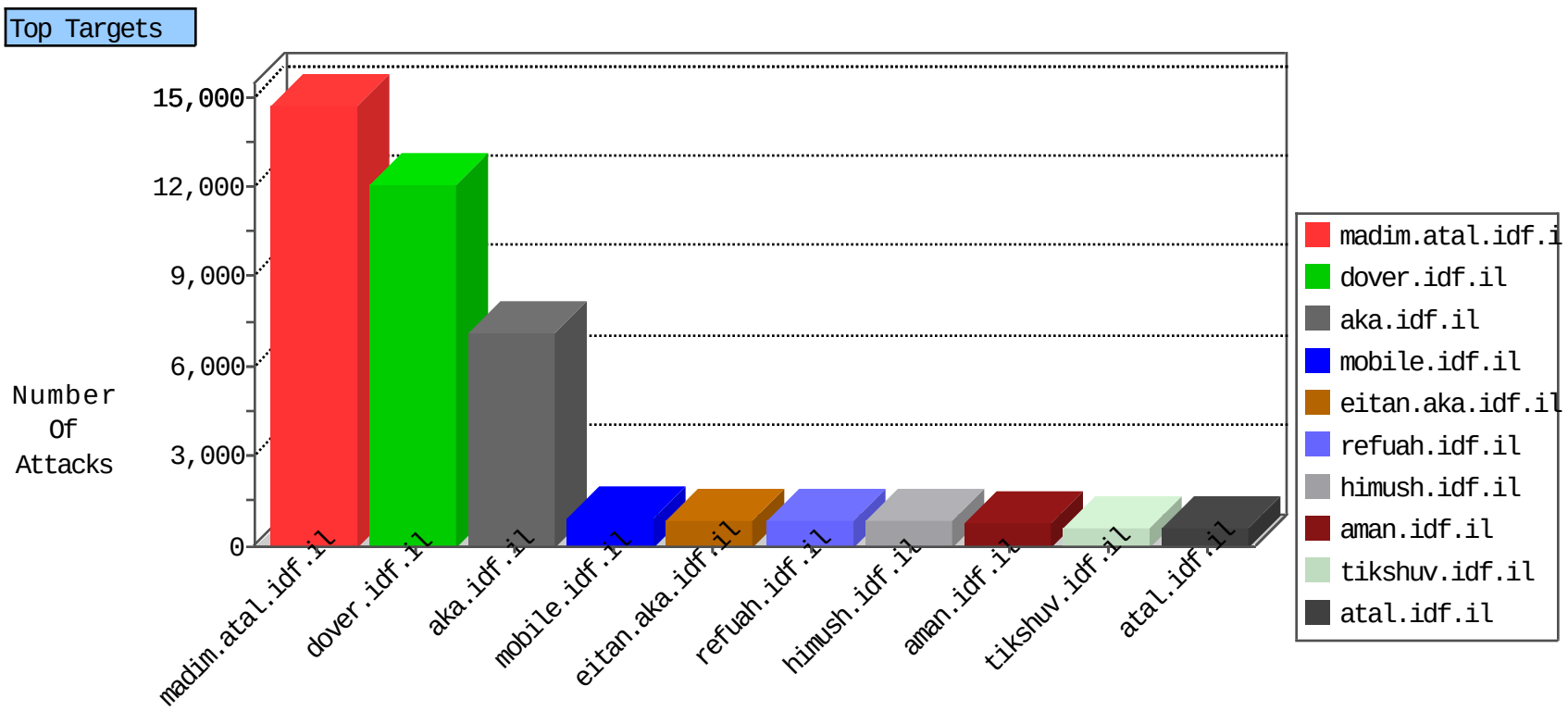
