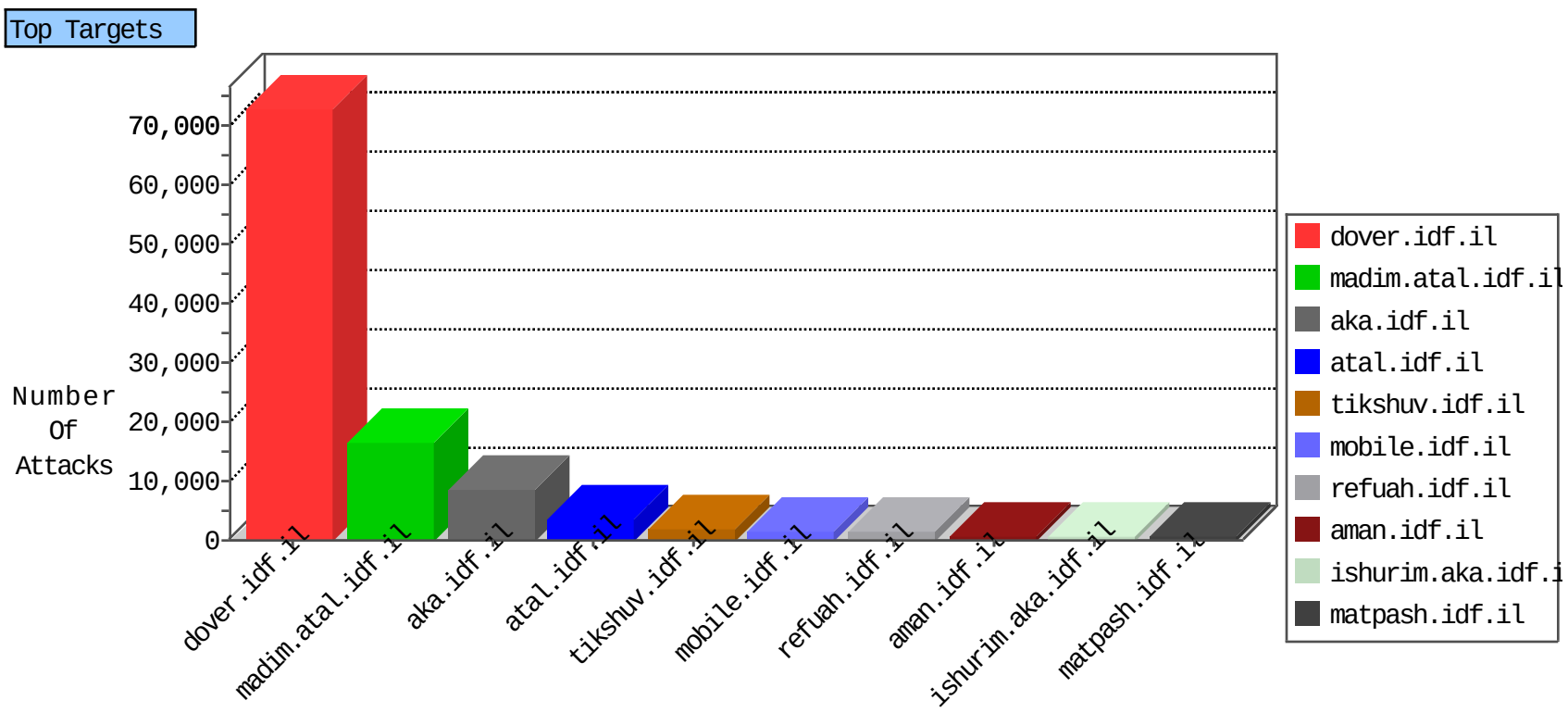
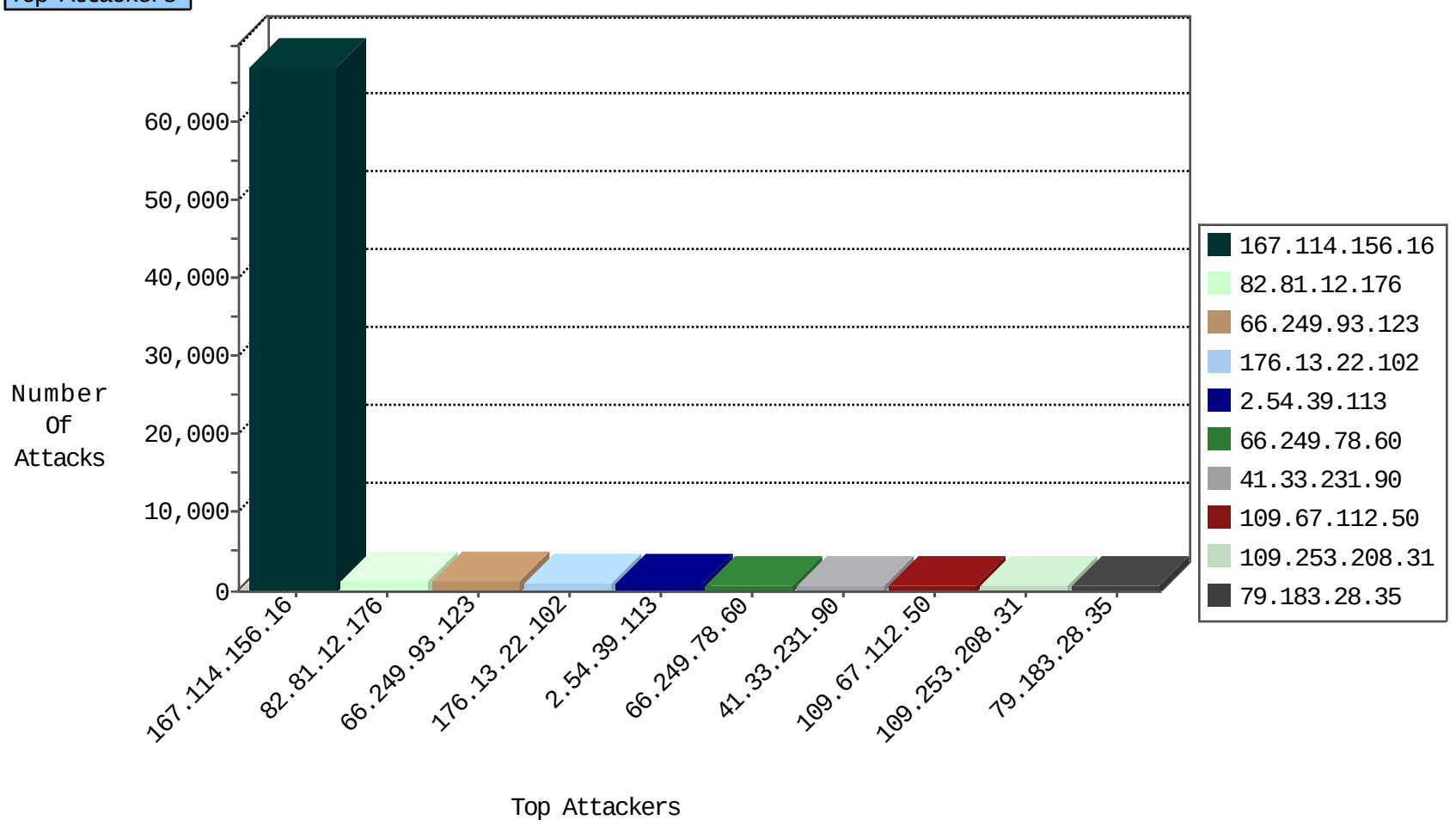
01-25-2016 to 01-26-2016

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-25-2016 to 01-26-2016

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	89318
105.108.43.183	Algeria	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	4197
66.249.78.146	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	2688
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	1446
66.249.78.160	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	694
207.232.36.181	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	438
37.26.146.196	Israel	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	256
81.218.241.26	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	212
80.246.136.151	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	202
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	197
204.93.154.199	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	194
204.93.154.212	United States	147.237.72.166	aka.idf.il	TCP Scan (vertical)	drop	191
81.218.241.26	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	88
80.246.136.151	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	forward	76
134.191.232.69	Israel	147.237.77.233	atal.idf.il	JLM_Purple_Con_Limit_Http	drop	37
213.151.37.196	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	19
109.186.185.69	Israel	147.237.72.166	aka.idf.il	SYN Flood unverified cookie	drop	18
109.186.185.69	Israel	147.237.72.166	aka.idf.il	SYN Flood out of context	drop	18
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	16
24.61.84.129	United States	147.237.72.166	aka.idf.il	SYN Flood unverified cookie	drop	12
8.37.237.22	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
31.168.232.150	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	10
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	9
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	6
109.64.179.249	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
82.132.230.244	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
130.75.174.172	Germany	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	6
82.145.216.174	Europe	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	6
212.179.54.237	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	5
115.230.124.164	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	4
79.179.178.126	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
141.0.15.191	Norway	147.237.77.233	atal.idf.il	Frk_Purple_Con_Limit_Http	drop	3
79.181.167.205	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
109.66.205.39	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
109.67.165.217	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
79.177.179.234	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
54.72.182.187	Ireland	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	3
168.235.197.216	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
54.67.38.74	United States	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	2
115.239.228.10	China	147.237.76.196	e.sviva.idf.il	JLM_Under_Attack_Con_Http	drop	2
66.102.9.10	United States	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	2
8.37.237.250	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
183.60.48.25	China	147.237.76.197	e.himush.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
117.79.146.2	China	147.237.76.196	e.sviva.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
8.37.237.22	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
141.0.15.191	Norway	147.237.77.233	atal.idf.il	Frk_Under_Attack_Con_Http	drop	2
14.105.246.213	China	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	2
79.183.219.19	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
168.235.196.224	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2

01-25-2016 to 01-26-2016

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
110.83.80.161	China	147.237.77.74	law.idf.il	C108: HTTP: Trying to locate existing FCKeditor	Block	8
