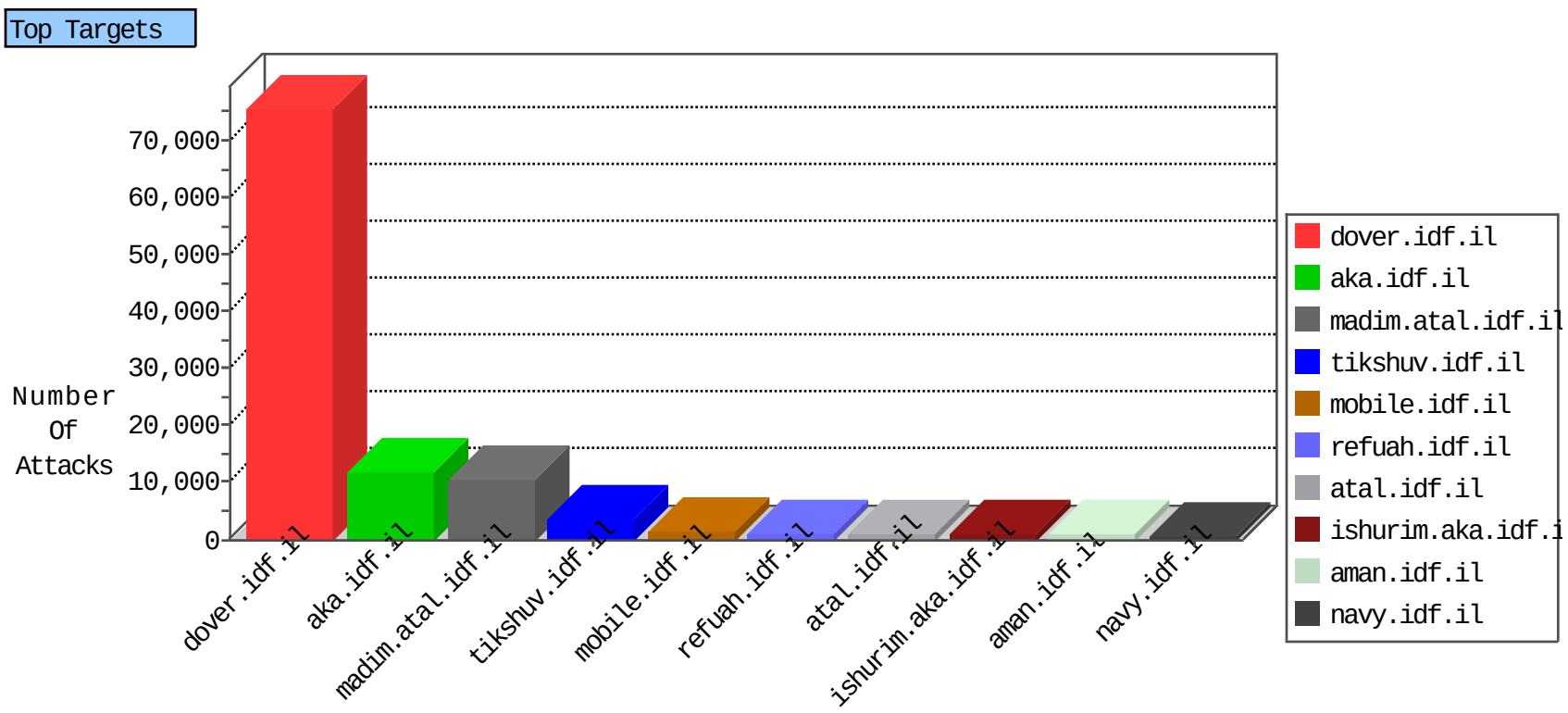
01-24-2016 to 01-25-2016

