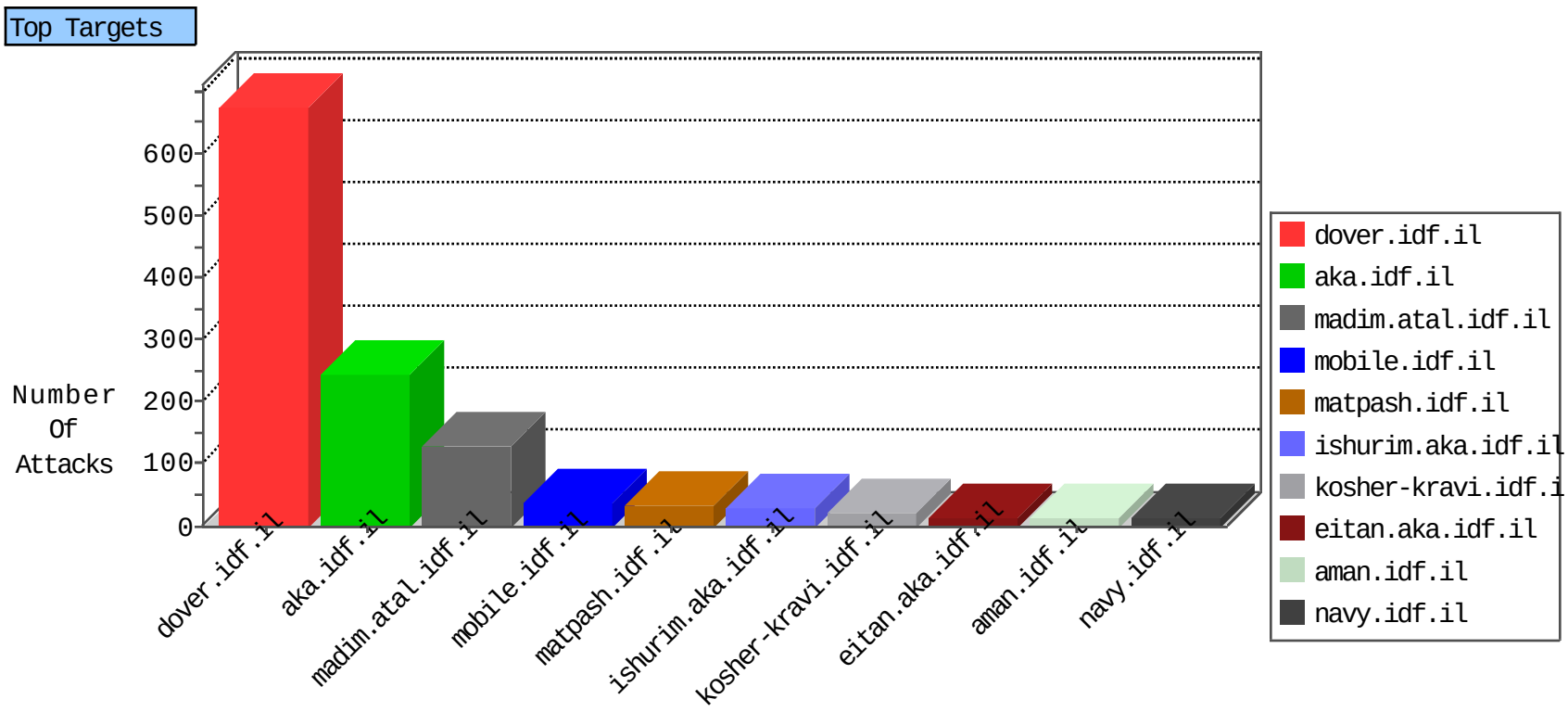
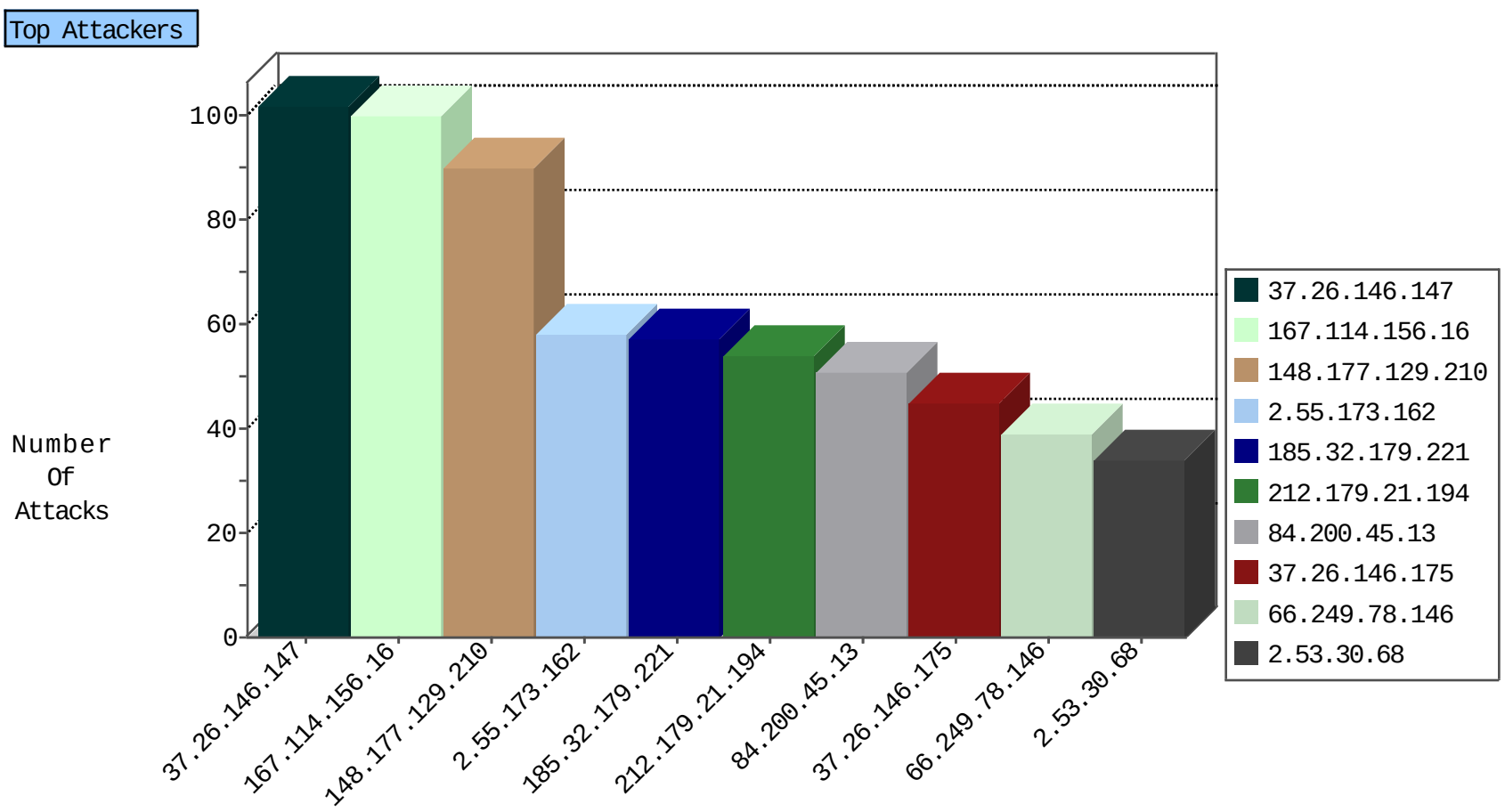
04-26-2016-11:04:04 to 04-26-2016-12:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-26-2016-11:04:04 to 04-26-2016-12:04:04

