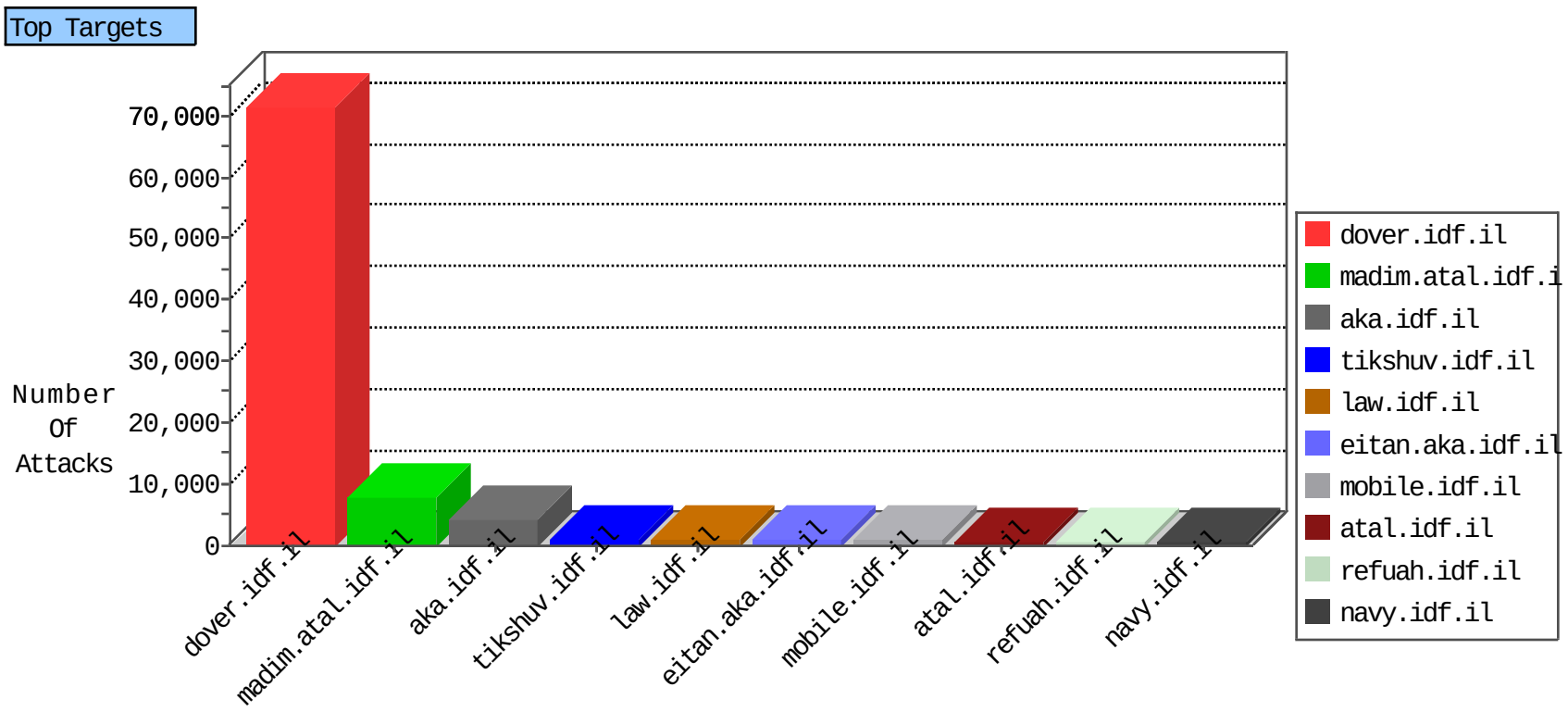
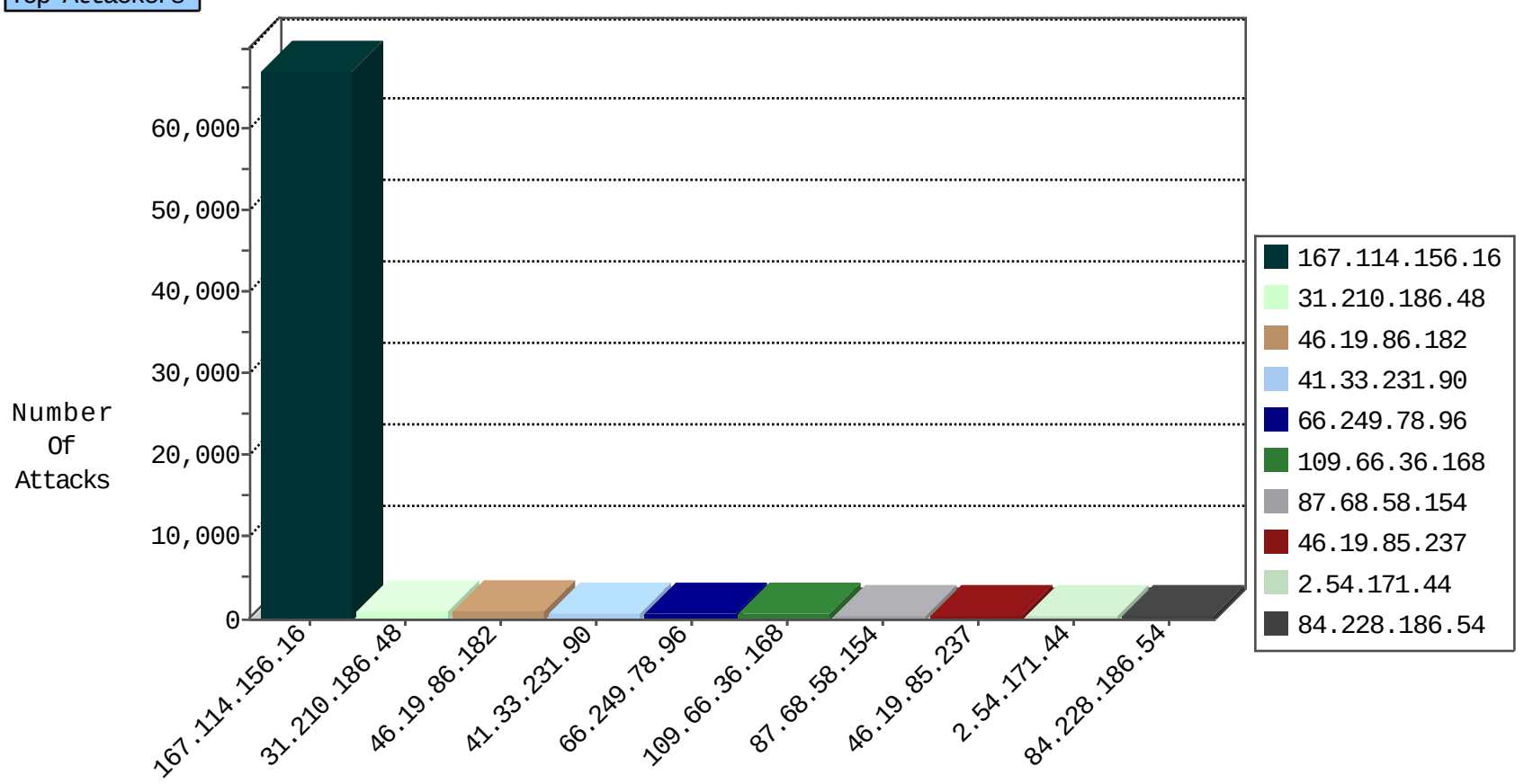
01-23-2016 to 01-24-2016

