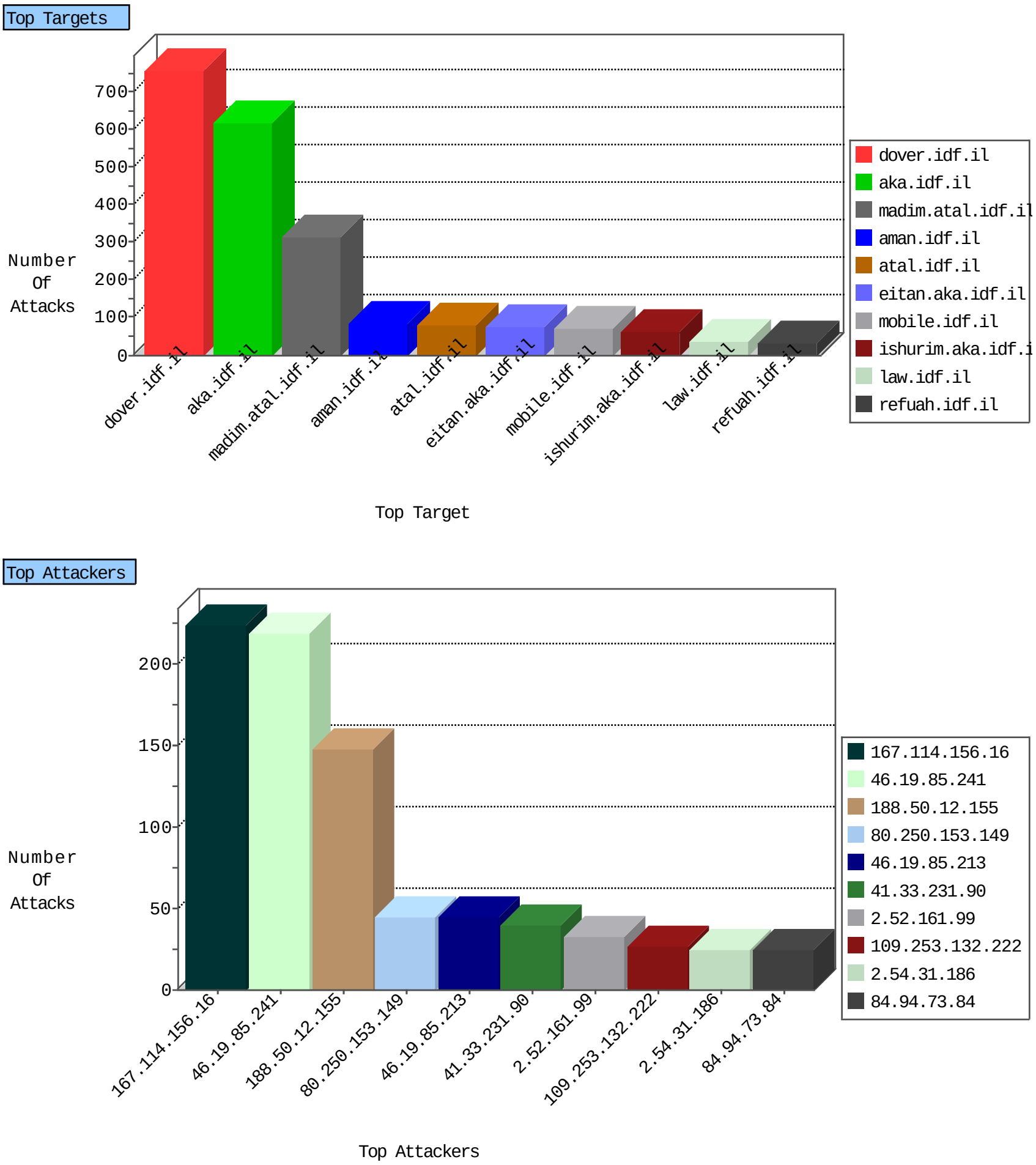
12-29-2015-16:04:08 to 12-29-2015-17:04:08

IDF Under Attack
Daily Report



12-29-2015-16:04:08 to 12-29-2015-17:04:08

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	4193
188.50.12.155	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	251
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	19
167.114.156.16	Canada	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	8
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
173.237.172.93	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
79.177.226.225	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
72.9.148.10	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
181.120.73.141	Paraguay	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
146.185.239.100	Russian Federation	147.237.72.156	aman.idf.il	block-sp-traf1	drop	1
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

12-29-2015-16:04:08 to 12-29-2015-17:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.105.232.28	Algeria	147.237.77.216	dover.idf.il	3886: HTTP: Cross Site Scripting in POST Request	Block	2
197.19.119.165	Tunisia	147.237.77.216	dover.idf.il	3886: HTTP: Cross Site Scripting in POST Request	Block	1

