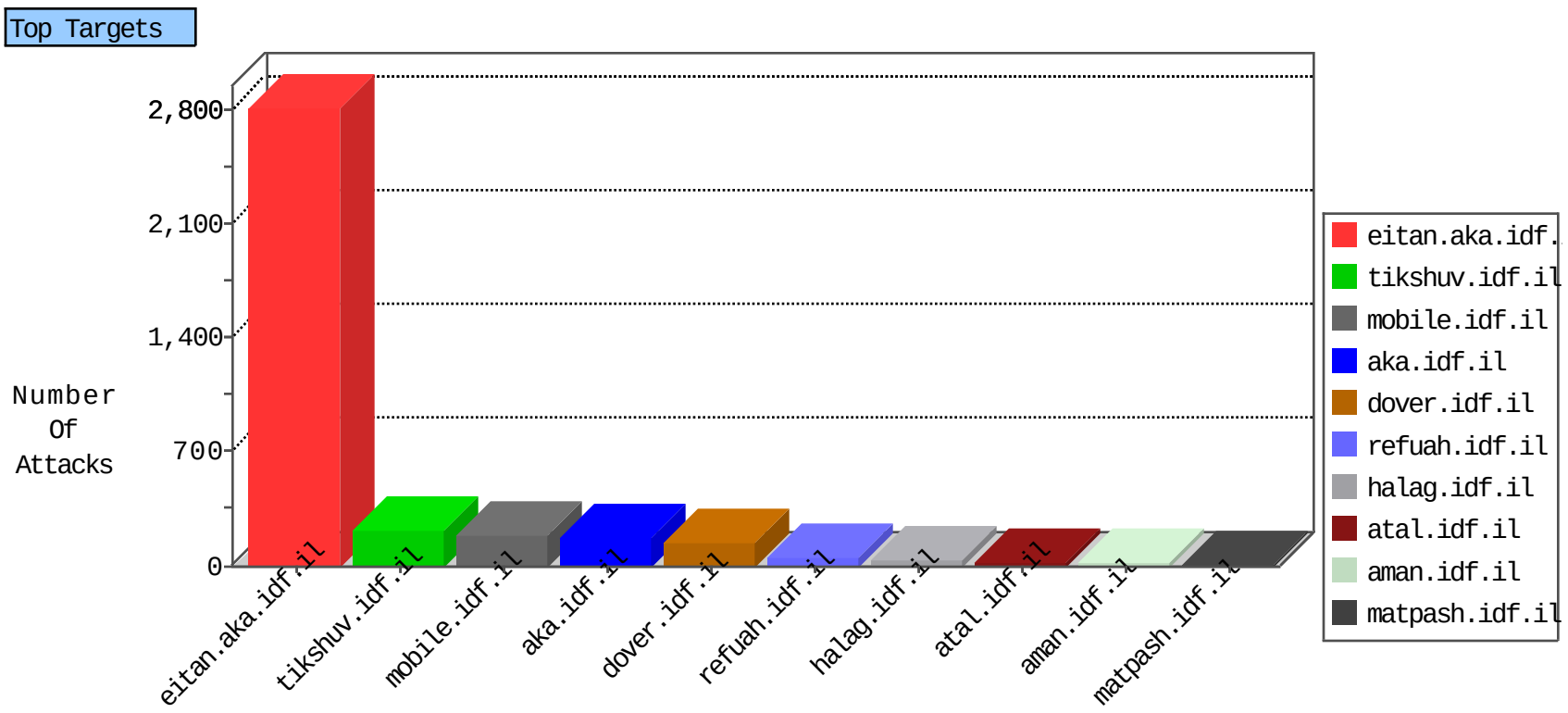
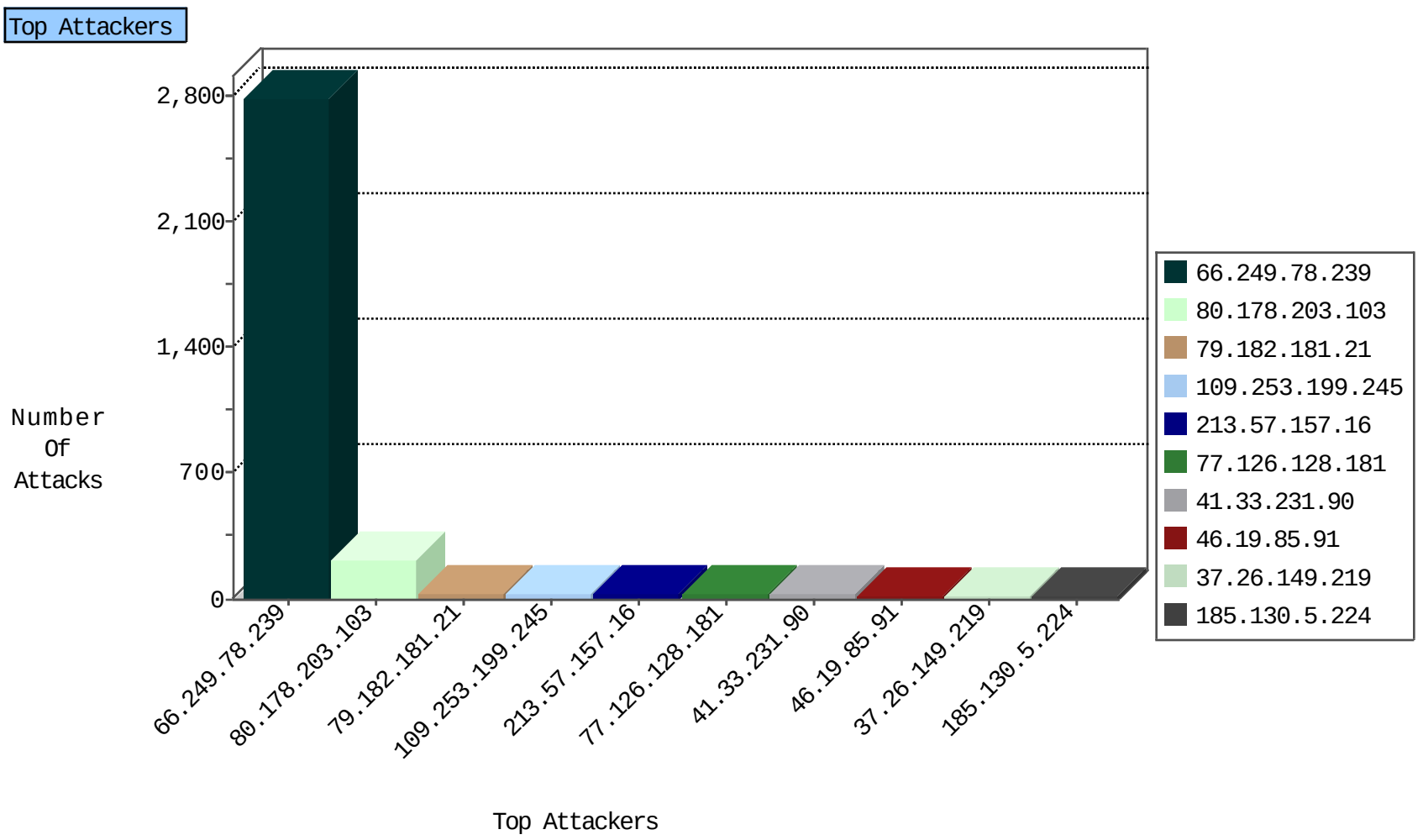
02-12-2016-20:04:09 to 02-12-2016-21:04:09

