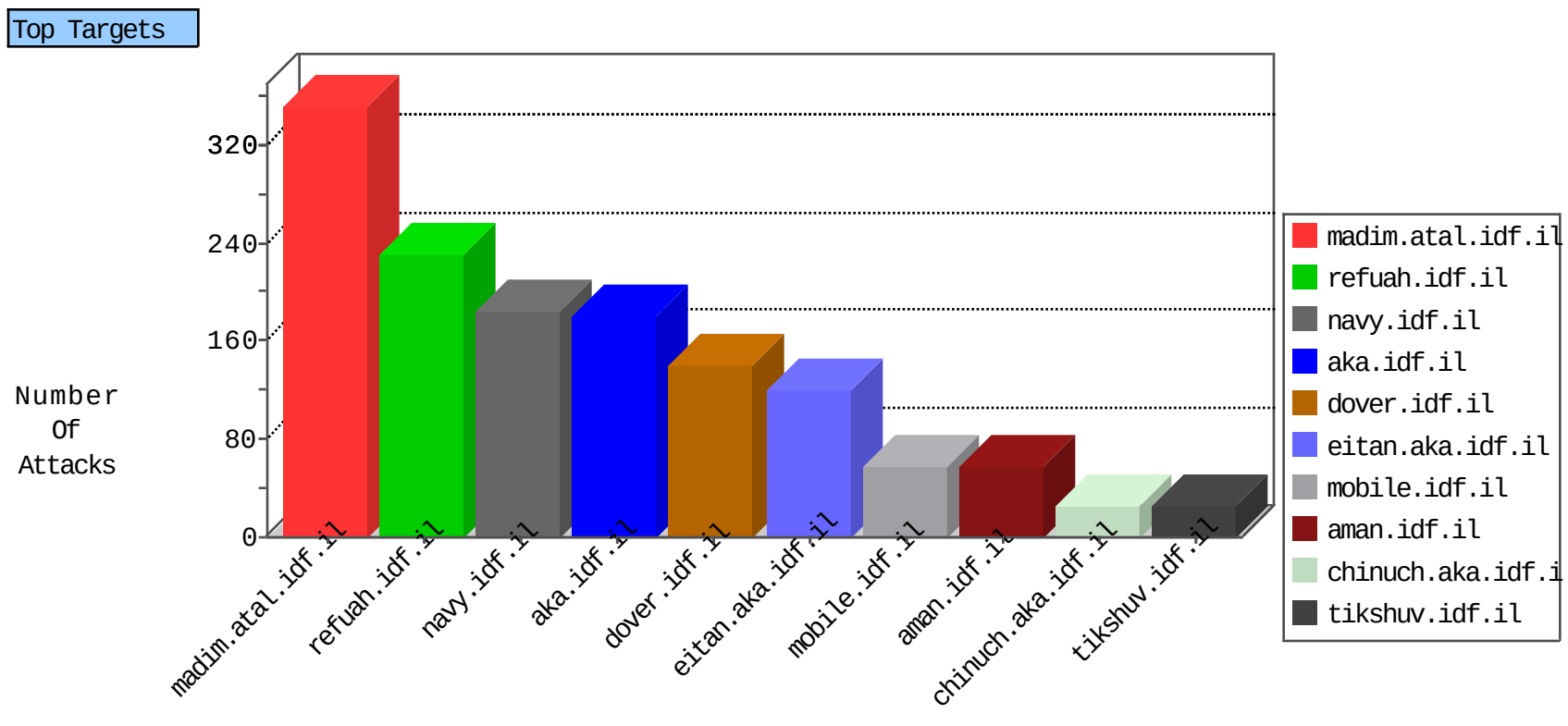
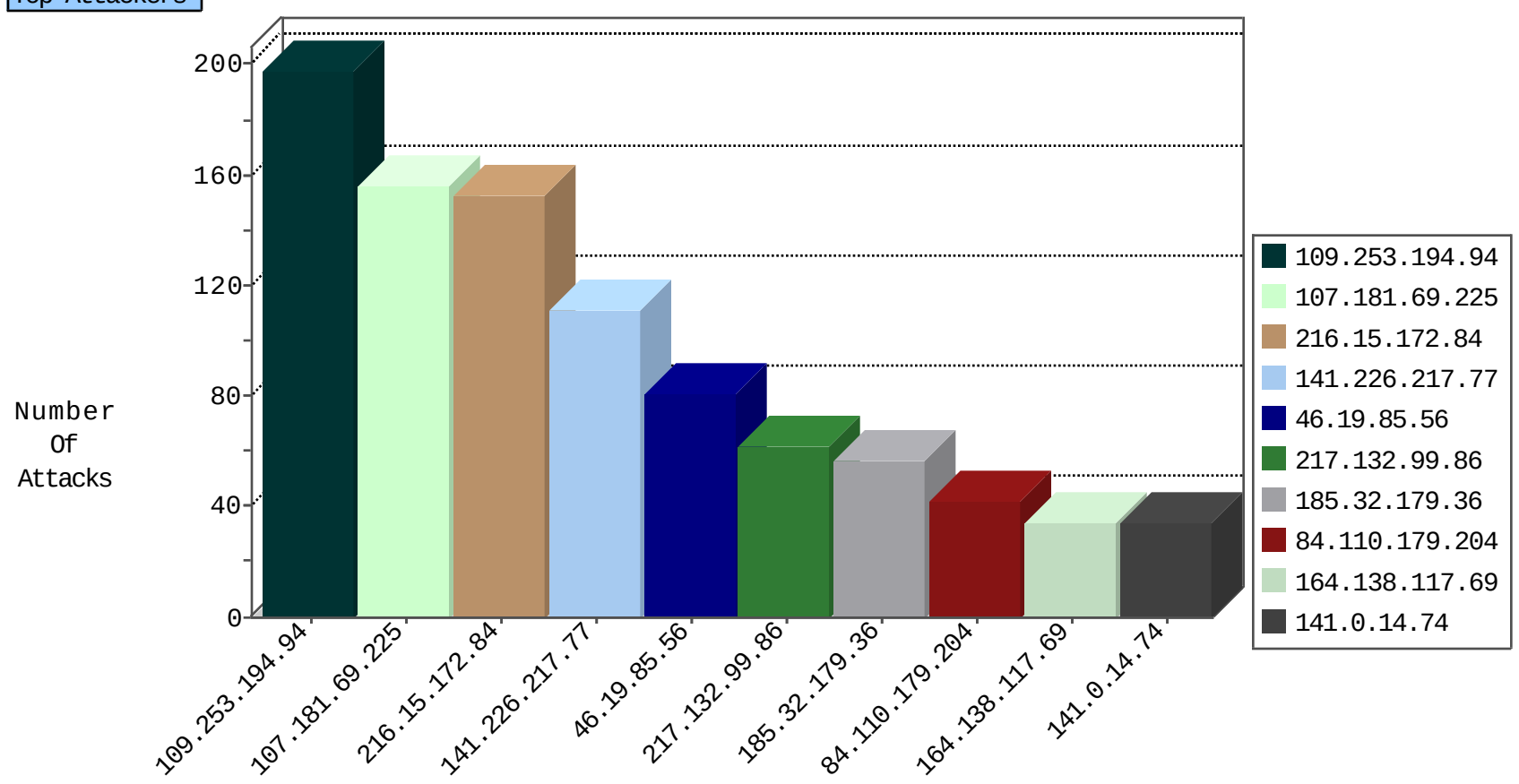
08-31-2016-21:04:05 to 08-31-2016-22:04:05