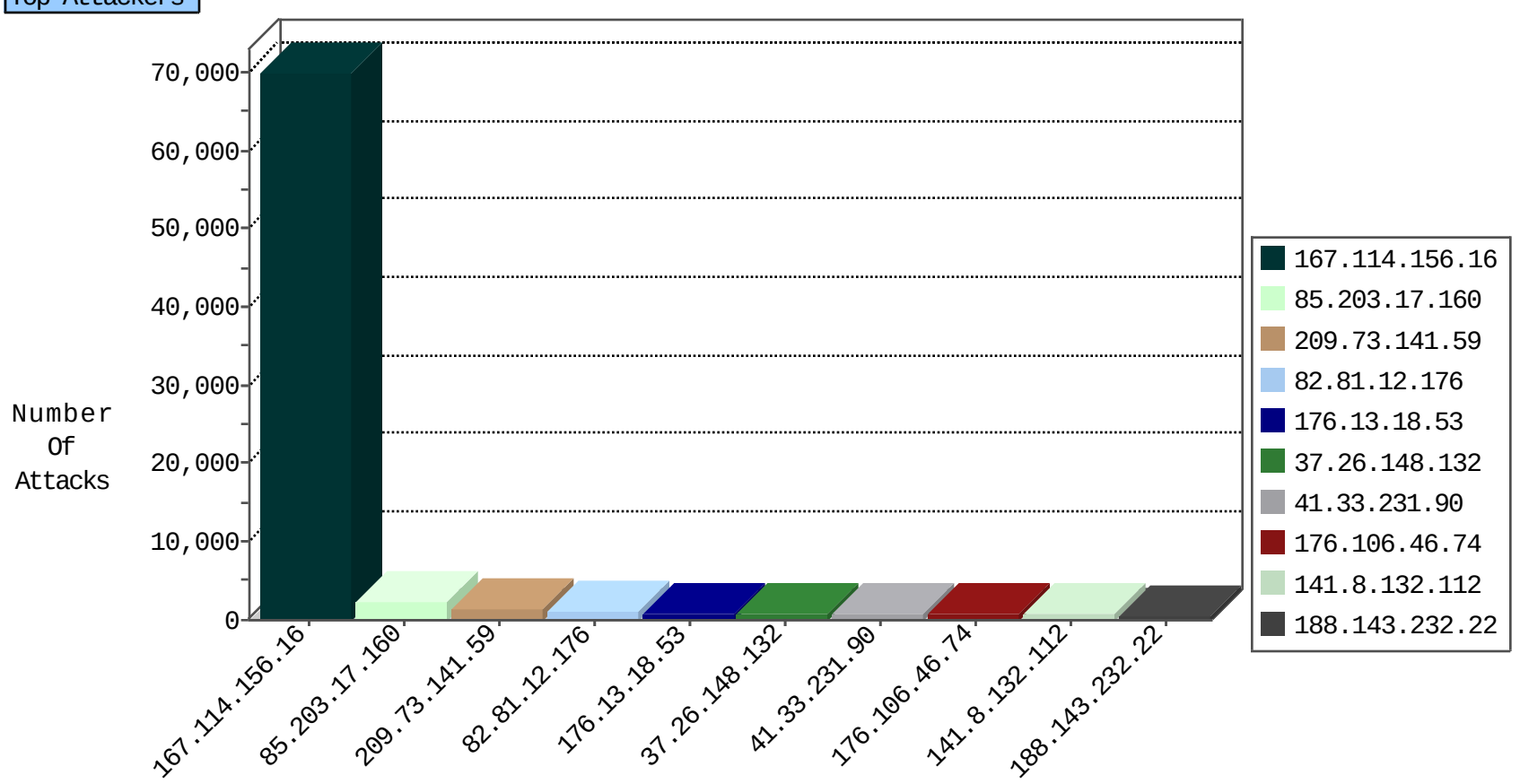
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

