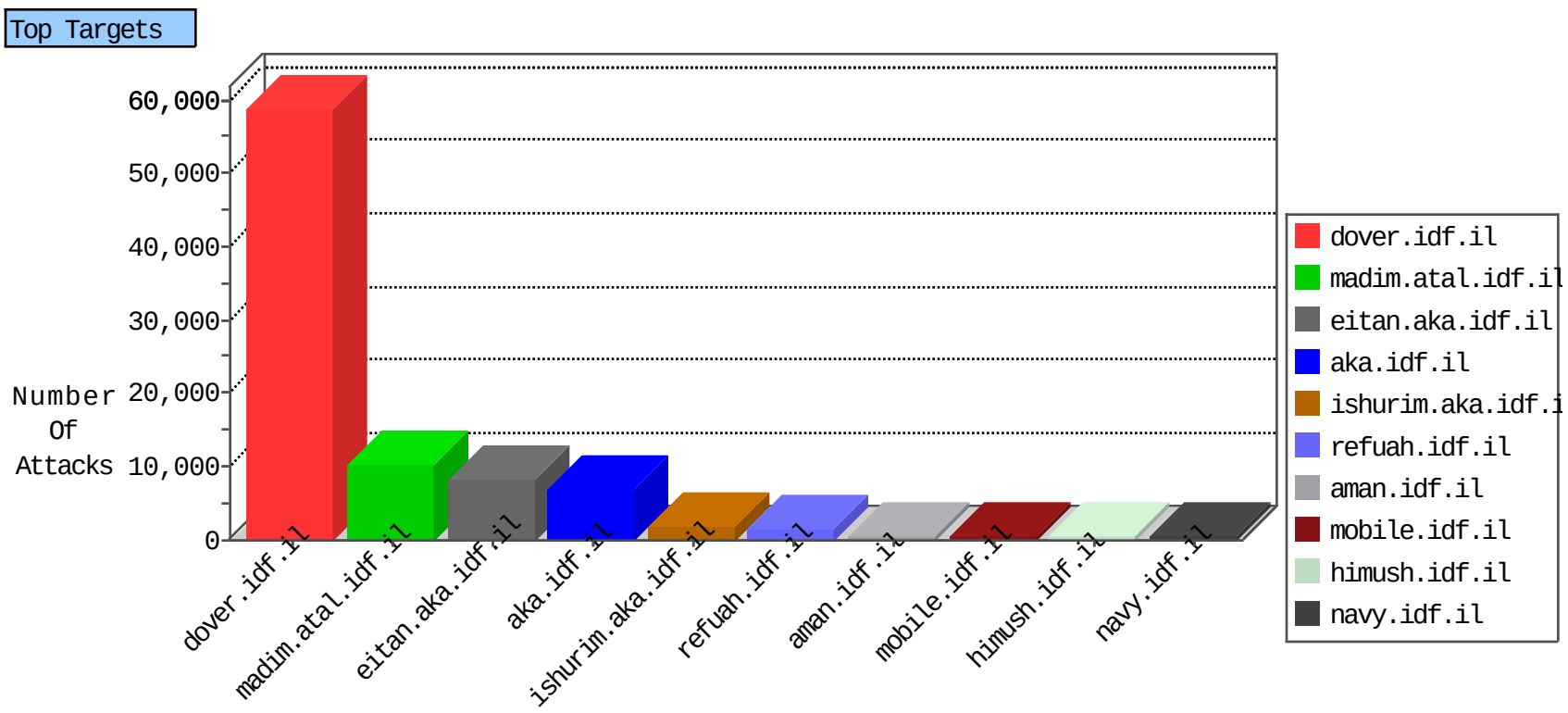
