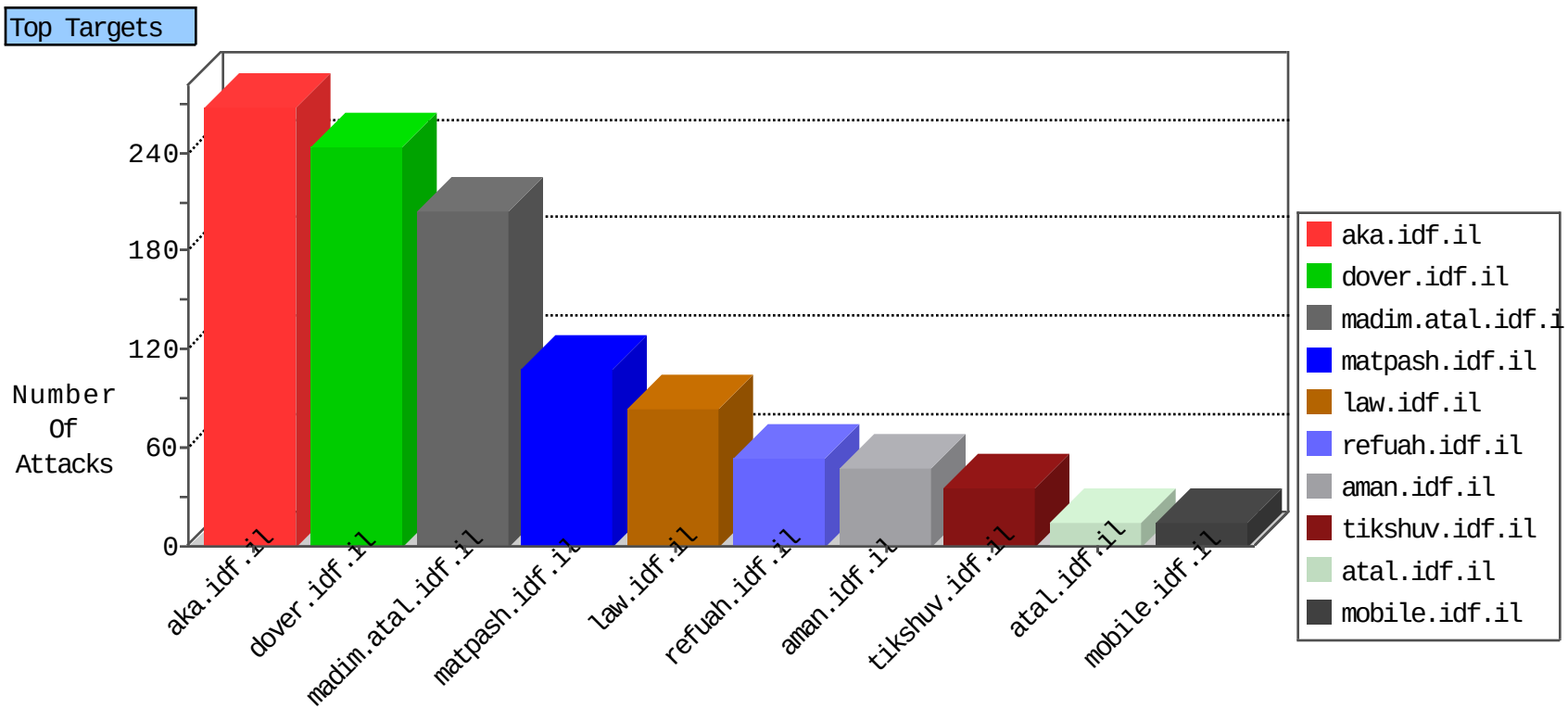
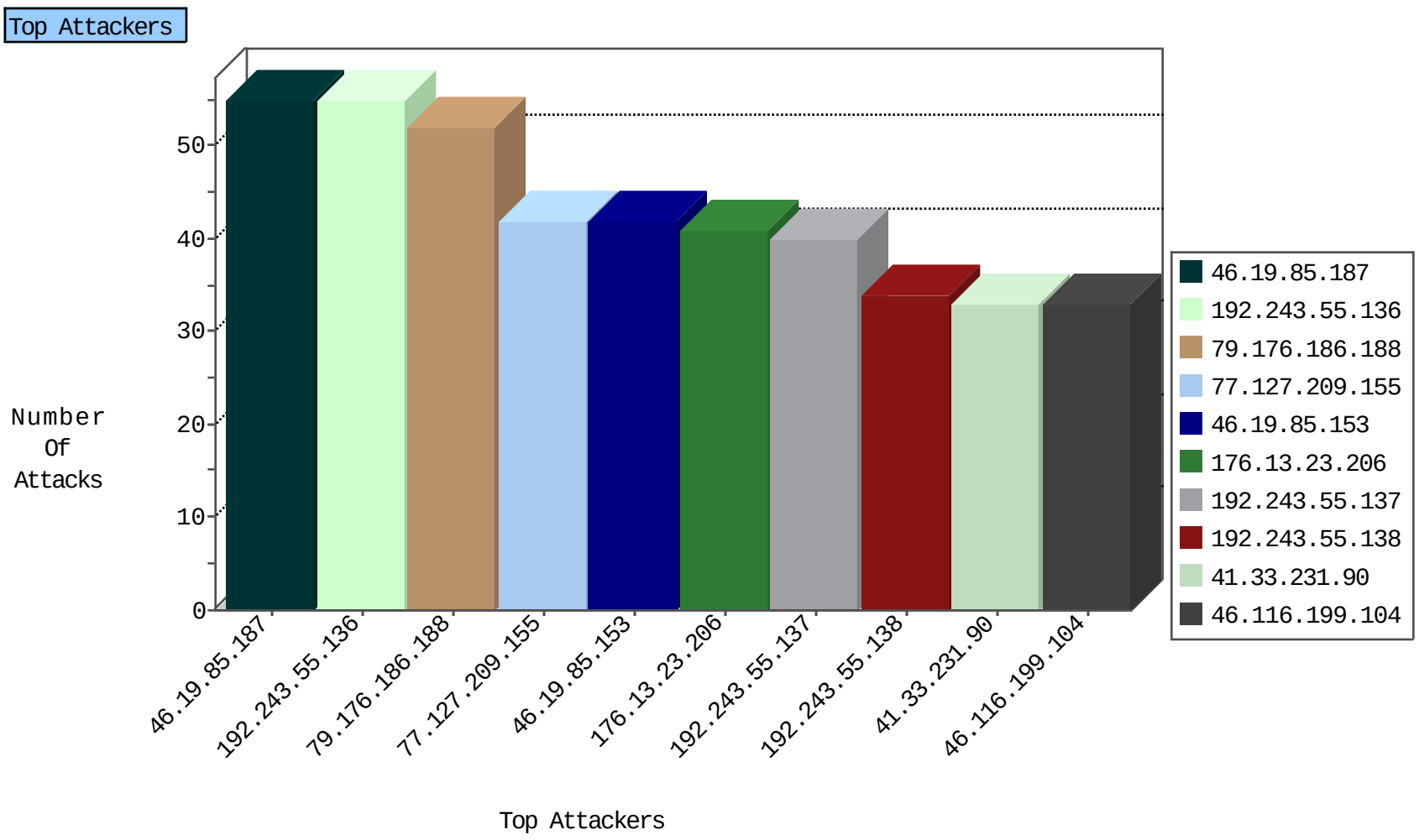
02-18-2016-21:04:09 to 02-18-2016-22:04:09

