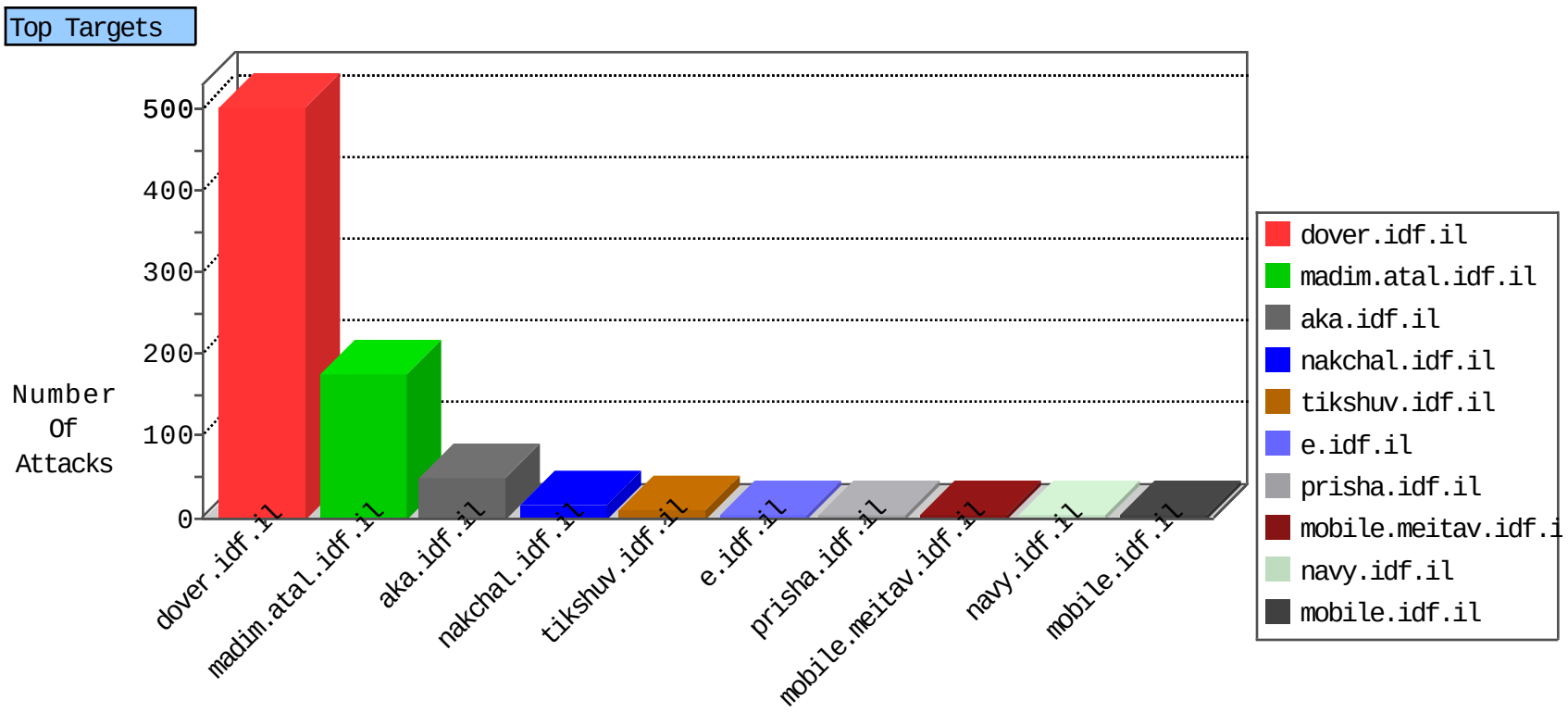
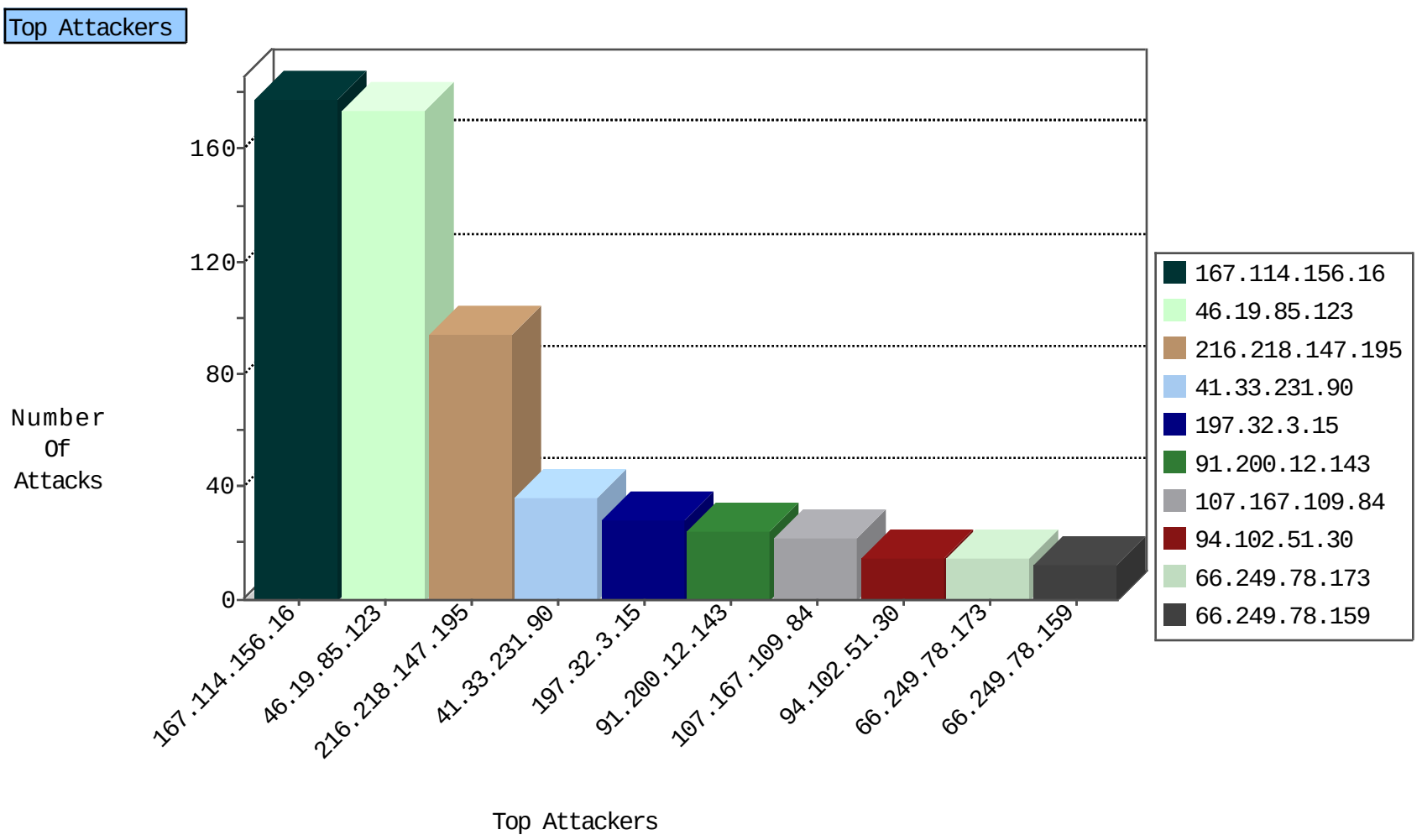
01-09-2016-08:04:00 to 01-09-2016-09:04:00