01-24-2016 to 01-25-2016

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	89974
66.249.78.146	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	10777
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	1086
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	454
207.232.36.181	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	403
212.199.154.194	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	268
212.199.154.194	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	219
81.218.241.25	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	201
66.249.78.97	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	123
91.231.193.150	Israel	147.237.76.42	refuah.idf.il	JLM_Purple_Con_Limit_Http	drop	85
2.54.23.34	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	67
46.19.86.208	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	57
91.231.193.150	Israel	147.237.76.42	refuah.idf.il	JLM_Purple_Con_Limit_Tcp	drop	35
79.182.220.133	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	15
85.64.45.225	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	15
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	10
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	10
79.178.99.58	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
79.182.196.41	Israel	147.237.72.166	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
95.86.71.43	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
109.67.125.101	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
213.8.204.81	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
197.114.30.13	Algeria	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
168.235.197.211	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	4
2.52.58.34	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
134.147.203.115	Germany	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	4
50.135.11.137	United States	147.237.72.167	ishurim.aka.idf.il	TCP handshake violation, first packet not syn	drop	4
212.179.54.237	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
2.54.29.111	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
134.147.203.115	Germany	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	3
81.218.56.245	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
31.168.133.226	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
79.183.227.154	Israel	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	3
109.66.160.66	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
31.168.225.146	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
82.81.12.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
134.147.203.115	Germany	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	2
134.147.203.115	Germany	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	2
8.37.231.199	Anonymous Proxy	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
134.147.203.115	Germany	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	2
85.25.217.80	Germany	147.237.0.200	m4u.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
115.230.124.164	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	2
183.60.48.25	China	147.237.76.196	e.sviva.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
66.102.9.118	United States	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	2
134.147.203.115	Germany	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	2
193.242.218.6	Switzerland	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	2
113.171.23.126	Vietnam	147.237.76.176	test.ncore.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
115.239.228.10	China	147.237.76.38	e.e.meitav.idf.il	JLM_Under_Attack_Con_Http	drop	2
134.147.203.115	Germany	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	2

01-24-2016 to 01-25-2016

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
119.97.146.76	China	147.237.77.216	dover.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	10
151.80.31.151	Italy	147.237.76.42	refuah.idf.il	C228: HTTP: AhrefBot crawler	Block	5
151.80.31.152	Italy	147.237.76.42	refuah.idf.il	C228: HTTP: AhrefBot crawler	Block	4
151.80.31.150	Italy	147.237.76.42	refuah.idf.il	C228: HTTP: AhrefBot crawler	Block	4
45.63.71.182		147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	3
151.80.31.153	Italy	147.237.76.86	navy.idf.il	C228: HTTP: AhrefBot crawler	Block	3
193.90.12.86	Norway	147.237.72.166	aka.idf.il	C067: HTTP: attempt to access .config page	Block	3
85.64.5.251	Israel	147.237.72.166	aka.idf.il	13444: HTTP: WhatWeb User-Agent Header	Block	3
151.80.31.153	Italy	147.237.76.42	refuah.idf.il	C228: HTTP: AhrefBot crawler	Block	2
151.80.31.154	Italy	147.237.76.42	refuah.idf.il	C228: HTTP: AhrefBot crawler	Block	2
61.218.36.252	Taiwan	147.237.77.216	dover.idf.il	C108: HTTP: Trying to locate existing FCKeditor	Block	2
45.32.64.53		147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	2
151.80.31.152	Italy	147.237.72.166	aka.idf.il	C228: HTTP: AhrefBot crawler	Block	2
151.80.31.151	Italy	147.237.72.166	aka.idf.il	C228: HTTP: AhrefBot crawler	Block	2
204.12.168.26	United States	147.237.0.34	tikshuv.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	2
119.97.146.76	China	147.237.77.216	dover.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	2
151.80.31.154	Italy	147.237.76.86	navy.idf.il	C228: HTTP: AhrefBot crawler	Block	2
45.32.225.19		147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	2
49.246.230.40	China	147.237.77.233	atal.idf.il	8479: HTTP: Suspicious HTTP Request	Block	2
151.80.31.153	Italy	147.237.72.166	aka.idf.il	C228: HTTP: AhrefBot crawler	Block	2
151.80.31.150	Italy	147.237.76.86	navy.idf.il	C228: HTTP: AhrefBot crawler	Block	2
151.80.31.154	Italy	147.237.72.166	aka.idf.il	C228: HTTP: AhrefBot crawler	Block	2
45.32.64.53		147.237.72.166	aka.idf.il	C008: HTTP: Xenu UserAgent	Block	2
151.80.31.151	Italy	147.237.77.74	law.idf.il	C228: HTTP: AhrefBot crawler	Block	2
151.80.31.151	Italy	147.237.0.34	tikshuv.idf.il	C228: HTTP: AhrefBot crawler	Block	1
40.84.157.59	United States	147.237.0.15	kosher-kravi.idf.il	10711: HTTP: ZmEu Vulnerability Scanner	Block	1
200.98.137.169	Brazil	147.237.72.166	aka.idf.il	C041: HTTP: Access to - index.php?option=com_jce	Block	1
188.165.15.21	France	147.237.76.31	nakchal.idf.il	C228: HTTP: AhrefBot crawler	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
208.98.56.66	United States	147.237.77.216	dover.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1
191.232.39.241	United States	147.237.72.166	aka.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	1
151.80.31.126	Italy	147.237.76.147	chinuch.aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1
88.150.221.26	United Kingdom	147.237.72.166	aka.idf.il	C008: HTTP: Xenu UserAgent	Block	1
185.130.5.247		147.237.0.19	madim.atal.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	1
46.119.121.146	Ukraine	147.237.77.74	law.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
40.84.157.59	United States	147.237.0.17	m.my-kosher-kravi.idf.il	10711: HTTP: ZmEu Vulnerability Scanner	Block	1
188.165.15.121	France	147.237.76.86	navy.idf.il	C228: HTTP: AhrefBot crawler	Block	1
66.176.172.168	United States	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
151.80.31.150	Italy	147.237.0.34	tikshuv.idf.il	C228: HTTP: AhrefBot crawler	Block	1
89.19.29.90	Turkey	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
185.130.5.247		147.237.77.216	dover.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
151.80.31.153	Italy	147.237.77.74	law.idf.il	C228: HTTP: AhrefBot crawler	Block	1
46.165.197.142	Germany	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	1
40.84.157.59	United States	147.237.0.19	madim.atal.idf.il	10711: HTTP: ZmEu Vulnerability Scanner	Block	1
208.98.56.66	United States	147.237.72.166	aka.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1
188.165.15.195	France	147.237.72.166	aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1
69.30.214.46	United States	147.237.72.166	aka.idf.il	C106: HTTP: majestic bot	Block	1
151.80.31.154	Italy	147.237.77.74	law.idf.il	C228: HTTP: AhrefBot crawler	Block	1
45.63.70.210		147.237.77.74	law.idf.il	C008: HTTP: Xenu UserAgent	Block	1
151.80.31.153	Italy	147.237.0.34	tikshuv.idf.il	C228: HTTP: AhrefBot crawler	Block	1

