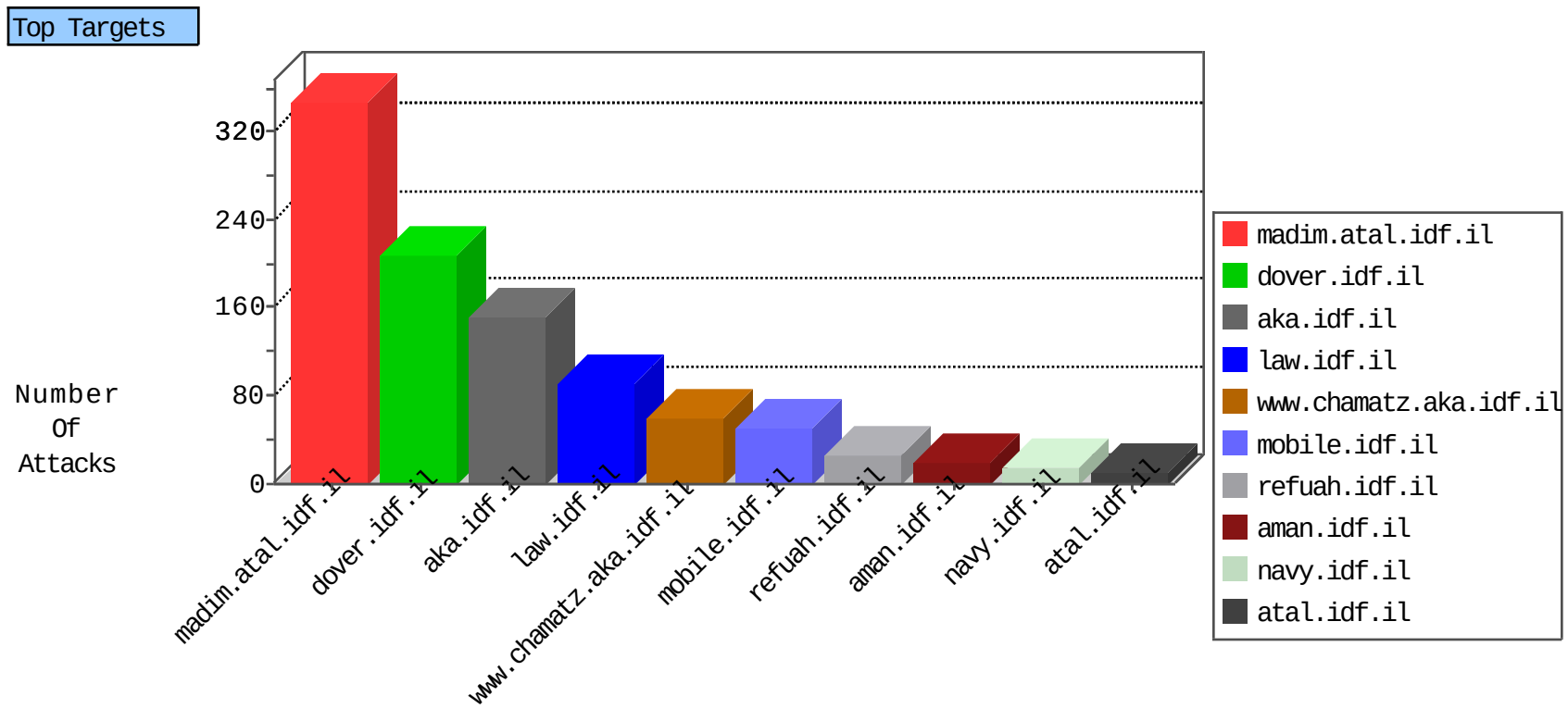
09-30-2016-11:04:03 to 09-30-2016-12:04:03

