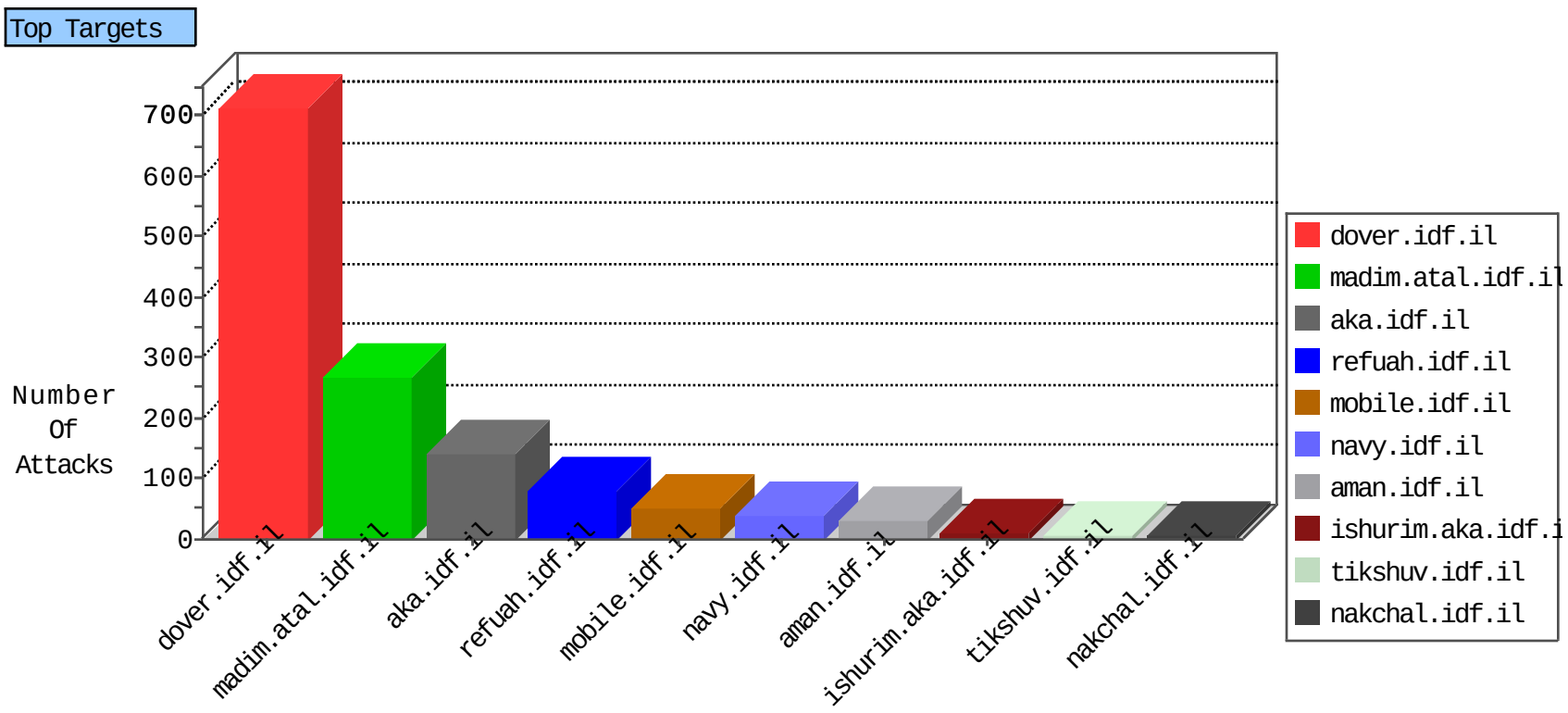
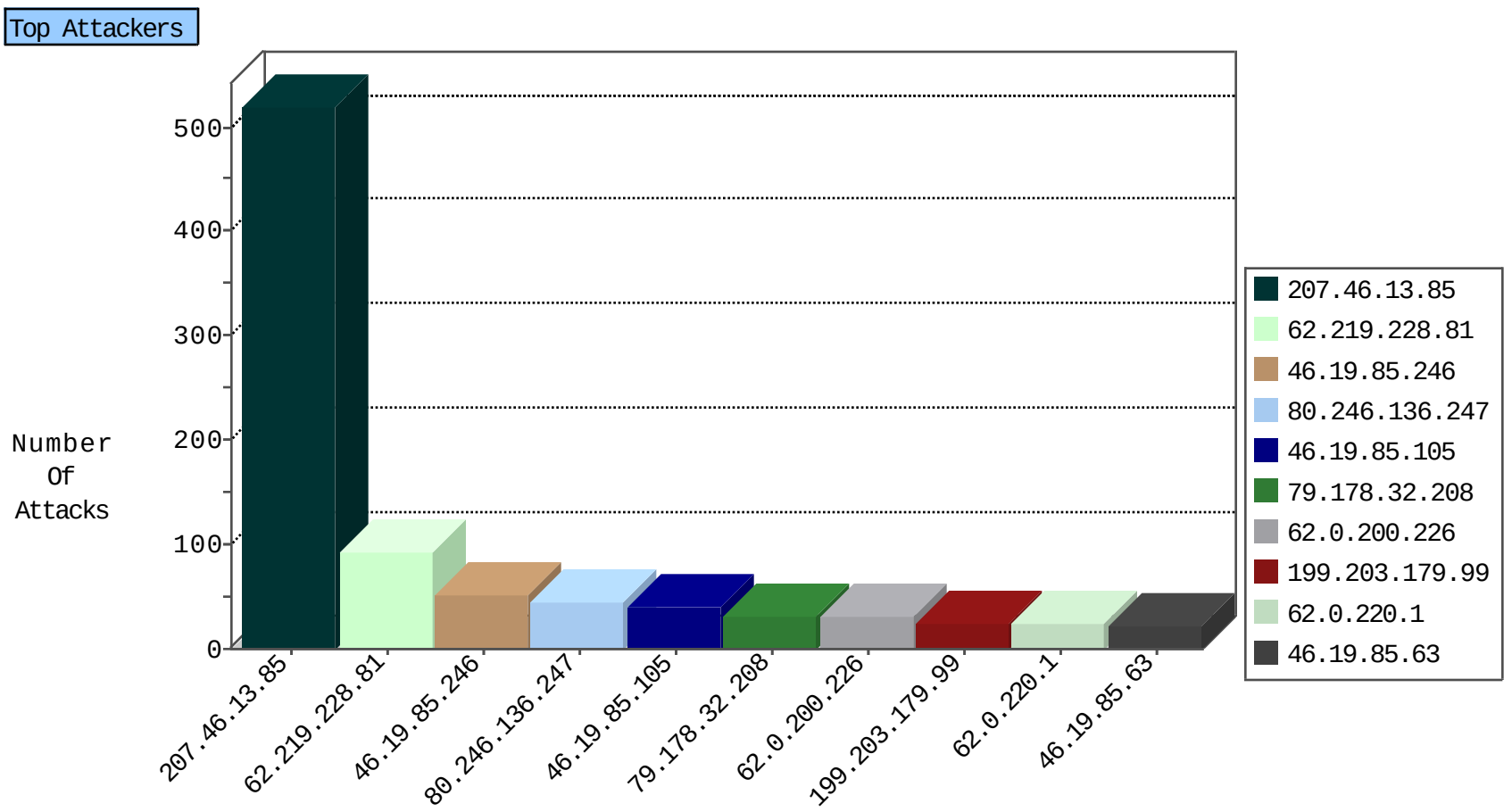
10-05-2016-08:04:02 to 10-05-2016-09:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-05-2016-08:04:02 to 10-05-2016-09:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
94.102.49.190	Netherlands	147.237.76.86	navy.idf.il	Black List	drop	1