IDF Under Attack
Daily Report

Top Targets



Top Attackers



08-31-2016-21:04:05 to 08-31-2016-22:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
182.92.131.191	China	147.237.76.44	e.refuah.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
120.132.50.135	China	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	2
185.94.111.1	Russian Federation	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1
154.16.199.217	United States	147.237.76.42	refuah.idf.il	Black List	drop	1
154.16.199.217	United States	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1

08-31-2016-21:04:05 to 08-31-2016-22:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
178.203.120.68	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	3
5.9.88.103	Germany	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	2
178.203.120.68	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

08-31-2016-21:04:05 to 08-31-2016-22:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	2
91.224.160.106	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	2
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	2
218.87.109.253	147.237.77.176	China	matpash.idf.il	ET SCAN Potential SSH Scan	1
2.55.133.33	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
91.224.160.106	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.86	Netherlands	navy.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN Potential SSH Scan	1
211.141.78.56	147.237.77.233	China	atal.idf.il	ET SCAN NMAP -sS window 1024	1
84.61.133.104	147.237.0.200	Germany	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
208.100.26.232	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 1024	1
50.116.123.135	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
185.141.27.44	147.237.0.16		my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
218.87.109.253	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
5.255.90.133	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.77.74	China	law.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
84.109.92.100	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
211.141.78.56	147.237.77.212	China	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
58.65.240.98	147.237.77.61	Indonesia	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
198.52.97.84	147.237.77.74	United States	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
146.185.146.112	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
45.79.91.37	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1

