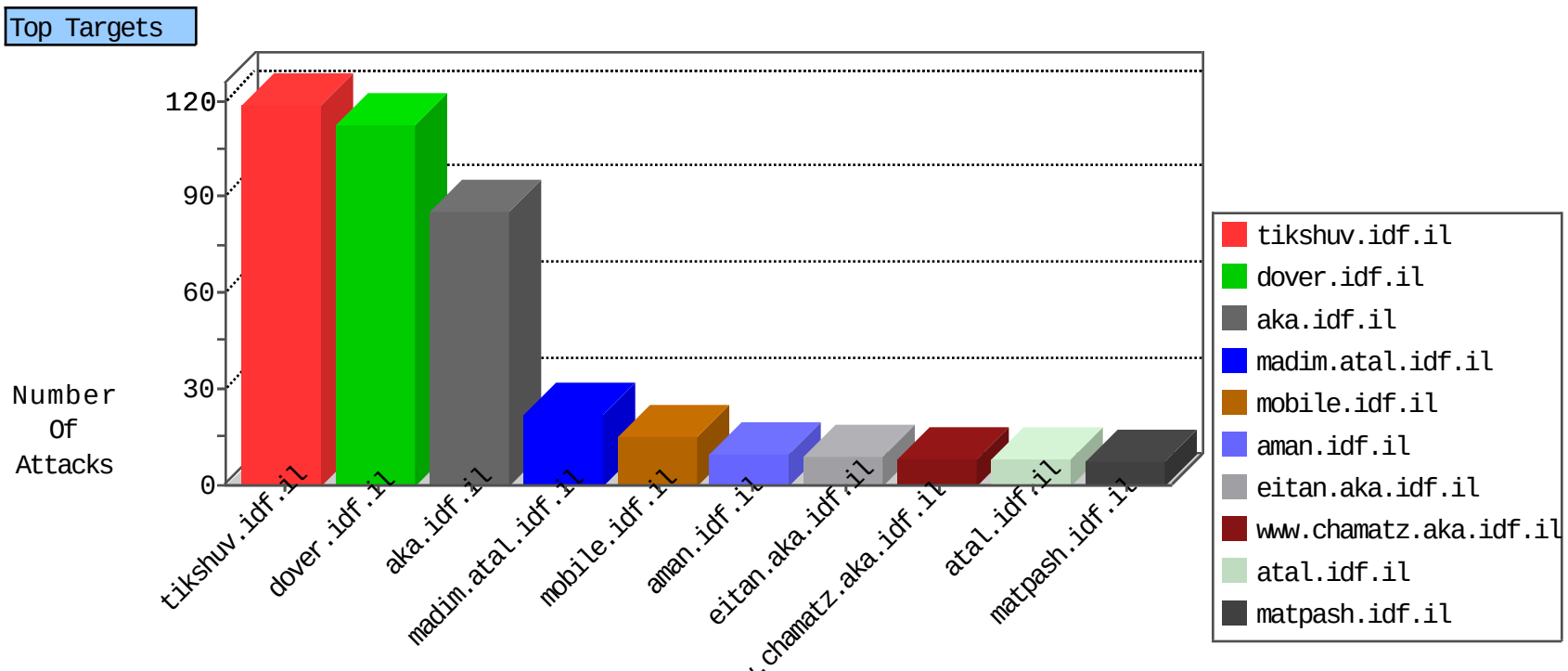
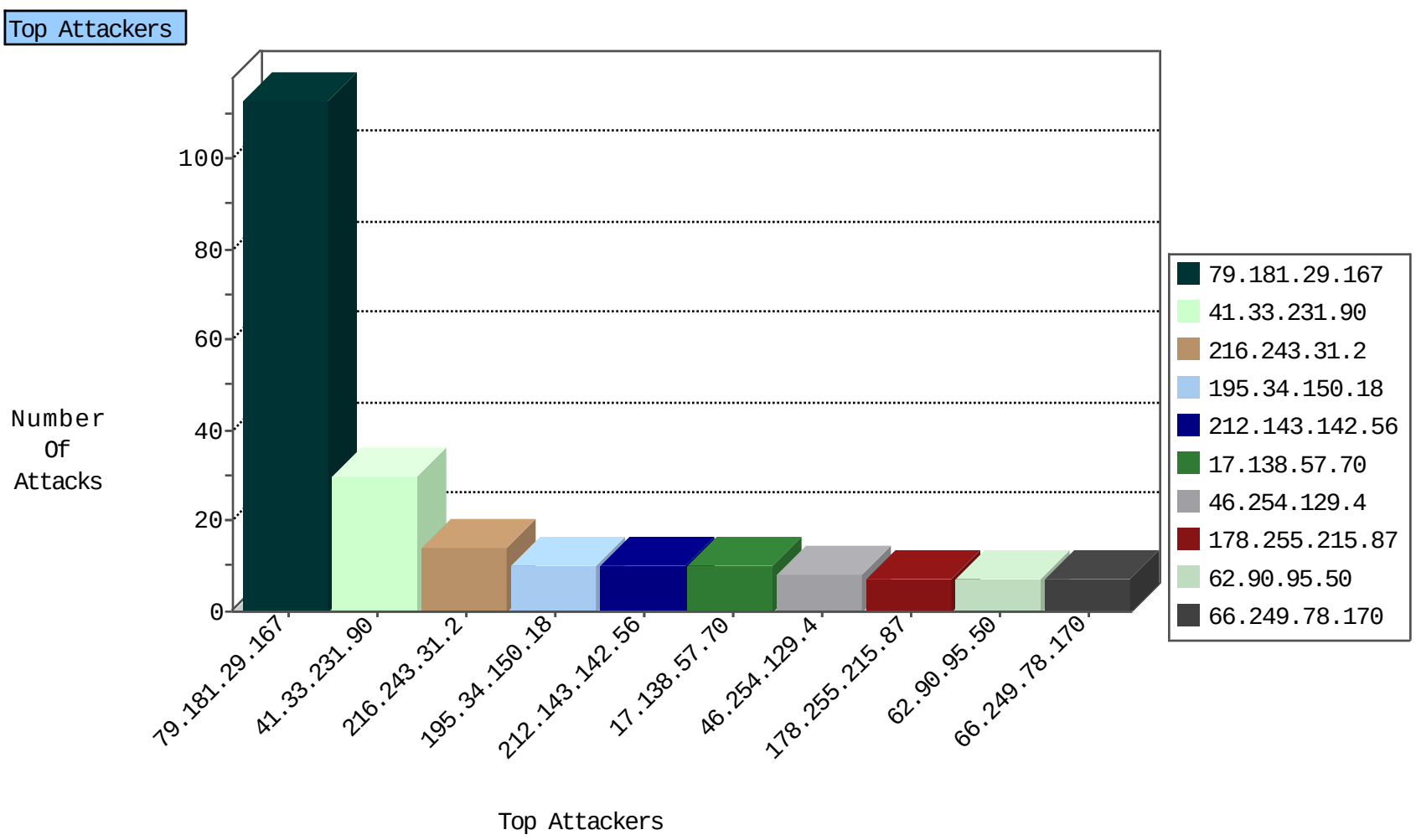
02-12-2016-22:04:03 to 02-12-2016-23:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-12-2016-22:04:03 to 02-12-2016-23:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
67.86.97.181	United States	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
67.86.97.181	United States	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
208.73.206.244		147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1

