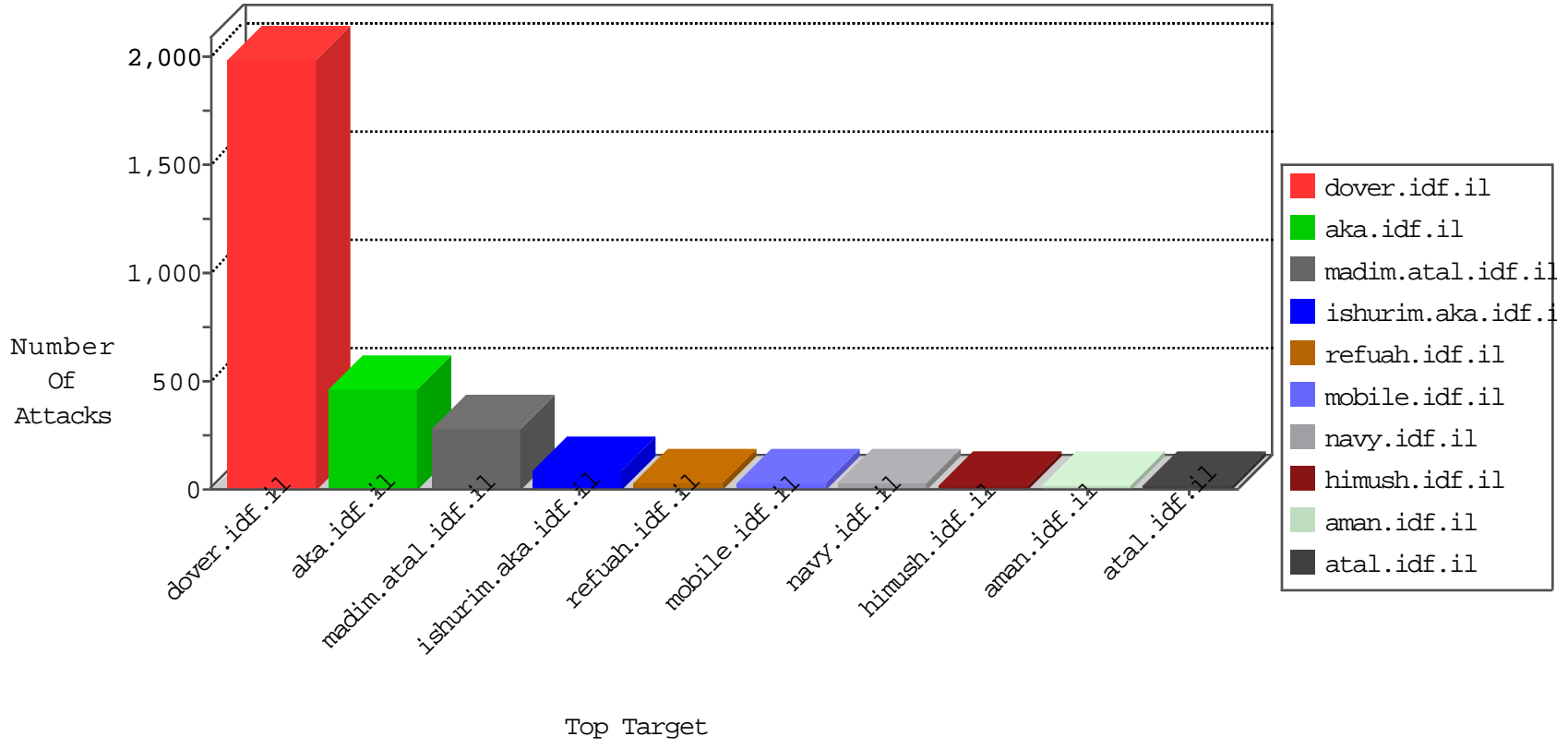


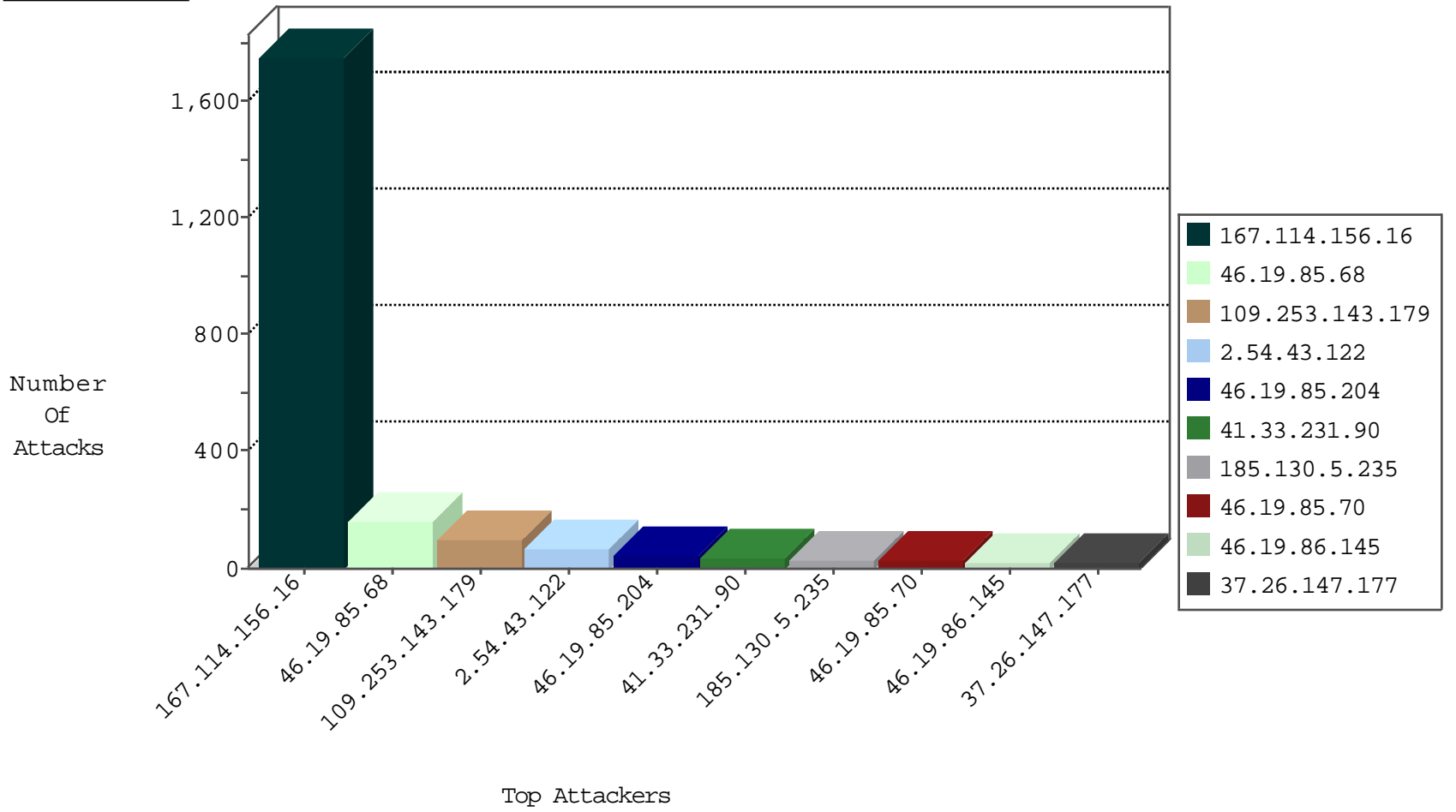
IDF Under Attack Daily Report



Top Targets



Top Attackers



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	3254
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	200
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	93
198.7.62.114	United States	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
107.150.60.242	United States	147.237.77.216	dover.idf.il	block-sp-trafl	drop	1
198.7.62.114	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
142.54.160.211	United States	147.237.77.176	matpash.idf.il	block-sp-trafl	drop	1
197.157.244.243	Somalia	147.237.76.44	e.refuah.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
89.248.174.4	Netherlands	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
208.67.1.50	United States	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
142.54.160.212	United States	147.237.76.30	himush.idf.il	block-sp-trafl	drop	1
198.7.62.114	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
107.150.55.212	United States	147.237.72.156	aman.idf.il	block-sp-trafl	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.130.5.235		147.237.76.30	himush.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
185.130.5.235		147.237.76.39	mobile.meitav.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
23.99.61.32	United States	147.237.77.216	dover.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
185.130.5.235		147.237.76.42	refuah.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
185.130.5.235		147.237.72.156	aman.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
185.130.5.235		147.237.76.39	mobile.meitav.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
23.99.61.32	United States	147.237.77.216	dover.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
185.130.5.235		147.237.72.166	aka.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
185.130.5.235		147.237.72.167	ishurim.aka.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
185.130.5.235		147.237.76.42	refuah.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
185.130.5.235		147.237.0.15	kosher-kravi.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
185.130.5.235		147.237.76.30	himush.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
185.130.5.235		147.237.0.19	madim.atal.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1

