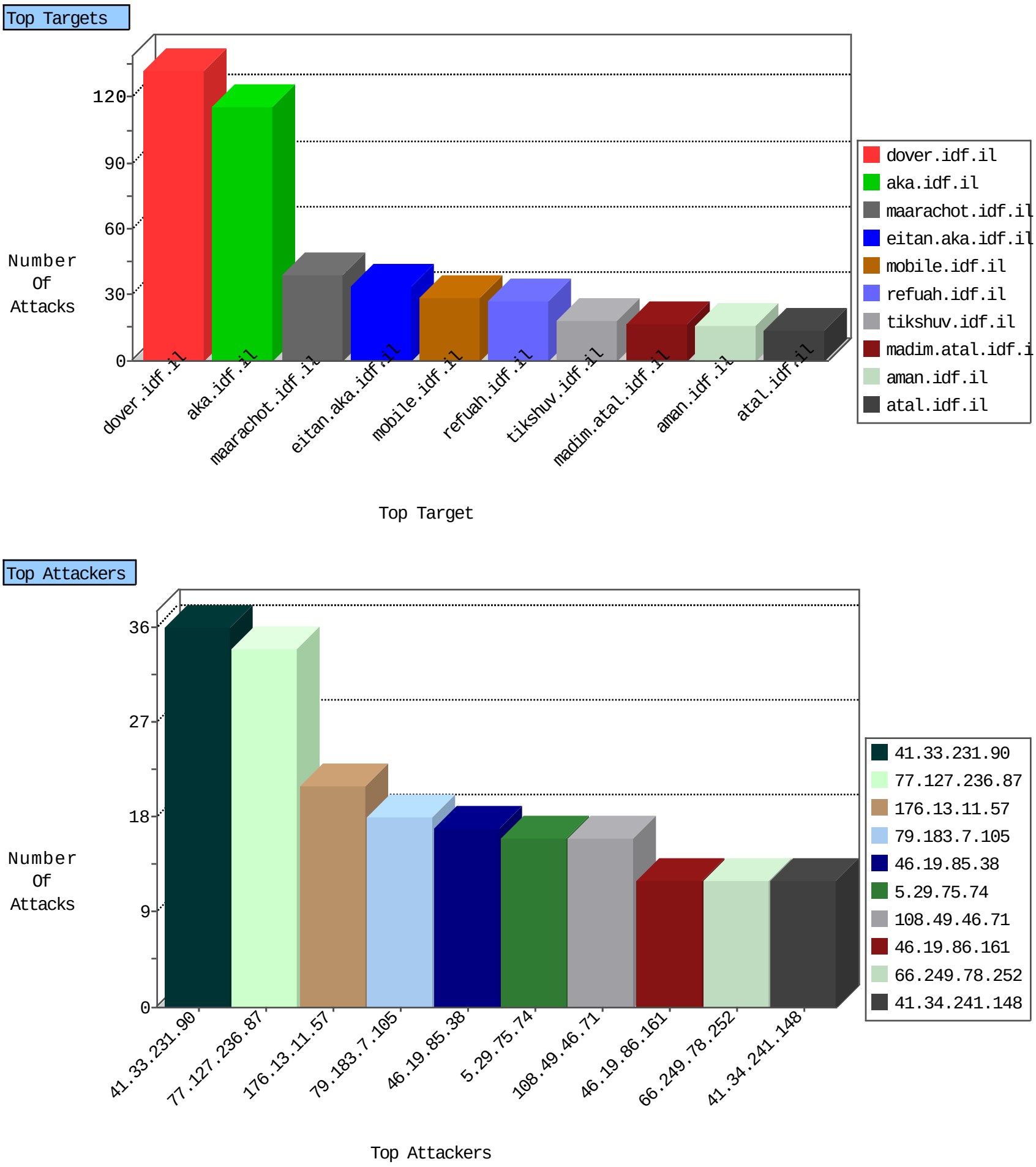
02-11-2016-00:04:03 to 02-11-2016-01:04:03

IDF Under Attack
Daily Report



02-11-2016-00:04:03 to 02-11-2016-01:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
142.54.169.163	United States	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	drop	1

02-11-2016-00:04:03 to 02-11-2016-01:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.127.236.87	Israel	147.237.77.170	maarachot.idf.il	C122: HTTP: Access to - .exe or .dll	Permit	7

02-11-2016-00:04:03 to 02-11-2016-01:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
77.127.236.87	147.237.77.170	Israel	maarachot.idf.il	WEB-FRONTPAGE /_vti_bin/ access	7
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
218.246.0.97	147.237.76.176	China	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
121.201.27.61	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
68.196.88.100	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
51.254.23.230	147.237.8.45	United Kingdom	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
51.254.23.230	147.237.0.33	United Kingdom	idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
177.245.83.35	147.237.72.14	Mexico	dover.idf.il(old)	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
51.254.23.230	147.237.72.217	United Kingdom	e.idf.il	ET SCAN Potential SSH Scan	1
51.254.23.230	147.237.8.28	United Kingdom	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1

