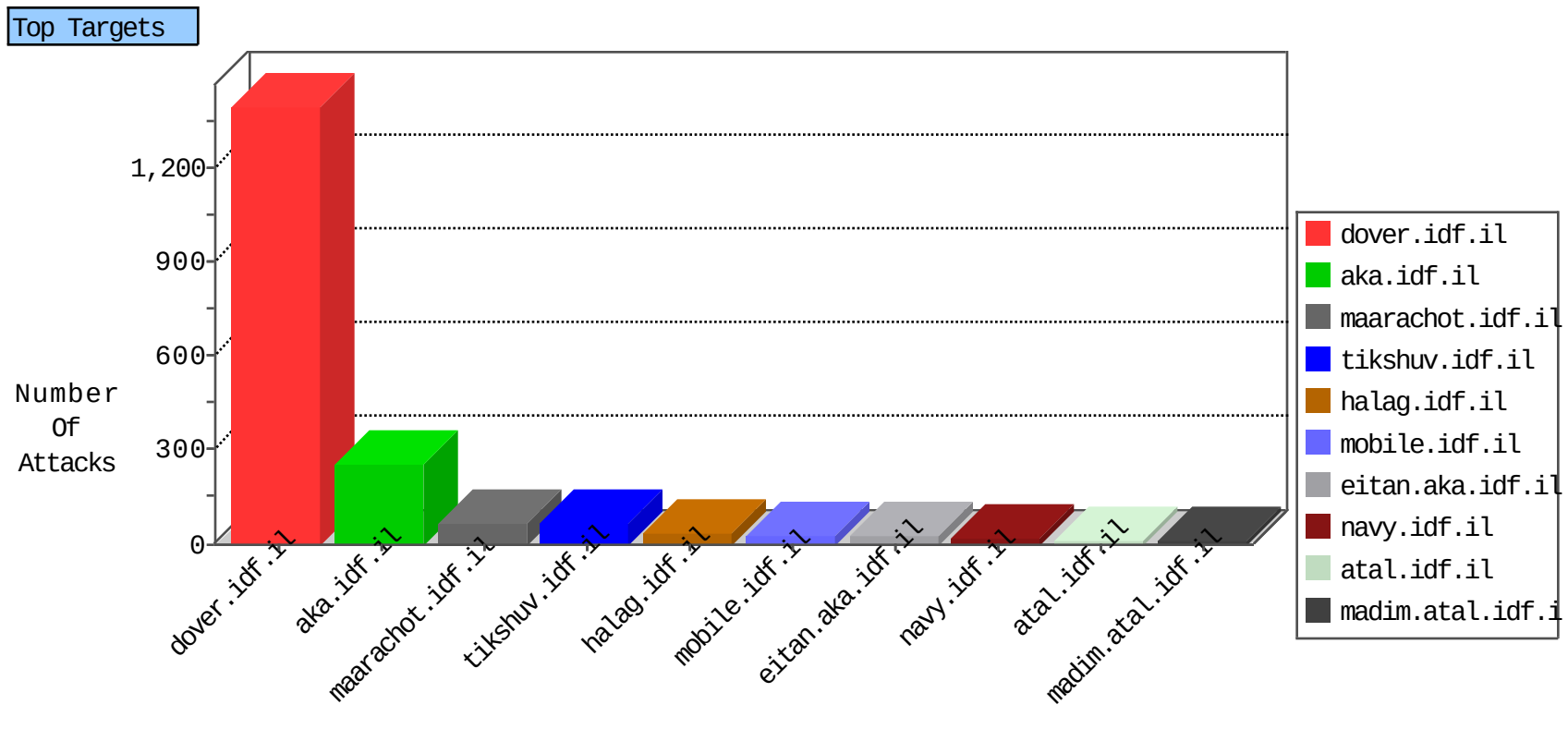
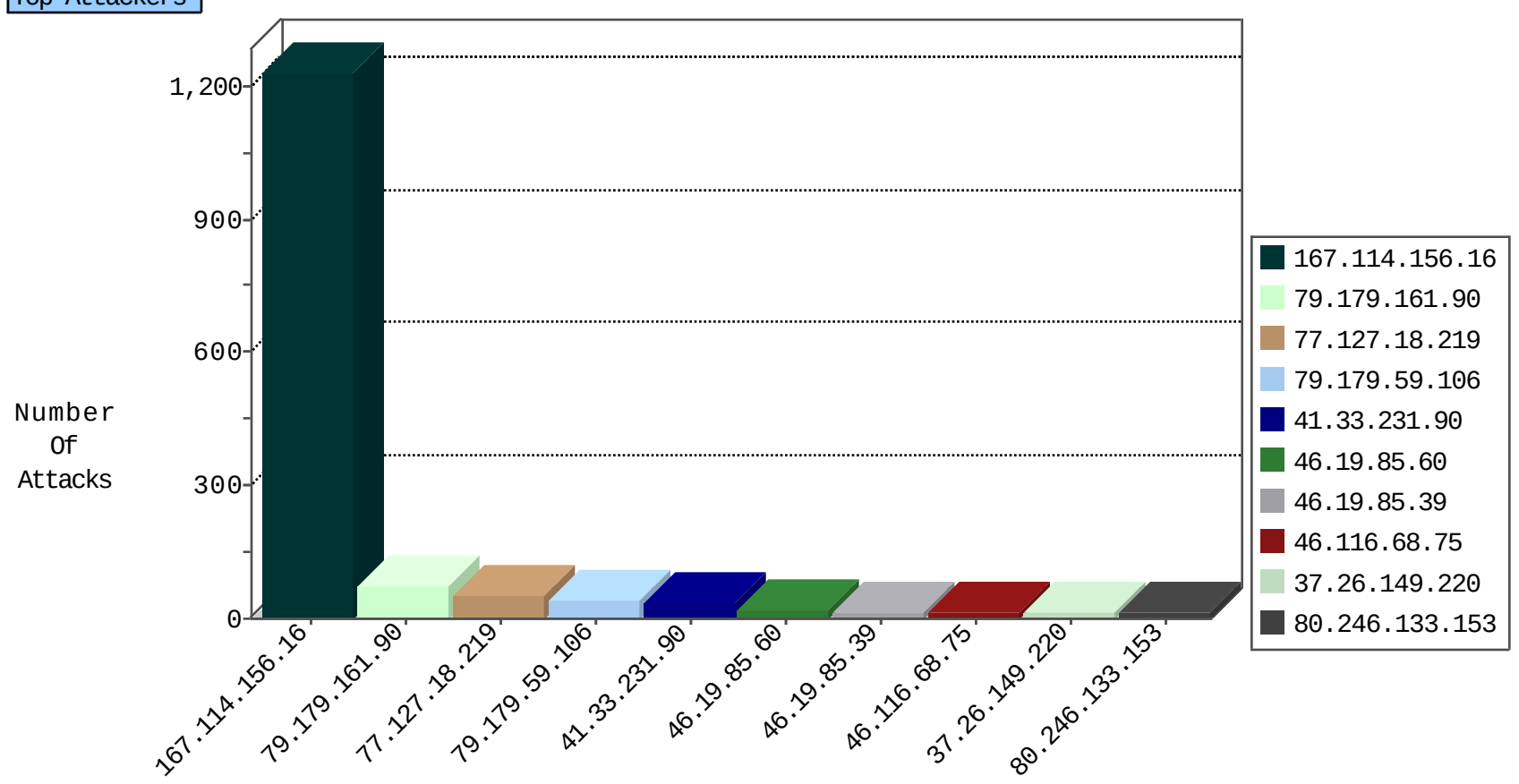
01-01-2016-19:04:00 to 01-01-2016-20:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-01-2016-19:04:00 to 01-01-2016-20:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3267
93.174.93.142	Netherlands	147.237.0.35	akaws.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
185.130.5.201		147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
106.75.199.192	China	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1

