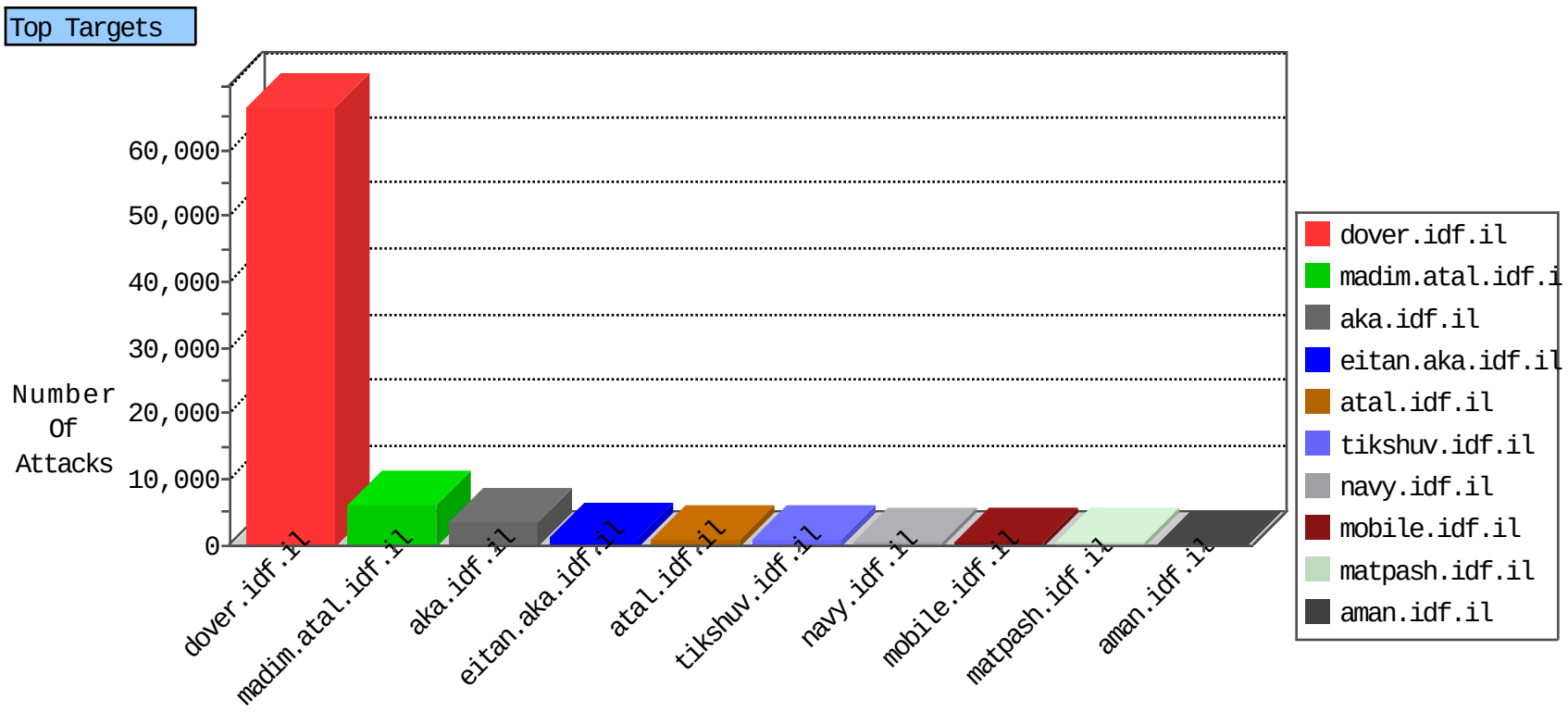
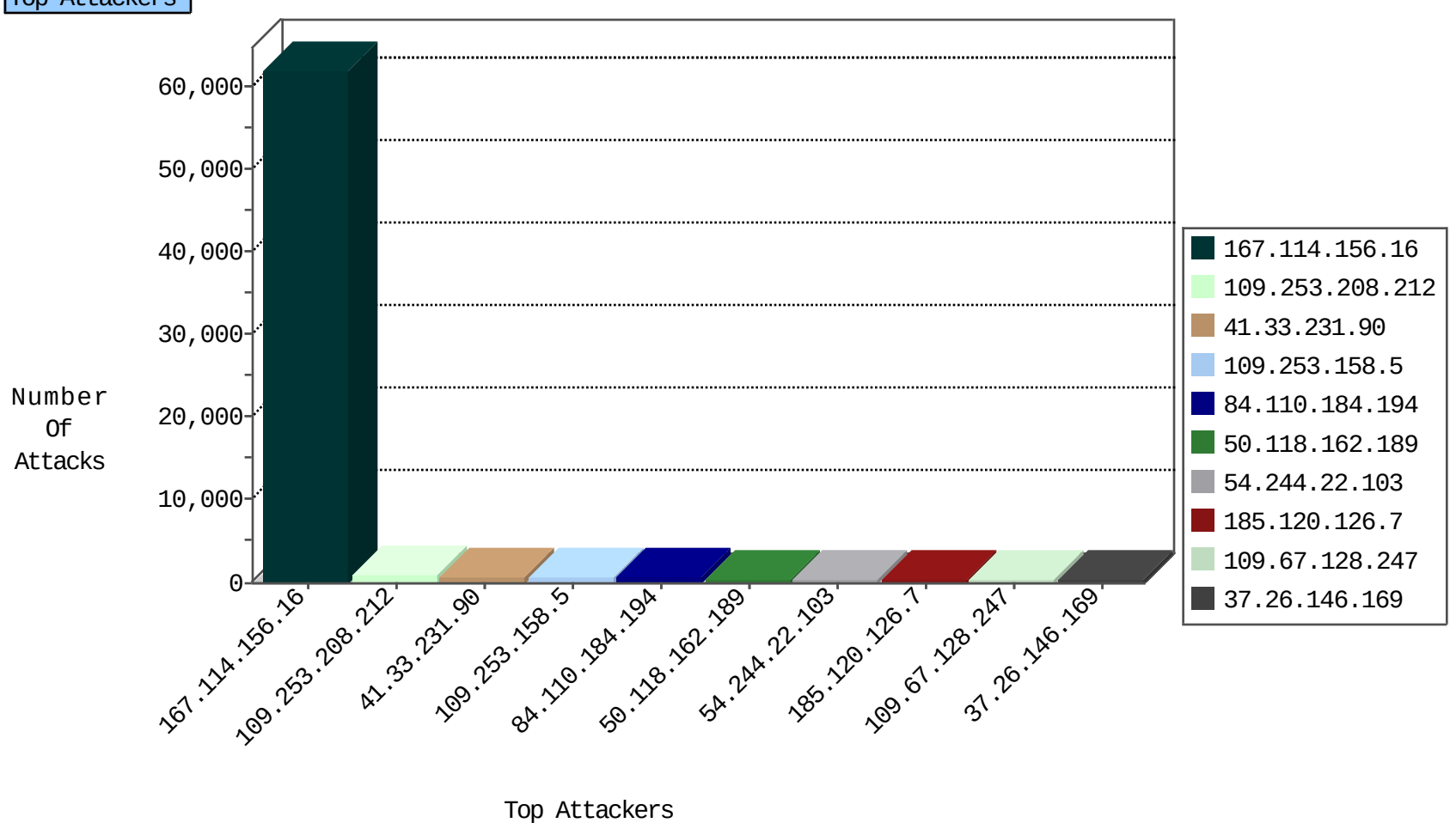
01-22-2016 to 01-23-2016

