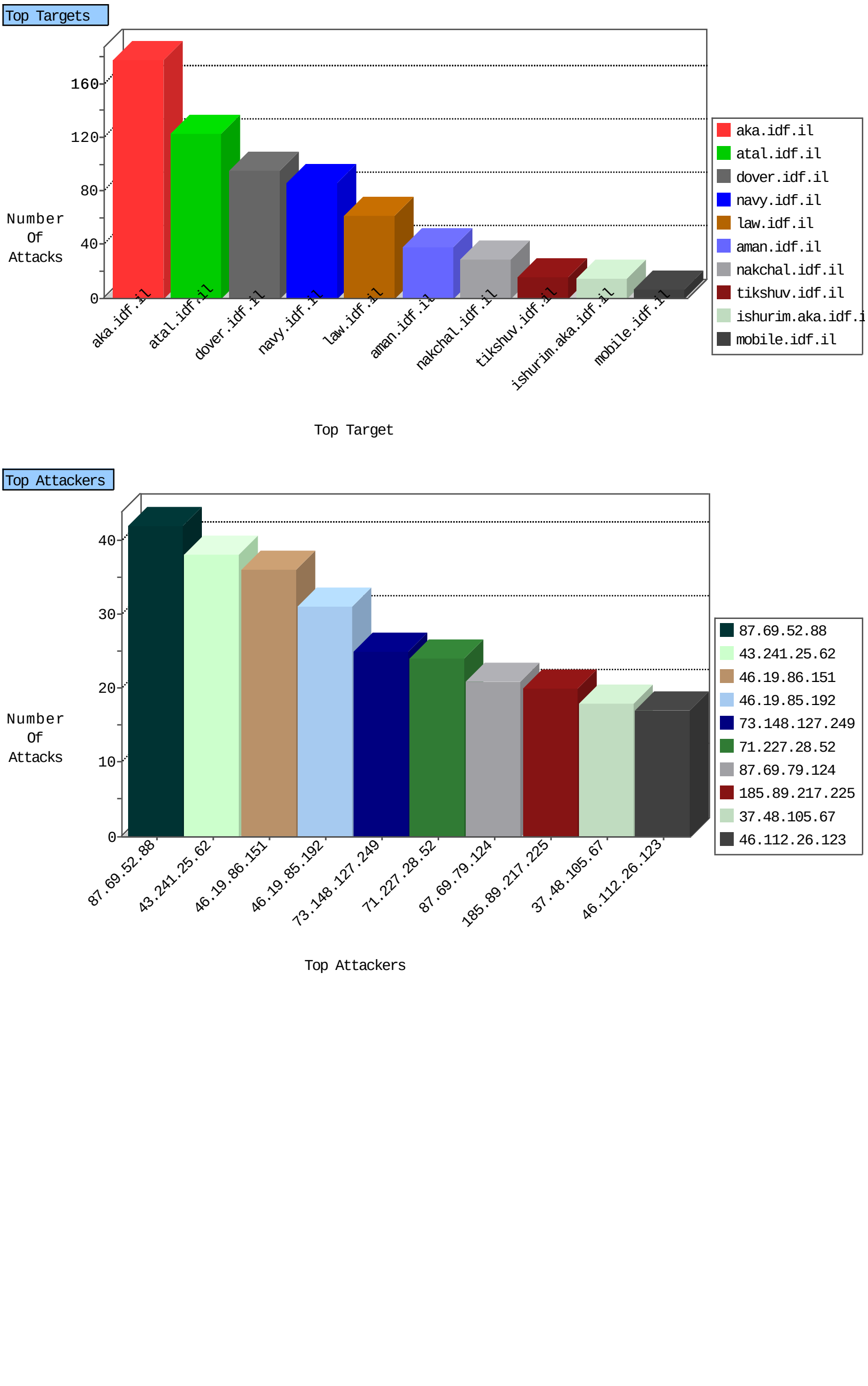
09-09-2016-22:04:04 to 09-09-2016-23:04:04

