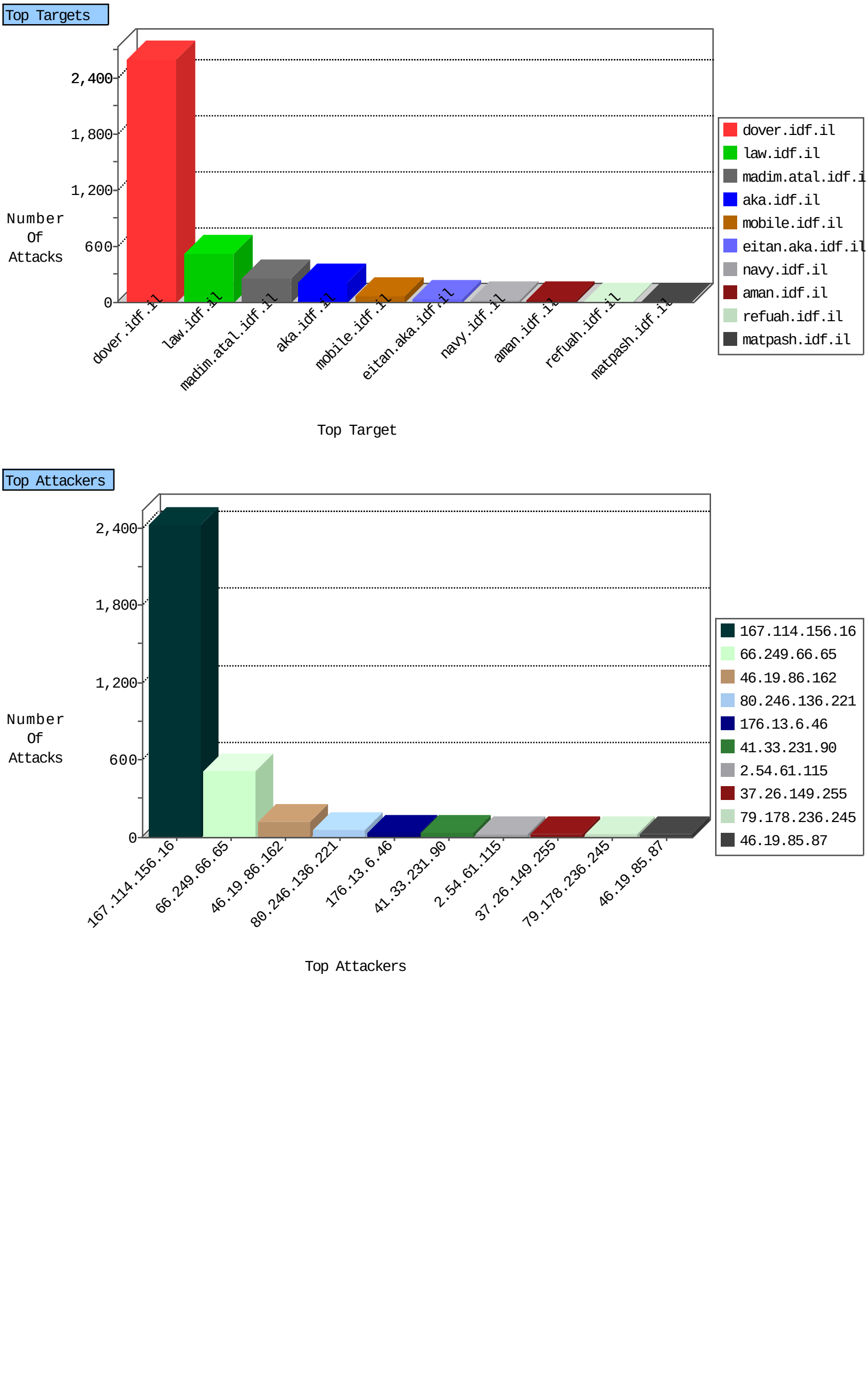
12-11-2015-10:04:06 to 12-11-2015-11:04:06

IDF Under Attack
Daily Report



12-11-2015-10:04:06 to 12-11-2015-11:04:06

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	3315
79.176.197.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
183.196.130.141	China	147.237.76.198	e.yohalan.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
204.42.253.2	United States	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	2
173.195.0.21	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
118.193.23.46	China	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
173.195.0.22	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
80.82.78.207	Netherlands	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
168.235.201.116	United States	147.237.77.176	matpash.idf.il	Frk_Under_Attack_Con_Http	drop	1
107.150.55.50	United States	147.237.0.19	madim.atal.idf.il	block-sp-traf1	drop	1

12-11-2015-10:04:06 to 12-11-2015-11:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
52.35.187.114	United States	147.237.76.30	himush.idf.il	C1000107: DDOS-Spoofed HTTP Packets	Block	1
106.38.241.147	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