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-22-2016 to 01-23-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	90209
50.118.162.189	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	59467
212.34.11.56	Jordan	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	1431
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	1380
41.99.55.118	Algeria	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	907
66.249.78.146	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	534
109.67.128.247	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	481
50.118.162.234	United States	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-Product	dest-reset	87
216.177.129.21	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	75
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	66
41.99.55.118	Algeria	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-Url	dest-reset	19
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	16
85.130.251.227	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	12
91.67.187.60	Germany	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
2.91.159.232	Saudi Arabia	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-cat	dest-reset	8
50.118.162.234	United States	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-Url	dest-reset	8
85.130.251.227	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
50.118.162.234	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
109.67.136.7	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	6
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
79.177.200.217	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
173.231.115.59	Canada	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
66.249.78.159	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
79.176.164.22	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
41.233.40.97	Egypt	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	3
199.255.210.118	Anonymous Proxy	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-Product	dest-reset	3
79.183.14.212	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
204.42.253.2	United States	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	2
115.239.228.10	China	147.237.76.202	e.halag.idf.il	JLM_Under_Attack_Con_Http	drop	2
200.35.95.235	Venezuela	147.237.0.35	akaws.idf.il	L4 Source or Dest Port Zero	drop	2
151.80.230.239	Italy	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	2
204.42.253.2	United States	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	2
134.147.203.115	Germany	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	2
222.186.56.70	China	147.237.76.31	nakchal.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
185.130.5.224		147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	2
204.42.253.2	United States	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	2
64.31.132.129	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	2
204.42.253.2	United States	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	2
14.208.125.151	China	147.237.76.148	gqcenter.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
134.147.203.115	Germany	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	2
223.158.153.54	China	147.237.77.170	maarachot.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
204.42.253.2	United States	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	2
123.151.149.222	China	147.237.76.196	e.sviva.idf.il	JLM_Under_Attack_Con_Tcp	drop	2