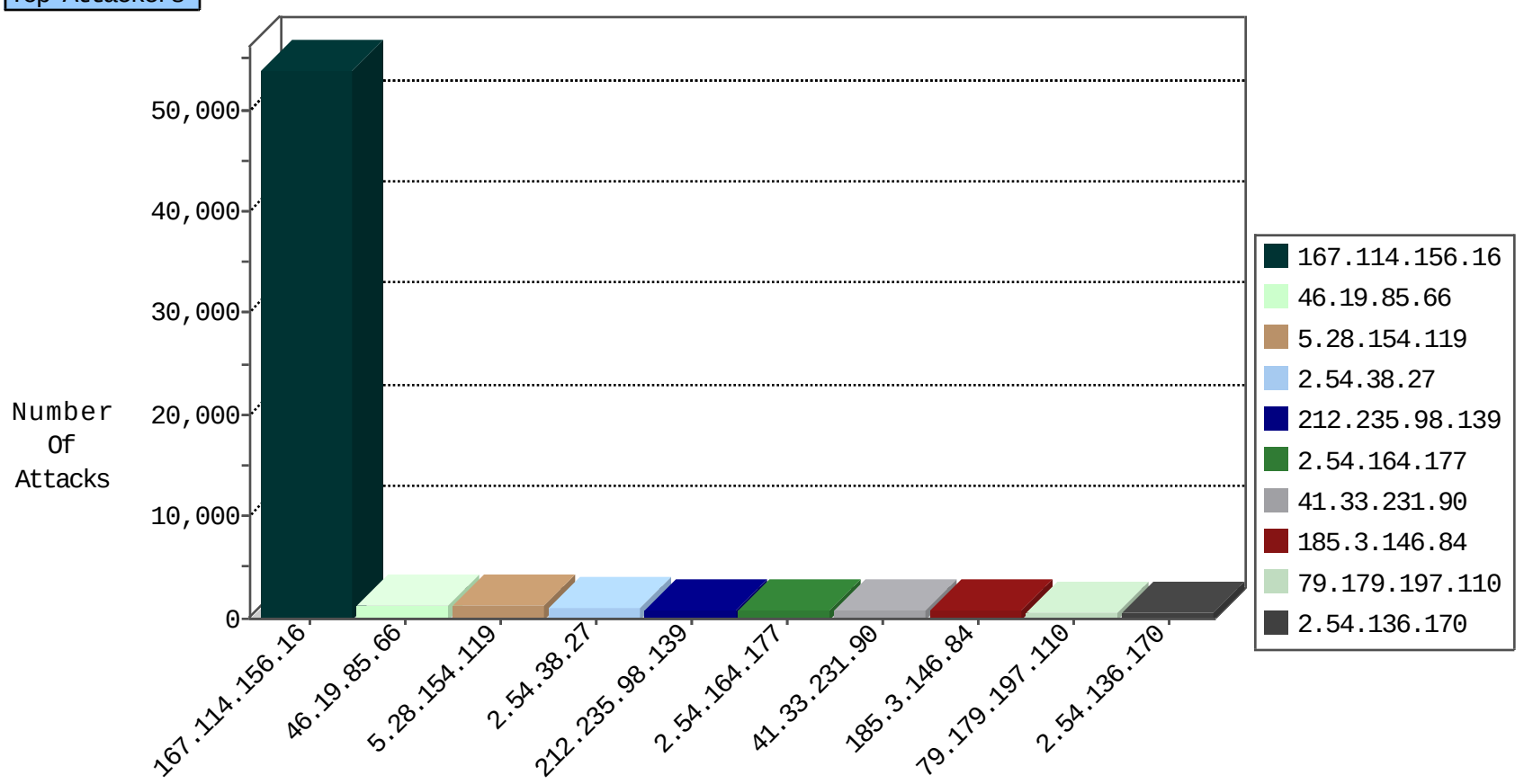
12-14-2015 to 12-15-2015