02-12-2016-22:04:03 to 02-12-2016-23:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
155.94.254.143	United States	147.237.0.15	kosher-kravi.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1

02-12-2016-22:04:03 to 02-12-2016-23:04:03

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	5
66.249.78.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
202.160.167.210	147.237.8.28	India	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
114.112.90.54	147.237.76.202	China	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
114.112.90.54	147.237.76.34	China	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.193	147.237.0.33	Netherlands	idf.il	ET SCAN NMAP -sS window 1024	1
80.82.64.68	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.76.200	China	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
114.112.90.54	147.237.76.44	China	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.193	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.193	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1

02-12-2016-22:04:03 to 02-12-2016-23:04:03

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	30
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
62.90.95.50	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
66.249.78.170	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
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	6
94.159.157.78	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.29.167	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.177.172.4	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
94.230.86.210	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
179.156.214.246	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
2.54.151.15	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.54.50.76	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
80.246.139.200	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
178.255.215.87	France	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
2.52.156.14	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.254.129.4	Bulgaria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
46.19.86.161	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.180.37	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.81.136	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.27.195	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.114.34	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.184.54	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.207.168	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.104.16	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.131.2	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
77.125.137.205	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.21.74	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.223	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.66	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.150.119	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.94.128	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
178.255.215.87	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
77.125.94.128	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
198.154.60.27	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
37.26.147.167	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
46.19.86.67	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
89.138.191.186	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
94.230.86.251	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
77.126.69.99	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
173.79.53.82	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
46.254.129.4	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
37.142.64.53	Israel	147.237.76.31	nakchal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
94.230.86.251	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
77.126.69.99	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
173.79.53.82	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
141.212.122.177	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.243.31.2	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
94.230.86.68	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

