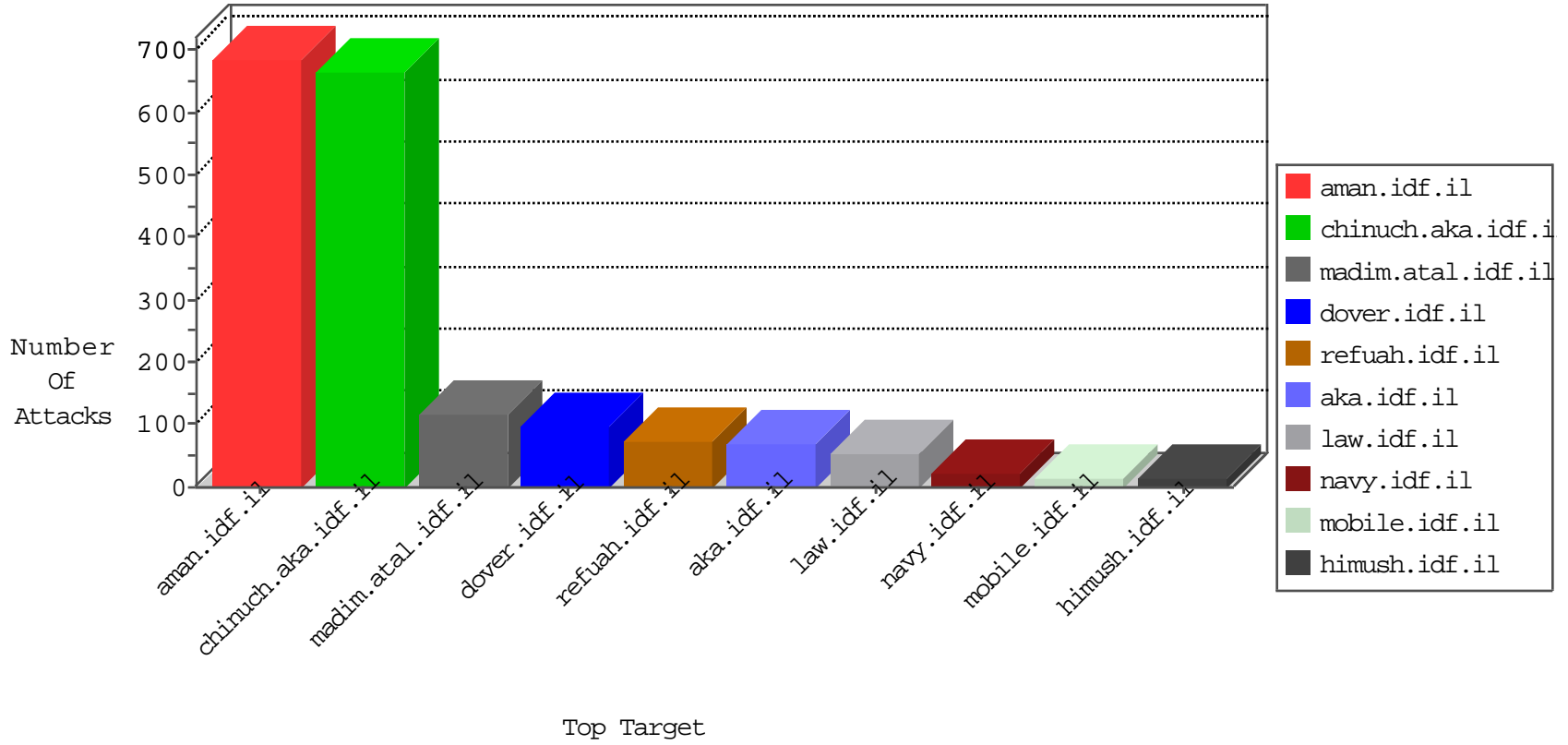


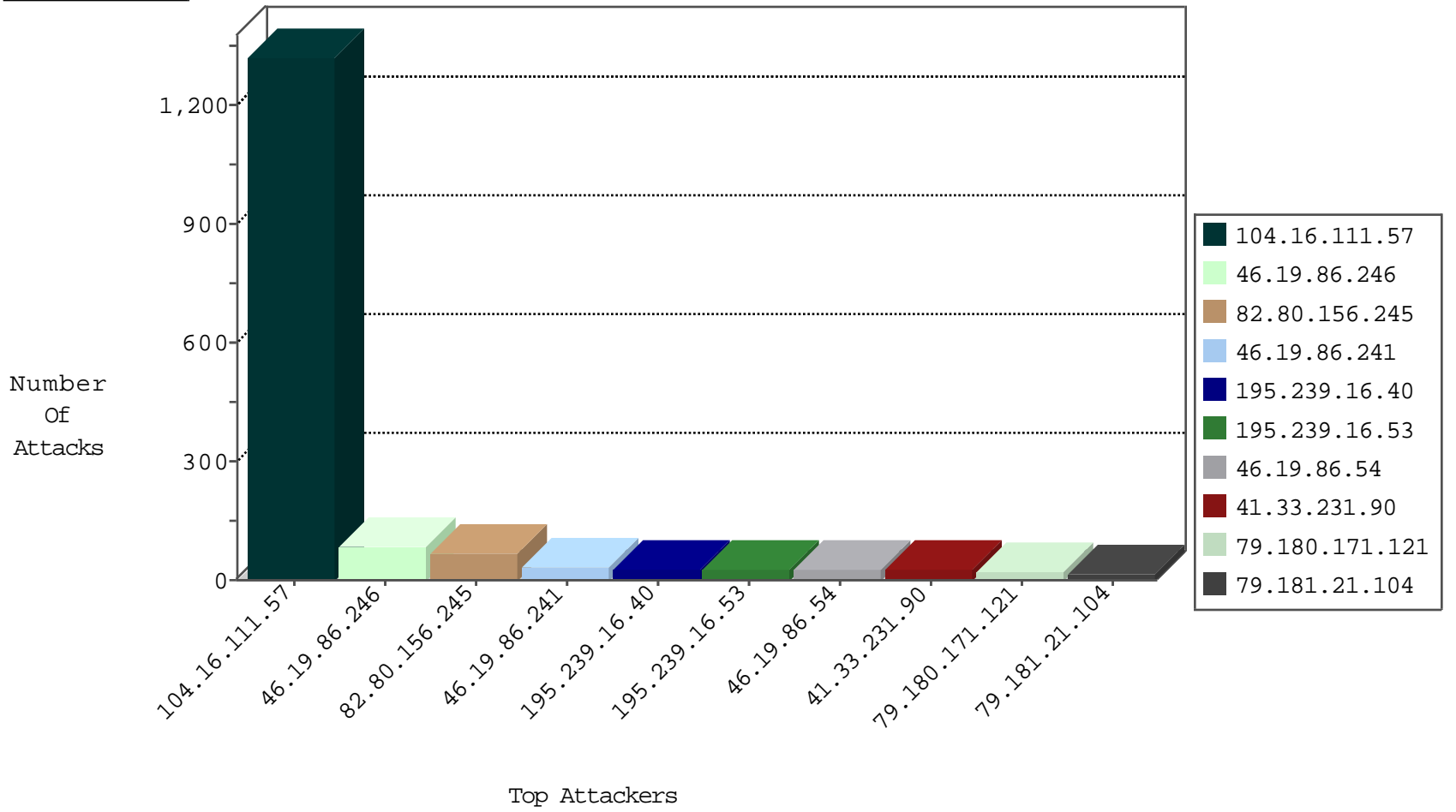
# IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.202.65.25	Germany	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.160.135.255	Israel	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
188.165.15.27	France	147.237.0.34	tikshuv.idf.il	C228: HTTP: AhrefBot crawler	Block	1

## 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
66.249.78.147	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
114.112.90.54	147.237.76.196	China	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
114.112.90.54	147.237.76.42	China	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
103.41.177.70	147.237.76.147		chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.66	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	147.237.72.217	China	e.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
209.126.116.147	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
182.72.109.162	147.237.77.226	India	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
114.112.90.54	147.237.76.176	China	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
103.41.177.70	147.237.76.147		chinuch.aka.idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.64	147.237.77.235	China	sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.64	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.64	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
104.16.111.57	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	660
104.16.111.57	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	659
82.80.156.245	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	65
195.239.16.53	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	26
195.239.16.40	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
79.181.21.104	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
69.227.159.44	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
46.19.86.54	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
46.19.86.145	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.86.54	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.194	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.180.171.121	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	6
46.19.86.54	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
37.26.149.209	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence		alert	4
37.26.149.209	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence		monitor	4
2.54.184.136	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.54	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
31.210.187.30	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.26.149.209	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.171.121	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	3
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.16.167	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.247	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.180.171.121	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
178.154.189.201	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.139.221.67	Spain	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
212.143.172.166	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.171.121	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.178.112.90	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
54.176.56.176	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
37.46.39.169	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.180.171.121	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