IDF Under Attack
Daily Report

Top Targets



Top Attackers



12-14-2015 to 12-15-2015

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	95399
46.19.86.38	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	2845
178.162.216.39	Germany	147.237.76.30	himush.idf.il	TCP handshake violation, first packet not syn	drop	2794
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	358
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	29
168.235.201.35	United States	147.237.77.216	dover.idf.il	JLM_Dover_Con_Limit_Https	drop	28
168.235.197.80	United States	147.237.77.216	dover.idf.il	JLM_Dover_Con_Limit_Https	drop	28
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	26
77.126.12.58	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	16
213.8.129.147	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	14
82.102.171.133	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
81.199.122.185	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
79.182.24.54	Israel	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	12
37.142.68.93	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
31.210.186.230	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
89.139.171.15	Israel	147.237.72.166	aka.idf.il	L4 Source or Dest Port Zero	drop	9
87.69.52.148	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
62.90.161.199	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
188.247.75.151	Jordan	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
109.67.203.38	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
31.168.240.21	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	8
82.145.220.23	Europe	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	7
84.109.112.159	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
185.32.179.73	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	6
79.178.178.138	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
85.64.254.209	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
132.70.66.12	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	4
217.132.48.176	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
82.132.214.244	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
82.81.12.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
37.26.149.174	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
213.57.155.110	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
212.179.64.162	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
79.181.153.182	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
82.80.217.70	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
194.90.115.195	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
141.0.14.75	Europe	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Http	drop	3
115.230.124.164	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	3
82.80.217.70	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
81.218.105.235	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
58.229.254.149	Korea, Republic of	147.237.76.202	e.halag.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
222.170.70.222	China	147.237.76.30	himush.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
115.231.222.40	China	147.237.76.199	e.nakchal.idf.il	JLM_Under_Attack_Con_Http	drop	2
183.60.48.25	China	147.237.76.176	test.ncore.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
168.235.201.35	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
93.174.93.153	Netherlands	147.237.76.176	test.ncore.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
79.178.54.173	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2

12-14-2015 to 12-15-2015

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.131.59	Israel	147.237.77.176	matpash.idf.il	14170: HTTP: Blank User-Agent (descriptor but no string)	Block	7
185.112.102.222		147.237.76.200	eitan.aka.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	7
185.112.102.222		147.237.76.31	nakchal.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	7
185.112.102.222		147.237.76.42	refuah.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	7
106.38.241.106	China	147.237.77.170	maarachot.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	6
188.165.234.129	France	147.237.77.216	dover.idf.il	16643: HTTP: Protected File Access (/proc/self/environ)	Block	2
193.246.63.31	Switzerland	147.237.77.216	dover.idf.il	16643: HTTP: Protected File Access (/proc/self/environ)	Block	2
185.112.102.222		147.237.76.200	eitan.aka.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
185.106.94.91		147.237.76.200	eitan.aka.idf.il	C003: HTTP: phpMyAdmin access	Block	1
162.210.196.129	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
66.249.64.243	Israel	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
212.179.177.148	Israel	147.237.72.166	aka.idf.il	C1000107: DDOS-Spoofed HTTP Packets	Block	1
185.112.102.222		147.237.76.31	nakchal.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
185.106.94.91		147.237.76.39	mobile.meitav.idf.il	C003: HTTP: phpMyAdmin access	Block	1
94.102.153.58	United Kingdom	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
59.67.153.212	China	147.237.0.19	madim.atal.idf.il	13076: HTTP: Apache Struts 2 OGNL Command Injection Vulnerability	Block	1
185.106.94.91		147.237.77.74	law.idf.il	C003: HTTP: phpMyAdmin access	Block	1
185.106.94.91		147.237.0.19	madim.atal.idf.il	C003: HTTP: phpMyAdmin access	Block	1
69.30.213.138	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
5.9.111.70	Germany	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
185.106.94.91		147.237.76.42	refuah.idf.il	C003: HTTP: phpMyAdmin access	Block	1
59.144.74.90	India	147.237.77.216	dover.idf.il	14062: HTTP: SpamBlockerUtility Fake Anti-Spyware User-Agent (SpamBlockerUtility x.x.x)	Block	1
185.106.94.91		147.237.77.170	maarachot.idf.il	C003: HTTP: phpMyAdmin access	Block	1
185.106.94.91		147.237.72.156	aman.idf.il	C003: HTTP: phpMyAdmin access	Block	1
87.106.179.116	Germany	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
185.112.102.222		147.237.76.42	refuah.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
37.205.0.60	Turkey	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
185.106.94.91		147.237.76.86	navy.idf.il	C003: HTTP: phpMyAdmin access	Block	1
146.255.98.7	Spain	147.237.76.42	refuah.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	1
61.181.128.8	China	147.237.0.17	m.my-kosher-kravi.idf.il	13076: HTTP: Apache Struts 2 OGNL Command Injection Vulnerability	Block	1
185.106.94.91		147.237.77.216	dover.idf.il	C003: HTTP: phpMyAdmin access	Block	1
185.106.94.91		147.237.72.166	aka.idf.il	C003: HTTP: phpMyAdmin access	Block	1
88.150.221.26	United Kingdom	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
46.10.32.72	Bulgaria	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
185.106.94.91		147.237.76.147	chinuch.aka.idf.il	C003: HTTP: phpMyAdmin access	Block	1
162.210.196.100	United States	147.237.77.233	atal.idf.il	C1000106: HTTP: majestic bot	Block	1
194.88.154.138	Poland	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
64.251.25.176	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
185.106.94.91		147.237.77.234	halag.idf.il	C003: HTTP: phpMyAdmin access	Block	1
185.106.94.91		147.237.72.167	ishurim.aka.idf.il	C003: HTTP: phpMyAdmin access	Block	1
88.246.245.10	Turkey	147.237.77.74	law.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1

