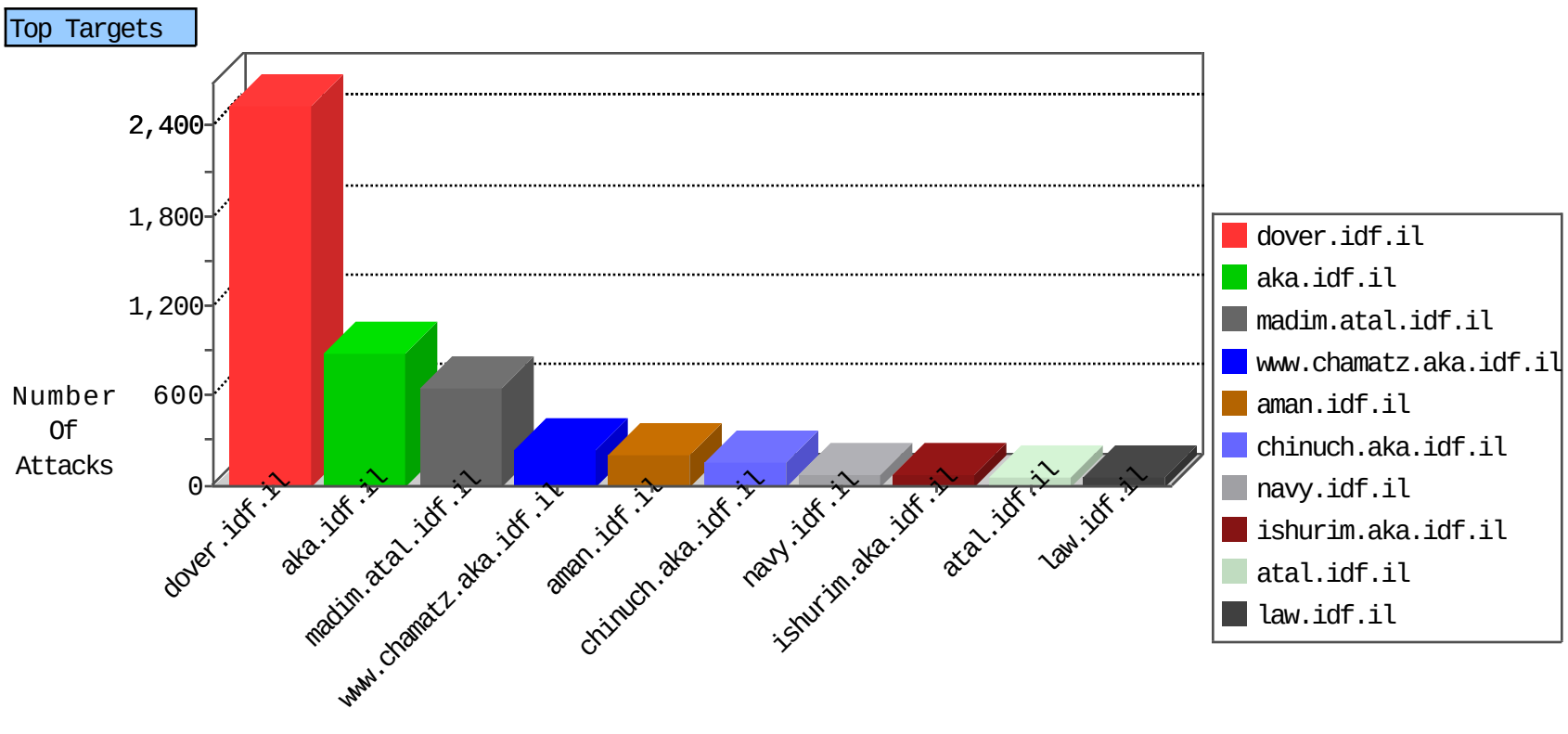
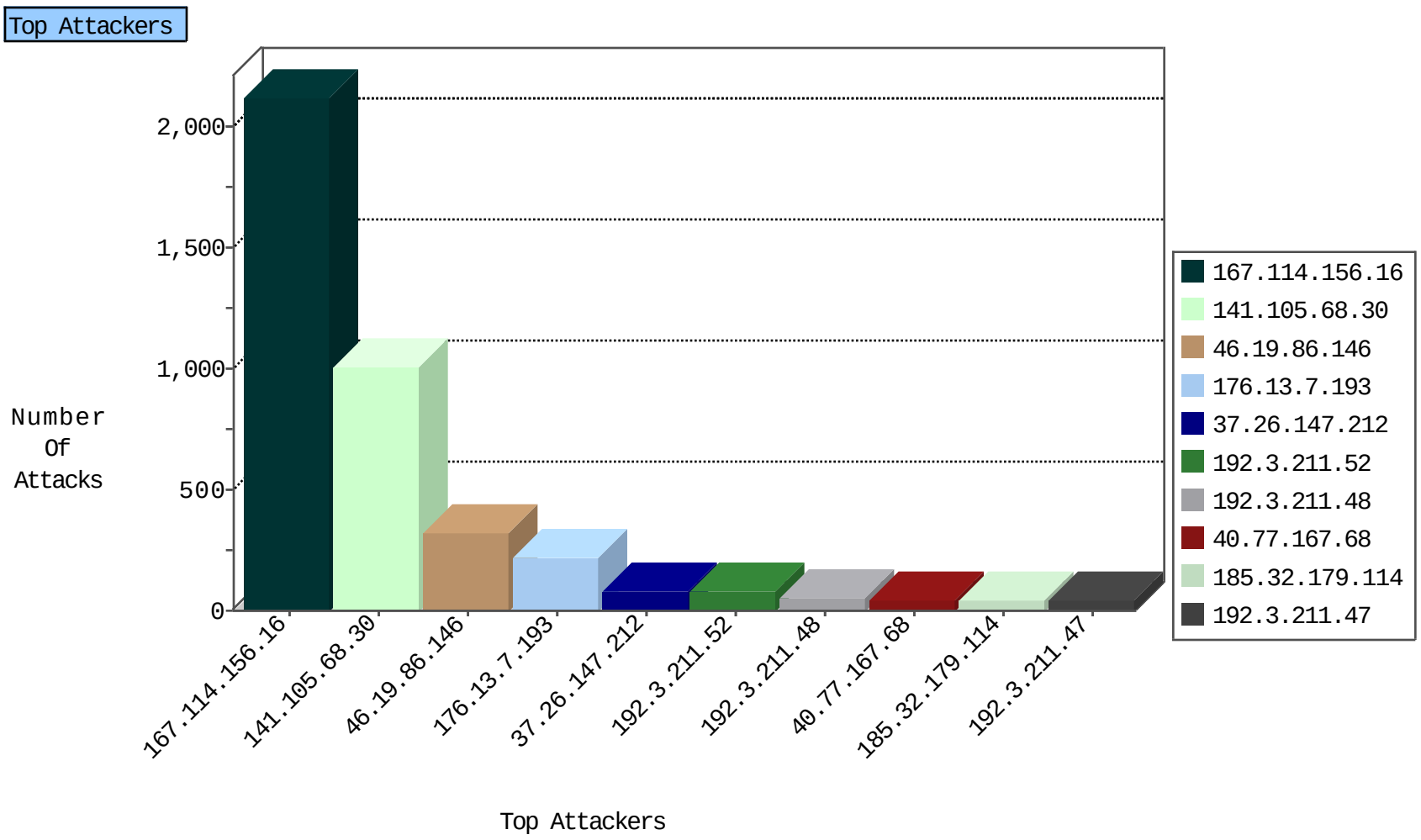
01-12-2016-15:04:07 to 01-12-2016-16:04:07

