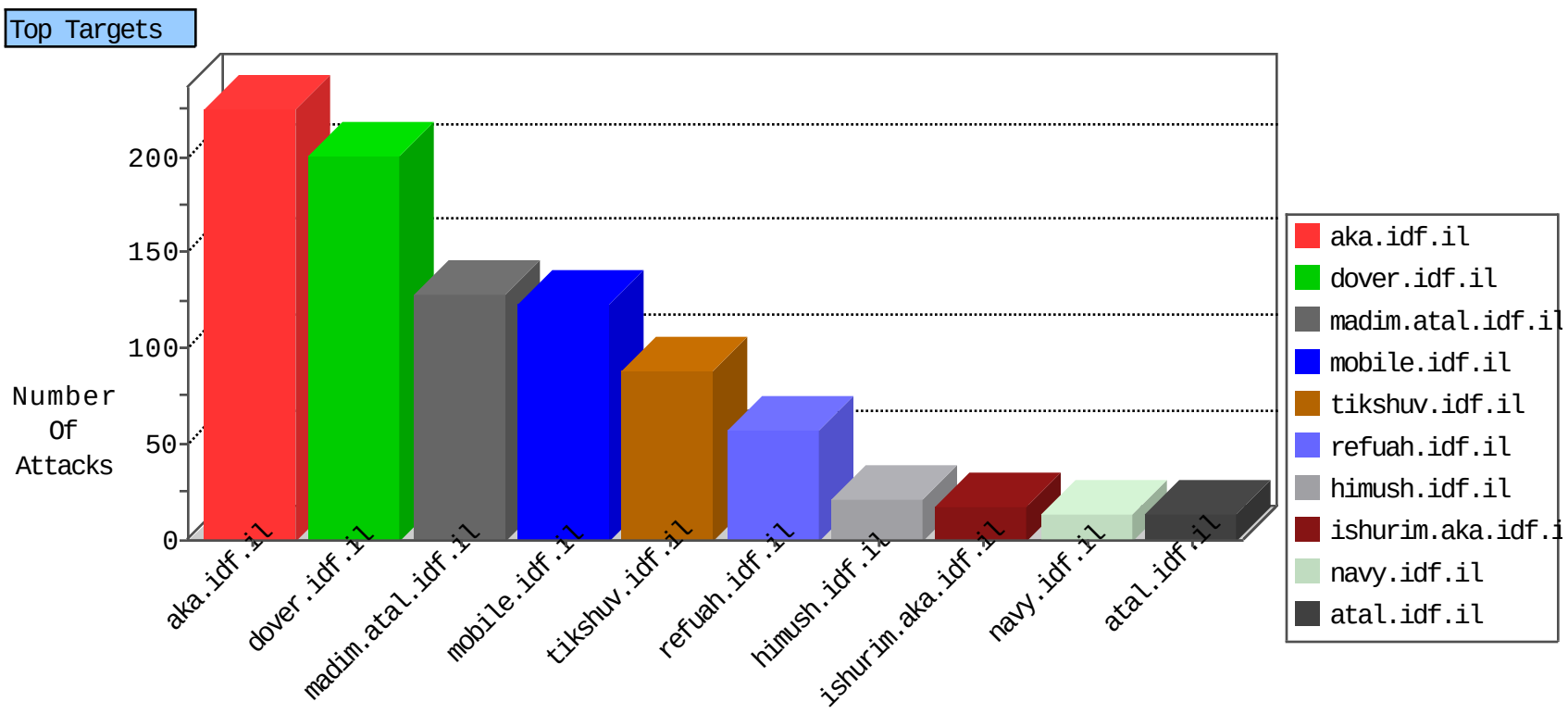
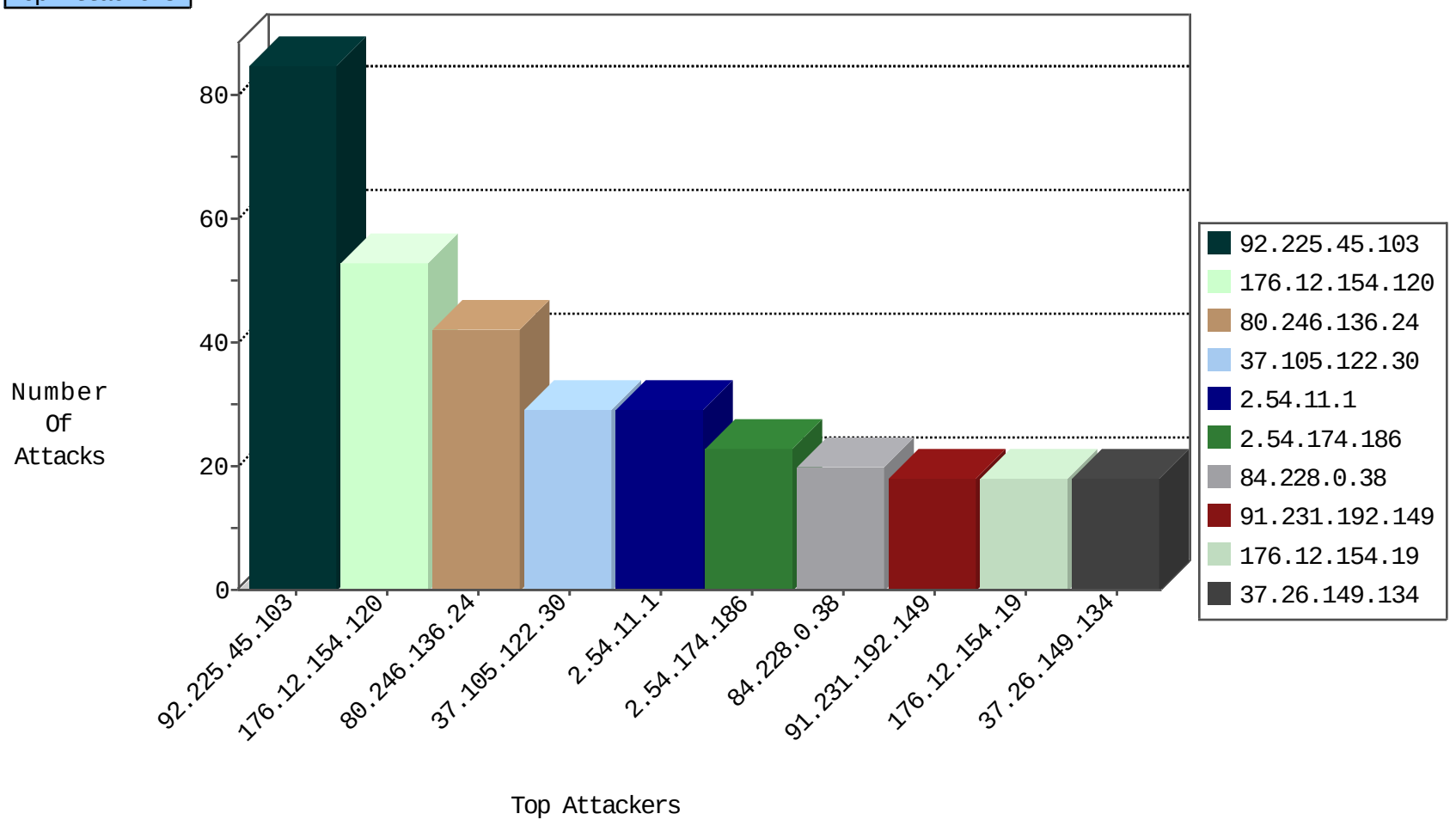
02-02-2016-12:04:07 to 02-02-2016-13:04:07