12-14-2015 to 12-15-2015

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	66
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	16
62.209.8.213	147.237.77.216	Bahrain	dover.idf.il	ET SCAN NMAP -sA (2)	6
188.165.234.129	147.237.77.216	France	dover.idf.il	Tehila - Perl LWP with fake user agent	6
218.58.80.75	147.237.76.201	China	e.atal.idf.il	GPL SCAN nmap TCP	6
66.249.64.190	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	5
212.179.177.148	147.237.77.216	Israel	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	5
212.179.177.148	147.237.72.167	Israel	ishurim.aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	5
193.246.63.31	147.237.77.216	Switzerland	dover.idf.il	Tehila - Perl LWP with fake user agent	4
185.32.179.132	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	4
94.102.153.58	147.237.77.233	United Kingdom	atal.idf.il	SQL Injection - Select From	4
37.205.0.60	147.237.77.74	Turkey	law.idf.il	SQL Injection - Select From	3
66.249.66.33	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	3
64.251.25.176	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	3
80.246.133.192	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
31.210.186.138	147.237.72.166	Israel	aka.idf.il	INDICATOR-SCAN myscan	2
80.74.125.29	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	2
194.88.154.138	147.237.72.166	Poland	aka.idf.il	SQL Injection - Select From	2
94.102.48.195	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	2
104.238.135.81	147.237.72.166		aka.idf.il	ET SCAN Potential SSH Scan	2
213.8.204.8	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
66.249.66.61	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
60.30.204.2	147.237.0.19	China	madim.atal.idf.il	GPL SCAN nmap TCP	2
66.249.64.195	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.70	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN NMAP -sA (2)	2
87.106.179.116	147.237.72.166	Germany	aka.idf.il	SQL Injection - Select From	2
31.210.186.138	147.237.72.166	Israel	aka.idf.il	GPL SCAN myscan	2
208.115.113.89	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	2
94.102.48.195	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	2
82.102.255.35	147.237.77.176	Palestinian Territory, Occupied	matpash.idf.il	ET SCAN NMAP -sA (2)	2
66.249.93.56	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
177.19.158.160	147.237.77.212	Brazil	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
115.29.2.4	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
220.79.189.33	147.237.0.16	Korea, Republic of	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
80.246.137.26	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
137.117.34.247	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
14.173.192.144	147.237.77.216	Vietnam	dover.idf.il	portscan: TCP Distributed Portscan	1
104.238.135.81	147.237.76.30		himush.idf.il	ET SCAN Potential SSH Scan	1
85.25.217.91	147.237.76.176	Germany	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
210.73.74.204	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.114	147.237.77.205	Ukraine	prisha.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
213.8.204.14	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.15.54	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.89.217.234	147.237.72.166		aka.idf.il	portscan: TCP Distributed Portscan	1
46.200.212.254	147.237.0.15	Ukraine	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
119.10.114.32	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
104.209.183.157	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1

