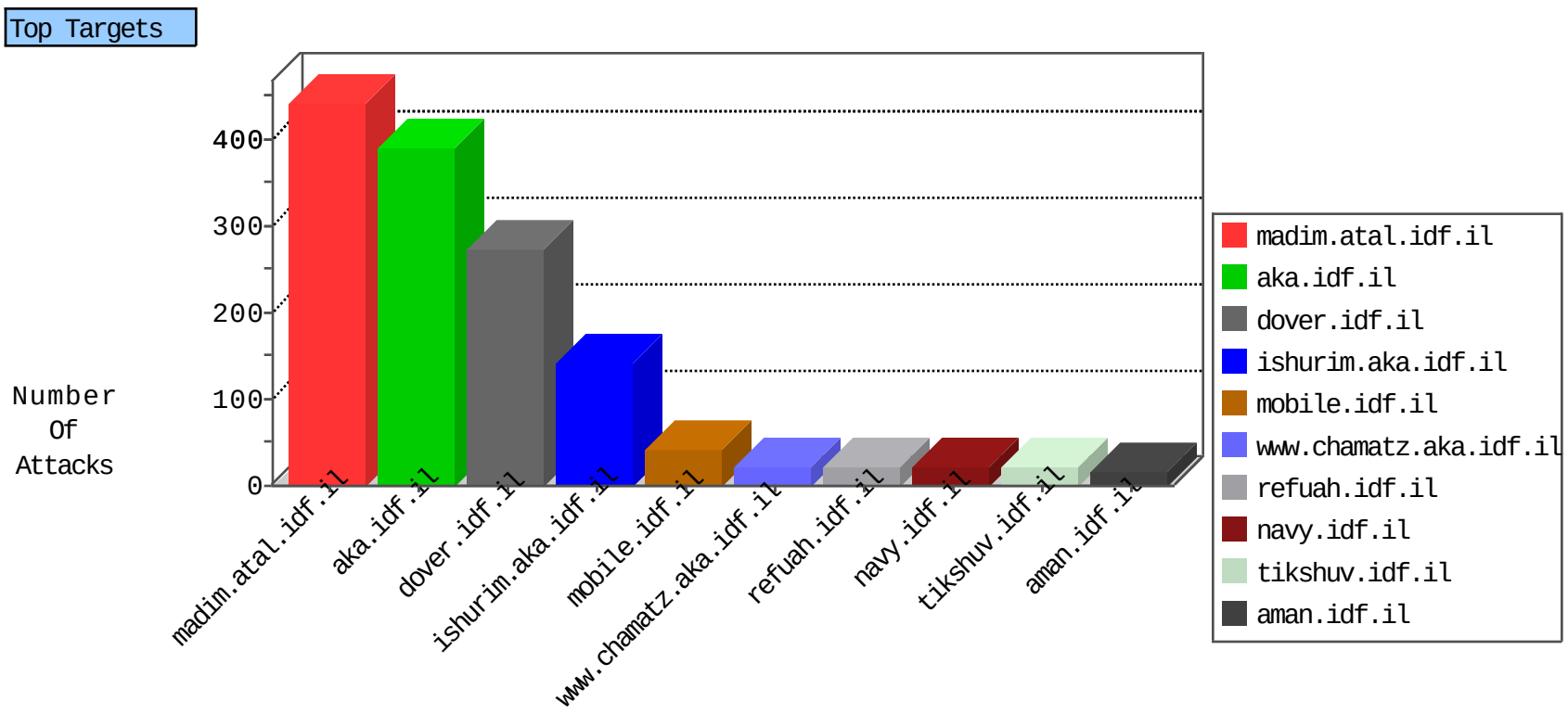
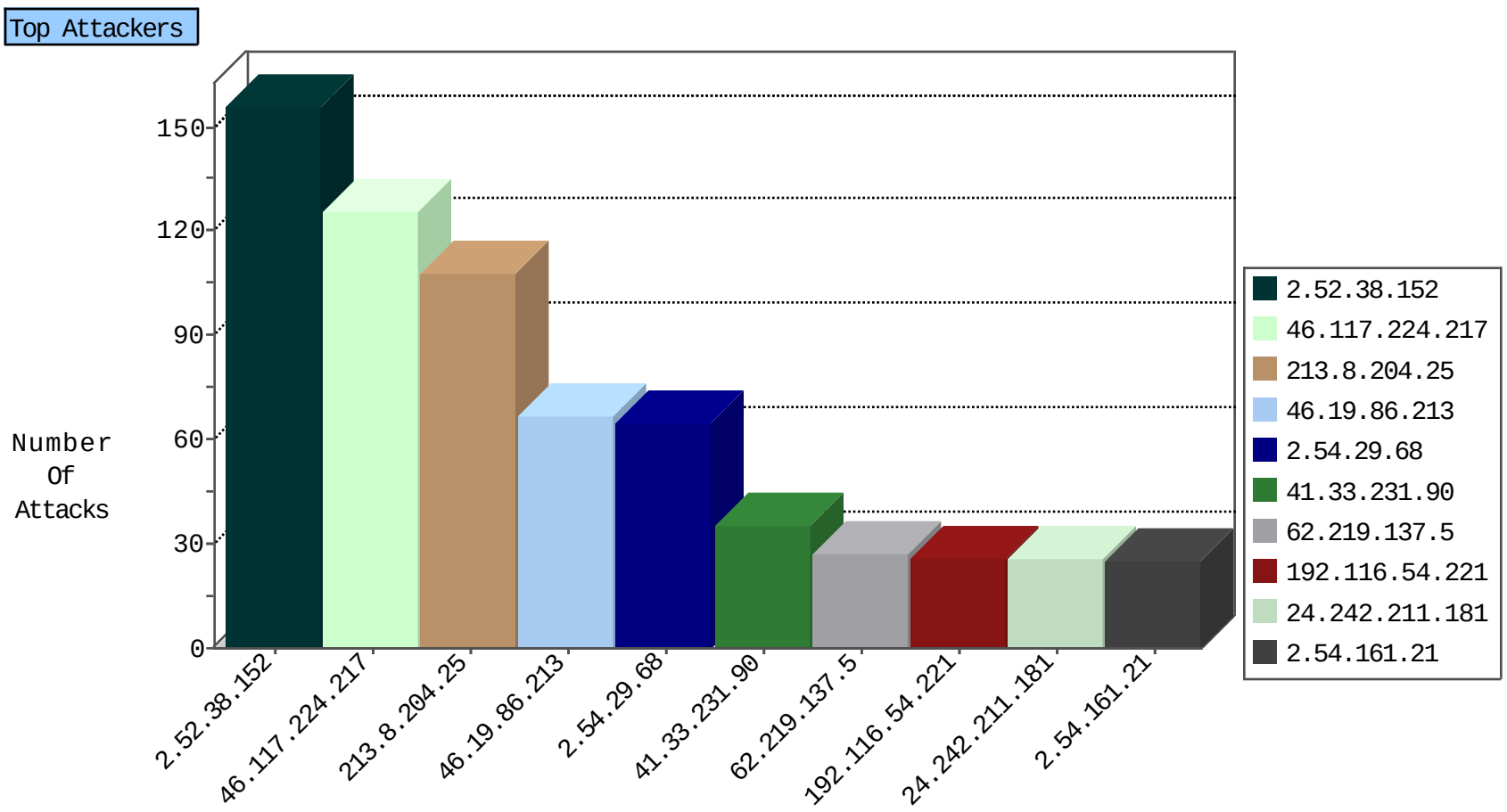
02-08-2016-21:04:07 to 02-08-2016-22:04:07