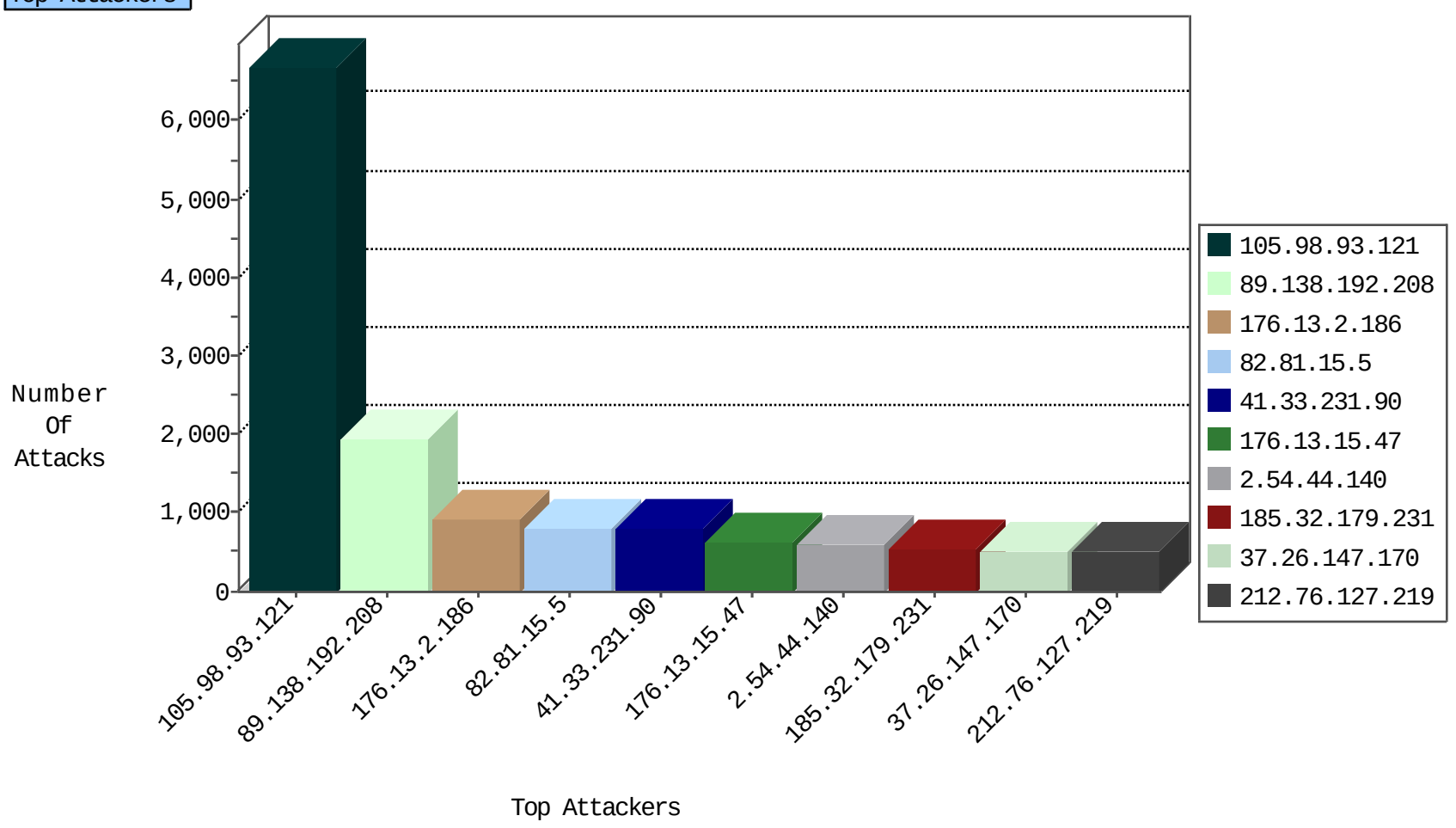
02-09-2016 to 02-10-2016