IDF Under Attack
Daily Report

Top Targets



Top Attackers



02-12-2016-20:04:09 to 02-12-2016-21:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.130.5.224		147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	2
185.130.5.224		147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	2
115.139.36.200	Korea, Republic of	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	2
185.130.5.224		147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	2
185.130.5.224		147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	2
185.130.5.224		147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	2
185.130.5.224		147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	2
185.130.5.224		147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
123.151.42.61	China	147.237.76.30	himush.idf.il	Block_Udp_All_Nets_Con_Limit	drop	1
185.130.5.224		147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
178.32.121.195	France	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
14.132.4.205	Japan	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1

02-12-2016-20:04:09 to 02-12-2016-21:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.40.10.131	Turkey	147.237.77.216	dover.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1

02-12-2016-20:04:09 to 02-12-2016-21:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.78.239	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN NMAP -sA (2)	2786
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
193.201.227.71	147.237.77.216	Ukraine	dover.idf.il	ET SCAN Potential SSH Scan	2
2.54.171.84	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
176.40.10.131	147.237.77.216	Turkey	dover.idf.il	SERVER-WEBAPP admin.php access	1
94.102.48.193	147.237.76.30	Netherlands	himush.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.76.196	China	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
201.86.139.182	147.237.76.31	Brazil	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
193.201.227.71	147.237.76.42	Ukraine	refuah.idf.il	ET SCAN Potential SSH Scan	1
177.139.157.117	147.237.8.28	Brazil	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
94.102.48.193	147.237.76.201	Netherlands	e.atal.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
203.115.68.103	147.237.76.30	India	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
193.201.227.71	147.237.76.86	Ukraine	navy.idf.il	ET SCAN Potential SSH Scan	1
193.201.227.71	147.237.0.35	Ukraine	akaws.idf.il	ET SCAN Potential SSH Scan	1

02-12-2016-20:04:09 to 02-12-2016-21:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.253.199.245	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
213.57.157.16	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
77.126.128.181	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
37.47.8.144	Poland	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
79.182.181.21	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
79.182.181.21	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	17
37.26.149.219	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
79.183.207.210	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.2.213	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
77.126.237.171	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.179.112.101	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.26.148.212	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
109.253.194.121	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.8	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
176.40.10.16	Turkey	147.237.76.30	himush.idf.il	drop	SAM rule	drop	7
31.210.187.190	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.91	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
77.127.209.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.184.54	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.91	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.91	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.254	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.91	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.125.87.78	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.68.251.37	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.89	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
94.230.86.184	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.180.128.139	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
213.57.194.80	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
46.19.85.89	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.8	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
188.120.148.10	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
141.0.14.69	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
31.210.187.157	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
213.57.194.80	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	4
178.255.215.87	France	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
141.8.183.16	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
213.8.204.60	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
109.65.189.46	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.14.104	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.149.78	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.165.1	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.92	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.92.234	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-12-2016-20:04:09 to 02-12-2016-21:04:09

