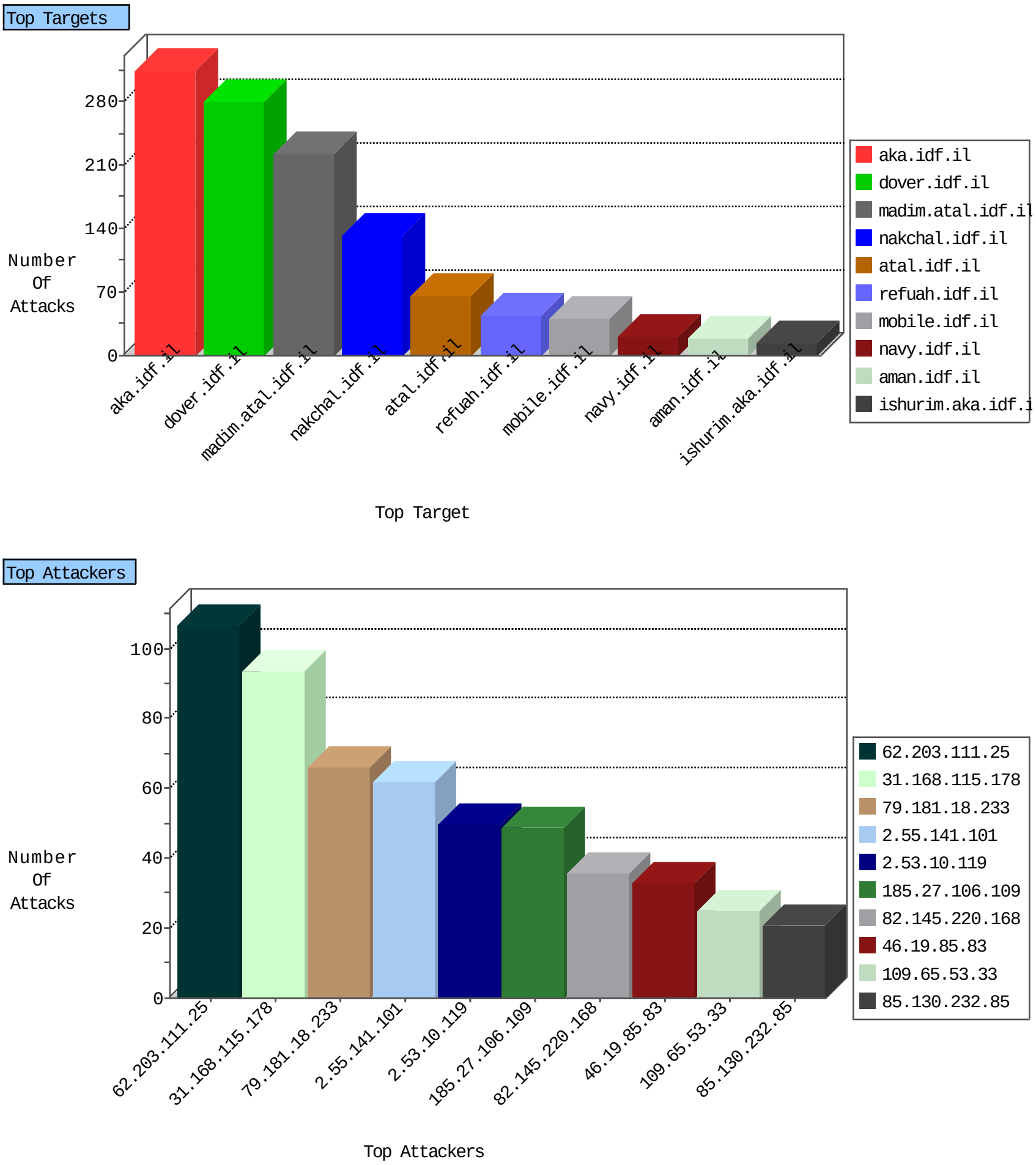
09-28-2016-20:04:07 to 09-28-2016-21:04:07

IDF Under Attack
Daily Report



09-28-2016-20:04:07 to 09-28-2016-21:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
194.177.16.3	Israel	147.237.76.86	navy.idf.il	Black List	drop	2
51.252.53.142	Saudi Arabia	147.237.77.216	dover.idf.il	block-sp-traf1	forward	2
185.94.111.1	Russian Federation	147.237.76.199	e.nakchal.idf.il	Black List	drop	1
198.44.110.25	United States	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1
80.246.136.39	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1