IDF Under Attack
Daily Report



09-09-2016-22:04:04 to 09-09-2016-23:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	6
185.89.217.232	Netherlands	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	3
134.147.203.115	Germany	147.237.76.38	e.e.meitav.idf.i	Black List	drop	2
185.89.217.226	Netherlands	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	2
109.253.206.207	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
98.139.135.129	United States	147.237.77.233	atal.idf.il	Invalid TCP Flags	drop	1
61.1.44.156	India	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
116.255.250.23	China	147.237.76.199	e.nakchal.idf.il	JLM_Purple_Con_Limit_Http	drop	1
66.240.219.146	United States	147.237.76.177	ncore.idf.il	Black List	drop	1

09-09-2016-22:04:04 to 09-09-2016-23:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.185.31.40	South Africa	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
71.227.28.52	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
72.167.131.22	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
84.245.33.104	Netherlands	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
187.17.109.161	Brazil	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	5
187.17.109.161	Brazil	147.237.77.74	law.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	1

09-09-2016-22:04:04 to 09-09-2016-23:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
71.227.28.52	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	18
41.185.31.40	147.237.72.166	South Africa	aka.idf.il	SQL Injection - Select From	8
84.245.33.104	147.237.77.74	Netherlands	law.idf.il	SQL Injection - Select From	8
72.167.131.22	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
187.17.109.161	147.237.77.74	Brazil	law.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
139.162.170.119	147.237.77.61	United States	e.cogat.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
150.242.238.99	147.237.8.14	China	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
106.186.20.183	147.237.0.17	Japan	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
216.81.230.167	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1
93.158.203.168	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
195.88.208.193	147.237.8.50	Russian Federation	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
190.69.54.66	147.237.77.121	Colombia	e.navy.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
176.58.124.35	147.237.76.196	United Kingdom	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.65	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
176.13.6.227	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
61.240.144.65	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
163.172.129.15	147.237.8.50	United Kingdom	e.tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.172.71.251	147.237.76.38	Ukraine	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.129.15	147.237.8.28	United Kingdom	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
43.241.25.62	147.237.72.166	India	aka.idf.il	ET WEB_SERVER Poison Null Byte	1
93.158.203.168	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
195.88.208.193	147.237.72.166	Russian Federation	aka.idf.il	ET SCAN NMAP -sS window 1024	1
93.158.203.149	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
190.69.233.191	147.237.0.34	Colombia	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
82.221.105.7	147.237.8.45	Iceland	e.eitan.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
176.58.124.35	147.237.72.166	United Kingdom	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.65	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
174.37.222.106	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
46.172.71.251	147.237.76.44	Ukraine	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.129.15	147.237.8.46	United Kingdom	e.chinuch.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

09-09-2016-22:04:04 to 09-09-2016-23:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
43.241.25.62	India	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	28
87.69.52.88	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	22
46.19.85.192	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	22
87.69.52.88	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	20
185.89.217.225	Netherlands	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	20
37.48.105.67	Netherlands	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	18
46.19.86.151	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
213.57.201.91	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	12
46.19.86.151	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
185.89.217.230	Netherlands	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	10
185.89.217.232	Netherlands	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	10
199.203.122.173	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	9
185.89.217.226	Netherlands	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	8
185.89.217.235	Netherlands	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	8
87.69.79.124	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
87.69.79.124	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
185.89.217.228	Netherlands	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	8
46.112.26.123	Poland	147.237.72.156	aman.idf.il	SYN Attack		monitor	7
64.34.186.9	United States	147.237.77.233	atal.idf.il	drop	SAM rule	drop	6
46.19.86.151	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
213.8.204.70	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.89.217.231	Netherlands	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	6
185.89.217.227	Netherlands	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	6
97.88.198.223	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	6
185.89.217.233	Netherlands	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	6
73.148.127.249	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	5
87.70.30.37	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.112.26.123	Poland	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
73.148.127.249	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
185.89.217.234	Netherlands	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	5
87.69.79.124	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
66.249.93.133	Europe	147.237.0.34	tikshuv.idf.il	Directory Traversal	directory traversal overflow	monitor	5
87.70.30.37	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
79.180.250.138	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	5
73.148.127.249	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
73.148.127.249	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
73.148.127.249	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	5
185.89.217.229	Netherlands	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	4
134.35.228.105	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.253.129.224	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
138.246.253.19	Germany	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
46.19.86.151	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.121.234.128	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
134.35.228.105	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.192	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
134.35.171.124	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
109.253.206.207	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.112.26.123	Poland	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
176.13.247.42	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3