12-29-2015-16:04:08 to 12-29-2015-17:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
197.19.119.165	147.237.77.216	Tunisia	dover.idf.il	SQL Injection - Select From	5
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
41.105.232.28	147.237.77.216	Algeria	dover.idf.il	SQL Injection - Select From	2
41.105.232.28	147.237.77.216	Algeria	dover.idf.il	GPL WEB_SERVER /etc/passwd	2
46.121.254.70	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
197.19.119.165	147.237.77.216	Tunisia	dover.idf.il	ET WEB_SERVER cmd.exe In URI - Possible Command Execution Attempt	1
197.19.119.165	147.237.77.216	Tunisia	dover.idf.il	ET WEB_SERVER Possible SQL Injection Attempt SELECT FROM	1
5.39.222.253	147.237.76.202	Netherlands	e.halag.idf.i	ET SCAN NMAP -sS window 1024	1
197.19.119.165	147.237.77.216	Tunisia	dover.idf.il	ET WEB_SERVER /bin/sh In URI Possible Shell Command Execution Attempt	1
176.13.13.255	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
112.101.149.174	147.237.77.61	China	e.cogat.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
197.19.119.165	147.237.77.216	Tunisia	dover.idf.il	SQL url ending in comment characters - possible sql injection attempt	1
89.139.60.164	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
197.19.119.165	147.237.77.216	Tunisia	dover.idf.il	SERVER-WEBAPP /etc/passwd file access attempt	1
84.109.162.230	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
197.19.119.165	147.237.77.216	Tunisia	dover.idf.il	POLICY-OTHER script tag in URI - likely cross-site scripting attempt	1
66.249.66.127	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
197.19.119.165	147.237.77.216	Tunisia	dover.idf.il	GPL WEB_SERVER /etc/passwd	1
46.19.85.141	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
197.19.119.165	147.237.77.216	Tunisia	dover.idf.il	ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt	1
197.19.119.165	147.237.77.216	Tunisia	dover.idf.il	ET WEB_SERVER /system32/ in Uri - Possible Protected Directory Access Attempt	1
149.78.143.51	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.199.182.150	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.122.179	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.138.190.175	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
197.19.119.165	147.237.77.216	Tunisia	dover.idf.il	SERVER-IIS cmd.exe access	1
66.249.93.184	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
197.19.119.165	147.237.77.216	Tunisia	dover.idf.il	OS-WINDOWS Microsoft Forefront UAG javascript handler in URI XSS attempt	1

12-29-2015-16:04:08 to 12-29-2015-17:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.85.213	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
37.26.148.171	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
46.19.86.54	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	22
188.50.12.155	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	18
188.50.12.155	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	18
212.143.186.38	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
154.121.4.229	Algeria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
31.168.218.168	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
84.94.73.84	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
2.52.10.35	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
84.94.73.84	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
79.176.43.124	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.206.115	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
2.54.31.35	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
80.250.153.149	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
80.250.153.149	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
79.178.58.248	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
2.52.161.99	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
54.151.42.39	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	10
213.57.131.2	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
80.250.153.149	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
173.237.172.93	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	10
79.182.135.87	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
80.250.153.149	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	9
2.54.182.53	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.52.128.97	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
2.54.31.186	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
109.64.60.191	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
37.26.147.249	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		alert	8
37.26.148.199	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
195.160.240.11	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
104.232.3.33		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.52.161.99	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	7
37.26.147.170	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.85.128	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
94.230.86.182	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.54.1.199	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
37.26.147.249	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	6
77.127.227.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
93.173.63.13	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
5.22.131.92	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.138	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.116.224.54	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
58.186.18.0	Vietnam	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.81	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.67.122.173	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.116.175.252	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
213.57.139.222	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6

12-29-2015-16:04:08 to 12-29-2015-17:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	155
46.19.85.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	64
109.253.132.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	27
77.125.145.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	20
176.12.149.35	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
46.19.85.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
109.253.139.204	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	10
41.105.232.28	Algeria	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 41.105.232.28	Block	9
213.140.59.158	Algeria	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 213.140.59.158	Block	8
77.127.201.70	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.127.201.70	Block	8
2.54.134.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
157.55.39.178	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
207.46.13.6	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
37.142.68.100	Israel	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	4
207.46.13.164	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
37.142.68.100	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/xmlrpc.php	Block	4
197.19.119.165	Tunisia	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 197.19.119.165	Block	3
2.52.10.35	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	3
46.19.85.219	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	3
37.142.184.152	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
37.26.148.254	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	2
109.253.139.204	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	2
185.32.179.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.148.254	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/step3.aspx	None	2
37.142.64.27	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
185.32.179.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.7.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.111.38.125	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.39	United States	147.237.0.16	my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	2
109.65.22.170	Israel	147.237.0.16	my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	2
79.177.49.193	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	2
77.125.112.10	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.125.112.10	Block	1
84.229.164.247	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
217.226.104.100	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
81.218.140.112	Israel	147.237.77.233	atal.idf.il	E-mail collector robots 14	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
62.219.140.154	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
132.66.62.239	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
79.183.165.38	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
40.77.167.41	United States	147.237.0.16	my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
77.127.201.70	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/navmenu/kkkkkkk=cd07baa9kkkkkkk_cd07baa9	Block	1
157.55.39.39	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
37.26.149.193	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.108.37.217	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/valtam	Block	1
77.40.129.123	Norway	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	1
46.116.224.54	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.223.215	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

12-29-2015-16:04:08 to 12-29-2015-17:04:08