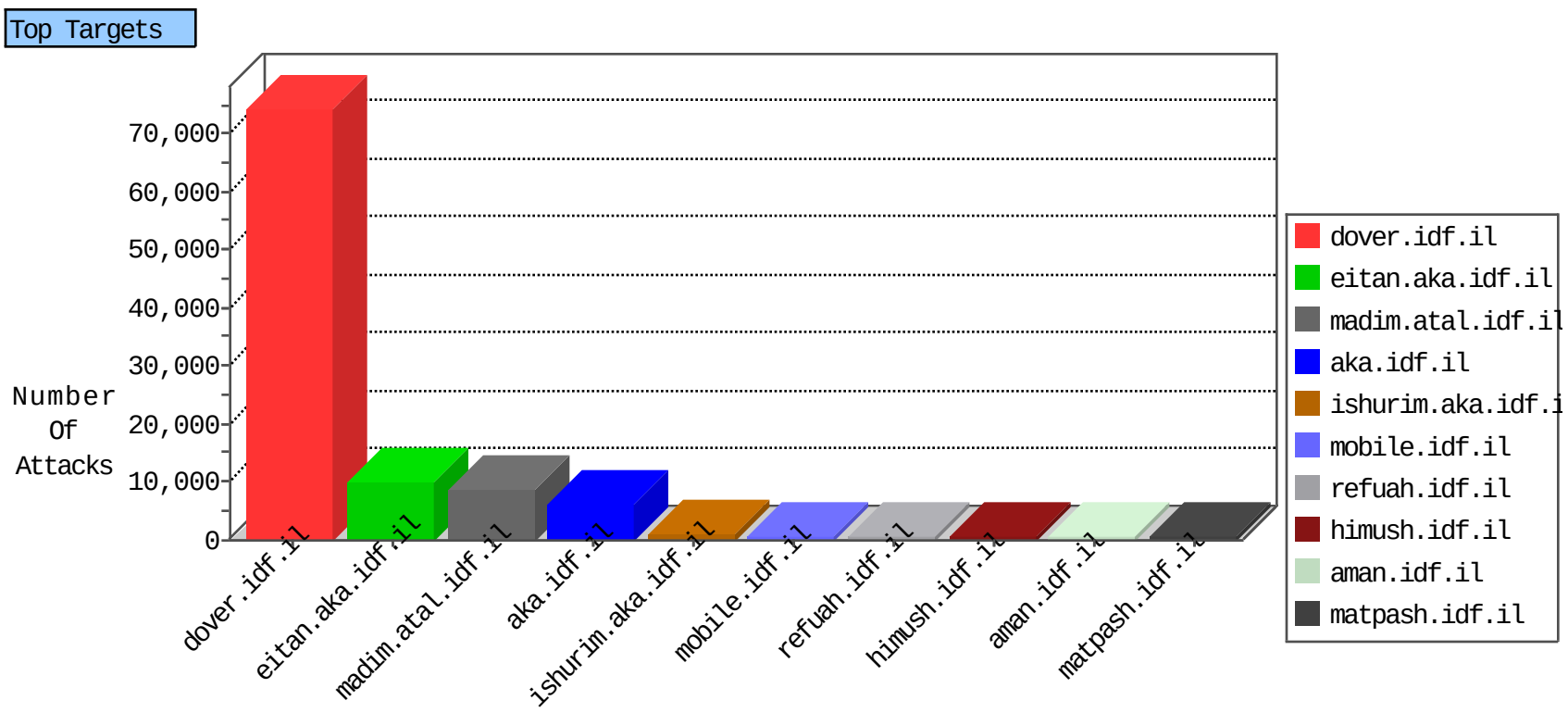