IDF Under Attack
Daily Report

Top Targets



Top Attackers



02-09-2016 to 02-10-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
105.98.93.121	Algeria	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	8061
105.98.93.121	Algeria	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3709
66.249.79.127	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2906
105.98.93.121	Algeria	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	503
212.199.112.144	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	241
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	232
2.54.36.162	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	219
82.166.137.19	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	157
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	120
81.218.241.25	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	98
91.231.193.150	Israel	147.237.76.42	refuah.idf.il	JLM_Purple_Con_Limit_Http	drop	51
79.179.195.92	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	51
66.249.64.171	Israel	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	43
66.249.79.75	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	34
69.22.187.155	Anonymous Proxy	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	33
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	30
109.67.50.138	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	27
212.126.112.171	Iraq	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	18
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	17
212.126.112.171	Iraq	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	14
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	10
66.249.79.77	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
109.67.136.152	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
84.110.211.103	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	6
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	6
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
84.111.164.157	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
109.67.127.155	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
188.138.57.11	Germany	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	5
188.138.57.11	Germany	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	5
66.249.81.212	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
104.131.226.73	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
105.98.93.121	Algeria	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
217.31.54.202	Czech Republic	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
105.224.174.217	South Africa	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
188.138.57.11	Germany	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	4
69.171.230.98	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
31.168.240.21	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
157.55.39.39	United States	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	3
185.75.56.139		147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	3
212.25.121.195	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
37.26.146.182	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
82.81.12.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
173.252.88.94	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
81.218.206.82	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
151.1.182.98	Italy	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
81.218.105.235	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2

02-09-2016 to 02-10-2016

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
197.41.23.12	Egypt	147.237.77.216	dover.idf.il	3886: HTTP: Cross Site Scripting in POST Request	Block	4
172.246.104.194	United States	147.237.77.233	atal.idf.il	0543: HTTP: php.cgi Access	Block	3
77.127.253.212	Israel	147.237.77.216	dover.idf.il	C017: HTTP: Malicous UserAgent FOCA	Block	3
41.100.105.185	Algeria	147.237.77.216	dover.idf.il	C091: HTTP: Access to - admin.asp	Block	2
89.216.115.8		147.237.77.216	dover.idf.il	17272: HTTP: Suspicious User-Agent (WindowsNT) With No Separating Space	Block	2
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	2
172.246.104.194	United States	147.237.77.216	dover.idf.il	0543: HTTP: php.cgi Access	Block	2
52.33.227.96	United States	147.237.77.216	dover.idf.il	17272: HTTP: Suspicious User-Agent (WindowsNT) With No Separating Space	Block	2
188.165.15.87	France	147.237.77.233	atal.idf.il	C228: HTTP: AhrefBot crawler	Block	1
70.89.127.77	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
151.80.31.133	Italy	147.237.77.176	matpash.idf.il	C228: HTTP: AhrefBot crawler	Block	1
96.47.2.10	United States	147.237.0.34	tikshuv.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
78.173.195.2	Turkey	147.237.72.166	aka.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
209.15.196.170	Canada	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
62.210.225.135	France	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
111.69.150.143	New Zealand	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
89.38.209.50	Romania	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
188.165.15.169	France	147.237.72.156	aman.idf.il	C228: HTTP: AhrefBot crawler	Block	1
70.89.127.77	United States	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	1
45.63.97.227		147.237.72.166	aka.idf.il	C041: HTTP: Access to - index.php?option=com_jce	Block	1
155.94.254.143	United States	147.237.0.17	m.my-kosher-kravi.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1
98.19.222.133	United States	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
79.231.114.143	Germany	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	1
64.31.44.6	United States	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
184.173.233.226	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
123.26.251.210	Vietnam	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
23.91.70.51	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
188.165.15.235	France	147.237.72.166	aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1
70.89.127.78	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
45.63.97.227		147.237.77.74	law.idf.il	C041: HTTP: Access to - index.php?option=com_jce	Block	1
155.94.254.143	United States	147.237.76.200	eitan.aka.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1
103.21.58.191	India	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
83.246.206.218	Russian Federation	147.237.8.46	e.chinuch.idf.il	13891: TLS: OpenSSL Encrypted/Unencrypted Heartbeat Packet	Permit	1
185.130.5.207		147.237.76.31	nakchal.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
66.76.174.2	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
123.125.125.79	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
38.87.46.138	United States	147.237.77.176	matpash.idf.il	C008: HTTP: Xenu UserAgent	Block	1
95.8.21.149	Turkey	147.237.77.216	dover.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
195.245.194.62	Latvia	147.237.72.166	aka.idf.il	3630: HTTP: SQL Injection (Boolean Identity)	Block	1
74.84.136.105	United States	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
105.98.93.121	Algeria	147.237.77.216	dover.idf.il	12026: HTTP: LOIC DDoS Tool (ONLY enable when under DoS attack)	Block	1
85.203.16.57	Netherlands	147.237.77.176	matpash.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
188.165.15.85	France	147.237.76.31	nakchal.idf.il	C228: HTTP: AhrefBot crawler	Block	1
66.96.128.60	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
128.69.30.132	Russian Federation	147.237.77.61	e.cogat.idf.il	13891: TLS: OpenSSL Encrypted/Unencrypted Heartbeat Packet	Permit	1
38.87.46.138	United States	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
95.211.213.213	Netherlands	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
172.246.104.194	United States	147.237.77.216	dover.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1
106.38.241.106	China	147.237.77.170	maarachot.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
87.106.179.116	Germany	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