84.94.181.18	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.26.149.209	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.46.39.243	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
77.127.174.206	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
195.239.16.53	Russian Federation	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
178.123.223.186	Belarus	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.246.86.77	Sweden	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	2
5.22.131.2	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.145	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid sequence number	monitor	2
195.239.16.40	Russian Federation	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
37.26.149.209	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	2
31.168.149.174	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
77.126.209.72	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
149.88.110.79	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	81
46.19.86.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
37.26.146.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
31.179.217.133	Poland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/dover.aspx/	Block	1
109.253.147.110	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestion\$96 in aka.idf.il/main/gyus/questionnaire.aspx	None	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1956-he/cogat.aspx	Block	1
50.21.188.68	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/wp/wp-admin/	Block	1
192.243.55.129	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.129	Block	1
80.246.139.75	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.74.106	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	1
146.200.218.53	United Kingdom	147.237.77.216	dover.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$txtEmail in www.idf.il/1038-en/dover.aspx	Block	1
72.34.33.170	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/blog/wp-admin/	Block	1
50.63.194.20	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 50.63.194.20	Block	1
217.132.13.245	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
82.80.156.245	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.74.108	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/3/111513.pdf	Block	1
37.142.64.48	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestion\$117 in aka.idf.il/main/gyus/questionnaire.aspx	None	1
178.49.154.143	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1044-he/ishurim.aspx	Block	1
79.177.127.90	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
50.63.194.20	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/wp-admin/	Block	1
84.228.155.233	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestion\$18 in aka.idf.il/main/gyus/questionnaire.aspx	None	1
66.249.79.31	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
184.106.10.128	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/old/wp-admin/	Block	1
79.178.97.33	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	1
64.19.78.242	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
95.154.214.2	United Kingdom	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/wordpress/wp-admin/	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1393-en/dover.aspx	Block	1
192.243.55.129	Dominica	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/gyus/kadatz	Block	1
79.178.97.33	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/2/	Block	1
66.249.74.104	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/4/108204.pdf	Block	1