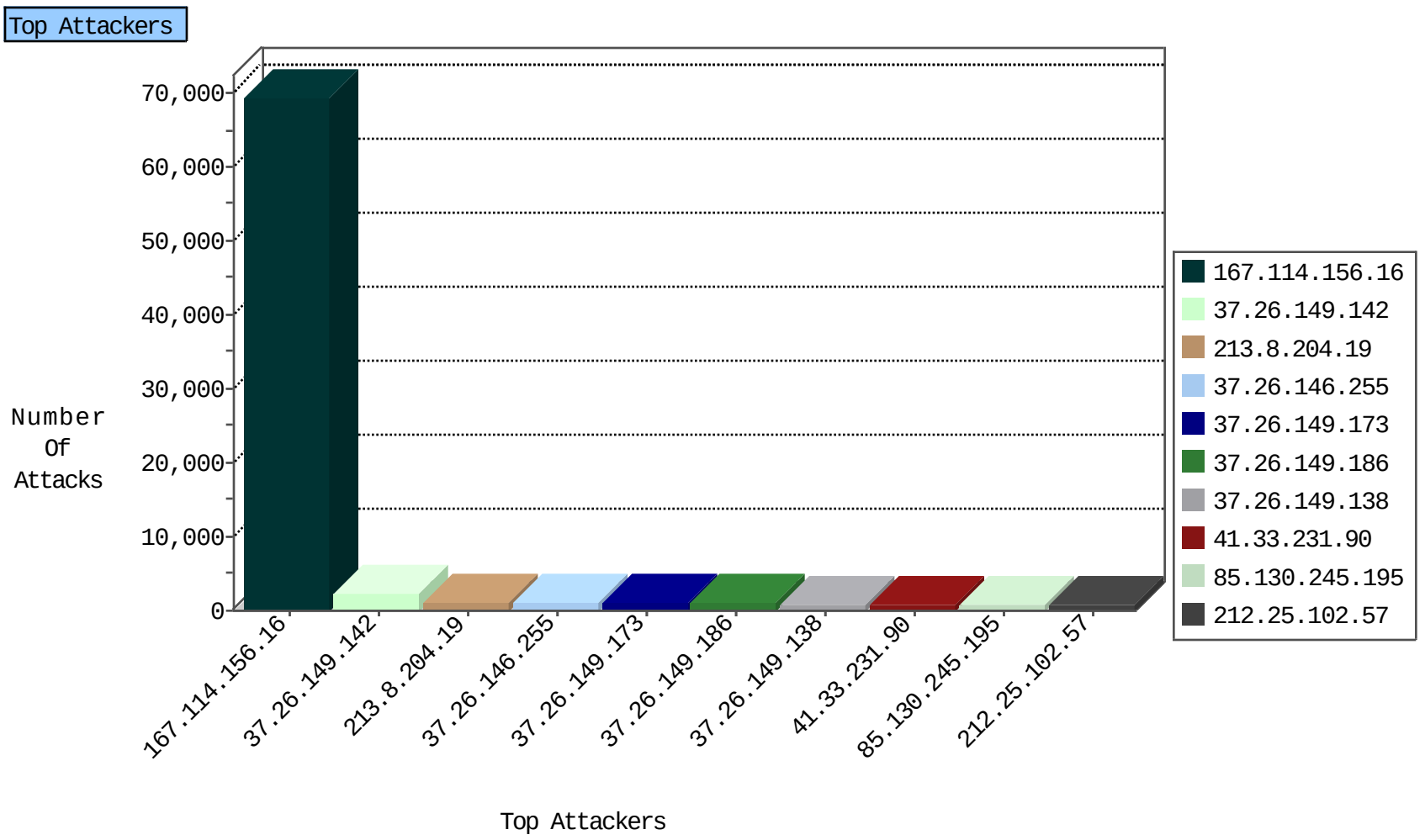
12-09-2015 to 12-10-2015