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-23-2016 to 01-24-2016

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	90085
46.116.161.104	Israel	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	30415
66.249.78.111	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	8737
66.249.78.146	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	4348
85.250.84.227	Israel	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	1809
85.250.84.227	Israel	147.237.72.166	aka.idf.il	TCP Scan (vertical)	drop	1694
66.249.78.97	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1157
66.249.78.104	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	170
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	18
46.19.86.153	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	11
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	9
79.181.167.157	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
79.181.120.205	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	5
66.249.78.166	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
84.109.131.47	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
168.235.196.234	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	4
2.54.13.189	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	4
151.0.151.137	Romania	147.237.0.16	my-kosher-kravi.idf.il	L4 Source or Dest Port Zero	drop	4
84.108.156.56	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
84.108.156.56	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
99.92.92.133	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
46.19.85.174	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
84.108.156.56	Israel	147.237.77.233	atal.idf.il	Block_Udp_All_Nets	drop	3
79.177.197.49	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
115.230.124.164	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	3
87.68.148.57	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
84.108.156.56	Israel	147.237.0.19	madim.atal.idf.il	Block_Udp_All_Nets	drop	3
134.147.203.115	Germany	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	2
183.60.48.25	China	147.237.76.148	gqcenter.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
115.239.228.10	China	147.237.76.30	himush.idf.il	JLM_Under_Attack_Con_Http	drop	2
134.147.203.115	Germany	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
149.78.154.69	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
115.239.228.10	China	147.237.76.177	ncore.idf.il	JLM_Under_Attack_Con_Http	drop	2
78.186.247.27	Turkey	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	2
112.119.174.72	Hong Kong	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	2
66.249.93.182	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	2
168.235.197.212	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
149.255.214.13	Iraq	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	2
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
134.147.203.115	Germany	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	2
115.239.228.10	China	147.237.76.200	eitan.aka.idf.il	JLM_Under_Attack_Con_Http	drop	2
183.60.48.25	China	147.237.0.33	idf.il	Frk_Under_Attack_Con_Tcp	drop	2
71.6.135.131	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets_Con_Limit	drop	2
173.252.90.105	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
134.147.203.115	Germany	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	2
168.235.196.111	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
149.78.48.74	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid TCP Flags	drop	1
89.163.132.132	Germany	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
222.161.223.219	China	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1

