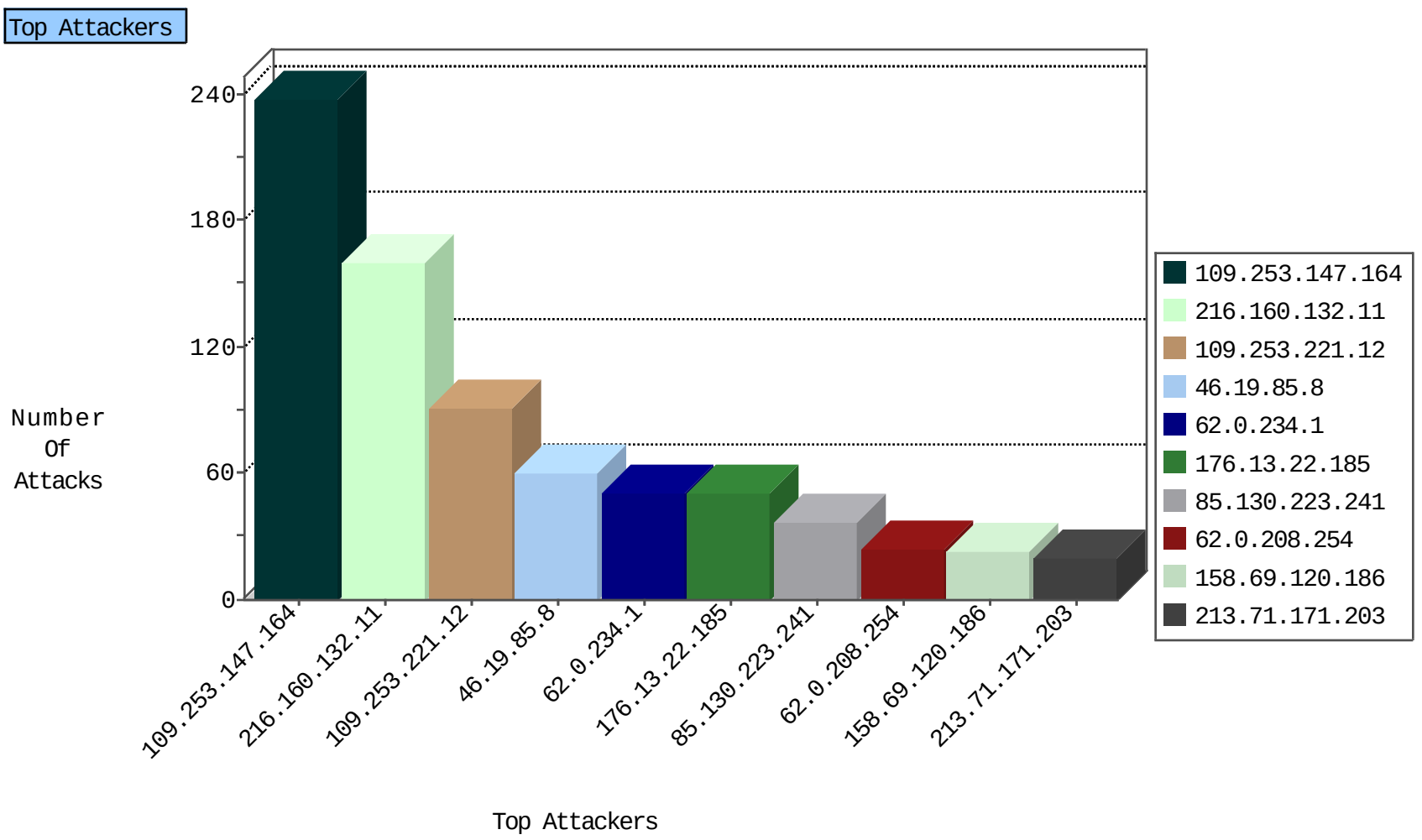
09-22-2016-08:04:02 to 09-22-2016-09:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-22-2016-08:04:02 to 09-22-2016-09:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
191.96.249.34	Chile	147.237.76.198	e.yohalan.idf.il	Black List	drop	1
45.32.196.8	United States	147.237.76.38	e.e.meitav.idf.il	Black List	drop	1
191.96.249.37	Chile	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1
45.32.205.187	Netherlands	147.237.76.38	e.e.meitav.idf.il	Black List	drop	1
2.53.49.66	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
185.103.198.32	Turkey	147.237.0.19	madim.atal.idf.il	Frk_Under_Attack_Con_Tcp	drop	1
5.152.207.142	United Kingdom	147.237.76.44	e.refuah.idf.il	Black List	drop	1