02-09-2016 to 02-10-2016

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	69
66.249.81.175	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	33
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	12
93.173.250.234	147.237.77.216	Israel	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	9
98.19.222.133	147.237.77.216	United States	dover.idf.il	SQL Injection - Select From	8
184.173.233.226	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	7
70.89.127.77	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	6
37.26.147.170	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	6
197.41.23.12	147.237.77.216	Egypt	dover.idf.il	GPL WEB_SERVER /etc/passwd	4
66.249.64.171	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	4
66.249.74.105	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	4
197.41.23.12	147.237.77.216	Egypt	dover.idf.il	SQL Injection - Select From	4
66.96.128.60	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	4
62.210.225.135	147.237.72.166	France	aka.idf.il	SQL Injection - Select From	4
209.15.196.170	147.237.77.74	Canada	law.idf.il	SQL Injection - Select From	3
103.21.58.191	147.237.77.233	India	atal.idf.il	SQL Injection - Select From	3
23.91.70.51	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	3
82.80.196.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	3
66.249.79.10	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	3
74.84.136.105	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	3
93.173.250.234	147.237.76.86	Israel	navy.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	3
70.89.127.78	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	3
89.38.209.50	147.237.77.74	Romania	law.idf.il	SQL Injection - Select From	3
66.249.69.77	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	2
77.127.174.110	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	2
121.201.27.61	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	2
43.252.228.61	147.237.76.42	Japan	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
66.249.64.233	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
59.45.79.117	147.237.77.205	China	prisha.idf.il	ET SCAN Potential SSH Scan	2
207.241.229.103	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	2
59.45.79.117	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	2
66.76.174.2	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	2
66.249.81.204	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
66.249.79.127	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
209.126.116.147	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 1024	2
96.47.2.10	147.237.0.34	United States	tikshuv.idf.il	SQL Injection - Select From	2
66.249.66.33	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.181	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
52.16.5.197	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	2
218.246.0.97	147.237.76.177	China	ncore.idf.il	ET SCAN NMAP -sS window 1024	2
64.31.44.6	147.237.77.216	United States	dover.idf.il	SQL Injection - Select From	2
59.45.79.117	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	2
89.244.231.130	147.237.77.74	Germany	law.idf.il	ET SCAN Potential SSH Scan	2
31.168.78.146	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
66.249.79.75	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
95.86.78.254	147.237.76.86	Israel	navy.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
74.73.166.84	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	2
79.183.202.132	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.201.227.65	147.237.76.44	Ukraine	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
149.78.154.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