01-22-2016 to 01-23-2016

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
159.253.145.150	United States	147.237.76.30	himush.idf.il	C095: Suspicious Addresses MFA	Permit	47
110.84.32.140	China	147.237.77.74	law.idf.il	C108: HTTP: Trying to locate existing FCKeditor	Block	8
149.78.250.185	Israel	147.237.77.216	dover.idf.il	1633: HTTP: WebDAV Protocol PROPFIND Method	Block	6
87.223.211.30	Spain	147.237.77.176	matpash.idf.il	C008: HTTP: Xenu UserAgent	Block	4
110.84.32.140	China	147.237.77.233	atal.idf.il	C108: HTTP: Trying to locate existing FCKeditor	Block	4
110.84.32.140	China	147.237.77.170	maarachot.idf.il	C108: HTTP: Trying to locate existing FCKeditor	Block	4
110.84.32.140	China	147.237.77.176	matpash.idf.il	C108: HTTP: Trying to locate existing FCKeditor	Block	4
110.84.32.140	China	147.237.77.226	www.chamatz.aka.idf.il	C108: HTTP: Trying to locate existing FCKeditor	Block	3
110.84.32.140	China	147.237.77.234	halag.idf.il	C108: HTTP: Trying to locate existing FCKeditor	Block	3
41.99.55.118	Algeria	147.237.77.216	dover.idf.il	10767: HTTP: Acunetix Security Scanner	Block	2
159.253.145.150	United States	147.237.77.216	dover.idf.il	C095: Suspicious Addresses MFA	Permit	2
41.99.55.118	Algeria	147.237.77.216	dover.idf.il	3999: HTTP: Cross Site Scripting Attack in HTTP Header	Block	2
172.245.218.130	United States	147.237.77.216	dover.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	2
149.200.166.51	Jordan	147.237.77.216	dover.idf.il	13444: HTTP: WhatWeb User-Agent Header	Block	2
110.84.32.140	China	147.237.77.216	dover.idf.il	C108: HTTP: Trying to locate existing FCKeditor	Block	2
31.193.130.137	United Kingdom	147.237.72.166	aka.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	2
174.34.135.242	United States	147.237.72.166	aka.idf.il	C106: HTTP: majestic bot	Block	1
188.165.15.202	France	147.237.77.216	dover.idf.il	C228: HTTP: AhrefBot crawler	Block	1
91.228.196.139	Poland	147.237.77.216	dover.idf.il	C076: HTTP: Access to - action=... (General)	Block	1
172.245.218.130	United States	147.237.76.86	navy.idf.il	0543: HTTP: php.cgi Access	Block	1
144.76.4.148	Germany	147.237.76.86	navy.idf.il	C106: HTTP: majestic bot	Block	1
198.50.134.71	Canada	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
88.246.96.192	Turkey	147.237.72.166	aka.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
177.185.192.77	Brazil	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
188.165.15.207	France	147.237.77.226	www.chamatz.aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1
95.70.232.65	Turkey	147.237.77.176	matpash.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
172.245.218.130	United States	147.237.77.216	dover.idf.il	0543: HTTP: php.cgi Access	Block	1
202.124.109.87	New Zealand	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
89.19.29.90	Turkey	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
178.151.143.163	Ukraine	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	1
168.235.155.26	Canada	147.237.77.233	atal.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
195.154.183.187	France	147.237.77.74	law.idf.il	19791: HTTP: WordPress N-Media PHP File Upload	Block	1
95.70.232.65	Turkey	147.237.77.216	dover.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
74.208.133.60	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
91.228.196.139	Poland	147.237.77.74	law.idf.il	C076: HTTP: Access to - action=... (General)	Block	1
178.175.142.50	Moldova, Republic of	147.237.8.46	e.chinuch.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
172.245.218.130	United States	147.237.72.166	aka.idf.il	0543: HTTP: php.cgi Access	Block	1
2.91.159.232	Saudi Arabia	147.237.77.216	dover.idf.il	10725: TCP: LOIC DDoS Tool	Block	1
115.163.56.112	Japan	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
197.242.159.42	South Africa	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
106.38.241.106	China	147.237.76.42	refuah.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
87.106.179.116	Germany	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
172.245.218.130	United States	147.237.77.233	atal.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1
151.236.51.169	United Kingdom	147.237.72.166	aka.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
91.228.196.139	Poland	147.237.77.170	maarachot.idf.il	C076: HTTP: Access to - action=... (General)	Block	1
185.130.5.207		147.237.77.216	dover.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
172.245.218.130	United States	147.237.76.42	refuah.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1
123.126.113.149	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
198.20.69.76	United States	147.237.8.46	e.chinuch.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