45.32.83.228		147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	8
110.83.80.161	China	147.237.77.176	matpash.idf.il	C108: HTTP: Trying to locate existing FCKeditor	Block	4
110.83.80.161	China	147.237.77.216	dover.idf.il	C108: HTTP: Trying to locate existing FCKeditor	Block	4
110.83.80.161	China	147.237.77.226	www.chamatz.aka.idf.il	C108: HTTP: Trying to locate existing FCKeditor	Block	4
110.83.80.161	China	147.237.77.233	atal.idf.il	C108: HTTP: Trying to locate existing FCKeditor	Block	4
110.83.80.161	China	147.237.77.170	maarachot.idf.il	C108: HTTP: Trying to locate existing FCKeditor	Block	4
110.83.80.161	China	147.237.77.234	halag.idf.il	C108: HTTP: Trying to locate existing FCKeditor	Block	4
89.132.195.59	Hungary	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	2
45.63.71.182		147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	2
83.97.83.125	Switzerland	147.237.76.42	refuah.idf.il	14331: HTTP: Suspicious User-Agent (My Session)	Block	2
45.32.225.19		147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	2
84.95.200.200	Israel	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	2
23.239.85.119	United States	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
105.108.43.183	Algeria	147.237.77.216	dover.idf.il	19591: HTTP: PHPMoAdmin Code Injection Vulnerability	Block	1
188.214.249.145	Romania	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
177.12.174.145	Brazil	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
80.91.162.99	Ukraine	147.237.72.166	aka.idf.il	C106: HTTP: majestic bot	Block	1
123.126.113.154	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
45.63.70.210		147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
217.131.79.34	Turkey	147.237.72.166	aka.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
105.108.43.183	Algeria	147.237.77.216	dover.idf.il	C107: DDOS-Spoofed HTTP Packets	Block	1
188.165.15.14	France	147.237.76.42	refuah.idf.il	C228: HTTP: AhrefBot crawler	Block	1
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
172.245.218.130	United States	147.237.76.86	navy.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1
40.115.43.204	United States	147.237.0.15	kosher-kravi.idf.il	10711: HTTP: ZmEu Vulnerability Scanner	Block	1
105.108.43.183	Algeria	147.237.77.216	dover.idf.il	19661: HTTP: Wordpress InBoundio Marketing PHP Upload Vulnerability	Block	1
195.234.228.90	Germany	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
177.185.194.92	Brazil	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
80.139.171.157	Germany	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	1
123.126.113.160	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
94.73.145.90	Turkey	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
188.165.15.60	France	147.237.76.31	nakchal.idf.il	C228: HTTP: AhrefBot crawler	Block	1
66.135.63.82	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
172.245.218.130	United States	147.237.77.176	matpash.idf.il	0543: HTTP: php.cgi Access	Block	1
41.101.248.37	Algeria	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
105.108.43.183	Algeria	147.237.77.216	dover.idf.il	19791: HTTP: WordPress N-Media PHP File Upload	Block	1
198.20.69.74	United States	147.237.76.196	e.sviva.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
182.96.195.239	China	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
46.19.86.214	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
158.69.200.204	United States	147.237.72.166	aka.idf.il	C106: HTTP: majestic bot	Block	1
105.108.43.183	Algeria	147.237.77.216	dover.idf.il	19535: HTTP: Maarch Multiple Products File Upload Vulnerability	Block	1
188.165.15.196	France	147.237.72.156	aman.idf.il	C228: HTTP: AhrefBot crawler	Block	1
74.84.136.105	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
172.245.218.130	United States	147.237.77.216	dover.idf.il	0543: HTTP: php.cgi Access	Block	1