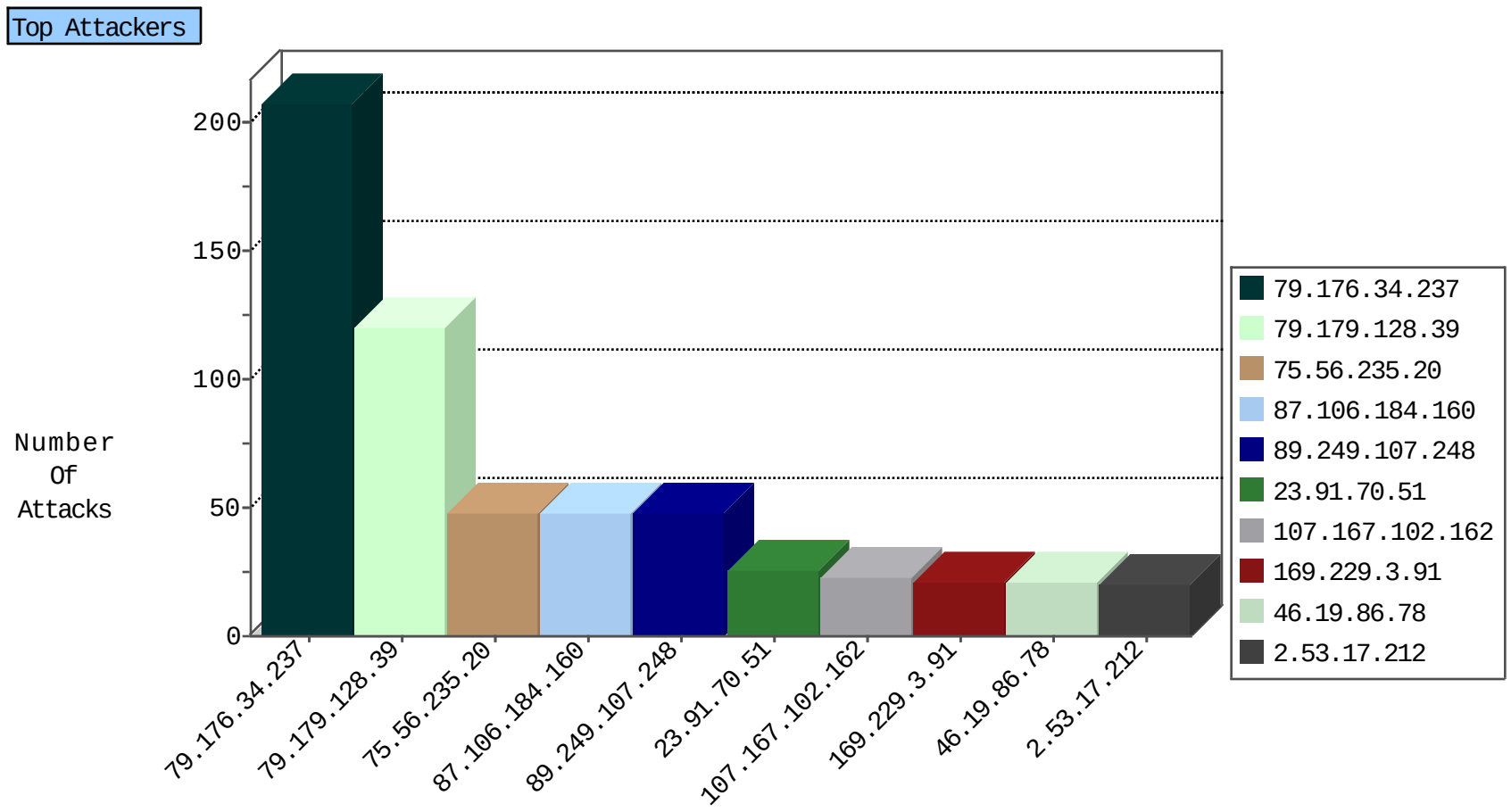
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

09-30-2016-11:04:03 to 09-30-2016-12:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.182.143.180	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	16
185.89.217.233	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	7
71.19.252.114	Canada	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
185.94.111.1	Russian Federation	147.237.76.176	test.ncore.idf.il	Black List	drop	1
91.210.104.40	Russian Federation	147.237.76.42	refuah.idf.il	Black List	drop	1
212.179.75.114	Israel	147.237.77.216	dover.idf.il	Black List	drop	1
77.138.52.97	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
176.13.249.195	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
78.129.171.175	United Kingdom	147.237.76.30	himush.idf.il	Black List	drop	1

09-30-2016-11:04:03 to 09-30-2016-12:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
75.56.235.20	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	12
87.106.184.160	Germany	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
23.91.70.51	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
87.106.184.160	Germany	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
23.91.70.51	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
162.210.196.100	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3
106.38.241.106	China	147.237.76.31	nakchal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
74.208.218.66	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	2

09-30-2016-11:04:03 to 09-30-2016-12:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
75.56.235.20	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	36
87.106.184.160	147.237.77.74	Germany	law.idf.il	SQL Injection - Select From	36
23.91.70.51	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	14
74.208.218.66	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	10
221.138.139.89	147.237.8.14	Korea, Republic of	e.orchot.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
62.210.113.73	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
183.60.48.25	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
167.58.40.222	147.237.77.61	Uruguay	e.cogat.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
125.65.82.44	147.237.76.42	China	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
106.187.45.144	147.237.0.17	Japan	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
66.249.93.135	147.237.77.233	Europe	atal.idf.il	ET SCAN NMAP -sA (2)	1
201.114.60.162	147.237.76.177	Mexico	ncore.idf.il	ET SCAN NMAP -sS window 3072	1
42.116.76.87	147.237.77.74	Vietnam	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.32.179.246	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
163.172.169.150	147.237.0.15	United Kingdom	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
125.65.82.44	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
202.67.237.220	147.237.77.212	Hong Kong	e.dover.idf.il	ET SCAN Potential SSH Scan	1
187.136.207.131	147.237.72.156	Mexico	aman.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