IDF Under Attack
Daily Report

Top Targets



Top Attackers



12-09-2015 to 12-10-2015

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	90146
66.249.78.82	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	11086
66.249.64.190	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3744
66.249.78.29	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1274
66.249.78.22	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	459
66.249.78.96	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	424
66.249.64.60	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	338
176.12.148.190	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	335
66.249.64.195	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	228
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	211
66.249.78.15	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	188
212.199.112.144	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	156
81.218.241.26	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	87
81.218.241.26	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	76
66.249.64.50	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	72
45.32.246.5		147.237.0.200	m4u.idf.il	Invalid TCP Flags	drop	8
45.32.246.5		147.237.0.33	idf.il	Invalid TCP Flags	drop	8
45.32.246.5		147.237.76.201	e.atal.idf.il	Invalid TCP Flags	drop	8
45.32.246.5		147.237.76.38	e.e.meitav.idf.il	Invalid TCP Flags	drop	8
45.32.246.5		147.237.76.177	ncore.idf.il	Invalid TCP Flags	drop	8
45.32.246.5		147.237.76.44	e.refuah.idf.il	Invalid TCP Flags	drop	8
45.32.246.5		147.237.77.226	www.chamatz.aka.idf.il	Invalid TCP Flags	drop	8
45.32.246.5		147.237.76.196	e.sviva.idf.il	Invalid TCP Flags	drop	8
45.32.246.5		147.237.76.202	e.halag.idf.il	Invalid TCP Flags	drop	8
45.32.246.5		147.237.76.199	e.nakchal.idf.il	Invalid TCP Flags	drop	8
45.32.246.5		147.237.76.176	test.ncore.idf.il	Invalid TCP Flags	drop	7
190.223.131.133	Peru	147.237.0.16	my-kosher-kravi.idf.il	L4 Source or Dest Port Zero	drop	6
45.32.246.5		147.237.77.19	law-forum.idf.il	Invalid TCP Flags	drop	5
45.32.246.5		147.237.0.35	akaws.idf.il	Invalid TCP Flags	drop	5
45.32.246.5		147.237.77.233	atal.idf.il	Invalid TCP Flags	drop	4
45.32.246.5		147.237.0.15	kosher-kravi.idf.il	Invalid TCP Flags	drop	4
45.32.246.5		147.237.8.24	e.lifestyle.idf.il	Invalid TCP Flags	drop	4
66.249.64.233	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
45.32.246.5		147.237.0.19	madim.atal.idf.il	Invalid TCP Flags	drop	4
192.118.132.185	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
45.32.246.5		147.237.72.14	dover.idf.il(old)	Invalid TCP Flags	drop	3
79.183.126.42	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
45.32.246.5		147.237.8.14	e.orchot.idf.il	Invalid TCP Flags	drop	3
45.32.246.5		147.237.77.212	e.dover.idf.il	Invalid TCP Flags	drop	3
5.28.154.35	Israel	147.237.77.74	law.idf.il	Invalid TCP Flags	drop	3
94.56.148.188	United Arab Emirates	147.237.72.156	aman.idf.il	L4 Source or Dest Port Zero	drop	3
212.179.64.162	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
146.185.57.7	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
71.6.135.131	United States	147.237.76.30	himush.idf.il	Block_Udp_All_Nets_Con_Limit	drop	3
79.181.2.140	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
45.32.246.5		147.237.77.227	e.hamaz.idf.il	Invalid TCP Flags	drop	3
39.58.22.49	Pakistan	147.237.77.205	prisha.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
45.32.246.5		147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2