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
79.183.170.195	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.50.121	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-12-2016-20:04:09 to 02-12-2016-21:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.178.203.103	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 80.178.203.103	Block	212
213.57.157.16	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	7
5.29.73.13	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
77.126.128.181	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
109.253.199.245	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
176.40.10.131	Turkey	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 176.40.10.131	Block	4
37.26.149.219	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
213.251.182.111	France	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 213.251.182.111	Block	4
176.40.10.131	Turkey	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
176.40.10.131	Turkey	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 176.40.10.131	Block	3
79.180.50.121	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	3
37.26.146.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
17.138.57.70	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	2
5.29.144.147	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.29.144.147	Block	2
87.68.250.12	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
176.13.2.213	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
77.126.237.171	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
89.139.73.190	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/index	Block	2
104.196.0.90	United States	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 104.196.0.90	Block	1
46.19.85.254	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
213.251.182.111	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
92.98.162.116	United Arab Emirates	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
195.154.173.103	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	1
79.180.24.251	Israel	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to kosher-kravi.idf.il/xmlrpc.php	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/4/2974.jpg	Block	1
109.67.202.42	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method	Block	1
213.8.204.60	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
104.196.0.90	United States	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Method [[#0]][[#0]][[#6]][[#4]][[#0]][[#0]][[#0]][[#0]][[#0]][[#0]][[#4]]@[[#0]][[#0]][[#0]][[#0]][[#0]][[#4]][[#8]][[#0]][[#0]][[#0]][[#0]][[#0]]@[[#0]][[#0]][[#0]][[#0]][[#5]][[#2]][[#0]][[#0]][[#0]][[#0]][[#1]]Â€ [[#0]][[#0]][[#7]][[#0]][[#0]][[#0]]&[[#1]]%[[#0]][[#0]][[#0]][[#1]][[#0]][[#0]][[#0]][[#0]]Â,Â„Â‡AÂˆÃ±£Ã,Ã¦Â'UÃ?GS[[#3]]*/*zÂ?ÂªiÃ'ÂšÃ„Ã€ WmpÂ-•[[#7]][[#31]][[#0]][[#0]][[#11]][[#1]]%[[#0]][[#0]][[#0]][[#3]][[#0]][[#0]][[#0]][[#1]][[#0]]Â,Â„Â‡Ã€Â¿Â¾[[#0	Block	1
190.136.82.249	Argentina	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
144.76.71.83	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/shared/usercontrols/headerupper/	Block	1
104.196.0.90	United States	147.237.77.216	dover.idf.il	NULL Character in Method [[#0]][[#0]][[#6]][[#4]][[#0]][[#0]][[#0]][[#0]][[#0]][[#0]][[#4]]@[[#0]][[#0]][[#0]][[#0]][[#0]][[#4]][[#8]][[#0]][[#0]][[#0]][[#0]][[#0]]@[[#0]][[#0]][[#0]][[#0]][[#5]][[#2]][[#0]][[#0]][[#0]][[#0]][[#1]]Â€ [[#0]][[#0]][[#7]][[#0]][[#0]][[#0]]&[[#1]]%[[#0]][[#0]][[#0]][[#1]][[#0]][[#0]][[#0]][[#0]]Â,Â„Â‡AÂˆÃ±£Ã,Ã¦Â'UÃ?GS[[#3]]*/*zÂ?ÂªiÃ'ÂšÃ„Ã€ WmpÂ-•[[#7]][[#31]][[#0]][[#0]][[#11]][[#1]]%[[#0]][[#0]][[#0]][[#3]][[#0]][[#0]][[#0]][[#1]][[#0]]Â,Â„Â‡Ã€Â¿Â¾[[#0]][[#0]][[#11	Block	1
46.116.215.177	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$45 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
198.23.188.201	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.asp	Block	1
92.98.162.116	United Arab Emirates	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
109.67.202.42	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
104.196.0.90	United States	147.237.77.216	dover.idf.il	Illegal Byte Code Character in URL	Block	1
190.136.82.249	Argentina	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
156.199.12.24		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	1
77.126.211.160	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl38$ctl01$ctl03$cblQuestion$2 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
104.196.0.90	United States	147.237.77.216	dover.idf.il	NULL Character in URL	Block	1
64.237.45.116	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
5.29.144.147	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/6_s3_	Block	1
200.51.198.160	Argentina	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
93.173.158.30	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
79.182.181.21	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1086-en/dover.aspx	Block	1
37.26.146.220	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
213.57.194.80	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
104.196.0.90	United States	147.237.77.216	dover.idf.il	Illegal HTTP Version HTTP/2.0	Block	1

02-12-2016-20:04:09 to 02-12-2016-21:04:09