01-24-2016 to 01-25-2016

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	63
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	51
2.52.164.248	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	15
37.26.148.132	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	11
212.199.57.197	147.237.72.166	Israel	aka.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	7
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	7
66.249.78.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	6
66.249.78.104	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	6
208.79.213.108	147.237.77.216	United States	dover.idf.il	SERVER-WEBAPP mod-plsql administration access	5
132.74.95.19	147.237.77.170	Israel	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	4
66.249.78.97	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	4
204.12.168.26	147.237.0.34	United States	tikshuv.idf.il	SQL Injection - Select From	4
176.13.18.53	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	4
89.19.29.90	147.237.77.233	Turkey	atal.idf.il	SQL Injection - Select From	3
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	3
163.172.13.173	147.237.72.166	United Kingdom	aka.idf.il	ET SCAN NMAP -sS window 1024	3
23.91.70.77	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	3
66.249.75.198	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
218.246.0.97	147.237.76.198	China	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	2
109.253.130.97	147.237.77.216	Israel	dover.idf.il	GPL SCAN myscan	2
163.172.13.173	147.237.8.50	United Kingdom	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.75.247	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	2
84.228.43.49	147.237.72.156	Israel	aman.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
119.97.146.76	147.237.77.216	China	dover.idf.il	ET WEB_SERVER Muieblackcat scanner	2
66.249.78.160	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
109.253.130.97	147.237.77.216	Israel	dover.idf.il	INDICATOR-SCAN myscan	2
188.120.135.12	147.237.72.166	Israel	aka.idf.il	GPL SCAN nmap TCP	2
66.249.78.2	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
85.233.76.49	147.237.0.34	Russian Federation	tikshuv.idf.il	Tehila - Perl LWP with fake user agent	2
191.240.136.5	147.237.77.170	Brazil	maarachot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
37.142.64.45	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
162.248.94.44	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -f -sS	1
93.174.93.181	147.237.77.233	Netherlands	atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
80.230.40.7	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
216.72.40.185	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.228.207.18	147.237.76.197	Germany	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
185.130.5.234	147.237.76.42		refuah.idf.il	ET SCAN Potential SSH Scan	1
2.52.39.145	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
112.168.26.199	147.237.77.216	Korea, Republic of	dover.idf.il	ET SCAN Potential SSH Scan	1
89.163.148.90	147.237.76.30	Germany	himush.idf.il	ET SCAN Potential SSH Scan	1
89.248.174.81	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
78.193.2.8	147.237.76.30	France	himush.idf.il	ET SCAN NMAP -sS window 1024	1
199.191.56.187	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.199	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
182.131.21.69	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
109.65.211.118	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.65.70.39	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
219.128.162.66	147.237.76.31	China	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.45.79.117	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1