IDF Under Attack
Daily Report





01-09-2016-08:04:00 to 01-09-2016-09:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.78.9	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	4449
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3344
216.218.147.195	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	76
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	38
197.32.3.15	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	15
66.249.78.173	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	13
66.249.78.159	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
167.114.156.16	Canada	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	7
45.35.64.142		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
157.55.39.2	United States	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
45.35.64.142		147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
37.26.147.110	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
207.46.13.157	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
157.55.39.2	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
173.208.136.170	United States	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
40.77.167.42	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
89.248.174.4	Netherlands	147.237.76.200	eitan.aka.idf.i	Block_Udp_All_Nets	drop	1
204.42.253.132	United States	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1

01-09-2016-08:04:00 to 01-09-2016-09:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.154	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
185.130.5.207		147.237.76.39	mobile.meitav.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
185.130.5.207		147.237.76.39	mobile.meitav.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	1

01-09-2016-08:04:00 to 01-09-2016-09:04:00

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	4
185.130.5.207	147.237.76.39		mobile.meitav.idf.il	ET WEB_SERVER Muieblackcat scanner	1
132.185.161.120	147.237.77.216	United Kingdom	dover.idf.il	portscan: TCP Distributed Portscan	1
121.201.27.61	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
94.102.56.238	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
94.102.48.195	147.237.72.166	Netherlands	aka.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.113	147.237.77.235	Ukraine	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.167.155	147.237.77.234	Netherlands	halag.idf.il	ET SCAN NMAP -sS window 1024	1
50.204.188.142	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
162.13.88.58	147.237.0.17	United Kingdom	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
121.201.27.61	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
94.102.56.238	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
94.102.51.30	147.237.72.166	Netherlands	aka.idf.il	ET SCAN NMAP -sS window 1024	1
93.174.93.203	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.113	147.237.77.235	Ukraine	sviva.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
52.90.147.148	147.237.76.197	United States	e.himush.idf.il	ET SCAN Potential SSH Scan	1
199.191.56.188	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 1024	1

01-09-2016-08:04:00 to 01-09-2016-09:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
107.167.109.84	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	22
216.218.147.195	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	21
216.218.147.195	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
91.200.12.143	Ukraine	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	12
91.200.12.143	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
198.211.102.104	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	8
216.218.147.195	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
216.218.147.195	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
216.218.147.195	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
79.183.101.40	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.139.165	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
85.65.71.200	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
91.200.12.106	Ukraine	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	4
94.242.228.108	Luxembourg	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
93.158.215.174	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
197.32.3.15	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
91.200.12.106	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
197.32.3.15	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.54.141.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.163.95	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
197.32.3.15	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
85.65.71.200	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.240.219.146	United States	147.237.76.177	ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
46.19.86.156	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
50.7.178.98	Netherlands	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
91.200.12.106	Ukraine	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
62.210.209.237	France	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
197.32.3.15	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
220.255.103.46	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
180.102.101.189	China	147.237.0.33	idf.il	drop		drop	2
208.115.113.89	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
45.35.64.142		147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
94.102.51.30	Netherlands	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.206	United States	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.146	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
37.26.147.110	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
81.169.237.146	Germany	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	1
70.39.186.218	Satellite Provide	147.237.72.166	aka.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
94.102.51.30	Netherlands	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.107	United States	147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
61.242.114.152	China	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.151	United States	147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.90	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
85.65.71.200	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.123	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	157
46.19.85.123	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.85.123	Block	17
188.143.232.21	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.143.232.21	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
2.52.18.75	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
79.183.21.237	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
40.77.167.69	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/giyus/qanda/default.asp	None	1
192.243.55.135	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/tizmoret/gallery	Block	1
157.55.39.2	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
209.190.20.61	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
188.143.232.21	Russian Federation	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 188.143.232.21	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.69.38	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1733	Block	1
46.19.85.25	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
192.243.55.136	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=62215	Block	1
157.55.39.222	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in tikshuv.idf.il/site/general.aspx	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
66.249.66.131	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.73.147	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
173.254.203.98	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
68.180.229.173	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.136	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/2970.jpg	Block	1
192.243.55.131	Dominica	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/giyus/kadatz	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18618-he/dover.aspx	Block	1
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	1
173.254.203.98	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/plus/mytag_js.php	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/9/2359.jpg	Block	1
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
31.7.56.133	Switzerland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1153-he/chinuch.aspx	Block	1
64.19.78.242	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
184.105.139.68	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
79.183.101.40	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.69.30	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1880	Block	1

01-09-2016-08:04:00 to 01-09-2016-09:04:00