IDF Under Attack Daily Report





02-08-2016-21:04:07 to 02-08-2016-22:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.134	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
89.138.28.156	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
31.168.240.21	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
77.127.160.250	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
185.94.111.1		147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
180.97.106.162	China	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1		147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
74.91.28.59	United States	147.237.77.19	law-forum.idf.il	block-sp-traf1	drop	1
142.54.160.211	United States	147.237.77.234	halag.idf.il	block-sp-traf1	drop	1
185.94.111.1		147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
74.91.28.61	United States	147.237.77.205	prisha.idf.il	block-sp-traf1	drop	1
165.91.4.60	United States	147.237.72.166	aka.idf.il	block-sp-traf1	drop	1

02-08-2016-21:04:07 to 02-08-2016-22:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
111.202.102.69	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

02-08-2016-21:04:07 to 02-08-2016-22:04:07

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
66.249.81.148	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
54.67.38.74	147.237.76.200	United States	eitan.aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
54.67.38.74	147.237.0.15	United States	kosher-kravi.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
46.77.66.31	147.237.77.121	Poland	e.navy.idf.il	ET SCAN NMAP -sS window 3072	1
218.246.0.97	147.237.77.176	China	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
46.45.137.67	147.237.77.234	Turkey	halag.idf.il	ET SCAN NMAP -sS window 1024	1
193.105.134.220	147.237.8.14	Sweden	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
179.43.141.234	147.237.0.15	Switzerland	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
116.25.139.207	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
89.138.93.151	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
54.67.38.74	147.237.0.16	United States	my-kosher-kravi.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
46.77.66.31	147.237.77.121	Poland	e.navy.idf.il	ET SCAN NMAP -sS window 4096	1
46.45.137.67	147.237.77.235	Turkey	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	1
179.43.141.234	147.237.72.14	Switzerland	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
176.13.5.239	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.113	147.237.77.235	Ukraine	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
84.108.80.188	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