12-11-2015-10:04:06 to 12-11-2015-11:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.66.65	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	516
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.66.1	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
138.186.92.212	147.237.77.205		prisha.idf.il	ET SCAN Potential SSH Scan	2
138.186.92.212	147.237.77.170		maarachot.idf.il	ET SCAN Potential SSH Scan	2
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	2
138.186.92.212	147.237.0.19		madim.atal.idf.il	ET SCAN Potential SSH Scan	2
96.22.224.103	147.237.0.200	Canada	m4u.idf.il	ET SCAN NMAP -sS window 3072	1
183.196.130.141	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
138.186.92.212	147.237.77.234		halag.idf.il	ET SCAN Potential SSH Scan	1
220.167.100.13	147.237.77.216	China	dover.idf.il	ET SCAN Tomcat Web Application Manager scanning	1
45.55.133.216	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
138.186.92.212	147.237.77.179		e.mazi.idf.il	ET SCAN Potential SSH Scan	1
220.167.100.13	147.237.76.86	China	navy.idf.il	ET SCAN Tomcat Web Application Manager scanning	1
138.186.92.212	147.237.76.199		e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
220.167.100.13	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Tomcat Web Application Manager scanning	1
138.186.92.212	147.237.76.34		yohalan.idf.il	ET SCAN Potential SSH Scan	1
218.249.175.234	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
138.186.92.212	147.237.0.200		m4u.idf.il	ET SCAN Potential SSH Scan	1
210.117.121.60	147.237.0.17	Korea, Republic of	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
111.127.141.193	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.128.144.131	147.237.77.19	Canada	law-forum.idf.il	ET SCAN NMAP -sS window 4096	1
183.196.130.141	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
96.22.224.103	147.237.0.200	Canada	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
183.196.130.141	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
220.167.100.13	147.237.77.216	China	dover.idf.il	SERVER-APACHE Apache Tomcat Web Application Manager access	1
220.167.100.13	147.237.76.86	China	navy.idf.il	SERVER-APACHE Apache Tomcat Web Application Manager access	1
220.167.100.13	147.237.0.15	China	kosher-kravi.idf.il	SERVER-APACHE Apache Tomcat Web Application Manager access	1
138.186.92.212	147.237.76.44		e.refuah.idf.il	ET SCAN Potential SSH Scan	1
218.249.175.234	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN NMAP -sS window 4096	1
138.186.92.212	147.237.76.30		himush.idf.il	ET SCAN Potential SSH Scan	1
210.117.121.60	147.237.0.17	Korea, Republic of	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
109.235.254.181	147.237.76.202	Turkey	e.halag.idf.il	ET SCAN NMAP -sS window 4096	1
183.196.130.141	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1

12-11-2015-10:04:06 to 12-11-2015-11:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
37.26.149.255	Israel	147.237.76.200	eitan.aka.idf..	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
79.178.236.245	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
2.54.61.115	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
46.19.85.87	Israel	147.237.76.200	eitan.aka.idf..	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.197	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
46.19.86.106	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
84.109.115.116	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.54.61.115	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
194.90.66.9	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.61.115	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.85.51	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.149	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.51	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.61.115	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.177.226.180	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
199.203.64.85	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.87	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.87	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
113.22.50.72	Vietnam	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
207.241.226.41	United States	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	5
207.241.226.41	United States	147.237.77.233	atal.idf.il	drop	SAM rule	drop	5
87.69.113.219	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
185.32.179.115	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.52.53.247	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
80.246.136.221	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.102.254.130	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.52.53.247	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.183.153.98	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
113.22.50.72	Vietnam	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	3
109.64.2.208	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
207.46.13.57	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.54.35.96	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.53.107	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
40.77.167.67	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.48.121	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.64.249.42	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
5.28.162.61	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.218.55.253	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
183.138.151.70	China	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.64.246	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.165.63	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.18.100	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
80.179.16.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.48.121	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
37.26.147.247	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

12-11-2015-10:04:06 to 12-11-2015-11:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	74
80.246.136.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	54
46.19.86.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	46
176.13.6.46	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
46.19.86.199	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
79.183.195.169	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
79.178.48.121	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	6
80.246.136.198	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
46.19.85.140	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
176.12.148.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1381-he/dover.aspx	Block	1
45.55.133.216		147.237.0.34	tikshuv.idf.il	Unauthorized Method HEAD for /	Block	1
109.235.189.141	Russian Federation	147.237.77.176	matpash.idf.il	Parameter Type Violation lang in www.cogat.idf.il/901-en/cogat.aspx	Block	1
66.249.64.17	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-en	Block	1
95.86.105.180	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/&sa=u&ved=0ahukewi62oiztnpjahuewbqkhqkqc70qfggimaa&usg=afqjcnhcvyyg7w1cq-yhd5_ammzoyodtwa	Block	1
87.69.11.68	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.166.139.20	Netherlands	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to 147.237.76.147/	Block	1
207.241.226.42	United States	147.237.76.200	eitan.aka.idf.il	Unknown Parameter r in www.eitan.aka.idf.il/templates/opcontactus/govcaptchaimage.axd	None	1
79.182.187.157	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.149.203	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.67.25.188	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter sOpenLinkIn in www.aka.idf.il/eitan/pratim/pirteychayal/	None	1
52.35.187.114	United States	147.237.76.30	himush.idf.il	NULL Character in Method	Block	1
220.167.100.13	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/manager/html	Block	1
93.173.150.9	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.121.78.175	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 46.121.78.175	Block	1
199.16.156.125	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/1/size220x0/11591.jpg	Block	1
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
74.82.47.2	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
46.19.85.51	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request request version	Block	1
109.235.189.141	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation lang in www.idf.il/1158-he/dover.aspx	Block	1
66.249.65.118	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/2828.jpg	Block	1
5.29.66.60	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$employmentStatus in aka.idf.il/main/sachar/payslips.aspx	None	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
87.69.113.219	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
46.166.139.20	Netherlands	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
212.179.177.148	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
178.17.174.99	Moldova, Republic of	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
45.55.80.152		147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to /	Block	1
109.235.189.141	Russian Federation	147.237.77.74	law.idf.il	Parameter Type Violation PageNum in www.mag.idf.il/487-he/patzar.aspx	Block	1
66.249.66.64	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	1
54.153.33.233	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
95.86.82.17	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.121.78.175	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
199.30.24.187	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
84.109.115.116	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.176.23.126	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.51	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version deflate, sdch	Block	1
176.12.138.68	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	1

12-11-2015-10:04:06 to 12-11-2015-11:04:06