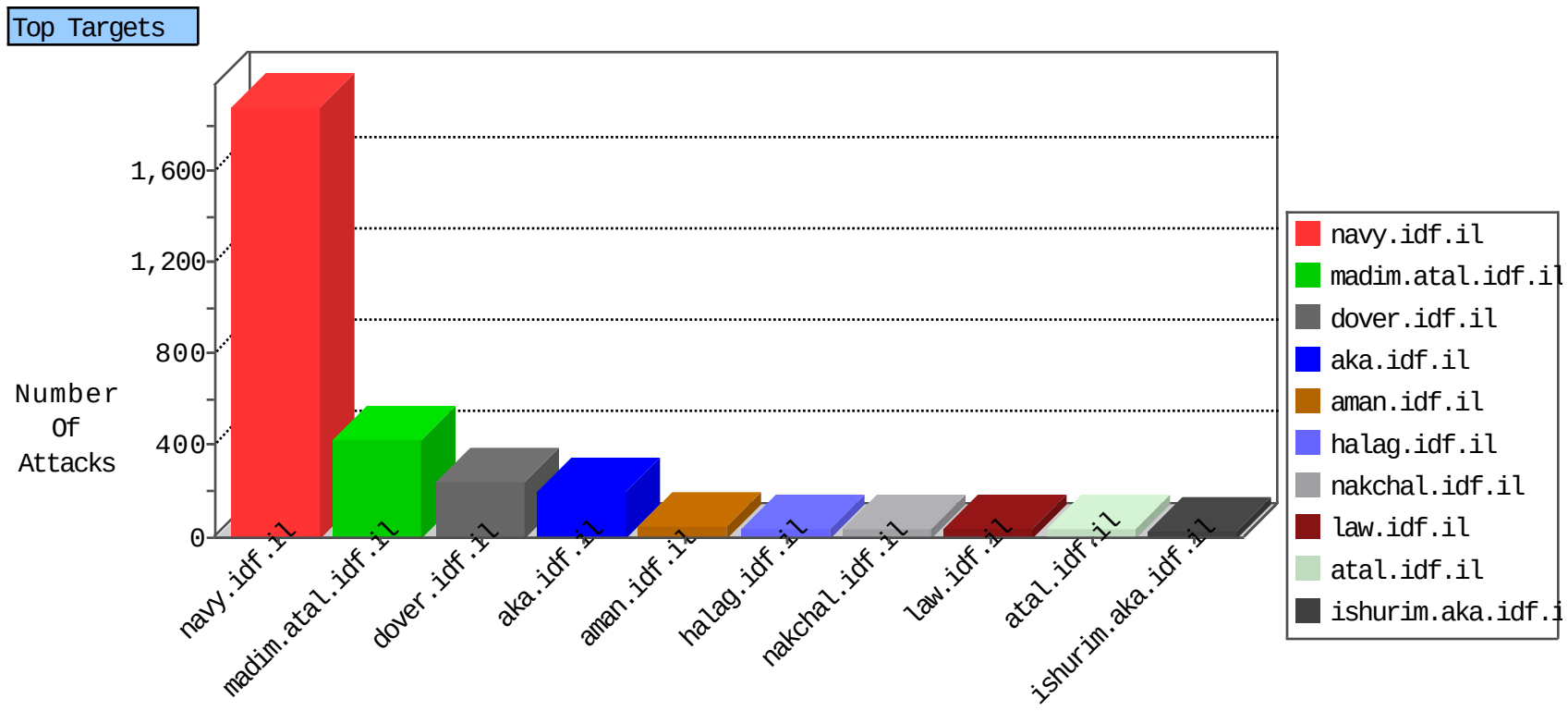
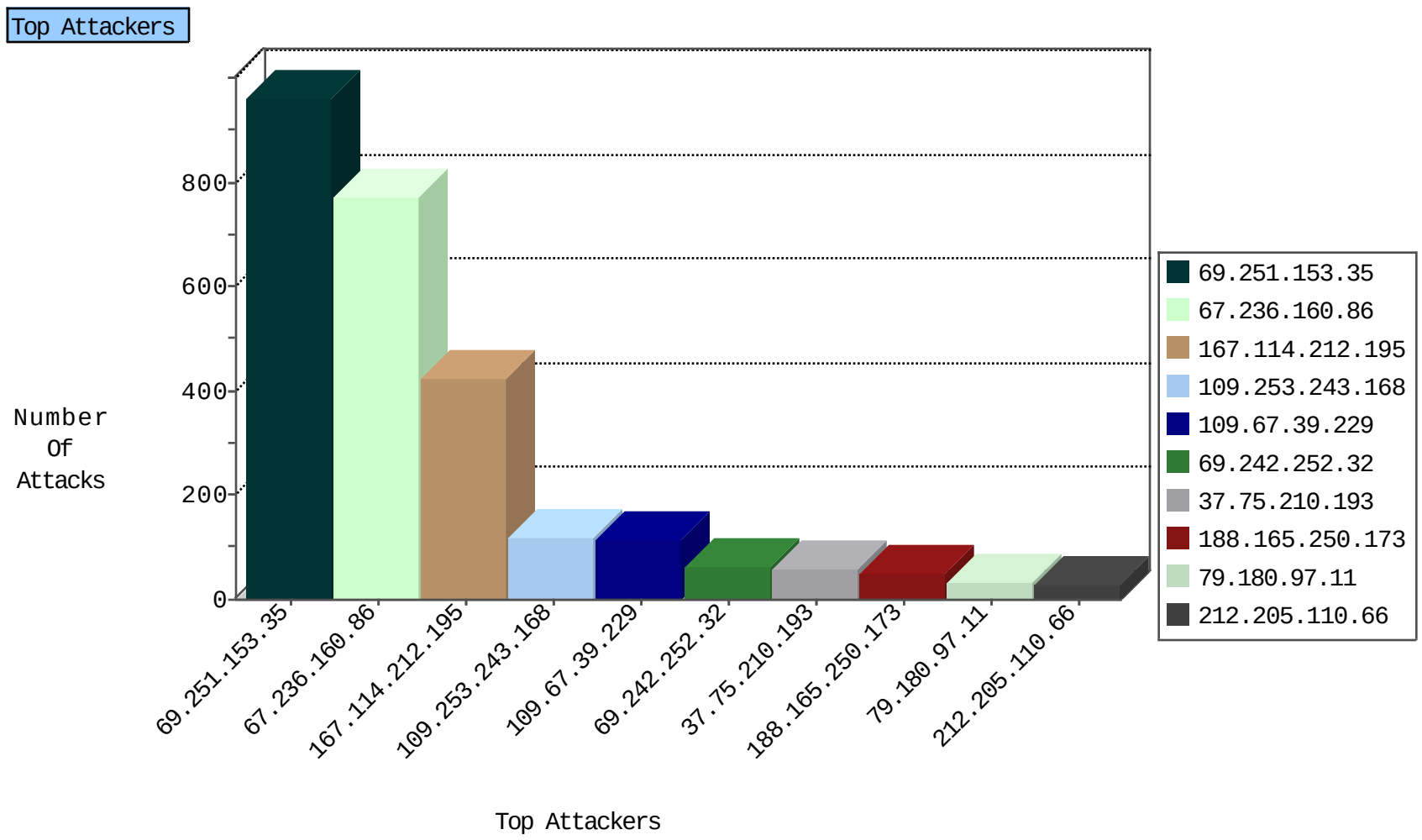
09-05-2016-23:04:04 to 09-06-2016-00:04:04

