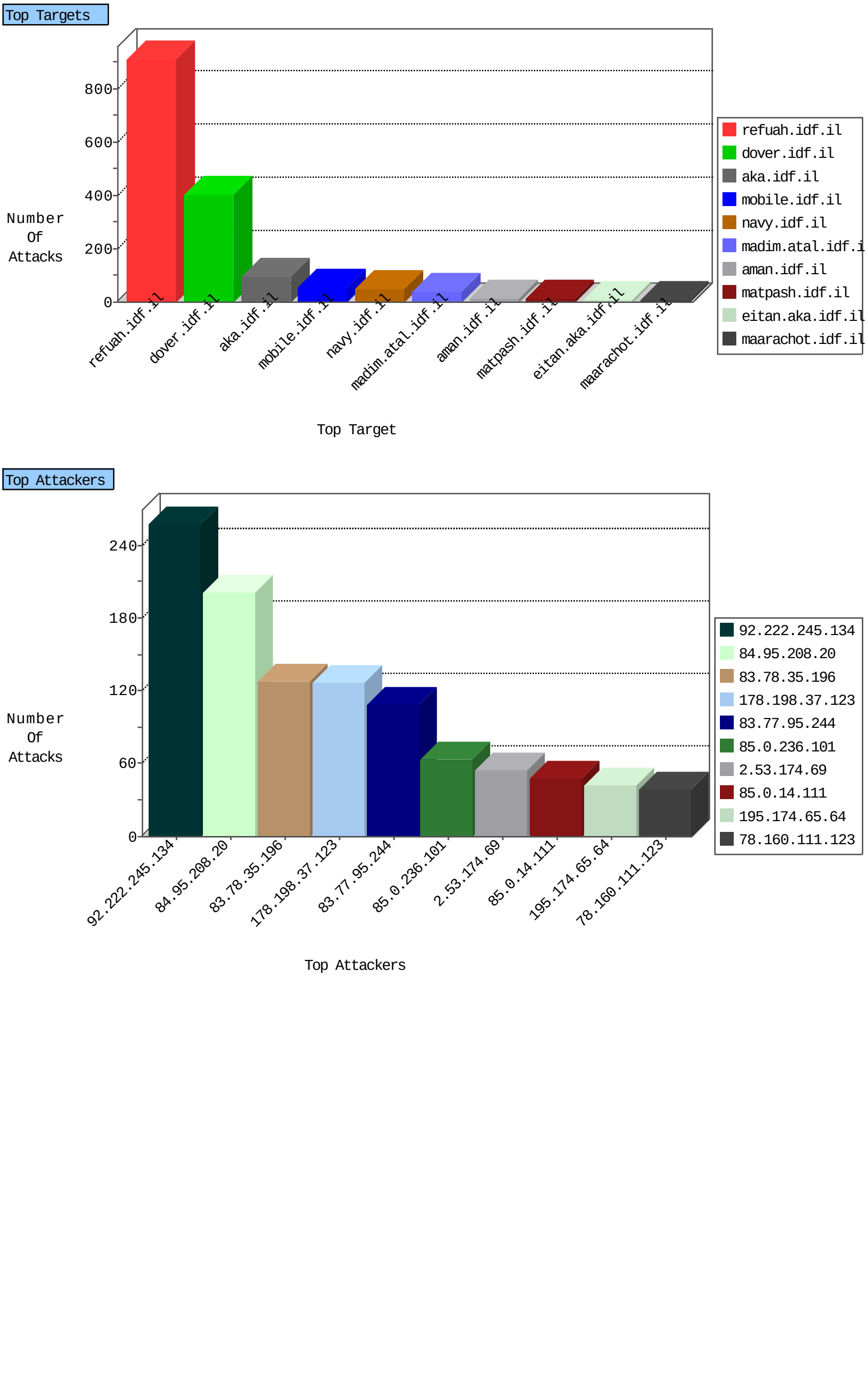
10-02-2016-19:04:04 to 10-02-2016-20:04:04