09-22-2016-08:04:02 to 09-22-2016-09:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
69.197.163.195	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-22-2016-08:04:02 to 09-22-2016-09:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
185.103.198.32	147.237.76.86	Turkey	navy.idf.il	ET SCAN Potential SSH Scan	1
163.172.134.160	147.237.77.121	United Kingdom	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
109.66.122.50	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.155	147.237.76.176	Ukraine	test.ncore.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
79.177.99.21	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.219.134.3	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.24.228.20	147.237.76.201	United Kingdom	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
212.235.47.253	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.46.157	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
194.56.215.218	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.103.198.32	147.237.76.39	Turkey	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
163.172.134.160	147.237.77.19	United Kingdom	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
106.38.241.106	147.237.72.166	China	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
84.108.88.175	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.125.9.199	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.154.81.38	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.156.240	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
199.203.215.1	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-22-2016-08:04:02 to 09-22-2016-09:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
216.160.132.11	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	160
62.0.234.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
62.0.208.254	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	24
213.71.171.203	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
46.19.85.8	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	19
46.19.85.8	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
62.0.234.1	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	15
199.203.215.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
82.166.200.204	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	12
156.109.18.122	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.8	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
46.19.85.8	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
62.0.234.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
189.172.49.231	Mexico	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
85.130.223.241	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
85.130.223.241	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
37.26.149.234	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
85.130.223.241	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.245	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.66.122.227	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.29	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.67	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
80.246.136.182	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.86.67	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
85.130.223.241	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
158.69.120.182	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
158.69.120.186	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.85.239	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
158.69.120.186	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	5
158.69.120.186	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	5
158.69.120.186	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
77.124.33.133	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
158.69.120.186	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
85.130.223.241	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
158.69.120.182	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	4
46.19.86.70	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
158.69.120.182	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	4
85.130.223.241	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	4
62.0.230.1	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	3
37.26.147.144	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.85.49	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
24.4.50.221	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	3
46.19.86.21	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
158.69.120.182	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
109.253.139.119	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
89.139.79.182	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
24.4.50.221	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
46.19.85.51	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
24.4.50.221	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
2.53.186.133	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

09-22-2016-08:04:02 to 09-22-2016-09:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.147.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	238
109.253.221.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	91
176.13.22.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	50
37.26.149.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.230.207	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.138.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.239.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.200.72	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.139.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.137.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.109.113.219	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 84.109.113.219	Block	2
180.97.106.161	China	147.237.72.167	ishurim.aka.idf.il	Illegal Byte Code Character in Method	Block	1
66.249.66.131	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/robots.txt	Block	1
207.46.13.176	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/540-he/patzar/aspx	Block	1
37.26.149.171	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	1
180.97.106.161	China	147.237.72.167	ishurim.aka.idf.il	NULL Character in Method	Block	1
66.249.76.18	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/apple-app-site-association	Block	1
84.108.125.230	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
46.19.86.145	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
180.97.106.161	China	147.237.76.31	nakchal.idf.il	Illegal Byte Code Character in Method	Block	1
109.253.198.127	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.76.54	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 66.249.76.54	None	1
46.19.86.221	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
180.97.106.161	China	147.237.76.31	nakchal.idf.il	NULL Character in Method	Block	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1399-en/dover.aspx	Block	1
2.53.186.133	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchildsubcategories/1423	Block	1
176.61.143.88	United States	147.237.72.167	ishurim.aka.idf.il	PHP Attempt	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.102.9.24	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
183.232.175.2	China	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/	Block	1
77.138.200.57	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	1

09-22-2016-08:04:02 to 09-22-2016-09:04:02