IDF Under Attack
Daily Report

Top Targets



Top Attackers



09-05-2016-23:04:04 to 09-06-2016-00:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
209.126.136.2	United States	147.237.76.177	ncore.idf.il	Black List	drop	1
217.23.9.123	Netherlands	147.237.76.201	e.atal.idf.il	Black List	drop	1

09-05-2016-23:04:04 to 09-06-2016-00:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.165.250.173	France	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	18
188.165.250.173	France	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
5.196.22.55	France	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
91.109.242.34	United Kingdom	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
85.65.245.178	Israel	147.237.72.156	aman.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
91.219.237.244	Hungary	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1

09-05-2016-23:04:04 to 09-06-2016-00:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
188.165.250.173	147.237.72.166	France	aka.idf.il	SQL Injection - Select From	26
91.109.242.34	147.237.72.166	United Kingdom	aka.idf.il	SQL Injection - Select From	14
5.196.22.55	147.237.72.166	France	aka.idf.il	SQL Injection - Select From	8
45.79.71.122	147.237.72.167	United States	ishurim.aka.idf.il	WEB-MISC Chunked-Encoding transfer attempt	2
46.120.122.219	147.237.77.170	Israel	maarachot.idf.il	Xenu Link Sleuth User Agent	2
109.253.159.41	147.237.76.42	Israel	refuah.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
103.207.36.31	147.237.72.166	Vietnam	aka.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.66	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
201.38.68.132	147.237.77.227	Brazil	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
195.88.154.2	147.237.77.170	Russian Federation	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
23.91.75.231	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
5.255.90.133	147.237.72.167	Netherlands	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.238.45	147.237.8.27	United Kingdom	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.169.150	147.237.76.86	United Kingdom	navy.idf.il	ET SCAN Potential SSH Scan	1
104.197.206.193	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
94.102.48.195	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
66.102.9.130	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	1
195.88.208.193	147.237.76.42	Russian Federation	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
23.91.75.231	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
190.255.143.186	147.237.0.34	Colombia	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
23.91.75.231	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 1024	1
185.32.179.220	147.237.72.156	Israel	aman.idf.il	ET SCAN NMAP -sA (2)	1
163.172.169.150	147.237.76.202	United Kingdom	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1

09-05-2016-23:04:04 to 09-06-2016-00:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
69.251.153.35	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	959
67.236.160.86	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	770
37.75.210.193	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
207.241.229.70	United States	147.237.77.216	dover.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	25
167.114.212.195	Canada	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	21
167.114.212.195	Canada	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	21
167.114.212.195	Canada	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	21
167.114.212.195	Canada	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	20
167.114.212.195	Canada	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	20
167.114.212.195	Canada	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	20
167.114.212.195	Canada	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	20
167.114.212.195	Canada	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	20
167.114.212.195	Canada	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	20
167.114.212.195	Canada	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	20
167.114.212.195	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	20
167.114.212.195	Canada	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
167.114.212.195	Canada	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
167.114.212.195	Canada	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
167.114.212.195	Canada	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
167.114.212.195	Canada	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
167.114.212.195	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
167.114.212.195	Canada	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	18
167.114.212.195	Canada	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	18
167.114.212.195	Canada	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
167.114.212.195	Canada	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
167.114.212.195	Canada	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
69.242.252.32	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	15
69.242.252.32	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
88.152.152.57	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
69.242.252.32	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	14
69.242.252.32	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
212.205.110.66	Greece	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.85.215	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
5.22.134.166	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.125	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
69.242.252.32	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	8
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
77.235.137.58	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.53.134.84	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
37.239.0.29	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
73.148.127.44	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
73.148.127.249	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
66.102.9.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.253.197.149	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.205.110.66	Greece	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
73.148.127.44	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
79.178.53.40	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.166	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
212.205.110.66	Greece	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
212.205.110.66	Greece	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6

09-05-2016-23:04:04 to 09-06-2016-00:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.243.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	118
109.67.39.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	114
79.180.97.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
2.53.186.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
37.26.149.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
37.26.147.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
217.153.185.109	Poland	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
213.8.204.20	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
185.120.124.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
37.26.149.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.55.49.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.138.250.178	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	3
185.32.179.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
157.55.39.115	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
109.253.138.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.230.227.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.139.174	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
174.223.5.82	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	2
31.154.81.34	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	2
80.230.226.38	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.230.226.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
46.117.170.66	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
164.138.113.87	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
87.71.69.246	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.230.226.22	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
77.138.56.243	France	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/favicon.ico	Block	1
66.249.69.97	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/956-he/patzar.aspx	Block	1
185.3.147.238	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/sip_storage/files/2/	Block	1
80.230.226.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
80.230.226.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
45.79.71.122	United States	147.237.72.167	ishurim.aka.idf.i	Multiple Malformed HTTP Header Line from 45.79.71.122	Block	1
79.181.155.155	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
24.185.34.175	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
80.230.227.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
80.230.227.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
207.46.13.181	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/navmenu/	Block	1
80.230.226.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
46.117.216.77	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
89.237.71.95	France	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mas.aspx	None	1
80.230.226.33	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
80.230.227.83	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
66.249.69.101	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/935-4488-he/patzar.aspx	Block	1
80.230.226.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
80.230.226.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
45.79.71.122	United States	147.237.72.167	ishurim.aka.idf.i	Multiple Malformed URL from 45.79.71.122	Block	1
109.253.197.149	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
80.230.226.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
80.230.227.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
80.230.227.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1

09-05-2016-23:04:04 to 09-06-2016-00:04:04