01-23-2016 to 01-24-2016

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	5
151.80.31.152	Italy	147.237.76.42	refuah.idf.il	C228: HTTP: AhrefBot crawler	Block	3
198.50.134.71	Canada	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	3
172.245.218.130	United States	147.237.76.42	refuah.idf.il	0543: HTTP: php.cgi Access	Block	2
188.165.225.121	France	147.237.76.86	navy.idf.il	0543: HTTP: php.cgi Access	Block	2
49.246.230.40	China	147.237.77.74	law.idf.il	8479: HTTP: Suspicious HTTP Request	Block	2
23.254.252.225	United States	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	2
172.245.218.130	United States	147.237.77.216	dover.idf.il	0543: HTTP: php.cgi Access	Block	2
151.80.31.154	Italy	147.237.76.42	refuah.idf.il	C228: HTTP: AhrefBot crawler	Block	2
151.80.31.151	Italy	147.237.76.42	refuah.idf.il	C228: HTTP: AhrefBot crawler	Block	2
185.130.5.224		147.237.77.19	law-forum.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	1
84.245.33.104	Netherlands	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
46.252.131.34	Germany	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	1
119.108.155.135	China	147.237.76.39	mobile.meitav.idf.il	C107: DDOS-Spoofed HTTP Packets	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
185.130.5.224		147.237.77.216	dover.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	1
63.143.34.37	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
185.130.5.224		147.237.76.30	himush.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	1
14.104.187.41	China	147.237.77.19	law-forum.idf.il	C107: DDOS-Spoofed HTTP Packets	Block	1
213.247.63.11	Netherlands	147.237.0.34	tikshuv.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
115.163.56.112	Japan	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
188.165.15.162	France	147.237.77.176	matpash.idf.il	C228: HTTP: AhrefBot crawler	Block	1
185.130.5.224		147.237.77.74	law.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	1
93.89.16.110	Turkey	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
188.165.225.121	France	147.237.77.216	dover.idf.il	0543: HTTP: php.cgi Access	Block	1
123.126.113.154	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
185.130.5.224		147.237.77.226	www.chamatz.aka.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	1
66.96.128.60	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
185.130.5.224		147.237.76.39	mobile.meitav.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	1
151.80.31.153	Italy	147.237.76.42	refuah.idf.il	C228: HTTP: AhrefBot crawler	Block	1
218.10.51.147	China	147.237.76.200	eitan.aka.idf.il	C107: DDOS-Spoofed HTTP Packets	Block	1
188.165.15.191	France	147.237.0.34	tikshuv.idf.il	C228: HTTP: AhrefBot crawler	Block	1
116.113.74.159	China	147.237.76.147	chinuch.aka.idf.il	C107: DDOS-Spoofed HTTP Packets	Block	1
185.130.5.224		147.237.77.170	maarachot.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	1
94.192.123.182	United Kingdom	147.237.77.216	dover.idf.il	C001: SCANNER: Havij sql injection scanner	Block	1
51.254.143.240	United Kingdom	147.237.72.166	aka.idf.il	C106: HTTP: majestic bot	Block	1
198.20.69.74	United States	147.237.76.197	e.himush.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
144.76.12.75	Germany	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	1
112.66.35.31	China	147.237.76.86	navy.idf.il	C155: HTTP: OPTIONS methods	Permit	1
188.165.15.19	France	147.237.76.30	himush.idf.il	C228: HTTP: AhrefBot crawler	Block	1
76.29.80.211	United States	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	1
185.130.5.224		147.237.76.86	navy.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	1
46.137.81.122	Ireland	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
218.10.62.192	China	147.237.76.147	chinuch.aka.idf.il	C155: HTTP: OPTIONS methods	Permit	1
188.165.15.204	France	147.237.76.30	himush.idf.il	C228: HTTP: AhrefBot crawler	Block	1
119.97.146.76	China	147.237.77.216	dover.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
185.130.5.224		147.237.77.176	matpash.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	1
106.7.248.43	China	147.237.77.19	law-forum.idf.il	C155: HTTP: OPTIONS methods	Permit	1