198.20.99.130	Netherlands	147.237.8.14	e.orchot.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
105.108.43.183	Algeria	147.237.77.216	dover.idf.il	19792: HTTP: WordPress Work The Flow PHP File Upload	Block	1
185.66.249.87	Netherlands	147.237.72.166	aka.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	1
84.95.200.200	Israel	147.237.72.166	aka.idf.il	C008: HTTP: Xenu UserAgent	Block	1

01-25-2016 to 01-26-2016

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.78.60	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	778
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	61
95.211.70.193	147.237.77.216	Netherlands	dover.idf.il	SQL Injection - Select From	17
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	15
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	9
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	6
95.211.70.193	147.237.77.216	Netherlands	dover.idf.il	ET WEB_SERVER ATTACKER SQLi - SELECT and Schema Columns	6
95.211.70.193	147.237.77.216	Netherlands	dover.idf.il	ET WEB_SERVER SQLi - SELECT and sysobject	5
66.249.78.96	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	4
80.246.136.78	147.237.0.19	Israel	madim.atal.idf.i	ET SCAN Possible SSL Brute Force attack or Site Crawl	4
66.135.63.82	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	4
66.249.81.183	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	4
177.185.194.92	147.237.77.233	Brazil	atal.idf.il	SQL Injection - Select From	3
217.194.206.108	147.237.72.156	Israel	aman.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	3
177.12.174.145	147.237.77.233	Brazil	atal.idf.il	SQL Injection - Select From	3
95.211.70.193	147.237.77.216	Netherlands	dover.idf.il	ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT	3
74.84.136.105	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	3
94.73.145.90	147.237.77.74	Turkey	law.idf.il	SQL Injection - Select From	3
59.45.79.117	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	3
95.211.70.193	147.237.77.216	Netherlands	dover.idf.il	SQL url ending in comment characters - possible sql injection attempt	3
5.102.254.106	147.237.72.156	Israel	aman.idf.il	GPL SCAN myscan	2
95.211.70.193	147.237.77.216	Netherlands	dover.idf.il	SQL generic sql update injection attempt - GET parameter	2
66.249.78.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.62	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
218.246.0.97	147.237.76.196	China	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.78.15	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
41.69.211.48	147.237.77.216	Egypt	dover.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
212.235.98.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
66.249.64.181	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
27.251.16.85	147.237.77.216	India	dover.idf.il	GPL SCAN nmap TCP	2
59.45.79.117	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential SSH Scan	2
82.205.37.170	147.237.77.176	Palestinian Territory, Occupied	matpash.idf.il	ET SCAN NMAP -sA (2)	2
5.102.254.106	147.237.72.156	Israel	aman.idf.il	INDICATOR-SCAN myscan	2
95.211.70.193	147.237.77.216	Netherlands	dover.idf.il	SQL union select - possible sql injection attempt - GET parameter	2
95.211.70.193	147.237.77.216	Netherlands	dover.idf.il	SQL declare varchar - possible SQL injection attempt	2
66.249.78.165	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
59.45.79.117	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	2
95.211.70.193	147.237.77.216	Netherlands	dover.idf.il	INDICATOR-OBFUSCATION large number of calls to char function - possible sql injection obfuscation	2
66.249.78.89	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
95.211.70.193	147.237.77.216	Netherlands	dover.idf.il	ET WEB_SERVER Possible SQL Injection Attempt UPDATE SET	2
66.249.69.76	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
79.179.197.5	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
66.102.8.139	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
