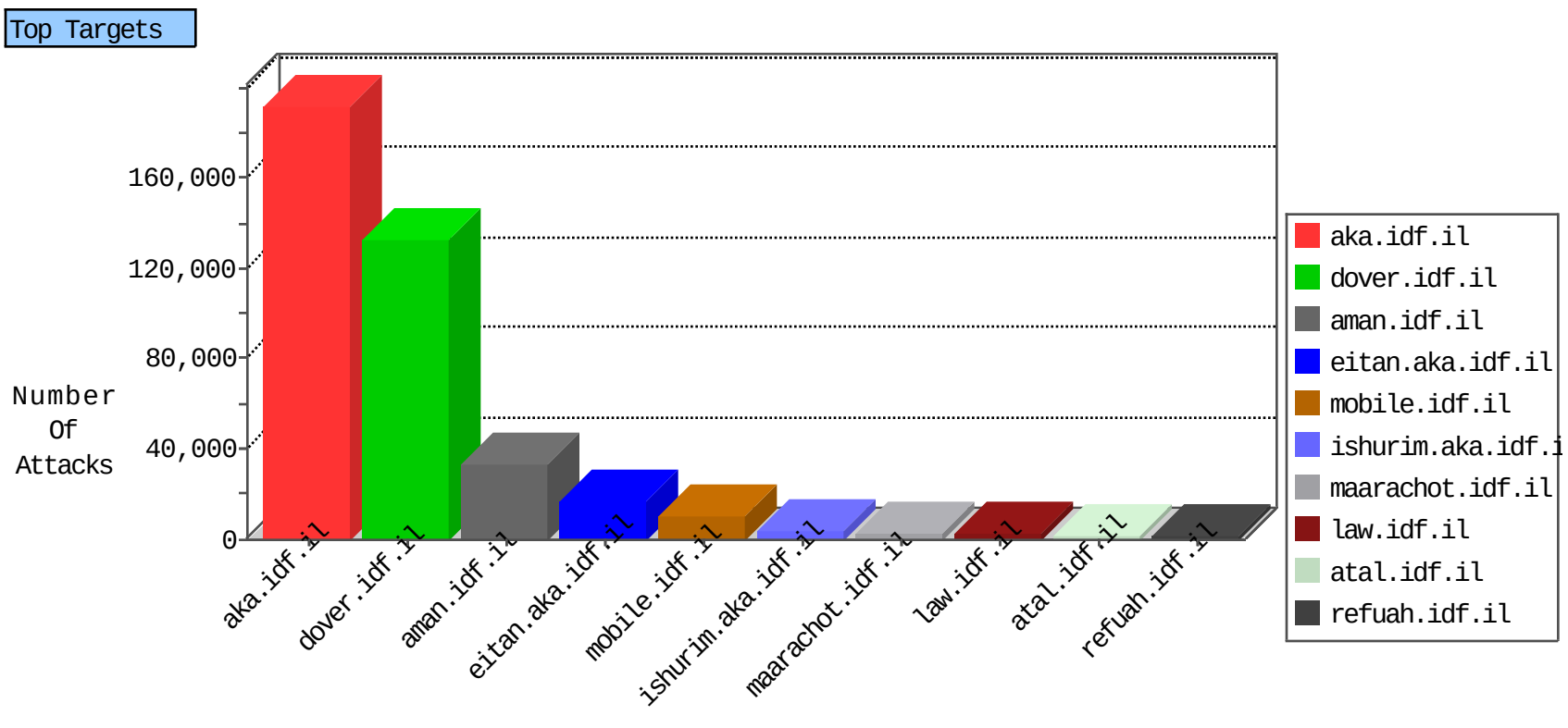