IDF Under Attack Daily Report



10-02-2016-19:04:04 to 10-02-2016-20:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.45.202	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
134.147.203.115	Germany	147.237.76.202	e.halag.idf.il	Black List	drop	2
104.168.146.142	United States	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1
141.212.122.91	United States	147.237.76.200	eitan.aka.idf.il	Black List	drop	1
115.146.126.249	Vietnam	147.237.76.199	e.nakchal.idf.il	Black List	drop	1
183.129.255.34	China	147.237.76.196	e.sviva.idf.il	JLM_Under_Attack_Con_Http	drop	1
115.146.126.249	Vietnam	147.237.76.200	eitan.aka.idf.il	Black List	drop	1
93.174.95.106	Netherlands	147.237.76.176	test.ncore.idf.il	Black List	drop	1

10-02-2016-19:04:04 to 10-02-2016-20:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.4.32.75	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

10-02-2016-19:04:04 to 10-02-2016-20:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
88.249.106.23	147.237.8.27	Turkey	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
209.95.50.84	147.237.76.86	United States	navy.idf.il	ET SCAN Potential SSH Scan	1
54.71.110.91	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
208.100.26.228	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
46.172.91.21	147.237.72.156	Ukraine	aman.idf.il	ET SCAN NMAP -sS window 1024	1
176.47.123.246	147.237.77.216	Saudi Arabia	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
95.59.136.118	147.237.72.156	Kazakstan	aman.idf.il	ET WEB_SERVER Poison Null Byte	1
91.201.236.155	147.237.76.148	Ukraine	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.72.14	Ukraine	dover.idf.il(old)	ET SCAN NMAP -sS window 2048	1
91.201.236.50	147.237.72.14	Ukraine	dover.idf.il(old)	ET SCAN NMAP -sS window 2048	1
91.201.236.50	147.237.72.14	Ukraine	dover.idf.il(old)	ET DROP Spamhaus DROP Listed Traffic Inbound	1
216.81.230.167	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
79.177.141.211	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
208.100.26.228	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
46.172.91.21	147.237.72.167	Ukraine	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
192.223.73.235	147.237.76.86	Bolivia	navy.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
163.172.129.15	147.237.77.19	United Kingdom	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.76.148	Ukraine	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 3072	1
91.201.236.155	147.237.72.14	Ukraine	dover.idf.il(old)	ET SCAN NMAP -sS window 4096	1
91.201.236.155	147.237.72.14	Ukraine	dover.idf.il(old)	ET SCAN NMAP -f -sS	1
91.201.236.50	147.237.72.14	Ukraine	dover.idf.il(old)	ET SCAN NMAP -f -sS	1