12-09-2015 to 12-10-2015

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
98.19.222.133	United States	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	24
158.85.253.245	United States	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	15
93.89.16.110	Turkey	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
66.76.174.2	United States	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
158.85.253.245	United States	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
106.38.241.147	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	6
185.106.94.2		147.237.77.226	www.chamatz.aka.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
217.16.180.93	Czech Republic	147.237.77.176	matpash.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	2
106.38.241.106	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	2
106.38.241.144	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	2
89.191.216.34	United Kingdom	147.237.77.216	dover.idf.il	C017: HTTP: Malicous UserAgent FOCA	Block	2
69.12.70.34	United States	147.237.77.205	prisha.idf.il	21609: HTTP: pChart Directory Traversal Vulnerability	Block	1
52.35.187.114	United States	147.237.0.34	tikshuv.idf.il	C1000107: DDOS-Spoofed HTTP Packets	Block	1
123.2.148.62	Australia	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
188.165.15.214	France	147.237.76.31	nakchal.idf.il	C228: HTTP: AhrefBot crawler	Block	1
5.9.111.70	Germany	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
158.85.253.245	United States	147.237.72.166	aka.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	1
111.94.200.3	Indonesia	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
69.12.70.34	United States	147.237.77.233	atal.idf.il	21609: HTTP: pChart Directory Traversal Vulnerability	Block	1
52.35.187.114	United States	147.237.77.19	law-forum.idf.il	C1000107: DDOS-Spoofed HTTP Packets	Block	1
188.165.15.26	France	147.237.76.30	himush.idf.il	C228: HTTP: AhrefBot crawler	Block	1
136.243.103.157	Germany	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
69.12.70.34	United States	147.237.76.39	mobile.meitav.idf.il	21609: HTTP: pChart Directory Traversal Vulnerability	Block	1
41.178.188.108	Egypt	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
167.114.229.247	Canada	147.237.77.179	e.mazi.idf.il	13891: TLS: OpenSSL Encrypted/Unencrypted Heartbeat Packet	Permit	1
112.111.188.201	China	147.237.76.42	refuah.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
69.30.218.234	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
188.165.15.98	France	147.237.77.226	www.chamatz.aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1
62.210.85.77	France	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
151.80.31.126	Italy	147.237.76.42	refuah.idf.il	C228: HTTP: AhrefBot crawler	Block	1
69.12.70.34	United States	147.237.77.74	law.idf.il	21609: HTTP: pChart Directory Traversal Vulnerability	Block	1
46.165.197.142	Germany	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
180.250.40.102	Indonesia	147.237.0.15	kosher-kravi.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	1
113.204.53.134	China	147.237.0.17	m.my-kosher-kravi.idf.il	13076: HTTP: Apache Struts 2 OGNL Command Injection Vulnerability	Block	1
78.46.50.246	Germany	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
188.165.15.98	France	147.237.77.233	atal.idf.il	C228: HTTP: AhrefBot crawler	Block	1
62.210.143.245	France	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
69.12.70.34	United States	147.237.77.176	matpash.idf.il	21609: HTTP: pChart Directory Traversal Vulnerability	Block	1
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
185.106.94.2		147.237.77.226	www.chamatz.aka.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
113.204.53.134	China	147.237.0.19	madim.atal.idf.il	13076: HTTP: Apache Struts 2 OGNL Command Injection Vulnerability	Block	1
188.165.15.160	France	147.237.77.216	dover.idf.il	C228: HTTP: AhrefBot crawler	Block	1
62.210.152.87	France	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1

12-09-2015 to 12-10-2015

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	73
66.249.65.9	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	70
98.19.222.133	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	64
158.85.253.245	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	35
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	30
50.28.43.206	147.237.77.74	United States	law.idf.il	Tehila - Perl LWP with fake user agent	23
66.76.174.2	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	15
66.249.64.190	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	11
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	11
93.89.16.110	147.237.77.74	Turkey	law.idf.il	SQL Injection - Select From	8
66.249.78.82	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	6
66.249.64.50	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	4
134.191.232.71	147.237.77.170	Israel	maarachot.idf.il	ET SCAN NMAP -sA (2)	4
80.246.136.165	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	3
66.249.79.14	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
177.74.89.101	147.237.0.17	Brazil	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
149.78.154.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
66.249.75.106	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
177.185.208.71	147.237.72.14	Brazil	dover.idf.il(old)	ET SCAN Potential SSH Scan	2
177.74.89.101	147.237.76.30	Brazil	himush.idf.il	ET SCAN Potential SSH Scan	2
177.185.208.71	147.237.77.170	Brazil	maarachot.idf.il	ET SCAN Potential SSH Scan	2
59.45.79.117	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	2
77.126.220.192	147.237.77.216	Israel	dover.idf.il	http_inspect: MULTIPLE HOST HEADERS DETECTED	2
66.249.81.215	147.237.77.216	Russian Federation	dover.idf.il	ET SCAN NMAP -sA (2)	2
185.24.163.166	147.237.76.39	United Kingdom	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.96	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.29	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.65.112	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	2
177.185.208.71	147.237.8.28	Brazil	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	2
177.185.208.71	147.237.77.176	Brazil	matpash.idf.il	ET SCAN Potential SSH Scan	2
185.24.163.166	147.237.77.170	United Kingdom	maarachot.idf.il	ET SCAN Potential SSH Scan	2
66.249.64.74	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sA (2)	2
185.24.163.166	147.237.0.17	United Kingdom	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
177.74.89.101	147.237.8.45	Brazil	e.eitan.idf.il	ET SCAN Potential SSH Scan	2
177.185.208.71	147.237.76.197	Brazil	e.himush.idf.il	ET SCAN Potential SSH Scan	2
177.74.89.101	147.237.76.201	Brazil	e.atal.idf.il	ET SCAN Potential SSH Scan	2
59.45.79.117	147.237.8.46	China	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
149.202.166.19	147.237.76.30	Germany	himush.idf.il	POLICY-OTHER Adobe ColdFusion admin interface access attempt	1
45.32.246.5	147.237.72.14		dover.idf.il(old)	ET SCAN NMAP -f -sS	1
104.236.232.195	147.237.0.16		my-kosher-kravi.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
209.90.171.35	147.237.76.44	Canada	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
88.235.253.46	147.237.76.30	Turkey	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.24.163.166	147.237.76.42	United Kingdom	refuah.idf.il	ET SCAN Potential SSH Scan	1
177.74.89.101	147.237.0.34	Brazil	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
45.32.246.5	147.237.77.226		www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 3072	1
118.69.85.243	147.237.0.16	Vietnam	my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
220.231.195.122	147.237.8.14	China	e.orchot.idf.il	ET SCAN NMAP -f -sS	1
5.139.195.139	147.237.76.31	Russian Federation	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
93.174.93.102	147.237.76.198	Netherlands	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
188.226.206.204	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN NMAP -sS window 1024	1