09-28-2016-20:04:07 to 09-28-2016-21:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-28-2016-20:04:07 to 09-28-2016-21:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
80.246.136.39	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	6
46.120.122.219	147.237.77.176	Israel	matpash.idf.il	Xenu Link Sleuth User Agent	2
82.165.26.202	147.237.76.201	Germany	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
82.165.26.202	147.237.76.34	Germany	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
82.165.26.202	147.237.0.33	Germany	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
81.27.85.27	147.237.76.197	United Kingdom	e.himush.idf.il	ET SCAN Potential SSH Scan	1
80.246.137.54	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
180.97.106.37	147.237.77.61	China	e.cogat.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
109.172.11.110	147.237.76.176	Russian Federation	test.ncore.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
82.165.26.202	147.237.76.197	Germany	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
82.165.26.202	147.237.76.31	Germany	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
82.165.26.202	147.237.0.17	Germany	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
80.246.138.92	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
180.97.106.37	147.237.77.235	China	sviva.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
180.97.106.37	147.237.76.39	China	mobile.meitav.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1

09-28-2016-20:04:07 to 09-28-2016-21:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.181.18.233	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	62
82.145.220.168	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
109.65.53.33	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	25
62.203.111.25	Switzerland	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	24
62.203.111.25	Switzerland	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	24
62.203.111.25	Switzerland	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	22
62.203.111.25	Switzerland	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	21
82.145.222.38	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	19
62.203.111.25	Switzerland	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
79.183.82.137	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
88.202.218.237	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
2.53.160.69	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
46.19.85.83	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
79.178.56.7	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
46.19.85.83	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.87	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
172.56.38.75	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
185.27.106.193	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.121.69.162	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.87	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
109.253.141.204	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.76	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.157	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.120.141.64	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.185.155	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.157	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.83	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.53.174.118	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
95.86.127.83	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.76	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.253.142.223	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.85.243	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.29.13.3	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
109.253.192.10	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
2.53.31.186	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
176.13.19.36	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
85.130.232.85	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	5
2.53.31.186	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.116.22.13	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
2.53.160.69	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
85.130.232.85	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
85.130.232.85	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
84.108.136.63	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.83	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.88	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
176.13.19.36	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.86.52	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
176.13.229.255	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
196.217.96.70	Morocco	147.237.77.216	dover.idf.il	drop		drop	4

09-28-2016-20:04:07 to 09-28-2016-21:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
31.168.115.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	94
2.55.141.101	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	62
2.53.10.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	50
185.32.179.157	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	7
77.127.2.178	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	6
185.27.106.109	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 185.27.106.109	Block	4
185.27.106.109	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 185.27.106.109	Block	4
185.27.106.109	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 185.27.106.109	Block	4
185.27.106.109	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	4
185.27.106.109	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 185.27.106.109	Block	4
185.27.106.109	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 185.27.106.109	Block	4
185.27.106.109	Israel	147.237.72.166	aka.idf.il	Multiple Illegal HTTP Version from 185.27.106.109	Block	3
37.46.39.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.120	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.121.69.162	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
185.27.106.109	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
79.178.46.53	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/sip_storage/files/2/71772.pdf‍	Block	2
185.27.106.109	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 185.27.106.109	Block	2
87.69.17.15	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/sip_storage/files/2/71772.pdf‍	Block	2
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	2
184.74.228.5	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/ishurim/main/	Block	2
176.228.220.173	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/general.aspx	Block	2
84.108.152.201	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	2
185.27.106.109	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 185.27.106.109	Block	2
5.28.129.51	Israel	147.237.0.19	madim.atal.idf.il	Distributed Unauthorized URL Access on madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	2
95.86.104.235	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 95.86.104.235	Block	2
185.27.106.109	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 185.27.106.109	Block	2
77.138.90.180	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	Block	1
185.27.106.109	Israel	147.237.72.166	aka.idf.il	Abnormally Long Header Line request header name	Block	1
66.249.66.180	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
180.97.106.37	China	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 180.163.113.82/check_proxy	Block	1
85.64.181.232	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
46.210.182.78	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationexplanation.aspx	None	1
185.27.106.109	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method 3a8NßJãbŸ‡¦Ñš›ÆM›O—ÏÄØ•Ñ&ý8[[#6]]-¿¥,Ïh)>*eEž[[#15]]9½¾—‹{ÿwÛ	Block	1
180.97.106.161	China	147.237.76.30	himush.idf.il	Unauthorized URL Access to 180.163.113.82/check_proxy	Block	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1379-he/dover.aspx	Block	1
217.132.44.95	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.249.64.166	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1754	Block	1
98.230.46.95	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/general.aspx	Block	1
46.19.86.226	Israel	147.237.76.31	nakchal.idf.il	Multiple Unknown HTTP Request Method from 46.19.86.226	Block	1
79.183.64.125	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/1/	Block	1
77.138.93.30	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/	Block	1
185.27.106.109	Israel	147.237.72.166	aka.idf.il	Abnormally Long Request method	Block	1
66.249.66.197	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/templates/sendtofriend/sendtofriend.aspx	Block	1
180.97.106.37	China	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on 180.163.113.82/check_proxy	Block	1
51.252.53.142	Saudi Arabia	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	1
185.27.106.109	Israel	147.237.72.166	aka.idf.il	Illegal HTTP Version	Block	1
79.181.18.233	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
180.97.106.161	China	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 180.163.113.82/check_proxy	Block	1

09-28-2016-20:04:07 to 09-28-2016-21:04:07