01-23-2016 to 01-24-2016

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.78.96	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	809
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	94
149.78.48.74	147.237.72.167	Israel	ishurim.aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	24
85.250.84.227	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sS window 1024	9
66.249.78.104	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	8
66.249.66.12	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	6
66.249.78.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	4
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	4
31.210.186.48	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	4
66.249.78.9	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	4
66.249.64.50	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	4
66.249.78.111	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	4
66.249.75.214	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	4
163.172.13.173	147.237.72.166	United Kingdom	aka.idf.il	ET SCAN NMAP -sS window 1024	4
46.137.81.122	147.237.77.216	Ireland	dover.idf.il	SQL Injection - Select From	3
66.96.128.60	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	3
200.59.205.238	147.237.76.86	Argentina	navy.idf.il	SQL Injection - Select From	3
84.245.33.104	147.237.77.216	Netherlands	dover.idf.il	SQL Injection - Select From	3
63.143.34.37	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	3
213.151.32.163	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
66.249.66.39	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.66.15	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
66.249.93.123	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.133	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	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.153	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
85.250.84.227	147.237.77.216	Israel	dover.idf.il	ET SCAN NMAP -sS window 1024	2
27.251.16.85	147.237.77.216	India	dover.idf.il	GPL SCAN nmap TCP	2
79.177.168.107	147.237.77.233	Israel	atal.idf.il	ET SCAN NMAP -sA (2)	2
213.247.63.11	147.237.0.34	Netherlands	tikshuv.idf.il	SQL Injection - Select From	2
66.249.66.129	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.66.21	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
66.249.93.127	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
66.249.93.32	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
162.222.185.165	147.237.76.44	United States	e.refuah.idf.il	ET SCAN Potential SSH Scan	2
117.21.248.87	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	2
85.250.84.227	147.237.72.166	Israel	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
59.45.79.117	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.97	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
79.182.51.17	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
59.45.79.117	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.79	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
174.37.194.144	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
91.201.236.113	147.237.76.199	Ukraine	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	1
193.201.227.18	147.237.76.38	Ukraine	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
159.122.111.166	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
105.228.102.141	147.237.0.16	South Africa	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
78.193.2.8	147.237.0.33	France	idf.il	ET SCAN NMAP -sS window 1024	1
50.204.188.142	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -f -sS	1

01-23-2016 to 01-24-2016

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	828
5.22.135.190	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	345
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	339
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	273
62.0.73.129	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	234
168.235.196.234	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	150
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	131
168.235.197.212	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	119
168.235.196.111	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	119
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	112
5.108.145.176	Saudi Arabia	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	105
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	94
157.55.39.168	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	87
79.181.209.136	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	81
2.54.13.189	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	67
217.132.235.50	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
109.253.135.189	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
157.55.39.169	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
46.120.162.164	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	53
212.179.102.136	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	50
212.179.102.136	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	50
66.249.66.188	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
46.19.86.137	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	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
79.176.53.162	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
213.57.160.89	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	44
212.179.102.136	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	40
176.13.11.146	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	40
176.13.20.146	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
109.160.189.28	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	35
109.160.189.28	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	35
79.179.151.160	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	35
46.19.86.91	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	35
66.249.69.122	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	34
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
212.76.127.219	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	33
85.250.188.220	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	33
85.250.211.101	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	32
149.88.8.214	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	32
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	32
157.55.39.114	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	32
5.28.158.181	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	30
80.178.6.32	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	28
185.120.125.32		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
80.178.6.32	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	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
5.28.184.202	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	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
41.103.71.57	Algeria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	25

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
31.210.186.48	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	672
46.19.86.182	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.86.182	Block	605
109.66.36.168	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	374
46.19.85.237	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.85.237	Block	311
46.19.86.182	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	311
87.68.58.154	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	305
31.210.186.48	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	264
2.54.171.44	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.54.171.44	Block	221
84.228.186.54	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	208
79.176.118.20	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	205
79.177.170.249	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	187
176.13.5.10	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	179
79.179.210.139	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	168
2.54.171.44	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	157
46.19.85.237	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	157
31.210.186.48	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	148
46.19.86.161	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	144
109.66.36.168	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	136
84.109.39.134	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	136
87.68.58.154	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	132
176.13.5.10	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	131
46.19.86.161	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	121
79.177.188.58	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	118
87.68.37.219	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	118
149.88.38.76	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	112
84.228.186.54	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 84.228.186.54	Block	111
84.228.186.54	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	110
87.68.37.219	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
79.182.100.146	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 79.182.100.146	Block	105
79.176.118.20	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
87.68.58.154	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
109.66.36.168	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
79.179.210.139	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	89
46.19.85.93	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	88
109.253.193.38	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	78
176.13.23.160	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	77
85.130.240.235	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	76
5.22.135.236	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	74
87.69.200.34	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	72
46.120.41.162	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 46.120.41.162	Block	70
109.160.165.195	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	69
89.138.65.130	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	68
2.54.171.44	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 2.54.171.44	Block	67
2.54.180.13	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	65
46.19.86.115	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	65
89.139.169.5	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	62
213.8.204.19	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 213.8.204.19	Block	58
149.88.38.76	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	55
87.68.37.219	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	55
2.54.42.226	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	51