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	2
23.99.61.32	147.237.77.216	United States	dover.idf.il	ET WEB_SERVER Muieblackcat scanner	1
185.130.5.235	147.237.72.167		ishurim.aka.idf.il	ET WEB_SERVER Muieblackcat scanner	1
185.130.5.235	147.237.0.19		madim.atal.idf.il	ET WEB_SERVER Muieblackcat scanner	1
185.130.5.234	147.237.77.216		dover.idf.il	ET SCAN Potential SSH Scan	1
179.124.45.195	147.237.72.156	Brazil	aman.idf.il	ET SCAN Potential SSH Scan	1
109.253.215.231	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.228.100.177	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.179.155.129	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.0.34.93	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.235	147.237.76.42		refuah.idf.il	ET WEB_SERVER Muieblackcat scanner	1
46.116.168.240	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.235	147.237.76.30		himush.idf.il	ET WEB_SERVER Muieblackcat scanner	1
185.130.5.235	147.237.72.156		aman.idf.il	ET WEB_SERVER Muieblackcat scanner	1
185.130.5.234	147.237.77.235		sviva.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.234	147.237.76.199		e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
179.124.45.195	147.237.0.16	Brazil	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.76.86	Netherlands	navy.idf.il	ET SCAN NMAP -sS window 1024	1
217.132.155.76	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.172	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
60.187.47.229	147.237.76.31	China	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.130.5.235	147.237.76.39		mobile.meitav.idf.il	ET WEB_SERVER Muieblackcat scanner	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.85.68	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	92
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
46.19.85.68	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.210.225.66	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
149.88.132.247	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
5.102.254.203	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
79.176.5.107	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
149.50.103.230	United States	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
109.253.150.116	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
5.22.129.180	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.86.181	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	8
81.218.241.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.45	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.145	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	7
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	7
89.187.221.10	Lebanon	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
80.246.137.89	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.208.137	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.45	Israel	147.237.76.42	refuah.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.81.175	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	6
84.228.32.208	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.147.141	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.223.29	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.50	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.145	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
87.69.154.130	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.179.121.233	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.50	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.145	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.95	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.179.126.77	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.45	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
37.46.39.215	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.177	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.106	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.145	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
66.249.93.192	Israel	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
46.19.86.44	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.10	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
66.249.81.198	United States	147.237.76.86	navy.idf.il	Directory Traversal	directory traversal overflow	monitor	4
46.19.86.119	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
84.228.252.55	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.147.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.252	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.210.226.11	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.68.34.134	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.54.32.208	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.143.179	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	74
2.54.43.122	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	63
46.19.85.68	Israel	147.237.72.166	aka.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.68	Block	53
46.19.85.204	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	42
109.253.143.179	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 109.253.143.179	Block	27
46.19.85.70	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	26
37.26.147.177	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 37.26.147.177	Block	18
80.246.137.146	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
46.19.85.67	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
80.246.136.28	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.25	Block	5
192.243.55.136	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.136	Block	4
46.116.195.214	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.148.170	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
192.243.55.138	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.138	Block	3
46.19.85.197	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.147.141	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.147.49	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
82.80.196.44	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
62.0.54.2	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	2
192.243.55.132	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.132	Block	2
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atall/izkor/view_imgtop.asp	Block	2
176.13.13.17	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.253.198.160	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	2
66.249.66.28	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.28	Block	2
37.26.146.253	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.19.85.200	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.86.254	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.24.207.9	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.146	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1
109.253.207.180	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
70.39.157.198	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
217.194.207.227	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https://www.idf.il/	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/2/size220x0/13032.jpg	Block	1
37.26.148.157	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.64.55.123	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.66.31	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.31	Block	1
62.0.41.2	Israel	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/templates/shared/usercontrols/promotioncube/	Block	1
192.243.55.129	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/chinuch/klali/default.asp?catid=42817	Block	1
5.231.208.97	Germany	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
84.108.35.43	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.52.46.255	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.183.138.110	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.47	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/	Block	1
66.249.78.172	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
212.179.21.194	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation ct100\$ContentPlaceholder1\$ucArticleLobbyControl\$txtSearch in www.idf.il/1283-en/dover.aspx	Block	1
37.26.147.141	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
95.108.158.146	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	1
2.54.141.68	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.32.179.39	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1