01-22-2016 to 01-23-2016

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.78.130	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	304
66.249.64.102	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	272
66.249.78.190	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	120
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	92
66.249.66.72	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	20
80.246.130.9	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	17
124.114.151.87	147.237.72.166	China	aka.idf.il	ET WEB_SERVER Possible SQL Injection (varchar)	10
188.120.148.137	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	10
158.85.253.245	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
66.249.78.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	6
163.172.13.173	147.237.72.166	United Kingdom	aka.idf.il	ET SCAN NMAP -sS window 1024	4
27.251.16.85	147.237.77.216	India	dover.idf.il	GPL SCAN nmap TCP	4
74.208.133.60	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	3
89.19.29.90	147.237.77.233	Turkey	atal.idf.il	SQL Injection - Select From	3
54.205.186.101	147.237.77.176	United States	matpash.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	3
202.124.109.87	147.237.76.42	New Zealand	refuah.idf.il	SQL Injection - Select From	3
87.106.179.116	147.237.77.233	Germany	atal.idf.il	SQL Injection - Select From	3
177.185.192.77	147.237.77.233	Brazil	atal.idf.il	SQL Injection - Select From	3
197.242.159.42	147.237.77.74	South Africa	law.idf.il	SQL Injection - Select From	3
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	3
66.249.66.77	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sA (2)	2
119.81.188.158	147.237.76.196	Hong Kong	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	2
213.204.101.24	147.237.76.86	Lebanon	navy.idf.il	ET SCAN NMAP -sA (2)	2
84.94.40.196	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sA (2)	2
66.249.66.33	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.93.95	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
212.106.77.23	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	ET SCAN NMAP -sA (2)	2
59.45.79.117	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	2
174.37.194.144	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sA (2)	2
66.249.65.112	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	2
174.37.194.144	147.237.0.33	United States	idf.il	ET SCAN NMAP -sA (2)	2
59.45.79.117	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	2
174.37.194.144	147.237.0.19	United States	madim.atal.idf.i	ET SCAN NMAP -sA (2)	2
66.249.64.55	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
59.45.79.117	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential SSH Scan	2
59.45.79.117	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	2
66.249.69.133	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
59.45.79.117	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	2
66.249.66.81	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sA (2)	2
59.45.79.117	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	2
66.249.66.75	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	2
66.249.66.39	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
59.45.79.117	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	2
66.249.93.99	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
159.8.109.19	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.66.12	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
119.30.47.130	147.237.76.86	Bangladesh	navy.idf.il	ET SCAN NMAP -sA (2)	2
66.249.65.34	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	2
108.168.185.133	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	2
59.45.79.117	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	2