09-09-2016-22:04:04 to 09-09-2016-23:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
110.89.17.48	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 110.89.17.48	Block	12
110.89.17.48	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	4
37.26.148.178	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	3
66.249.66.78	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/shared/ajax/setivgallerycontrol.aspx	Block	2
195.90.103.48	Poland	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
109.67.174.110	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
66.249.66.176	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
43.241.25.62	India	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method q[[#0]][[#0]][[#0]]%9L•Åj[[#3]]ÑbJ[[#24]]o©Ð[[#31]]%›ìêvÚoî6N[[#23]][[#1]]¼H[[#18]]»D«Õ	Block	1
176.13.6.227	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
80.179.188.234	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
43.241.25.62	India	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
213.8.204.48	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/.aspx	Block	1
5.29.138.189	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dover/site/mainpage.asp	Block	1
66.249.66.251	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/kamlar/adv.asp	Block	1
43.241.25.62	India	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL d¯ßƴg[[Ꮭ#25…ûŒ×[]]82#[[$c;mv]]¦t-Ùgb³¨[[#3]]÷w[[#30]]	Block	1
185.89.217.226	Netherlands	147.237.77.233	atal.idf.il	URL is Above Root Directory www.atal.idf.il/../images/shared/ie.gif	Block	1
89.138.222.85	Israel	147.237.76.42	refuah.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
43.241.25.62	India	147.237.72.166	aka.idf.il	Unknown HTTP Request Method q[[#0]][[#0]][[#0]]%9L•Åj[[#3]]ÑbJ[[#24]]o©Ð[[#31]]%›ìêvÚoî6N[[#23]][[#1]]¼H[[#18]]»D«Õ in URL d¯ßƴg[[Ꮭ#25mv]]	Block	1
213.8.204.70	Israel	147.237.77.243	mobile.idf.i	Distributed Suspicious Response Code	Block	1
66.249.93.137	Israel	147.237.0.34	tikshuv.idf.	Distributed URL is Above Root Directory	Block	1
43.241.25.62	India	147.237.72.166	aka.idf.il	Illegal HTTP Version	Block	1
185.159.37.6		147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 185.159.37.6	Block	1
94.142.238.190	Czech Republic	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/general.aspx	Block	1
66.102.9.2	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
43.241.25.62	India	147.237.72.166	aka.idf.il	Abnormally Long Request method	Block	1
139.162.185.240	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
68.180.229.190	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1589-en/dover.aspxthe	Block	1
43.241.25.62	India	147.237.72.166	aka.idf.il	Malformed URL d¯ßƴg[[Ꮭ#25]]03#[[w÷]]3#[[¨³bgÙ-t¦…ûŒ×[]]82#[[$c;mv]]	Block	1
188.161.30.115	Palestinian Territory, Occupied	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/favicon.ico	Block	1
109.65.102.254	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
43.241.25.62	India	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name	Block	1
157.55.39.253	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	1
79.177.157.25	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
43.241.25.62	India	147.237.72.166	aka.idf.il	NULL Character in Method q[[#0]][[#0]][[#0]]%9L•Åj[[#3]]ÑbJ[[#24]]o©Ð[[#31]]%›ìêvÚoî6N[[#23]][[#1]]¼H[[#18]]»D«Õ	Block	1

09-09-2016-22:04:04 to 09-09-2016-23:04:04