02-12-2016-22:04:03 to 02-12-2016-23:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.181.29.167	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 79.181.29.167	Block	106
17.138.57.70	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.138.57.70	Block	10
185.32.179.64	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
2.54.21.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.64.109.198	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 85.64.109.198	Block	3
46.19.86.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.142.68.19	Israel	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
37.142.68.19	Israel	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	2
37.142.64.53	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	2
79.181.180.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
85.95.254.197	Turkey	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
91.210.146.225	Ukraine	147.237.72.166	aka.idf.il	Admin Blocking	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
66.249.69.24	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/2379.jpg	Block	1
149.88.207.248	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl38$ctl01$ctl03$cblQuestion$2 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
109.65.56.248	Israel	147.237.0.15	kosher-kravi.idf.il	PHP Attempt	Block	1
207.46.13.55	United States	147.237.72.166	aka.idf.il	Unknown Parameter 177afae0 in aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
66.249.78.170	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter searchText in www.eitan.aka.idf.il/982-en/eitan.aspx	None	1
109.67.202.42	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
91.210.146.225	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 91.210.146.225	Block	1
79.181.29.167	Israel	147.237.0.34	tikshuv.idf.il	Too Many 404: Response Code per Session	Block	1
66.249.69.40	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/2424.jpg	Block	1
109.65.56.248	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/xmlrpc.php	Block	1
85.64.109.198	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/default.aspx	Block	1
66.249.78.230	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/milluim/index	Block	1
46.254.129.4	Bulgaria	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
109.67.202.42	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method #Âœc_[[#28]]Â¦ÂˆÃ¿Ã'Â§%Ã–"Â¤Y[[#11]]Âµs[[#12]][[#28]]ÃštÃ SMo[[#29]]Ã‡0Â¸sÂžÂ“Ã³;Â»Ã…Ã»Â²0&Ã¬Â…Â¥SÃ¸ÂªÃ„[[#23]]wRÃƒÃ Ã½Â³p/yÂš[[#7]]Â°Ã‡BÃ¬\Âª$eYÃ ÂžOÃ‰Â¢Â€Ã·Ã°`[[#15]]Â¬Ã«Ã€Â,Â²ÃŠ[[#3]]p[[#19]]EvÃŽÂ‰Â¥Â•OÃ°a61Ã?9Ã"HÂ¾Ã»Â¢ÃŠTÂ²Ã¯hÃ¨gÃ£Â?Â Ã®O[[#1]]Ã£Â¢X@Â°@ÃƒÃ·0[[#2]]ÂœÂ“Ã Ã…Â†Ã…Ã?Â±Â°WU[[#21]]Ã›;{W[[#16]]Ã—Â¸Ã€o[[#23]]\C[[#3]]*nÂˆÃ¶[[#1]]vÂŒ3Â ÃžÂ‡HÃ™jÂ Ã,WÂ¾Ã—Ã¹Â?Â"[[#17]]ÃŽÂ¼[[#27]]ÃŸÃ¹Â"[[#16]][[#31]]Ã¿Ã?Ã°Âš6Ã¦Ã,=Ã†vÃ¾Z[[#23]][[#8]]hÃ…Â°uSpÂ‹Â'ÂªÂ…Â²Â¬[[#11]]Â'AÂŸ	Block	1
37.142.64.53	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 37.142.64.53	Block	1
91.210.146.225	Ukraine	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
193.201.224.170	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/894-he/chinuch.aspx	Block	1
66.249.78.80	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding j.e[8l2tEjLR>S>2vSL;*$zzuM(&4WRz in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
109.65.56.248	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 109.65.56.248	Block	1
37.142.233.253	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
85.64.113.49	Israel	147.237.72.166	aka.idf.il	Unknown Parameter id in aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
66.249.64.229	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1403-he/atal.aspx	Block	1
109.67.202.42	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
91.210.146.225	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-login.php	Block	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
66.249.78.87	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	1
109.65.56.248	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1
45.43.8.117		147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1362-he/dover.aspx	Block	1
66.249.64.234	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1401-he/atal.aspx	Block	1
109.67.202.42	Israel	147.237.72.166	aka.idf.il	Unknown HTTP Request Method #Âœc_[[#28]]Â¦ÂˆÃ¿Ã'Â§%Ã–"Â¤Y[[#11]]Âµs[[#12]][[#28]]ÃštÃ SMo[[#29]]Ã‡0Â¸sÂžÂ“Ã³;Â»Ã…Ã»Â²0&Ã¬Â…Â¥SÃ¸ÂªÃ„[[#23]]wRÃƒÃ Ã½Â³p/yÂš[[#7]]Â°Ã‡BÃ¬\Âª$eYÃ ÂžOÃ‰Â¢Â€Ã·Ã°`[[#15]]Â¬Ã«Ã€Â,Â²ÃŠ[[#3]]p[[#19]]EvÃŽÂ‰Â¥Â•OÃ°a61Ã?9Ã"HÂ¾Ã»Â¢ÃŠTÂ²Ã¯hÃ¨gÃ£Â?Â Ã®O[[#1]]Ã£Â¢X@Â°@ÃƒÃ·0[[#2]]ÂœÂ“Ã Ã…Â†Ã…Ã?Â±Â°WU[[#21]]Ã›;{W[[#16]]Ã—Â¸Ã€o[[#23]]\C[[#3]]*nÂˆÃ¶[[#1]]vÂŒ3Â ÃžÂ‡HÃ™jÂ Ã,WÂ¾Ã—Ã¹Â?Â"[[#17]]ÃŽÂ¼[[#27]]ÃŸÃ¹Â"[[#16]][[#31]]Ã¿Ã?Ã°Âš6Ã¦Ã,=Ã†vÃ¾Z[[#23]][[#8]]hÃ…Â°uSpÂ‹Â'ÂªÂ…Â²Â¬[[#11]]Â'AÂŸnÂ¦{Ã"Â‹Ã'	Block	1
109.64.59.160	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 109.64.59.160	Block	1
37.142.64.53	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/8/	Block	1
84.109.9.109	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$11 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
198.58.102.158	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1

02-12-2016-22:04:03 to 02-12-2016-23:04:03

02-12-2016-22:04:03 to 02-12-2016-23:04:03