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	HTTP-POST-Segmented-DoS	dest-reset	5137
80.246.139.201	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3073
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	10
146.185.57.8	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3
94.102.52.10	Netherlands	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
14.215.3.26	China	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
118.106.22.181	Japan	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1

04-26-2016-11:04:04 to 04-26-2016-12:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-26-2016-11:04:04 to 04-26-2016-12:04:04

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	3
222.186.34.195	147.237.0.35	China	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
80.246.140.136	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.68.132.170	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.145.52	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.115.248.2	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.88.127.27	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
106.38.241.106	147.237.72.166	China	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
222.186.56.42	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
104.219.234.3	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.34.195	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.171.122.176	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.34.195	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
84.109.185.4	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
222.186.34.195	147.237.0.15	China	kosher-kravi.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
79.179.126.60	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.74	147.237.77.178	United States	e.matpash.idf.il	ET DROP Dshield Block Listed Source	1
5.29.234.25	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.116.94.130	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.144.165	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
104.219.234.3	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.56.42	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
104.171.122.176	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
222.186.34.195	147.237.76.86	China	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
87.69.64.48	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

04-26-2016-11:04:04 to 04-26-2016-12:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.26.146.147	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	102
148.177.129.210	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	90
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
84.200.45.13	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
2.53.30.68	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
37.26.146.175	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
77.127.13.135	Israel	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	20
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
207.241.231.201	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	18
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
89.139.183.96	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
84.229.30.52	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.96.215	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
172.56.41.181	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
89.139.183.96	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
109.253.193.138	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
217.132.223.201	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
198.12.110.138	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
37.26.146.175	Israel	147.237.77.176	matpash.idf.il	drop		drop	8
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
95.5.231.142	Turkey	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	7
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
185.3.144.89	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
89.139.183.96	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
185.3.147.119	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
97.74.24.189	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
94.159.229.185	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
104.42.198.99	United States	147.237.72.156	aman.idf.il	drop	SAM rule	drop	5
2.53.30.68	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
149.78.133.121	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.55.25.128	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
79.180.182.174	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.179.54.237	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
124.105.17.4	Philippines	147.237.76.39	mobile.meitav.idf.i	drop	First packet isn't SYN	drop	3
176.13.21.180	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.162	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.179.220.186	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.35.195	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.154.190.32	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.81.4.86	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.66.50	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-26-2016-11:04:04 to 04-26-2016-12:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.32.179.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	57
2.55.173.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	57
109.65.208.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
5.22.131.121	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/4/112174/pdf	Block	4
79.181.187.210	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/5/112745.pdf	Block	3
85.65.183.235	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 85.65.183.235	Block	3
46.19.85.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.146.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.178.19.134	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 79.178.19.134	Block	2
109.64.108.233	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.64.108.233	Block	2
84.109.32.42	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	Malformed URL	Block	1
23.81.90.154	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
52.221.225.3	Singapore	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
141.212.122.161	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to 147.237.76.147/	Block	1
84.109.32.42	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 84.109.32.42	None	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1043-he/cogat.aspx	Block	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	Unknown HTTP Request Method ?[[#24]]…[[#2]]Àçzý0 in URL	Block	1
38.102.226.16	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
52.221.225.3	Singapore	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on 147.237.76.147/	Block	1
212.117.143.250	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	Illegal Byte Code Character in Header Name [[#5]]~lSM,FQÛq[[#22]]KY_•î>6¿#011,Ã2[[#30]]Yæ}`‰	Block	1
5.29.179.244	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
77.126.68.139	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/homepage/mobile	Block	1
183.91.14.219	Vietnam	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
109.64.108.233	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/login.aspx	Block	1
80.179.220.186	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/gius	Block	1
54.166.155.86	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
212.199.174.101	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	Illegal Byte Code Character in Method ?[[#24]]…[[#2]]Àçzý0	Block	1
5.29.254.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
85.65.183.235	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/sachar/	Block	1
79.177.10.240	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
46.120.69.104	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 46.120.69.104	Block	1
81.218.62.34	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.66.123	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/2392.jpg	Block	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	Malformed HTTP Header Line 1	Block	1
5.29.254.139	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	1
94.102.9.212	Turkey	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
79.178.19.134	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 79.178.19.134	Block	1
52.8.32.153	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
198.12.148.134	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	Block	1
109.67.42.248	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/general/mobile	Block	1

04-26-2016-11:04:04 to 04-26-2016-12:04:04