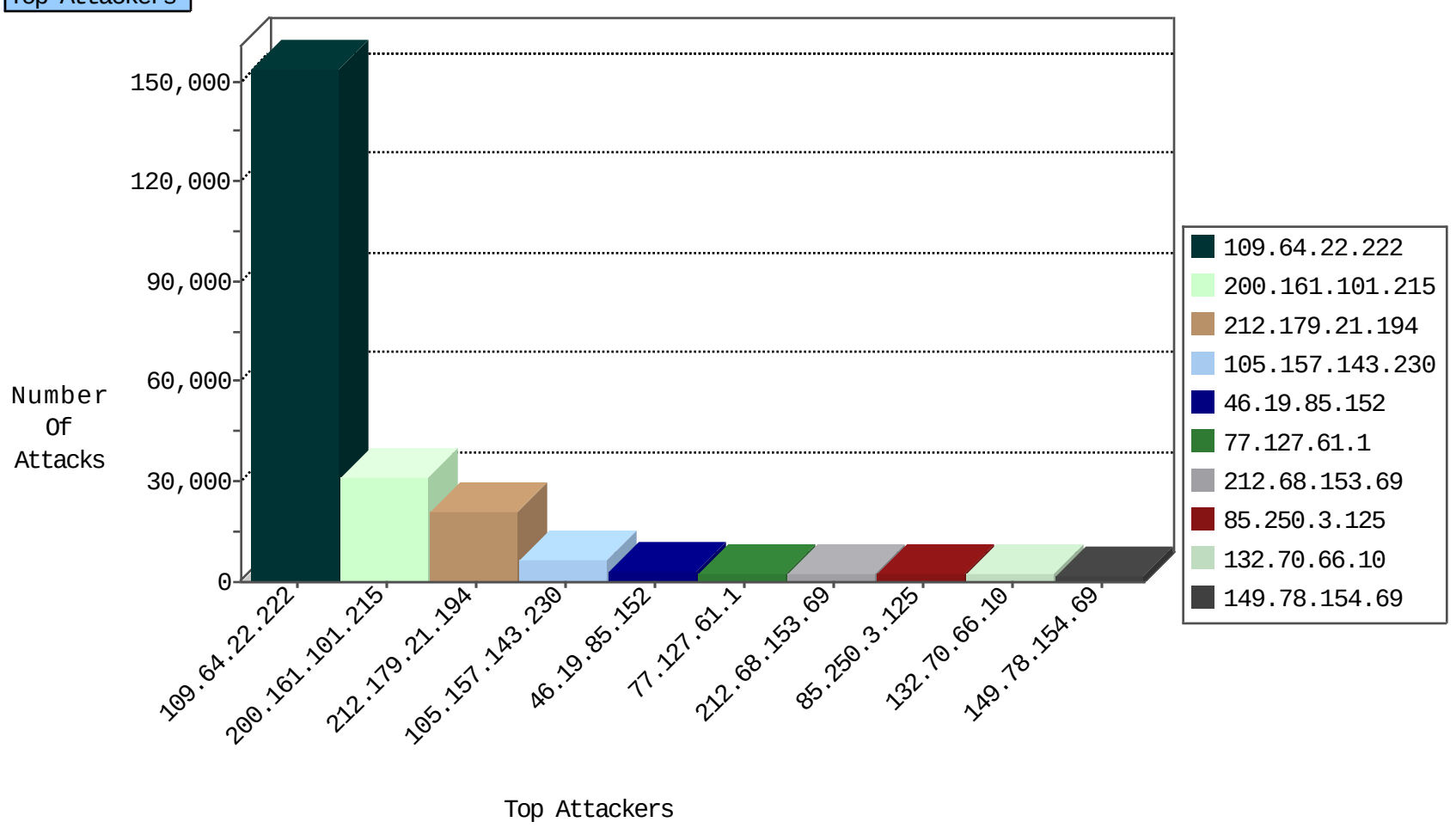
10-29-2015 to 10-30-2015