94.76.5.177	147.237.76.44	Bahrain	e.refuah.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
82.205.9.67	147.237.77.176	Palestinian Territory, Occupied	matpash.idf.il	ET SCAN NMAP -sA (2)	1
218.246.0.97	147.237.8.46	China	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
62.219.154.185	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.234	147.237.8.14		e.orchot.idf.il	ET SCAN Potential SSH Scan	1
37.143.82.50	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN NMAP -sS window 3072	1
109.186.166.37	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

01-25-2016 to 01-26-2016

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	746
66.249.93.123	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	664
66.249.93.123	United States	147.237.77.233	atal.idf.il	drop		drop	374
79.180.174.86	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	273
64.233.172.198	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	188
46.116.176.101	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	176
77.127.165.76	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	174
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	171
66.249.93.123	United States	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	154
66.249.93.123	United States	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	153
80.246.133.210	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	143
66.249.93.67	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	120
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	111
37.217.186.35	Saudi Arabia	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	110
168.235.197.216	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	100
141.0.15.191	Norway	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	98
80.179.241.10	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	97
100.100.128.69		147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	93
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	92
168.235.196.224	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	90
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	90
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	88
212.76.127.219	Israel	147.237.76.30	himush.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	84
144.172.234.107	Canada	147.237.77.74	law.idf.il	drop	SAM rule	drop	82
66.249.93.127	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	79
196.3.50.254	Switzerland	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	78
144.172.234.107	Canada	147.237.72.156	aman.idf.il	drop	SAM rule	drop	76
66.249.93.127	United States	147.237.77.233	atal.idf.il	drop		drop	73
2.54.47.37	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
2.54.148.112	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	66
68.180.229.94	United States	147.237.0.15	kosher-kravi.idf.i	drop	SAM rule	drop	66
212.76.127.10	Israel	147.237.76.30	himush.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	65
66.249.81.163	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	62
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	57
178.154.189.201	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
46.18.18.254	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	53
5.102.196.71	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	49
109.253.142.45	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
37.26.149.172	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
212.76.127.111	Israel	147.237.76.30	himush.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	45
66.249.93.123	United States	147.237.77.233	atal.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	44
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
66.249.93.67	United States	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	43
79.179.55.205	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
107.167.112.158	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	42