09-30-2016-11:04:03 to 09-30-2016-12:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
89.249.107.248	Croatia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
107.167.102.162	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	23
37.26.148.150	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	13
46.19.86.78	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
185.89.217.235	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	10
46.19.86.78	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
185.89.217.226	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	8
185.89.217.229	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.99	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.55.29.92	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.89.217.225	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.99	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
62.0.223.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
83.130.68.240	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.220.220	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.78	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.78	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.89.217.228	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
176.13.2.8	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
2.53.17.212	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
185.89.217.234	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	4
2.53.17.212	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
66.249.93.79	Europe	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.1	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
185.89.217.230	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	4
2.53.17.212	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.53.17.212	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
185.89.217.227	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	4
79.178.27.92	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
2.53.17.212	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
185.89.217.233	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	4
2.55.164.232	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
46.151.209.187	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
93.172.96.134	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.97	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.85.97	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
185.89.217.232	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	3
5.102.195.155	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
176.13.6.68	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
2.53.164.202	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
91.140.76.219	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.116.42.69	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.1	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
109.65.98.57	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
157.55.39.145	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
37.26.148.242	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
77.139.21.46	France	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.116.42.69	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
178.59.231.224	Greece	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2

09-30-2016-11:04:03 to 09-30-2016-12:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.176.34.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	208
79.179.128.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	120
176.13.249.195	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/login parameter Password	Block	10
80.246.138.97	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter NewPassword	Block	9
109.253.209.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
89.249.107.248	Croatia	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 89.249.107.248	Block	5
80.246.138.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
77.139.96.184	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	3
62.128.45.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.12	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	3
109.64.57.226	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.139.68.202	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	3
87.69.171.96	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.19.86.127	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
5.29.147.10	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
84.95.208.20	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
169.229.3.91	United States	147.237.76.30	himush.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
77.127.84.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
2.53.27.64	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/null	Block	1
185.27.106.228	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation aspxerrorpath in www.idf.il/error.htm	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
169.229.3.91	United States	147.237.76.39	mobile.meitav.idf.il	NULL Character in Method n“[[#0]]Ÿ‘lÿ`&[[#1]]>Ý4[[#19]]ê,êú„"ÔúQ¹ÄwX[[#2]][[#22]]ù©[[#31]]ÊÓ9•‹¦3Šs9‘æØ[[#7]]•(CÛU‰	Block	1
66.249.66.101	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
23.247.85.14	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
79.181.71.112	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
169.229.3.91	United States	147.237.76.39	mobile.meitav.idf.il	Abnormally Long Request method	Block	1
77.138.70.180	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/null	Block	1
2.55.156.180	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
192.243.55.134	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.134	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	PHP Attempt	Block	1
77.139.213.24	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	Block	1
169.229.3.91	United States	147.237.76.39	mobile.meitav.idf.il	Unknown HTTP Request Method n“[[#0]]Ÿ‘lÿ`&[[#1]]>Ý4[[#19]]ê,êú„"ÔúQ¹ÄwX[[#2]][[#22]]ù©[[#31]]ÊÓ9•‹¦3Šs9‘æØ[[#7]]•(CÛU‰ in URL =Ùz[[`ıı#18ЖП]]±	Block	1
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/edim/theproj/	Block	1
109.253.220.220	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
43.226.15.161	Cambodia	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar	Block	1
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.il	Unknown HTTP Request Method ,ÝA³}"¾L»ƒf[[#5]]ÐØ	Block	1
169.229.3.91	United States	147.237.76.39	mobile.meitav.idf.il	Illegal Byte Code Character in Method n“[[#0]]Ÿ‘lÿ`&[[#1]]>Ý4[[#19]]ê,êú„"ÔúQ¹ÄwX[[#2]][[#22]]ù©[[#31]]ÊÓ9•‹¦3Šs9‘æØ[[#7]]•(CÛU‰	Block	1
77.139.50.126	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
66.102.6.23	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
89.249.107.248	Croatia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
192.243.55.134	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=62296&docid=77012	Block	1
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Distributed PHP Attempt	Block	1
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.il	Abnormally Long Request method	Block	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Abnormally Long Request method	Block	1
66.249.93.85	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/3v2	Block	1
169.229.3.91	United States	147.237.76.39	mobile.meitav.idf.il	Illegal Byte Code Character in URL =Ùz[[`ıı#18Жп]]±	Block	1
77.139.52.146	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	1

09-30-2016-11:04:03 to 09-30-2016-12:04:03