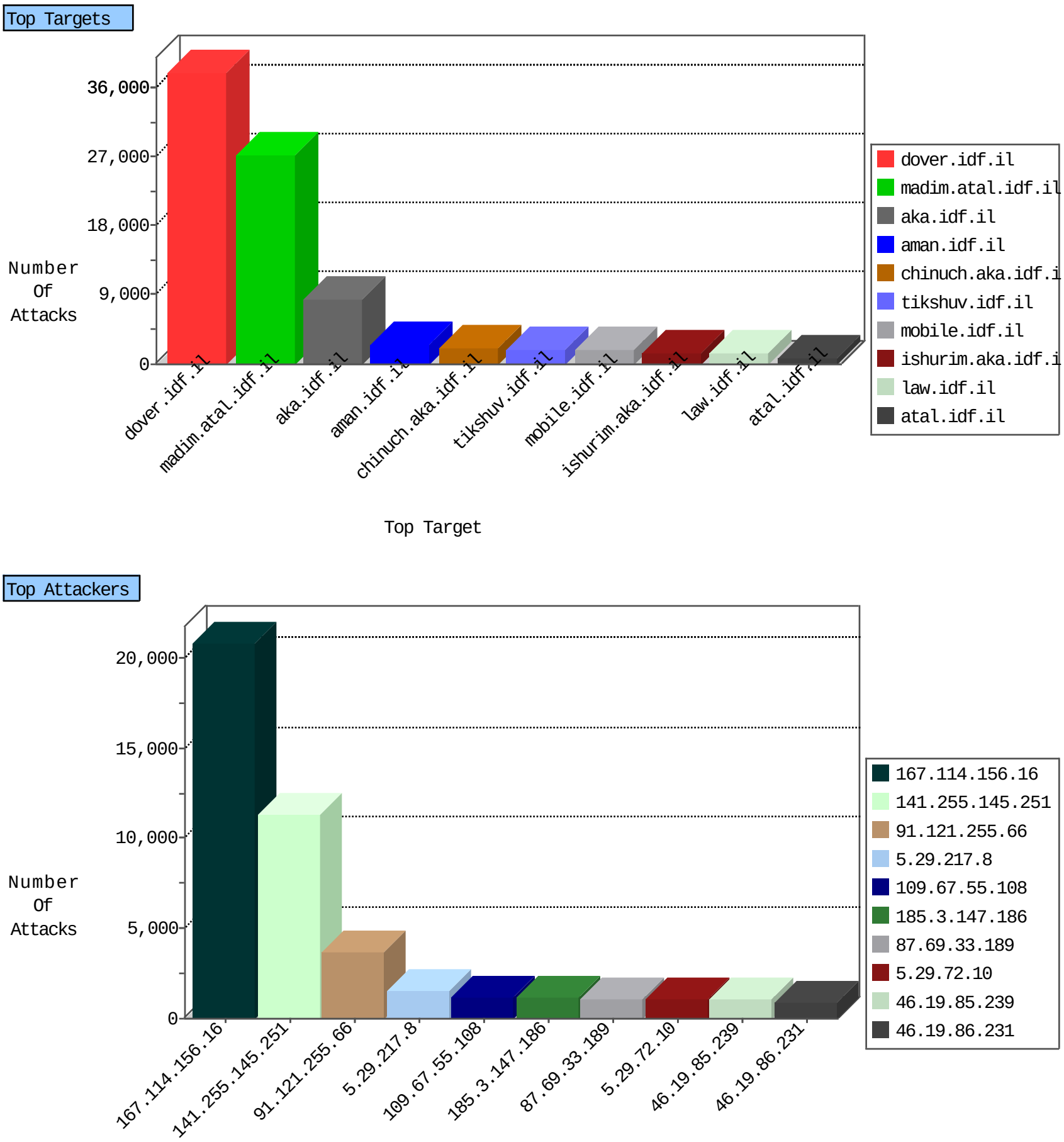
01-26-2016 to 01-27-2016

IDF Under Attack
Daily Report



01-26-2016 to 01-27-2016

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	27490
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	4441
141.255.145.251	Netherlands	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	4018
141.255.145.251	Netherlands	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3768
141.255.145.251	Netherlands	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	1747
66.249.78.160	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1247
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	837
66.249.78.146	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	558
141.255.145.251	Netherlands	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	518
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	368
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	308
212.199.112.144	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	307
66.249.78.104	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	248
204.93.154.211	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	194
46.19.86.117	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	134
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	134
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	44
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	37
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	10
149.88.132.247	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
201.46.158.229	Brazil	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
93.174.93.132	Netherlands	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	8
216.185.39.80	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
58.58.183.2	China	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	6
49.80.254.226	China	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	6
84.108.204.65	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
109.65.117.248	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
80.246.139.102	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	6
109.65.6.68	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	5
101.228.246.121	China	147.237.76.199	e.nakchal.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
183.142.131.166	China	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	5
66.249.78.173	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
14.209.240.45	China	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	5
180.118.31.168	China	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	4
60.181.28.172	China	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	4
120.39.148.218	China	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	4
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
216.170.126.191	United States	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-Url	dest-reset	4
58.45.121.27	China	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	4
85.130.251.227	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
96.245.39.39	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
198.58.102.158	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
109.65.6.68	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
81.218.206.82	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
79.181.147.158	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
81.218.206.82	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
79.181.147.158	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
118.248.41.23	China	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	3

