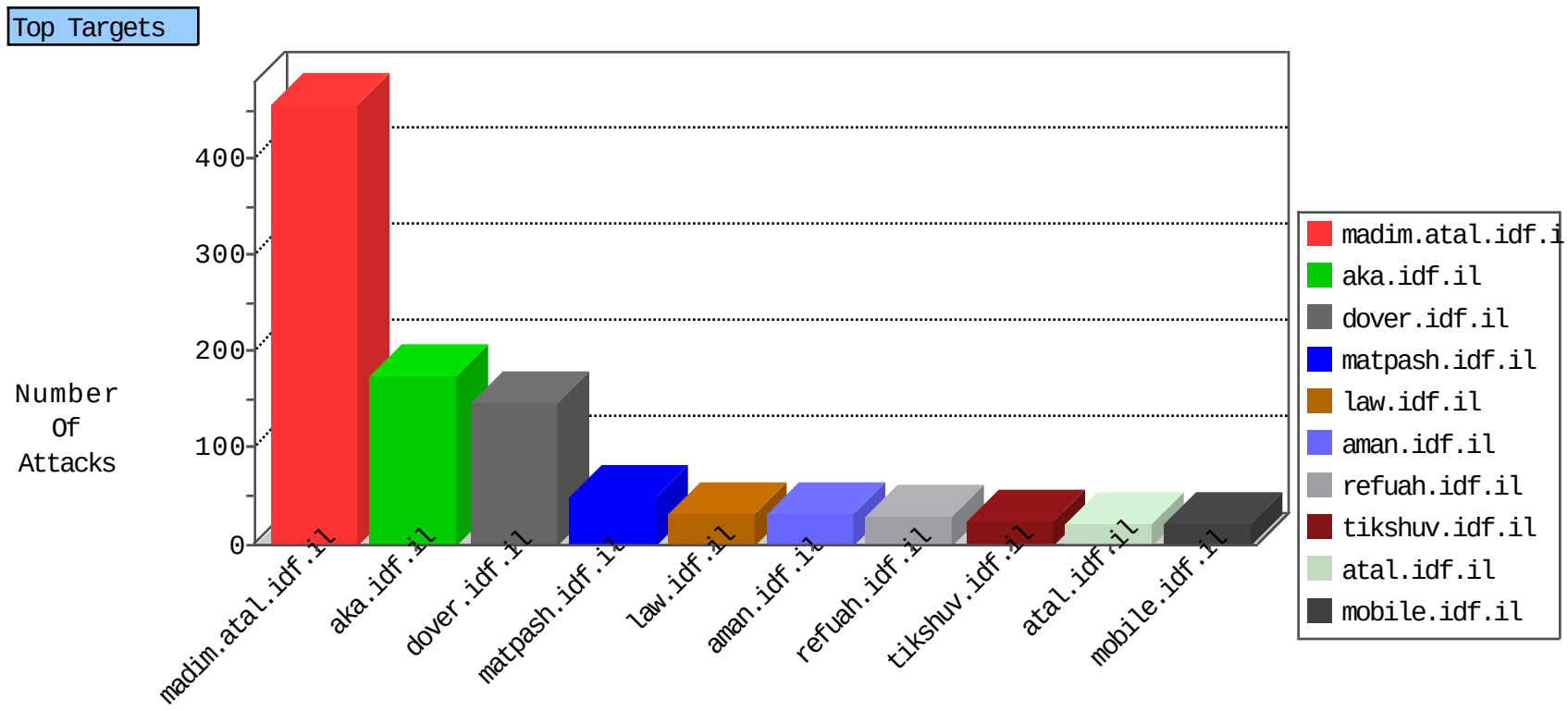
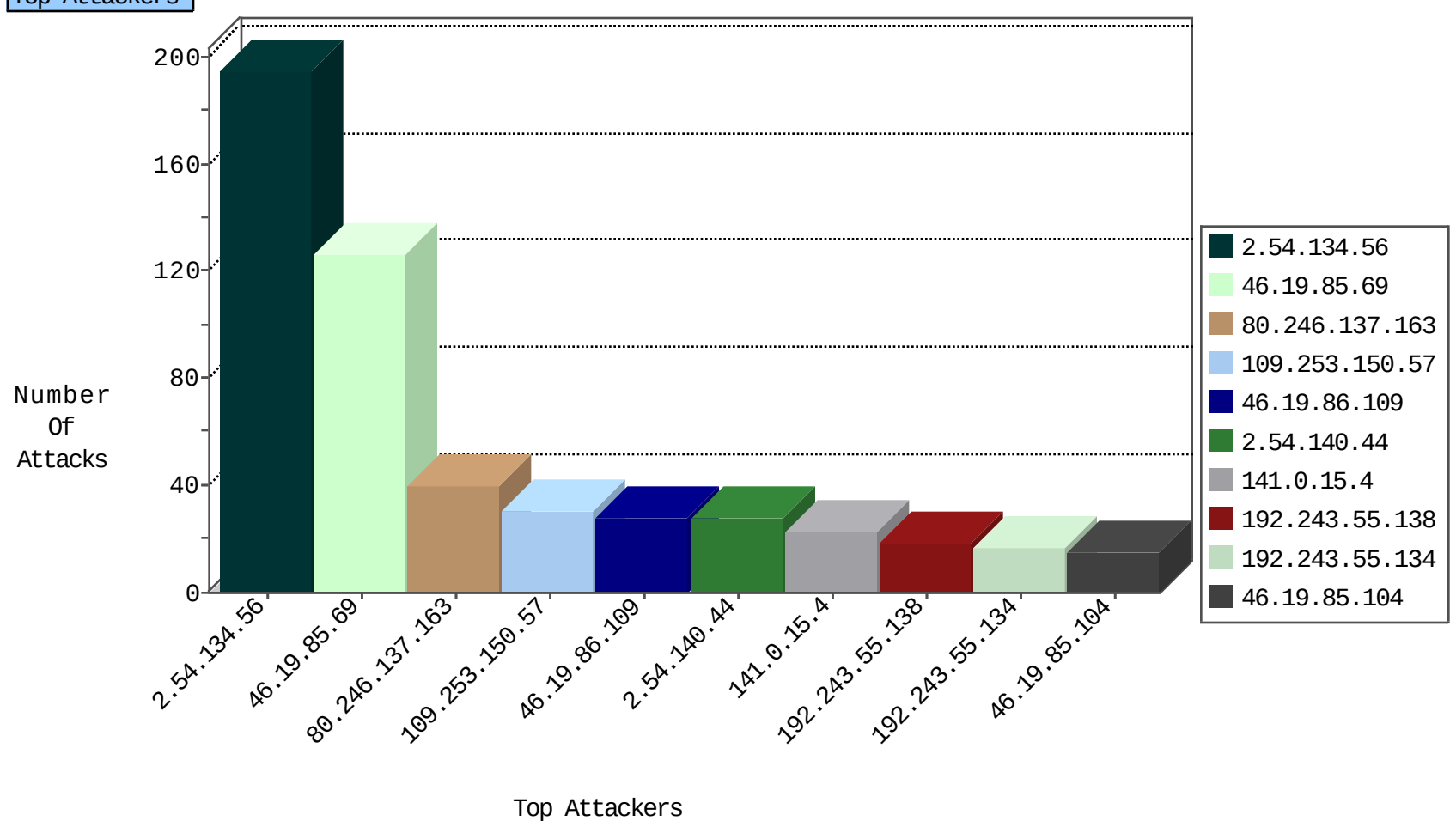
03-09-2016-12:04:07 to 03-09-2016-13:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-09-2016-12:04:07 to 03-09-2016-13:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.241.25	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	94
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
185.130.5.201		147.237.8.27	e.madim.atal.idf.il	Block_Udp_All_Nets	drop	1
58.238.76.41	Korea, Republic of	147.237.77.233	atal.idf.il	Block_Udp_All_Nets	drop	1
108.163.253.194	United States	147.237.76.30	himush.idf.il	JLM_Under_Attack_Con_Https	drop	1
193.242.218.6	Switzerland	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	1
71.6.167.142	United States	147.237.77.61	e.cogat.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.109	United States	147.237.8.24	e.lifestyle.idf.il	Block_Udp_All_Nets	drop	1
184.105.247.203	United States	147.237.8.28	e.mobile-ks.idf.il	Block_Udp_All_Nets	drop	1