10-05-2016-08:04:02 to 10-05-2016-09:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
162.210.196.100	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	4
62.210.250.212	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
69.30.234.186	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

10-05-2016-08:04:02 to 10-05-2016-09:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
109.236.86.32	147.237.77.176	Netherlands	matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
52.57.110.155	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 4096	1
194.56.215.218	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.172.91.21	147.237.0.16	Ukraine	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.169.150	147.237.76.30	United Kingdom	himush.idf.il	ET SCAN NMAP -sS window 1024	1
109.236.86.32	147.237.77.19	Netherlands	law-forum.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
109.236.86.32	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
109.236.86.32	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
208.100.26.228	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
80.246.136.134	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
208.100.26.228	147.237.76.197	United States	e.himush.idf.il	ET SCAN Potential SSH Scan	1
66.249.75.149	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	1
208.100.26.228	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
52.57.110.155	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
180.150.177.188	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
109.236.86.32	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
109.236.86.32	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
109.236.86.32	147.237.76.197	Netherlands	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
109.236.86.32	147.237.72.167	Netherlands	ishurim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
209.126.230.71	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 1024	1
109.236.86.32	147.237.8.24	Netherlands	e.lifestyle.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
208.100.26.228	147.237.76.201	United States	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.93.156	147.237.76.86	Europe	navy.idf.il	ET SCAN NMAP -sA (2)	1
208.100.26.228	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1

10-05-2016-08:04:02 to 10-05-2016-09:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
207.46.13.85	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	520
79.178.32.208	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	30
62.0.200.226	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	30
62.0.220.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
46.19.85.63	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
199.203.179.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
2.55.152.2	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.85.105	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
46.19.85.105	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
82.166.200.204	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	9
62.0.230.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.105	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
213.57.159.128	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.105	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
72.173.128.245	United States	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
37.26.148.166	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.95	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
81.218.170.183	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
80.246.138.84	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.65.8	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.114	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.146.214	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
147.236.34.135	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.237	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.237	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.197	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
109.253.196.243	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.85.174	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
213.57.159.128	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	4
81.218.170.183	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
46.19.85.154	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.253.196.243	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
109.253.130.162	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.85.75	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
185.32.179.61	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	3
37.26.148.162	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
46.19.85.120	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.174	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
212.179.21.194	Israel	147.237.8.27	e.madim.atal.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
185.32.179.61	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
46.19.85.174	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
176.13.3.133	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
80.246.139.231	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.127	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.174	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.86.55	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
80.246.139.231	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
212.25.102.63	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2

10-05-2016-08:04:02 to 10-05-2016-09:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.219.228.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	91
46.19.85.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	52
80.246.136.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	44
185.32.179.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	20
109.253.158.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	19
80.246.137.35	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
87.68.28.172	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	4
2.53.178.46	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
81.218.56.171	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.56.171	Block	4
2.53.130.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
62.0.102.190	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 62.0.102.190	Block	3
185.32.179.199	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.132.77.12	Azerbaijan	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	2
194.90.254.244	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 194.90.254.244	Block	2
85.132.77.12	Azerbaijan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/images/	Block	2
80.246.138.84	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
212.143.66.4	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar	Block	1
68.180.229.178	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/french/nahal.stm.	Block	1
66.249.64.30	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8974-he/refuah.aspx	Block	1
185.23.60.4	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	1
2.55.158.172	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/lomdim	Block	1
66.249.79.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/toolfs.asp	Block	1
176.13.243.107	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
62.0.102.190	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
81.218.118.124	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	1
212.179.155.129	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
68.180.229.184	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1
66.249.64.33	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9698-he/refuah.aspx	Block	1
185.23.60.4	United Kingdom	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
5.255.253.34	Russian Federation	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il/robots.txt	Block	1
194.90.254.244	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/4/	Block	1
66.249.93.83	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/layout.css	Block	1
183.129.160.229	China	147.237.76.42	refuah.idf.il	Malformed HTTP Header Line 1	Block	1
2.53.148.237	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
84.94.192.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
77.138.3.123	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
66.249.75.153	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/navy/general.aspx	Block	1
195.160.242.40	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.93.85	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/1.he/scroller/skin.css	Block	1
183.129.160.229	China	147.237.76.42	refuah.idf.il	Malformed URL	Block	1
84.111.171.47	Israel	147.237.0.34	tikshuv.idf.il	PHP Attempt	Block	1
77.139.106.112	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/information.aspx	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/3/71573.pdf	Block	1
46.19.86.24	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
80.246.138.84	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
203.133.168.162	Korea, Republic of	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/iiyvi/xkoko/templates/sendtofriend/sendtofriend.aspx	Block	1
66.249.93.87	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
66.102.9.24	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
183.129.160.229	China	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method test in URL	Block	1

10-05-2016-08:04:02 to 10-05-2016-09:04:02