IDF Under Attack
Daily Report

Top Targets



Top Attackers



10-29-2015 to 10-30-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.67.20	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	53250
66.249.67.67	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	39461
66.249.67.34	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	37626
66.249.67.27	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	34383
66.249.69.85	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	28064
66.249.67.210	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	9956
66.249.78.159	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8972
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	8298
37.26.148.143	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7170
51.254.143.241	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6301
66.249.69.77	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	5700
66.249.67.194	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	5664
66.249.69.50	United States	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	3159
66.249.67.79	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3134
46.120.68.102	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3002
66.249.67.73	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2932
66.249.64.103	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	2790
66.249.67.6	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	2341
66.249.64.14	United States	147.237.0.15	kosher-kravi.idf.il	TCP handshake violation, first packet not syn	drop	2271
66.249.64.4	United States	147.237.0.15	kosher-kravi.idf.il	TCP handshake violation, first packet not syn	drop	2231
66.249.69.76	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2202
66.249.93.196	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1835
66.249.78.197	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	1798
66.249.78.173	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1737
176.43.78.149	Turkey	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	1675
46.19.85.21	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1647
66.249.79.77	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1600
66.249.69.92	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1556
66.249.67.122	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1552
208.115.111.73	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1501
66.249.69.84	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1393
66.249.93.192	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1243
79.181.114.103	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	999
66.249.75.68	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	870
66.249.78.190	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	854
194.90.239.2	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	747
52.23.199.183	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	657
66.249.64.200	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	616
46.19.86.129	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	566
80.246.133.50	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	549
66.249.64.133	United States	147.237.77.234	halag.idf.il	TCP handshake violation, first packet not syn	drop	547
46.19.86.145	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	543
66.249.75.44	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	532
66.249.69.69	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	518
213.57.118.66	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	478
52.29.83.65	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	451
66.249.78.166	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	378
66.249.69.128	United States	147.237.77.234	halag.idf.il	TCP handshake violation, first packet not syn	drop	374
194.90.178.37	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	305
66.249.69.34	United States	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	296

10-29-2015 to 10-30-2015

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
223.73.44.148	China	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	24
82.80.9.134	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	18
84.108.110.39	Israel	147.237.76.42	refuah.idf.il	1633: HTTP: WebDAV Protocol PROPFIND Method	Block	16
79.180.54.197	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	10
223.73.44.148	China	147.237.77.216	dover.idf.il	0854: HTTP: upload* Access	Block	9
192.115.252.2	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
80.179.19.55	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
84.94.199.239	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
46.121.120.109	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
149.202.52.100	Germany	147.237.77.235	sviva.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	4
78.135.61.182	Turkey	147.237.77.216	dover.idf.il	2809: HTTP: IIS TRACK Method	Block	3
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	2
31.154.91.115	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
85.102.241.204	Turkey	147.237.77.216	dover.idf.il	2809: HTTP: IIS TRACK Method	Block	2
89.138.234.62	Israel	147.237.77.216	dover.idf.il	C1000098: Block - dns poisoning	Block	2
200.161.101.215	Brazil	147.237.72.156	aman.idf.il	13444: HTTP: WhatWeb User-Agent Header	Block	2
31.154.33.190	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
81.218.33.77	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
213.87.120.15	Russian Federation	147.237.77.74	law.idf.il	12580: HTTP: SQL Injection (Cookie Header)	Block	1
195.160.240.11	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
85.102.173.242	Turkey	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
200.161.101.215	Brazil	147.237.72.156	aman.idf.il	C003: HTTP: phpMyAdmin access	Block	1
78.160.189.5	Turkey	147.237.72.166	aka.idf.il	10767: HTTP: Acunetix Security Scanner	Block	1
188.138.17.205	France	147.237.76.177	ncore.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
89.163.148.58	Germany	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
81.218.160.79	Israel	147.237.77.176	matpash.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
216.221.146.186	United States	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
198.20.69.74	United States	147.237.8.50	e.tikshuv.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
115.42.137.250	Singapore	147.237.77.216	dover.idf.il	12347: HTTP: PHP-CGI Query String Parameter Information Disclosure Vulnerability	Block	1
200.161.101.215	Brazil	147.237.72.156	aman.idf.il	C015: HTTP: Suspicious Dir Access	Block	1
36.239.3.136	Taiwan	147.237.77.74	law.idf.il	12580: HTTP: SQL Injection (Cookie Header)	Block	1
93.173.50.12	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
198.20.69.74	United States	147.237.76.198	e.yohalan.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
69.30.213.82	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
144.76.7.107	Germany	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
85.102.241.204	Turkey	147.237.77.216	dover.idf.il	3909: HTTP: Cross Site Scripting (Alert function)	Block	1
200.161.101.215	Brazil	147.237.72.156	aman.idf.il	C1000158: HTTP(S): Hacked in the Payload	Block	1
37.215.9.140	Belarus	147.237.77.216	dover.idf.il	12580: HTTP: SQL Injection (Cookie Header)	Block	1
193.201.225.12	Ukraine	147.237.77.176	matpash.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
94.188.161.145	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
200.161.101.215	Brazil	147.237.72.156	aman.idf.il	0360: HTTP: Protected Directory Access (~root)	Block	1
149.202.52.100	Germany	147.237.77.235	sviva.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
81.110.84.149	United Kingdom	147.237.77.74	law.idf.il	C1000106: HTTP: majestic bot	Block	1
213.8.241.210	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
195.154.169.85	France	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
78.135.61.182	Turkey	147.237.77.216	dover.idf.il	3643: HTTP: Nikto HTTP Request	Block	1
89.139.191.39	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1