01-26-2016 to 01-27-2016

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
94.76.10.253	Bahrain	147.237.77.205	prisha.idf.il	C107: DDOS-Spoofed HTTP Packets	Block	4
24.108.170.158	Canada	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	4
198.50.134.71	Canada	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	3
84.111.208.176	Israel	147.237.72.166	aka.idf.il	14062: HTTP: SpamBlockerUtility Fake Anti-Spyware User-Agent (SpamBlockerUtility x.x.x)	Block	2
89.132.195.59	Hungary	147.237.72.166	aka.idf.il	C008: HTTP: Xenu UserAgent	Block	2
77.248.12.153	Netherlands	147.237.76.42	refuah.idf.il	14331: HTTP: Suspicious User-Agent (My Session)	Block	2
42.101.154.233	China	147.237.77.216	dover.idf.il	13764: HTTP: China Chopper Malware Communication Attempt	Block	2
81.100.56.209	United Kingdom	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	1
191.232.39.241	United States	147.237.77.176	matpash.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	1
46.19.86.137	Israel	147.237.77.216	dover.idf.il	12890: TCP: Windows TCP/IP Denial-of-Service Vulnerability (ONLY enable when under DoS attack)	Block	1
162.210.196.97	United States	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	1
92.241.44.198	Jordan	147.237.0.34	tikshuv.idf.il	0361: HTTP: Protected File Access (/etc/passwd)	Block	1
69.30.214.46	United States	147.237.72.166	aka.idf.il	C106: HTTP: majestic bot	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
2.54.181.237	Israel	147.237.72.156	aman.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
188.165.15.49	France	147.237.72.167	ishurim.aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1
94.76.10.253	Bahrain	147.237.77.216	dover.idf.il	C107: DDOS-Spoofed HTTP Packets	Block	1
191.232.39.241	United States	147.237.77.216	dover.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	1
52.1.90.117	United States	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
176.33.137.159	Turkey	147.237.72.166	aka.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
92.241.44.198	Jordan	147.237.0.34	tikshuv.idf.il	0363: HTTP: Protected File Access (/etc/motd)	Permit	1
74.84.136.105	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
216.177.128.57	United States	147.237.77.216	dover.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
5.9.85.4	Germany	147.237.72.166	aka.idf.il	C106: HTTP: majestic bot	Block	1
188.165.15.75	France	147.237.0.15	kosher-kravi.idf.i	C228: HTTP: AhrefBot crawler	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
85.250.187.143	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
195.234.228.90	Germany	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
176.58.117.133	United Kingdom	147.237.0.34	tikshuv.idf.il	3885: HTTP: PHP File Include Exploit	Block	1
92.241.44.198	Jordan	147.237.0.34	tikshuv.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1
74.115.1.68	Anonymous Proxy	147.237.77.216	dover.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
216.249.107.200	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
188.165.15.176	France	147.237.77.74	law.idf.il	C228: HTTP: AhrefBot crawler	Block	1
123.125.125.30	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
198.20.69.74	United States	147.237.76.202	e.halag.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
62.109.7.46	Russian Federation	147.237.77.216	dover.idf.il	C196: HTTP: Block admin login to gov.il sites ?q=user	Block	1
184.173.50.36	United States	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
92.241.44.198	Jordan	147.237.77.216	dover.idf.il	13444: HTTP: WhatWeb User-Agent Header	Block	1
188.165.15.177	France	147.237.77.170	maarachot.idf.il	C228: HTTP: AhrefBot crawler	Block	1
136.243.103.165	Germany	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	1
92.241.44.198	Jordan	147.237.0.34	tikshuv.idf.il	0345: HTTP: Shell Command Execution (uname -a)	Block	1
66.176.172.168	United States	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
188.165.15.37	France	147.237.77.233	atal.idf.il	C228: HTTP: AhrefBot crawler	Block	1