03-09-2016-12:04:07 to 03-09-2016-13:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.181.134.55	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	13
192.118.12.102	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
207.46.13.70	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
207.46.13.98	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-09-2016-12:04:07 to 03-09-2016-13:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
108.163.253.194	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sA (2)	2
137.226.113.7	147.237.76.200	Germany	eitan.aka.idf.il	ET SCAN Suspicious User-Agent Containing Web Scan/er, Likely Web Scanner	1
5.29.107.170	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.201.25	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.132.36	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
108.163.253.194	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 3072	1
217.132.2.206	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.193	147.237.76.197	Netherlands	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
212.179.90.106	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.81.194.168	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
77.126.174.48	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.238	147.237.77.178		e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
62.219.231.16	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
182.188.45.62	147.237.77.235	Pakistan	sviva.idf.il	ET SCAN NMAP -sS window 3072	1
31.168.226.178	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
122.141.236.69	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
5.29.61.67	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.178.27	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.131.19	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
108.163.253.194	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sA (2)	1
218.246.0.97	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.193	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
213.8.59.241	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.193	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
212.143.240.242	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.80.196.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.114.88.216	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.75.215	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
185.130.5.113	147.237.76.202		e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
46.116.25.132	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

03-09-2016-12:04:07 to 03-09-2016-13:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.54.140.44	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	28
141.0.15.4	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	23
46.19.85.235	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
192.115.177.203	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.69	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.136.46	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
109.64.157.79	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
38.111.147.88	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.123	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.130.127	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.104	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.54.128.172	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
85.65.228.52	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.195	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.104	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
185.3.147.150	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.132	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
185.32.179.172	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.9	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
212.179.213.153	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.182.140.164	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.19.6	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.166.21.26	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.9	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
213.57.75.189	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.34.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.178.27	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.154.189.8	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.19.235	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.138	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.94.97.11	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.187.98	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.86.54	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.80.193.240	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
2.54.34.148	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.218.131.145	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.138	Dominica	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
46.19.85.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.219.231.16	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.135.199	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.94	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.179.222.225	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
207.232.27.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

03-09-2016-12:04:07 to 03-09-2016-13:04:07

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
2.54.3.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.104	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
212.179.213.153	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

03-09-2016-12:04:07 to 03-09-2016-13:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.134.56	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	193
46.19.85.69	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	119
80.246.137.163	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	40
109.253.150.57	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	30
46.19.86.109	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	28
80.246.136.22	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
2.52.36.82	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	6
80.246.139.103	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
198.71.227.4	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 198.71.227.4	Block	5
176.13.17.68	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
85.65.76.196	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 85.65.76.196	Block	2
2.54.134.56	Israel	147.237.0.19	madim.atal.idf.i	Cookie Tampering on cookie Login: Expected ********** ********** ********** **********, Observed ********** ********** ********** **********	None	2
85.65.76.196	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
38.111.147.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 38.111.147.88	Block	2
80.178.210.181	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	2
194.114.146.227	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 194.114.146.227	Block	2
176.13.4.101	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.54.33.180	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/size100x0/sip_storage	Block	2
46.116.28.206	Israel	147.237.72.156	aman.idf.il	Multiple Abnormally Long Request from 46.116.28.206	Block	1
198.71.227.4	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
79.179.33.19	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00_ctl00_ctl00_ScriptManager1_HiddenField in www.aka.idf.il/main/giyus/pniotfindanswer.aspx	None	1
185.112.248.32		147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/	Block	1
66.102.7.226	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
5.22.134.215	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/xmlrpc.php	Block	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	NULL Character in Header Name at	Block	1
109.8.124.41	France	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.116.28.206	Israel	147.237.72.156	aman.idf.il	Multiple Unknown HTTP Request Method from 46.116.28.206	Block	1
194.114.146.227	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/0/size338x0/1640.jpg	Block	1
37.26.148.160	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.13.10.96	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
77.77.241.23	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
46.116.28.206	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	Abnormally Long Request method	Block	1
46.116.28.206	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Header Name from 46.116.28.206	Block	1
213.57.84.82	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
79.180.150.131	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl61 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
46.19.85.69	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
192.243.55.130	Dominica	147.237.77.176	matpash.idf.il	Distributed Suspicious Response Code	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
27.75.169.150	Vietnam	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	Unknown HTTP Request Method]}à¦[[#4]]ªñã¸ÐnÚ¢,[[#31]]Yw” in URL	Block	1
109.64.197.252	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
46.116.28.206	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 46.116.28.206 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
46.116.28.206	Israel	147.237.72.156	aman.idf.il	Abnormally Long Header Line request header name	Block	1
195.244.23.42	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationexplanation.aspx	None	1
77.77.241.23	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
54.84.196.179	United States	147.237.77.233	atal.idf.il	Distributed PHP Attempt	Block	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	Illegal Byte Code Character in Header Name	Block	1
46.116.28.206	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Method from 46.116.28.206	Block	1
217.69.133.15	Russian Federation	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list.htm	Block	1

03-09-2016-12:04:07 to 03-09-2016-13:04:07