10-29-2015 to 10-30-2015

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	64
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	62
66.249.67.27	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	34
66.249.67.73	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	7
176.12.144.246	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	7
95.86.80.23	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	6
176.43.78.149	147.237.77.216	Turkey	dover.idf.il	ET SCAN NMAP -sS window 1024	5
66.249.69.84	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	5
66.249.67.20	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	4
192.198.151.45	147.237.72.167	Europe	ishurim.aka.idf.il	ET SCAN NMAP -sA (2)	4
66.249.75.53	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sA (2)	4
66.249.69.69	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	3
200.161.101.215	147.237.72.156	Brazil	aman.idf.il	SERVER-WEBAPP backup access	3
66.249.64.195	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	3
82.80.196.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	3
59.46.193.114	147.237.76.148	China	gqcenter.aka.idf.il	GPL SCAN nmap TCP	2
218.24.171.223	147.237.76.148	China	gqcenter.aka.idf.il	GPL SCAN nmap TCP	2
54.72.0.55	147.237.77.216	Ireland	dover.idf.il	portscan: TCP Distributed Portscan	2
66.249.93.224	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
46.162.116.98	147.237.77.19	Sweden	law-forum.idf.il	ET SCAN NMAP -sS window 1024	2
79.181.108.212	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
59.45.79.117	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	2
66.249.75.60	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.55	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	2
66.249.69.85	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	2
47.88.13.149	147.237.77.216	Canada	dover.idf.il	SQL Injection - Select From	2
66.249.69.77	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	2
66.249.65.40	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.190	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
101.51.144.109	147.237.8.14	Thailand	e.orchot.idf.il	ET SCAN Potential SSH Scan	2
46.162.116.98	147.237.76.176	Sweden	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.64.60	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	2
85.102.241.204	147.237.77.216	Turkey	dover.idf.il	SERVER-WEBAPP client negative Content-Length attempt	2
2.54.11.118	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.173.252.13	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
222.186.34.238	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
79.178.22.42	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
197.45.38.75	147.237.8.50	Egypt	e.tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.45.79.117	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
149.88.69.194	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.147.253	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
101.51.144.109	147.237.76.202	Thailand	e.halag.idf.il	ET SCAN Potential SSH Scan	1
84.229.30.152	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.143.134.129	147.237.77.216	Israel	dover.idf.il	INDICATOR-SCAN myscan	1
176.106.227.93	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.117.190.123	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
118.244.216.171	147.237.8.45	China	e.eitan.idf.il	ET SCAN NMAP -f -sS	1
46.183.219.66	147.237.77.216	Latvia	dover.idf.il	ET SCAN NMAP -sS window 1024	1
122.114.17.100	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
5.102.198.124	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