02-09-2016 to 02-10-2016

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
105.98.93.121	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4065
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	764
212.76.127.219	Israel	147.237.76.30	himush.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	372
41.100.105.185	Algeria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	280
212.143.134.129	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	240
105.98.93.121	Algeria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	228
109.65.119.196	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	141
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	135
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	122
2.54.163.223	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	120
132.66.237.27	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	105
212.76.127.10	Israel	147.237.76.30	himush.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	102
176.13.20.21	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	96
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	91
79.182.112.246	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	84
8.37.225.14	Anonymous Proxy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	83
92.241.38.120	Jordan	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	81
207.241.229.103	United States	147.237.72.166	aka.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	81
192.116.218.93	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	71
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	71
8.37.225.14	Anonymous Proxy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	71
8.37.226.24	Anonymous Proxy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	70
109.64.193.167	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	65
212.235.22.215	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	55
79.176.224.43	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
105.98.93.121	Algeria	147.237.77.216	dover.idf.il	SYN Attack		reject	53
85.65.100.83	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	50
62.0.200.202	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	46
79.177.174.203	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	43
8.37.226.24	Anonymous Proxy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	41
192.116.218.93	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	40
212.126.112.166	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
212.76.127.10	Israel	147.237.77.226	www.chamatz.aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	36
31.168.240.21	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
2.52.9.63	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	36
128.194.131.235	United States	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	36
46.19.86.109	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
82.145.216.138	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	35
205.155.141.254	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
109.253.217.252	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
149.78.30.23	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	31
212.126.112.171	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
46.19.86.110	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
2.52.150.22	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
128.194.131.235	United States	147.237.72.166	aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	30
212.76.127.111	Israel	147.237.76.30	himush.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	30
109.253.146.232	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
37.26.148.253	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
31.168.126.163	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
212.76.127.44	Israel	147.237.76.30	himush.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	27

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.138.192.208	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	1202
176.13.2.186	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	579
89.138.192.208	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	569
82.81.15.5	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	444
2.54.44.140	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	348
176.13.15.47	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	310
185.32.179.231	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	307
46.19.85.37	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	283
2.54.184.118	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	269
37.26.147.170	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 37.26.147.170	Block	263
109.253.129.142	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	238
80.246.136.33	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	232
2.54.46.132	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.54.46.132	Block	224
176.13.2.186	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	216
176.13.15.47	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	211
37.26.149.156	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	209
2.54.36.162	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.54.36.162	Block	207
176.13.2.235	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	202
46.19.85.37	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	201
82.81.15.5	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 82.81.15.5	Block	199
89.138.192.208	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	173
80.246.136.194	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	171
37.26.149.156	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	170
176.13.2.235	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	163
79.182.7.37	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 79.182.7.37	Block	163
82.81.15.5	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	160
2.54.36.162	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	155
37.26.147.147	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	154
185.32.179.231	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	143
2.54.46.132	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	140
46.19.85.46	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	136
2.54.44.140	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 2.54.44.140	Block	135
46.19.86.157	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	133
176.13.2.186	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	130
37.26.147.170	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	126
2.54.184.118	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	124
80.246.136.33	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	121
46.19.86.157	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	121
79.182.7.37	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	119
212.76.127.219	Israel	147.237.76.30	himush.idf.il	Distributed Too Many of the Same Response Code (404)	Block	118
37.26.147.170	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 37.26.147.170	Block	118
46.19.85.46	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.85.46	Block	117
176.13.15.47	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	115
37.142.209.244	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	111
79.178.189.229	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 79.178.189.229	Block	110
109.253.157.178	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	110
109.253.146.62	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	110
37.142.209.244	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 37.142.209.244	Block	109
109.253.129.142	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
109.253.211.98	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107