IDF Under Attack
Daily Report

Top Targets



Top Attackers



02-18-2016-21:04:09 to 02-18-2016-22:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
87.71.31.161	Israel	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
46.172.71.174	Ukraine	147.237.76.147	chinuch.aka.idf.il	L4 Source or Dest Port Zero	drop	1

02-18-2016-21:04:09 to 02-18-2016-22:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.111.81.211	Israel	147.237.0.34	tikshuv.idf.i	C1000212: HTTP: prefix 1.01 in the URL	Block	6
5.29.218.128	Israel	147.237.0.34	tikshuv.idf.i	C1000212: HTTP: prefix 1.01 in the URL	Block	2
51.255.207.28	United Kingdom	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	2
51.255.207.28	United Kingdom	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	2
136.243.152.18	Germany	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	2
136.243.152.18	Germany	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	2
79.176.209.54	Israel	147.237.76.31	nakchal.idf.i	C1000004: HTTP: options method (Microsoft)	Block	1
186.202.153.87	Brazil	147.237.76.30	himush.idf.il	19813: HTTP: WordPress Theme Divi Directory Traversal Vulnerability	Block	1
198.1.79.36	United States	147.237.77.234	halag.idf.il	19813: HTTP: WordPress Theme Divi Directory Traversal Vulnerability	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	1
66.249.64.185	Israel	147.237.0.34	tikshuv.idf.i	C1000212: HTTP: prefix 1.01 in the URL	Block	1
5.29.118.44	Israel	147.237.77.74	law.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1