10-29-2015 to 10-30-2015

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13123
105.157.143.230	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6205
200.161.101.215	Brazil	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	3017
109.64.22.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2784
46.19.85.152	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2764
212.68.153.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2568
200.161.101.215	Brazil	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2066
200.161.101.215	Brazil	147.237.72.156	aman.idf.il	drop		drop	1914
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1384
78.135.61.182	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1020
77.126.169.188	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1018
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	917
190.24.146.71	Colombia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	909
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	906
200.161.101.215	Brazil	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	889
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	748
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	733
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	732
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	709
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	704
77.127.61.1	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	699
5.28.139.186	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	697
212.150.189.2	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	681
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	679
37.26.149.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	671
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	667
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	581
204.93.58.133	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	552
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	548
46.19.85.55	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	490
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	435
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	411
200.161.101.215	Brazil	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	395
2.54.7.90	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	388
79.178.113.2	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	381
32.208.112.21	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	366
151.80.31.112	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	365
92.62.170.94	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	357
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	339
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	334
31.154.27.186	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	328
92.62.170.95	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	316
168.235.196.45	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	310
46.121.110.157	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	308
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	294
2.52.158.119	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	293
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	289
37.239.8.38	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	287
151.90.254.205	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	287
95.86.124.108	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	274

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.64.22.222	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 109.64.22.222	Block	98876
109.64.22.222	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	27921
109.64.22.222	Israel	147.237.72.166	aka.idf.il	Automated Vulnerability Scanning	Block	24487
200.161.101.215	Brazil	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 200.161.101.215	Block	22332
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3990
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 212.179.21.194	Block	3285
85.250.3.125	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2220
132.70.66.10	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2120
77.127.61.1	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1935
80.178.157.40	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	1155
81.218.179.164	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	764
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	705
46.19.86.31	Israel	147.237.72.167	ishurim.aka.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.86.31	Block	615
105.157.143.230	Morocco	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 105.157.143.230	Block	557
93.172.42.33	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	480
63.141.217.113	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 63.141.217.113	Block	465
109.64.219.228	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	435
79.178.113.2	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	345
66.249.64.200	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.200	Block	345
66.249.64.60	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	330
84.108.102.161	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	300
84.108.102.161	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	300
139.193.132.90	Indonesia	147.237.77.170	maarachot.idf.il	Multiple Illegal Byte Code Character in Header Value from 139.193.132.90	Block	298
139.193.132.90	Indonesia	147.237.77.74	law.idf.il	Multiple Illegal Byte Code Character in Header Value from 139.193.132.90	Block	296
31.154.91.205	Israel	147.237.72.166	aka.idf.il	Too Many of the Same Response Code (404) in Session from 31.154.91.205	Block	285
66.249.64.55	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	270
95.86.96.250	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	261
79.181.103.112	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	255
66.249.64.195	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.195	Block	255
79.181.103.112	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	249
84.108.110.39	Israel	147.237.76.42	refuah.idf.il	Unauthorized HTTP Method	Block	225
149.78.197.36	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/login parameter Password	Block	225
84.108.110.39	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/images/shared/green_tri_left.gif	Block	225
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.190	Block	224
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	210
87.68.156.73	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	210
37.26.149.243	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/login parameter Password	Block	195
66.249.64.50	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	195
176.106.227.136	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	195
63.141.217.113	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 63.141.217.113	Block	180
50.118.162.35	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 50.118.162.35	Block	180
176.106.227.124	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	180
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	180
46.117.14.189	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.117.14.189	Block	173
212.179.21.194	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	150
176.13.12.223	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	150
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	150
213.151.39.41	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	150
213.151.39.41	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	150
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	150