IDF Under Attack
Daily Report

Top Targets



Top Attackers



01-12-2016-15:04:07 to 01-12-2016-16:04:07

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	3203
85.130.251.227	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	12
66.249.69.26	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
212.179.64.162	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
31.168.152.92	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	3
109.64.68.161	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
31.168.152.92	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
222.186.56.87	China	147.237.76.148	gqcenter.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
202.179.85.72	India	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1

01-12-2016-15:04:07 to 01-12-2016-16:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
208.52.161.177	United States	147.237.77.216	dover.idf.il	C003: HTTP: phpMyAdmin access	Block	1

01-12-2016-15:04:07 to 01-12-2016-16:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
85.65.206.14	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
222.186.56.87	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
80.246.136.32	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.143.43.94	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.49.174	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.168.68.2	147.237.72.14	Slovakia	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
66.249.66.33	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	1
195.168.68.2	147.237.0.33	Slovakia	idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	1
164.39.11.198	147.237.0.15	United Kingdom	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
141.105.68.30	147.237.72.166	Russian Federation	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.137	147.237.77.226	Israel	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	1
109.64.233.149	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.136.227	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.171.10.208	147.237.77.216	France	dover.idf.il	portscan: TCP Distributed Portscan	1
222.186.56.87	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
80.246.140.224	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.2.117	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.168.68.2	147.237.76.197	Slovakia	e.himush.idf.il	ET SCAN Potential SSH Scan	1
66.249.73.214	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
195.168.68.2	147.237.0.35	Slovakia	akaws.idf.il	ET SCAN Potential SSH Scan	1
62.219.120.46	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
168.62.238.153	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.74	China	law.idf.il	ET SCAN Potential SSH Scan	1
141.105.68.30	147.237.77.216	Russian Federation	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
109.226.48.128	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.149.150	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.250.112.98	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

01-12-2016-15:04:07 to 01-12-2016-16:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
141.105.68.30	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	219
141.105.68.30	Russian Federation	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	173
141.105.68.30	Russian Federation	147.237.72.166	aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	151
192.3.211.52	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	38
192.3.211.52	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	37
40.77.167.68	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	37
79.178.1.247	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	34
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
192.3.211.48	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	22
192.3.211.48	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	22
192.3.211.47	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	19
192.3.211.47	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	19
46.19.86.237	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
37.142.64.29	Israel	147.237.77.176	matpash.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
2.54.129.239	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.85.163	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
192.3.211.50	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
192.3.211.50	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
192.3.211.49	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
192.3.211.51	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
192.3.211.51	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
89.249.107.248	Croatia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
192.3.211.53	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
192.3.211.53	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
5.29.212.105	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
37.26.149.231	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.245	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
185.32.179.114	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
192.3.211.49	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
46.19.85.245	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
46.19.85.54	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.86.100	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
5.22.131.14	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.54	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
185.32.179.114	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
185.120.125.32		147.237.72.166	aka.idf.il	drop	SAM rule	drop	8
185.32.179.114	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
109.66.151.110	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
37.26.146.139	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
141.105.68.30	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	7
31.168.155.165	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.152	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.149.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.210.188.67	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.3.144.42	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.134.138	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.201	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.160.242.175	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.147.222	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.69	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

01-12-2016-15:04:07 to 01-12-2016-16:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
141.105.68.30	Russian Federation	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 141.105.68.30	Block	318
46.19.86.146	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	165
46.19.86.146	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.146	Block	147
176.13.7.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	106
176.13.7.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	95
37.26.147.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	76
141.105.68.30	Russian Federation	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 141.105.68.30	Block	72
79.179.200.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
109.64.233.149	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	24
141.105.68.30	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Multiple Unauthorized URL Access from 141.105.68.30	Block	16
141.105.68.30	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 141.105.68.30	Block	13
141.105.68.30	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 141.105.68.30	Block	11
176.13.7.193	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 176.13.7.193	Block	9
141.105.68.30	Russian Federation	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 141.105.68.30	Block	8
46.19.86.146	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtStreet in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	7
31.168.65.25	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 31.168.65.25	Block	4
2.54.129.239	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
2.54.129.239	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	3
141.105.68.30	Russian Federation	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 141.105.68.30	Block	3
176.13.19.98	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.139.29	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
109.253.214.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.22.131.40	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3
89.139.160.41	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 89.139.160.41	Block	3
31.168.65.25	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	3
85.250.24.203	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â	Block	2
185.32.179.114	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
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	2
84.111.138.67	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/www.tikshuv.idf.il	Block	2
37.26.149.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
188.165.89.85	France	147.237.77.176	matpash.idf.il	Distributed Suspicious Response Code	Block	2
208.115.111.72	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	2
188.165.89.85	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
141.105.68.30	Russian Federation	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/kiosk/kiosk.aspx	Block	2
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	2
46.121.44.229	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.76.97.10	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.178.157.105	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.181	Israel	147.237.76.42	refuah.idf.il	Malformed URL	Block	1
139.181.48.2	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/bamahane	Block	1
77.125.79.184	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.13.42	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.147.222	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
109.64.53.189	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.64.53.189	Block	1
5.29.53.99	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
89.139.160.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	1
66.249.66.191	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/size100x0/3049.jpg	Block	1
149.78.136.147	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

01-12-2016-15:04:07 to 01-12-2016-16:04:07