01-26-2016 to 01-27-2016

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.19.85.152	147.237.76.31	Israel	nakchal.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	119
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	63
46.19.85.142	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	18
212.199.57.192	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	16
213.204.101.24	147.237.76.30	Lebanon	himush.idf.il	ET SCAN NMAP -sA (2)	10
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	9
80.246.130.225	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	7
46.19.86.49	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	6
31.44.135.165	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	5
66.249.78.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	4
216.249.107.200	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	4
94.76.14.237	147.237.76.176	Bahrain	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	4
94.76.10.253	147.237.77.226	Bahrain	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	3
94.76.10.253	147.237.77.216	Bahrain	dover.idf.il	ET SCAN NMAP -sS window 1024	3
85.233.76.49	147.237.77.74	Russian Federation	law.idf.il	Tehila - Perl LWP with fake user agent	3
94.76.10.253	147.237.76.198	Bahrain	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	3
80.246.139.102	147.237.77.216	Israel	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	2
66.249.83.125	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
183.60.48.25	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
109.253.206.187	147.237.0.19	Israel	madim.atal.idf.il	GPL SCAN myscan	2
80.82.79.104	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	2
59.45.79.117	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	2
81.202.58.210	147.237.77.234	Spain	halag.idf.il	ET SCAN Potential SSH Scan	2
218.246.0.97	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	2
208.80.155.224	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	2
5.22.131.72	147.237.77.216	Israel	dover.idf.il	GPL SCAN myscan	2
27.251.16.85	147.237.77.216	India	dover.idf.il	GPL SCAN nmap TCP	2
59.45.79.117	147.237.77.233	China	atal.idf.il	ET SCAN Potential SSH Scan	2
46.19.86.74	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
59.45.79.117	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	2
66.249.93.140	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
92.241.44.198	147.237.0.34	Jordan	tikshuv.idf.il	SQL xp_cmdshell attempt	2
163.172.13.173	147.237.72.166	United Kingdom	aka.idf.il	ET SCAN NMAP -sS window 1024	2
183.60.48.25	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
66.249.78.159	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
109.253.206.187	147.237.0.19	Israel	madim.atal.idf.il	INDICATOR-SCAN myscan	2
66.249.78.79	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
108.60.209.3	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	2
81.202.58.210	147.237.8.28	Spain	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	2
59.45.79.117	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	2
212.86.219.134	147.237.77.170	Germany	maarachot.idf.il	Tehila - Perl LWP with fake user agent	2
66.249.78.9	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
84.94.158.134	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
5.22.131.72	147.237.77.216	Israel	dover.idf.il	INDICATOR-SCAN myscan	2
59.45.79.117	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	2
59.45.79.117	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	1
113.171.23.126	147.237.76.177	Vietnam	ncore.idf.il	ET SCAN Potential SSH Scan	1
42.119.247.121	147.237.76.42	Vietnam	refuah.idf.il	ET SCAN NMAP -sS window 4096	1
94.76.10.253	147.237.76.196	Bahrain	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1

01-26-2016 to 01-27-2016

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
141.255.145.251	Netherlands	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3421
141.255.145.251	Netherlands	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2920
141.255.145.251	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2270
91.121.255.66	France	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1787
91.121.255.66	France	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1592
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	786
84.94.22.10	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	780
141.255.145.251	Netherlands	147.237.77.216	dover.idf.il	drop		drop	739
5.29.217.8	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	658
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	435
54.173.9.10	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	317
52.0.86.232	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	285
91.121.255.66	France	147.237.76.147	chinuch.aka.idf.il	SYN Attack		reject	222
93.174.93.132	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	186
94.76.10.253	Bahrain	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	182
54.173.9.10	United States	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	172
141.255.145.251	Netherlands	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	165
64.22.71.223	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	150
176.2.34.129	Germany	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	135
141.255.145.251	Netherlands	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	134
52.7.32.143	United States	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	133
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	119
94.76.10.253	Bahrain	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	115
66.102.6.77	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	115
54.85.198.156	United States	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	101
64.22.71.223	United States	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	100
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	91
84.228.158.52	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
168.235.196.204	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	87
66.249.69.30	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	84
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	82
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	74
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	73
94.76.14.237	Bahrain	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	64
109.64.81.123	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	63
84.94.158.140	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	63
81.218.60.42	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	61
66.102.6.80	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	59
209.200.29.36	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	59
209.200.29.36	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	59
148.251.130.181	Germany	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	58
148.251.130.181	Germany	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	58
213.8.245.58	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	57
82.166.232.129	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	54
37.26.148.237	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	54
46.19.85.177	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
46.120.17.104	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
85.130.254.113	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	53
37.26.149.214	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	53
37.26.149.214	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	53

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.29.217.8	Israel	147.237.72.166	aka.idf.il	Automated Vulnerability Scanning	Block	847
109.67.55.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	674
46.19.86.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	615
185.3.147.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	611
5.29.72.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	611
46.19.85.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	587
87.69.33.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	524
87.69.33.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	491
46.19.85.198	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	397
5.29.72.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	371
2.54.22.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	307
77.126.94.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	307
185.3.147.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	300
109.67.55.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	279
46.121.27.64	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	274
2.54.33.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	268
46.19.85.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	263
37.142.68.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	260
109.253.199.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	258
109.67.55.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	256
95.35.153.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	241
46.121.27.64	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	237
46.19.86.226	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	231
2.52.40.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	220
185.3.147.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	214
95.35.153.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	212
194.90.88.105	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	211
46.19.86.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	208
109.253.199.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	208
176.13.18.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	205
46.19.86.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	203
46.19.85.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	199
2.54.22.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	194
46.19.86.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	185
2.54.143.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	184
109.253.156.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	182
2.54.143.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	179
2.52.173.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	176
109.253.158.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	175
176.13.19.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	174
176.13.20.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	170
185.32.179.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	166
46.19.86.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	166
2.54.40.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	164
2.52.173.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	164
2.54.142.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	161
80.246.136.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	161
2.54.36.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	161
77.126.94.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	158
46.19.86.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	155

01-26-2016 to 01-27-2016