02-08-2016-21:04:07 to 02-08-2016-22:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
213.8.204.25	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	108
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
24.242.211.181	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
192.116.54.221	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
85.130.253.120	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
31.210.188.87	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
192.116.54.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
89.139.228.31	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
2.54.161.21	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
31.154.14.46	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
37.26.147.129	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
31.210.187.230	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
66.249.81.152	United States	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	8
62.219.137.5	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
5.22.135.97	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
185.3.144.123	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.13.193.147	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
209.88.157.203	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
77.126.95.226	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.210.186.17	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
62.219.137.5	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
77.127.13.139	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
217.132.147.29	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.207	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.176.160.70	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.178.96.97	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.228.43.55	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.48.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.120.125.32		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.219.137.5	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	6
109.253.130.48	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.161.21	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
2.54.161.21	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.54.161.21	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
31.168.24.58	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
187.36.7.58	Brazil	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.202	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
66.249.78.184	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
62.219.137.5	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.207	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.46.38.98	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.74	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.86.101	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.22.130.238	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	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
77.127.160.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.52.11.4	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3

02-08-2016-21:04:07 to 02-08-2016-22:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.117.224.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	87
2.52.38.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	79
2.54.29.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	65
46.19.86.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	65
2.52.38.152	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	42
46.117.224.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	39
2.52.38.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	29
37.26.149.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
46.19.85.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
188.64.102.215	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	3
93.173.250.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.67.169.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.199.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.12.118	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1381	Block	2
84.229.42.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.142.184.228	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/size220x0/sip_storage	Block	2
2.52.11.4	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1214-he/miluim.aspx	Block	1
185.3.144.123	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
109.66.37.187	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion $71 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Parameter Name ÂŒ cÃ¿fr[[#31]]Â®Â¥:×£×€rR[[#22]][[#14]]Ö¾Â?Â£×'[RÖµÖ½×"×›8Ãš 1K[[#12]]Ãœ*×–Â²;c)o0Ã›[[#7]]â€¢1â€¹[[#7]][[#6]]Ö¼5K0^ÂŸ Ö¸R[[#3]][[#29]]ÃŠ×™ÂŸÂ®Â¬tw;-:XN^L*â,¬Â´Â¹rÂ?jÖ³qË†×¤rnÂŒ P;[[#0]]xÃžÃ¿Â¶8[[#0]]×œa[[#28]]Â±ÃŸÂ¨Â¡JÂ¥	Block	1
89.139.228.31	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.79.225	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
165.91.4.62	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
54.67.38.74	United States	147.237.0.15	kosher-kravi.idf.il	Multiple Untraceable SSL Sessions from 54.67.38.74 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
93.190.140.235	Netherlands	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/admin/cms_wysiwyg/directive/index/	Block	1
46.19.86.162	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 217.194.198.104 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
37.26.146.130	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl38$ctl01$ctl03$cblQuestion $2 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
81.200.91.15	Russian Federation	147.237.77.74	law.idf.il	Parameter Type Violation PageNum in www.law.idf.il/163-en/patzar.aspx	Block	1
185.3.147.114	Israel	147.237.76.200	eitan.aka.idf.il	PHP Attempt	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	1
90.161.119.178	Spain	147.237.77.74	law.idf.il	PHP Attempt	Block	1
46.19.85.148	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request request version	Block	1
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Query String ÂŒcÃ¿fr[[#31]]Â®Â¥:×£×€rR[[#22]][[#14]]Ö¾Â?Â£×'[RÖµÖ½×"×›8Ãš1K[[#12]]Ãœ*×–Â²;c)o0Ã›[[#7]]â€¢1â€¹[[#7]][[#6]]Ö¼5K0^ÂŸÖ¸R[[#3]][[#29]]ÃŠ×™ÂŸÂ®Â¬tw;-:XN^L*â,¬Â´Â¹rÂ?jÖ³qË†×¤rnÂŒP;[[#0]]xÃžÃ¿Â¶8[[#0]]×œa[[#28]]Â±ÃŸÂ¨Â¡JÂ¥	Block	1
77.126.16.135	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl38$ctl01$ctl03$cblQuestion $6 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
2.54.132.41	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/favicon.ico	Block	1
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Distributed Abnormally Long Header Line	Block	1
176.13.12.118	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 176.13.12.118	Block	1
54.67.38.74	United States	147.237.0.16	my-kosher-kravi.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
109.64.129.23	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/kesher	Block	1
46.19.86.207	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
217.194.198.104	Israel	147.237.72.166	aka.idf.il	NULL Character in Parameter Name ÂŒcÃ¿fr[[#31]]Â®Â¥:×£×€rR[[#22]][[#14]]Ö¾Â?Â£×'[RÖµÖ½×"×›8Ãš1K[[#12]]Ãœ*×–Â²;c)o0Ã›[[#7]]â€¢1â€¹[[#7]][[#6]]Ö¼5K0^ÂŸÖ¸R[[#3]][[#29]]ÃŠ×™ÂŸÂ®Â¬tw;-:XN^L*â,¬Â´Â¹rÂ?jÖ³qË†×¤rnÂŒP;[[#0]]xÃžÃ¿Â¶8[[#0]]×œa[[#28]]Â±ÃŸÂ¨Â¡JÂ¥	Block	1
37.26.148.142	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion $7 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Distributed Malformed URL	Block	1
84.108.237.62	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
185.3.147.114	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/xmlrpc.php	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
46.120.24.109	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1

02-08-2016-21:04:07 to 02-08-2016-22:04:07