01-22-2016 to 01-23-2016

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	813
50.118.162.189	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	511
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	380
46.19.86.66	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	354
37.26.146.169	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	339
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	270
216.177.129.21	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	235
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	129
77.127.135.136	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	120
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	108
2.54.59.148	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	108
46.185.135.58	Jordan	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	100
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	93
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	70
37.26.147.135	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	66
2.54.161.144	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	57
41.141.1.42	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	55
212.101.249.140	Lebanon	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	55
212.101.249.140	Lebanon	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	53
80.246.130.158	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	52
109.67.206.153	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	51
176.13.19.10	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
109.160.174.42	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	46
109.160.174.42	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	46
141.8.184.5	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	42
93.172.183.141	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	40
212.179.225.7	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	40
79.183.193.153	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
84.109.7.149	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	38
109.66.27.189	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	37
85.64.112.177	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
178.154.189.201	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
79.177.203.190	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	36
107.167.112.143	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	35
202.40.137.198	Hong Kong	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	35
109.160.243.123	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	28
141.8.184.25	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
79.183.17.23	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
195.239.16.40	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
195.239.16.53	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
37.26.147.186	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
109.65.196.175	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	25
46.19.86.96	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
87.68.155.149	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
82.145.218.4	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	24
109.66.151.90	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
79.181.185.103	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24

01-22-2016 to 01-23-2016

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
5.170.24.187	Italy	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.208.212	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 109.253.208.212	Block	655
84.110.184.194	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	360
109.253.158.5	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 109.253.158.5	Block	318
109.253.208.212	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 109.253.208.212	Block	281
185.120.126.7		147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	213
79.177.116.58	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	195
185.120.126.7		147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	183
109.67.128.247	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	182
79.179.202.238	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	180
2.52.169.90	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.52.169.90	Block	152
109.67.128.247	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	145
46.19.86.153	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	142
46.19.86.153	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	137
46.19.86.216	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	133
109.253.200.140	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	133
2.52.169.90	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	132
109.253.158.5	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 109.253.158.5	Block	124
109.253.158.5	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	124
109.253.200.140	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	122
109.253.208.212	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	114
79.179.202.238	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
84.110.184.194	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	104
84.110.184.194	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
79.178.162.184	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	93
79.179.171.207	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	88
79.176.191.206	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	86
109.253.142.172	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	84
79.183.143.102	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 79.183.143.102	Block	79
185.32.179.13	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	73
79.178.162.184	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 79.178.162.184	Block	73
79.176.191.206	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	72
109.253.205.13	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	67
79.177.116.58	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 79.177.116.58	Block	58
2.54.167.125	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	57
2.54.1.184	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	53
37.26.147.136	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	49
109.253.195.225	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	48
109.253.142.172	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 109.253.142.172	Block	48
46.19.86.216	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	46
87.68.44.232	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	44
2.52.177.172	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	43
46.117.11.180	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	43
79.179.171.207	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	37
109.253.208.212	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	37
109.253.150.48	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	36
109.253.205.13	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	35
217.132.133.164	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	33
176.228.15.90	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	30
109.65.149.245	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	30
109.253.200.140	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	30