12-14-2015 to 12-15-2015

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3263
46.19.85.66	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1254
5.28.154.119	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1122
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	833
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	758
185.3.146.84	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	651
2.54.136.170	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	555
79.177.2.129	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	489
2.54.189.255	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	474
79.178.113.45	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	450
79.178.203.165	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	432
185.120.126.58		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	362
183.79.221.9	Japan	147.237.76.200	eitan.aka.idf.il	drop	SAM rule	drop	217
194.39.218.10	Europe	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	184
185.120.126.58		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	182
80.246.133.233	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	147
79.176.151.155	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	132
46.19.85.17	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	108
183.79.220.161	Japan	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	102
213.57.137.52	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	96
194.90.25.122	Israel	147.237.76.201	e.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	81
168.235.197.80	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	79
141.0.14.184	Europe	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	74
109.67.145.13	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
141.0.14.75	Europe	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	68
82.166.185.109	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	68
80.246.133.142	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	63
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
194.90.192.10	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	55
46.19.86.68	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	55
183.79.220.161	Japan	147.237.76.200	eitan.aka.idf.il	drop	SAM rule	drop	48
66.249.66.39	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	46
46.19.86.160	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	46
80.178.67.254	Israel	147.237.76.30	himush.idf.il	drop	First packet isn't SYN	drop	43
46.19.85.203	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	43
46.19.86.17	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	43
46.19.85.62	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	42
212.76.101.15	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
185.3.146.175	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
213.57.128.142	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	42
46.19.85.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
168.235.201.35	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	41
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	40
176.13.12.155	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	40
207.241.229.110	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	40
213.57.137.52	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	39
213.57.128.142	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	38
219.143.118.237	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
82.166.185.109	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	36
2.54.152.168	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36

12-14-2015 to 12-15-2015

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.38.27	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.38.27	Block	649
176.12.146.253	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	470
2.54.164.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	457
79.179.197.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	368
185.32.179.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	301
2.54.38.27	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 2.54.38.27	Block	299
213.8.204.8	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 213.8.204.8	Block	284
2.54.12.24	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.12.24	Block	250
109.67.185.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	244
95.35.145.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	238
46.19.85.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	230
2.54.164.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	225
213.8.204.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	213
176.13.22.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	210
183.79.220.161	Japan	147.237.76.200	eitan.aka.idf.il	Multiple Abnormally Long Request from 183.79.220.161	Block	208
183.79.220.161	Japan	147.237.76.200	eitan.aka.idf.il	Multiple Illegal HTTP Version from 183.79.220.161	Block	208
212.25.102.57	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	206
138.134.192.10	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 138.134.192.10	Block	203
176.13.7.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	200
176.13.5.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	193
79.178.210.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	192
176.13.5.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	182
84.109.65.2	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	180
79.179.197.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	172
5.28.154.119	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	162
2.54.12.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	161
46.19.85.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	148
176.13.7.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	141
2.54.184.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	139
185.32.179.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	126
79.178.210.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	122
213.151.42.56	Israel	147.237.72.166	aka.idf.il	Too Many of the Same Response Code (404) in Session from 213.151.42.56	Block	118
46.19.85.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	118
95.35.145.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	117
149.88.69.169	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	115
109.67.185.215	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 109.67.185.215	Block	115
95.35.145.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	112
79.179.197.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	112
2.54.38.27	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	109
2.54.164.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
176.13.22.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
185.3.146.84	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 185.3.146.84	Block	104
77.126.211.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
109.67.185.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
46.19.85.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	103
46.19.86.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	100
79.178.210.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	100
212.76.101.15	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	96
37.26.146.190	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	93
77.126.211.187	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 77.126.211.187	Block	85

12-14-2015 to 12-15-2015