IDF Under Attack
Daily Report

Top Targets



Top Attackers



02-02-2016-12:04:07 to 02-02-2016-13:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
91.231.192.149	Israel	147.237.76.42	refuah.idf.il	JLM_Purple_Con_Limit_Http	drop	81
91.231.192.149	Israel	147.237.76.42	refuah.idf.il	JLM_Purple_Con_Limit_Tcp	drop	31
109.160.241.13	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
2.52.179.238	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
185.130.5.224		147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
185.130.215.3		147.237.77.216	dover.idf.il	L4 Source or Dest Port Zero	drop	1
185.130.5.224		147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
185.130.215.3		147.237.77.226	www.chamatz.aka.idf.il	L4 Source or Dest Port Zero	drop	1
185.130.215.3		147.237.76.196	e.sviva.idf.il	L4 Source or Dest Port Zero	drop	1
109.160.241.13	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
185.130.215.3		147.237.77.205	prisha.idf.il	L4 Source or Dest Port Zero	drop	1

02-02-2016-12:04:07 to 02-02-2016-13:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.105.122.30	Saudi Arabia	147.237.77.216	dover.idf.il	3886: HTTP: Cross Site Scripting in POST Request	Block	8
216.17.111.245	United States	147.237.77.19	law-forum.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1

02-02-2016-12:04:07 to 02-02-2016-13:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
37.105.122.30	147.237.77.216	Saudi Arabia	dover.idf.il	SQL Injection - Select From	9
37.105.122.30	147.237.77.216	Saudi Arabia	dover.idf.il	GPL WEB_SERVER /etc/passwd	4
87.69.246.20	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.65.183.112	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.110.36.73	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.80.196.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.74.107.254	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
168.62.238.153	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
50.204.188.142	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 3072	1
132.66.152.214	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.235.254.181	147.237.77.243	Turkey	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.146.185	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.139.164.143	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.154.62.66	147.237.77.216	Oman	dover.idf.il	portscan: TCP Distributed Portscan	1
84.111.38.78	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.108.60.33	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.139.6	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
62.219.21.30	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
168.62.238.153	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.51	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
121.201.27.61	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
91.214.5.128	147.237.77.216	United Kingdom	dover.idf.il	portscan: TCP Distributed Portscan	1

02-02-2016-12:04:07 to 02-02-2016-13:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
92.225.45.103	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	67
80.246.136.24	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
92.225.45.103	Germany	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	18
176.12.154.19	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	17
46.19.85.18	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
82.46.117.100	United Kingdom	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	12
176.12.154.216	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.60	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
94.230.93.232	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
94.230.93.200	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
84.228.0.38	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
84.228.0.38	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
5.22.129.99	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
185.32.179.242	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
94.230.93.191	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.69.88	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.11.1	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.66.109.191	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.11.1	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
79.180.163.253	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
94.230.93.175	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.64.2.166	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
94.230.93.136	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.11.1	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	6
37.26.149.134	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
2.54.174.186	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.11.1	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
80.74.100.131	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
2.54.174.186	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
2.54.174.186	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
176.12.154.221	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.54.174.186	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
85.64.2.166	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
176.12.154.221	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
84.228.0.38	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
80.246.139.197	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
5.102.254.151	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.7	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
85.130.223.17	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.7	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
37.26.149.134	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
65.55.210.115	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.32	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.202.232	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.230.93.143	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.72.212	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.130.223.17	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
176.12.154.66	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-02-2016-12:04:07 to 02-02-2016-13:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.12.154.120	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	53
2.54.184.1	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
37.26.149.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
176.12.154.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
37.105.122.30	Saudi Arabia	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 37.105.122.30	Block	7
2.54.172.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
37.26.146.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.12.155.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
81.218.245.1	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-he	Block	3
2.54.191.62	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
2.54.131.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
76.115.96.90	United States	147.237.77.74	law.idf.il	Suspicious Response Code	Block	3
109.66.109.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.46.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.12.154.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.12.154.13	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.131.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
192.117.135.216	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 192.117.135.216	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	2
46.19.86.96	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
5.29.146.213	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
176.12.155.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.78.80	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
2.52.138.9	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
31.154.161.187	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	2
176.12.154.66	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
37.26.149.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.136.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.13.39	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 2.54.13.39 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
74.82.47.4	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
156.172.43.239		147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1133-he/dover.aspx	Block	1
62.219.225.247	Israel	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/faq.aspx	Block	1
191.232.136.91	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/main/giyus/giyus/general.aspx	Block	1
95.135.13.241	Ukraine	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1072-he/nakhal.aspx	Block	1
79.181.217.210	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl71 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
176.12.154.122	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
169.229.3.91	United States	147.237.77.19	law-forum.idf.il	Illegal Byte Code Character in Method Â˜2*Ã—gÃ?Ã•(eTÂ®1}Â†Â³Â‡ iÂœ[[#27]]0Â-Â^npÃ¤h&ZÃ?Ã†OlÂªwÃ‹Â†K	Block	1
109.65.198.76	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
37.105.122.30	Saudi Arabia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/nosuchpage123	Block	1
218.161.34.107	Taiwan	147.237.76.42	refuah.idf.il	Parameter Type Violation PageNum in www.refua.atal.idf.il/1226-he/refuah.aspx	Block	1
2.54.13.39	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
176.12.154.26	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/step3.aspx	None	1
74.82.47.4	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
66.249.78.18	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/894-he/atal.aspx	Block	1
157.55.39.248	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/templates/qsystemform/	Block	1
37.26.148.157	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
95.135.13.241	Ukraine	147.237.76.31	nakchal.idf.il	Parameter Type Violation SortDir in www.nakhal.idf.il/1072-he/nakhal.aspx	Block	1
80.246.130.122	Israel	147.237.76.42	refuah.idf.il	Distributed Parameter Type Violation on www.refua.atal.idf.il/1518-he/refuah.aspx parameter ctl00$ContentPlaceHolder1$txtContent	Block	1

02-02-2016-12:04:07 to 02-02-2016-13:04:07