01-24-2016 to 01-25-2016

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
85.203.17.160	Netherlands	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	2358
209.73.141.59	Anonymous Proxy	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1420
176.106.46.74	Palestinian Territory, Occupied	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	700
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	685
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	615
93.173.244.219	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	408
85.130.246.101	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	372
5.29.212.105	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	263
69.31.51.182	Anonymous Proxy	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	200
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	129
168.235.197.211	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	117
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	112
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	95
2.52.61.88	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
141.8.184.5	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
141.8.184.25	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	78
2.54.143.99	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	75
93.158.152.31	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	75
85.130.232.75	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
87.68.69.66	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	67
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	66
46.19.85.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	66
8.37.231.199	Anonymous Proxy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	64
188.143.232.22	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	64
37.34.60.109	Netherlands	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	61
212.179.215.75	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
79.183.175.49	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	53
84.228.158.92	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	51
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	51
84.95.60.216	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	49
85.130.255.138	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
46.19.86.217	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	47
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	47
85.64.235.73	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	47
107.167.104.229	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	46
77.126.104.155	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	45
66.249.78.130	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	44
188.161.48.7	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
81.218.241.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	44
94.159.147.232	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	43
94.159.147.232	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	43
46.19.86.96	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
79.183.135.160	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
2.54.10.50	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	42
5.22.135.66	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	41
2.54.36.122	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	39
46.19.86.35	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
212.76.127.10	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	36
212.235.103.211	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid sequence number	monitor	35

01-24-2016 to 01-25-2016

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.18.53	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	477
37.26.148.132	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	473
188.143.232.22	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.143.232.22	Block	372
176.13.18.53	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	287
185.32.179.30	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	251
37.26.148.132	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 37.26.148.132	Block	237
46.19.85.38	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	234
109.253.150.48	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	227
109.253.150.48	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	220
37.142.64.72	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	205
2.54.187.213	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	193
85.250.183.25	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 85.250.183.25	Block	192
109.253.209.192	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	178
185.32.179.78	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	162
2.54.17.148	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	154
89.139.254.211	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	151
46.19.85.38	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	146
2.52.160.247	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	139
2.52.160.247	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	133
2.54.17.148	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	128
46.19.86.198	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	125
2.54.24.103	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	118
109.253.200.60	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	117
185.32.179.30	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	116
5.28.142.29	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 5.28.142.29	Block	114
89.139.254.211	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	113
2.54.187.213	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	112
46.19.86.198	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	112
37.142.191.52	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	111
176.13.18.165	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	110
46.19.86.32	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	108
37.142.64.72	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
185.32.179.30	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	106
149.78.210.145	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	105
37.26.148.132	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
46.19.85.117	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	103
46.19.86.186	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	102
176.13.18.53	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	101
79.179.134.200	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	100
2.54.162.120	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	98
46.19.85.117	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	97
2.54.24.103	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	96
79.181.104.5	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	96
46.19.86.176	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	95
2.54.189.24	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	89
176.13.1.255	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	89
176.228.71.215	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	86
176.13.22.114	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	86
46.19.85.103	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	81
109.253.141.34	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	80

01-24-2016 to 01-25-2016