01-01-2016-19:04:00 to 01-01-2016-20:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
198.20.69.74	United States	147.237.8.14	e.orchot.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

01-01-2016-19:04:00 to 01-01-2016-20:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
79.179.161.90	147.237.72.166	Israel	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
66.249.93.107	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
168.62.238.153	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 1024	1
41.140.253.9	147.237.76.147	Morocco	chinuch.aka.idf.il	ET SCAN NMAP -sS window 3072	1
41.140.253.9	147.237.76.147	Morocco	chinuch.aka.idf.il	ET SCAN NMAP -f -sS	1
210.7.23.62	147.237.76.30	Fiji	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
173.192.46.45	147.237.0.15	United States	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
104.143.14.247	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
41.140.253.9	147.237.76.147	Morocco	chinuch.aka.idf.il	ET SCAN NMAP -sS window 2048	1

01-01-2016-19:04:00 to 01-01-2016-20:04:00

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
79.179.59.106	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	33
46.19.85.39	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
37.26.149.220	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
80.246.133.153	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
46.116.68.75	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.177.169.78	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.142.64.91	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
77.127.147.246	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.177.215.192	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
109.65.162.230	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
80.246.133.173	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
46.117.175.126	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
66.249.66.90	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
37.142.136.137	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
46.121.94.141	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
176.13.7.122	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.155	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.116	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.155	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.142.193.90	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
2.54.181.148	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.59.106	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
46.19.86.242	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
66.102.9.54	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
31.210.188.115	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.129	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
73.0.2.149	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
85.64.8.29	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
46.19.85.60	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
31.210.187.232	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.178.30.90	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
87.69.194.111	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
109.160.149.200	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
84.111.24.94	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
79.183.166.189	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.86.220	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
84.229.198.7	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
46.19.85.152	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.136.187	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
193.43.246.250	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	3
207.46.13.5	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.179.196.69	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
109.64.166.55	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.68.145.231	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.85.60	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
77.127.153.29	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3

01-01-2016-19:04:00 to 01-01-2016-20:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.127.18.219	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	53
79.179.161.90	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 79.179.161.90	Block	5
79.179.161.90	Israel	147.237.72.166	aka.idf.il	Multiple Malformed HTTP Header Line from 79.179.161.90	Block	5
79.179.161.90	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 79.179.161.90	Block	5
79.179.161.90	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 79.179.161.90	Block	5
79.179.161.90	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 79.179.161.90	Block	5
79.179.161.90	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 79.179.161.90	Block	5
79.179.161.90	Israel	147.237.72.166	aka.idf.il	Multiple Illegal HTTP Version from 79.179.161.90	Block	4
79.179.161.90	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 79.179.161.90	Block	4
79.179.161.90	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 79.179.161.90	Block	4
79.179.161.90	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 79.179.161.90	Block	4
87.69.238.45	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 87.69.238.45	Block	3
79.179.161.90	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 79.179.161.90	Block	3
84.109.49.68	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
87.69.238.45	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
176.13.16.126	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	2
93.172.163.112	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
207.46.13.62	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
46.19.86.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.52.155.195	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/sachar/registrationwizard/step3.aspx parameter	None	2
79.179.161.90	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Url from 79.179.161.90	Block	2
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
79.176.106.120	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.21	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
109.66.54.41	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
46.19.85.40	Israel	147.237.77.216	dover.idf.il	Multiple Malformed URL from 46.19.85.40	Block	1
79.179.161.90	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name &[[#26]]Ã† Ã¶Â?Ã«$[[#25]][[#27]]Ã‡Ã…%LÃˆ	Block	1
207.46.13.59	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/chamatz/miktzoa/default.asp	None	1
79.177.21.94	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/xmlrpc.php	Block	1
149.78.83.230	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.44.145	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.179.161.90	Israel	147.237.72.166	aka.idf.il	NULL Character in Method [[#0]]BÂ¨6!Â¯Â?ÂŠ1n[[#29]]Tg?;Ã˜Â¹Ã‡Ã &Ã rÂ†Â„5ÂœOÂˆYS]3^>[[#26]]Ã?Â«xÃˆÂ¥O;Â˜ Â±[[#23]][[#7]]Â?=Ã§l[[#18]]KÃ¦Â°f#Ã©ÂŒÂ®Ã½Ã¿[[#23]]KbÂ'Â¡Ã—2x[[#24]]Â¡[[#12]]Â'#]Â"Â¯Ã˜/Â†Ãœ	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
79.179.161.90	Israel	147.237.72.166	aka.idf.il	Illegal URL Path Encoding cÂ«[[#30]][[#15]]o\Â?Â¾kÂ°Ãžâ, ª[[#17]]`Â´8>>Â»}rÂ¦[[#26]]7"kqÃš[[#12]]Â©Â?â€Ž×›×™â,¬.}ÃŠ Â©j[[#2]]Ö³[[#8]][[#1]][[#11]]kÃ»×¢Â¥Â¾Ã»wo;â€¦0Öµ× fÃž×™ [[#29]]"×šamf×žË†ywvË†/9×"×–×?[[#19]]Â½â€ °[[#17]]Â´×?Â¶g[[#20]]jÖ¾%Ö¿ke!{ÂŠÂ«ekÂ»pÂ¶â€ °b×¥Â¡[[#28]]g[[#26]]×²â,¬Ö½Ã?×–×?×?[[#18]][[#18]]ÂŠ×±rÂ?câ€š Â±×ª[[#24]]Ö´la.<â€°Öµ	Block	1
46.19.86.94	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.147.195	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.181.190.248	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/watch	Block	1
79.178.217.139	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl83 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
79.179.161.90	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Method from 79.179.161.90	Block	1
77.126.58.244	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.201.154.235	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
54.183.184.150	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
79.179.161.90	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Value	Block	1
46.19.85.40	Israel	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 46.19.85.40	Block	1
84.110.39.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
79.177.21.94	Israel	147.237.77.234	halag.idf.il	PHP Attempt	Block	1

01-01-2016-19:04:00 to 01-01-2016-20:04:00