02-18-2016-21:04:09 to 02-18-2016-22:04:09

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
132.252.173.4	147.237.77.216	Germany	dover.idf.il	GPL SCAN nmap TCP	2
180.97.106.37	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
37.26.149.253	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.199.182.150	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.103.34.100	147.237.8.46	Korea, Republic of	e.chinuch.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
180.97.106.162	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.161	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
149.78.154.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.151.52.253	147.237.0.34	Ukraine	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
2.52.181.158	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.76.196	China	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
180.97.106.162	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.162	147.237.8.27	China	e.madim.atal.idf.i	ET SCAN Potential SSH Scan	1

02-18-2016-21:04:09 to 02-18-2016-22:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
77.127.209.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
2.54.40.61	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.116.199.104	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
79.177.109.145	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
46.116.199.104	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	15
46.19.85.153	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
46.19.85.153	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.86.1	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
87.69.132.142	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	11
192.243.55.136	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
46.19.85.153	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
46.19.85.153	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
192.243.55.134	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
185.120.126.35		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.136	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
87.70.31.91	Israel	147.237.72.166	aka.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
79.180.139.72	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
5.102.228.100	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.161.152	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
192.243.55.138	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
84.228.170.38	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.102.9.107	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	5
5.102.254.140	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.102.254.228	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.137	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
66.102.9.117	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.243.55.137	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.136	Dominica	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
37.46.41.27	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
192.243.55.136	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
79.176.186.188	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
192.243.55.134	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
31.210.188.123	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
80.246.137.84	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.243.55.138	Dominica	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
77.127.114.108	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.214.242	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.132.11	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
192.243.55.133	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3

02-18-2016-21:04:09 to 02-18-2016-22:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	55
79.176.186.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
176.13.23.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
2.54.168.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
109.186.148.199	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
5.29.118.44	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 5.29.118.44	Block	5
2.54.142.228	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
2.54.169.146	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
17.138.58.138	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/apple-app-site-association	Block	2
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	2
109.253.138.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.120.98.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.182.174.30	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	2
79.176.186.152	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	2
79.182.174.30	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/xmlrpc.php	Block	2
66.249.93.174	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
77.127.114.108	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
176.13.15.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.109.49.139	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
2.54.14.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
79.176.12.245	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 79.176.12.245 (Open Mode)	None	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8967-he/refuah.aspx	Block	1
194.187.168.236	Poland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-	Block	1
79.182.162.78	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$117 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
212.85.108.202	Poland	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
73.226.77.42	United States	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method Â¬[[#0]][[#0]][[#0]]p;[[#23]]ÃœÂ‘ 0W'[[#31]]DÂ¹Â°ÃºÃªmCvÃ°ÂžFÂšÂ¸ AÂµÂŸÃ¿ÃªÂ²Â…/Ã¤Âš r_iÂ¡[[#2]]bRÂ˜IÃ¥Ã¼[[#30]]Â›KhvÃ—Â¥Ã“[[#6]]Â?Â°Ã·}[[#11]]Ã°Ã—Ã„ Ã?Â±	Block	1
37.26.146.201	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
87.71.31.161	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
79.176.100.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
73.226.77.42	United States	147.237.76.42	refuah.idf.il	Abnormally Long Request method	Block	1
197.38.197.170	Egypt	147.237.76.31	nakchal.idf.il	PHP Attempt	Block	1
8.37.71.71	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/&usg=alkjrhj05xqomjgixetmegk4tkuejhfehq	Block	1
212.85.108.202	Poland	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/xmlrpc.php	Block	1
77.125.113.226	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/images/0108-	Block	1
37.46.39.171	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
87.71.31.161	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	1
73.226.77.42	United States	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in Method Â¬[[#0]][[#0]][[#0]]p;[[#23]]ÃœÂ‘ 0W'[[#31]]DÂ¹Â°ÃºÃªmCvÃ°ÂžFÂšÂ¸ AÂµÂŸÃ¿ÃªÂ²Â…/Ã¤Âš r_iÂ¡[[#2]]bRÂ˜IÃ¥Ã¼[[#30]]Â›KhvÃ—Â¥Ã“[[#6]]Â?Â°Ã·}[[#11]]Ã°Ã—Ã„ Ã?Â±	Block	1
197.38.197.170	Egypt	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/xmlrpc.php	Block	1
109.253.146.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
50.62.208.36	United States	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
14.222.215.21	China	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/usercontrols/headerupper/	Block	1
77.125.113.226	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
37.187.114.171	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to /sap/hana/admin/	Block	1
93.172.240.219	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
197.38.197.170	Egypt	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1
73.226.77.42	United States	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in URL	Block	1
149.78.42.240	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1

02-18-2016-21:04:09 to 02-18-2016-22:04:09