08-31-2016-21:04:05 to 08-31-2016-22:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
141.226.217.77	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	106
217.132.99.86	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	62
164.138.117.69	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	34
141.0.14.74	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
107.181.69.225	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	24
107.181.69.225	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	24
107.181.69.225	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	23
84.110.179.204	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	21
107.181.69.225	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	21
84.110.179.204	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
216.15.172.84	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	20
216.15.172.84	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	20
216.15.172.84	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
107.181.69.225	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	19
216.15.172.84	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
216.15.172.84	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
216.15.172.84	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
216.15.172.84	United States	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
216.15.172.84	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	18
100.92.42.106		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	16
107.181.69.225	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	15
107.181.69.225	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	14
77.124.14.139	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.165	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.19.86.165	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
107.181.69.225	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid sequence number	monitor	9
46.19.86.22	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
95.163.144.203	Russian Federation	147.237.0.15	kosher-kravi.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	9
2.53.151.137	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
77.138.86.15	France	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	8
174.201.9.165	United States	147.237.77.74	law.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
185.3.146.205	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
107.181.69.225	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid sequence number	alert	6
37.242.224.133	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.26.149.208	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
176.13.21.138	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
176.13.229.178	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
157.55.39.175	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.22	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
39.35.46.41	Pakistan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.112.236.32	Poland	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
46.19.86.22	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
46.19.85.40	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.112.236.32	Poland	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
77.138.86.15	France	147.237.72.156	aman.idf.il	Streaming Engine: TCP SYN Modified Retransmission	Data received before SYN-ACK was acknowledged. Stripping all packet data.	drop	3
2.53.139.83	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.226.217.77	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
31.154.81.31	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.40	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

08-31-2016-21:04:05 to 08-31-2016-22:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.194.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	195
46.19.85.56	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	81
185.32.179.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	57
37.26.147.226	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/login parameter Password	Block	8
77.138.53.169	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	5
46.19.86.144	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	4
87.71.30.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.136.35	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.139.240.61	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	2
77.138.53.169	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.138.53.169	Block	2
37.142.219.171	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
31.154.9.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.76.83	Block	2
2.55.39.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
188.120.154.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
213.57.57.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.29.69.55	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
213.57.91.199	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
5.102.218.170	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mas.aspx	None	1
80.230.220.105	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/size100x0/2971.jpg	Block	1
109.253.223.180	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
80.230.220.37	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/size100x0/2277.jpg	Block	1
80.230.221.194	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery.plugins/jquery.equalheights.js	Block	1
80.230.221.161	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/datepicker.css	Block	1
80.230.220.84	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/2288.jpg	Block	1
84.109.124.50	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
66.102.9.24	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
80.230.220.130	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/2090.jpg	Block	1
208.100.26.232	United States	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	1
80.230.220.70	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/size100x0/2808.jpg	Block	1
80.230.221.226	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery/global.js	Block	1
80.230.220.46	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/size100x0/2689.jpg	Block	1
80.230.221.206	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/scriptresource.axd	Block	1
37.46.39.110	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
80.230.220.119	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/size100x0/3250.jpg	Block	1
180.97.106.37	China	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on 180.163.113.82/check_proxy	Block	1
80.230.220.18	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/size100x0/2294.jpg	Block	1
80.230.221.171	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/1.he/scroller/skin.css	Block	1
2.53.24.253	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
80.230.220.93	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/size220x0/3200.jpg	Block	1
89.139.124.191	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.230.220.80	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/5/size100x0/3045.jpg	Block	1
80.230.221.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/images/shared/home.png	Block	1
80.230.221.153	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/960.css	Block	1
180.97.106.162	China	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on 180.163.113.82/check_proxy	Block	1
80.230.220.58	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/size100x0/2427.jpg	Block	1
80.230.221.217	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery/jquery-ui.js	Block	1
46.19.86.238	Israel	147.237.77.74	law.idf.il	Unknown HTTP Request Method en;q=0.4 in URL	Block	1
80.230.220.126	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/5/size100x0/3365.jpg	Block	1
5.255.253.34	Russian Federation	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1

08-31-2016-21:04:05 to 08-31-2016-22:04:05