12-09-2015 to 12-10-2015

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.26.149.142	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1692
37.26.149.186	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	927
37.26.146.255	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	915
37.26.149.173	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	864
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	710
37.26.149.138	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	561
149.78.26.248	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	498
94.159.142.109	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	438
79.176.178.223	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	432
66.249.79.6	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	212
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	204
85.130.245.195	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	192
85.130.245.195	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	177
85.130.245.195	Israel	147.237.76.30	himush.idf.il	drop	First packet isn't SYN	drop	153
213.8.204.19	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	144
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	107
46.19.86.204	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	95
46.19.86.67	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	93
194.177.16.3	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	83
5.28.158.63	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	83
5.28.158.63	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	78
81.218.76.25	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	76
46.19.86.249	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	75
2.54.37.51	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	74
5.28.154.78	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	73
5.28.154.78	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	73
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	69
79.180.248.73	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	54
92.239.176.150	United Kingdom	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	48
85.130.235.195	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
172.58.136.138	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
207.232.37.138	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid sequence number	monitor	46
66.249.74.6	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	44
212.179.224.209	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	43
46.19.86.138	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	43
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
85.130.245.195	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	42
46.19.86.232	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	42
46.19.86.163	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	42
5.28.147.154	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	40
5.28.155.49	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	40
5.28.155.49	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	40
79.183.211.114	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	40
213.244.82.139	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	40
5.28.147.154	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	40
79.177.174.40	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	39
94.159.152.34	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	38
94.159.152.34	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	37
85.130.245.195	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	37

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.8.204.19	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	865
212.25.102.57	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	585
37.26.149.142	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	458
46.19.86.81	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	304
176.13.17.124	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	292
2.54.149.173	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.54.149.173	Block	279
2.52.167.236	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	226
80.246.136.164	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	216
176.13.2.196	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	213
46.19.85.37	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	212
176.12.148.190	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	205
37.26.146.255	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.146.255	Block	197
46.19.85.37	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	194
2.54.149.173	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	193
176.13.14.105	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	187
37.26.149.138	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	187
46.19.86.219	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	186
37.26.149.173	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	183
2.52.167.236	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	177
176.13.17.124	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	166
37.26.146.153	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	157
79.177.180.33	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	152
2.52.182.220	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	150
37.26.146.153	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	149
46.19.85.92	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	147
213.57.175.86	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	147
213.8.204.19	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 213.8.204.19	Block	145
2.52.182.220	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	140
2.54.171.235	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	133
176.12.148.190	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	130
31.154.85.119	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	117
80.246.136.164	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	115
2.54.171.235	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
2.54.134.53	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
46.19.86.81	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
46.19.86.219	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
46.19.86.81	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	107
37.26.148.163	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	107
80.246.136.165	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
46.19.85.92	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
37.26.149.186	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.149.186	Block	100
2.54.173.180	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	97
2.54.134.53	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	93
2.52.178.203	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	90
176.13.17.124	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 176.13.17.124	Block	90
176.13.14.105	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	88
109.65.11.208	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	87
37.26.149.242	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	86
46.19.86.244	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	82
207.241.226.41	United States	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 207.241.226.41	Block	82