66.249.93.67	United States	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	42
107.167.108.144	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	41
46.121.123.18	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	40
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	39
109.66.200.104	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.22.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	588
2.54.39.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	567
109.67.112.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	481
109.253.208.31	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.208.31	Block	389
46.19.85.35	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	367
79.183.28.35	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	333
109.253.200.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	333
176.13.22.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	328
46.19.85.117	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	327
46.19.86.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	295
80.246.136.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	241
109.67.112.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	239
2.52.166.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	230
79.183.28.35	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	228
2.52.34.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	216
109.253.208.31	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 109.253.208.31	Block	212
79.183.204.72	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	209
2.52.166.124	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.52.166.124	Block	208
109.65.162.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	201
62.219.226.228	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	196
176.13.16.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	196
46.19.85.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	187
2.54.39.113	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 2.54.39.113	Block	186
46.19.86.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	182
109.253.213.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	166
82.102.169.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	151
79.180.163.232	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	148
46.19.85.35	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	147
176.13.22.102	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 176.13.22.102	Block	142
46.19.86.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	141
212.179.21.194	Israel	147.237.72.167	ishurim.aka.idf.i	Too Many of the Same Response Code (404) in Session from 212.179.21.194	Block	135
46.19.85.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	132
46.19.85.117	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	132
79.183.204.72	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	132
46.19.86.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	131
2.52.6.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	129
46.19.85.35	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	128
80.246.136.151	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	127
82.102.169.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	123
80.246.136.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	123
176.13.8.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	120
176.13.8.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	120
84.108.235.32	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	118
109.253.199.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	117
46.19.86.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	117
109.253.199.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	116
46.19.85.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	113
46.19.85.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	113
80.246.136.151	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	113
2.54.39.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	110