02-11-2016-00:04:03 to 02-11-2016-01:04:03

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
176.13.11.57	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
79.183.7.105	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.86.161	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.249.78.252	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.116.42.172	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
62.219.213.32	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.38	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.85.38	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.71	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
77.126.103.233	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.35.186	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
91.200.12.106	Ukraine	147.237.76.200	eitan.aka.idf.il	drop	SAM rule	drop	4
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
91.200.12.143	Ukraine	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
105.128.63.176	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
85.130.246.228	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
91.200.12.143	Ukraine	147.237.76.200	eitan.aka.idf.il	drop	SAM rule	drop	4
85.130.246.228	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
37.26.148.246	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
91.200.12.106	Ukraine	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
79.181.206.37	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.157.46	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
72.14.229.81	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
105.128.63.176	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
128.194.3.195	United States	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
79.178.152.159	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.129.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.176.109	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
115.186.243.50	Australia	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.184.144	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.180	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.5.126	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
128.194.3.195	United States	147.237.72.166	aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
5.28.190.72	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.177.233	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.38	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.187.160	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
77.127.150.244	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.26.15	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.46.192	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
93.158.152.49	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.80.130.133	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.24.51	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.19.218	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-11-2016-00:04:03 to 02-11-2016-01:04:03

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
79.179.222.172	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.130.246.228	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
109.67.111.173	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-11-2016-00:04:03 to 02-11-2016-01:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.29.75.74	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
77.127.236.87	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 77.127.236.87	Block	12
37.26.146.153	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1432	Block	8
108.49.46.71	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	7
77.127.236.87	Israel	147.237.77.170	maarachot.idf.il	Multiple _vti_ from 77.127.236.87	Block	7
108.49.46.71	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 108.49.46.71	Block	7
46.19.85.71	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.136.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.67.202.42	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 217.194.198.104 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	2
79.177.171.153	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/sachar	Block	2
37.26.147.223	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	2
108.49.46.71	United States	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/1065-en/dover.aspx parameter SearchText	Block	2
66.249.64.58	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/4/109444.pdf	Block	1
177.228.5.182	Mexico	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/2063-en/congat.aspx	Block	1
109.67.202.42	Israel	147.237.72.166	aka.idf.il	Malformed HTTP Header Line 2	Block	1
41.34.241.148	Egypt	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/xmlrpc.php	Block	1
41.34.241.148	Egypt	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	1
213.57.182.159	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/main/rabanut/general.aspx	None	1
157.55.39.41	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/modiin/modiin/modiin/default.aspx	Block	1
41.34.241.148	Egypt	147.237.77.74	law.idf.il	PHP Attempt	Block	1
66.249.64.239	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/templates/shared/usercontrols/navmenu/undefined	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1065-he/kkkkkkk=5463f033kkkkkkk_5463f033	Block	1
109.67.202.42	Israel	147.237.72.166	aka.idf.il	NULL Character in Header Name at mÂ'@JÂŽÃ¸6Ã™&Ã‹.[[#19]]Â¾Ã³.Â†ÂŠ =hY-Â¹[[#22]]ÂµÃ›d[[#15]]+Â‡Â»pJÃ§Ã¤_[[#24]][[#24]]Â?Ã°Ã¨Ã€ CÂ²m]Â¯DÃŸKÃ•Â,Â'[[#12]]Â"Ã°Â-,Â'Ã¼[[#8]]Ã·G[[#8]]Â¡h[[#16]])Ã† CÂ®+>Ã€o3[[#6]]Â•{Bn/Â‰Ã‹ [[#25]][[#19]]BÂ?[[#25]]Ã±q*[[#22]]5[[#3]][[#18]]!bÂ…6Â¹Â…Â–Ã^ ,Â³KÂ±[[#25]]Â§Ã»[[#16]]Â²^jÃ›Ã‰[[#5]]ÂƒÂ½Â?[[#31]]Â´Â,sÂ' BÂ¡I*G(j[[#20]]Ã vÂ®(7Â'OHD[[#31]]Ã…mÃ¸ÃšMÃ†Â¾Â£dÂ¢'ÂªVÃ"Ã' Âº0gÂµ[[#31]]Â"Âœ<?@{iÂ¦Â¢ÃœFÃ²5AÂ«=Ã-pÂ·'Ã½Â€[[#0]]?Â¦Â½`Ã† Â‰Â–[[#8]]ZÃ®Ã?VÃ¸Â²Ã¨Â°-RkÃžÃªw'8•Ã¦_uÂ¿Â </Ã‡Âª,[[#4]]CÃ"Â…	Block	1
41.34.241.148	Egypt	147.237.77.233	atal.idf.il	PHP Attempt	Block	1
87.246.192.21	Poland	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
41.34.241.148	Egypt	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/xmlrpc.php	Block	1
213.151.60.159	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9709-he/refuah.aspx	Block	1
46.19.85.71	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.113	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
41.34.241.148	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
77.127.236.87	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/_vti_bin/owssvr.dll	Block	1
197.162.22.131	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.66.131	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/1.he/print.css	Block	1
41.34.241.148	Egypt	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/xmlrpc.php	Block	1
41.34.241.148	Egypt	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 41.34.241.148	Block	1
87.246.192.21	Poland	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
69.112.159.86	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
46.120.227.235	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
162.243.212.144	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 162.243.212.144	Block	1
41.34.241.148	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
109.67.202.42	Israel	147.237.72.166	aka.idf.il	Abnormally Long Request method	Block	1
197.162.22.131	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
66.249.66.136	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/clientscripts.js	Block	1
128.194.3.195	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
41.227.110.134	Tunisia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
41.34.241.148	Egypt	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
105.128.63.176	Morocco	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1

02-11-2016-00:04:03 to 02-11-2016-01:04:03