10-02-2016-19:04:04 to 10-02-2016-20:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
92.222.245.134	France	147.237.76.42	refuah.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	254
195.174.65.64	Turkey	147.237.76.42	refuah.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	42
78.160.111.123	Turkey	147.237.76.42	refuah.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	39
2.53.157.190	Israel	147.237.77.243	mobile.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
83.78.35.196	Switzerland	147.237.76.42	refuah.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	27
178.198.37.123	Switzerland	147.237.76.42	refuah.idf.i	Bad TCP sequence	SYN retransmit with different sequence	monitor	26
83.78.35.196	Switzerland	147.237.76.42	refuah.idf.i	Bad TCP sequence	SYN retransmit with different sequence	monitor	26
178.198.37.123	Switzerland	147.237.76.42	refuah.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	26
178.198.37.123	Switzerland	147.237.76.42	refuah.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	26
83.78.35.196	Switzerland	147.237.76.42	refuah.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	26
83.78.35.196	Switzerland	147.237.76.42	refuah.idf.i	Bad TCP sequence	SYN retransmit with different sequence	alert	25
178.198.37.123	Switzerland	147.237.76.42	refuah.idf.i	Bad TCP sequence	SYN retransmit with different sequence	alert	24
178.198.37.123	Switzerland	147.237.76.42	refuah.idf.i	Bad TCP sequence	Invalid ACK number	monitor	24
190.5.48.35	Chile	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
83.78.35.196	Switzerland	147.237.76.42	refuah.idf.i	Bad TCP sequence	Invalid ACK number	monitor	24
83.77.95.244	Switzerland	147.237.76.42	refuah.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	24
83.77.95.244	Switzerland	147.237.76.42	refuah.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	24
83.77.95.244	Switzerland	147.237.76.42	refuah.idf.i	Bad TCP sequence	SYN retransmit with different sequence	alert	21
107.167.107.249	India	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	20
83.77.95.244	Switzerland	147.237.76.42	refuah.idf.i	Bad TCP sequence	SYN retransmit with different sequence	monitor	20
83.77.95.244	Switzerland	147.237.76.42	refuah.idf.i	Bad TCP sequence	Invalid ACK number	monitor	20
82.145.208.40	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	19
85.0.236.101	Switzerland	147.237.76.42	refuah.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
85.0.236.101	Switzerland	147.237.76.42	refuah.idf.i	Bad TCP sequence	SYN retransmit with different sequence	monitor	13
2.53.174.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
85.0.236.101	Switzerland	147.237.76.42	refuah.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	13
85.0.236.101	Switzerland	147.237.76.42	refuah.idf.i	Bad TCP sequence	SYN retransmit with different sequence	alert	12
2.53.174.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
85.0.236.101	Switzerland	147.237.76.42	refuah.idf.i	Bad TCP sequence	Invalid ACK number	monitor	11
85.0.14.111	Switzerland	147.237.76.42	refuah.idf.i	Bad TCP sequence	SYN retransmit with different sequence	monitor	10
85.0.14.111	Switzerland	147.237.76.42	refuah.idf.i	Bad TCP sequence	Invalid ACK number	monitor	10
85.0.14.111	Switzerland	147.237.76.42	refuah.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
85.0.14.111	Switzerland	147.237.76.42	refuah.idf.i	Bad TCP sequence	SYN retransmit with different sequence	alert	9
2.53.174.69	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
79.182.46.159	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
1.39.57.54	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
85.0.14.111	Switzerland	147.237.76.42	refuah.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	9
46.19.86.137	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
62.238.118.145	Netherlands	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
52.3.127.144	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
83.77.94.157	Switzerland	147.237.76.42	refuah.idf.i	Bad TCP sequence	SYN retransmit with different sequence	alert	6
46.19.86.17	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.150	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
185.32.179.161	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.85.150	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.116.64.61	Israel	147.237.77.243	mobile.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
83.77.94.157	Switzerland	147.237.76.42	refuah.idf.i	Bad TCP sequence	Invalid ACK number	monitor	6
84.95.208.20	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
176.13.225.153	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6

10-02-2016-19:04:04 to 10-02-2016-20:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	151
176.13.246.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	14
5.28.146.103	Israel	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	Block	7
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	5
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	5
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	3
80.246.138.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.226.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
83.77.252.251	Switzerland	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/sites/home/default.asp	Block	3
93.37.190.218	Italy	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.51	Block	2
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
66.249.65.52	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_moreinfo.asp	Block	1
213.8.204.18	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/piwik.php	Block	1
77.139.56.173	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
46.19.86.71	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	1
66.249.65.53	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
80.246.133.213	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	1
66.249.65.8	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/apple-app-site-association	Block	1
66.249.65.60	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8847-he/refuah.aspx	Block	1
5.28.146.103	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/sip_storage/files/4/	Block	1
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	1
66.249.76.117	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
23.240.213.120	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/div.item	Block	1
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
77.138.136.173	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
46.19.85.110	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	1

10-02-2016-19:04:04 to 10-02-2016-20:04:04